Buckeye cyberespionage group shifts gaze from US to Hong Kong

Several organizations in Hong Kong are being targeted by a cyberespionage group known as Buckeye.
By: Symantec Security Response Symantec Employee

Created 06 Sep 2016

Buckeye (also known as APT3, Gothic Panda, UPS Team, and TG-0110) is a cyberespionage group that is believed to have been operating for well over half a decade. Traditionally, the group attacked organizations in the US as well as other targets. However, Buckeye's focus appears to have changed as of June 2015, when the group began compromising political entities in Hong Kong. Since March 2016, the group has appeared to mostly focus on organizations in Hong Kong, sending malicious emails to targets as recently as August 4, and attempting to spread within compromised networks in order to steal information.

Using the combined threat intelligence of Symantec and Blue Coat Systems, we have built a clear and concise picture of how Buckeye has evolved its tactics in recent years. This has allowed us to further enhance our protection capabilities against the group's campaigns.

Background

Symantec has observed Buckeye activity dating back to 2009, involving attacks on various organizations in several regions. Buckeye used a remote access Trojan (Backdoor.Pirpi) in attacks against a US organization's network in 2009. The group delivered Backdoor.Pirpi through malicious attachments or links in convincing spear-phishing emails. Symantec has identified additional tools used by the group, which will be discussed later.

Buckeye has been known to exploit zero-day vulnerabilities in the past, such as CVE-2010-3962 in an campaign in 2010 and CVE-2014-1776 in 2014. Although other zero-day attacks have been reported, they have not been confirmed by Symantec. All zero-day exploits known, or suspected, to have been used by this group are for vulnerabilities in Internet Explorer and Flash.

Shifting focus of attacks

More recently, Symantec telemetry has revealed Backdoor.Pirpi connections from compromised computers based in Hong Kong dating back to August 2015. The infections significantly increased in number towards the end of March 2016 and the beginning of April 2016. Additional investigations discovered related malware samples and determined that targeted organizations were political entities in Hong Kong.

In at least some of these recent attacks, Buckeye used spear-phishing emails with a malicious .zip attachment. The .zip archive attached to the email contains a Windows shortcut (.lnk) file with the Microsoft Internet Explorer logo. Clicking on the shortcut ultimately leads to Backdoor.Pirpi being downloaded and executed on the affected computer.

Who's being targeted?

From 2015 to date, Symantec identified approximately 82 organizations in various regions that had Buckeye tools present on their network. However, this is not an accurate picture of the targets of interest to Buckeye. The group casts a wide net while trawling for targets but only remains active on the networks of organizations it is interested in. Symantec determined a more accurate picture of Buckeye's targets by looking at where Buckeye remained active on the network longer than a day, deployed additional tools, and spread onto multiple computers. After these filters were applied to our data, we found a total of 17 organizations, located in Hong Kong (13), the US (3), and the UK (1).

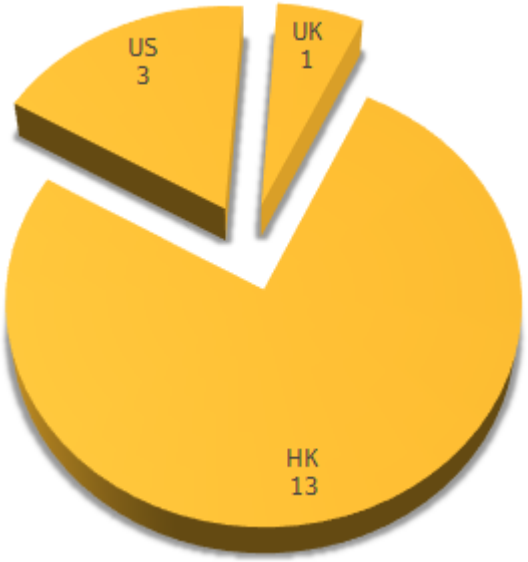

Figure 1. Buckeye victims of interest by region (2015 to date)

It should be noted that this data goes back to 2015 and that the proportion of targets in Hong Kong from March 2016 would be considerably higher. Up to mid-2015, Buckeye's traditional targets were varying categories of US organizations, which match the types of victims seen in the UK. Buckeye interests changed substantially around June 2015 when the group began infecting organizations in Hong Kong. Infections in the UK and US ceased shortly after this time.

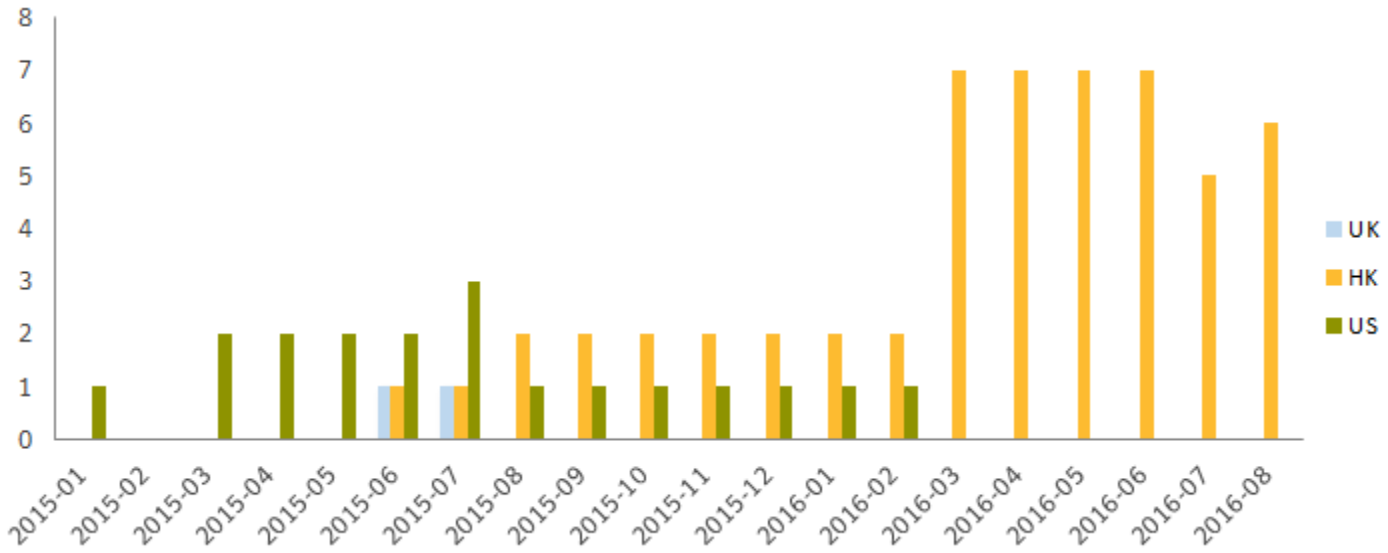

Figure 2. Organizations that Buckeye targeted over time, per region

Malware and tools

Buckeye uses a number of hacking tools as well as malware. Many of the hacking tools are open source applications that have been patched or modified in some manner by Buckeye in an attempt to evade detection.

Buckeye uses Backdoor.Pirpi, a remote access Trojan capable of reading, writing, and executing files and programs. Backdoor.Pirpi also collects information about the target's local network, including the domain controller and workstations.

As mentioned previously, Buckeye also uses a number of hacking tools, including the following:

Keylogger: The keylogger is configured using the command line parameters: NetworkService, Replace, Install, Register and Unregister. These parameters install it as a service. The keylogger then records

keystrokes in encrypted files, for example: thumbcache_96.dbx. It also gathers network information such as the MAC address, IP address, WINS, DHCP server, and gateway.

RemoteCMD: This tool executes commands on remote computers, similar to the PsExec tool. Usage is: %s shareIp domain [USER INFORMATION|[USER NAME AND PASSWORD]] [/run:[COMMAND]]

The commands to be passed consist of upload, download, Service (create, delete, start, stop), delete, rename, and AT

PwDumpVariant: This tool imports lsremora.dll (often downloaded by the attacker as part of the toolset) and uses the GetHash export of this DLL. On execution, the tool injects itself into lsass.exe and is triggered with the argument "dig".

OSinfo: OSInfo is a general purpose, system information gathering tool. It has the following command line argument help:

```
info  <Server/Domain> [options]
[options]:
  -d Domain
  -o OsInfo
  -t TsInfo
  -n NetuseInfo
  -s ShareInfo ShareDir
  -c Connect Test
  -a Local And Global Group User Info
  -l Local Group User Info
  -g Global Group User Info
  -ga Group Administrators
  -gp Group Power Users
  -gd Group Domain Admins
  -f <infile> //input server list from infile, OneServerOneLine
info <\\server> <user>
```

ChromePass: A tool from NirSoft used for recovering passwords stored in the Chrome browser.

Lazagne: A compiled Python tool that extracts passwords from various locally installed application classes, such as web browsers. The full list is: chats, svn, wifi, mails, windows, database, sysadmin, and browsers.

Buckeye seems to target file and print servers, which makes it likely the group is looking to steal documents. This, coupled with the group's use of zero-day exploits in the past, customized tools, and the types of organizations being targeted would suggest that Buckeye is a state-sponsored cyberespionage group.

Protection

Symantec, Norton, and Blue Coat products protect against the activities of this cyberespionage group.

Symantec and Norton products offer the following detections:

Antivirus

- Backdoor.Pirpi
- Backdoor.Pirpi!dr
- Backdoor.Pirpi!gen1
- Backdoor.Pirpi!gen2
- Backdoor.Pirpi!gen3

- Backdoor.Pirpi!gen4
- Backdoor.Pirpi.A
- Backdoor.Pirpi.B
- Backdoor.Pirpi.C
- Backdoor.Pirpi.D
- Downloader.Pirpi
- Downloader.Pirpi!g1

Intrusion prevention system

- System Infected: Backdoor.Pirpi Activity 3

Update–September 14, 2016:

Indicators of compromise

We have compiled a list of indicators of compromise for the campaigns described in this blog.

```
Symantec Security Response - Buckeye Indicators of Compromise
==============================================================
Published: Sep 14, 2016

Network IoCs
------------

Domain/URLs

ste.mullanclan.com
[http://]ste.mullanclan.com/v/images/323020339.gif
[http://]ste.mullanclan.com/v/PHH55901496.html
[http://]ste.mullanclan.com/v/images/rec.exe
[http://]ste.mullanclan.com/v/i/Typ24883839.html
[http://]ste.mullanclan.com/v/images/fvp.exe
[http://]ste.mullanclan.com/v/13.js
[http://]ste.mullanclan.com/v/Typ72954330.html

parent.kaapagrains.com
[http://]parent.kaapagrains.com/web/images/eof.exe
[http://]parent.kaapagrains.com/web/images/mms.exe
[http://]parent.kaapagrains.com/web/l/logo.zip
[http://]parent.kaapagrains.com/web/images/calc.exe
[http://]parent.kaapagrains.com/web/i/logo.xap

ptr.holmessupply.com
[http://]ptr.holmessupply.com/http/l/logo.zip
[http://]ptr.holmessupply.com/http/i/logo.zip

lite.ultralitedesigns.com

Host based IoCs
---------------

SHA256

7b1a3c32e7a32b501248e68be2961309b8f461f3f405f6520cd521e08446395e
0dee1dbbbbc86c69e349eb23788174984bfa27c34ee171ea05f86942230bca82
2a5a0bc350e774bd784fc25090518626b65a3ce10c7401f44a1616ea2ae32f4c
f935ee8a25b60d39b6451d62c35e2eec130799837f41a9beba4e264e15d95314
8caa179ec20b6e3938d17132980e0b9fe8ef753a70052f7e857b339427eb0f78
02ea3fce33fa23ff825a6957df99dfe6cabae9281ba3c34e6c596599f5d55352
0867cd1f022baa98902a60dd0dd47e4180dc22420b0a1a537534eb1673d596d2
```

0cb178b26488c7fc52cacf3acddbabe2a5077d606dc23c4917f785a662fd0ba8
0d8d6d388a2d4ba94f3a91ad79e209fbdf1a8e1af86a6ed8d518b53d72a5be4e
18fa855b1f522ed8261980bbec0631e8f9b1e85de15c2cc34521cf0adcaea656
2241248cbb80483d15b764eb4ab149e7a94b38a49c466e58fd7ce9b0b20af4ba
2528c9df3d7ed7c18d790d690ebb4bcacf25292fd4e7d3c73ba42d3d3cba20a2
2febab3f0d1e3df0ee64b52ac1e0154305ff3f6aeada4a79a8f10ef5e84f5dac
313ad88b6a8e6c1e53a355a12ad18a19c5d04abc021549b4a451aee7cec024b9
389f0c0f19095baa8f9ad6a8642a939d09b3c943ebdcade11dda04c06cf0dd66
3c7c30ff0bb6eb04819d121e51a36dadecc6af747718e2373489bde18cbce001
3c8dfd965f4e583ec971b5953edfb2a4bda029425599c35e103dc364fdb57b9c
3ca85ff1cbca6672fcdcb483fccb977bc787affaecfb9983ee3b0c5e7fdef0d2
3dc4f9d2083667acf1e83dfd8f1535c068c51f0a5b9f5db808a4c0227d0d9d7a
3f040f17ea9f87b48558f79121165c12e06c5f1707ee8f7492cd99886b459378
4436c961470f4a552bc819976a934aba24de853fa91b8d9fc8c0009665f7aadb
4ca207f0c1b6fd5dc7f25e54f83d2b63cda4d909661fe8378cfae2ea7c55b289
4d353eff55d4b51540215af44063aa5ef2e4d2cd6764eb124291e6beb0303550
6510bd08678f5c63a962bf1f68b8c34c648ac53fbea25392c61d6d576923ac41
65ea6ec4ff174c62992f6304ebf1356fad6497fb48db90d2c6af5654d49f08f3
669fe38efa1bc5a3b0aa0b4637434371d2309875015112068eb58ec4b8eb2e64
6c39d97e44cef085eae55e89ea966ce47251b96d2b842021685ef347425d2326
707ddb9b4c5bf3a2a7a2c04cb41ebbfb631e0ac6005dbfe586825e0ea86f40bf
75c366e900351f64681f9dffc379f2c7f2d4c7a83ab37d94ea9e61bb8696f86a
79db4a9260d6cfe7b704f4e665a98c9f4ebc5da648926cdd589190ae089c229e
847a5fcc43979cb7bcbac38838ca2d0e219ba55262aea7100dffc4e433d69e7a
8f6c8467d38ff5ee3f3d962efb065099358693910dee6eaf8d9a9db56163e16c
8fd99e69ab51c12a99a6bdd59192807d9b082e25a25d511f8c2296f93b0f8b79
93a05f94a649f56a46a94cc3230003757e9e08905c78080ee56b4f920a40d8c2
984f88df411ff2ee8f6d75a45c0d86b7a17622db5312970f7cdde42fc18517d5
9e5a482663a5d238c41d2a2284239a7c217c568a3dbfd417e71e12a80db2ea0a
a624844a5f8a18200ec248814b9e19fc57f2b0e31ca002f3293be72c1c7a5479
a6a548e551c51535faca671f15c3a828d7fc9ce98befddb7c22c378d2bba7ada
aafb980a962a96e4c383502788fe960f1e185b9351d91300a72eb03859e4d902
adb2e638d4e53b8bafbded625aaff8e70cc391f30c3a6f469c39b794c7822cbb
b30c159531295f7d4594e3620f7ad13537656ca45e4fd617dce5266bac5e14f3
b501a2aa82219c485813a8e50dae14046f22ed7f36a06b5fe6f5b9778d569072
b70151afffe4ad4289c436306ca868b9d839dc9b5d49104ed20fb95465a8068b
bd979176dc3e2f094f226889c8b7e520feb1d5f2869a360354baad679f10b7b7
c4097125684bd24aa5b7afa63301d554abf09e33b952ec358a369b3b2ba21556
c432d07480c0881fd60b786500b119c8fb6848e7909863a1fc20a6652cd4c8b8
c59815e52eb12f6e9286235e2ed4b9650bdc3a4eaf7bc78221bd69ee95a2b1f9
d3bbe6999af3d3129f0a2520b26e04bdfa1bf1b19e99f2fb6d5397e4a33cba4a
d42fe1956351a858b9d69660da4d54ae1ccffab9af93014cc69bbeef2767b105
d4cc2031f70de07060f84569a2eb2d43b5063da01c8406bf59a17767752da0c8
db32548e62eea0dbd2033d9fe9d4b826a6adf9ad92533d12b430fd0918bcd6d3
db3cd325b38fabd205bb8eb0a143df3e8e244b6265369230097946b4127b57a2
ddfbf0c97aa640d3bc28f8dcf40ae16835e27a376d2bf0c4319ab15feac84dc4
e11849d7e36a9d96aa2a643b54d270d84dccf0d299013a6308861df835ecaca0
e238ce16838f07f5d28fe7261437f340c3dddbc4d1c5b0dfebec6b3458602df7
e2fb0a6ed6fe0ee946bec6eadc1e71f0d3564a8a00e97ec6542e91e642b5b5e3
ea37ef8479c0586e2e60031a97eeba355d13d4682d9bdd8c19cc8a2fd8ef784f
eab49dfbdd419adfbc4e987c5704c1f58ffa19780915cb63058f2d4b8d0222bc
f06307d3e03e4533257b7d98dcc2d04548299bbe01aa5a01d9c0389899c761e0
faf2c76bd553223dc6d84917ed02b7abf5a88b79a267d5494fd04521e5e6ea4f
fba36a40d7e038e493385a5efea1f416d86d9c0804f1961f1b4c28baf0eace28