Software Engineering Institute

Investigating Advanced Persistent Threat 1 (APT1)

Deana Shick
Angela Horneman

May 2014

TECHNICAL REPORT
CMU/SEI-2014-TR-001

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0000855

Table of Contents

List of Figures

List of Tables

Acknowledgments

We would like to thank Michael Hanley and Timur Snoke, who guided us through the process of compiling this report; Jonathan Spring and Edward Stoner, who pulled data from internal databases that we used in our analysis; and Rhiannon Weaver, who helped us with the sample and statistics.

Abstract

In February 2013, Mandiant uncovered Advanced Persistent Threat 1 (APT1)—one of China's alleged cyber espionage groups—and provided a detailed report of APT1 operations, along with 3,000 indicators of the group's activity since 2006. This report analyzes unclassified data sets in an attempt to understand APT1's middle infrastructure: the system of hops, distribution points or relays, and the command and control (C2) servers that sit between APT1's victims and main C2 servers located overseas. To build that infrastructure, APT1 chose and exploited particular organizations to obfuscate communications while remaining in plain sight.

This analysis, based on data from IP addresses known to be associated with APT1 and domain names provided by Mandiant, was conducted using a combination of System for Internet Level Knowledge (SiLK) tools, Microsoft Excel, and custom Python scripts. The study detailed in this report can be replicated easily using available sources and tools. By combining key unclassified information, the authors successfully described a large, malicious network used to steal important information.

1 Introduction

Since Mandiant released its report regarding China's suspected cyber espionage unit, Advanced Persistent Threat 1 (APT1), in February 2013, there has been increased media attention on cyber capabilities in the international arena. Although the details of cyber missions are hidden under veils of secrecy, the footprints left behind during and after execution are increasingly apparent in various pieces of unclassified data. Our goal is to marry unclassified data sets to understand the infrastructure of APT1. We want to understand both what is necessary for APT1 to be successful in its mission and why the group chose particular machines as the vehicle for the exfiltration of sensitive data. This study uses IP addresses known to be associated with APT1, collected from the Joint Indicator Bulletins (JIBs) INC260425 and INC260425-2, and domain names provided by Mandiant. We analyzed this combined set against several unclassified data sets: the Internet Census 2012, Open Resolver list, Neustar GeoPoint data, and the Internet Storm Center data. We include indicator expansion algebra to best capture our process.

This study does not include targets; rather, it is aimed at the vast network of *middle infrastructure*, which we define as the pieces that sit between end targets and the home base. This middle infrastructure comprises intermediary command and control (C2) servers, malware servers, and hop points used to push sensitive information along to APT1. Our data begins with combining the JIBs and the reverse domain name server (rDNS) information from Mandiant's report [Mandiant 2013]. The resulting 1,386 IP addresses form our analysis domain.

2 Data Sources

2.1 JIBs INC260425 and INC260425-2

On February 18, 2013 and February 26, 2013, the U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) released two Traffic Light Protocol (TLP) Green documents of APT1 internet protocol (IP) addresses, hostnames, and second-level domains known to be associated with APT1 activity. Combining the two JIB IP sets [US-CERT 2013a, 2013b] into one was the first step of this study.

2.2 Internet Census 2012

The Internet Census 2012 is a project that scanned the IPv4 address space using the nmap Scripting Engine (NSE) between March and December 2012 [Unknown 2013]. The nmap open-source security tool is used to enumerate hosts on a network and compile a network map of them. As an nmap tool, NSE allows users to write unique scripts to use nmap for their individual needs [nmap.org 2013]. Instead of scanning a personal network, the creator of the Internet Census (identity unknown) used a personal NSE script to port scan the /0 address space. The creator conducted the scan by developing the Carna botnet that deployed a small binary onto a group of nonsecure sample machines [Unknown 2013]. These nonsecure machines were used to build a port scanner for the entire IPv4 address space. The botnet consisted of a central server for data collection and analysis, middle nodes to transmit large pieces of data to the central server, and many devices for data collection. The data collection machines scanned other machines via a slew of Python scripts from the binary on Telnet, port 23, which transferred data back to middle nodes. Those nodes would forward off the information to the main server for data collection and analysis [Unknown 2013].The data was released into the public domain in early 2013 for further research. The Internet Census contains 9.6 terabytes of data. The following types of scans were performed and saved by the conductor of the Internet Census, but not necessarily used in our analysis:

- Internet Control Message Protocol (ICMP) ping: When an ICMP ping scan is sent to a device, it measures the time the device takes to return a response. The response will return one of the following: network unreachable, host unreachable, communication administratively prohibited, alive, alive from A.B.C.D, or unreachable from A.B.C.D. For the purposes of the IPv4 scan, the ICMP ping scan results tell if the address was reachable and, if not, what IP address was used for the scan. This scan sent an ICMP ping to every address every few days [Unknown 2013].
- reverse DNS (rDNS) scan: This scan queried every domain name for the IPv4 address space, sending queries to the top 16 DNS servers for each IP address. Once compiled, the DNS records were sent back to the collection server [Unknown 2013].
- service probes: Service probe scans look for responses on various ports that can be attributed to certain services. The probed IP address would return a state of 1 for open, 2 for open reset, 3 for open timeout, 4 for closed reset, and 5 for timeout. Only IP addresses returning a state of 1 provide any information in the request. Although 175 billion probes were saved, only a small minority of the data showed any useful information [Unknown 2013].
- host probe: Host probe scans relay to a researcher regardless of whether the IP address exists [Unknown 2013].

- SyncScan queries: SyncScan queries inform a researcher if a particular IP address has open, open-filtered, or closed ports. This scan contains every IP address in the IPv4 address space. The SyncScan data provided in the Internet Census is divided by CIDR /8 netblock; each /8 netblock contains its own unique file [Unknown 2013]. The data lists all the open, open-filtered, and closed ports associated with each IP address in the /8 netblock. In many cases, the IP address in question has all three statuses and therefore three different lines in the file. The SyncScan query also provides the type of packet sent to a particular IP address, a UNIX timestamp for when the data was received, and the type of packet sent to each port. Table 1 shows examples of an APT1 IP address listing in an Internet Census SyncScan file.

Table 1: SyncScan Examples

IP Address	Timestamp	Status	Reason	TCP/UDP	Open Ports
38.104.203.222	1334544300	open	syn-ack	tcp	1723,3389
38.104.203.222	1335746700	closed	reset	tcp	20,21,22,23,25,53,80,110,111,143,443,993,995, 3306,5900,8080

- TCP/IP fingerprint: This scan attempts to gather information that will identify the type of device and the operating system (OS) running on the machine [Unknown 2013]. It appears that the nmap tool used in the scan was modified to store the response used in the determination of the fingerprint. The standard nmap program captured the OS results but did not keep the actual response used in fingerprinting. The OS results were not provided in the Internet Census data. Like the SyncScan queries, the fingerprint data is divided by CIDR /8 netblock; each /8 netblock contains its own unique file.

  Table 2 shows examples of APT1 IP address listings in a fingerprint file.

Table 2: Fingerprint Examples

IP Address	Timestamp	Fingerprint
161.58.177.111	1346465700	SCAN(V=6.01%E=4%D=1/2%OT=21%CT=22%CU=%PV=N%DC=I%G=N%TM=19DB3%P=mipsel-openwrt-linux-gnu),SEQ(SP=105%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=0),OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS),WIN(W1=4000%W2=4000%W3=4000%W4=4000%W5=4000%W6=4000),ECN(R=Y%DF=N%TG=80%W=4000%O=M5B4NW0NNS%CC=N%Q=),T1(R=Y%DF=N%TG=80%S=O%A=S+%F=AS%RD=0%Q=),T2(R=Y%DF=N%TG=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=),T3(R=Y%DF=N%TG=80%W=4000%S=O%A=S+%F=AS%O=M5B4NW0NNT00NNS%RD=0%Q=),T4(R=Y%DF=N%TG=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=),T5(R=Y%DF=N%TG=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=),T6(R=Y%DF=N%TG=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=),T7(R=Y%DF=N%TG=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=),U1(R=N),IE(R=Y%DFI=S%TG=80%CD=Z)

IP Address	Timestamp	Fingerprint
71.8.243.14	1346481900	SCAN(V=6.01%E=4%D=9/1%OT=21%CT=26%CU=43452%PV=N%DS=15%DC=I%G=N%TM=5041B319%P=mipsel-openwrt-linux-gnu),SEQ(SP=BF%GCD=1%ISR=C1%TI=Z%CI=Z%TS=7),SEQ(CI=Z),OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11),WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0),ECN(R=Y%DF=Y%T=3C%W=16D0%O=M5B4NNSNW7%CC=Y%Q=),T1(R=Y%DF=Y%T=3C%S=O%A=S+%F=AS%RD=0%Q=),T2(R=N),T3(R=Y%DF=Y%T=3C%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11NW7%RD=0%Q=),T4(R=Y%DF=Y%T=3C%W=0%S=A%A=Z%F=R%O=%RD=0%Q=),T5(R=Y%DF=Y%T=3C%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=),T6(R=Y%DF=Y%T=3C%W=0%S=A%A=Z%F=R%O=%RD=0%Q=),T7(R=Y%DF=Y%T=3C%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=),U1(R=Y%DF=N%T=3C%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G),IE(R=Y%DFI=N%T=3C%CD=S)

- traceroute: This scan provides the path a data packet took from a source address to the destination.

Our analysis focuses on the TCP/IP fingerprints and SyncScan data from the Internet Census. We did not look into host probe or ICMP ping scans because the SyncScan query data contains the same information. If an IP address was unreachable as per the ICMP ping scan, the SyncScan query data of that IP address would return only closed ports. Additionally, the time it took for the packet to return a response was not necessary for our analysis. For purposes of our data collection, we were only interested in open ports, further making the ICMP ping and host probe data unnecessary.

Although we did expand our APT1 indicators to include domain names, we did not use the rDNS records found within the Internet Census. The information in that source only used the top 16 name servers; we wanted to ensure we had a full picture for our APT1 data sets and instead chose a different source for this information.

The service probe scan files contain the most information in the Internet Census. Unfortunately, only a handful of our IP addresses returned information when probed. After going through the results of our probed IP addresses manually, we found no interesting information that either confirmed other pieces of our data or led us down new paths.

The traceroute information did not return any results for the APT1 IP address set, either as start/endpoints or hop points within other traceroutes.

There are some ethical considerations in using the Internet Census 2012 data. Since it was obtained through a botnet doing network scans without permission, should researchers use it? In answering this question, it is important to understand which data is lacking and where else it could be found.

The Internet Census 2012 data set contains machine information, not personally identifiable information (e.g., Social Security numbers, birthdates, places of birth). While some names, email addresses, and phone numbers occur in rDNS and service probe results, they are not considered private information. The email addresses and phone numbers all appear to be valid and point to IT helpdesks; the service probes stored all responses, which were occasionally error messages from the probed machines or their proxies or firewalls. Furthermore, the information in the Internet Census data set is not an up-to-date picture of the internet as a whole or its individual components. The devices connected to the internet change frequently from being connected and disconnected, installing software patches and upgrades, and implementing firewall configuration changes. This means the data set only provides an accurate picture of its components at the time of the nmap scans.

Whether the information from these scans is public or private is another question. Some of the information is public so the internet can work as it should, while other parts could be obtained in other manners. The main difference between the Internet Census 2012 data set and other similar data sets is the breadth of the information released.

2.3 Security Information Exchange at the Internet System Consortium (SIE@ISC): rDNS Data

The Internet Census data did not provide us with comprehensive rDNS information associated with each IP address because information was only pulled from the top 16 name servers. To get a wider range of results, we used the passive domain name server (pDNS) records collected by the Security Information Exchange at the Internet System Consortium (SIE@ISC) for the transformation of IP addresses to domain names and vice versa [Ziegast 2010]. These domain names or IP addresses were pulled during a time frame similar to that of the Internet Census.

2.4 Mandiant's Report on APT1: *Exposing One of China's Cyber Espionage Units*

On February 18, 2013, Mandiant published its report exposing APT1, which has been operational since 2006 and successfully compromised a slew of U.S. targets in sectors privy to Chinese government interests [Mandiant 2013]. Mandiant analyzed patterns in the security breaches of its clients and tracked APT1's activities to four networks in the Pudong New Area of Shanghai. APT1 maintained a stronghold in its target's infrastructure for months and, in some cases, for years. Its success is attributed to being a state-sponsored secret of the Chinese government, who provide the group ample funding for cyber missions [Mandiant 2013]. In its report, Mandiant provided the APT1 attack lifecycle, the types of software used to exploit the targets, and reoccurring identities found in the company's data collection [Mandiant 2013]. Along with that report, Mandiant released 3,000 indicators of APT1 activity that included descriptions of APT1's malware, MD5 hashes of the malware, self-signed secure sockets layer (SSL) certificates, indicators of compromise (IOCs), and fully qualified domain names (FQDNs) [Mandiant 2013].

The Mandiant report sparked our interest in APT1 and was an excellent resource when we questioned APT1's motives and attack strategy. The information provided in the report's appendices was invaluable and gave us many additional data points in our research. By using the FQDNs, in particular, we expanded our APT1 IP address set and, thus, were able to get a fuller picture of APT1 activity.

2.5 Open Resolvers Data

Open resolvers, which are best known for amplifying distributed denial of service (DDoS) attacks, were recently in the public eye when on March 27, 2013, Spamhaus—an organization that tracks internet spammers—was hit in the biggest DDoS attack in history [Leyden 2013]. The Open Resolver data set, provided by the Open Resolver Project at openresolverproject.org, is the list of DNS resolvers that have been configured to allow recursive DNS requests [Open Resolver Project 2013]. Since the end of March 2013, new lists have been released weekly. We used the April 7, 2013 list in this study.

2.6 Neustar GeoPoint Data

Neustar GeoPoint provides two types of data published monthly: geo-location information and routing data for IP addresses [Neustar 2013]. We used the available files closest to the Internet Census time frame to determine the country and state (or province if outside the United States) of origin for analysis.

The Neustar data uses the term *route type* as others use *media type*: the physical device that connects machines to the wider internet, not the logical application of internet routing. The Neustar route types include the connection method to the internet, like a fixed or satellite connection. Some route types are also associated with connection types, which indicate the connection medium, such as fiber optic, digital subscriber line (DSL), or leased line. A category is defined as unknown for both routing and connection type, indicating that Neustar did not have data on a particular IP address. For purposes of the study, we maintained consistency with the Neustar terms for both the geo-location and routing information.

2.7 Internet Storm Center Data

The Internet Storm Center DShield data provides a sample of internet traffic containing source IP addresses and destination ports that were blocked on any particular day [Internet Storm Center 2013]. We used information from January 1, 2012 through December 31, 2012 for our analysis. This data set did not provide information that was useful in determining a profile, but it was interesting to note that the most frequently blocked ports were also those that were most often open in the Internet Census. Since the Internet Storm Center data is just a daily sampling of occurrences, it might have been useful if the JIBs contained information for more of the IP addresses. Also, preserving the destination IP address in the data set might have enabled us to better determine how each IP address from the bulletins was being used.

2.8 Other Data Sources

Several different data sources went into determining who owned the IP addresses in the lists. Those addresses were associated with autonomous system numbers (ASNs) using a combination of data from the University of Oregon Route Views Project and the Réseaux IP Européens (RIPE) Network Coordination Centre Routing Information Service (RIS). We used information from potaroo.net to determine ASN ownership and several search engines to identify the line of business for those owners.

3 Data Issues

3.1 Available Data Is a Partial View of APT1 Operations

Although it includes information from the JIBs and the pDNS records that are linked to Mandiant’s domain names, our data is not a full representation of APT1 activities; rather, it is only a snapshot of how the IP address devices looked at a particular point in time. We also believe there are many more compromised IP addresses from around the world that we do not know about.

3.2 Timeline of Data

APT1 has been operational since 2006. We do not have enough information from our collective resources to establish a timeline for the IP addresses found in the Mandiant report or the JIBs. The combined IP address set could represent active IP addresses that APT1 used continually since 2006, or it could be a set active for only a period in time anywhere between January 2006 and February 2013.

The Internet Census data gave us a time frame of several months for our analysis: March to December 2012. To mitigate uncertainty in our analysis, we used the available data in each data source that corresponded most closely with the March to December time frame.

3.3 Internet Census Data Constraints

Although the Internet Census data provided great insight into the IPv4 address space, we are limited to only several months of data. We cannot track changes over time with this data. We confront the same issue with the timeline of the JIB and Mandiant IP addresses; we assume the APT1 IP addresses were actively used during the Internet Census time frame.

The Internet Census is very rich in content, but we found some issues while working with it. Many scans repeated during the Internet Census, providing us with conflicting information. This was especially true in regards to the TCP/IP fingerprint data. While analyzing that data, we found that a minority of APT1 IP addresses contained two unique fingerprints. In order to resolve these conflicts, we chose the fingerprint with the highest percentage match of the two to use in our analysis. The Internet Census is not perfect, but it does provide very rich data in the public domain.

4 Tools

Our analysis was aided by various Linux commands, the System for Internet Level Knowledge (SiLK), Excel, and several Python scripts. The Linux commands `grep`, `awk`, and `cut` helped extract the needed data from the Internet Census data files, as well as the Neustar GeoPoint file. SiLK provided the ability to efficiently combine, intersect, and difference the data, as well as to quickly create IP address sets. Excel was very useful in sorting and visualizing data and deriving statistics. Python scripts were created to turn TCP/IP fingerprint scan results into the OS or device those fingerprints represent. We chose SiLK, Linux, and Python for their robustness and availability to others wanting to do similar analysis. We chose Excel because it is used extensively, gives us the ability to quickly create tables and charts, and allows us to combine data from various sources in an easily readable format.

4.1 Linux Commands

Various Linux commands provided the ability to retrieve the relevant APT1 data from the large text files making up much of our data sets. The `grep`, `awk`, and `cut` commands were especially helpful in preprocessing the data files. Because the Internet Census data files are so large (ranging from several hundred MB to several GB), we used these commands to pull out and format the relevant entries for analysis or further preprocessing with SiLK, Excel, or Python scripts. Occasionally, we ran into memory-usage problems with the `grep` command that required us to run certain commands outside of normal business hours.

4.2 SiLK

SiLK is a set of network-traffic, flow-analysis tools created by the Network Situational Awareness team, which is part of the Carnegie Mellon® Software Engineering Institute's CERT Division [SEI 2013]. We used SiLK for its speed and ability to translate IP lists into flow sets for comparisons and combinations. The commands `rwsetbuild`, `rwsetcat`, `rwsettool --intersect`, and `rwuniq --pmap` were most helpful. We used the `rwuniq --pmap` command with several custom pmap files built to allow efficient attribution of IP addresses to other data, such as geo-location and routing types.

4.3 Excel

Excel's `VLOOKUP`, `CONCATENATE`, and various sorting and filtering functions enabled quick concatenation of the data from the various data sources. The `COUNTIF`, `COUNTIFS`, and `SUMIFS` functions allowed us to efficiently summarize data. Installing the Data Analysis add-in enabled us to correlate some of the data. Excel had some memory issues when creating tables for port analysis using the `VLOOKUP` function. As mitigation, we did sections of the data at a time, and then copied and pasted the results as values into a different table. That way, we kept the number of cells containing functions in any one workbook to a minimum.

® Carnegie Mellon is a trademark owned by Carnegie Mellon University.

4.4 Python Scripts

We used Python to code a script comparing the TCP/IP fingerprints from the Internet Census data to the nmap-os-db file to determine the OS identity for each available IP address. The script opens a tab-delimited fingerprint file and outputs a tab-delimited identity file. Due to differences in how Microsoft Windows and Linux/UNIX machines handle carriage returns and line feeds, we created one script for use on Windows machines and one for Linux/UNIX-based machines. We stayed consistent with the nmap fingerprint labels and used those terms in our analysis.

5 Indicator Expansion

5.1 Defining Variables and Expansions

Indicator expansion allows us to capture how we arrived at conclusions given our data sets and provides readers the best step-by-step process of our data manipulations in hopes they can recreate our data elsewhere.[1] The algebra first defines the variables, which are uppercase letters. For example, IP addresses are denoted as I. To go from IP addresses to domain names, D, the process is denoted by two variables side by side. The algebra is read from left to right.

$$ID$$

5.2 Defining the Same Type of Data from Two Sources

To denote data sets that contain the same type of data from different sources, the variables will have a subscript for the data source. For example, if we have two IP address sets, one from x and another from y, the variables will be expressed as the following:

$$I_x$$

$$I_y$$

To denote that the IP sets are conjoined, the variables will be connected with a plus sign, $+$. All the transformations to the conjoined IP address set are done to both sets as if the sets were concatenated:

$$I_x+I_y$$

5.3 Defining the Range of a Data Set

At times, our data requires excluding a particular percentage of the data from the data set. To allow this transformation, our data must reflect a range that is included, 75%-100%, along with denoting the data as being a percentage by using p instead of %. For example, if we wanted to exclude any IP addresses with fingerprints, F that contains less than a 75% match, the algebra would be the following:

$$F_{p75}$$

A similar method is used for non-percentage ranges. For example, if we want to show fingerprints that occur between two and four times, the algebra would be

$$F_2^4$$

[1] For more information, see *An Algebra for Describing the Steps in an Indicator Expansion*, written by J. M. Spring and scheduled to be published in October 2013 as part of the eCrimes Research Summit proceedings.

6 Method

Each step of our analysis is reflected using indicator expansion.[2] We saved all our source data and data manipulations onto a shared server. Each expansion explained in the section below is shown in the order of how we analyzed the data and is an independent analysis.

6.1 Variables Used

Table 3 contains a list of the variables used in this study and their descriptions.

Table 3: Indicator Expansion Variables

Variable	Description
A	autonomous system number
C	country
D	domain name
F	fingerprint
I_j	IP addresses in the JIB
I_m	IP addresses associated with Mandiant domain names
I_n	IP addresses in the non-routable IP space
M	malicious code
N	service probes returning a state of 1
O	open resolvers
P	open ports
R	routing data
S	IP address set of IPv4 sample

6.2 APT1 Address Set

We provided an explanation of how we analyzed our data along with the commands used for our analysis. Note that the dollar symbol ($) used at the beginning of a command indicates the bash prompt and a new command.

6.2.1 I_j: JIBs' IP Addresses

The JIBs dated February 18, 2013 and February 26, 2013 contained 855 IP addresses known to be associated with APT1 malicious activity. To streamline our analysis, we first combined the IP addresses found in both JIBs into one text document called Ij.list and then turned that document into a SiLK set for use later in analysis through this command:

```
$ rwsetbuild Ij.list Ij.set
```

[2] For more information, see *An Algebra for Describing the Steps in an Indicator Expansion*, written by J. M. Spring and scheduled to be published in October 2013 as part of the eCrimes Research Summit proceedings.

- From this large, concatenated document, we created a second file, putting each IP address into regular expression notation, `^127\.0\.0\.1[[:blank:]]`, in order to use the `grep -f` command later in our analysis. The file was called Ij_reg.list.
- We manually divided the concatenated list into smaller, individual files based on the Classless Inter-Domain Routing (CIDR) /8 netblock for each IP address. This step was necessary because the Internet Census data was divided already by /8 netblocks and searching through each file in some of the scan data for all the IP addresses was inefficient and caused memory issues.

6.2.2 I_jD: IP Address Set in JIB to Domain Names

To execute this expansion, we ran a pDNS search on I_j to get a list of domain names. Once we received the results, we associated the IP address with its domain name and saved the combination into a single Excel document. We used the Excel `SORT` command and its filtering functionality to analyze the domain names.

6.2.3 $I_m = D_m I\text{-}I_n$: Mandiant IP Address Set

Mandiant published a list of FQDNs associated with APT1 activity as an appendix to its report. We performed an rDNS search via the SIE@ISC to retrieve the IP addresses, saving the associated IP addresses with their corresponding domain names into a single Excel document. Any non-routable IP address returned from the search was not included in the final list. The retrieved IP addresses were saved into a file called Im.list that we turned into a SiLK set for use later in analysis through this command:

```
$ rwsetbuild Im.list Im.set
```

- There were 622 IP addresses in total after the rDNS lookup.
- From the Im.list document, we created a second file, putting each IP address into regular expression notation, `^127\.0\.0\.1[[:blank:]]`, in order to use the `grep -f` command later in our analysis. The file was called Im_reg.list.
- We manually divided the concatenated list into smaller, individual files based on the CIDR /8 netblock for each IP address. This step was necessary because the Internet Census data was divided into individual files for each /8 netblock for each data set. We put each IP address into regular expression notation to use the `grep -f` command later in our analysis.

6.2.4 I_j+I_m: Union of Mandiant and JIB IP Address Sets

We took the 855 IP addresses from the I_j IP address set and the 622 from the I_m IP address set and combined them into one file with the associated domain names for each IP address, making sure duplicates were removed.

- There are 1,386 IP addresses in the Ij+Im set.
- We made several different files from this data to use with the different tools and commands used for analysis.
  - We retained a file with the IP addresses in standard notation in case we needed to refer back to the original set for any reason. This file was called Ij+Im.list.
  - Using SiLK's `rwsetbuild` command, we created a set of these IP addresses to aid in our analysis and use with other SiLK commands:

    ```
    $ rwsetbuild Ij+Im.list Ij+Im.set
    ```

- We created a file called Ij+Im_reg.list that contained the IP addresses in regular expression notation to use with `grep -f` commands.

6.2.5 Internet Census Data

The bulk of our analysis came from the Internet Census and its TCP/IP fingerprint and SyncScan data. We needed to augment certain types of the data in order to return the information we needed. These changes are outlined in the sections below, along with how we performed the analysis.

6.2.5.1 I_j+$I_m$$F_{p75}$: Fingerprints of the I_j+I_m Set Given a 75% Match

The I_j+I_m IP addresses separated into CIDR /8 netblocks were used to find the fingerprints. We used the following command to run the I_j+I_m netblock sets against the corresponding netblock found in the fingerprint data:

```
$ grep -f Ij+Im_reg.list X > Ij+ImF_X.txt
```

The `X` is the netblock in the Internet Census data, which is how the fingerprint files are named (the files have no file extensions). Upon finding the fingerprints for all the netblocks, we concatenated them into a single file using the command below:

```
$ cat * >> all_Ij+ImF.txt
```

We ran the file through our Python script to give us usable data as shown in Table 4. We put the corresponding fingerprint data into our working Excel document containing the I_j+I_m IP addresses and domain names. Using primarily the `SORT` and `COUNTIF` commands in Excel, we categorized and counted the various firewall, switch, gateway, and OS types.

Table 4: Fingerprinting Script Results

IP Address	%Match	Description of Operating System Type
161.58.177.111	0.825049702	Microsoft Windows Server 2003 Enterprise Edition SP2
71.8.243.14	0.926865672	Linux 2.6.32

It is important to note that the resulting fingerprint match string comes directly from the nmap database file. This means there may be some ambiguity in the resulting match. For instance, some fingerprints will match the string “Microsoft Windows Server 2003 SP2,” while others may match “Microsoft Windows Sever 2003 Service Pack 1 or 2.” For the second instance, the fingerprint was not specific enough to match the particular SP2 template, but it did match a template that belongs to either service pack 1 or service pack 2.

6.2.5.2 P: Internet Census Data Containing Only Open Ports

The SyncScan data found in the Internet Census was one of the most important pieces to this study. The data contains lists of open, open-filtered, and closed ports for all IP addresses in the IPv4 address space. To help us extract the APT1 data, we found it helpful to manipulate the SyncScan data before using it. We created a file listing each IP address in the IPv4 space containing only open ports to streamline analysis using the following command:

```
$ grep "[[:blank:]]open[[:blank:]]" * > syncscan_open.list
```

Then, we used the command below to remove the timestamp and the syn-ack TCP/UDP fields associated with the open port list:

```
$ cut -f1,6 syncscan_open.list >  P.list
```

6.2.5.3 I_j+I_mP: Port Analysis

We put the I_j+I_m IP addresses into regular expression notation and concatenated them into one document to find open ports. We used the command below to pull the list of open ports associated with each IP address in I_j+I_m:

```
$ grep –f Ij+Im_reg.list P.list > Ij+ImP.txt
```

- Once all the open ports were returned, we changed the delimiters in the file to be semicolons instead of commas using the Replace function in a normal text editor. We did that to ensure that any program we used for analysis would interpret the ports as individual values and not one long number.
- Using Excel, we manipulated the data to repeat the IP address with each associated open port to best analyze the data:
  - I_j+$I_m$$P_{20}$, I_j+$I_m$$P^{15}_{10}$,I_j+$I_m$$P^{9}_{5}$;$I_j$+$I_m$$P^{3}_{1}$ broke down the instances of IP addresses having various ports running by 20+ times, 10-15 times, 5-9 times, and 1-3 times.
  - The Excel `VLOOKUP`, `COUNT`, and `COUNTIF` commands aided our analysis.
  - Pivot tables helped us visually understand the data.
  - We plotted the distribution of open ports.
- Once we found all the open ports, we ran pair correlations to identify any unusual port pairing that occurred frequently in the data set.

6.2.5.4 N: Service Probes Returning a State of 1

The service probe data that we found in the Internet Census was very intriguing for our APT1 analysis. We hoped to find interesting data buried in the response to the service probes for the I_j+I_m set. To find that data easily, we created a SiLK IP address set that contained all the IP addresses returning a response of 1 to a service probe. The commands were

```
$ grep “[[:blank:]]1[[:blank:]]” */* > serviceprobe_1.list

$ cut –f1 serviceprobe_1.list > serviceprobe_1_IPS.list

$ rwsetbuild serviceprobe_1_IPS.list serviceprobe_1_IPS.set
```

6.2.5.5 I_jN: Service Probe Data

Using SiLK, we found the intersection between I_j and N using the command below:

```
$ rwsettool --intersect Ij.set serviceprobe_1_IPS.set | rwsetcat | sort \
        > Ij_sp1_intersection.txt
```

Once the intersection returned, we broke these IP addresses into CIDR /8 netblocks, resulting in four different files. We used the command below to pull out the responses associated with each IP address from the service probe data. The `X` is the netblock in the Internet Census data, which is how the service probe files are named (there are no file extensions). The `Y` represents the names of each of the four separate files created from the intersection.

```
grep –f Y */X > Ij_sp1.list
```

- 17 IP addresses returned information from the service probe scans.
- We analyzed the resulting search data manually in Excel.

6.2.6 I_j+I_mA: Autonomous System Numbers (ASNs)

SiLK enabled us to make pmap files and then use the `rwtuc` command to find the ASNs associated with each IP address. The pmap files contained just the ASNs associated with IP addresses.

```
$ rwpmapbuild --in=IP_ASN --out=IP_ASN.pmap
```

The IP_ASN file was created based on information from the Oregon Route Views Project and the RIPE Routing Information Service, and contains associations for the advertised IP address space. Once the pmap file was created, we used the command below to associate the APT1 IP address list with the appropriate ASN:

```
$ rwtuc --field=sip Ij+Im.list | rwuniq --pmap-file=asn:IP_ASN.pmap -- \
      field=src-asn --no-col > Ij+ImA.txt
```

- After determining the ASN for each IP address, we mapped the numbers to the registered companies via a dictionary file created from potaroo.net data.
- We did not combine subsidiary companies into the parent company or acquired companies into their new ownership.
- We manually researched the services provided by the ASN owners, such as internet service, hosting provider, education, or government.
- We used Excel to analyze the IP addresses and their corresponding ASNs.
- We used the SORT and FILTER tools, and the `COUNTIF` and `VLOOKUP` commands as needed to analyze the data.
- We used Pivot tables to examine visually how many IP addresses were associated to the same ASN.

6.2.7 I_j+I_mR and I_j+I_mC: Routing Data and Country Code

Instead of using ASN registration to determine country code, we decided to use Neustar data to determine the routing type and country code because it is more accurate. The Neustar data includes an address range, country code, city, and state where this address range is located, and a routing and connection type. The routing type is associated with the connection type (fiber, DSL, etc.). If there was no routing type but a connection type was listed in the file for an IP address range, we ignored the connection type in our analysis, cut the IP address ranges and the routing data, and then used SiLK to make a pmap. Next, we replicated the process containing city and state, and once again used SiLK to create a pmap. We used these commands:

```
$ gzip -dc neustar.csv.gz | cut -d"," -f1,2,5 | awk -F"," '{print $1 " " \
      $2  " " $3}' | awk -F"\"" '{print $2 " " $4 " " $6}' | grep -v \
      "start" | rwpmapbuild --in=- --out=routingConnection.pmap
$ gzip -dc neustar.csv.gz | cut -d"," -f1,2,5 | awk -F"," '{print $1 " " \
      $2 " " $3}' | awk -F"\"" '{print $2 " " $4 " " $6}' | grep -v \
      "start" | rwpmapbuild --in=- --out=countryState.pmap
$ rwtuc --field=sip Ij+Im.list | rwuniq --pmap- \
      file=route:routingConnection.pmap --field=src-route --no-col > \
      Ij+ImR.txt
```

```
$ rwtuc --field=sip Ij+Im.list | rwuniq --pmap- \
       file=country:countryState.pmap --field=src-country --no-col > \
       Ij+ImC.txt
```

Upon completion, we concatenated the IP addresses and the pmap data into a single tab-separated document for analysis. We used Pivot tables, and Excel's SORT and FILTER tools and `COUNTIF` command for the data analysis.

6.2.8 I_j+I_mO: Open Resolvers

The Open Resolver data was provided in a gzip file. Using these commands, we unpacked the file, created an IP address list, and then built a SiLK set:

```
$ gzip -dc open_resolvers.out.gz | grep ":0:1:[0-9]" | cut –d":" –f3 \
       > open_resolvers.list
$ rwsetbuild open_resolvers.list open_resolvers.set
```

Next, we used SiLK to find the intersection between the I_j+I_m set against the Open Resolver List and marked in our working document which IP addresses were open resolvers:

```
$ rwsettool --intersect open_resolvers.set Ij+Im.set | rwsetcat \
       | sort > Ij+ImO.txt
```

6.2.9 I_jDM: Malicious Code

Using runtime analysis efforts from CERT, we associated malicious code hashes with the domain names from the I_j set:

- We took the domain names provided in I_j and ran them against metadata from CERT's runtime analysis efforts to get the domain names known for hosting malicious code on their networks.
- Then, we reviewed these results and found the intersection between the malicious code domains provided by the metadata and the malicious code hashes in the Mandiant report.

6.3 IPv4 Address Sample

We created an IPv4 sample to use as a baseline for comparison with the I_j+I_m data set findings. If the findings were similar to what we found in the IPv4 sample, we would have to assume that our hypothesis (APT1 has specific requirements for its infrastructure) is incorrect. Differences in the findings between the two data sets would bolster our theory. Our sample did not include private, multicast, or loopback IP addresses. We found that between 5.5% and 7.5% of our sample IP addresses were not advertised at any given time during the March to December 2012 time frame.

6.3.1 S: Sample Set

We first made an IP address set of the entire IPv4 address space with SiLK called all_ips.set. This set excluded any reserved IP address space. We then used SiLK to create a random sample set of IP addresses from the entire IPv4 IP set. The sample size was 100,000 to give us a good picture of the IPv4 space and to ensure that our findings were a representative portion of the address space and acceptable for making comparisons and drawing conclusions. We used this command:

```
$ rwsettool --sample --size 100000 all_ips.set | rwsetcat | sort > S.list
```

As with the I_j+I_m data set, we saved the data into different formats to suit our needs:

- We retained the S.list file with just the random sample IP addresses in standard notation in case we had to refer to the original set for any reason.
- Using SiLK, we used this command to create a SiLK set of these IP addresses to aid in our analysis and called the file S.set:

  ```
  $ rwsetbuild S.list S.set
  ```
- Next, we created a file containing the IP addresses in regular expression notation, called S_reg.list. Then, using the IP addresses in regular expression notation, we broke down the IP addresses into CIDR /8 netblocks in accordance to the format of the Internet Census data.

6.3.2 SR and SC: Routing Data and Country Code

Like for our APT1 data, we decided to use Neustar data to determine the routing type and country code of the sample IP addresses. We used the same pmap files that we created above for both the routing/connection type and country code in these commands:

```
$ rwtuc S_list --field=sip | rwuniq --pmap-file=route: \

      routingConnection.pmap --field=sip,src-route --no-col > SR.txt

$ rwtuc S_list --field=sip | rwuniq --pmap- \

      file=country:countryState.pmap --field=sip,src-country --no-col \

      > SC.txt
```

We used the Excel `SORT`, `FILTER`, and `COUNTIF` commands, as well as Pivot tables for the data analysis.

6.3.3 S_{p75}: Fingerprints of the S Set Given a 75% Match

We used the S IP addresses separated into CIDR /8 netblocks to find the fingerprints. We used this command to run the S netblock sets against the corresponding netblock found in the fingerprint data:

```
$ grep -f S_reg.list X > S_X.txt
```

The `X` is the netblock in the Internet Census data, which is how the fingerprint files are named. Upon finding the fingerprints for all the netblocks, we concatenated them into a single file using this command:

```
$ cat * > all_SF.txt
```

We ran the file through our Python script to give us usable data. Then, we put the corresponding fingerprint data into our working Excel document containing the S IP addresses. For our analysis, we primarily used the Excel SORT and FILTER tools, and `COUNTIF` and `VLOOKUP` commands.

6.3.4 SP: Port Analysis

We used the S IP addresses in regular expression notation to find open ports. This command pulled the lists of open ports associated with each IP address in S:

```
$ grep -f S_reg.list P.list > SP.txt
```

- Once all the open ports were returned, we changed the delimiters in the file to be semicolons instead of commas using the Replace function in a normal text editor. Doing so ensured that any program we used for analysis would interpret the ports as individual values and not one long numnumber.

- We manipulated the data to repeat each IP address with each of its associated open ports. The result was a file with an IP address and single port on each line, which helped our data analysis.
  - SP_{20}, SP_{10}^{15} ,SP_{5}^{9};SP_{1}^{3} broke down the instances of IP addresses having various ports running by 20+ times, 10-15 times, 5-9 times, and 1-3 times.
  - The Excel `SORT`, `FILTER`, `COUNT`, and `COUNTIF` commands helped our analysis.
  - Pivot tables helped us visually understand the data.
  - We plotted the distribution of open ports.
- Once we found all the open ports, we ran pair correlations to identify any unusual port pairing that occurred frequently in the data set.

6.3.5 SR and SC: Routing Data and Country Code

Like the I_j+I_m IP set, we decided to use Neustar data to determine the routing type and country code because it is more accurate. We used the pmaps created above for the I_j+I_m set to analyze our sample, replicated the process containing city and state for our sample, and once again used SiLK to create a pmap. We used these commands:

```
$ rwtuc --field=sip S.list | rwuniq --pmap- \
          file=route:routingConnection.pmap --field=src-route --no-col \
          > SR.txt
$ rwtuc --field=sip S.list | rwuniq --pmap- \
          file=country:countryState.pmap --field=src-country --no-col \
          > S.txt
```

7 Results: APT1

7.1 I_jD: JIB Domain Names

The pDNS search connects IP addresses to domain names. While the names from the I_j set did not have many exact matches to those found in the Mandiant report, many of them were similar, often having the same second-level domain name. There were 3,573 domain name entries for the I_jD expansion. We broke those down into four categories: (1) deliberately deceptive domain names, (2) seemingly random alphanumeric domain names, (3) domain names that appear to belong to legitimate organizations but are known to be malicious, and (4) domain names that appear to be legitimate and do not have a reputation for malware or phishing. Categories 1-3 are described below.

7.1.1 Deliberately Deceptive Domain Names

Many of the domain names appeared to be deliberately deceptive and mimic legitimate domains. For example, many contain forms of “Apple Soft Update,” “CNN Daily,” “Yahoo Daily,” “Firefox Update,” “Symantec Online,” “AOL Daily,” or “NY Times News.” Below is a list of takes on several well-known domain names and the number of occurrences.

Table 5: Recognizable Organizations Found in Domain Names and Frequency of Occurrence

Organizations Used Deceptively in Domains	**Count**
Apple (as Apple Soft)	18
NY Times	15
MSN	10
CNN	8
Google	7
Symantec	6
Yahoo	6
McAfee	3
Microsoft	2
Firefox	2

Below is a small sample of the deliberately deceptive domains found in the pDNS results for the I_j set:

- epa.yahoodaily.com
- weather.yahoodaily.com
- fashion.cnnnewsdaily.com
- news.cnndaily.com
- flash.aoldaily.com
- update8.firefoxupdata.com
- download.applesoftupdate.com
- update.symentec.org

- update.livemymsn.com
- microsoft.standards-updates.com
- url.googlevipmail.net

7.1.2 Pseudo-Random Alphanumeric Domain Names

Instead of containing company names that many target users would know, other domains contained strings appearing to be pseudo-random alphanumeric sequences. This type of domain name occurs for approximately 25% of the entire I_jD set. Examples include

- 29ig82qwpxkfsaege4gapfw3jigmdoe4vn6otcpivtuowr5v3a.41.cgfde.com
- ae4en558r8gcmj9sbsra7u5e8d8v45rt7froujsbrvkumrep.45.okjyu.com
- 9urdkpdpnd33t2uvaq7hkkejq6eawvb6b32dumgf4ldd6sbgve.41.nhtyd.com

At times, these names are associated with another second-level domain name that is not random, for example

- q10765919.299.vpszuyong.com
- q1811815333.69vps.vpszuyong.com
- ns-00275-11412.irl-dns.info
- xn--12c4b5a2g9a5b.dmc.tv
- ns.44691d0d_cdc4b217_18521.dns.irl.cs.tamu.edu

7.1.3 Malicious Domain Names

Many of the other domain names found appear to belong to legitimate businesses but either currently host malware or have hosted it in the past. The owners of these domains may not know malware is being hosted on their sites, while others may be hosting malicious content deliberately. Examples of malicious domain names include

- lanteckstudios.com
- pietros.com
- johnspizzerianyc.com

7.2 I_jDM Malicious Code

After analyzing the domain names in I_jD, the next logical step was to discover malicious code associated with the domain names found with the pDNS queries. The Mandiant hashes available to us contained over 1,000 unique hashes.

- 266 unique malicious code hashes were found in 2012 in the metadata from CERT’s runtime analysis efforts linked to I_jD.
- Of the hashes found in the metadata, only seven were also found in the Mandiant report:
    - Those seven hashes occurred on eight different domains.
    - Three of those eight domains were found in the Mandiant list:
        - flash.cnndaily.com
        - japan.yahoodaily.com
        - flash.cnndaily.com

  - The remaining five of those eight domains were not found in the Mandiant list:
    - engineer.lflinkup.org
    - news.hoenjet.org
    - news.hqrls.com
    - report.crabdance.com
    - www.freelanceindy.com
  - The metadata identified 80 unique domains with malware hashes.
- 15 hashes occurred two times each; the remaining 251 occurred only one time.

7.3 DI_m: Mandiant IP Address Set

The Mandiant report provided many domain names associated with APT1 activity. We performed an rDNS search to retrieve a set of IP addresses associated with these domains.

- A total of 622 IP addresses were found.
- 91 overlapping IP addresses were already found in I_j.
- 531 unique IP addresses made up the I_m set.

7.4 I_j+I_m: IP Addresses Concatenated from Both Working IP Address Sets

For the purposes of our analysis, we found it beneficial to combine the I_j and I_m sets, but we did not create a separate variable for comparing them. In this report, we include our overall analysis of the combined set that contained 1,386 IP addresses.

7.5 I_j+I_mF_{p75}: TCP/IP Fingerprints of I_j+I_m Given a 75% Match

When we began this project, we speculated that APT1 would be targeting low-hanging fruit while building its infrastructure. Many times this comes in the form of using old OSs that still have exploitable vulnerabilities. Although these machines are not targets, APT1 needs to control hop points to exfiltrate data from the targets. Out of the 1,386 IP addresses, 451 were fingerprinted, constituting 32.5% of the combined set:

- 27.9 % were Linux machines.
- 65.4% were Microsoft Windows machines.
- The remaining 6.7% ran an OS other than Linux or Windows.

7.5.1 $(I_j$+$I_mF_{p75})_2$: TCP/IP Fingerprints with Multiple Instances

As we suspected, the top fingerprints were versions of Windows and Linux from 2009 or before. The top Windows fingerprints were from OSs released before 2005. Likewise, the top Linux kernels fingerprinted were versions from 2010 and earlier, but most of them date to around 2009. There is a time frame of 5-6 years between the Windows machines and Linux kernels. This data point challenged our initial hypothesis that all OSs would be dated around the same time and may suggest that APT1 changed operations to include more Linux machines after initially targeting Windows. The top five fingerprints made up 50% of the data. All fingerprints with five or more occurrences are listed in Figure 1. Figure 2 represents the fingerprints with two to four occurrences. Table 6 lists the top five most frequently occurring fingerprint matches with the total occurrences and percentage of the overall data set. Note that many of the fingerprints do not match exact versions or service packs but rather match an OS range.

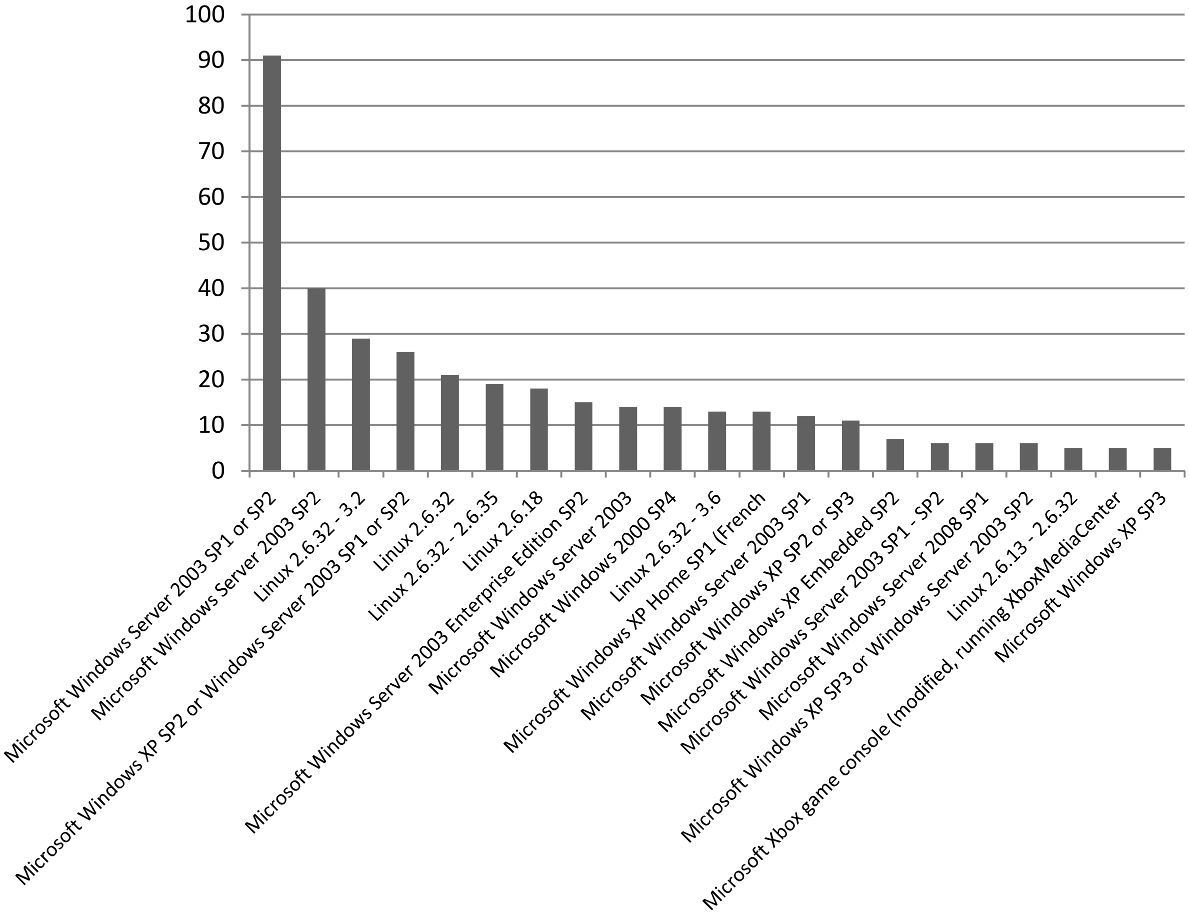

Figure 1: Fingerprints with Five or More Occurrences

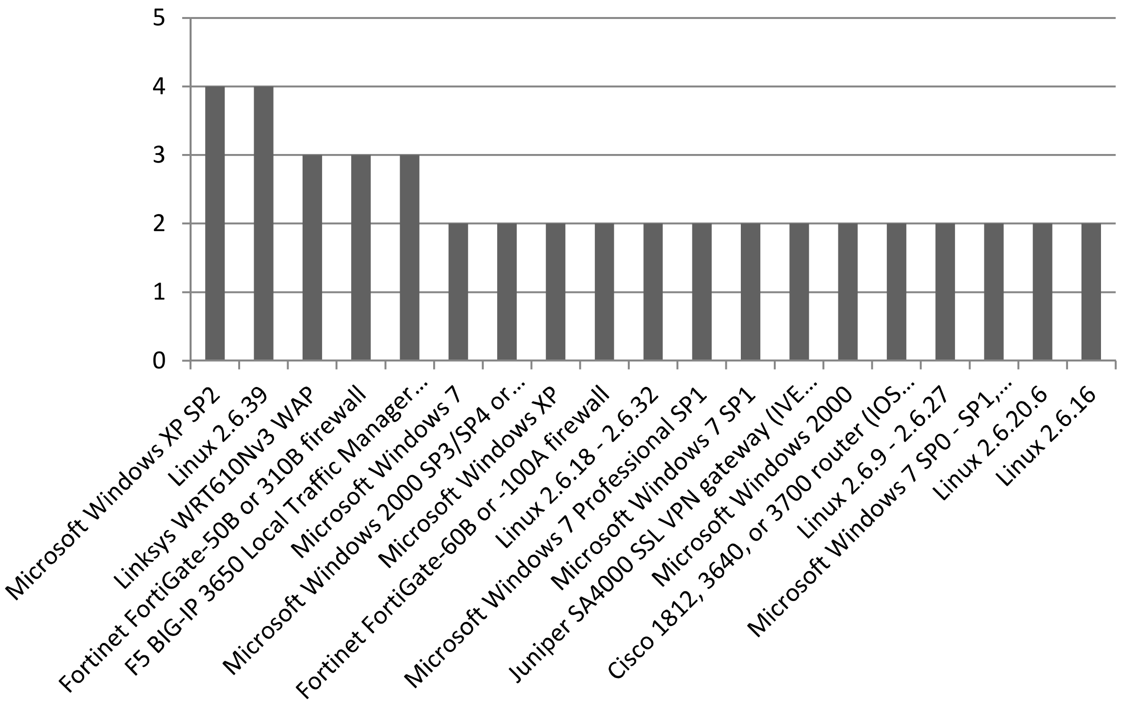

Figure 2: Fingerprints with Two to Four Occurrences

Table 6: Top Five Fingerprints in I_j+I_m

Fingerprint	**Count**	**% Total of IPs with Fingerprint Data in I_j+I_m**	**% Total of I_j+I_m**
Microsoft Windows Sever 2003 Service Pack 1 or 2	97	21.5%	7.0%
Microsoft Windows Server 2003 SP2	42	9.3%	3.0%
Linux 2.6.32 - 3.2	34	7.5%	2.5%
Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2	29	6.4%	2.1%
Linux 2.6.32	24	5.3%	1.7%

7.5.2 I_j to I_m TCP/IP Fingerprint Comparison

We compared the fingerprints in I_j and I_m. The sets were very similar in their frequency and distribution but differed in two ways:

1. Linux 2.6 versions occurred twice as often in the I_m set.
2. The Microsoft Xbox Game Console occurred five times in the I_m set but not at all in the I_j data set.

Figure 3 categorizes the various fingerprints for each data set. Table 7 represents the top 10 fingerprint comparisons between I_j and I_m as a percentage of the corresponding IP address set.

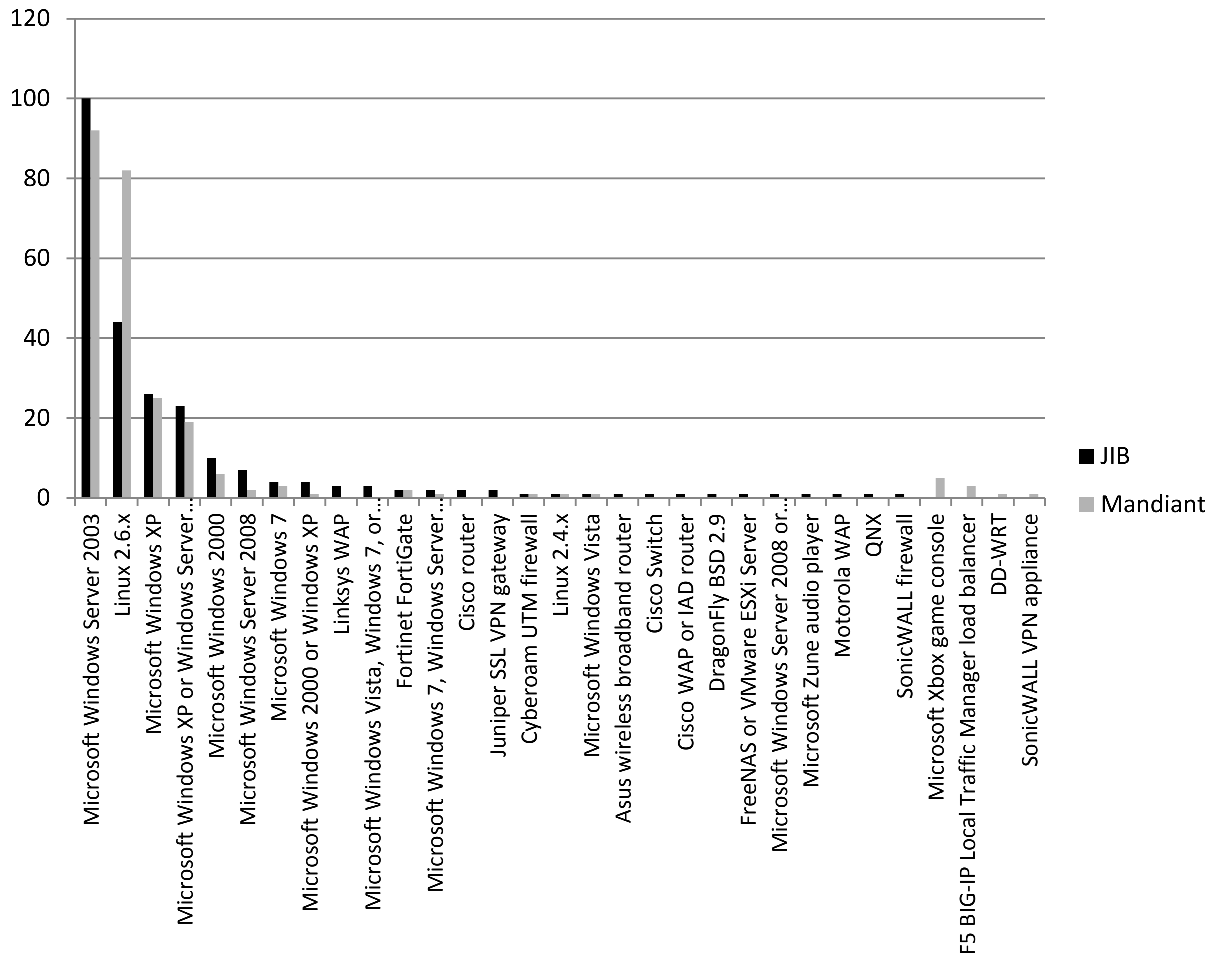

Figure 3: Fingerprint Comparison of I_j and I_m

Table 7: Top 10 Fingerprint Comparison of I_j and I_m

Fingerprints	I_j Count	I_m Count	I_j %	I_m %
unknown	610	376	71.3%	60.5%
Microsoft Windows Server 2003	100	92	11.7%	14.8%
Linux 2.6.x	44	82	5.2%	13.2%
Microsoft Windows XP	26	25	3.0%	4.0%
Microsoft Windows XP or Windows Server 2003	23	19	2.7%	3.1%
Microsoft Windows 2000	10	6	1.2%	1.0%
Microsoft Windows Server 2008	7	2	0.8%	0.3%
Microsoft Windows 7	4	3	0.5%	0.5%
Microsoft Windows 2000 or Windows XP	4	1	0.5%	0.2%
Microsoft Xbox game console	0	5	0.0%	0.8%

7.6 I_j+I_mP: Port Analysis

Along with the TCP/IP fingerprint information, the open ports allow us to best categorize what APT1 found necessary in its infrastructure. We looked at the open ports to understand what types of pathways are needed for APT1 operations:

- 791 IP addresses (or 51.1%) in I_j+I_m had open ports.
- 4 IP addresses (possibly proxy servers) had more than 100 ports open.
- 609 unique open ports are represented in the data.

Figure 4 reflects the count of open ports per IP address. Most IP addresses in I_j+I_m have fewer than 16 ports open. Running correlations between ports did not present any high-correlation pairs. We surmise there would be high correlations if we could break down the IP addresses into groups based on the exact role they play in the infrastructure. However, this was not possible with the data available for this study.

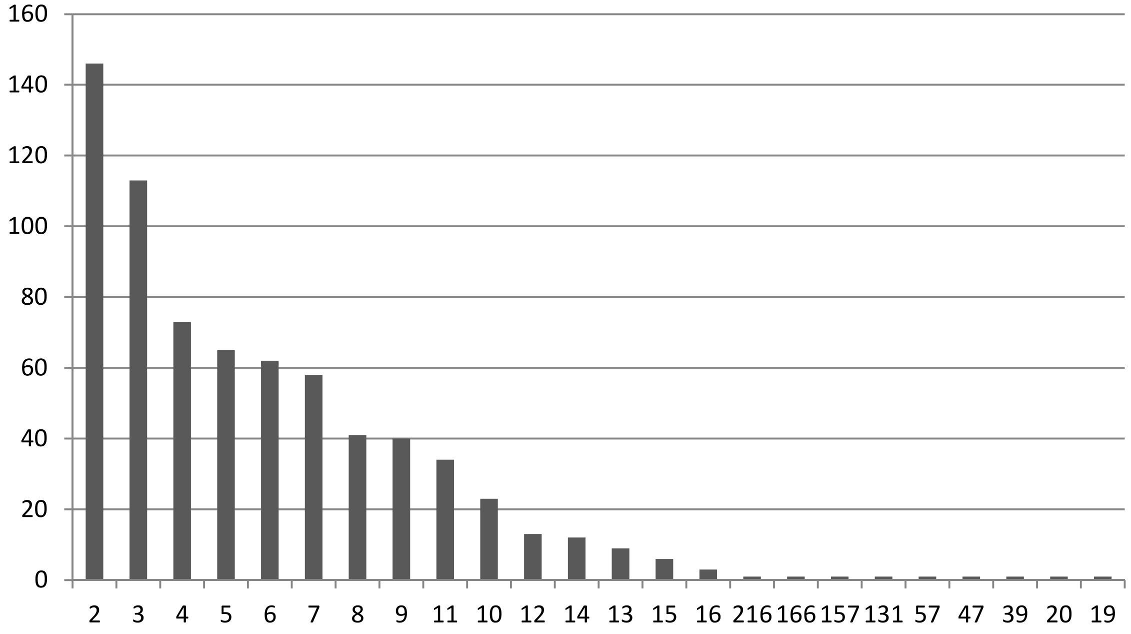

Figure 4: Count of Open Ports per IP Address in I_j+I_m

7.6.1 Most Common Open Ports in I_j+I_m

Table 8 reflects the most common open ports, each occurring in more than 10% of the IP addresses having open ports in I_j+I_m.

Figure 5shows the distribution of open ports and the frequency of occurrence for the open ports with more than 20 occurrences.

Table 8: Ports Representing 10+% of Open Ports

Port	Count	% Total IP Addresses with Open Ports in I_j+I_m	% Total IP Addresses in I_j+I_m
80	655	82.8%	47.3%
3389	434	54.9%	31.3%
443	312	39.4%	22.5%
21	305	38.6%	22.0%
25	217	27.4%	15.7%
135	212	26.8%	15.3%
53	165	20.9%	11.9%
22	162	20.5%	11.7%
1025	156	19.7%	11.3%
3306	146	18.5%	10.5%
139	145	18.3%	10.5%
445	137	17.3%	9.9%
1723	123	15.5%	8.9%
110	117	14.8%	8.4%
1026	101	12.8%	7.3%
143	86	10.9%	6.2%

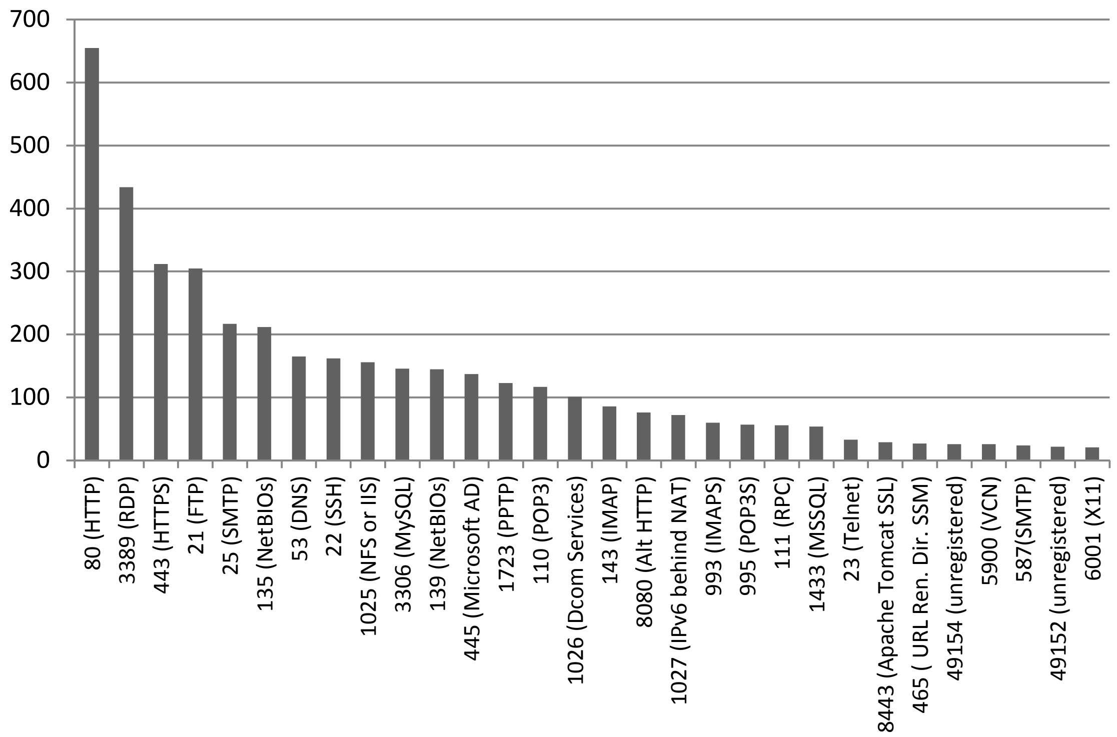

Figure 5: Count of IP Addresses for Ports Occurring 20+ Times in I_j+I_m

7.6.2 I_j to I_m Port Comparison

When comparing the number of open ports in the I_j and I_m sets, we noticed a similar distribution. However, I_m had a higher percentage of open ports:

- 51.7% of the I_j set were open (442 IP addresses).
- 77.2% of the $I_{m,}$ set were open (410 IP addresses).

When analyzing the common but less frequent ports, we noticed that ports 22, 445, and 111 occurred more frequently in I_m than in I_j. Figure 6 highlights the comparisons between the two data sets.

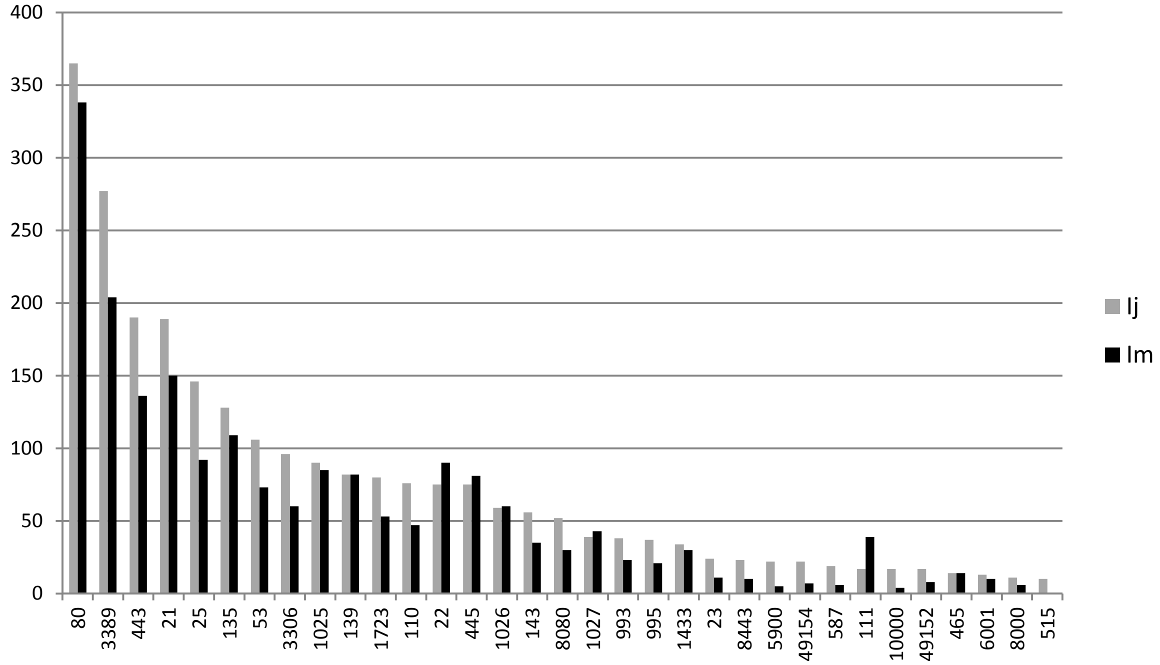

Figure 6: Port Comparison of I_j and I_m

7.7 I_j+I_mA: Autonomous System Numbers

We mapped the IP addresses in I_j+I_m to their respective ASNs for two reasons. First, we wanted to see what types of companies were represented. Second, we wanted to understand if the infrastructures of any particular companies were being targeted:

- All the IP addresses were mapped (1,386).
- In the I_j+I_m list, there were 388 unique ASNs, belonging to 362 different organizations.
- Organization types included internet service providers (ISPs), hosting providers, universities, and state governments. We could not determine a type for a small number of the ASN owners.

7.7.1 Types of Organizations Represented

The majority of the ASNs represented either hosting or internet service providers. The minority represented educational institutions, or local or state government. The majority of the hosting and ISPs are fairly well known; of the top 20 hosting companies, approximately 50% are represented in the I_j+I_m set.

7.7.2 Targeted Organizations

If IP addresses are clustered within ASNs, it is reasonable to assume the companies owning those ASNs have been targeted for some particular reason. IP addresses that are distributed across many ASNs have likely been chosen randomly. Approximately half of the IP addresses in I_j+I_m appear clustered in a small number of ASNs.

Figure 7 reflects the 28 organizations with 10 or more IP addresses in the data set. Table 9 reflects the top five companies and the percentage of IP addresses that resolve to them:

- 28 organizations (or 51.9%) were associated with 10 or more IP addresses.
- 208 organizations were associated with only one IP address.
- 127 organizations were associated with 2 to 9 IP addresses.

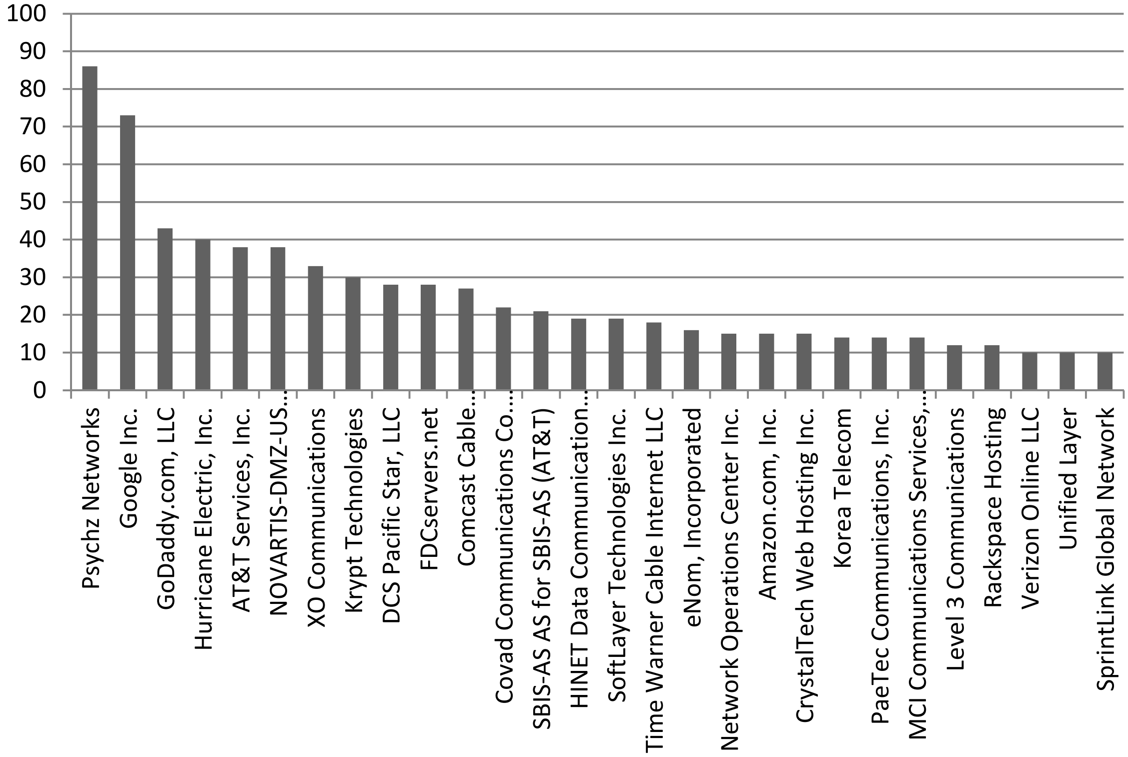

Figure 7: Organizations with 10 or More IP Addresses

Table 9: Top Five Organizations in Registering IP Addresses in I_j+I_m

Company	**Associated IP Addresses**	**Percentage of Total IP Addresses**
Psychz Networks	86	6.2%
Google Inc.	73	5.3%
GoDaddy.com, LLC	43	3.1%
Hurricane Electric, Inc.	40	2.9%
AT&T Services, Inc.	38	2.7%

Company	**Associated IP Addresses**	**Percentage of Total IP Addresses**
NOVARTIS-DMZ-US (Qwest/CenturyLink)	38	2.7%

Some of the companies found in I_j+I_m are known to be malicious outside of APT1 operations. Many have contained malware used by other malicious groups during various operations of their own. For instance, Psychz Networks and Krypt Technologies popped up very frequently, more frequently than the biggest hosting sites. Research on these two companies indicates they both provide bulletproof hosting services. Psychz Networks in particular has a reputation of hosting a slew of malicious websites.

7.8 I_j+I_mC: Location of IP Addresses

The I_j+I_m IP addresses are associated with 54 different countries, 45 U.S. states, and the District of Columbia. Figure 8 reflects the distribution of companies with more than five resolving IP addresses by U.S. state. Figure 9 shows the non-U.S. countries with resolving IP addresses.

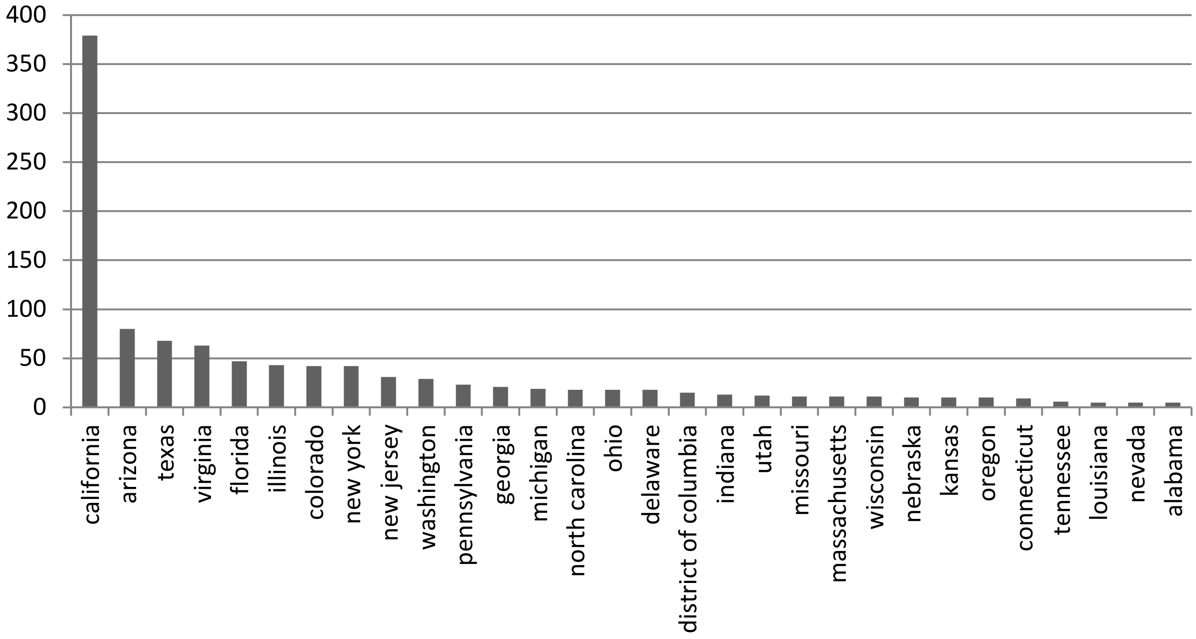

Figure 8:   U.S. States with Five or More Associated IP Addresses

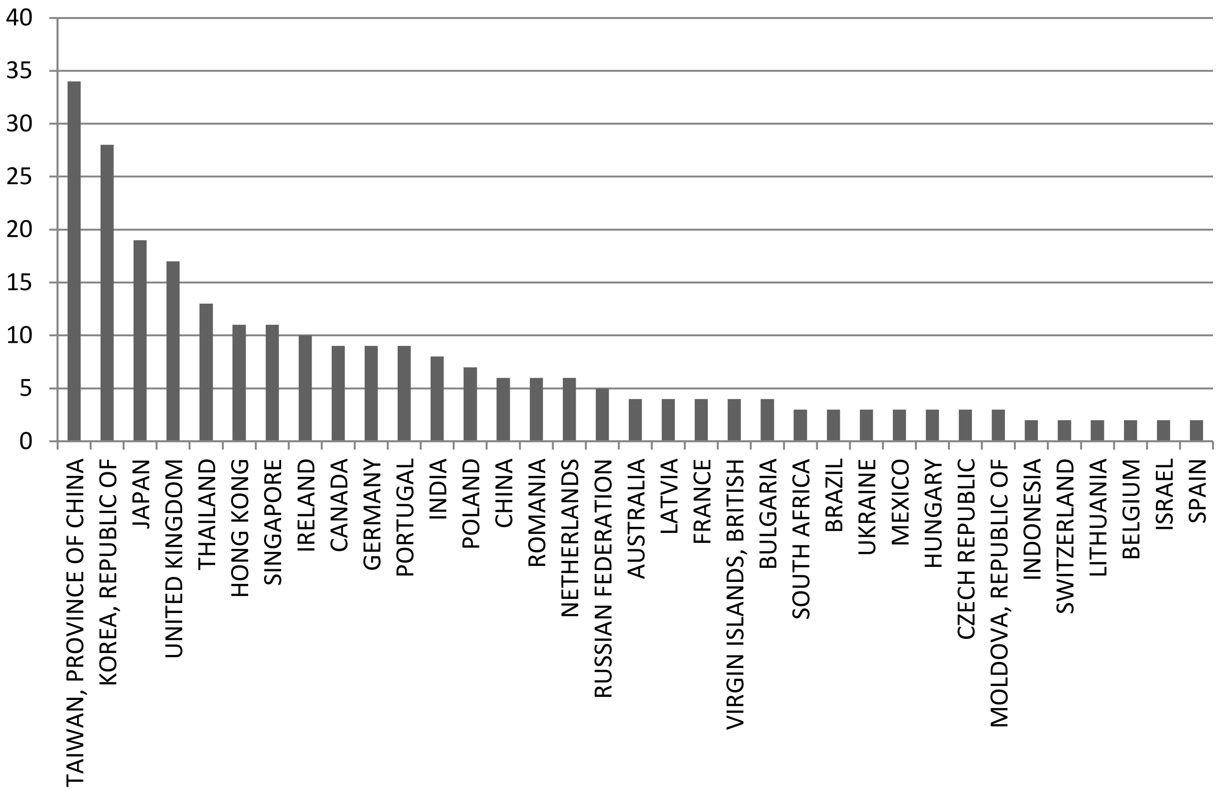

Figure 9: Non-U.S. Countries with Two or More Occurrences

7.9 I_j+I_mR: Routing Data

The routing data allows us to identify how the IP addresses are connected to the internet, whether through a fixed, dynamic, or other connection. Figure 10 shows the types of routing data found for I_j+I_m:

- *Fixed, dedicated* lines are lease lines or fiber connections, which indicate this is a connection from a mid-sized to large organization.
- *Fixed, other* lines constitute all other fixed connections such as DSL or cable.
- *Pop* represents a dial-up connection.
- *Other* is any other type of connection, for example, a connection through an international proxy or gateway.

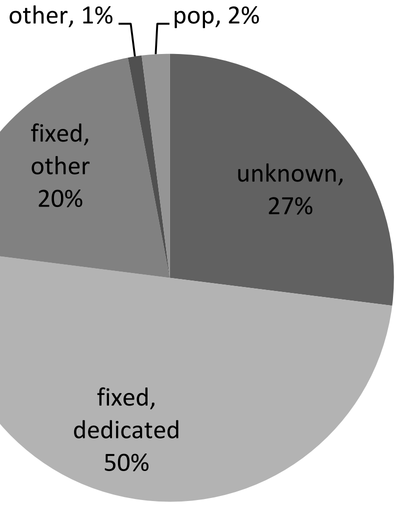

Figure 10: Neustar Routing Types in I_j+I_m

In the figure, note that

- 1,000 IP addresses have routing types.
- 50% of those addresses have fixed connections through leased lines or optical fiber cable, indicating they likely belong to organizations and not individuals.
- 984 IP addresses have connection types, which means their routing type is fiber, leased line, DSL, cable, or dial-up.

7.10 I_j+I_mO: Open Resolvers

An open resolver is a misconfigured DNS server that answers recursive queries for hosts outside its network. We wanted to see whether open resolvers appeared to be an important factor for the APT1 infrastructure. Several open resolvers occur in the data set, and several of the companies represented in the set have more than one open resolver in our list:

- There are a total of 43 open resolvers in I_j+I_m.
- They constitute 3.1% of I_j+I_m.
- They belong to 30 different organizations.
- The biggest offenders with more than one open resolver are listed in Table 10.

Table 10: Organizations Associated with More Than One Open Resolver

Company Name	**Number of Open Resolvers**
Comcast Cable Communications, Inc.	6
CrystalTech Web Hosting, Inc.	5
MegaPath Networks, Inc.	3
Charlotte Colocation Center, LLC	2
NOVARTIS-DMZ-US (Qwest/CenturyLink)	2

7.11 APT1 Analysis Summary

Within the APT1 data set, all IP addresses had information for at least ASN and country. Almost 24% (329) of the IP addresses also have a fingerprint, at least one open port, and routing data. Less than 13% (177) of the IP addresses lacked a fingerprint, open ports, and routing data.

8 Results: IPv4 Sample

To confirm our analysis from the I_j+I_m data set, we had to know what the IPv4 address space looked like in contrast to the data associated with APT1. Then, we had a baseline of what we would expect to see with TCP/IP fingerprint information and SyncScan data in the APT1 data set if there was nothing special about the IP addresses and the infrastructure they represent. We found the sample to differ considerably from the I_j+I_m data, which confirmed our speculation that APT1 has special requirements for its infrastructure.

8.1 SF_{p75}: TCP/IP Fingerprints of S Given a 75% Match

Of the 100,000 IP addresses in our sample, 11,132—or 11.13% of the entire sample set—were fingerprinted:

- 686 of them were unique.
- 35.2% of the fingerprinted machines ran Linux, 12.9% ran Microsoft Windows, and 51.9% ran neither.

8.1.1 Top TCP/IP Fingerprints

Unlike the I_j+I_m set, none of the Microsoft Windows OSs breaks the top five occurring fingerprints. Instead, those top five contain two Linux OSs and three other, unrelated identities. Table 11 reflects the top five fingerprints, the number of occurrences, the percentage of the fingerprinted data, and the percentage of the sample.

Table 11: Top Five Fingerprints in S

Fingerprint	Count	% Total of IP Addresses with Fingerprints in S	% Total IP Addresses in S
Linux 2.6.32	734	6.6%	0.7%
VxWorks	691	6.2%	0.7%
Linux 2.6.18	463	4.2%	0.5%
Linksys WRT610Nv3 WAP	451	4.0%	0.5%
AVM FRITZ!Box FON WLAN 7170 WAP (Linux 2.6.13)	418	3.8%	0.4%

Figure 11shows the top 30 fingerprint occurrences for the IPv4 sample and the number of times each particular fingerprint occurs.

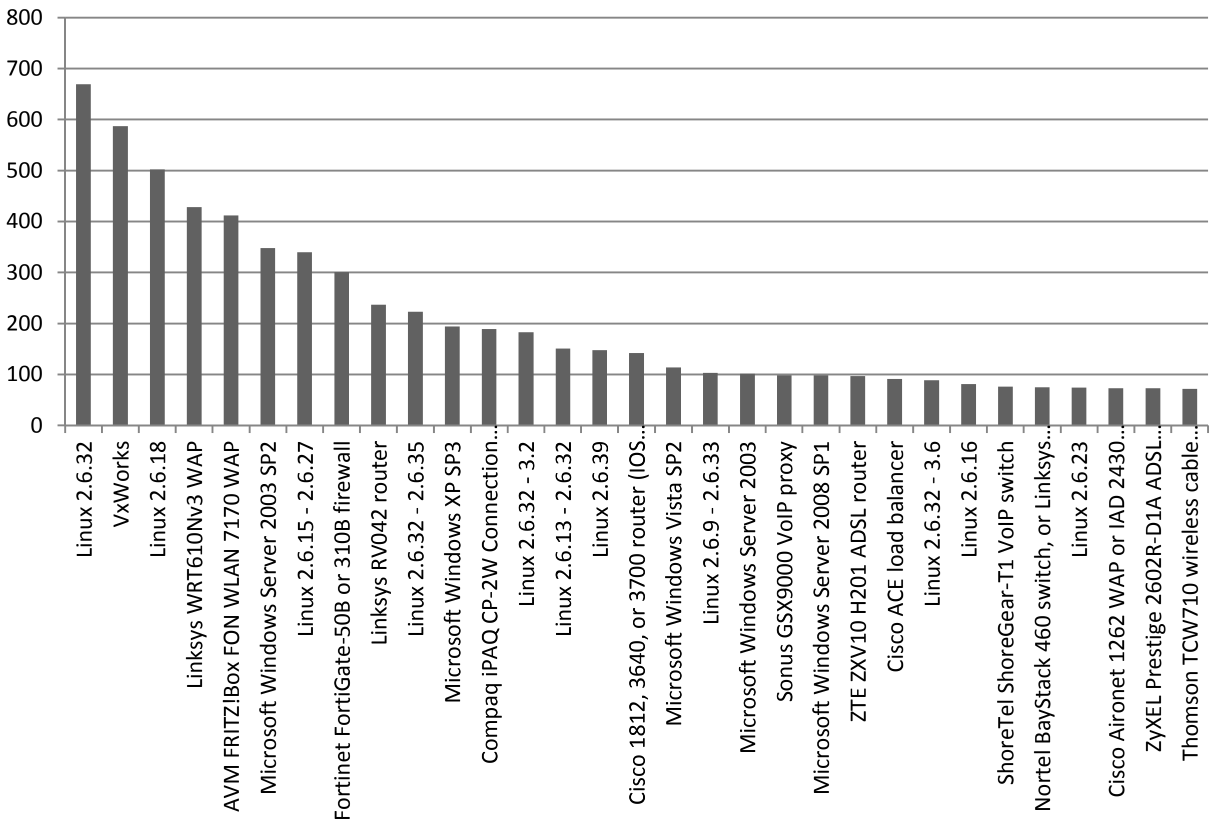

Figure 11: Top 30 Fingerprints in S's IP Addresses

8.2 $I_j+I_mF_{p75}$ and SF_{p75} Comparison

The IPv4 sample is crucial because it tells us what we should expect to see throughout the IPv4 space. If APT1 was not targeting something specific, we should expect similar results to the sample:

- Of the IPv4 sample, only 11.13% of the IP addresses returned fingerprints, compared to 32.5% in the I_j+I_m set.
- No single fingerprint constituted more than 1% of the total IP addresses in S.
- No single fingerprint constituted more than 7% of the total fingerprinted IP addresses in S.

While the Linux percentages in the I_j+I_m and S sets were close, the Windows OSs diverged considerably as shown in Table 12. The S set had a greater percentage of non-Windows and non-Linux machines than the I_j+I_m set: We would expect these differences if APT1 was targeting specific architecture.

Table 12: Operating System Comparison Between I_j+I_m and S

Operating System	**I_j+I_m**	**S**
Linux	30.8%	35.2%
Windows	71.6%	12.9%
Other	7.3%	51.9%

8.2.1.1 I_j+$I_m$$F_{p75}$ and SF_{p75} Top TCP/IP Fingerprint Comparison

Although we found the I_j+I_m set's top fingerprints in the sample, they occurred in a much lower percentage of the IP addresses. Additionally, we found that three of the top five most frequently occurring OSs in the sample were nonexistent in the I_j+I_m set. Microsoft Windows Server 2003 machines, in particular, had a much higher percentage of occurrences in the I_j+I_m data. This further supports the theory that APT1 was targeting specific architecture. Table 13 compares the top fingerprints of the I_j+I_m and S sets.

Table 13: Top Fingerprint Comparison Between I_j+I_m and S

Fingerprint	% Total IP Addresses with Fingerprints in I_j+I_m	% Total IP Addresses with Fingerprints in S
Microsoft Windows Sever 2003 Service Pack 1 or 2	21.5%	0.6%
Microsoft Windows Server 2003 SP2	9.3%	3.0%
Linux 2.6.32 - 3.2	7.5%	1.8%
Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2	6.2%	0.2%
Linux 2.6.32	5.3%	6.6%
VxWorks	0%	6.2%
Linux 2.6.18	4.2%	4.2%
Linksys WRT610Nv3 WAP	0.2%	4.1%
AVM FRITZ!Box FON WLAN 7170 WAP (Linux 2.6.13	0%	3.8%

Figure 12 shows the top 30 fingerprints found in the IPv4 sample data. The fingerprints shown in black also occur in the top 10 fingerprints of the I_j+I_m data. Only 5 of the top 10 fingerprints in I_j+I_m are in the top 30 of the S data set.

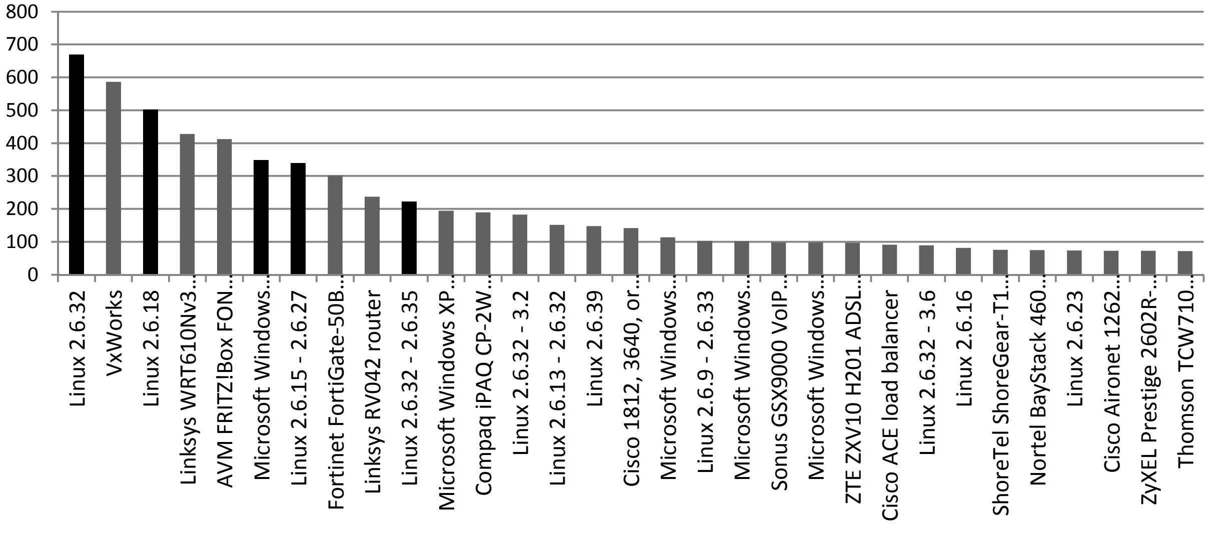

Figure 12: Top 30 Fingerprints in S and Top 10 Overlap with I_j+I_m

8.3 SP: Open Ports of S set

Along with the TCP/IP fingerprint information of the sample, open port analysis allows us to confirm what pathways APT1 found necessary to its infrastructure:

- 33,573 IP addresses (33.6%) in the S set have open ports.
- 222 IP addresses had more than 100 ports open.
- One IP address had 249 ports open.
- 14,024 unique open ports are represented in the data.

Figure 13 reflects the count of open ports per IP address. About 95% of the IP addresses have three or fewer open ports at once. About 99% of the IP addresses have 13 or fewer open ports.

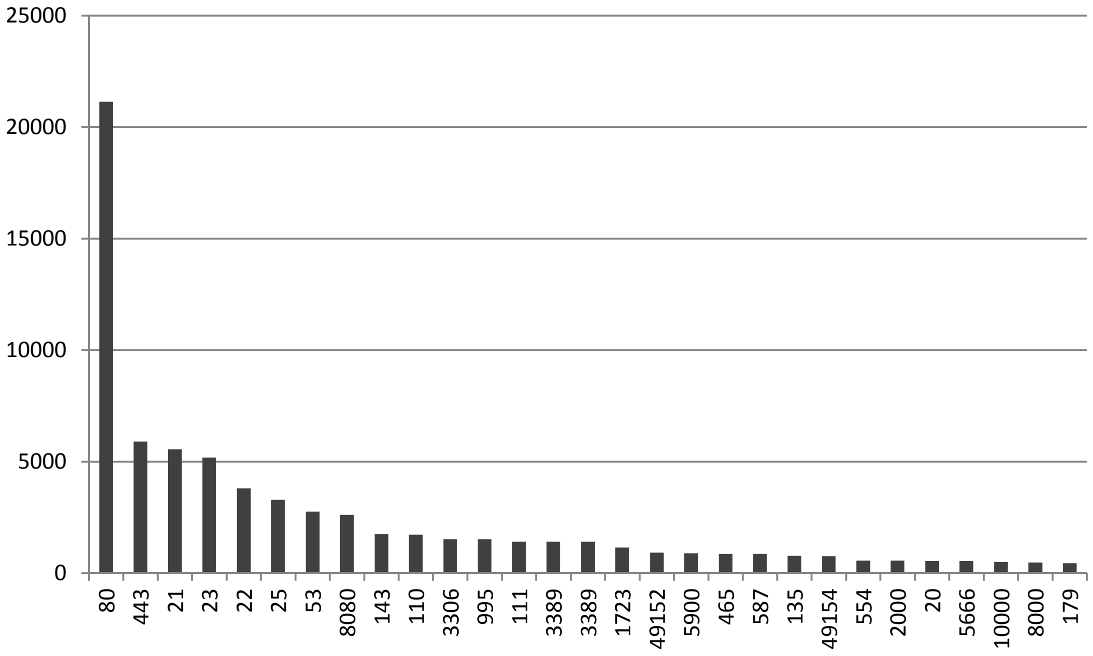

Figure 13: Count of IP Addresses per Top 30 Ports in S

8.3.1 Most Common Open Ports

Table 14 reflects the most common open ports occurring in at least 5% of the IP addresses having one or more open ports in the S data set.

Table 14: Ports Representing 5+% of Open Ports

Port	Count	% Total IP Addresses with Open Ports in S	% Total IP Addresses in S
80	21140	63.0%	21.1%
443	5897	17.6%	5.9%
21	5557	16.6%	5.6%
23	5184	15.4%	5.2%
22	3808	11.3%	3.8%

Port	Count	% Total IP Addresses with Open Ports in S	% Total IP Addresses in S
25	3295	9.8%	3.3%
53	2768	8.2%	2.8%
8080	2614	7.8%	2.6%
110	1731	5.2%	1.7%

8.4 I_j+I_mP and SP Comparison

Like with the fingerprint data, comparing open ports between the I_j+I_mP and SP data sets reveals noticeable differences:

- Of the IPv4 sample, only 33.6% of the IP addresses had open ports, compared with 57.1% in the I_j+I_m set.
- Only 5 different ports were open on more than 10% of the IP addresses in the sample, compared to 16 in the I_j+I_m set.

8.4.1.1 I_j+I_mP and SP: Top Open Port Comparison

The top fingerprints for the I_j+I_m set were also found in the sample; however, the rate at which they occur is very different between the two sets. The top 15 open ports in the I_j+I_m set occur at a rate of between 2 and 17 times as frequently as in the S set, with the exception of port 80. The rates of occurrence of ports 3389, 443, 25, 135, 1025, and 445 especially stand out.

Table 15: Port Data Comparison Between I_j+I_m and S, All IP Addresses

Port	% Total IP Addresses in I_j+I_m	% Total IP Addresses in S
80	47.3%	21.1%
3389	31.3%	1.5%
443	22.5%	5.9%
21	22.0%	5.6%
25	15.7%	3.3%
135	15.3%	1.1%
53	11.9%	2.8%
22	11.7%	3.8%
1025	11.3%	0.5%
3306	10.5%	1.4%
139	10.5%	0.5%
445	9.9%	0.3%
1723	8.9%	1.2%
110	8.4%	1.7%
1026	7.3%	0.5%
143	6.2%	1.6%
8080	5.4%	2.6%

Port	% Total IP Addresses in I_j+I_m	% Total IP Addresses in S
23	2.4%	5.2%

Port data comparison between IP addresses in the entire set is shown in Table 16.

Table 16: Port Data Comparison Between I_j+I_m and S, Open Port IP Addresses Only

Port	% Total IP Addresses with Open Ports in I_j+I_m	% Total IP Addresses with Open Ports in S
80	82.8%	63.0%
3389	54.9%	4.3%
443	39.4%	17.6%
21	38.6%	16.6%
25	27.4%	9.8%
135	26.8%	3.2%
53	20.9%	8.2%
22	20.5%	11.3%
1025	19.7%	1.4%
3306	18.5%	4.2%
139	18.3%	1.4%
445	17.3%	1.0%
1723	15.5%	3.4%
110	14.8%	5.2%
1026	12.8%	1.5%
143	10.9%	4.8%
8080	9.6%	2.6%
23	4.2%	5.2%

8.5 SC: Location of IP Addresses for S Set

The S data set contained 193 different countries; North Korea, Iran, and the Virgin Islands (British) were not represented. All 50 U.S. states were represented, along with the District of Columbia. Figure 14 reflects the distribution of U.S. states with more than 180 resolving IP addresses.

Figure 15 shows the countries with more than 350 resolving IP addresses. These countries represent 92.3% of the data.

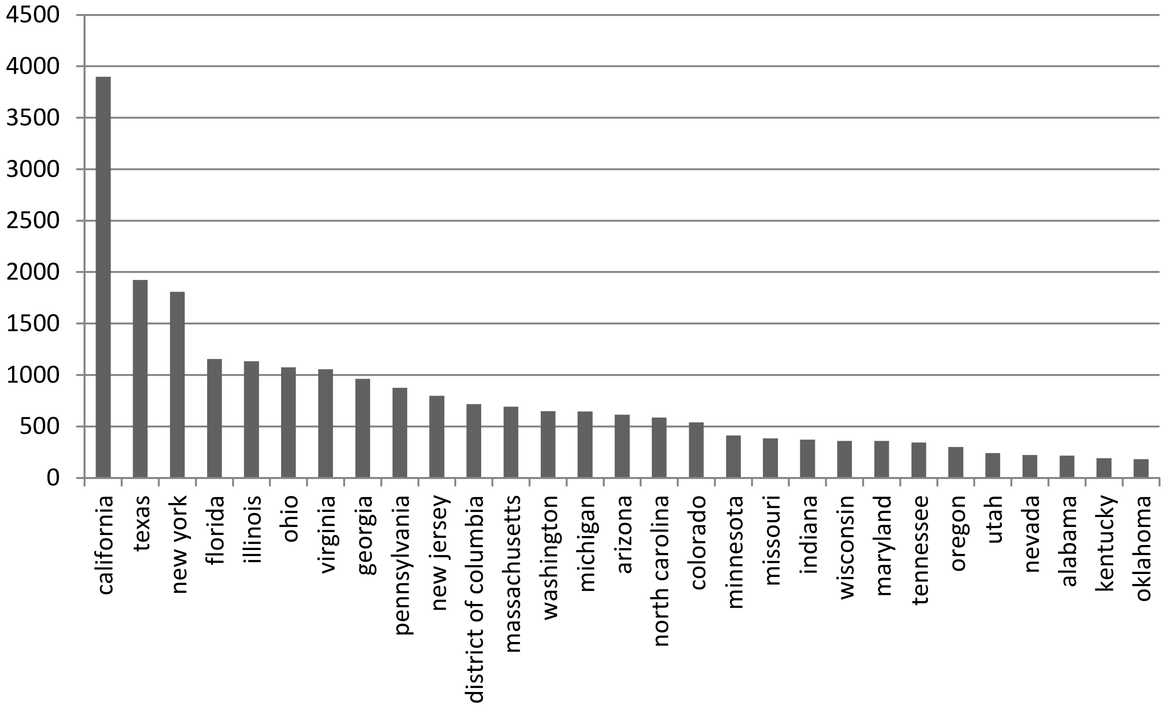

Figure 14: U.S. States Containing More Than 180 IP Addresses

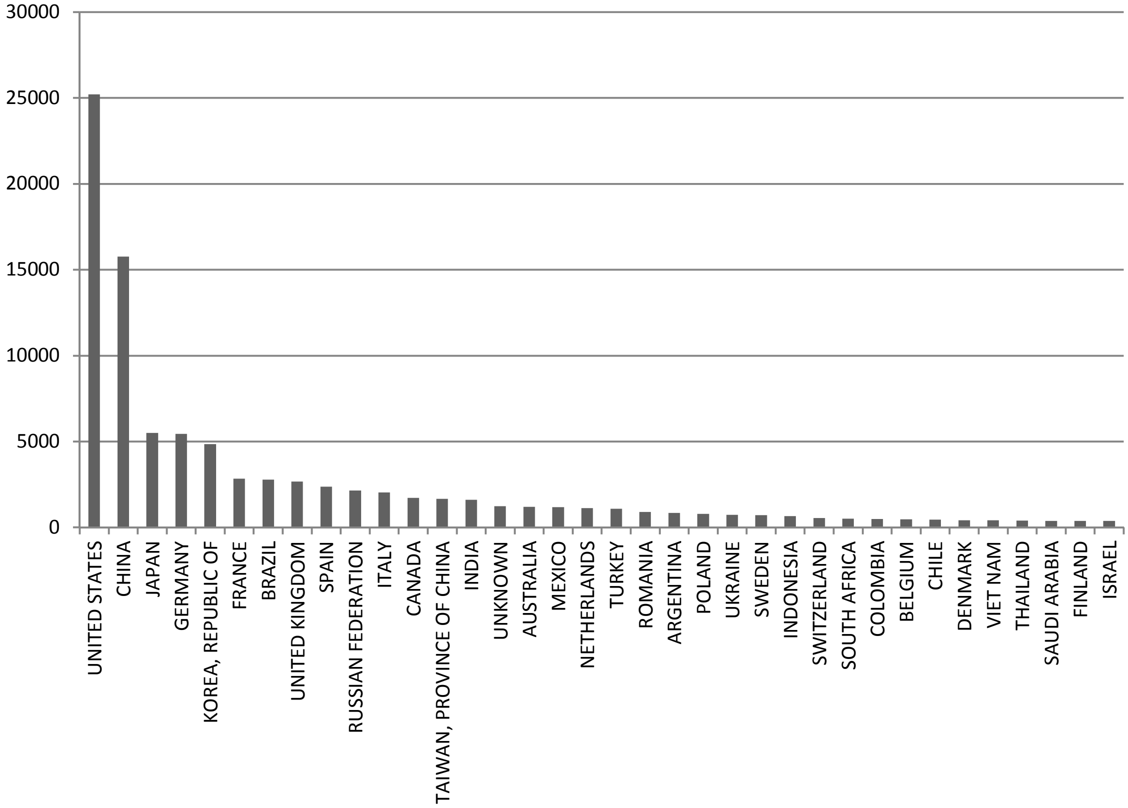

Figure 15: Countries Containing More Than 350 IP Addresses

8.5.1 I_j+I_mC and SC Comparison

There are disparities between the percentages of countries represented in the I_j+I_m set and what we would expect to see in the IPv4 address space. The biggest difference is the group of IP addresses resolving to the United States. The U.S. IP addresses in the I_j+I_m data set occurred three times more frequently than in the S set. There were also many more IP addresses resolving to China in S than in I_j+I_m. Table 17 provides a comparison between the most frequently occurring countries in the I_j+I_m and S data sets.

Table 17: Comparison of IP Location Between I_j+I_m and S

Country	Percentage of APT1 IP Set (1,386)	Percentage of Sample IP Set (100,000)
United States	79.73%	25.21%
Taiwan, Province of China	2.45%	1.66%
Korea, Republic of	2.02%	4.84%
Japan	1.37%	5.51%
United Kingdom	1.23%	2.67%
Thailand	0.94%	0.41%
Hong Kong	0.79%	0.33%
Singapore	0.79%	0.28%
Ireland	0.72%	0.21%
Canada	0.65%	1.72%
Germany	0.65%	5.44%
Portugal	0.65%	0.38%
India	0.58%	1.62%
Poland	0.51%	0.79%
China	0.43%	15.76%
Romania	0.43%	0.91%
Netherlands	0.43%	1.14%
Russian Federation	0.36%	2.15%

8.6 SR: Routing Data for S set

We found the routing types of the sample in the same way we did for the I_j+I_m IP data set. We broke the data into four categories: (1) fixed, dedicated, (2) fixed, other, (3) pop, and (4) unknown. Figure 16 reflects the types of Neustar routing data found for S:

- 65,440 IP address have routing types.
- 65,595 IP addresses have connection types, which means the routing type is fiber, leased line, DSL, cable, or dial-up.
- Of the IP addresses with routing types, only 11% have fixed, dedicated lines through either leased lines or optical fiber cable, indicating they belong to medium- to large-sized organizations, not individuals.

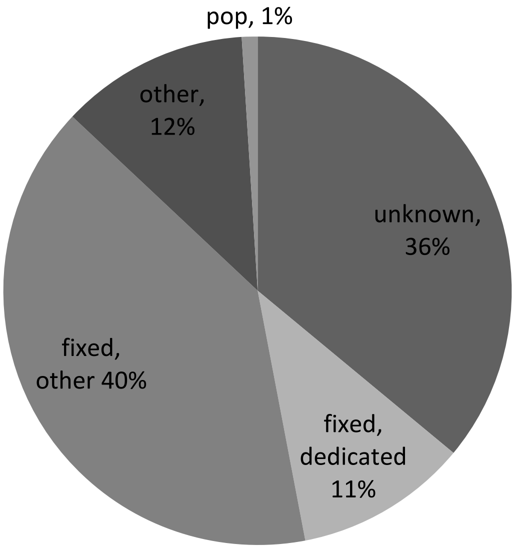

Figure 16: Neustar Routing Types in S

8.6.1 I_j+I_mR and SR Comparison

The routing type indicates how well connected certain machines are to the internet. The “fixed, dedicated” routing type suggests the most stable infrastructure. This category appears almost five times as frequently in I_j+I_m than in S. The “fixed, other” category is less stable than “fixed, dedicated” and occurs twice as frequently in S than in I_j+I_m. There is also a higher occurrence of “other” (various proxies or gateways) routing types in S than in I_j+I_m. Table 18 provides a comparison between the I_j+I_m and S data sets by percentage.

Table 18: Comparison of Routing Type Between I_j+I_m and S

Routing Types	Percent of I_j+I_m (1,386 IP Addresses)	Percent of S (100,000 IP Addresses)
fixed, other	20%	40%
fixed, dedicated	50%	11%
other	1%	12%
pop	2%	1%
other	27%	36%

9 Discussion

Given the analysis we conducted, we made some generalizations about the attributes of the devices used in APT1's middle infrastructure. These generalizations reflect the Mandiant report's description of how APT1 works. Our data is representative of machines already involved in APT1 activity; the data reflects what APT1 was using in its infrastructure, not necessarily what it was looking for when it chose which machines to exploit. We can only provide a high-level generalization of its operations, not detailed analysis. We first discuss each of the attribute points: infrastructure owners, location, fingerprints, and open ports. We then provide generalizations for the infrastructure: intermediary C2 servers, malware servers, hop points, and inactive servers.

9.1 Infrastructure Owners

The research based on the ASNs and domain names suggests that APT1 was choosing stable organizations to build its middle infrastructure. This is also confirmed by the Neustar routing analysis: APT1 was targeting fixed, dedicated routing types as part of its infrastructure instead of something less stable. APT1 was hidden in plain sight; it was not using obscure ISPs or hosting providers. Rather, most of the companies chosen are very well known and easily found during a web search. After analyzing the routing data, we can also conclude that APT1 targeted fixed connections such as fiber, T1, and DSL. This makes sense because it would be costly and inefficient for APT1 to use infrastructure that was unstable and potentially unresponsive for active C2 servers.

We found that APT1 seemed to target certain ASNs, with over half the IP addresses in the I_j+I_m set clustered within a small number. These may have been exploited, but it is also possible that APT1 was purchasing the hosting services of some of these organizations. The remaining IP addresses occurred in a more distributed manner across many ASNs. These may have been used as anonymizing hop points or belonged to clusters where the other IP addresses were just not present in the I_j+I_m set.

9.2 Location

The majority of the IP addresses are located in the United States, though some come from around the world. Taiwan and other Asian countries account for four out of the top five non-U.S. countries associated with I_j+I_m IP addresses. Most other non-U.S. countries have fewer than 10 IP addresses in the data set. In the United States, a majority of the IP addresses resolve to California, which holds almost five times the IP addresses found in Arizona—the second highest. This may be deliberate or could simply be the result of California being the location of both Psychz Networks and Krypt Technologies.

9.3 Fingerprint Data

The data suggests that APT1 was targeting Windows machines dating to the time period when it began operations in 2006. The top fingerprints resolve to Microsoft Windows Server 2003, Service Packs 1 and 2, and Microsoft Windows XP Service Pack 2. Although these machines seem outdated in 2013, they were very common in 2006 and would have been likely targets for either zero day exploits or unpatched machines. The high occurrence of Linux kernels in the range of 2.6.32 - 3.2 suggests that APT1 may have switched OS preferences around 2010 [Linux Kernel Organization 2013].

One fingerprint that surprised us was the occurrence of Microsoft Xbox game consoles. All these reside on fixed, optical cable connections, with three in France and two in the United States. All five IP addresses belong to an ASN registered to Google Inc. Since these fingerprints are just within our cutoff range of a 75% fingerprint match, we suspect they may be misidentified.

9.4 Malicious Code

The 259 unique malicious code hashes found in the meta data from CERT's runtime analysis efforts suggest there is a potentially larger infrastructure of APT1 operations than what was released to the public.

9.5 Port Data

Since we are looking at the middle infrastructure, we believe that some of these machines in our data were used purely for hop points, while others were used to directly compromise the target. Mandiant suggested that APT1 C2 servers are located in Shanghai and gather information from the servers located in the United States. Our data suggests that part of the middle infrastructure was used as "intermediary C2 servers," which pushed off information to the main C2 servers located in Shanghai. Other machines in the infrastructure are used purely as vehicles for exploitation. There is depth between the C2 servers and the ultimate targets; however, our data does not suggest how much depth exists.

9.6 Intermediary C2 Servers

Two distinctions in C2 servers were identified. Most of the C2 servers appear to use port 443, which is used for several of the malware programs identified by the Mandiant report, but there is also a smaller set that uses port 111. In general, intermediary C2 servers

- are webservers
- have fixed connections, either leased lines or optical fiber
- reside on IP addresses assigned to well-known, well-connected organizations
- are located in the United States or Asia

Those relying on port 443

- also often use port 3389 once the infrastructure has been compromised, as identified by the Mandiant report
- or have three or more other open ports, including one or more of the following
  - 21
  - 25
  - 135
  - 53
  - 22
  - 1025
  - 3306
  - 139
  - 445

  - 1723
  - 110
  - 1026
  - 143

Those using port 111 (ONC RPC or Sun RPC)

- are Linux 2.6.32 or higher
- often also have port 22 (SSH) open

9.7 Malware Servers

These machines are used, for instance, as malware distribution points or mail relays. They

- likely are also web servers that contain malware that can be pushed to target machines in some manner
- either have ports 21 or 3389 open, or have three or more open ports, including one or more of the following
  - 1723
  - 135
  - 139
  - 25
  - 110

9.8 Hop Points and Inactive Servers

The available data sets did not allow determination of a profile for IP addresses with no open ports or those with only port 80 open. These are assumed to be hop points, inactive C2 servers, or inactive distribution points. The hop points were used to anonymize traffic and do not necessarily require capabilities beyond handling web traffic.

10 Future Work

Many other aspects of APT1 are worth exploring, such as understanding the role of bulletproof hosting providers in the APT1 data. Because at least two of the ASNs in the data set provide bulletproof hosting services, it would be interesting to determine if APT1 was purchasing services or exploiting those organizations. Another question to explore is if the low occurrence of an ASN that occurs in this data set indicates an instance of random exploitation, incomplete information (for instance, more IP addresses of that ASN have actually been compromised but were not flagged or released as being used by APT1), a single exploited company that was using multiple ISPs, or some other unrelated reason. Exploring the role of the few dial-up connections may also provide additional insight into APT1 operations in the future.

11 Conclusion

This study sought to understand what was necessary for APT1 infrastructure. JIBs INC260425 and INC260425-2, along with a pDNS search of Mandiant-released domain names provided us with 1,386 IP addresses associated with APT1 activity. The Internet Census 2012, Open Resolver list, SIE@ISC rDNS data, and Neustar GeoPoint data contributed information associated with the APT1 IP addresses that was helpful in analysis. Actual owners of the middle infrastructure and its location, fingerprints, and open ports provide insight into what appears to be used for the APT1 intermediary C2 servers, malware servers, and hop points.

APT1 uses stable, well-connected infrastructure from either hosting providers or ISPs in the United States. Most of the middle infrastructure runs Windows 2003, Windows XP, or the range of Linux kernels 2.6.18 - 2.6.32. Additionally, APT1 infrastructure may be evolving because the Windows machines appear to be much older than the Linux ones.

Useful data for enumerating a particular infrastructure does not need to be classified or proprietary. Our study illustrates that unclassified data from multiple sources, when used together, can draw, at a relatively low cost, many of the same conclusions of an expensive study. Our analysis is easily replicated, and our process can be used to easily evaluate the infrastructure of other malicious groups.

Appendix: DNS Names Pulled from the Security Information Exchange Data

0007722.com
0016.qq.bjxidebao.com
001rtys.com
00234.com
0104.qq.bjxidebao.com
023boys.com
029zh.info
03877.com
0410dj.com
0471.qq.bjxidebao.com
0551dm.com
0575.me
06kv.com
0755ktxs.com
0755mdkt.com
0776.qq.bjxidebao.com
0893.qq.bjxidebao.com
0dwx.com
10.258982.com
1069sc.com
110.bm110.com.cn
110ld.cn
1124.qq.bjxidebao.com
12.258982.com
1205.info
123050.com
12341090.cn
1234abcd.com
125801069.com
128556.net
132l.com
1337legendenbude.zapto.org
133wg.w99.1860php.com
1367.qq.bjxidebao.com
1379.xmhost.ludaoidc.com
144654.com
14ts.com
14vd.com
152330.com
1546.qq.bjxidebao.com
155.258982.com
15dushi.com
1639762.com
164.258982.com
1674.qq.bjxidebao.com
173-163-133-177-centralpennsylvania.hfc.comcastbusiness.net
173-252-255-52.take2hosting.com
177456.com
1775.qq.bjxidebao.com
179444.com
188.258982.com
18renti.info
192.258982.com
19466.com
1staab.com
1staffonline.com
1staffonline.net
1staffonline.org
1stmob.com
1svc1.exchange.1-service.com
1xtx.com
2.79dbb44ec739a693.griddnsd.global.sonicwall.com
2000365.com
2001365.com
201.258982.com
2012jerseyswholesale.org
202-176-81-175.static.asianet.co.th
204-14-142-210.utilitytelephone.net
204-74-218-145.take2hosting.com
208.37.108.211.ptr.us.xo.net
208.43.154.7-static.reverse.softlayer.com
210.249.196.216.ded-dsl.fuse.net
210.ylbanqian.com
2253.qq.bjxidebao.com
2255.qq.bjxidebao.com
225577.co.cc
227227.com
228royal.com
235158.com
2352.ylbanqian.com
2365.qq.bjxidebao.com
246899.com
25.258982.com
258982.com
262999.com
266488.com
2705.qq.bjxidebao.com
2791.999hhh.net
2795.999hhh.net
29ig82qwpxkfsaege4gapfw3jigmdoe4vn6otcpivtuowr5v3a.41.cgfde.com
311345.com
3233.qq.bjxidebao.com

331888.com
333773.com
34563456.com
345mmm.com
3470.ylbanqian.com
355179.com
359999.com
3604.ylbanqian.com
37.600dns.info
3739.ylbanqian.com
3745.ylbanqian.com
391456.com
3cshopping.com
3jnjpharma.com
4104.ylbanqian.com
4105.ylbanqian.com
4109.ylbanqian.com
4111.ylbanqian.com
4117.ylbanqian.com
4228.qq.bjxidebao.com
4256.qq.bjxidebao.com
4405.qq.bjxidebao.com
444456.com
445456.com
44hb.com
44zg.com
456mmm.com
458441.com
46.258982.com
463456.com
464747.com
477877.com
488889.com
4j28.com
4thwatchersportal.com
500029.info
50919.com
51.258982.com
518jzsc.37.600dns.info
51xxkj.com
52.16.1343.static.theplanet.com
521999.com
5219999.com
521ufo.com
52diany.com
53.258982.com
545188.com
558333.com
558558.com
559.258982.com
5611.qq.bjxidebao.com
581888.com
582888.com
584.258982.com
58518.co.cc
586.258982.com
5869.com
59.258982.com
59-120-140-156.hinet-ip.hinet.net
594107com.37.600dns.info
598928.com
5pur.com
624444.com
64.258982.com
64.3.53.146.ptr.us.xo.net
64.3.53.148.ptr.us.xo.net
65.97.169.210.nw.nuvox.net
65-114-195-226.dia.static.qwest.net
6529.qq.bjxidebao.com
65cq.com
66-111-37-26.static.sagonet.net
66-178-7-201.reverse.newskies.net
6647.qq.bjxidebao.com
665171.com
66567.com
6674.qq.bjxidebao.com
668bc.net
67.109.132.202.ptr.us.xo.net
67-133-107-131.dia.static.qwest.net
67-135-235-198.dia.static.qwest.net
6774.qq.bjxidebao.com
67896789.com
678mmm.com
678vip.com
68-72-242-130.ded.ameritech.net
688678.com
69-152-184-182.ded.swbell.net
6923.qq.bjxidebao.com
69-2-71-205.static.networktel.net
6vrelay.com
70-89-213-145-rees-funeral-home-inc-in.hfc.comcastbusiness.net
70-89-213-181-genesis-health-care-il.hfc.comcastbusiness.net
70-89-213-201-kgc-services-inc-il.hfc.comcastbusiness.net
70-89-213-241-glenbrook-excavating-and-concrete-inc-il.hfc.comcastbusiness.net
70-89-213-249-lake-shore-country-club-il.hfc.comcastbusiness.net
70-89-213-66-arlington-limosine-il.hfc.comcastbusiness.net
70-90-53-170-fresno.hfc.comcastbusiness.net
70chun.balutianjia.com
70ph.com

7123.qq.bjxidebao.com
71-6-51-180.static-ip.telepacific.net
71-6-51-181.static-ip.telepacific.net
720am.visualradio.org
74-92-102-227-philadelphia.hfc.comcastbusiness.net
7642.qq.bjxidebao.com
771321.com
777796.com
77links.info
77rh.com
789mmm.com
7909.qq.bjxidebao.com
79907.com
7perhour.co.uk
803.cc
818456.com
818758.com
82.sophio.com
855233.com
857999.com
8595.qq.bjxidebao.com
866999.com
875678.com
8809.qq.bjxidebao.com
8833.qq.bjxidebao.com
8849.qq.bjxidebao.com
887suncity.com
8989f.net
900828.com
911.cnnnewsdaily.com
915443.com
91epay.com
92.15.5646.static.theplanet.com
94-195-239-81.zone9.bethere.co.uk
9500.fuanna.njslrc.com
9535.qq.bjxidebao.com
9628.qq.bjxidebao.com
9799.qq.bjxidebao.com
988648.com
99286.net
99407.com
9962.qq.bjxidebao.com
9999978.com
999usa.net
999xyz.net
99sqz.com
99way.net
9lele.3322.org
9pk123.com
9urdkpdpnd33t2uvaq7hkkejq6eawvb6b32dumgf4ldd6sbgve.41.nhtyd.com
aa2007031190d2f9508d.userreverse.dion.ne.jp
aa5.com
a-ad.arrowservice.net
aameinv.com
aaragon.net
abcballetschool.org
about.purpledaily.com
abssatellite.com
ac963.com
academybullets.usswim.net
accordinc.com
acousticaldesign.com
acousticaltreatments.letgoonsale.com
a-craft.zapto.org
acujody.com
ad.sctzzj.com
adamsrestequip.com
adbegone.com
adcoservices.com
addtimes3.com
admin.arrowservice.net
admin.datastorage01.org
ads.dragbike.com
adsl-072-148-171-041.sip.bct.bellsouth.net
adsl-072-151-101-055.sip.asm.bellsouth.net
adsl-074-165-093-005.sip.chs.bellsouth.net
adsl-63-195-112-159.dsl.snfc21.pacbell.net
adsl-75-52-111-62.dsl.ltrkar.sbcglobal.net
advantageempower.com
advantageoutsource.com
advertiser-serbia.com
ae4en558r8gcmj9sbsra7u5e8d8v45rt7froujsbrvkumrep.45.okjyu.com
aerys3.servegame.com
afcea.csproject.org
affiliatefilecabinet.com
affm.info
affordwatch.com
agma.ipsecsl.net
ahit.oncourselearning.com
aidincorporated.org
aig3.com
aigocc.com
aiic.arrowservice.net
aikongtiao.cn
aims.ws
aimscomputersystems.com
aimssecuresite.com
aip.comrepair.net
airbus.downloadsite.me
airforce.newsonlinesite.com
airmaxbrand.com
ait.busketball.com

ak326.info
alarm.arrowservice.net
albumarchive.us
algosys.com
alidalyssens.com
alixandkristin.com
all-energy.niau.org
allston.accesssoftek.com
alphapenguins.com
altrusaofcharlotte.org
alysem.marineaugust.com
am.ber88.com
amdg.anniemooresnyc.com
americanenergyproduction.com
amethyst-hill.com
amicuspublico.com
a-million-bucks.com
amk-services.com
amne.purpledaily.com
ams.busketball.com
amsc.usswim.net
amusementparksigns.com
amx.lcdtv65.com
amyandersonportfolio.com
andrijailic.com
anglo.arrowservice.net
anhraf.net
annettehetsko.com
anniemooresnyc.com
anshun.saomen.com
antayundongxie.mannasoft.cn
anything.com.sg
aol.arrowservice.net
a-ol.arrowservice.net
apa.infosupports.com
apaitpdc.apaitonline.org
a-pep.arrowservice.net
aperaceparts.com
app.satelliteclub.info
apple.bostonheartdx.com
apss.newsonet.net
aralco.ky
ares.aunewsonline.com
arg.auestrap.com
a-ri.comrepair.net
arinc.info.tm
arinc.us.to
arinternationaltrade.com
arm.armed.us
army.newsonlinesite.com
arnoldliao.com
arozeny.com
asiaengineering.co.th
asiaexotic.com.sg
asian.1staab.com
asiaprecision.com
asiaprecision.net
asp.businessconsults.net
asp.busketball.com
assets.myweddingworkbook.com
asterthai.com
astore.onedaysweet.com
asw2.htoademos.com
aswdemo1.htoademos.com
aswdemo10.htoademos.com
aswdemo11.htoademos.com
aswdemo18.htoademos.com
aswdemo7.htoademos.com
aswrewards.com
atc.info.tm
atch.ipsecsl.net
a-tim.infobusinessus.org
ativomedia.net
atom.busketball.com
atspdx.com
attnpower.com
atxedk.com
au23.com
a-uac.arrowservice.net
auto.aoldaily.com
auto.companyinfosite.com
auto.gmailboxes.com
auto.livemymsn.com
autoaccidentattorneyindianapolis.com
autobarncatalog.com
autodiscover.bostonheartdx.com
autodiscover.csceng.com
autodiscover.jackmont.com
autodiscover.lornet.com
autodiscover.lwpc.com
autodiscover.treepeople.org
autopartsfreak.com
autopartswarehousedirect.com
auto-trak.net
awogb34.coffeeteastationary.com
a-za.businessconsults.net
a-za.infobusinessus.org
b2networx.com
b2networx.net
back.sux.ms
back.tang.la
backg.organiccrap.com
bag.replicagarden.com
bah001.blackcake.net

baidu.sdjyjy.com
baike.chengrenchaoshi.com
bandcprintwear.com
bangkokcity.co.th
bangnacomplex.co.th
bangzhongbang.net
banners.dragbike.com
bannerserv.dragbike.com
barsprogram.com
baselewis.com
basketball.todayusa.org
bass.busketball.com
baxleywells.com
bbbvent.zapto.org
bbs.busketball.com
bbs.caifutx.com
bbs.itrmall.com
bbs.sctzzj.com
bc2.bananajob.co
bcbgdressesoutlet.net
bcsmail.bridgewaybh.com
bcsmail.bridgewaycounseling.com
bctechnologies.org
bda.arrowservice.net
bdjiafeng.com
bdxw.ns06.net
beauty.mrslove.com
beautyvalleys.com
bebeposhe.com.sg
bechtel.twilightparadox.com
bedook001.info
bedrock.cyberhq.com
bee.businessconsults.net
bellamodathai.com
bellfamilynursery.com
benbensons.com
berkeleyaquatic.org
berzeshop.info
best.bestseo.hk
bestalbum4you.com
bestbanjos.letgoonsale.com
bestboatcovers.letgoonsale.com
bestboats.letgoonsale.com
bestcasuals.com
bestexercisefitness.letgoonsale.com
bestforexliveroom.com
bestgamingkeyboards.letgoonsale.com
bestlenses.letgoonsale.com
bestoakleysunglasses.net
bestphoto4you.com
bestpoolladders.letgoonsale.com
bestprogramming.letgoonsale.com
bestserviceplans.letgoonsale.com
bevlyne.com
bfl-llc.com
biassm.org
bibleview.org
biblicaltours.eilatinter.co.il
bigborethumpers.com
bigdigi.net
bikesbicyclesbest.letgoonsale.com
birdrf.com
bitsovegas.com
bizconf.com
bj.2schina.net
bjtxgc.com
bksy.businessconsults.net
black-cables.org
blancobydesign.com
blast.usswim.net
blockheadautoparts.com
blockheadautoparts.sophio.com
blog.arrowservice.net
blog.scaneagle.com
blog2.lflinkup.com
blogs.mrbasic.com
blogweb.mrslove.com
blokstudio.net
blue.mk.co.kr
bluefin.aunewsonline.com
bluestarredimix.com
bnhqah.com
bo.ber88.com
boats.savebigsale.com
bobbycaldwell.com
bonbons.com
bookmark4seo.com
bookmarkitnow.com
books.mrface.com
boothdermatology.com
borasparts.com
boseathorsham.com
boston.longbit.com
boston.padhost.net
boyametal.com
boyer-boyer.net
boyerfamilypa.org
bpgc88.com
bpserver.biz
bpwpa.com
brankopavlovic.rs
bravocreative.com.hk
bretkepnerphotos.com
bretonhouse.ca

bridgeclubbeveren.be
bridgewaycounseling.com
brockracing.com
brocksperformance.com
brokebuster.com
brooklynnets.com
bst.dtstech.net
bswt.purpledaily.com
budreck.com
bug.pudnet.net
buildagreatwebsite.com
built.arrowservice.net
bulklist.info
bullseye.yolk.com.sg
buniqe.com
businessview.net
buttetarpons.usswim.net
buycow.busketball.com
buyer.arrowservice.net
bydremonster.com
byid.mylftv.com
c01.philippi.pmcc4w.org
cache.aolon1ine.com
caci.blackcake.net
caci.businessconsults.net
caci.infosupports.com
caci2.blackcake.net
caci2.businessconsults.net
caci2.infosupports.com
cadfait.softsolutionbox.net
caifutx.com
calendar.fitz.k12.mi.us
camdensc.org
cameronians.com
campdiscovery.net
canadianloans2.ca
cannonts.cannondesign.com
canyonsunskincare.com
captainlen.com
card.mydad.info
carfaxdentalmedical.com
cargo-unlimited.com
cargo-unlimited.indexware.com
carkhabri.com
carolinahomeadditions.com
carpartsplace.com
carpenterracing.com
carsiotis.com
cars-repair.com
cash-nows.com
catalog.bennettauto.com
catalog.bucks4x4.com
catalog.gmpartsnow.com
catalog.lacroixtuning.com
catalog.palacroix.com
catalystrental.com
caymangolftour.com
caymanturnings.ky
cbrzone.com
ccagency.com
ccghm.com
cdi.infosupports.com
cdmswin2kws.cdmsinc.net
cdpa-architects.com
celetex.com
center.busketball.com
cestquoieducationlandmark.com
cfs-server.callawayfinancial.com
cfyci.com
cgdininggeniusv3.caffegrazie.com
chaba.thaiinterhost.com
chahao8.net
chamus.gmailboxes.com
chanel-bag8.com
chaplinpr.com
chascomachine.com
chat.webdirectbrands.com
chatwithroger.informedvoter.info
cheapbigbrand.com
cheap-papers.org
check.staycools.net
chineseroom.org
chongzuo.saomen.com
chris.oncecalledearth.com
chs.ujheadph.com
chtchronicles.net
chuckfaganco.com
city.gmailboxes.com
cityhallnewyork.com
civis.com
clarksafeclark.com
clarkseifclark.com
class.arrowservice.net
classified.8800.org
client.seotool.com
climate.undo.it
clocks.savebigsale.com
cloudtcm.com
cloudtcmpro.com
clsupreme.com
cmp.gmailboxes.com
cnnnews.yourtrap.com
cntc8848.net
coachfactoryoutletor.com

coachmotor.com
coapt.com
cobolweeda.in
code.jobsadvanced.com
code.mcafeepaying.com
coffeenuts.wdbdev.com
coffeespoons.com
combathelp.com
combat-help.com
commeagle.com
commoditymanagementblog.com
community.bostonheartdiagnostics.com
computerpossibilities.com
conf.callamerica.com
connomac.com
conour.com
conourlaw.com
contact.bigish.net
contact.jobsadvanced.com
cope.3322.org
cordlesstoolbhc.letgoonsale.com
corn.busketball.com
corpdns.vizvaz.com
cosmanchem.com
cotton.vo3.net
cottonwood-charlotte.org
couragetoleap.com
cowboy.bigish.net
coy9.info
cp.enshi.us
cp.rs
cp0288.com
cpms.ky
cp-train1.kb.net
cqboys.com
crab.arrowservice.net
creativecivilization.com
crmserver.frankwilliams.com
crnojevic.rs
cruiserzone.com
crumb.ns06.net
crying.crabdance.com
crystalsolutionsllc.org
cscbdc01.csceng.com
csceng.com
ctx-na.purpledaily.com
cutsingerchiropractic.com
cva1.tnpaschershop.com
cwj5.info
cyberspacehosts.com
cyberspacehosts.cyberspacehosts.com
cyberspacemagic.com
cycleconceptsracing.com
cz668.net
d.csceng.com
da.comrepair.net
dae4.ns06.net
daewoo.com.au
dagent.com
dagent.net
dangernet.com
danxia-china.com
danxia-sanitaryware.com
darkinfinity.zapto.org
darktr4k4.no-ip.org
data.toythieves.com
databaidu.com
datastratum.com
datatek-inc.com
date.gmailboxes.com
date.rssadvanced.org
daten-loeschen.org
dating.silversurfersguide.com
daumberto.lanteck.net
daumbertonyc.com
davisdisposal.com
d-cham.com
dci.dyndns.tv
ddoserbot1231.no-ip.info
de.pc-free-games.com
deborahspark.com
deco.ns06.net
dedq138.dmt-portal.com
deeshashop.info
delsperformance.com
demesstified.com
demo.homefrontsandiego.com
demone2011.no-ip.org
demos.coapt.com
denis-home-1.csceng.com
dentino.com
dentino.net
dentino.org
deqn.net
derrickdenis-08.csceng.com
designercheapwallets.net
designerwalletmall.com
dezenaa.zapto.org
df2342.co.cc
dfait-kl.worthhummer.net
dfgz88.com
dg.saomen.com
dgv3.vino212.com
dh.abc41.info

diamondsti.com
dickdyermercedes.com
dickdyeronline.com
dickdyervolvo.com
dietliesrevealed.com
digitalagent.us
digougaiban.com
dilcosolar.com
dillernursery.com
dinkydonuts.com
diqing.saomen.com
dir.oem-bmw-parts.com
dir.oem-mercedes-benz-parts.com
directoryservers.letgoonsale.com
ditor.ns06.net
dj.ezeze.tk
dl.biblebible.com
dlghotel.com
dltxsl.com
dm808.w99.1860php.com
dmcmy.com
dmcspkj.com
dmt-portal.com
dns.elevation.com.tw
dns.welcomehomeloans.com
dns1.dnet.net
dns1.retrbol.com
dns1.trackaadg.com
dns2.retrbol.com
dns2.tcnoc.com
dns2.trackaadg.com
doc.sjolzy.cn
domain.busketball.com
done.succourtion.org
dongying.saomen.com
down2.sst1.info
down2shop.com
downalarm.com
download.acmetoy.com
download.applesoftupdate.com
downloads.applesoftupdate.com
downloads.ikwb.com
downs.mooo.com
draeger.rs
dragbike.com
dragbikephotos.com
dreamsurface.net
drinkwater.gmailboxes.com
drivecontrols.com
drjs.com
drmartens.com.sg
drp.itdevworks.com
drs.infosupports.com
ds.solution.com.sg
dsl092-012-252.sfo1.dsl.speakeasy.net
dtccatalyst.com
dubai-groups.com
duboselaw.com
du-ia-diamond.ia.drexel.edu
duingusnin.info
duk.asia
duokee.com
dwmerkey.com
dyfjt.com
dyn.newsonet.net
dzcpm.com
e.sese.pm
eadparts.com
eagle.zyns.com
eaglemagnetic.com
earphonesbeats.com
eastcoastautoparts.net
easy-investment.biz
eatmyink.com
ec2-184-72-82-144.compute-1.amazonaws.com
ecli-cow.infobusinessus.org
eclipsecmfwrf.infobusinessus.org
economic.mooo.com
ecsunglasses.com
edifyconsultant.com
education.gardenriver.ca
education.rssadvanced.org
eecs745.jasonfugett.com
eerduosi.saomen.com
efactor.amerifac.com
egame.mooo.com
egoldinvestment.org
ei2u.com
eilatindia.eilatinter.co.il
eilatinfo.com
eldonspecialties.com
electronicdrums.savebigsale.com
elem.vpnhouse.net
elevation.com.tw
emascenter.com
emasweb.com
embasjtu.com
embassy.india.sh
emersonlimited.com
emmarossosteopathypractice.com
emp.eadsmurraypugh.com
empowerone.com
engineer.lflinkup.org
engineering.newsonlinesite.com

entech-group.com
entheos.com.sg
entrustrm.com
enviroment.us.to
environment.mooo.com
environment.uk.to
epa.yahoodaily.com
equipic.com
equiv.ipsecsl.net
equiv.ocry.com
eri.serveuser.com
erniesgallery.com
ershou.saomen.com
es.pc-free-games.com
e-shoppingguide.com
esku.eilatinter.co.il
esoterism.org
etonnant.com
eum.businessconsults.net
eurosatory.mit-info.com
evolvemotorsports.com
exa.coastmaritime.org
exactearth.info.tm
exchange.ashtonplace.com
exchange.babelroad.net
exchange.bostonheartlab.com
exchange.golfnaperville.com
exchange.itsystemworks.com
exchange.thomsclan.com
exchange.vestarcapital.com
express.pmac.com
f.i7life.com
f.vaone.info
f.vpncup.com
f1f.ns06.net
faahsai.com
faan.cn
fairwaves.com
fangchan.saomen.com
fangqi.6600.org
fansex.mynetav.org
faq.bird-technologies.com
fasa.bigish.net
fasa.marsbrother.com
fasa.newsonet.net
fasa.purpledaily.com
fashion.cnnnewsdaily.com
fastbygast.com
fbrshop.com
fccmv.com
fcop.net
feaceblog.mefound.com
feedback.changeip.net
feedback.dynamic-dns.net
feedback.itemdb.com
feedback.justdied.com
feedback.longmusic.com
feedback.qpoe.com
feedback.youdontcare.com
feedback.zyns.com
feigou.cc
fel.labutes.com
fengqiuxian.com
fengziyu.net
ffea.fitz.k12.mi.us
fhc.alphagammadelta.org
fijishaadi.com
file.myftp.info
file.nytimesnews.net
file.serveusers.com
files.downloadsite.me
filmat36.com
finance.cnnnewsdaily.com
finance.thehealthmood.net
finance.todayusa.org
finance.usnewssite.com
finekl.worthhummer.net
firebirdgifts.com
firedgv1.firebirdrestaurant.com
firenapolitano.com
first.voiceofman.com
fishingreels.savebigsale.com
fitworks-anderson.com
fjddz.com
fjiao.net
flagulfbeachvacations.com
flash.aoldaily.com
flash.aunewsonline.com
flash.cnndaily.com
flash.jobsadvanced.com
flash.livemymsn.com
flash.mcafeepaying.com
flash.themafia.info
flash.usnewssite.com
flash.yahoodaily.com
flash4ui.com
flex.ns06.net
floradelmar.net
floydleeband.com
flqz.net
flucare.worthhummer.net
fmslaw.net
fni.newsonet.net
fom-prokuplje.co.rs

food.msnhome.org
football.canoedaily.com
forex-investments.biz
forex-live-day-trading.com
forexroomreviews.com
forexrose.com
forextradingradio.com
form.daumbertonyc.com
forum.bestseo.hk
forums.dragbike.com
fountaininjurylaw.com
fourforchrist.org
fourseasonsrestaurant.com
foxjet.usswim.net
fr.pc-free-games.com
free.gmailboxes.com
free.vssigma.com
freeappfans.com
freedom-discount.org
freelanceindy.com
freesexdoor.com
freewave.us.to
freeworkerscompreview.com
freshreaders.net
fresnofirst.com
friendsdd.com
frodo.lornet.com
frt6.info
fsyuxin.com
ftcarson.countertrade.com
ftp.aimscomputersystems.com
ftp.cctconsulting.com
ftp.ics-no.org
ftp.ieee.mynumber.org
ftp.mrduffy.com
ftp.netdisk.serveuser.com
ftp.purpledaily.com
ftp.safavieh.com
ftp.somervilleinc.com
ftp.sophio.com
ftp.tpt.com
ftp.xuping.net
ftp2.topcon.com
fullmoonlightnin.com
fullmovies.freesexdoor.com
funtravelbaby.letgoonsale.com
fuxiang.se
fwb.blackcake.net
fwb.infosupports.com
fwmo.businessconsults.net
fwmo.newsonet.net
fzl22.cn
gabdaddy.com
gallerywestnowhere.com
game.aoldaily.com
ganyuyin.com
garde.ns06.net
gardenriver.ca
garyclarkracing.com
gassper.no-ip.biz
gastongators.usswim.net
gatecrafters.tom.wdbdev.com
gatesupply.wdbdev.com
gateway1.usa.artinhand.com
gatu.arrowservice.net
gay315.com
gay61.com
gay-6910.com
gaycq.com
gayongpasak.org
gd.2schina.net
gdasmoney.com
gege.newsonet.net
gelixs.com
genbukan.ca
geogridwalls.com
getcd.org
ggder.com
gija.mk.co.kr
gimli.lornet.com
gimli2.lornet.com
girlse.info
girlsloveshoes.info
gl.gmailboxes.com
glassesdesignerframes.com
glex2012.niau.org
glfp.info
glj.purpledaily.com
glzyswim.org
gm.sophio.com
gmdsystems.net
gmpartsnow.com
gmpartswarehouse.net
gmqsct.w99.1860php.com
goknives.com
goldenbayinc.com
goldtowne.biz
goldtowneusa.com
golfclubs19.com
golfnaperville.com
google.applesoftupdate.com
gorgg.org
gottabeamazing.com
goucsc.com

gps.aidtax.com
graceislandresort.com
graduateslandmarkeducation.com
graduateslandmarkforum.com
grandlabel.com
gravitybound.org
greasetrapmaintenance.com
greatesoft.net
grifonenyc.com
grillssmokers.savebigsale.com
groupware.cas-architekten.ch
gsdftp.dtstech.net
gsxrzone.com
gszone.biz
gtaautoparts.ca
guage.ns06.net
guage.vpnhouse.net
guigang.saomen.com
gunstorage.letgoonsale.com
guynight.com
gylehua.com
gz.saomen.com
gzcityhotels.com
h1.hw247.net
h69-11-244-91.mdsnwi.dedicated.static.tds.net
habad.eilatinter.co.il
hack568.com
hackerstyler.no-ip.biz
hagermanparts.com
haibei.saomen.com
haipiy.com
handicraftvilla.com
handsperformance.com
haogw7.com
haoyun.xmhost.ludaoidc.com
hapaxsearch.com
haran.dougpoland.com
haran.dougpoland.net
haran.heathermariedesigns.com
haran.polandconsulting.net
haran.polands.org
harcoalgrillsbest.letgoonsale.com
harris.info.tm
hayabusazone.com
hayneedle.seotool.com
hb12369.org
hc7.beotel.net
hcbi.org
hcgdgs.com
hdg.cc
hdhfc.com
hdlgdxcbs.com
hdmimall.com
hdzdjj.com
health.jobsadvanced.com
healthbelieve.com
healthcareinteriorsdigest.com
hearingbest.letgoonsale.com
heavypayments.com
heb.2schina.net
hebja.com
heirloomrosedays.com
hektargroup.com
hektargroup.com.my
hektargroup.comwww.hektargroup.com
hello.usposters.net
help.dns-dns.com
help.dynamic-dns.net
help.thehealthmood.net
hen.2schina.net
hendrickseng.com
herculesafe.com
hexianguan.com
heyjude.eilatinter.co.il
hezuo18.com
hg93.com
hh2.1526.25u.com
hh2.5042.25u.com
hh2.58946.25u.com
hh2.woa-8927.25u.com
hh3.5278.25u.com
hh3.58946.25u.com
hh3.8692.25u.com
hh3.h02-xi03.25u.com
hh3.tlww-089.25u.com
hideawaybingo.com
hifo.net
highlandsranch.usswim.net
hikingbootsrated.letgoonsale.com
hill.arrowservice.net
hill.businessformars.com
hill-billyboggers.com
hk.4ren.net
hk-cpa.hkwww.com
hm-cca.com
hn.2schina.net
hnhks.com
holidayadventureslsa.com
holidayways.com
holleman.rs
holyzhou.com
home.brandywinema.com
home.sctzzj.com
home.staycools.net

homefrontsandiego.com
homefrontsandiego.org
homer.welcomehomeloans.com
hometown-insurance.net
homeworz.com
honkweasel.com
host121.porar.com
hostmaster.carfaxdental.com
hostmaster.emmarossosteopathypractice.com
hostmaster.kgartsindia.com
hostmaster.storeinamerica.com
hotshotzz.com
hotspotautoparts.com
house-sales.info
hp4cb09a.jackmont.com
hp-networking.pcpronet.com
hq.vectorsinc.com
htiins.com
htoa.com
htoaarda.com
htoademos.com
htoamemberinfo.com
http.progammerli.com
https.khhahaxd.net
https.lksoftvc.net
https.mrbasic.com
huachengxyk.com
huaikoeng.com
huntpropertynow.com
huochepiao.org.cn
hw247.net
hxsnn.com
hydrangeaplus.com
hyh886288.com
hziso9001.com
i8sj.com
iadc.niau.org
icmti2011.com
icoppinyc.com
idcmailer.com
idealauto.ca
ideallc.net
idi.mooo.com
idudu.net
ieceetest.com
ieee.mynumber.org
iglesiaebenezer.radio1234.com
ihmgjt.org
ilga96.zapto.org
ilovecayman.com
ilovelandmarkeducation.jp
ilovepossibility.com
im33.gulfup.com
image.usnewssite.com
imageone.ujheadph.com
imap.csceng.com
img.bo2k.idv.tw
img.getcd.org
img.ujheadph.com
imnku.com
implants-event.niau.org
indianahuntersforum.com
indykiwi.com
info.applesoftupdate.com
info.authorizeddns.net
info.companyinfosite.com
info.dns-stuff.com
info.freshreaders.net
info.mcafeepaying.com
info.ourhobby.com
info.rssadvanced.org
info.serveusers.com
info.symanteconline.net
info.usnewssite.com
infobusinessus.org
information.aunewsonline.com
information.cnndaily.com
information.defenceonline.net
informedvoter.info
infras.ipsecsl.net
injectorwarehouse.com
inmarsat.dynet.com
innovativos.com
insighterp.com
insitugroup.com
insitugroup.net
insitupacific.com.au
instanc.ipsecsl.net
insulation-tubing.com
integ.info.tm
internationalmolding.com
internetvisionary.com
inthezonestuff.com
inversible.com
invest.gmailboxes.com
invitefeedback.com
iorl.net
ip-208-109-49-66.ip.secureserver.net
ip67-93-15-229.z15-93-67.customer.algx.net
ip67-93-30-146.z30-93-67.customer.algx.net
ip67-93-4-89.z4-93-67.customer.algx.net
ip67-93-54-130.z54-93-67.customer.algx.net
ip67-93-54-98.z54-93-67.customer.algx.net
ip-72-167-162-96.ip.secureserver.net

ip-72-167-34-212.ip.secureserver.net
ip-72-167-37-238.ip.secureserver.net
ipserver.ee.ntu.edu.tw
iris.strangled.net
is.miyays.com
isabelmarantsoldeparis.com
isatap.jackmont.com
ischool.fitz.k12.mi.us
iss.businessconsults.net
issuenews.strangled.net
issues.ignorelist.com
istpl.com
it.newsonlinesite.com
it.pc-free-games.com
item.taobao.com.kolim12.tk
item.taobao.com.kolim18.tk
item.taobao.com.kolim2.tk
item.taobao.com.kolim3.tk
item.taobao.com.kolimj8.tk
item.taobao.com6h.tk
it-leaked.com
itri.auestrap.com
itrmall.com
itsystemworks.com
jackmont.com
jackstraw.coapt.com
jackypow.com
jandstours.com
jandvp.com
japan.yahoodaily.com
jasonschultz.ca
jaszz.net
jaxd168.com
jbigdeal.com
jchbjc.com
jennettespier.net
jennettespier.org
jericho.orderhq.com
jeromedownes.info
jiandadn.com
jianxi.tk
jianyu.com.sg
jiaozuo.saomen.com
jieyang.saomen.com
jinanyanchu.com
jingxuanwu.com
jiuaidu.com
jiuyangshop.info
jiuzhabi.com.cn
jjtristate.com
jm-dc2.jackmont.com
jm-mail.jackmont.com
jm-sql2.jackmont.com
jmtools.cn
jn9988.cn
jnepay.com
jnzljd.37.600dns.info
job.dima.ac.kr
jobbigger.com
jobskillsonline.com
joeasy.info
johnspizzerianyc.com
joyyard.cn
jp57.info
jstcyh001.host.znearly.com
julitg.com
junglejewelsreptiles.com
junzhifu.com
jxwh.net
jxyichun.saomen.com
k211.com
kaiyangroup.com
katos.info.tm
katos.it.cx
kayauto.net
kb.seotool.com
kbadmin-train1.kb.net
kbapi-train1.kb.net
kdzhijia.com
kearnyalumni.org
kentstotz.com
kentstotzracing.com
keplerresearch.dynet.com
keruite.net
kesam.eilatinter.co.il
kesolutions123.nameserverpool.com
kettlekross.com
kfoassoc.com
kgartsindia.com
kiattana.co.th
kidsoutdoorfurniture.letgoonsale.com
kieti.ipsecsl.net
kindadi.com
kingboll.com
kingworlds.com
kiosk05.kis-kiosk.com
kitchenfaucetswwi.letgoonsale.com
kk2.5042.25u.com
kk2.58946.25u.com
kk2.safe-110.25u.com
kk3.13213.25u.com
kk3.5278.25u.com
kk3.58946.25u.com
klati.newsonet.net

klcg.ujheadph.com
kl-hqun.gmailboxes.com
kl-hqun.newsonet.net
kliee.newsonet.net
kl-mfa.newsonet.net
klnrdc.newsonet.net
klnrdc.purpledaily.com
kl-rfc.newsonet.net
kl-rio.newsonet.net
kluscc.newsonet.net
klwest.purpledaily.com
kmcmold.com
kmhs.lornet.com
kodapumpingunits.com
kratos.us.to
krkovic.com
ks.lamer.la
ksjdh.com
kuaib.cc
kusw.blackcake.net
kyaiyue.com
kyantai.net
kybj.net
kyominthai.com
kysns.com
ky-vc.com
kzzone.com
l-3.dsmtp.com
labsmate.com
ladwigracing.com
lakenormanhandyman.com
lakeville.usswim.net
lamonsprinting.com
landmarkeducationlagi-vn.com
landmarkexecutiveforum.com
landmarkgraduate.com
lanteckstudios.com
laramie.usswim.net
larrymcbride.com
laserdyne.com
lasvegasunwired.com
lasvegasunwired.org
lawyerview.cn
lazerporting.com
lbkymm.com
lc3.bostonheartlab.com
lcdtv65.com
learnforexmarkets.com
leets.hugesoft.org
leiboy.com
lenlayman.com
leos.auestrap.com
letgoonsale.com
lfmeinv.com
lfu86.cobolweeda.in
lgb-static-208.57.237.141.mpowercom.net
lhcjt.com
liaoyuan.saomen.com
libertyreservefunds.com
libertyreservehyip.org
licenses.xssoftware.com
lietuvinas.no-ip.org
limsurgery.com
lin.emilynaples.com
lingd.cn
link.applesoftupdate.com
linmae.com
lion.hw247.com
lishui.saomen.com
liskas.com
littlerockokay.com
liuhec.37.600dns.info
live.sunscrolling.com
livefuturesdaytrading.com
livemymsn.com
livingstonroads.org
ljczy.com
lknhandyman.com
ll.unndc.com
lllolI.net
llrenti.info
lms.ttinao.com
load.mooo.com
locumrelief.com
loeonw.com
login.aolon1ine.com
login.businessconsults.net
login.pcanywhere.net
logo.staycools.net
logon.dynssl.com
logs.sportreadok.net
losethatweightguaranteed.com
lotsoshup.com
love.msnhome.org
loveapp.me
lovemm78.com
lovetop.keren.la
lovingchristianl.com
lqlap03.jackmont.com
lqy.cc
lubo3d.com
lucy.businessconsults.net
lucy2.infosupports.com
ludaoidc.com

luxuryairrsvp.com
luxuryairrsvp.htoademos.com
lvunwired.com
lvunwired.net
lw.infobusinessus.org
lwave.arrowservice.net
m.it-leaked.com
mach5auto.com
magazine.yahoodaily.com
magnismunchies.com
mail.3jnj.com
mail.3jnjpharma.com
mail.7perhour.co.uk
mail.absotech.com
mail.acdragon.com
mail.adbarker.com
mail.affm.info
mail.ahidistribution.com
mail.aidincorporated.org
mail.a-i-m.ie
mail.aiscea.com
mail.arrowservice.net
mail.athomecontracting.com
mail.audiobible.com
mail.avowners.com
mail.balearics.com
mail.bareart.com
mail.barkingcrow.com
mail.belmapangratz.com
mail.bent-severin.com
mail.bestcasuals.com
mail.bevlyne.com
mail.bfl-llc.com
mail.biblebible.com
mail.biohealth.com.sg
mail.blaze-inc.com
mail.bluestarredimix.com
mail.boseathorsham.com
mail.bosshosshelp.com
mail.boyer-boyer.net
mail.boyerfamilypa.org
mail.brantleycustomhomes.com
mail.bretonhouse.ca
mail.broadtechsolutions.com
mail.btsnetworks.net
mail.buniqe.com
mail.businessconsults.net
mail.callawayfinancial.com
mail.canyonsunskincare.com
mail.carmela.com
mail.carticacapital.com
mail.carzrus1.com
mail.catalystgroupjax.com
mail.ccagency.com
mail.cdpa-architects.com
mail.cgsuslaw.com
mail.chileexe77.com
mail.choointhang.com
mail.clsinc.net
mail.colatitude.com
mail.computerpossibilities.com
mail.conour.com
mail.convexoptical.com
mail.creativecivilization.com
mail.crestwood.com
mail.csworship-pa.net
mail.customorderpolicespecialties.com
mail.dalipchand.com
mail.datatek-inc.com
mail.daten-loeschen.org
mail.diamondsti.com
mail.dickdyermercedes.com
mail.dillernursery.com
mail.dotsquares.net
mail.drzingaro.com
mail.dunnbenefit.com
mail.eadsmurraypugh.com
mail.echampions.org
mail.edifyconsultant.com
mail.elevation.com.tw
mail.emerge-systems.net
mail.emersonlimited.com
mail.emmarossosteopathypractice.com
mail.empowerednotary.com
mail.essexpropertylettings.co.uk
mail.fabonline.net
mail.fantasyhusband.com
mail.fastpack.net
mail.fbresearch.org
mail.fijishaadi.com
mail.fountaininjurylaw.com
mail.frankwilliams.com
mail.freesexdoor.com
mail.galiservice.com
mail.genbukan.ca
mail.ghsscsa.net
mail.glacctg.com
mail.gmtca.com
mail.goaskdavid.com
mail.goldmanlawoffices.com
mail.good-dogs.co.uk
mail.googlemart.com
mail.hektargroup.com
mail.hendrickseng.com

mail.hetsco.com
mail.hgburacker.com
mail.hideawaybingo.com
mail.homemaidsolutions.com
mail.hometown-insurance.net
mail.hudson.org
mail.hudsondc.org
mail.icu.com.sg
mail.idealauto.ca
mail.indykiwi.com
mail.instantlinksite.com
mail.insulation-tubing.com
mail.intelidataexpress.com
mail.internetdesignconcepts.com
mail.iorl.net
mail.it-leaked.com
mail.jackmont.com
mail.jennettespier.net
mail.josievenable.com
mail.kaiyangroup.com
mail.kedco.us
mail.lamonsprinting.com
mail.langeed.com
mail.lastwordedits.com
mail.latitudecg.com
mail.lksoftvc.net
mail.locumrelief.co.uk
mail.lornet.com
mail.lotsoshup.com
mail.m.it-leaked.com
mail.madsen-howell.com
mail.mariescatering.com
mail.mercies.com
mail.midwestcat.com
mail.mrduffy.com
mail.musicvisionsound.com
mail.nab.org.za
mail.nabr.org
mail.nbcir.net
mail.neocreative.net
mail.newwayedu.com
mail.nfms.net
mail.nodenine.net
mail.nodeninestudios.com
mail.northfieldcorp.com
mail.nuoglobal.com
mail.oneflewsouthatl.com
mail.orienradio.com
mail.oryanlawfirm.com
mail.oshkoshchristian.com
mail.osmb.bz
mail.othersellers.com
mail.oviedosafetylights.com
mail.pangratz.net
mail.pc-free-games.com
mail.pcpronet.com
mail.pcpronet.net
mail.pdllc.net
mail.penncorp.net
mail.pentagonsi.com
mail.persol.cn
mail.philliasrecords.com
mail.pixeintl.com
mail.planningpod.com
mail.planningpodevents.com
mail.planningpodpersonal.com
mail.pocketcaddie.co.za
mail.pocketrsvp.co.za
mail.powz.com
mail.praxi.gr
mail.profinancialservices.com
mail.prohoists.com
mail.projectfile.com.sg
mail.raj-enterprises.com
mail.rcsweb2.com
mail.rcswebmail.com
mail.rdconsultingllc.com
mail.reallysmile.com
mail.redseasports.co.il
mail.reloadinteractive.com
mail.rfrick.com
mail.rginy.com
mail.richmondcommercialsvcs.com
mail.ronish.ca
mail.ronishcomputers.com
mail.rsdu.org
mail.serenitysalonllc.com
mail.shawnaboyer.com
mail.sheridanpatterson.com
mail.sheridanpatterson.org
mail.shipsinaday.com
mail.silversurfersguide.com
mail.solution.com.sg
mail.somervilleinc.com
mail.sonfishgear.com
mail.sonshineriders.com
mail.sorenen.com
mail.soundnotes.com
mail.spiritofjefferson.com
mail.ssaukchildtracking.org
mail.starliteleasing.net
mail.statusholidays.com
mail.stevema.net
mail.storeinuk.com

mail.stricklandministries.com
mail.sunnytools.com
mail.swingsetsbydesign.com
mail.symbionet.com
mail.symbiosys.co.za
mail.syntecmedia.com
mail.takeone.net
mail.tawservices.net
mail.technilinkint.com
mail.thecrownsgolf.org
mail.thegraphicsbiz.com
mail.thepinkhousebrighton.co.uk
mail.tilpc.com
mail.timboyer.net
mail.tnslaw.com
mail.toldya.com
mail.trans-acc.com
mail.traveloutlaw.com
mail.treepeople.org
mail.tutorcare.co.uk
mail.udb.in
mail.ukfexmail5.co.uk
mail.uktraveldirectory.net
mail.unionjackspeedway.com
mail.uniquedreambuilders.com
mail.valerierichards.biz
mail.vbgmaild2.co.uk
mail.ventafish.com
mail.verbatimsystems.com
mail.vestarcapital.com
mail.vitalconnections.com.vn
mail.vlci.net
mail.vrhs1970.com
mail.wardins.com
mail.ward-moore.com
mail.wellandrealty.com
mail.wellmaxcpa.com
mail.wilshore.com
mail.wmins.com
mail.wowtally.com
mail.wwgc.com
mail.xcellenet.com
mail.yeastar.com
mail.yfchou.com
mail.yourfarmlife.com
mail01.bbsignal.com
mail01.theanderco.com
mail01.utilunlimited.com
mail1.rfrick.com
mail1.virtualorlando.com
mail2.drzingaro.com
mail2.nuoglobal.com
mail2.rfrick.com
mail2.ward-moore.com
mail3.ward-moore.com
mailbkp.majesticproductions.com
mailto.lornet.com
main.busketball.com
mainnab.com
maisonprojects.com
makingmypayment.info
man123.tk
mangomail.com
mantech.info.tm
manufacturerscup.info
map.auestrap.com
marcohering.com
marines.defenceonline.net
markered.info
martialartsembroidery.com
martyladwigracing.com
master.ronishcomputers.com
masterpiece.reload.com.sg
masterpiece-systems.com
mats-n-covers.com
matthewpoole.com
mattpolito.com
mauicomputermedics.com
mbl-82-57-109.dsl.net.pk
mc.bigish.net
mchs.countertrade.com
mcintoshmachineandfabrication.com
mcintoshswingarms.com
mdf-net.com
me.busketball.com
medef.pursuebusiness.com
media.paramountexport.net
medicalmanagement.com
medicus8.net
mediterraneonyc.com
medizineinc.com
meeting.toh.info
meilinhongkong.com
members.freesexdoor.com
members.tnns.net
meta.vpnhouse.net
method.ns06.net
metroiaq.com
metstorebkk.com
mh9527.com
mhakimigun.com
micemagazine.com
michaeluhrich.com
micro.applesoftupdate.com

microsoft.standards-updates.com
midamericasound.com
midgame.com
midlifecrisisband.org
midwest-autoparts.com
midwestcat.com
mightyimpiety.com
mikeromine.com
milengineer.com
milport.com
minamiguchi-bearings.com
miniddl.com
mir19.com
missionsystems.co.th
mitre.us.to
miyays.com
mjsz.net
mk.ber88.com
mkgisa.mk.co.kr
mkysmtp.mky.com
mlfbj.com
mm.xxuz.com
mmouu.com
moncler.bestseo.hk
moncleroutletonlines.net
mondopraha.com
moneyinvestment.biz
moon.24livehost.com
moonset.info
mooreshade.com
moparresto.com
mostequip.com
movie.canadatvsite.com
movies.infobusinessus.org
mowerstractors.savebigsale.com
moxnixsgt.com
mrduffy.com
msdn.bigish.net
msdsinc.com
msfiles.myftp.info
murdochracing.com
music.fitz.k12.mi.us
music.todayusa.org
mwdym.com
mx.linmae.com
mx.nuoglobal.com
mx11.ezinedirector.net
mx2.nuoglobal.com
mx3.shopthecage.com
mx85.l3tsfuck1ts3xy.su
mxbackup.alphagammadelta.org
mxbackup.rileytech.com
mxbackup.waynetaylorracing.com
mxbkup.alphagammadelta.org
mxbkup.freelanceindy.com
mxbkup.tbilawyer.com
mxbkup.tortslaw.com
mxbkup.uslaws.com
myautopartswholesale.com
myfile.steachs.com
myipy.com
myphoto.steachs.com
mysecretwebcam.com
naciyo.net
nacogdoches.k12.tx.us
naimap.ujheadph.com
name1.dunnbenefit.com
name2.dunnbenefit.com
nanping.saomen.com
nasa.newsonlinesite.com
nasa.usnewssite.com
nashins.com
nationalgroup.ca
nationaltransportation.ca
nb.saomen.com
nb5555.com
nbafenxi.com
nbd288.com
nbowood.com
nbqiangsheng.com
nclo83.faster1500foryou.in
ne.hugesoft.org
nefflandscape.com
neo.surgeservers.net
neo.ujheadph.com
neonatologija.rs
neptune.etonnant.com
nermal.civis.com
nestandards4.org
netbook.savebigsale.com
netclassroom.musowls.org
netdisk.serveuser.com
netmax.co.za
netro.mrduffy.com
nevershaveagain.co.in
new.mingxichina.com
news.advanbusiness.com
news.airwater.co.za
news.aoldaily.com
news.applesoftupdate.com
news.bdr.to
news.busketball.com
news.ccs.pl
news.cnndaily.com

news.cnnnewsdaily.com
news.decipherment.net
news.defenceonline.net
news.downloadsite.me
news.floydleeband.com
news.freshreaders.net
news.hoenjet.org
news.hqrls.com
news.lksoftvc.net
news.mil.nf
news.myftp.info
news.nytimesnews.net
news.rssadvanced.org
news.saltlakenews.org
news.serveuser.com
news.staycools.net
news.yahoodaily.com
newsonet.net
newspace.ujheadph.com
newstar.nytimesnews.net
newwayedu.com
new-xp.no-ip.biz
nexfilestore.info.tm
nexpartb2c.sophio.com
nextin.mobi
nflelitejerseys.org
nga.mil.nf
ngo.niau.org
nhcp.usswim.net
nikeairmaxpaschere.com
njdiningguide.net
njhndj.com
nlbconference.com
nmc.itdevworks.com
nnpkl.newsonet.net
nod.downloadsite.me
nodenine.net
nodeninestudios.com
nofailedstings.com
north-face-coats.net
northfacedownjacket.net
northface-fleecejackets.com
notaxfactory.com
notaxme.com
novamedic.ba
ns.408e16e3_cdc4b217_17282.dns.irl.cs.tamu.edu
ns.44609e97_cdc4b217_18521.dns.irl.cs.tamu.edu
ns.44670ac8_cdc4b217_15220.dns.irl.cs.tamu.edu
ns.44691d0d_cdc4b217_18521.dns.irl.cs.tamu.edu
ns.4adce43a_cdc4b217_18621.dns.irl.cs.tamu.edu
ns.62a3dd8d_cdc4b217_13814.dns.irl.cs.tamu.edu
ns.62add0cc_cdc4b217_15220.dns.irl.cs.tamu.edu
ns.affm.info
ns.biassm.org
ns.bretonhouse.ca
ns.etonnant.com
ns.floydleeband.com
ns.fullmoonlightnin.com
ns.gaktechnologies.com
ns.gardenriver.ca
ns.jasonschultz.ca
ns.lamonsprinting.com
ns.litchfieldil.com
ns.mostequip.com
ns.nationalgroup.ca
ns.nationaltransportation.ca
ns.oncecalledearth.com
ns.schoolsirvine.com
ns.searchmont.com
ns.seatrade.com.pk
ns.servicerental.ca
ns.servicerentals.ca
ns.sorenen.com
ns.ssmnoc.net
ns.syntecmedia.ca
ns.syntecmedia.com
ns.trading-post.ca
ns.ukfexmail5.co.uk
ns.vbgmaild2.co.uk
ns.wamusa.com
ns_44091017_cdc4b217_05889.dns.irl.cs.tamu.edu
ns_cdc4b217.irl-dns.info
ns-00081-11412.irl-dns.info
ns-00275-11412.irl-dns.info
ns-00390-11412.irl-dns.info
ns-00793-11412.irl-dns.info
ns-00836-11412.irl-dns.info
ns-00845-11412.irl-dns.info
ns-01333-11412.irl-dns.info
ns-01516-11412.irl-dns.info
ns-01878-11412.irl-dns.info
ns-02147-11412.irl-dns.info
ns-02521-11412.irl-dns.info
ns-02556-11412.irl-dns.info
ns-02621-11412.irl-dns.info
ns-02737-11412.irl-dns.info
ns-02913-11412.irl-dns.info
ns-02924-11412.irl-dns.info
ns-03084-03098.irl-dns.info
ns-03359-11412.irl-dns.info
ns-03849-03893.irl-dns.info
ns-03875-11412.irl-dns.info
ns-04128-11412.irl-dns.info
ns-04598-11412.irl-dns.info

ns-05374-11412.irl-dns.info
ns-05500-05586.irl-dns.info
ns-05541-11412.irl-dns.info
ns-05731-11412.irl-dns.info
ns-06723-11412.irl-dns.info
ns-06845-11412.irl-dns.info
ns-07746-11412.irl-dns.info
ns-08066-11412.irl-dns.info
ns-08123-11412.irl-dns.info
ns-08644-11412.irl-dns.info
ns-08773-11412.irl-dns.info
ns-09155-11412.irl-dns.info
ns-09307-11412.irl-dns.info
ns-09712-11412.irl-dns.info
ns1.7planets.com
ns1.bayway.net
ns1.bushnell.com
ns1.celetex.com
ns1.civis.com
ns1.cyberbury.net
ns1.daifukuamerica.com
ns1.daten-loeschen.org
ns1.dougpoland.com
ns1.dougpoland.net
ns1.dubai-groups.com
ns1.easy-investment.biz
ns1.egoldinvestment.org
ns1.egold-investments.biz
ns1.equinoxnetwork.com
ns1.forex-investments.biz
ns1.freesexdoor.com
ns1.ftswebdesign.com
ns1.fxtrades.info
ns1.heathermariedesigns.com
ns1.ideaexpert.co.th
ns1.it-leaked.com
ns1.itsystemworks.com
ns1.joeasy.info
ns1.jpmicro.net
ns1.lanteckstudios.com
ns1.libertyreservefunds.com
ns1.libertyreservehyip.org
ns1.microd.com
ns1.mie.co.th
ns1.moneyinvestment.biz
ns1.myctnews.com
ns1.onsalebestdeal.com
ns1.on-sale-stores.com
ns1.patternshop.biz
ns1.peachtreeed.com
ns1.polandconsulting.net
ns1.polands.org
ns1.power-public-relations.com
ns1.powerpublicrelations.org
ns1.pprmail.net
ns1.rfrick.com
ns1.schange.com
ns1.spiritofjefferson.com
ns1.ssmnoc.net
ns1.stockinvestment.biz
ns1.templatemedias.info
ns1.tnets.net
ns1.ukfexmail5.co.uk
ns1.vbgmaild2.co.uk
ns1.virtual-credit-cards.org
ns1.worldpost.com
ns1.worldpost.org
ns1.xcellenet.com
ns1.yewtec.net
ns-10252-11412.irl-dns.info
ns-11123-11412.irl-dns.info
ns-12506-11412.irl-dns.info
ns-13083-11412.irl-dns.info
ns-14371-11412.irl-dns.info
ns-15190-11412.irl-dns.info
ns-15780-11412.irl-dns.info
ns-15974-11412.irl-dns.info
ns-16094-11412.irl-dns.info
ns-16170-11412.irl-dns.info
ns-16453-11412.irl-dns.info
ns-16575-11412.irl-dns.info
ns-16757-11412.irl-dns.info
ns-16958-11412.irl-dns.info
ns-17125-11412.irl-dns.info
ns-17148-11412.irl-dns.info
ns-17429-11412.irl-dns.info
ns-18084-11412.irl-dns.info
ns-18086-11412.irl-dns.info
ns-18870-11412.irl-dns.info
ns2.absolutelyhosting.com
ns2.atchurch.org
ns2.broadtechsolutions.com
ns2.cdmsinc.net
ns2.civis.com
ns2.daten-loeschen.org
ns2.dmt-portal.com
ns2.etonnant.com
ns2.freepdfpaper.com
ns2.freesexdoor.com
ns2.fxtrades.info
ns2.gadgetshopgirl.com
ns2.hkwww.com
ns2.index.net.br
ns2.it-leaked.com

ns2.joeasy.info
ns2.lanteckstudios.com
ns2.lawopp.net
ns2.llloll.net
ns2.logisolve.com
ns2.luvnut.net
ns2.lxhost.net.br
ns2.ncaquariums.com
ns2.ncaquariums.net
ns2.ncaquariums.org
ns2.nogran.net
ns2.nuniv.net
ns2.paramountexport.net
ns2.power-public-relations.com
ns2.pprmail.net
ns2.rfrick.com
ns2.seatrade.com.pk
ns2.seven-labs.com
ns2.slifter.com
ns2.spiritofjefferson.com
ns2.srv32.com
ns2.ukfexmail5.co.uk
ns2.vbgmaild2.co.uk
ns2.yewtec.net
ns2.ytci.com
ns3.allinteractive.co.th
ns3.digitaloutrage.com
ns3.dnsthai.com
ns3.dzygroup.com
ns3.eguideconnect.com
ns3.it-graphic.com
ns3.luminos-media.com
ns3.netdesignthailand.com
ns3.porar.com
ns3.smokybyte.com
ns3.ssmnoc.net
ns3.threewise-monkeys.com
ns3.tnets.net
ns4.jpmicro.net
ns4.triangulum.co.za
ns7.24livehost.com
ns7.24livhost.com
ns8.enbss.com
nserv5.imprimistechnologies.com
nserv6.imprimistechnologies.com
ns-facebook-01750-16227.irl-dns.info
ns-facebook-02759-16227.irl-dns.info
ns-facebook-03131-16227.irl-dns.info
ns-facebook-03397-16227.irl-dns.info
ns-facebook-03585-16227.irl-dns.info
ns-facebook-03754-16227.irl-dns.info
ns-facebook-03797-16227.irl-dns.info
ns-facebook-03810-16227.irl-dns.info
ns-facebook-04342-16227.irl-dns.info
ns-facebook-04469-16227.irl-dns.info
ns-facebook-04548-16227.irl-dns.info
ns-facebook-04628-16227.irl-dns.info
ns-facebook-04858-16227.irl-dns.info
ns-facebook-05155-16227.irl-dns.info
ns-facebook-05490-16227.irl-dns.info
ns-facebook-05609-16227.irl-dns.info
ns-facebook-05831-16227.irl-dns.info
ns-facebook-06077-16227.irl-dns.info
ns-facebook-06514-16227.irl-dns.info
ns-facebook-06516-16227.irl-dns.info
ns-facebook-06922-06984.irl-dns.info
ns-facebook-06922-06984.m.irl-dns.info
ns-facebook-06929-06984.irl-dns.info
ns-facebook-06929-06984.m.irl-dns.info
ns-facebook-07658-16227.irl-dns.info
ns-facebook-08441-16227.irl-dns.info
ns-facebook-08547-16227.irl-dns.info
ns-facebook-08623-16227.irl-dns.info
ns-facebook-08780-16227.irl-dns.info
ns-facebook-09166-16227.irl-dns.info
ns-facebook-09207-16227.irl-dns.info
ns-facebook-09214-16227.irl-dns.info
ns-facebook-09683-16227.irl-dns.info
ns-facebook-09746-16227.irl-dns.info
ns-facebook-09903-16227.irl-dns.info
ns-facebook-10049-16227.irl-dns.info
ns-facebook-10819-16227.irl-dns.info
ns-facebook-10826-16227.irl-dns.info
ns-facebook-10866-16227.irl-dns.info
ns-facebook-11057-16227.irl-dns.info
ns-facebook-11275-16227.irl-dns.info
ns-facebook-11685-16227.irl-dns.info
ns-facebook-12933-16227.irl-dns.info
ns-facebook-13737-16227.irl-dns.info
ns-facebook-13843-16227.irl-dns.info
ns-facebook-14100-16227.irl-dns.info
ns-facebook-14480-16227.irl-dns.info
ns-facebook-15233-16227.irl-dns.info
nt2.exsbs.net
nt3.exsbs.net
ntzone.com
ntzt.info
nunoelectric.com
nvd.strangled.net
nwsc.usswim.net
nwunwired.net
oberon.co.za
oem-bmw-parts.com
oem-mercedes-benz-parts.com

oempartsgarage.com
oewarehouse.com
officiagroup.com
ofurn.com
oilamericagroup.com
old.hisd.us
old1.brocksperformance.com
oliver.arrowservice.net
omegalogos.org
omegawatch.replicagarden.com
once.downloadsite.me
oncecalledearth.com
oncourselearning.net
oneabs.com
onedaysweet.com
one-world-cargo.com
online.livemymsn.com
online.mcafeepaying.com
online.quickcert.com
on-reflection.org
onyxweb.streamguys.com
o-o.preferred.telkom-cpt1.v11.lscache3.c.youtube.com
o-o.preferred.telkom-cpt1.v11.lscache4.c.android.clients.google.com
o-o.preferred.telkom-cpt1.v2.lscache1.c.youtube.com
o-o.preferred.telkom-cpt1.v2.lscache4.c.youtube.com
o-o.preferred.telkom-cpt1.v20.lscache2.c.youtube.com
ooocar.com
ope.coastmaritime.org
opisolutions.com
opp.coastmaritime.org
or-69-69-94-3.sta.embarqhsd.net
orderhelper.com
orderparts.smythautomotive.com
oregonunwired.com
oscar.gotdns.com
otto.rs
outdao.com
outlook.somervilleinc.com
owa.itsystemworks.com
owa.softsolutionbox.net
pacific.worthhummer.net
paddi.ns06.net
paddi.vpnhouse.net
page-me.net
paladin-ent.com
pandawn.com
pantechinc.com
papper.booksonlineclub.com
parker.creativecivilization.com
parts.alsautomotive.com
pasco.ujheadph.com
pashe.rs
patternshop.biz
pay.freshreaders.net
paydayloanshut1b.com
pc-free-games.com
pcpronet.com
pdllc.net
pdxservers.com
peakwaves.usswim.net
peixun.saomen.com
penncorp.net
penndelswim.org
penndelswim.usswim.net
pentagonsi.com
perfectmulchproducts.com
performax.co.th
pfo.globalsecuriy.org
phb.arrowservice.net
philippi.pmcc4w.org
phoenix2.csceng.com
photoshop-eilat.com
pickmeup.tk
pick-nick-frituur.be
pietros.com
pirlsandiego.net
pistonson.us
planningpod.com
planningpodevents.com
plasamusic.com
play.reload.com.sg
pmcc4thwatch.com
pmcc4thwatch.eu
pmcc4thwatch.sg
pmcc4thwatchtruth.info
pmcc4w.org
pmcc4wme.org
podbeaver.com
poolheaterscсr.letgoonsale.com
pop.amk-services.com
pop.csceng.com
pop.richmondcommercialsvcs.com
pop3.amk-services.com
pop3.csceng.com
post.ghsscsa.net
powermax.kr
power-public-relations.com
pprmail.net
praxi.gr
prc.newsonet.net
prefix.usapappers.com
press.gift186.com

press.ipsecsl.net
preunicollege.com.au
preventionpoint.com
programming.savebigsale.com
progressivepreschool.org
projectfile.com.sg
prolabnj.com
prolect.com
propanegillsbest.letgoonsale.com
proracegear.com
proroofingsv.com
providegift.com
providers.thepathway.org
prsec.ssps.ntpc.edu.tw
ps3pojie.mannasoft.cn
psp.advanbusiness.com
psp.staycools.net
psu.nytimesnews.net
pt.pc-free-games.com
puruide.com
pushlawnttc.letgoonsale.com
q10765919.299.vpszuyong.com
q1811815333.69vps.vpszuyong.com
q807822998.299.vpszuyong.com
qa.astadia.com
qaportal.bostonheartlab.com
qdcbs8.com
qdhnj.com
qexide.com
qiche.saomen.com
qiqiang777.com
qq405488562.299.vpszuyong.com
qqchaxun.net
qqwu5.com
qqzuanz.com
qtk77.com
qualitymachinecompany.com
quantumgrphinc.com
quickfunds4u.in
qvodo.com
racecranks.com
racewayoftheamericas.com
radioafsana.com
radiokorissos.radio1234.com
radiotipaza.radio1234.com
radius.network-free.com
raj-enterprises.com
ranchofn.com
rankmyspace.net
rantnrave.com
raocala.com
ratedmarineelectronics.letgoonsale.com
ratedrecorders.letgoonsale.com
ratedwatches.letgoonsale.com
ravelandmarkeducation.com
ray-optics.com
rcsexch.richmondcommercialsvcs.com
rcsmusic.com
rcsmusic.net
rcswebmail.com
rd.bostonheartlab.com
rdyi.net
reallysmile.com
rebecca.dvrlists.com
reconsecurity.org
record.companyinfosite.com
recreation.gardenriver.ca
recyclingequipmentinc.com
red1engineering.com
redesign.tpt.com
redneckexpress.com
redseasports.co.il
refresh.goalslive.com
reinventateimage.com
rel.ipsecsl.net
reload.com.sg
reloadinteractive.com
remedylife.com
remedyonline.com
remi-ny.com
remote.americanrivers.org
remote.amrivers.org
remote.comrepair.net
remote.eadsmurraypugh.com
remote.handlingsystems.com
remote.lwpc.com
remote.parterss.com
remote.veryspecialplace.org
remote.welcomehomeloans.com
renderhope.com
report.crabdance.com
reports.jackmont.com
res.decipherment.net
res.federalres.org
reservations.uinn.biz
reviewgreenenergy.com
reviewopportunity.com
rfrick.com
rhythm937.com
rhythm947.com
ricbyrne.com
richardpullin.com
richmondcommercialsvcs.com
ridgeview19.org

riggeals.com
rightnowautoparts.com
rightnowautoparts.sophio.com
rileymotorsport.com
rileytech.com
riverroadwine.com
rnskh.info
robinsonindustriesinc.com
roc-designs.com
rockwellcollins.info.tm
rogerhedgecock.homefrontsandiego.org
ronishcomputers.com
ronwebbracing.com
root.saltlakenews.org
rose-team.co.uk
rose-woman.net
roujian2011.info
rowerdink.com
roxschoolofdancing.co.uk
roxychemical.com
royalsky.co.th
royaltyware.com
rrbrink.com
rrcs-24-123-91-70.central.biz.rr.com
rrcs-24-199-240-74.midsouth.biz.rr.com
rrcs-24-39-5-85.nys.biz.rr.com
rrcs-24-43-98-12.west.biz.rr.com
rrcs-70-62-232-98.central.biz.rr.com
rrvywahoos.usswim.net
rsdu.org
rwiamerica.com
ryanschnitz.com
s0000.com
s01.home.guaylo.com
s3ksolutions.com
saber.gfnet.com
sac.auestrap.com
sag.kr
sale.advanbusiness.com
sale.staycools.net
sales.sawtel.com
sametime01.solutions-ii.com
sandcco.com
sandpipers.net
savebigsale.com
sbcbs.com
sc.tzlts.net
sc3.shoutsrv.com
scaneagle.com
schnitzracing.com
schoolsirvine.com
science.bil-nasalab.com
sclc-rc.org
scp.interradiology.com
sctzzj.com
sd.2schina.net
sdtwy.com
se.sese.pm
se5656.com
search.searchforca.com
seasonsnyc.com
seatsushions.letgoonsale.com
seawebau.com
secure.aimscomputersystems.com
secure.angelsneuro.com
secure.dinkumware.com
secure.verticco.com
secure121.porar.com
secure1and1.sophio.com
secure2.drvfinancing.com
secure2.labwerks.com
securelogin.codexact.com
s-ehrlich.net
sek7.net
sell.dragbike.com
sells.usnewssite.com
semi.marineaugust.com
sensextoday.net
sentinelsacramento.com
seo.csceng.com
seotool.com
serenitysalonllc.com
server.applesoftupdate.com
server.glenbrookexcavating.com
server.proxydns.com
server.welcomehomeloans.com
server1.myjazznetwork.com
server10.midiamail.com.br
server3.adbus.com
server9.netpronto.com
service.applesoftupdate.com
service.issnbgkit.net
service.symanteconline.net
servicemaxcredit.com
servicemaxinc.com
servicerental.ca
servicerentals.ca
services.busketball.com
sex-store.com.au
sextoomuch.net
sexywomenclothes.com
sh.2schina.net
shaoxing.saomen.com
share.usnewssite.com

sharefx.com
shbjzx.info
shcup.com
shelton-farretta.com
shenghuo.saomen.com
sheridanrec.com
shiff.eilatinter.co.il
shmandarintools.com
shoes.e-cardsshop.com
shop.dragbike.com
shop.microd.com
shop.newsonlinesite.com
shopacdelco.com
shopinjectors.com
shopping.usnewssite.com
shopthecage.com
shorten.ws
showroomadvantage.com
showroomscan.com
shrineofdemocracychorus.org
shumeiyuan.com
shunleepalace.lanteck.net
shuozhou.saomen.com
siamchemplus.co.th
signworksgraphics.com
silverbirdcinemas.com
silverbirdgroup.com
silverbirdtv.com
silversurfersguide.com
sirenaristorante.com
sj0.w99.1860php.com
sjh.lornet.com
sjzhyjl.com
sjzjlc.com
sk2.gmailboxes.com
skill.purpledaily.com
sklcenter.newsonet.net
skracing.com
sky.applesoftupdate.com
sky.canoedaily.com
sky.theagenews.com
skyfly35.37.600dns.info
skypeuae.com
skyward.ridgeview19.org
slallc.com
slnoa.newsonet.net
smart-at.hkwww.com
smartphoneapp.savebigsale.com
smokybyte.com
smrt.com.sg
smtp.cmjit.com
smtp.csceng.com
smtp.nuoglobal.com
smtp.stupidrules.com
smtp1.baselewis.com
smtp2.mainnab.com
smtp2.nuoglobal.com
smtp3.adbus.com
smtp9.netpronto.com
snoringindiana.com
social.reload.com.sg
soft.advanbusiness.com
soft.nytimesnews.net
software.advanbusiness.com
software.nytimesnews.net
sohu.sdjyjy.com
soi.auestrap.com
solarpanels.savebigsale.com
solution.com.sg
soso4020.no-ip.org
soundnotes.com
source.livemymsn.com
southernohiosolar.com
space.auestrap.com
space.canadatvsite.com
spacenews.botanict.com
spec.ipsecsl.net
spiritofjefferson.com
sports.auestrap.com
sports.newsonlinesite.com
sports.nytimesnews.net
sports.rssadvanced.org
sports.staycools.net
sports.stream-media.net
sports.todayusa.org
sports.usnewssite.com
sportsandtravelonline.com
spot.auestrap.com
spot.decipherment.net
spotmart.com
squik.bigish.net
srs.businessconsults.net
ssa.saltlakenews.org
ssdd.no-ip.biz
ssileadman.com
ssl.aimscomputersystems.com
ssl.aimssecuresite.com
ssmnoc.net
sstpvpn228us.blacklogic.com
ssun.arrowservice.net
stacks.tridenttech.edu
staff.lflinkup.org
staff.onmypc.org
staging.tpt.com

starfarer.com
starkinterior.com
starliteleasing.net
stars.nytimesnews.net
starsandstripesmedia.com
starthrone.com
static-129-44-254-139.buff.east.verizon.net
static-72-248-239-146.ngn.onecommunications.net
statisnt.com
steeringgearsuperstore.com
stevericeracing.com
sthuzk.cn
stingraycity.org
stingrayimages.com
stjameselectricllc.com
stockinvestment.biz
stopyipping.com
storeinamerica.com
storeinuk.com
stotzracing.com
stratosglobal.info.tm
strollers.savebigsale.com
studio-monster.com
study.microsoftsupgrade.com
studycm.com
stulaw.bigish.net
stupidrules.com
sturelanum.in
stuwal.newsonet.net
subscriber.streamguys.com
suburbancarandtruck.com
succkl.ignorelist.com
sumernet.org
summit.biz.tm
sun.arrowservice.net
sunnytools.com
sup58.com
supermoney2010.com
support.advanbusiness.com
support.applesoftupdate.com
support.dns-dns.com
support.itsaol.com
support.paladin-ent.com
support.satellitebbs.com
support.searchforca.com
support.symanteconline.net
support.zyns.com
suzhounet.com
svn.sophio.com
swcpd.hkwww.com
sweetestfruit.com
swiga.com
swimindex.usswim.net
sword.bigish.net
swotm.googlesearchbot.com
sxmn.info
sxqzwh.com
sxshop.37.600dns.info
sy2100.com
syhhdfc.com
symantec.softmall.com.tw
symantecdl.softmall.com.tw
sync.ns06.net
syntecmedia.ca
syntecmedia.com
systechnologies.info.tm
szjgp.com
szpmh.com
szsmh.com
t.cz668.net
t.netjz.net
t.sctzzj.com
tablechairetc.com
tabletopgrills.letgoonsale.com
tabletopgrillstup.letgoonsale.com
takeachanceonrockandroll.org
taltraining2.ehosts.net
tana10.no-ip.biz
tangent.tangent.com
taobao.pp198.com
tape.purpledaily.com
tawimail.com
tb-huaxian.com
tbilawyer.com
tcfsspzyd.a.njslrc.com
tcscasebase.net
tdm.seotool.com
teach.usabbs.org
tech.firefoxupdata.com
tech.m3th.org
tech.saltlakenews.org
tech.usapappers.com
technilinkint.com
technosci.info.tm
techontime.ca
tel.usposters.net
telecomsys.dynet.com
teledyne.dynet.com
telescopesrated.savebigsale.com
televisions.savebigsale.com
temudjin.com
tenso.strangled.net
terminal1.aciint.com
test6666.w99.1860php.com

tetratech.zyns.com
thaieasyweb.com
thaifoam.com
thales.info.tm
thales.mooo.com
thales.uk.to
the-apparel.com
thebarsprogram.com
thecatalystcompany.com
thecrownsgolf.org
thelawmatrix.com
thepinkhousebrighton.co.uk
theraodifference.com
thgfmlt.com
thinkdesign.co.th
thomsclan.com
threefriends.info
ti5juws8skjgka49n4phksnsu6e4xl6opkxggl4jv3scn4k8.43.vuytd.com
tiandimei.com
tiaonline.americanunfinished.com
tidalwave.usswim.net
tieling.saomen.com
tielu110.com
tiger.hw247.com
timboyer.net
time.issnbgkit.net
times.nytimesnews.net
timhaileyworld.com
timvitaman.com
tj.2schina.net
tk2.trkhosting.com
tlwkdp.com
tm.sektori.org
tnets.net
tnniketnpascher.com
tnrequintnfr.com
tolovana.net
topcadet.com
topeagle-th.com
topmoney.purpledaily.com
topoo.cn
tortsurfer.com
totalrecall.entrustrm.com
tower.celetex.com
tplinkwuxianwang.mannasoft.cn
tpt.com
trade.daev.ca
tradeforexparttime.com
trading-post.ca
trainwiththepain.com
trans.vpnhouse.net
trans-personnelcorp.com
trends.signalfcc.com
trust.ns06.net
ts.dtstech.net
ts02.dtstech.net
ts2.safavieh.com
tsg-tech.com
tt22699.com
ttieurope.co.uk
tti-global.com
tti-india.com
ttinao.com
ttp.xssoftware.com
tutorcare.co.uk
tv.361fy.com
tv.wnwl.net
tw.emasweb.com
twistedsanta.com
twodaydietshop.com
twowheelextreme.com
tx-67-76-57-77.sta.embarqhsd.net
txrx.com
tzlts.net
u15208005.onlinehome-server.com
u15286567.onlinehome-server.com
uc277.com
udb.in
ug-asg.hugesoft.org
ug-nema.hugesoft.org
ug-opm.hugesoft.org
uiu.crabdance.com
ukfexmail5.co.uk
uktraveldirectory.net
un.linuxd.org
ungdungvui.com
unionjackspeedway.com
uniqtek.com
uniquedreambuilder.com
uniquegroup.net
uniqueindustrialsolutions.com
unitycambridge.org
unityinthecity.org
unitymass.com
unseenplanet.com
update.advanbusiness.com
update.dns05.com
update.dns-dns.com
update.freshreaders.net
update.ghsscsa.net
update.ikwb.com
update.jetos.com
update.livemymsn.com

update.longmusic.com
update.misecure.com
update.msnhome.org
update.reutersnewsonline.com
update.searchforca.com
update.staycools.net
update.symanteconline.net
update.symentec.org
update.theagenews.com
update.thehealthmood.net
update8.firefoxupdata.com
ups.businessconsults.net
url.googlevipmail.net
us.issnbgkit.net
us.madesky.com
us.t28.net
us16.vipin.us
us2.blacklogic.com
us8.vipin.us
usaid.countertrade.com
usaprc.us
usatax.us
usatotalsuccess.com
uscc.twilightparadox.com
use.gamezaz.com
users.mediaxsds.net
usns2.micros.com
usswim.net
usu.mooo.com
utfe86.sturelanum.in
uu88sc.com
uwnews.washington.edu
v.havevpn.com
v.oouka.com
v1.kangle.pw
v2.veryhave.com
v208-69-32-230.ash.opendns.com
v208-69-32-231.ash.opendns.com
v3.veryhave.com
v4.veryhave.com
va2.inethostco.com
valid.ns06.net
vanderlaanbrothers.com
vbgmaild2.co.uk
vcbeta.net
vehiclepartsexpress.com
venture.rostra.com
verbatimsystems.com
veryly.cn
verynicer.biz
vhd.overseasvotefoundation.org
victory915.ativomedia.net
victory915.visualradio.org
video-converter.biz
vijaymago.com
vino212.com
vip.001878.com
vip.sportreadok.net
virtual-credit-cards.org
visco.infosupports.com
visualradio.org
vlci.net
vmx.trans-personnelcorp.com
voa.canoedaily.com
vockl.bigish.net
voguesupra.com
volanscouture.com
vpn.crestwood.com
vpn.itsystemworks.com
vpn.jackmont.com
vpn.madesky.com
vpn.nebraska.gov
vpn.tawservices.net
vps.mmouu.com
vps.savebigsale.com
vqya86.duingusnin.info
vrhs1970.com
vsens.net
vst.alphagammadelta.org
vvfactory.com
vwsrf.com
vxbceiqgmfkluojq.6674.qq.bjxidebao.com
wabuv.com
waltronix.com
wandw.com
wangsaithong.com
wardins.com
ward-moore.com
wardperformance.com
wasa.arrowservice.net
watches.savebigsale.com
wcsa.usswim.net
weather.usnewssite.com
weather.yahoodaily.com
web.advanbusiness.com
web.birdrf.com
web.companyinfosite.com
web.livemymsn.com
web.thehealthmood.net
web.webservicesupdate.com
web11315246.w99.1860php.com
webblogs.dnsrd.com
webdirectbrands.net
weberconcrete.com

webinsyte.com
webmail.blackcake.net
webmail.btsnetworks.net
webmail.esgsats.com
webmail.nationalboiler.com
webmail.sunnytools.com
webmail.sunriseofficesystems.com
webmail.tnslaw.com
websensce.com
webserver.coe-dmha.org
wefada.com
weidlerlodge.com
weightsolution.com
welcomehomeloans.com
weliveinthefridge.com
wellnesscentre.ky
wesinco.com
wesinstallation.com
west.steeringgearsuperstore.com
westbrookcapital.com
westkl.worthhummer.net
westmall.com.sg
wewillplay.oncecalledearth.com
wgw.businessconsults.net
what.arrowservice.net
whatislandmarkeducation.cn
whatislandmarkforum.co.il
whatsthedealaboutlandmark.com
wheelies.ca
whir.li
wholesalecarkeys.net
wide4.worldwidemailing.org
width.vpnhouse.net
wifiserver.coppernet.net
wildlifememoriesgallery.com
willisdragracing.com
windycitymetals.com
wjoo83.quickfunds4u.in
wlanb2b1.no-ip.org
wm.bostonheartlab.com
wmins.com
wmp.businessconsults.net
wnam.businessconsults.net
wnew.businessconsults.net
wolfone.cn
woodhavenrange.com
worldbestpriceautoparts.com
worldwidebearings.com
wow.sg
wpad.csceng.com
wpad.jackmont.com
wpot.arrowservice.net
wpot.businessconsults.net
wstat.ns06.net
wstat.vpnhouse.net
wudingya.com
wundercarparts.com
wunfccc.businessconsults.net
wvw.mmouu.com
wwvv.comrepair.net
www.00234.com
www.029zh.info
www.03877.com
www.0410dj.com
www.0475woool.com
www.0543xxw.com
www.06kv.com
www.0755ktxs.com
www.0755mdkt.com
www.0797top.com
www.0dwx.com
www.1000net.org
www.1069sc.com
www.110ld.cn
www.123050.com
www.12341090.cn
www.1234abcd.com
www.123lk.cn
www.132l.com
www.133335.com
www.138bt.com
www.14ts.com
www.14vd.com
www.15dushi.com
www.169444.com
www.177456.com
www.179444.com
www.17jieyan.info
www.17sexs.info
www.188799.com
www.193338.com
www.19466.com
www.1perfectday.com
www.1xtx.com
www.2000365.com
www.2001365.com
www.2011y2011.tk
www.20356.com
www.22222pk.com
www.228royal.com
www.235158.com
www.246899.com
www.266488.com
www.2schina.net

www.311345.com
www.330678.com
www.331888.com
www.34563456.com
www.345mmm.com
www.355179.com
www.36ladys.info
www.382848.com
www.39593.com
www.3d8288.co.cc
www.3jnjpharma.com
www.400812.com
www.43mr.net
www.444456.com
www.445456.com
www.446456.com
www.44hb.com
www.456mmm.com
www.463456.com
www.477877.com
www.488889.com
www.4j28.com
www.4thwatchersportal.com
www.50919.com
www.517bocaitong.com
www.518928.com
www.51ips.info
www.51jiaozhuliao.com
www.51natco.com
www.51ttam.com
www.521ufo.com
www.52diany.com
www.52weishe.com
www.5551666.com
www.558333.com
www.558558.com
www.565t.com
www.577456.com
www.577678.com
www.581888.com
www.582888.com
www.5869.com
www.598928.com
www.5iau.com
www.5pur.com
www.604444.com
www.60584.com
www.66567.com
www.66889788.co.cc
www.669456.com
www.669777.com
www.67896789.com
www.678mmm.com
www.688678.com
www.69tu.com
www.70ph.com
www.725999.com
www.776456.com
www.776567.com
www.777796.com
www.77links.info
www.77rh.com
www.789mmm.com
www.79907.com
www.7k2.com
www.7kdp.com
www.7perhour.co.uk
www.803.cc
www.855133.com
www.86-0576.com
www.860708.com
www.866777.com
www.868gg.com
www.875678.com
www.880015.com
www.88846666.com
www.88886sf.com
www.8989f.net
www.91epay.com
www.91ppkk.com
www.92kmv.com
www.92yxj.com
www.94sqz.com
www.97sqz.com
www.990799.com
www.99407.com
www.995345.com
www.998996.tk
www.99s.com
www.99sqz.com
www.abcbrandbags.com
www.absempower.com
www.acousticaldesign.com
www.acra-pac.com
www.adamsrestequip.com
www.adamtrade.com
www.adcoservices.com
www.addweb.com
www.adendejager.com
www.advantageempower.com
www.affordwatch.com
www.agenceisrael.com
www.agrosolutions.net
www.aholidayadventure.com

www.aidincorporated.org
www.aig3.com
www.aigocc.com
www.aikongtiao.cn
www.aims.ws
www.aimscomputersystems.com
www.aimssecuresite.com
www.airmaxbrand.com
www.alahousurvey.org
www.allgarment.net
www.altrusaofcharlotte.org
www.americanenergyproduction.com
www.amusementparksigns.com
www.andushop.com
www.anhesiwang.com
www.anniemooresnyc.com
www.anxinxd.com
www.anything.com.sg
www.apaitonline.org
www.aquatomics.com
www.aquatomics.org
www.arany.info
www.arinternationaltrade.com
www.arozeny.com
www.artas.org.sg
www.arthurpriceseptic.com
www.ashfordmotel.com
www.ashishpandey.com
www.astd2012.co.za
www.aswrewards.com
www.ativomedia.org
www.au23.com
www.auestrap.com
www.autobarncatalog.com
www.autopartsforever.com
www.autopartsmidwest.com
www.autopartswarehousedirect.com
www.auto-trak.net
www.badaj.info
www.bagazm.com
www.bagvw.com
www.baillieroofing.com
www.bancocajasocial.com-r.in
www.bandcprintwear.com
www.bannlosangeles.com
www.baselewis.com
www.baxleywells.com
www.bayk.info
www.bbs-xiaomi.com
www.bcbgdressesoutlet.net
www.bch.com.sg
www.bdbyd.cn
www.bdjiafeng.com
www.bebeposhe.com.sg
www.beechenghiang.com.sg
www.benbensons.com
www.ber88.com
www.bestforextradingroom.com
www.bestlife100.com
www.bestoakleysunglasses.net
www.bevlyne.com
www.bfl-llc.com
www.biohealth.com.sg
www.birdrf.com
www.bird-technologies.com
www.bjchyx.com
www.bjsybd.com
www.bjtxgc.com
www.blancobydesign.com
www.blockheadautoparts.com
www.bobbycaldwell.com
www.bonweshop.cn
www.borasparts.com
www.boseathorsham.com
www.bpwpa.com
www.brankopavlovic.rs
www.brost.jp
www.budreck.com
www.buniqe.com
www.businessview.net
www.buycheapwholesalejerseys.com
www.buytkt.com
www.bweidkw.com
www.caffegrazie.com
www.caidumj.com
www.caifutx.com
www.camdensc.org
www.cameronians.com
www.campdiscovery.net
www.camquest.co.uk
www.canyonsunskincare.com
www.carfaxdental.com
www.carfaxdentalmedical.com
www.cargosvc.com
www.carolinahomeadditions.com
www.carpartsplace.com
www.cars-repair.com
www.cash-nows.com
www.ccghm.com
www.ccytkj.com
www.cdwangchuan.com
www.cfyci.com
www.chahao8.net
www.chaplinpr.com

www.chascomachine.com
www.cheapfivefingersale.com
www.chem-ju-nju-edu.com
www.chengxueedu.com
www.chinachenglei.com
www.chinapv114.com
www.chtchronicles.net
www.cincicreative.com
www.cityhallnewyork.com
www.clsupreme.com
www.cn365days.com
www.cncevolution.com
www.cncsys.co.jp
www.cnhangyu.com
www.cniom.com
www.cnsusc.com
www.cntc8848.net
www.coachhandbagswell.com
www.coapt.com
www.combat-help.com
www.commoditymanagementblog.com
www.conference.com.sg
www.connomac.com
www.converseallstarfr.com
www.coolcat-designs.com
www.coretrades.com
www.coseclinic.com
www.cqflqjf.com
www.cqgeton.com
www.cqty99.com
www.crcengrg.com
www.creativecivilization.com
www.csceng.com
www.cuiqingfen.in
www.custombikephotos.com
www.cxheatsink.com
www.cxsite.com
www.cxzssz.com
www.cysrb.com
www.cz668.net
www.daciro.com
www.dahuabiaoqing.cn
www.dalipchand.com
www.dangernet.com
www.danxia-china.com
www.datatek-inc.com
www.daumbertonyc.com
www.davisdisposal.com
www.d-cham.com
www.deandetrailers.com
www.delmarvaswim.org
www.dentino.com
www.deqn.net
www.designerwalletmall.com
www.devvillas.com
www.diabetesfocusonline.com
www.dickdyeronline.com
www.digitalagent.org
www.digitalagent.us
www.dillernursery.com
www.dingsonggui.com
www.djbca.com
www.dlghotel.com
www.dmcmy.com
www.dmt-portal.com
www.dohwanyc.com
www.doocoor.com
www.dragbike.com
www.drivecontrols.com
www.drjs.com
www.drstevecohen.com
www.dtccatalyst.com
www.duboselaw.com
www.duingusnin.info
www.duk.asia
www.dunnbenefit.com
www.duokee.com
www.dx-56.com
www.dyfjt.com
www.dzcpm.com
www.dzgrcw.com
www.eadparts.com
www.eaglemagnetic.com
www.eastcoastautoparts.net
www.ebrainnetwork.net
www.ecsunglasses.com
www.ei2u.com
www.eilatartists.com
www.eilatinter.co.il
www.elkindgroup.com
www.emascenter.com
www.emasweb.com
www.embasjtu.com
www.emersonlimited.com
www.emmarossosteopathypractice.com
www.empowerone.com
www.engineer.lflinkup.org
www.englishinbrightonwithus.com
www.entheos.com.sg
www.entrustrm.com
www.equipic.com
www.eretz-israel.com
www.erniesgallery.com
www.ettusais.com.sg

www.ettusais.sg
www.everright.cn
www.executivecmr.co.uk
www.faan.cn
www.fabienne-opal.com
www.fangtrade.com
www.fanthuatshop.com
www.fartech.com.sg
www.feigou.cc
www.fengqiuxian.com
www.fiji411.com
www.fijishaadi.com
www.file.3-a.net
www.firebirdgifts.com
www.firebirdrestaurant.com
www.firenapolitano.com
www.fjiao.net
www.flash4ui.com
www.flfh.cn
www.fmslaw.net
www.forexroomreviews.com
www.forum.redseasports.co.il
www.fourforchrist.org
www.fra-air.com
www.fraserscentrepoint.com
www.freelanceindy.com
www.freesexdoor.com
www.freeworkerscompreview.com
www.friendsdd.com
www.fwq.rd-c.cn
www.fx1314.cn
www.fzl22.cn
www.gabrielsbarandrest.com
www.gallerywestnowhere.com
www.game-menu.com
www.ganyuyin.com
www.gay315.com
www.gay61.com
www.gay61.net
www.gayongpasak.org
www.gelixs.com
www.geruier.net
www.ggder.com
www.ggrenti.com
www.gigapixels.com
www.gladiatorsod.com
www.glassesdesignerframes.com
www.glfp.info
www.glzyswim.org
www.gmdsystems.net
www.gmpartsnow.com
www.goaskdavid.com
www.goe6.com
www.goknives.com
www.golfnaperville.com
www.goodyearduraplus.com
www.google.co.ls
www.gottabeamazing.com
www.grace-gift.net
www.graceislandresort.com
www.greatesoft.net
www.gstz.cc
www.gtaautoparts.ca
www.gtnr.info
www.guccipascherefr.com
www.gzcityhotels.com
www.hagermanparts.com
www.haipiy.com
www.handangang.com
www.handicraftvilla.com
www.hantailang.com
www.happyreplicawatches.com
www.haveatw.com
www.hbbaisheng.com
www.hbkaoyan.cn
www.hbwdyt.com
www.hcgdgs.com
www.hdg.cc
www.hdhfc.com
www.hdzdjj.com
www.heatingmaintenancespares.co.uk
www.hebsl.com.cn
www.hektargroup.com
www.hektargroup.com.my
www.hendrickseng.com
www.heracles-sk.com
www.heracles-sk.net
www.hermessupplies.com.sg
www.hezuo18.com
www.hg699.com
www.hg93.com
www.hideawaybingo.com
www.hifo.net
www.highgrow.com.sg
www.hipsurfacing.co.uk
www.hlt71.com
www.hnhks.com
www.hoangpeople.com
www.holidayadventureslsa.com
www.holidayways.com
www.hollandseclub.org.sg
www.homefrontsandiego.com
www.homefrontsandiego.org
www.hometown-insurance.net

www.hotshotzz.com
www.hotspotautoparts.com
www.htoa.com
www.htoaarda.com
www.htoademos.com
www.htoamemberinfo.com
www.huntpropertynow.com
www.huochepiao.org.cn
www.hw247.com
www.hzflzs.com
www.i8sj.com
www.icoppinyc.com
www.icu.com.sg
www.idealauto.ca
www.idudu.net
www.ieee.mynumber.org
www.iglesiaebenezer.radio1234.com
www.ihmgjt.org
www.ii5088.com
www.ii8508.com
www.ii99.info
www.im33.gulfup.com
www.informedvoter.info
www.injectorwarehouse.com
www.innovativos.com
www.insitugroup.com
www.insitugroup.net
www.instantlinksite.com
www.internationalmolding.com
www.inthezonestuff.com
www.isralya.com
www.it-leaked.com
www.itnegypt.com
www.itrmall.com
www.jackmont.com
www.jackypow.com
www.jcdf777.com
www.jdl168.com
www.jerseysdiscountstore.com
www.jiajia1234.com
www.jianyu.com.sg
www.jiaoyuxia.com
www.jinanyanchu.com
www.jinglvjie.com
www.jinlida1234.com
www.jiuidc.cn
www.jiuzhabi.com.cn
www.jjj.com
www.jkcommercial.com.sg
www.jlzcwl.com
www.jn9988.cn
www.jnepay.com
www.jnsanmutang.com
www.johnspizzerianyc.com
www.joinnet.cn
www.joyyard.cn
www.js3888.com
www.jsgp168.com
www.jtjd.net
www.julitg.com
www.junglejewelsreptiles.com
www.junjingli.cn
www.junzhifu.com
www.jxsky.net
www.jxwh.net
www.kaitlinshiver.com
www.kaiyuanzhenzi.com
www.kayauto.net
www.kayngeetanarchitects.com
www.kbeconsultancy.com
www.kdzhijia.com
www.kearnyalumni.org
www.keruite.net
www.kfd348.dp.gl
www.kfd350.dp.gl
www.kflxz.com
www.kfoassoc.com
www.kgartsindia.com
www.kingboll.com
www.kmcmold.com
www.kodapumpingunits.com
www.kuaib.cc
www.kundixin.com
www.kynjj.com
www.kyominthai.com
www.kysns.com
www.ky-vc.com
www.l70.cn
www.labcaseworks.com
www.ladwigracing.com
www.lakenormanhandyman.com
www.lanseyinxiang.com
www.lanteckstudios.com
www.leiboy.com
www.leixiaoys.com
www.lfmeinv.com
www.lianyoupige.com
www.lifespace.com.sg
www.lillamanagementconsulting.com
www.lingd.cn
www.lingshengwang.com
www.litchfieldil.com
www.littlerockokay.com
www.livingstonroads.org

www.lknhandyman.com
www.llrenti.info
www.love5566.com
www.lqy.cc
www.lrm8.com
www.lubo3d.com
www.ludaoidc.com
www.luxuryairrsvp.com
www.lvbaomu.com
www.lxtrq.com
www.mabeizhan.cn
www.mach5auto.com
www.maheshwarimunch.com
www.mainnab.com
www.maiqiangxie.info
www.maiqiqiang.info
www.maisonprojects.com
www.marktrestaurant.com
www.martyladwigracing.com
www.mats-n-covers.com
www.mediterraneonyc.com
www.medizineinc.com
www.meizhenxiang.com
www.mh9527.com
www.michaeluhrich.com
www.microd.com
www.midamericasound.com
www.midgame.com
www.midinfo.net
www.midwest-autoparts.com
www.midwestcat.com
www.mightyimpiety.com
www.military.sg
www.milport.com
www.mishi8.com
www.miyays.com
www.mlfbj.com
www.mljj100.com
www.mmouu.com
www.monclerjacketsonlines.com
www.moncleroutletonlines.net
www.mooreshade.com
www.moparresto.com
www.mppl.us
www.mringshop.com
www.mrks.cn
www.musclecarsetc.com
www.muwaifan.cn
www.myautopartswholesale.com
www.nab.org.za
www.nacogdoches.k12.tx.us
www.naturestops.com
www.natureveg.com
www.nbowood.com
www.neicolec.com
www.nestandards2.org
www.nestandards4.org
www.nevershaveagain.co.in
www.nfljerseycustom.com
www.nikeairmaxpaschere.com
www.njdiningguide.net
www.nlbconference.com
www.nodenine.net
www.nodeninestudios.com
www.nongminfa.com
www.north-face-clearance.net
www.northfaceclearances.com
www.northfacefleecejacket.org
www.notaxfactory.com
www.ntzone.com
www.ntzt.info
www.oem-bmw-parts.com
www.oem-mercedes-benz-parts.com
www.oempartsgarage.com
www.oewarehouse.com
www.ofurn.com
www.oilamericagroup.com
www.ok6988.com
www.ok8.in
www.olunbao.com
www.omegalogos.org
www.oneabs.com
www.onedaysweet.com
www.oneflewsouthatl.com
www.onewoo.net
www.opisolutions.com
www.orderhelper.com
www.outdao.com
www.outletmonclerjassen.com
www.paint-coatings.com
www.paladin-ent.com
www.pandawn.com
www.pantechinc.com
www.paramountexport.net
www.pastdust.com
www.pcpronet.com
www.pcpronet.net
www.pcserve.cn
www.pdllc.net
www.penncorp.net
www.penndelswim.org
www.photoshop-eilat.com
www.pianyikongjian.com
www.pickmeup.tk

www.pietros.com
www.pkf.com.sg
www.play.reload.com.sg
www.pmcc4thwatch.com
www.pmcc4thwatch.eu
www.pmcc4thwatch.info
www.pmcc4thwatch.sg
www.pmcc4w.org
www.pocketcaddie.co.za
www.pocketrsvp.co.za
www.policedog.cn
www.potian002.com
www.pp198.com
www.pratts.biz
www.praxi.gr
www.preunicollege.com.au
www.progressivepreschool.org
www.projectfile.com.sg
www.prolect.com
www.psushi.com
www.pulsarcomponents.com
www.purpledaily.com
www.puruide.com
www.pwdqiy.com
www.pygrg.com
www.qdhnj.com
www.qeeke.com
www.qianyuan9303.com
www.qinyange.net
www.qiqi95.com
www.qiu006.com
www.qmwjjx.com
www.qq-123.com
www.qqcccc.com
www.qquue.net
www.qqwu5.com
www.qt339.com
www.quantumgrphinc.com
www.quickfunds4u.in
www.qvodo.com
www.qvodweb.org
www.qw85.com
www.qwoool.net
www.ra8488.com
www.rackpinionwhse.com
www.radio1234.com
www.radioafsana.com
www.ragnbone.com.sg
www.raj-enterprises.com
www.ramyzx.com
www.ray-optics.com
www.reallysmile.com
www.recyclingequipmentinc.com
www.redseasports.co.il
www.redstripe.rs
www.reliancetelecom.com.au
www.reload.com.sg
www.reloaddev.sg
www.reloadinteractive.com
www.remartautoparts.com
www.remedymagazine.com
www.remedyonline.com
www.remi-ny.com
www.reshamm.com
www.retrbol.com
www.richmondcommercialsvcs.com
www.ridgeview19.org
www.rightnowautoparts.com
www.rileytech.com
www.riverroadwine.com
www.roc-designs.com
www.ronishcomputers.com
www.ronnierainbow.com
www.rose-woman.net
www.rowerdink.com
www.roxschoolofdancing.co.uk
www.roxychemical.com
www.rrbrink.com
www.rwiamerica.com
www.sabdoo.rs
www.sag.kr
www.sager.com.sg
www.s-air.net
www.sandcco.com
www.saomen.com
www.sastbearings.com
www.sbcbs.com
www.scaneagle.com
www.sctzzj.com
www.sdjyjy.com
www.sdzrw.cn
www.seasonsnyc.com
www.s-ehrlich.net
www.sek7.net
www.sensextoday.net
www.sentinelsacramento.com
www.servicemaxinc.com
www.servicetraq.com
www.sfgm9.com
www.sharefx.com
www.shawnaboyer.com
www.shcup.com
www.shequstore.com
www.shopacdelco.com

www.shopinjectors.com
www.shopsteeringracks.com
www.shopthecage.com
www.shoujixwodi.com
www.showroomadvantage.com
www.showroomscan.com
www.shuiyisheng123.com
www.shumeiyuan.com
www.shxedk.com
www.signworksgraphics.com
www.silversurfersguide.com
www.simplefood.com.sg
www.sjzhyjl.com
www.smrt.com.sg
www.snoringindiana.com
www.softechglobal.com
www.softmar.com
www.sokkia.com.sg
www.someyx.com
www.sotogoo.com
www.soundnotes.com
www.soundrecall.com
www.specialtyinstallations.com
www.sportsandtravelonline.com
www.spotmart.com
www.ssaukchildtracking.org
www.ssbbx.cn
www.starfarer.com
www.starkinterior.com
www.starthrone.com
www.statisnt.com
www.steeringgearsuperstore.com
www.stjameselectricllc.com
www.stoin.org
www.stonecenterplus.com
www.storeinuk.com
www.studio-monster.com
www.sturelanum.in
www.suburbancarandtruck.com
www.suncoaste.com
www.sun-dynamic.com
www.supermoney2010.com
www.suzhounet.com
www.sweetestfruit.com
www.swimdog.net
www.sxqzwh.com
www.syhhdfc.com
www.symbiosys.co.za
www.szjgp.com
www.szmeidikongtiao.com
www.szpmh.com
www.szpuchun.com
www.szruilide.com
www.szsincere.com
www.szsmh.com
www.sztx.org.cn
www.taoyungao.com
www.tawimail.com
www.tawservices.net
www.tb-huaxian.com
www.tbntimes.com
www.tcscasebase.net
www.technilinkint.com
www.techontime.net
www.tese2000.com
www.the-apparel.com
www.thebrassrailnj.com
www.thecatalystcompany.com
www.thecrownsgolf.org
www.thelawmatrix.com
www.thelingzhi.com
www.thenorthfaceoutlet-shop.com
www.thepinkhousebrighton.co.uk
www.theseoulautogallery.com
www.thinkstudio.cc
www.tiankongruanjian.cn
www.tiffanylovers.com
www.timboyer.us
www.timezone.com.sg
www.tleyy.com
www.tnniketnpascher.com
www.tnrequintnfr.com
www.topoo.cn
www.top-replicaluxury.com
www.topsalesagent.com
www.toqun.com
www.toushipai.info
www.toushipukew.info
www.tpt.com
www.trackaadg.com
www.travelersmotorlodge.com
www.truecar.net
www.tsg-tech.com
www.tskwk.com
www.tt2sffb.com
www.tti-global.com
www.ttinao.com
www.tuiuvy.com
www.twowheelextreme.com
www.txrx.com
www.tzlcw.cc
www.u15286567.onlinehome-server.com
www.uadsale.com
www.uc611.com

www.udb.in
www.uktraveldirectory.net
www.uniquedreambuilders.com
www.uslaws.com
www.usswim.net
www.uuu9.org
www.va.com.sg
www.valerierichards.biz
www.vanderlaanbrothers.com
www.vcd8899.org
www.vehiclepartsexpress.com
www.verbatimsystems.com
www.veryera.com
www.veryly.cn
www.viceversarestaurant.com
www.vico.com.sg
www.video-converter.biz
www.vino212.com
www.vitalconnections.com.vn
www.vlci.net
www.volanscouture.com
www.voteyourmoney.org
www.vrhs1970.com
www.vsens.net
www.wabuv.com
www.wandw.com
www.wardins.com
www.ward-moore.com
www.warnerwong.com
www.warplink.net
www.watergator.net
www.web5173.com
www.weberconcrete.com
www.webnegotiator.com
www.wedarina.com
www.wefada.com
www.weightsolution.com
www.welcomehomeloans.com
www.wepushgrass.com
www.wepushgrass.net
www.wesinco.com
www.westbrookcapital.com
www.westmall.com.sg
www.whoneedscash.net
www.windowcleanser.com
www.windycitymetals.com
www.wituo.com
www.wmins.com
www.wolfone.cn
www.woodhavenrange.com
www.worldbestpriceautoparts.com
www.worldwideweeks.com
www.wow.sg
www.wowarchitects.com
www.wudingya.com
www.wundercarparts.com
www.wzson.com
www.wzzhuye.com
www.xbmy88.com
www.xchnba.com
www.xghdtz.com
www.xglmr.com
www.xingaijiqiao.org
www.xingtaishuaikang.com
www.xlsgc.com
www.xmjasun.com
www.xn--p3clgfhca0f0a6b.com
www.xproasia.com
www.xuping.net
www.xx55555.com
www.xxmi.net
www.xyg001.com
www.xylb.cn
www.xylshgj.com
www.y200.cn
www.yacht4sale.co.il
www.yangtai-jal.com
www.ycglfj.com
www.yeastar.com
www.ygdy.net
www.yinmanshop.com
www.yinyueyule.com
www.yixinjz.com
www.yiyanys.com
www.ylbanqian.com
www.ylhuagong.com
www.ymcacompetitiveswim.org
www.ymcaswimminganddiving.org
www.yolandabag.com
www.yongzhijixie.com
www.youxiazai.com
www.ys44.com
www.yswimmingnewyork.org
www.yuanfenwu.com
www.yusuanyuan.net
www.yxman.com
www.yy77.com
www.yzjs.org
www.z3721.com
www.zazanyc.com
www.zbbaoqian.com
www.zdcm.net
www.zdkji.com
www.zg114.org

www.zgyycs.net
www.zgzj2008.com
www.zhxgb.com
www.zh-xxb.com
www.zjmumen.com
www.zk170.com
www.zl889.com
www.zq314.com
www.zqcot.com
www.zs.cccgn.com
www.zzgyfamen.com
www1.booksonlineclub.com
www1.infosupports.com
www2.bigc.co.th
www2.dentino.net
www2.zwsj2008.com
www3.puruide.com
www6.qkyszlxt.com
www-ctr.businessconsults.net
wwww.sese.pm
wwwxz.com
wyzm.net
x4034ff14.ip.e-nt.net
xbart.net
xchgj.com
xdscity.w99.1860php.com
xenapp2.nationalboiler.com
xiazaibo.com
xingaijiqiao.org
xingfuxiaozhen.com
xk31.com
xman.businessconsults.net
xmfish2.xmhost2.ludaoidc.com
xn--12c1enj5azhpc.dmc.tv
xn--12c4b5a2g9a5b.dmc.tv
xn--12c4c0a4c0a8i.dmc.tv
xn--12c7bmwlbb3c9db3d.dmc.tv
xn--12cb3eb1hqf1b.dmc.tv
xn--12cf6db9be0i.dmc.tv
xn--12cg6dxbh2a.dmc.tv
xn--12cgi8dk3avmg1fxd4cuf.dmc.tv
xn--12cl0dxd3av.dmc.tv
xn--12coo3cf8cuf3az.dmc.tv
xn--22c6b7a3a0b1b5d.dmc.tv
xn--22cdl0eedf8dd1bzgsa3cb36a.dmc.tv
xn--22cj5gra7b.dmc.tv
xn--42c1b3ajb1bd8d7b.dmc.tv
xn--42c1dbg8af3cbc.dmc.tv
xn--42c4bbtwbcca3c2c4a9a0b9b.dmc.tv
xn--42ca5dxbaa0ax42a.dmc.tv
xn--42cf7cvb2bn1b.dmc.tv
xn--42cm5bc6bkabab3c2h7a.dmc.tv
xn--42cm7b8aia4c6cd2a.dmc.tv
xn--72c1a4b0c.dmc.tv
xn--72c2b1azag6clw2p.dmc.tv
xn--72c3b3a4cb3n.dmc.tv
xn--72c7cc5bn.dmc.tv
xn--72c9a3a4bn.dmc.tv
xn--72ca1etdh.dmc.tv
xn--72cf4ec0c3c1d2a1c.dmc.tv
xn--72cf6ebe4gra0g.dmc.tv
xn--82c4aff9bye6aw.dmc.tv
xn--82cap9bycyc9abv1j2f.dmc.tv
xn--b3c2adb9bl8c2bc5ay.dmc.tv
xn--b3c4bij6h.dmc.tv
xn--b3c6akvb2ita3d.dmc.tv
xn--b3c8bdc8eva7a.dmc.tv
xn--b3csuo0ab7m1bzg.dmc.tv
xn--f3cud1bb8af9de5ay9v.dmc.tv
xn--k3cokuac7b3fuaf.dmc.tv
xn--l3cb6b4c.dmc.tv
xn--l3cbbe6dycuc2a0q.dmc.tv
xn--m3c6an5d.dmc.tv
xn--m3camf4iiw.dmc.tv
xn--o3ccd8a3czajzu.dmc.tv
xn--o3ccdf5a0hwat.dmc.tv
xn--o3cd3ac5a2d0a9n.dmc.tv
xn--p3clgfhca0f0a6b.com
xn--p3cte0a3j.dmc.tv
xn--q3cju6cub7h.dmc.tv
xn--r3chqf7fqa.dmc.tv
xn--r3codca8f0aw0q.dmc.tv
xn--r3crbz5a6at.dmc.tv
xn--z3cf4f.dmc.tv
xproasia.com
xstdsl.zyns.com
xuancheng.saomen.com
xuping.co
xuping.net
xupingjewelrywholesale.com
xvie.ipsecsl.net
xx55555.com
xylshgj.com
y1819.com
y200.cn
yaels.eilatinter.co.il
yaindy.org
yamahazone.biz
yantai.saomen.com
yfnt.net
ygdy.net
yinlongmotor.com
yirunsha.com
yisok.com

yitcm.com
ykaol.com
ylfdyc.com
ymcaswimminganddiving.usswim.net
ynoo.net
yogou88.com
yolandabag.com
yongtaiabrasives.com
yorkhikingclub.com
youku.sdjyjy.com
yourcyberworld.com
ys44.com
ysj149.w99.1860php.com
yswimmingnewyork.org
ytwlkd.com
yuhong.info
yukecn.37.600dns.info
yunfu.saomen.com
yunfu1.anzsan.com
yxjy.info
yxman.com
yx-promo.com
yxsyf.com
yy77.com
yzjnpm.com
yzjs.org
z.netjz.net
z4z.us
zazanyc.com
zdcm.net
zdkji.com
zeica.hkwww.com
zero1898.com
zgrsl.zyns.com
zgyycs.net
zgzj2008.com
zh.debuz.com
zhangge5566.info
zhaopin.saomen.com
zhaoqing.saomen.com
zhaosf.592gm.com
zhoujian.host.vpszuyong.com
zhvy.info
zhxgb.com
zjmumen.com
zk.ber88.com
zk170.com
zl889.com
zns463-7129.tw.yokogawa.com
zns463-7129.yokogawa.com.tw
zongq024.37.600dns.info
zs06-135.webzonet.net
zuitty.com
zxzone.com
zzgyfamen.com
zznr.info
zzsxy.net

Bibliography

URLs are valid as of the publication date of this document.

[Internet Storm Center 2013]
Internet Storm Center. *DShield API*. https://isc.sans.edu/api/ (2013).

[Leyden, 2013]
Leyden, John. *Biggest DDoS Attack in History Hammers Spamhaus*. http://www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood/ (March 27, 2013).

[Linux Kernel Organization 2013]
The Linux Kernel Organization. *The Linux Kernel Archives*. https://www.kernel.org/ (2013).

[Mandiant 2013]
Mandiant. *APT1: Exposing One of China's Cyber Espionage Units*. http://intelreport.mandiant.com/?gclid=CJuo9_aYsrkCFUXNOgodVRQA4w (2013).

[Neustar 2013]
Neustar. *GeoPoint 7 Data*. Neustar, 2013.

[nmap.org 2013]
nmap.org. *NMAP*. http://nmap.org/ (2013).

[Open Resolver Project 2013]
Open Resolver Project. *Open Resolver Project*. http://openresolverproject.org/ (2013).

[SEI 2013]
Software Engineering Institute. *SiLK*. http://tools.netsa.cert.org/silk/index.html (2013).

[Unknown 2013]
Unknown. *Internet Census 2012*. http://internetcensus2012.bitbucket.org/paper.html (2013).

[US-CERT 2013a]
US-CERT. *Joint Indicator Bulletin (JIB)-INC260425*. US-CERT, 2013.

[US-CERT 2013b]
US-CERT. *Joint Indicator Bulletin (JIB) - INC260425-2*. US-CERT, 2013.

[Ziegast 2010]
Ziegast, E. *Introduction to SIE*. Flocon 2010, New Orleans, LA, January 11-14, 2010. http://www.cert.org/flocon/2010/proceedings.html (2010).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY
(Leave Blank)

2. REPORT DATE
May 2014

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
Investigating
Advanced Persistent Threat 1 (APT1)

5. FUNDING NUMBERS
FA8721-05-C-0003

6. AUTHOR(S)
Deana Shick & Angela Horneman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2014-TR-001

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFLCMC/PZE/Hanscom
Enterprise Acquisition Division
20 Schilling Circle
Building 1305
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

In February 2013, Mandiant uncovered Advanced Persistent Threat 1 (APT1)—one of China's alleged cyber espionage groups—and provided a detailed report of APT1 operations, along with 3,000 indicators of the group's activity since 2006. This report analyzes unclassified data sets in an attempt to understand APT1's middle infrastructure: the system of hops, distribution points or relays, and the command and control (C2) servers that sit between APT1's victims and main C2 servers located overseas. To build that infrastructure, APT1 chose and exploited particular organizations to obfuscate communications while remaining in plain sight.

This analysis, based on data from IP addresses known to be associated with APT1 and domain names provided by Mandiant, was conducted using a combination of System for Internet Level Knowledge (SiLK) tools, Microsoft Excel, and custom Python scripts. The study detailed in this report can be replicated easily using available sources and tools. By combining key unclassified information, the authors successfully described a large, malicious network used to steal important information.

14. SUBJECT TERMS
APT1, Fingerprinting, Internet Census Data, Open Ports, Analysis, IPv4 Sample

15. NUMBER OF PAGES
100

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL