Scope of ‘KeyBoy’ Targeted Malware Attacks

By Jaeson Schultz

Published: 2013-06-13 · Archived: 2026-04-05 22:35:20 UTC

Skip to content

On June 6, 2013, malwaretracker.com released an analysis of Microsoft Office-based malware that was exploiting a previously unknown vulnerability that was patched by MS12-060. The samples provided were alleged to be targeting Tibetan and Chinese Pro-Democracy Activists. On June 7, 2013, Rapid7 released an analysis of malware dubbed ‘KeyBoy,’ also exploiting unknown vulnerabilities in Microsoft Office, similarly patched by MS12-060, but allegedly targeting interests in Vietnam and India. The indicators of compromise (IoCs) listed by Rapid7 match some of the indicators of compromise listed previously by malwaretracker.com.

command and control domains (partial list):
board.nboard.net
98.126.9.34
comsskk.wordpress.com
comsskk.sosblogs.com
comsskk.livejournal.com
www.tigdiho.com
114.142.147.51
tianshao007.vicp.cc
rss.groups.yahoo.com
wut.mophecfbr.com
radiomusictv.wordpress.com
wikipedia.authorizeddns.org (pitty tiger)
login.aerotche.com (Creation date: 05 Jun 2013 13:58:00)
HHGJGOCNHIHADCCNDC.terhec.com (Creation date: 06 Jun 2013 07:24:00)
silence.phdns01.com
cpnet.phmail.us
imlang.phmail.org

IoCs published by malwaretracker.com.

Analysis of the Protocol

The backdoor tries to contact the following domains until it gets a response from an active one:

- silence.phdns1.com
- cpnet.phmail.us
- imlang.phmail.org

The Indian backdoor tries to contact the following domains instead:

- creey.zyns.com
- preter.epac.to
- backto.ddns.name

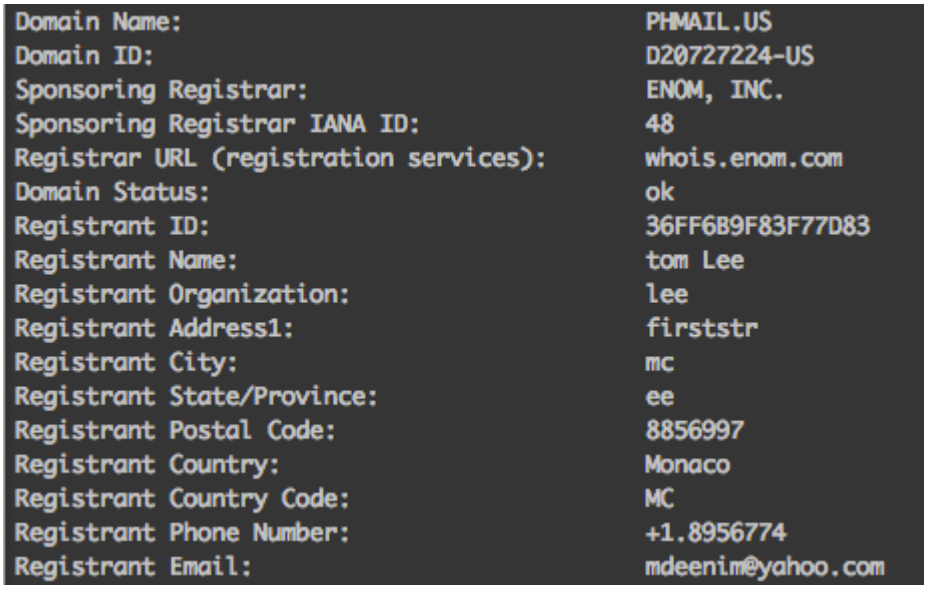
In the first set of domains they are either registered with Whois proxy services or with fake identities. In the second set they are making use of a dynamic DNS service by ChangeIP.com.
Following are traces collected from passive DNS data relevant to the hosts involved in these attacks:

Domain	First Seen	Last Seen	IPs	ASN
silence.psdns01.com	May 21st 2013	May 25th 2013	199.193.66.51 (TTL: 1800)	6939 - HURRICANE - Hurricane Electric, Inc.
cpnet.phmail.us	May 10th 2013	May 24th 2013	199.193.66.51 (TTL: 1800)	6939 - HURRICANE - Hurricane Electric, Inc.
imlang.phmail.org	May 22nd 2013	May 23rd 2013	199.193.66.51 (TTL: 1800)	6939 - HURRICANE - Hurricane Electric, Inc.
vtt.phdns01.com	March 9th 2013	April 19th 2013	199.193.66.51 (TTL: 1800)	6939 - HURRICANE - Hurricane Electric, Inc.
preter.epac.to	May 31st 2013	May 31st 2013	1.235.10.28 (TTL: 30)	9318 - HANARO-AS Hanaro Telecom Inc.
preter.epac.to	May 18th 2013	May 28th 2013	113.160.44.154 (TTL: 30)	45899 - VNPT-AS-VN VNPT Corp

IoCs published by Rapid7.

As we have seen in some previous targeted malware attacks, the attackers in this incident are taking advantage of services like changeip.com to establish free subdomains in their infrastructure. While TRAC is sure that many subdomains used at changeip.com have no malicious purpose, there is no denying the fact that attackers mounting targeted attacks are also attracted to these ‘free’ services. Blending in with legitimate traffic is a common tactic used by attackers to help fly under the radar. Not many professional organizations have valid reasons to allow traffic to domains offered by changeip.com, so blacklisting these domains is an option.

One of the second-level domains listed as an IoC is phmail.us. Subdomains at phmail.us have been linked to malicious activity dating back as far as December 2011. Based on the patterns of subdomain registration over time in DNS, TRAC believes this is an example where the attackers registered their own second-level domain. The WHOIS data, including the address, postal code and telephone number, is obviously forged.



```
Domain Name:                          PHMAIL.US
Domain ID:                            D20727224-US
Sponsoring Registrar:                 ENOM, INC.
Sponsoring Registrar IANA ID:         48
Registrar URL (registration services): whois.enom.com
Domain Status:                        ok
Registrant ID:                        36FF6B9F83F77D83
Registrant Name:                      tom Lee
Registrant Organization:              lee
Registrant Address1:                  firststr
Registrant City:                      mc
Registrant State/Province:            ee
Registrant Postal Code:               8856997
Registrant Country:                   Monaco
Registrant Country Code:              MC
Registrant Phone Number:              +1.8956774
Registrant Email:                     mdeenim@yahoo.com
```

Fake WHOIS record data for phmail.us.

An eclectic group of subdomains has been used at phmail.us, including the following:

cpnet.phmail.us
dnd.phmail.us
hoasen.phmail.us

inquirer.phmail.us
phattai.phmail.us
rfa.phmail.us
sscdtt.phmail.us
ttbc.phmail.us
www.phmail.us
yah00.phmail.us
yl.phmail.us
ynsc.phmail.us

While watching some of these domains using passive DNS a peculiar pattern emerges. For a long period of time, many of the DNS responses for a hostname will return 127.0.0.1, but every so often, presumably when a likely target is on-the-hook, the domain name servers return a routable IP. Perhaps this is a tactic designed to evade or postpone eventual detection and assist in staying below the radar. Note in the following graphic the DNS server replied 717 times with 127.0.0.1; however during that same time, the real routable IPs were also offered to certain requesters.

bailiwick	**phmail.us.**
count	0
first seen	2011-12-15 09:16:58 -0000
last seen	2011-12-15 09:16:58 -0000
ynsc.phmail.us.	A 118.114.197.165

bailiwick	**phmail.us.**
count	6
first seen	2012-01-05 01:03:46 -0000
last seen	2012-01-05 06:35:56 -0000
ynsc.phmail.us.	A 125.70.20.181

bailiwick	**phmail.us.**
count	10
first seen	2011-12-07 09:28:57 -0000
last seen	2011-12-08 01:18:47 -0000
ynsc.phmail.us.	A 125.70.21.254

bailiwick	**phmail.us.**
count	717
first seen	2011-10-22 07:31:57 -0000
last seen	2012-03-07 00:44:11 -0000
ynsc.phmail.us.	A 127.0.0.1

Another IoC second-level domain from this group (phdns01.com) exhibits exactly the same WHOIS and passive DNS patterns:

silence.phdns01.com
symantec.phdns01.com
www.phdns01.com
hanoihcm.phdns01.com
sscd.phdns01.com

bailiwick	**phdns01.com.**
count	11
first seen	2010-12-06 04:05:02 -0000
last seen	2010-12-07 12:43:40 -0000
sscd.phdns01.com.	A 58.103.18.53

bailiwick	**phdns01.com.**
count	47
first seen	2010-12-04 16:02:42 -0000
last seen	2010-12-07 22:53:54 -0000
sscd.phdns01.com.	A 127.0.0.1

TRAC recommends analyzing DNS traffic for these IoCs on your own networks. In this case, maintaining the latest patches would also have thwarted the attacks, and is always an excellent idea. Additionally, blacklisting the domains offered by changeip.com using local RPZs, firewalls, Cisco IronPort Web Security Appliance (WSA), or Cloud Web Security (CWS) are additional options that can help add an extra level of security.

Thanks to Craig Williams and Emmanuel Tacheau for their assistance in co-writing this blog post.

Authors

Cisco Cybersecurity Viewpoints

Where security insights and innovation meet. Read the e-book, see the video, dive into the infographic and more...

Why Cisco Security?

Explore our Products & Services

Source: https://blogs.cisco.com/security/scope-of-keyboy-targeted-malware-attacks