Recent Watering Hole Attacks Attributed to APT Group “th3bug” Using Poison Ivy

researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/

Jen Miller-Osborn, Ryan Olson September 19, 2014

By Jen Miller-Osborn and Ryan Olson

September 19, 2014 at 3:30 PM

Category: Cybersecurity, Malware, Unit 42

Tags: Poison Ivy, Remote Administration Tool, th3bug, WildFire

We’ve uncovered some new data and likely attribution regarding a series of APT watering hole attacks this past summer. Watering hole attacks are an increasingly popular component of APT campaigns, as many people are more aware of spear phishing and are less likely to open documents or click on links in unsolicited emails. Watering hole attacks offer a much better chance of success because they involve compromising legitimate websites and installing malware intended to compromise website visitors. These are often popular websites frequented by people who work in specific industries or have political sympathies to which the actors want to gain access.

The attacks discussed in this blog are related to an APT campaign commonly referred to as “th3bug”, named for the password the actors often use with their Poison Ivy malware. Of note, only the older of the samples we cover in this blog used that password. We don’t know the reason the actors changed this, but it could possibly be in reaction to information widely published on the Internet about their activities, which use that password as a key component to tie the activity together. FireEye in particular published a paper describing several APT campaigns whose activity they correlate using Poison Ivy passwords.

In contrast to many other APT campaigns, which tend to rely heavily on spear phishing to gain victims, “th3bug” is known for compromising legitimate websites their intended visitors are likely to frequent. Over the summer they compromised several sites, including a well-known Uyghur website written in that native language.

While we were unable to recover the initial vulnerability used, it is possibly the same CVE 2014-0515 Adobe Flash exploit first reported by Cisco TRAC in late July. We cannot confirm the initial compromised sites, but we noted traffic to several known re-direct sites and the malware was configured to use the same command and control (C2) server.

In addition, the download dates of many of our files pre-date those noted by Cisco by only a few days. All of the malware were variants of the Poison Ivy Remote Administration Tool (RAT) and were properly identified as such by our WildFire platform. The targets of the attack were:

- Uyghur sympathizers
- An East Asian office for a major US based computer manufacturer
- A major US university
- An international wholesale and retail telecom provider

We saw the first sample on July 14, 2014. This sample had an interesting PDB string - C:\Users\sophie\documents\visual studio 2010\Projects\init\Release\init.pdb with a time date string that exactly matched the PE timestamp of 11 July, 2014.

Table 1

SHA256	ba509a1d752f3165dc2821e0b1c6543c15988fd7abd4e56c6155de09d1640ce9
MD5	18ad696f3459bf47f97734f2f14506e3
File Name	diff.exe
File Size	97280
First Seen	2014-07-14 13:55:36
Download URL	www.npec.com .tw/flash/diff.exe
Resolution	203.69.42.22
C2 Domain	diff.qohub.info
Resolution	115.23.172.151

The next day we collected several copies of the same malware intended for the same industry. They were downloaded from one of the download URLs in the below table, but all had the same MD5 and C2 domain.

Table 2

SHA256	9d149baceaaff2a67161fec9b8978abc22f0a73a1c8ce87edf6e2fb673ac7374
MD5	1ea41812a0114e5c6ae76330e7b4af69
File Name	diff.exe

File Size	126976
First Seen	2014-07-15 18:22:25
Download URLs	www.aanon.com .tw/flash/diff.exewww.npec.com .tw/flash/diff.exeuyghurweb .net/player/gmuweb.exe
Resolution	203.69.42.22
C2 Domain	diff.qohub.info
Resolution	115.23.172.151

On July 16 WildFire picked up a malicious executable hosted on uyghurweb.net, a legitimate Uyghur website that was compromised to infect users. The file was named “PYvBte.jar” but was actually a Windows executable. The file has the characteristics listed in Table 3, and appears to be a stand-alone executable version of the Metasploit Meterpreter shell. When this file runs, it downloads a payload from uyghurweb.net/player/gmuweb.exe and executes it. This file is the same Poison Ivy RAT described in Table 2.

The Meterpreter payload masquerades as a copy of the ApacheBench tool made by the Apache Software Foundation.

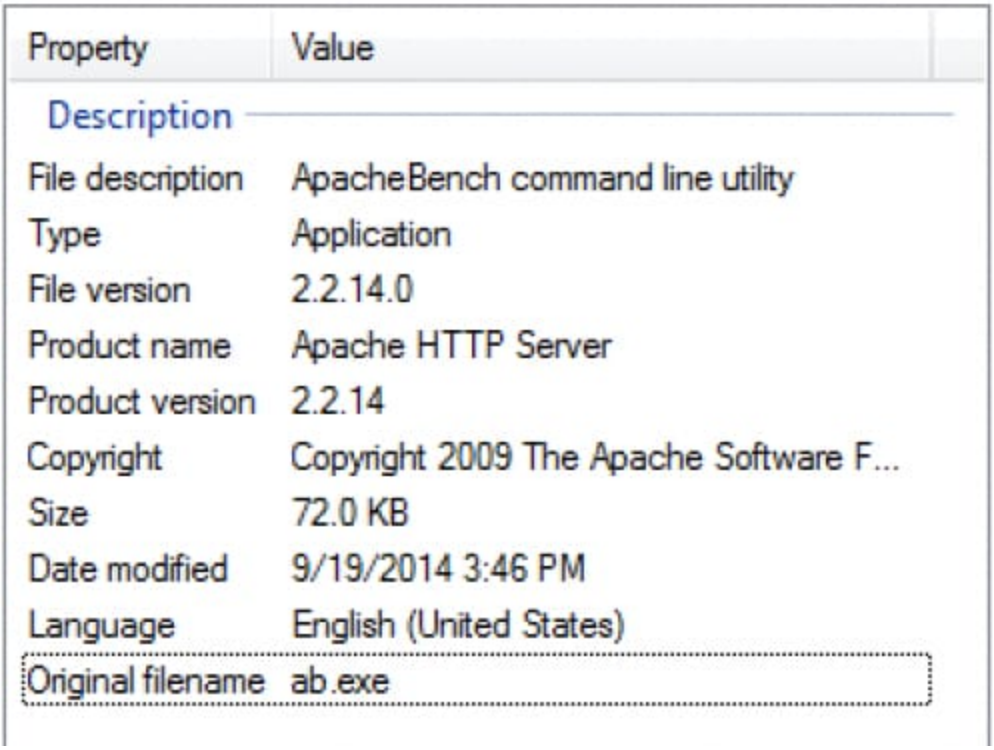

Table 3

SHA256	ccfe61a28f35161c19340541dfd839075e31cd3b661f0936a4c667d805a65136

MD5	7b0cb4d14d3d8b6ccc7453f7ddb33997
File Name	PYvBte.jar
File Size	73802
First Seen	2014-07-16 01:42:24
Download URL	uyghurweb .net/player/PYvBte.jar

On 21 July, we detected another sample that was noted in the Cisco TRAC blog. The initial download URL and IP resolution were different than the previous samples, but the C2 domain and resolution matched. This file is also a Poison Ivy variant.

Table 4

SHA256	7f39e5b9d46386dd8142ef40ae526343274bdd5f27e38c07b457d290a277e807
MD5	efad656db0f9cc92b1e15dc9c540e407
File Name	setup.exe
File Size	126976
First Seen	2014-07-21 05:09:56
Download URL	www.ep66.com .tw/setup.exe
Resolution	203.69.42.23
C2 Domain	app.qohub.info
Resolution	115.23.172.151

Based on historical IP resolution overlaps between the above C2 domains and other domains that have also resolved to the same IPs, we found an additional sample from the beginning of this year.

Interestingly, the first sample was not logged in VirusTotal prior to our submission, despite the sample having been in use in the wild for at least seven months. In addition, it is the only sample tied to this activity we found that used the Poison Ivy password “th3bug”. AVAST wrote a blog related to the activity we describe here and tied a file with the same name, but the sample we found doesn’t match any other details of the file they documented.

Also of note, the IP resolution for this C2 domain was changed to match the IP resolution of the C2 domains used in the July activity only a few days after these samples were seen. Additionally, the files PE timestamp was January 21, the day before we detected the sample. Targeted industries for this series are listed below.

- Another international wholesale and retail telecom provider
- A major visual computing company headquartered in the US
- A state-owned East Asian financial services company

Table 5

SHA256	e3d02e5f69d3c2092657d64c39aa0aea2a16ce804a47f3b5cf44774cde3166fe
MD5	0cabd6aec2555e64bdf39320f338e027
File Name	AppletLow.jar
File Size	53248
First Seen	2014-01-22 18:47:03
Download URL	140.112.158 .132/phpmyadmin/test/AppletLow.jar
C2 Domain	2014year.qpoe .com
Resolution	192.168.1.3

Watering hole attacks will continue to be popular with APT campaigns, as they are much harder to defend against then spear phishing attacks. There is no way for people browsing to these websites to know in advance the normally trusted website has been compromised and will serve them malware when they visit it.

Ensuring web browsers and operating system software is fully patched and up-to-date is the best way to defend against this type of threat. However, to increase success rates APT campaigns can use zero-day exploits, so even a properly patched system would be compromised. Palo Alto Networks users should use our firewall's ability to block executable downloads unless the user specifically authorizes it. If you want to allow executables through but prefer that they be analyzed for malicious activity, use our WildFire platform, which correctly identified all of the files listed in this blog as malware and provides users with a full report on the samples host and network-based activities.

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.