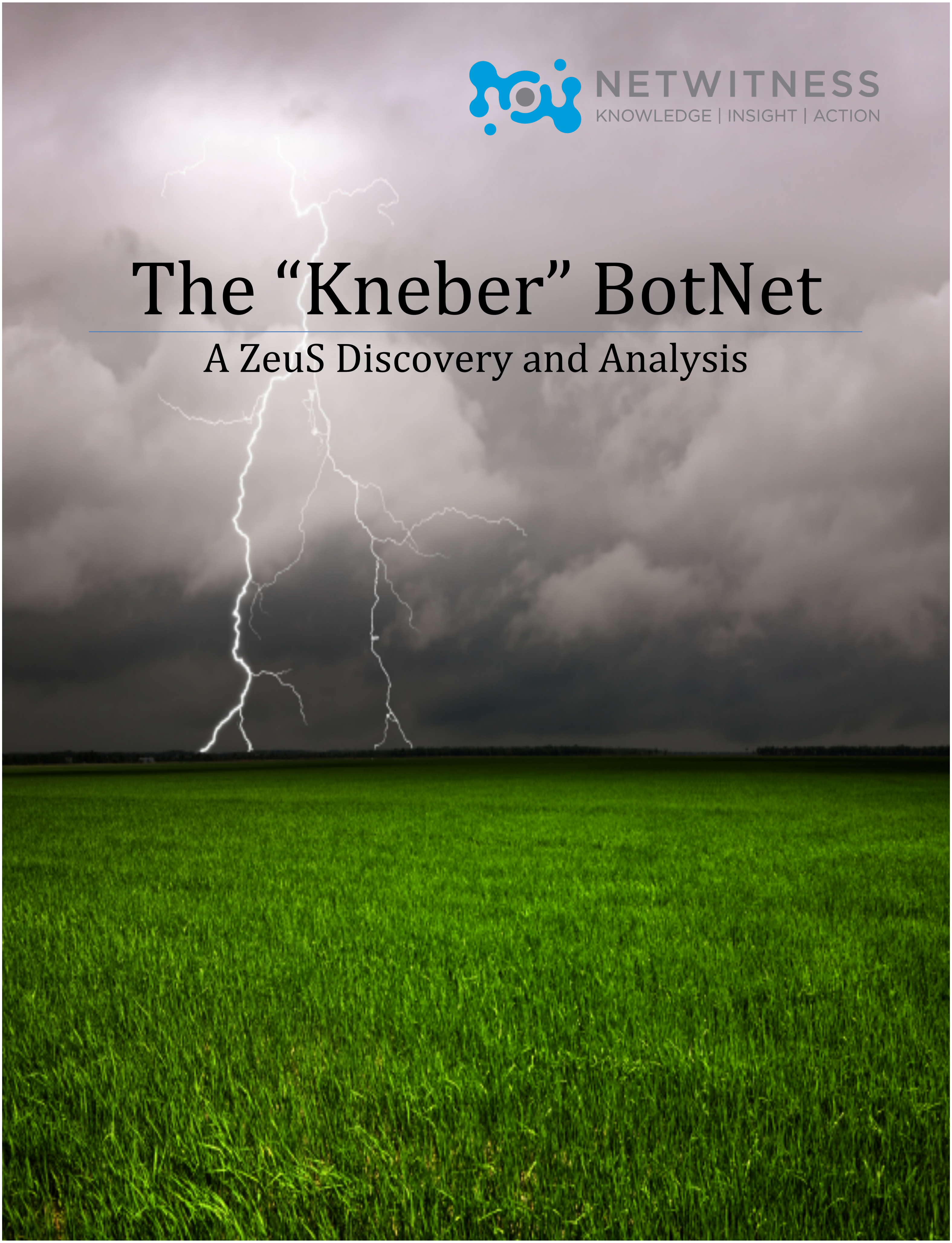
NETWITNESS

KNOWLEDGE | INSIGHT | ACTION



The “Kneber” BotNet

A ZeuS Discovery and Analysis

TABLE OF CONTENTS

THE "KNEBER" BOTNET

A ZeuS Discovery and Analysis

ABSTRACT

On Tuesday, January 26th, 2010 as part of routine analytic tasks related to an evaluation of an enterprise network, NetWitness discovered a 75+ gigabyte cache of stolen data - the result of the activities of an unknown miscreant using a large botnet to control and monitor more than 74,000 compromised PCs. This compromise was discovered by using NetWitness NextGen™ to identify and observe a known member of an existing botnet downloading a new executable. NetWitness provides a series of security analytic applications based on a patented network forensic engine. The use of network forensic methods enables analytic paths and detective capabilities which are specifically required to deal with advanced threats.

One such capability, enabled through real-time automated forensics, provides alerts to security analysts within an organization when obfuscated executables are being downloaded. This particular malicious executable had less than a 10 percent detection rate among all antivirus products and the botnet communication was not identified by existing intrusion detection systems. This compromise, the scope of global penetration and the sheer magnitude of the collected data illustrates the inadequacy of signature based network monitoring methods used by most commercial and public sector organizations today. Full packet capture systems coupled with analytic methods that provide content and context from the network to the application layers are a fundamental requirement today to address advanced threats.

In this case, multi-level analysis of network traffic and active malware analysis using NetWitness, led to some very insightful information about this botnet.

WHAT IS ZEUS?

The format and structure of the logged data indicate a ZeuS Trojan botnet.

At its core, ZeuS is a botnet system designed to steal information from an infected host. Unlike a traditional keylogger system, which records every keystroke, ZeuS can specifically target information desired by the criminal miscreant. It does this through a number of means, but is used primarily to do the following:

- Capture data typed into web forms that are often used for authentication to sensitive systems. By capturing traffic prior to encryption on the endpoint, encrypted authentication mechanisms are subverted.
- Inject additional form elements into target webpages to prompt for additional information from the victim.
- Parse out relevant portions of system URLs that may contains login credentials or session IDs.
- Capture cookie information, which is often used to store credentials and session information for websites.

ZeuS Sequence of Infection

ZeuS receives command and control information from the controlling server via the HTTP protocol. The sequence of infection is typically as follows:

1. A ZeuS executable is run on a target system, either though a social engineering ruse or technical exploit – both are quite common.

- Access and copy credential information stored in a web browser’s ‘protected store”. An example of this is the system used by Microsoft Internet Explorer to save usernames and passwords.

Additionally ZeuS can:

- Search for and capture any file that is resident on the victim host.
- Allow full remote control capability on the victim host using VNC.
- Download and execute arbitrary executables.
- Remotely destroy the host by deleting required elements of the host operation system.

ZeuS uses common malware techniques in order to maximize the amount of time it is resident on a system. These include:

- Using registry entries to survive system reboots.
- Using rootkit technology to hide the malware files and logged data.
- Injecting into running processes to mask traffic and bypass host firewalls.

2. Once installed, the ZeuS bot downloads a configuration file from the command and control server, which directs the bot to capture desired data.
3. Periodically the bot uploads captured information to a “drop zone.”
4. Checks in on a schedule for updates, including updated binaries or configuration files. This allows the criminal miscreant to change the configuration of the botnet at will.

BotNet “Kneber”

BotNet Make-up

Based on analysis of the information cache discovered, this botnet uses the internal name “BTN1”. The data appears to be a one-month dump of data from the controlling server’s database. BTN1 is typically the default name given to a newly created ZeuS botnet.

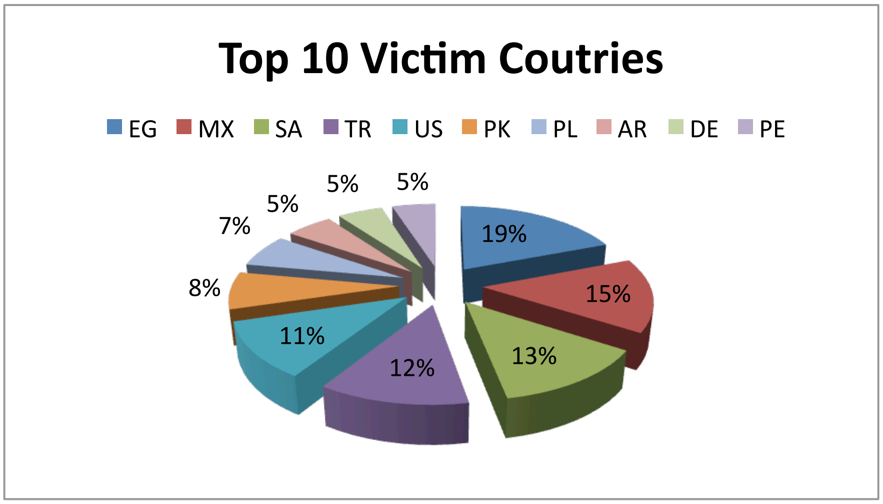
Approximate Size

By counting unique IDs assigned by the ZeuS system, we estimated that BTN1 is composed of 74,126 hosts. Because these logs represent a snapshot in time, the current actual size of the botnet is difficult to measure.

Geographic Scope of Compromise

The ZeuS Trojan records the location of the host when the bot checks into the command and control server. The logs indicate that the following countries are the top five sources for compromised machines:

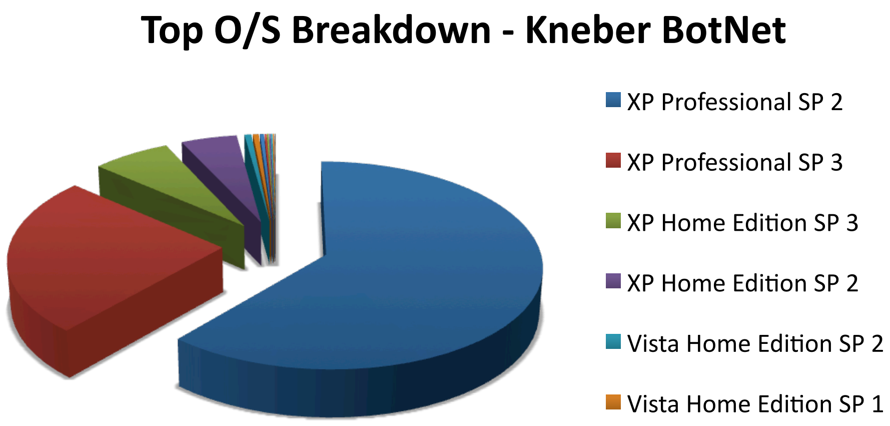
- Egypt
- Mexico
- Saudi Arabia
- Turkey
- United States



In total, the geographic scope of this botnet is 196 unique countries.

Operating System Breakdown

The ZeuS Trojan is purpose-built to infect the Microsoft Windows operating system, and this data reflects that. The top five Windows versions that are infected are as follows:

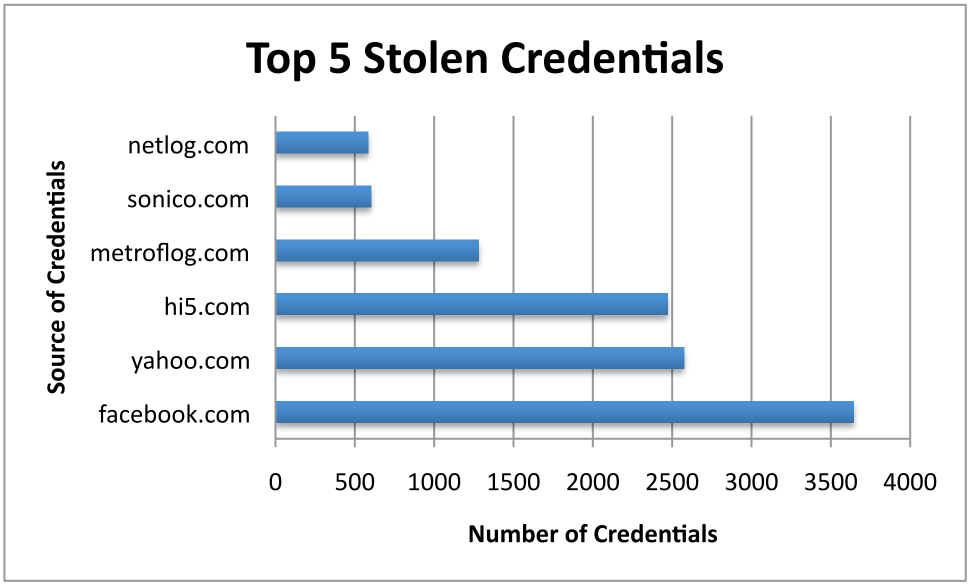


Additionally, but on a much smaller scale, Windows Server and Embedded systems are also represented. The implications of compromises on embedded systems requires additional analysis

Compromised Data

Number of Compromised Credentials

NetWitness analysis clearly shows that this botnet was focused for a period on theft of credentials. The data we analyzed contain over 68,000 stolen credentials during a 4-week period. Although credentials exist for many systems, the following graph shows the 5 most prolific systems represented in this data set.



The top credentials stolen illustrate a focus on social networks and email systems.

Significant Organizational Involvement

When comparing US-based botnet members to IP address-to-organization mapping systems, the following markets and organizations are represented, which include Fortune 500 enterprises:

- Local, State and Federal Government Agencies
- Financial Institutions
- Energy Companies
- Internet Service Providers
- Educational Institutions
- Technology Companies

In total, the scope of organizational compromises by this botnet is 374 unique US-based entities, and 2411 unique global entities.

Certificate Theft

The ZeuS Trojan allows for the theft of any file that is resident on an infected system, and a common target for this capability are encryption certificates used for access to banking, corporate VPN and other sensitive systems.

There were 1972 unique certificates files in the data set.

Banking Focus

By conducting malware analysis on the source malware for this drop, it appears that this data set is from an earlier campaign designed to target social networking and email sites. The most recent configuration file that was downloaded by the malware prior to the site's takedown was almost exclusively designed to target credentials for banking and/or digital currency sites. Please remember, the sites in question may be well managed and adequately secured. The infected machines were simply scraping information when users communicated with the sites below.

A partial list follows:

https://internetbanking.gad.de
https://www.citibank.de
http://ebay.com/
https://www.us.hsbc.com
https://www.e-gold.com
https://online.wellsfargo.com
https://www.paypal.com
https://www.usbank.com
https://www.tdcanadatrust.com
https://onlinebanking.nationalcity.com
https://www.citizensbankonline.com
https://onlinebanking.nationalcity.com
https://www.suntrust.com

https://www.53.com
https://web.da-us.citibank.com
https://onlineeast.bankofamerica.com
https://online.wamu.com
https://onlinebanking.wachovia.com
https://resources.chase.com
https://bancaonline.openbank.es
https://extranet.banesto.es
https://empresas.gruposantander.es
https://www.bbvanetoffice.com
https://www.bancajaproximaempresas.com
https://probanking.procreditbank.bg
https://ibank.internationalbanking.barclays.com
https://online-offshore.lloydstsb.com
http://www.hsbc.co.uk
https://www.nwolb.com
https://home.ybonline.co.uk
https://home.cbonline.co.uk
https://internetbanking.gad.de
https://www.citibank.de
http://ebay.com/
https://www.us.hsbc.com
https://www.e-gold.com
https://online.wellsfargo.com
https://www.paypal.com
https://www.usbank.com
https://www.tdcanadatrust.com
https://onlinebanking.nationalcity.com
https://www.citizensbankonline.com
https://onlinebanking.nationalcity.com
https://www.suntrust.com
https://www.53.com
https://web.da-us.citibank.com
https://onlineeast.bankofamerica.com
https://online.wamu.com
https://onlinebanking.wachovia.com
https://resources.chase.com
https://bancaonline.openbank.es
https://extranet.banesto.es
https://empresas.gruposantander.es
https://www.bbvanetoffice.com
https://www.bancajaproximaempresas.com
https://probanking.procreditbank.bg
https://ibank.internationalbanking.barclays.com
https://online-offshore.lloydstsb.com
http://www.hsbc.co.uk
https://www.nwolb.com

Credit Card Numbers

While not the primary purpose of Zeus, occasionally credit card numbers are recorded as part of the Trojan’s logging activity. In this data set across thousands of systems, only several hundred unique credit card numbers were present.

Social Security Numbers

The Zeus Trojan can also record social security numbers during logging activity. Only a few hundred unique SSNs were present.

https://home.ybonline.co.uk
https://home.cbonline.co.uk

This targeted attack against banking infrastructures on a worldwide scale includes e-banking and other entities. In many cases, form elements are injected into these login pages to provide answers to common “security questions” such as:

- “What is your mother’s maiden name?”
- “What street did you grow up on?”
- “What was your first pet’s name?”

Because these questions are often used to allow remote reset of passwords and credentials, it shows a desire and potential for the miscreant to be able to leverage the compromise onto other systems for additional access.

Connection to Waledac BotNet

One very interesting observation is that more than half of the ZeuS bots are logging traffic from additional infections on the same host that are indicative of Waledac command and control traffic. Waledac is a peer-to-peer spamming botnet that is often used as a delivery mechanism for additional malware. Additional analysis needs to be conducted, but this raises the possibility of direct enterprise-to-enterprise communication of Waledac bot peers in addition the existing C2 traffic from the Zeus botnet.

While it is not uncommon for compromised hosts to have multiple strains of malware, the sheer amount of Waledac traffic in this data set suggests a possible link between this ZeuS infrastructure and the Waledac botnet and their respective controlling entities. At the very least, two separate botnet families with different C2 structures can provide fault tolerance and recoverability in the event that one C2 mechanism is taken down by security efforts.

Attribution

Attributing this activity to a single individual or group of individuals is exceptionally difficult to do well without global cooperation across disparate technology and organizational systems. However, some key information can be revealed about the miscreants involved with this operation by tying IP, domain and registry information together.

WEB OF MALICIOUSNESS

The initial domain that was the source of this cache revealed a single registrant as follows:

hilarykneber@yahoo.com

Cross referencing this email address with the Malware Domain List[1] results in a network of malicious activity including a focus on ZeuS and the use of exploit kits:

vkontalte.cn - PDF exploits and Trojan installs
online-counter.cn – Exploit Kit, PDF exploits and Trojan installs
bizuklux.cn – ZeuS Controller
liagand.cn – El Fiesta Exploit kit2, PDF exploits, Trojan installs
morsayniketamere.cn – ZeuS Controller
mydailymail.cn – ZeuS Controller
grizzli-counter.com – Exploit kit and Trojan install
tds-info.net – Exploit Kit and Trojan install
kolordat482.com – ZeuS Controller
yespacknet.org – Yes Exploit Kit3, PDF exploits, Trojan install
scriptwb.com – Yes Exploit Kit, Trojan install
qbzq16.com – ZeuS Controller
mega-counter.com – Trojan install
silence7.cn – ZeuS Controller
iuylqb.cn – ZeuS Controller
pidersli.net – ZeuS Controller
klalkius.com – Liberty Exploit Kit4, Flash and PDF exploits, Trojan install
secureantibot.net – Yes Exploit Kit, PDF exploits, Trojan installs
adobe-config-s3.net – ZeuS Controller

GLOBAL DISPERSION

When these domain names are resolved to their associated IP addresses, a global distribution of servers is evident, with a focus on Chinese IPs:

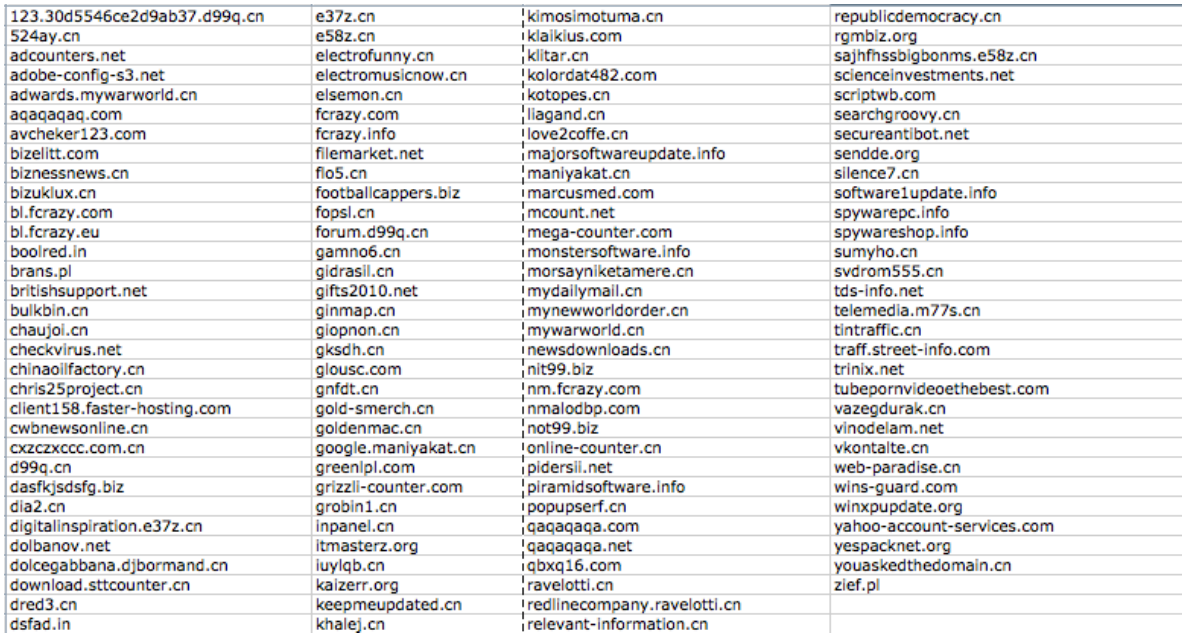
IP Address	Country	Organization
113.105.152.71	CN	CHINANET-BACKBONE No.31,Jin-rong Street"
122.115.63.17	CN	JINGXUN Beijing Jingxun Public Information Technology Co., Ltd"
122.225.117.147	CN	CHINANET-BACKBONE No.31,Jin-rong Street"
125.46.60.222	CN	CHINA169-BACKBONE CNCGROUP China169 Backbone"
218.93.205.19	CN	CHINANET-BACKBONE No.31,Jin-rong Street"
218.93.205.246	CN	CHINANET-BACKBONE No.31,Jin-rong Street"
58.218.199.186	CN	CHINANET-BACKBONE No.31,Jin-rong Street"

[1] Malware Domain List -http://www.malwaredomainlist.com – an open forum and database of malware-related activity with contributions from the security research community.
[2] http://blog.novirusthanks.org/2008/12/website-spreading-virus-through-exploits-elfiesta-exploit-kit/
[3] http://evilfingers.blogspot.com/2009/05/yes-exploit-system-manipulating-safety.html
[4] http://blog.webroot.com/2009/09/18/one-click-and-the-exploit-kits-got-you/

IP Address	Country	Organization
58.218.199.239	CN	CHINANET-BACKBONE No.31,Jin-rong Street"
59.53.91.102	CN	CHINANET-BACKBONE No.31,Jin-rong Street"
60.12.117.147	CN	CHINA169-BACKBONE CNCGROUP China169 Backbone"
61.235.117.71	CN	CRNET CHINA RAILWAY Internet(CRNET)"
61.235.117.86	CN	CRNET CHINA RAILWAY Internet(CRNET)"
61.4.82.216	CN	DXTNET Beijing Dian-Xin-Tong Network Technologies Co., Ltd."
193.104.110.88	CZ	SOFTNET Software Service Prague s.r.o."
95.169.186.103	DE	KEYWEB-AS Keyweb AG"
222.122.60.186	KR	KIXS-AS-KR Korea Telecom"
217.23.10.19	NL	WORLDSTREAM WorldStream"
85.17.144.78	NL	LEASEWEB LEASEWEB AS"
200.106.149.171	PA	Hosting Panama"
200.63.44.192	PA	Eveloz"
200.63.46.134	PA	Eveloz"
91.206.231.189	RU	WEBALTA-AS Wahome networks"
124.109.3.135	TH	SERVENET-AS-TH-AP ServeNET Solution Limited Partnership"
61.61.20.134	TW	KGTNET-TW KG Telecommunication Co., Ltd"
91.206.201.14	UA	ANSUA-AS PE Sergey Demin"
91.206.201.222	UA	ANSUA-AS PE Sergey Demin"
91.206.201.8	UA	ANSUA-AS PE Sergey Demin"
216.104.40.218	US	SINGLEHOP-INC - SingleHop"
69.197.128.203	US	WII-KC - WholeSale Internet, Inc."

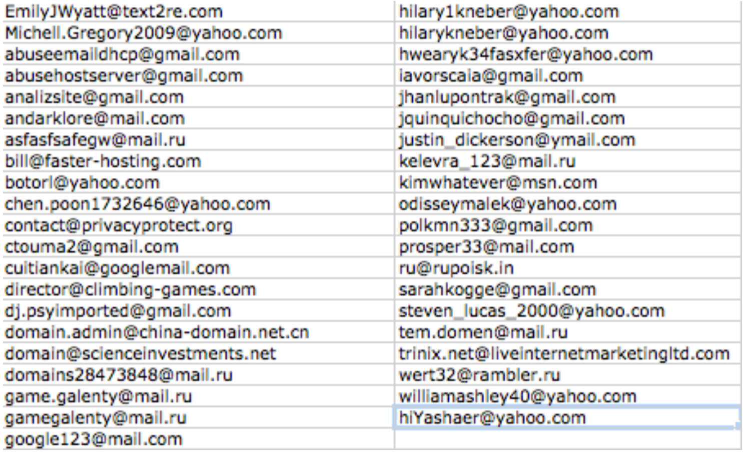
Multiple Aliases

Tying the IP addresses back into the Malware Domain List expands the “associated miscreant“ list to include a total of 126 malicious domains:



123.30d5546ce2d9ab37.d99q.cn
524ay.cn
adcounters.net
adobe-config-s3.net
adwards.mywarworld.cn
aqaqaqaq.com
avcheker123.com
bizelitt.com
biznessnews.cn
bizuklux.cn
bl.fcrazy.com
bl.fcrazy.eu
boolred.in
brans.pl
britishsupport.net
bulkbin.cn
chaujoi.cn
checkvirus.net
chinaoilfactory.cn
chris25project.cn
client158.faster-hosting.com
cwbnewsonline.cn
cxzczxccc.com.cn
d99q.cn
dasfkjsdsfg.biz
dia2.cn
digitalinspiration.e37z.cn
dolbanov.net
dolcegabbana.djbormand.cn
download.sttcounter.cn
dred3.cn
dsfad.in
e37z.cn
e58z.cn
electrofunny.cn
electromusicnow.cn
elsemon.cn
fcrazy.com
fcrazy.info
filemarket.net
flo5.cn
footballcappers.biz
fopsl.cn
forum.d99q.cn
gamno6.cn
gidrasil.cn
gifts2010.net
ginmap.cn
giopnon.cn
gksdh.cn
glousc.com
gnfdt.cn
gold-smerch.cn
goldenmac.cn
google.maniyakat.cn
greenlpl.com
grizzli-counter.com
grobin1.cn
inpanel.cn
itmasterz.org
iuylqb.cn
kaizerr.org
keepmeupdated.cn
khalej.cn
kimosimotuma.cn
klaikius.com
klitar.cn
kolordat482.com
kotopes.cn
liagand.cn
love2coffe.cn
majorsoftwareupdate.info
maniyakat.cn
marcusmed.com
mcount.net
mega-counter.com
monstersoftware.info
morsayniketamere.cn
mydailymail.cn
mynewworldorder.cn
mywarworld.cn
newsdownloads.cn
nit99.biz
nm.fcrazy.com
nmalodbp.com
not99.biz
online-counter.cn
pidersii.net
piramidsoftware.info
popupserf.cn
qaqaqaqa.com
qaqaqaqa.net
qbxq16.com
ravelotti.cn
redlinecompany.ravelotti.cn
relevant-information.cn
republicdemocracy.cn
rgmbiz.org
sajhfhssbigbonms.e58z.cn
scienceinvestments.net
scriptwb.com
searchgroovy.cn
secureantibot.net
sendde.org
silence7.cn
software1update.info
spywarepc.info
spywareshop.info
sumyho.cn
svdrom555.cn
tds-info.net
telemedia.m77s.cn
tintraffic.cn
traff.street-info.com
trinix.net
tubepornvideoethebest.com
vazegdurak.cn
vinodelam.net
vkontalte.cn
web-paradise.cn
wins-guard.com
winxpupdate.org
yahoo-account-services.com
yespacknet.org
youaskedthedomain.cn
zief.pl

And 41 malicious registrants by email address:

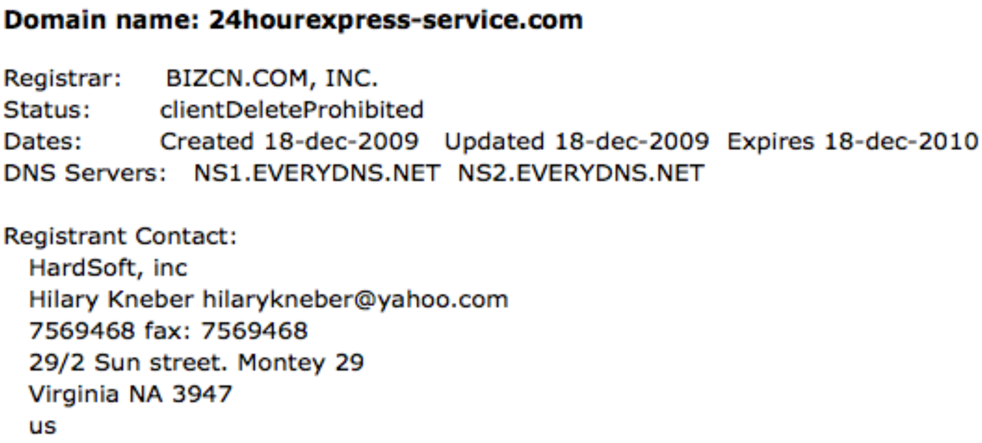


EmilyJWyatt@text2re.com
Michell.Gregory2009@yahoo.com
abuseemaildhcp@gmail.com
abusehostserver@gmail.com
analizsite@gmail.com
andarklore@mail.com
asfasfsafegw@mail.ru
bill@faster-hosting.com
botorl@yahoo.com
chen.poon1732646@yahoo.com
contact@privacyprotect.org
ctouma2@gmail.com
cuitiankai@googlemail.com
director@climbing-games.com
dj.psyimported@gmail.com
domain.admin@china-domain.net.cn
domain@scienceinvestments.net
domains28473848@mail.ru
game.galenty@mail.ru
gamegalenty@mail.ru
google123@mail.com
hilary1kneber@yahoo.com
hilarykneber@yahoo.com
hwearyk34fasxfer@yahoo.com
iavorscaia@gmail.com
jhanlupontrak@gmail.com
jquinquichocho@gmail.com
justin_dickerson@ymail.com
kelevra_123@mail.ru
kimwhatever@msn.com
odisseymalek@yahoo.com
polkmn333@gmail.com
prosper33@mail.com
ru@rupoisk.in
sarahkogge@gmail.com
steven_lucas_2000@yahoo.com
tem.domen@mail.ru
trinix.net@liveinternetmarketingltd.com
wert32@rambler.ru
williamashley40@yahoo.com
hiYashaer@yahoo.com

Indications of Monetization Activity:

A Google search for the original email address (hilarykneber@yahoo.com) also reveals website registration activity pertaining to money-mule recruitment. This is a common way for criminal miscreants to monetize online fraud in which they use unsuspecting "employees" to do deposits, withdrawals, and wires to offshore accounts. Once the money has been transferred to these locations, the miscreant quickly withdraws the currency to stymie victim organization fraud recovery efforts.

http://www.bobbear.com/24-hour-express-service.html



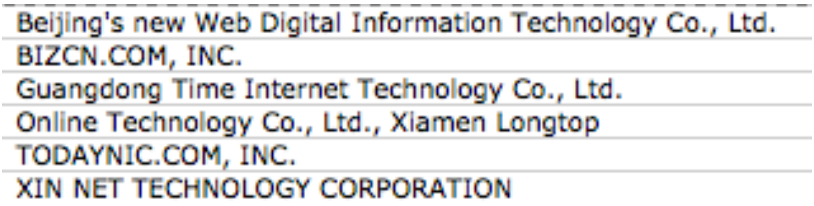
Domain name: 24hourexpress-service.com

Registrar: BIZCN.COM, INC.
Status: clientDeleteProhibited
Dates: Created 18-dec-2009 Updated 18-dec-2009 Expires 18-dec-2010
DNS Servers: NS1.EVERYDNS.NET NS2.EVERYDNS.NET

Registrant Contact:
HardSoft, inc
Hilary Kneber hilarykneber@yahoo.com
7569468 fax: 7569468
29/2 Sun street. Montey 29
Virginia NA 3947
us

Abuse of Chinese Registration Services:

.CN domains make up a subset of the observed criminal domains and the following registrars appear to bear the brunt of the abuse. All are Chinese.

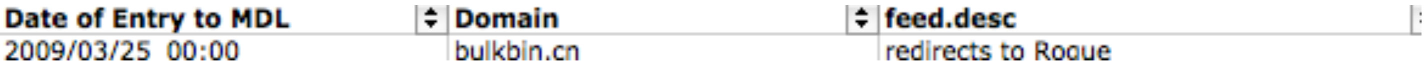


Beijing's new Web Digital Information Technology Co., Ltd.
BIZCN.COM, INC.
Guangdong Time Internet Technology Co., Ltd.
Online Technology Co., Ltd., Xiamen Longtop
TODAYNIC.COM, INC.
XIN NET TECHNOLOGY CORPORATION

A Long-Running Criminal Enterprise

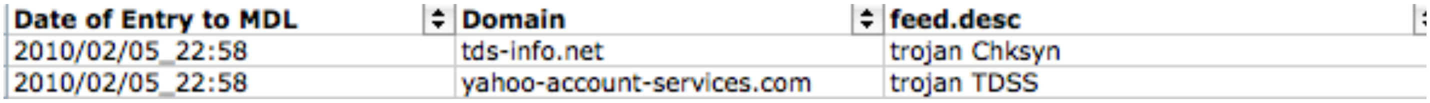
Taken as a whole, the associated IP, domain and network tie-ins show that this exploit campaign has been running for nearly a year and is still active.

Initial reports of maliciousness with this data set date back to March 25th, 2009.



Date of Entry to MDL	Domain	feed.desc
2009/03/25 00:00	bulkbin.cn	redirects to Rogue

The most recent report of maliciousness with this data set is February 5th, 2010



Date of Entry to MDL	Domain	feed.desc
2010/02/05_22:58	tds-info.net	trojan Chksyn
2010/02/05_22:58	yahoo-account-services.com	trojan TDSS

Targeting the Government Sector

Recent events also show this miscreant group targeting the government sector specifically via phishing emails as detailed here:

http://www.krebsonsecurity.com/2010/02/zeus-attack-spoofs-nsa-targets-gov-and-mil/

Conducting malware analysis on the involved samples reveals command and control systems that reside in the same network location as other involved servers:

updatekernel.com. 3144 IN A 115.100.250.119

WHOIS information for this domain indicates a connection to previously used registration information:

Domain Name: UPDATEKERNEL.COM
Registrar: TODAYNIC.COM, INC.
Email: abuseemaildhcp@gmail.com
Creation Date: 31-jan-2010

TODAYNIC.COM is one of the previously listed abused Chinese registrars, and "abuseemaildhcp@gmail.com" was used in a previous exploit campaign initially reported on August 18th, 2009:

Domain Name: popupserf.cn
Registrar: Guangdong Time Internet Technology Co., Ltd.
Administrative Email: abuseemaildhcp@gmail.com
Registration Date: 2009-07-24 23:04

This activity shows that this miscreant group is not only using exploit kits to steal banking login credentials and propagate their malware (as previously detailed), but is now also targeting government agencies with convincing phishing emails (that correctly identify existing projects) with a high degree of success. In this case, the National Intelligence Council's "2020 Project"5 was used as a social engineering hook.

IMPLICATIONS

There are a number of key threat intelligence findings and implications derived from our analysis of the activities of the controlling miscreant:

1. Zeus, typically considered a "Banking Trojan", also is being employed specifically to target social networking and email sites.

This bot shows that the developers of the ZeuS system have a deep understanding of the nature of the Web and the manner in which people use their computers. While targeting financial sites ultimately may result in financial gain for the miscreant, targeting logon credentials to social networks and email gives them the "keys to the castle." This personal information is pivotal for stealing identities and crafting very well targeted and convincing criminal and espionage campaigns.

Social networks are among the most popular and oft-visited websites on the Internet. Compromising these accounts provides the miscreant a network of "friends" who will inherently trust the compromised account and would be more likely to click on phishing and other exploit messages from that account. Additionally social networks offer a centralized repository of data on an individual that can be used for highly sensitive activities, such as password resets, credit account creation, or other types of identity-oriented fraud.

Email accounts are often the critical part of the credentialing process of many sites on the Internet because they form the "username" component of the login process. Email accounts are used for contact points, authentication mechanisms, alerting, information distribution, password resets and much more. Controlling an email account gives the criminal miscreant an enormous leverage point for the compromise of additional systems associated with the end-user. These systems could include banking systems as previously discussed, but also could include corporate or government systems because many people utilize the same password constructs for both personal and professional environments.

5 http://www.dni.gov/nic/NIC_2020_project.html

2. Miscreants are not limiting themselves to a single geographic target area.

The analysis of this incident data shows a worldwide dispersion of command and control structures, exploit systems, infected hosts and compromised credentials. This indicates an interest in all types of data regardless of language and geo-political boundaries.

Miscreants are using specifically targeting Government Agencies as well as Private Firms

The previously detailed phishing attack on US Government agencies shows miscreants using relevant process names and inside knowledge of government organization to craft convincing email messages designed to gain access to information and further propagate their botnets. This event illustrates a desire to penetrate sensitive organizations for data gathering. Observing this criminal element’s activities over time, lead to the highly likely scenario that such insider knowledge came from previously successful infection campaigns. This discovery supports previous stories that foreign intelligence services are purchasing government data from criminal hackers.

3. Criminal “gangs” may be working together to provide sustainability to their botnets

The link between ZeuS and Waledac in this finding provides valuable threat intelligence because it shows hosts being infected with two different families of botnet malware at the same time. It is highly improbable that such crosspollination of botnets went unnoticed. If the owners of these two botnets are working together, there is the strong potential for additional resilience for both systems.

In the event that one of the two botnet command and control structures is disrupted by security efforts, the surviving C2 could be used to “recover” the disrupted activity. This could be as simple as providing a new configuration file to a ZeuS bot in order to reassign a new C2 server, to pushing a new malware system and control method altogether.

4. Cyber-criminals operate with impunity for extended periods of time.

Connecting the dots of this incident shows a world-wide dispersal of exploitation and botnet command and control activity, the use multiple families of malware and exploitation technology to accomplish specific goals and the world-wide abuse of registration services regardless of language barrier.

5. Ultimate End-User of these data is unknown.

It is well known that an underground criminal data mart exists where these vast harvests of account numbers, email and social network accounts, and other PII can be bought and sold. Although the operator of this botnet may have had certain specific theft objectives during a period, the ultimate consumer of these data could range from criminal enterprises for certain pieces, to terrorist groups and state-sponsored entities for other credentials and information that would be useful to their specific enterprises and end goals. The ultimate implications of these undetected data losses and infestations of public and commercial organizations are far-reaching and complex and transcend simple labels attached to them.

SUMMARY

While this is a large-scale botnet with large volumes of collected information, it is ultimately a very small portion of the amount of data being stolen from individuals, corporations, and government agencies on an ongoing basis. This is illustrated by both the limited time frame of stolen information in this cache (only one-month’s capture), as well as the evidence supporting the existence of a large and dispersed criminal enterprise.

The analysis of this activity plainly depicts the scale and sophistication of one botnet. It reiterates what security professionals with even a modest understanding of the current threat environment already know:

Advanced threats have festered their way into thousands of enterprises. The widely deployed security technologies modern enterprises use to protect themselves such as firewalls, antivirus and intrusion detection technologies, even when well managed, are ineffective in countering the current and ongoing threat to our information systems posed by a focused criminal adversary or nation-state.

Social Networking, Online Banking, Corporate Security, National Security, Intellectual Property Theft, and nearly every other information security concern are inextricably linked by the data being siphoned off to criminal and sponsored adversaries. In an environment where compromised systems are key to broad data theft, security professionals can no longer afford to turn a blind eye to problems by categorizing them broadly as affecting other markets. Nearly all security vendors who cover these specific examples of malicious code have lumped them into a category of "banking Trojan." Analysis of the Kneber data reveals the keys to thousands of corporate networks around the world, and activities specifically targeting the United States Department of Defense. Neither nation-state nor criminal adversaries are concerned with how we categorize their exploits. They are diligently focused on stealing sensitive information using increasingly sophisticated methods and evading the rudimentary security capabilities so many organizations continue to rely on with a false sense of security.

This white paper was written by Alex Cox and Gary Golomb, NetWitness Corporation, 500 Grove Street, Suite 300, Herndon, VA 20170. http:// www.netwitness.com.

If you would like to know more about how we discovered Kneber using NetWitness technology; or how your organization can detect advanced threats and problems such as Kneber, and avoid costly and damaging problems, please contact NetWitness for a proof-of-concept. sales@netwitness.com. Download the freeware version of NetWitness Investigator today: http://download.netwitness.com and see what’s really happening on your network.