Buckeye cyberespionage group shifts gaze from US to Hong Kong

By By

Published: 2016-09-06 · Archived: 2026-04-29 07:25:17 UTC

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).

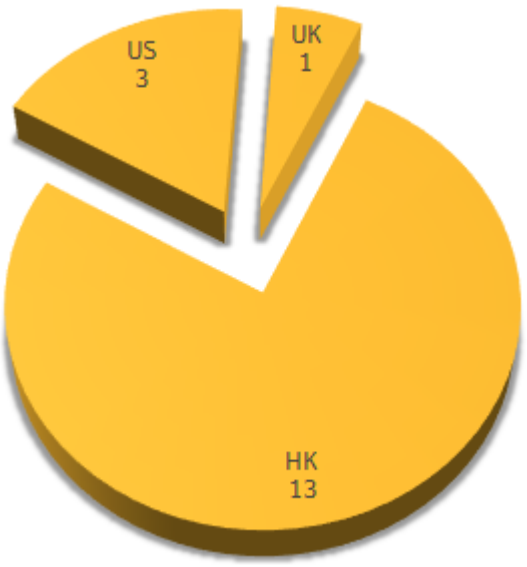

Figure 1. Buckeye victims of interest by region (2015 to date)

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.

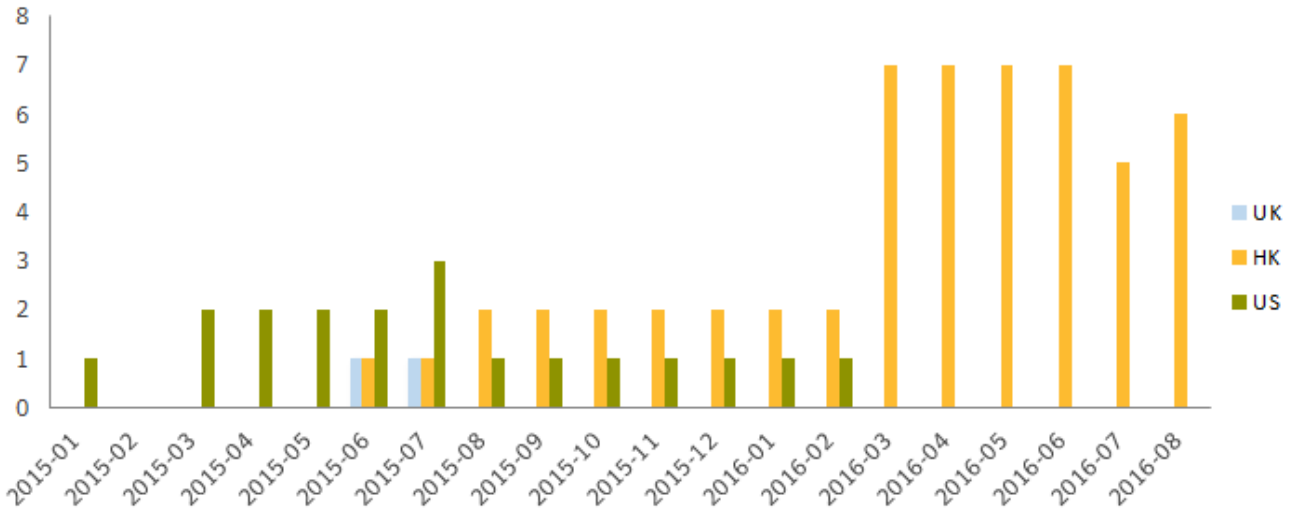

Figure 2. Organizations that Buckeye targeted over time, per region

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.
