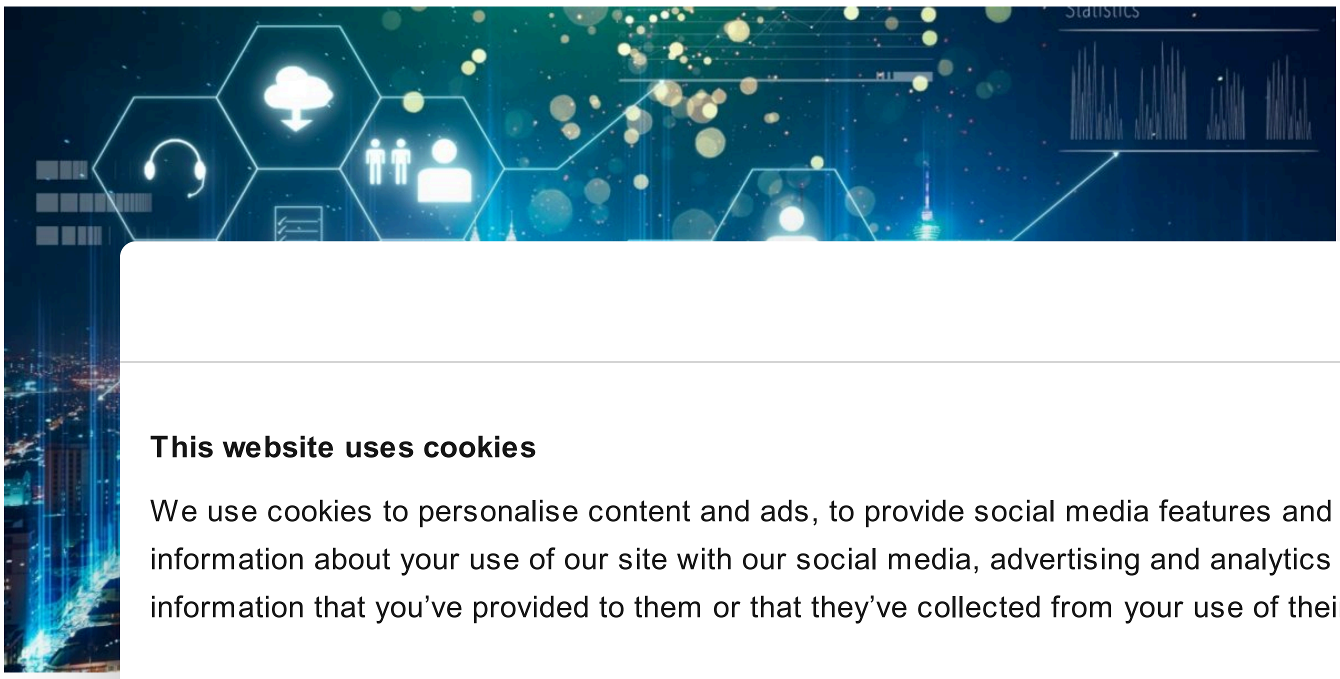
FIN7.5: the infamous cybercrime rig “FIN7” continues its activities

APT REPORTS 08 MAY 2019 10 minute read



KSB WEBINARS

02 FEB 2021, 12:00PM

2021 predictions, episode 1: financial cyberthreats

Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
●	○	○	○

Show details ›

Use necessary cookies only | Allow all cookies

// AU

YUR

On Augu
individua
numerou
2015. Int
penteste
goal beh
cards, or get access to financial data or computers of finance department employees in order to conduct wire transfers to offshore accounts.

In 2018-2019, researchers of Kaspersky Lab’s Global Research and Analysis Team analyzed various campaigns that used the same Tactics Tools and Procedures (TTPs) as the historic FIN7, leading the researchers to believe that this threat actor had remained active despite the 2018 arrests. In addition, during the investigation, we discovered certain similarities to other attacker groups that seemed to share or copy the FIN7 TTPs in their own operations.

Recent FIN7 campaigns

The FIN7 intrusion set continued its tailored spear phishing campaigns throughout last year. Kaspersky Lab has been able to retrieve some of these exchanges from a FIN7 target. The spear phishing campaigns were remarkably sophisticated from a social engineering perspective. In various cases, the operators exchanged numerous messages with their victims for weeks before sending their malicious documents. The emails were efficient social-engineering attempts that appealed to a vast number of human emotions (fear, stress, anger, etc.) to elicit a response from their victims. One of the domains used by the attackers in their 2018 campaign of spear phishing contained more than 130 email aliases, leading us to think that more than 130 companies had been targeted by the end of 2018.

Malicious Documents

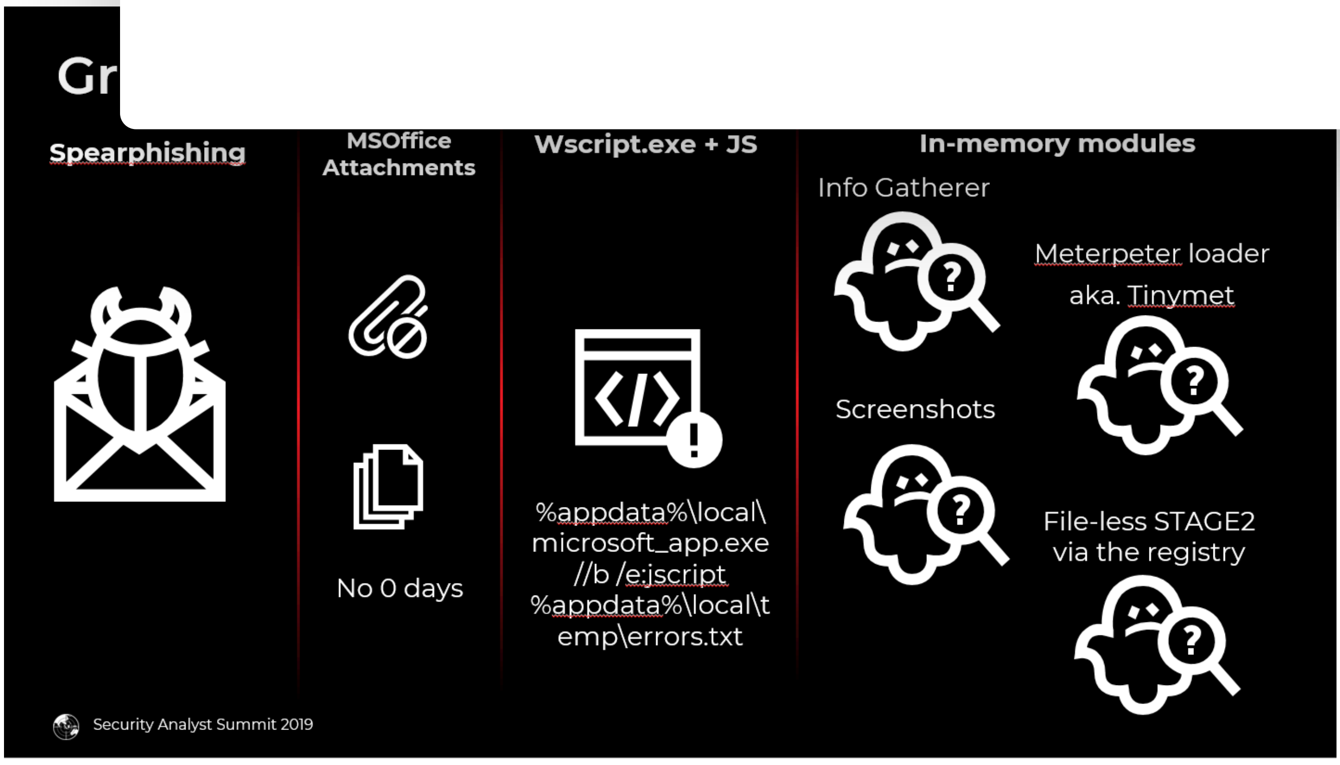
We have seen two types of documents sent to victims in these spear phishing campaigns. The first one exploits the INCLUDEPICTURE feature of Microsoft Word to get context information about the victim’s computer, and the availability and version number of Microsoft Word. The second one, which in many cases is an Office document protected with a trivial password, such as “12345”, “1234”, etc., uses macros to execute a GRIFFON implant on the target’s computer. In various cases, the associated macro also scheduled tasks to make GRIFFON persistent.

Interestingly, following some open-source publications about them, the FIN7 operators seems to have developed a homemade builder of malicious Office document using ideas from ThreadKit, which they employed during the summer of 2018. The new builder inserts random values in the Author and Company metadata fields. Moreover, the builder allows these to modify different IOCs, such as the filenames of wscript.exe or sctasks.exe copies, etc.

wscript.exe copy	sctasks copy	Task name	C2
byzNne10.exe	byzNne17.exe	TaskbyzNne	logitech-cdn.com
c9FGG10.exe	c9FGG17.exe	Taskc9FGG	logitech-cdn.com
zEsb10.exe	zEsb17.exe	TaskzEsb	servicebing-cdn.com

Author
mogjxjtvt
soxvremv
gareljtjhv

GRIFF


Gr
Spearphishing
MSOffice Attachments
No 0 days
Wscript.exe + JS
%appdata%\local\microsoft_app.exe //b /e:jscript %appdata%\local\temp\errors.txt
In-memory modules
Info Gatherer
Meterpeter loader aka. Tinymet
Screenshots
File-less STAGE2 via the registry
Security Analyst Summit 2019

Griffon Malware attack pattern

The GRIFFON implant is a lightweight JScript validator-style implant without any persistence mechanism. The malware is designed for receiving modules to be executed in-memory and sending the results to C2s. We were able to obtain four different modules during the investigation.

Reconnaissance module

The first module downloaded by the GRIFFON malware to the victim’s computer is an information-gathering JScript, which allows the cybercriminals to understand the context of the infected workstation. This module mainly relies on WMI and Windows objects to deliver results, which will be sent back to the operators. Interestingly, more than 20 artifacts are retrieved from the system by this implant during the reconnaissance stage, from the date and time of operating system installation and membership in a Windows domain to a list of and the resolutions of the workstation’s monitors.

Meterpreter downloader

The second module is used by the operators to execute an obfuscated PowerShell script, which contains a Meterpreter downloader widely known as “*Tinymet*“. This downloader, seen in past FIN7 campaigns, downloads a one-byte XOR-encrypted (eg. with the key equal to 0x50 or 0x51) piece of meterpreter shellcode to execute.

Screenshot module

The third module allows the operators to take a screenshot of the remote system. To do that, it also drops a PowerShell script on the workstation to execute. The script executes an open-source .I
“%TMP%

Persist

The last
attacker
another
PowerLi
GRIFFON
before e

Through
Even tho
operator
workstat

On tl

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
●	●	●	●

Show details ›

Attackers make mistakes, and FIN7 are no exception. The major error made by its operators allowed us to follow the command and control server of the GRIFFON implant last year. In order to trick blue teams and other DFIR analysts, the operators created fake HTTP 302 redirection to various Google services on their C2s servers.

```
HTTP/1.1 302 Found
Server: nginx
Date: [retracted]
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Location: https://cloud.google.com/cdn/
```

Returned headers for most of the GRIFFON C2s servers on port 443

This error allowed us to follow the infrastructure week by week, until an individual pushed on Twitter the heuristic to track their C2 at the end of December 2018. A few days after the tweet, in January 2019, the operators changed their landing page in order to prevent this type of tracking against their infrastructure.

Fake pentest company

FROM THE SAME AUTHORS

Cybersecurity of connected healthcare 2020: Overview and predictions

cial
rview

cial
view

ncial
hat to

ulletin
er
te

During the investigation related to the GRIFFON infrastructure, we found a strange overlap between the WHOIS record of an old GRIFFON C2 and the website of a fake company.

According to the website, that domain supposedly belongs to a legitimate security company “fully owned by the Russian Government” (sic.) and having offices in “Moscow, Saint Petersburg and Yekaterinburg”, but the address says the company is located in Trump Tower, in New York. Given FIN7’s previous use of false security companies, we decided to look deeper into this one.

As we were looking at the content of the website, it became evident that almost all of the text used was lifted from legitimate security-company websites. Phrases and sentences were borrowed from at least the following companies/sites:

- DKSec – www.dksec.com
- OKIOK – www.okiok.com/services/tailored-solutions
- MainNerve – www.mainnerve.com
- Datics – www.datatics.com/cyber-security
- Perspective Risk – www.perspectiverisk.com
- Synack – https://www.synack.com/company
- FireEye – https://www.fireeye.com/services/penetration-testing.html

This com
translato
advertis

In additio
that som
business

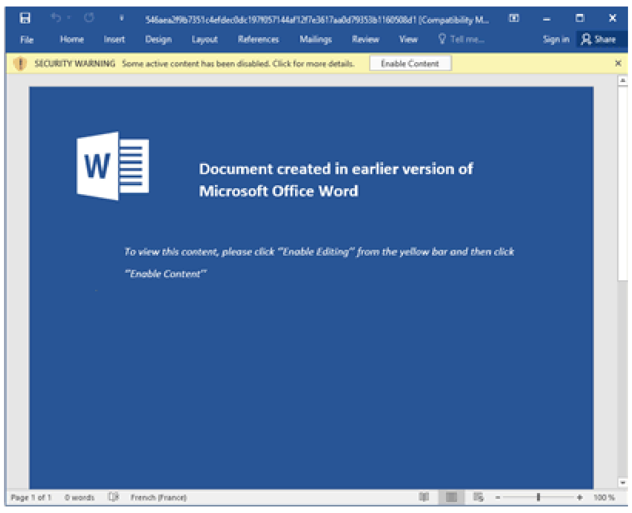
Links

While tra
beginnin
the FIN7
decided

Cobalt

In his his
This activity cluster, which Kaspersky Lab has followed for a few years, uses various implants for targeting mainly banks, and developers of banking and money processing software solutions. At the end of 2018, the cluster started to use not only CobaltStrike but also Powershell Empire in order to gain a foothold on the victims’ networks. After a successful penetration, it uses its own backdoors and the CobaltStrike framework or Powershell Empire components to hop to interesting parts of the network, where it can monetize its access.

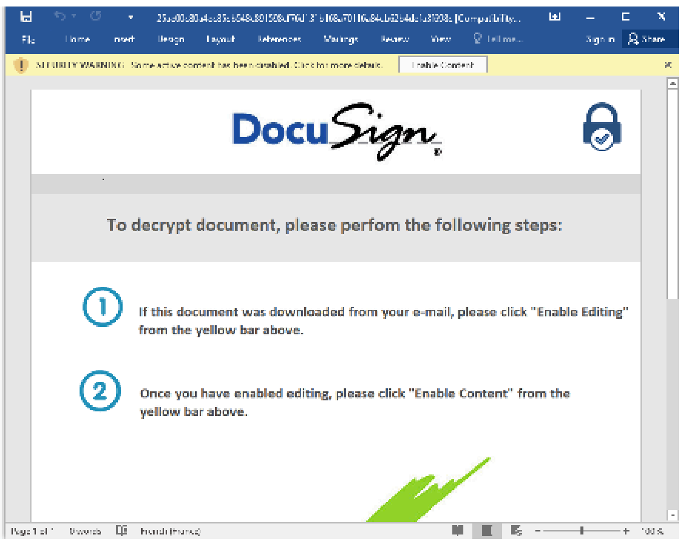
FIN7’s last campaigns were targeting banks in Europe and Central America. This threat actor stole suspected of stealing €13 million from Bank of Valetta, Malta earlier this year.



SECURITY WARNING Some active content has been disabled. Click for more details.

Document created in earlier version of Microsoft Office Word

To view this content, please click “Enable Editing” from the yellow bar and then click “Enable Content”



SECURITY WARNING Some active content has been disabled. Click for more details.

To decrypt document, please perfom the following steps:

1. If this document was downloaded from your e-mail, please click "Enable Editing" from the yellow bar above.
2. Once you have enabled editing, please click "Enable Content" from the yellow bar above.

Example of malicious documents used in the end of 2018 to beginning of 2019

A few interesting overlaps in recent FIN7 campaigns:

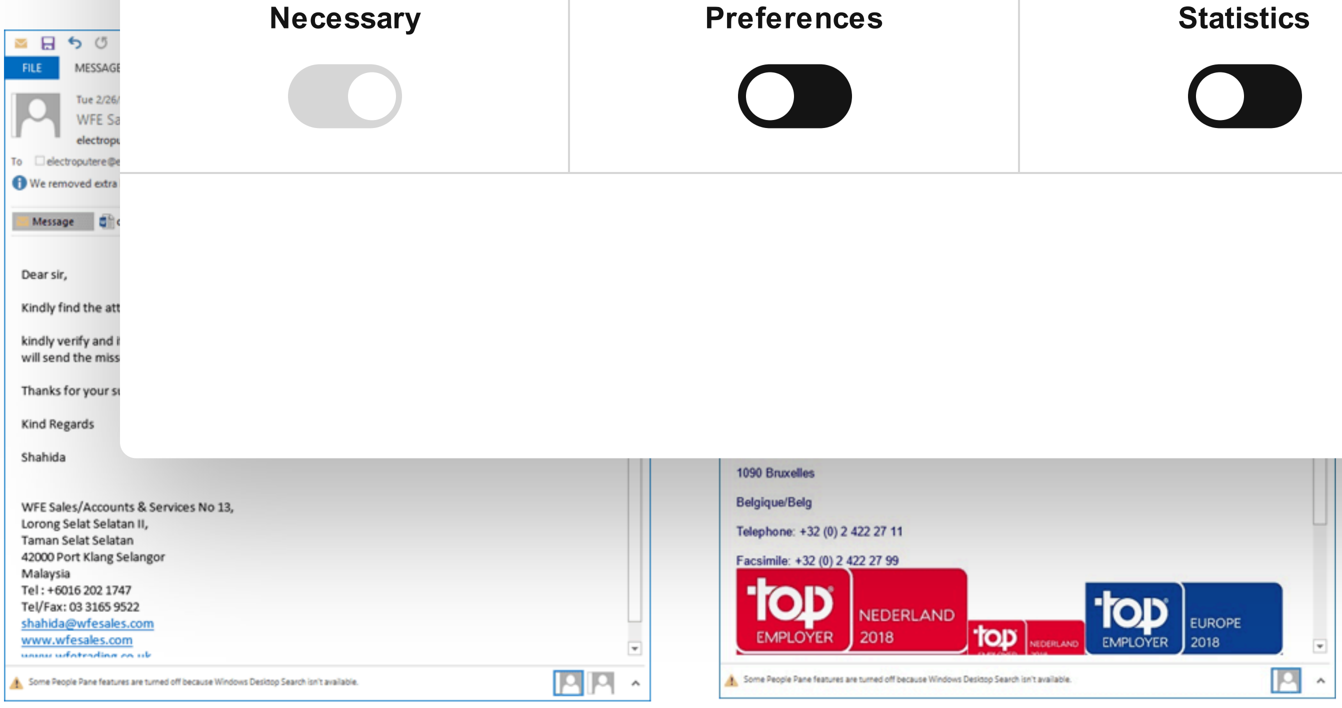
- Both used macros to copy wscript.exe to another file, which began with “ms” (mses.exe – FIN7, msutil.exe – EmpireMonkey).
- Both executed a JScript file named “error” in %TEMP% (Errors.txt in the case of FIN7, Errors.bat for EmpireMonkey).
- Both used DocuSign decoy documents with different macros. The macros popped the same “Document decryption error” error message—even if macro code remain totally different.

We have a high level of confidence in a historic association between FIN7 and Cobalt, even though we believe that these two clusters of activity are operated by different teams.

AveMaria

AveMaria is a new botnet, whose first version we found in September 2018, right after the arrests of the FIN7 members. We have medium confidence that this botnet falls under the FIN7 umbrella
various t
keylogge
extracte

To delive
attachm
CVE-201
passwor
ask targ


FILE MESSAGE

Tue 2/26/
WFE Sa
electropu
To electroputere@e
We removed extra

Message

Dear sir,

Kindly find the att

kindly verify and i
will send the miss

Thanks for your s

Kind Regards

Shahida

WFE Sales/Accounts & Services No 13,
Lorong Selat Selatan II,
Taman Selat Selatan
42000 Port Klang Selangor
Malaysia
Tel : +6016 202 1747
Tel/Fax: 03 3165 9522
shahida@wfesales.com
www.wfesales.com

Some People Pane features are turned off because Windows Desktop Search isn't available.

1090 Bruxelles

Belgique/Belg

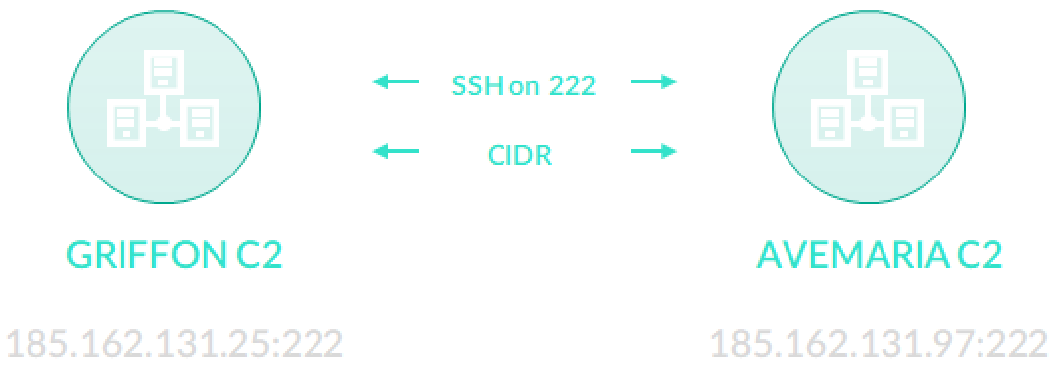
Telephone: +32 (0) 2 422 27 11

Facsimile: +32 (0) 2 422 27 99

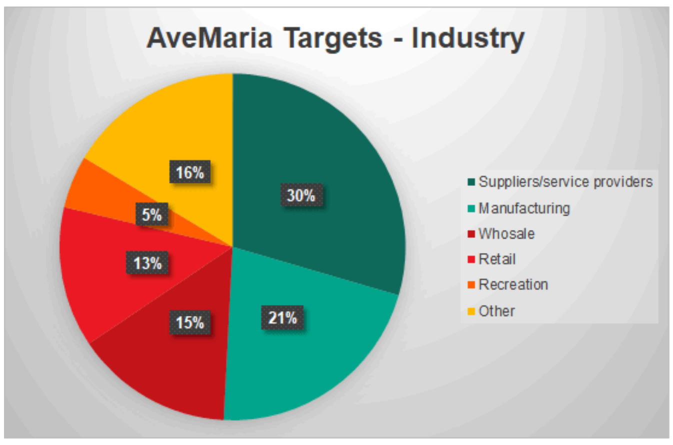
Some People Pane features are turned off because Windows Desktop Search isn't available.

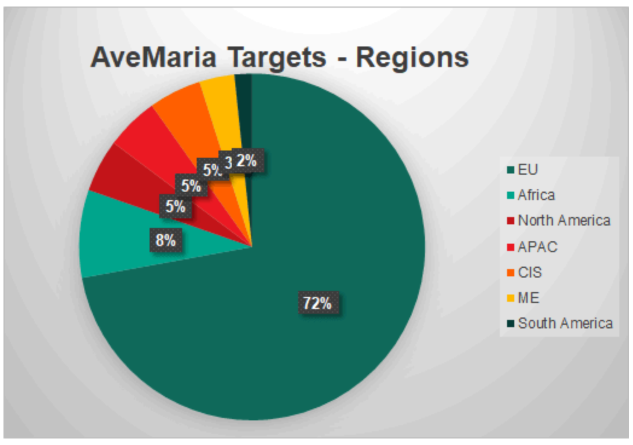
Example of AveMaria spearphing emails. Criminals suggest calling them.

During the investigation into FIN7, our threat-hunting systems found an interesting overlap in between the infrastructure of FIN7 and AveMaria. Basically, two servers in the same IP range and AS14576 (autonomous system) share a non-standard SSH port, which is 222. One of the servers is a Griffon C2, and the other one, an AveMaria C2.



Distribution of targets is another factor suggesting that these two malware families may be connected. We analyzed AveMaria targets during February and March of 2019. The spearphishing emails were sent to various kinds of businesses only and did not target individuals. Thirty percent of the targets were small and medium-sized companies that were suppliers or service providers for bigger players and 21% were various types of manufacturing companies. We also spotted several typical FIN7 targets, such as retailers and hotels. Most AveMaria targets (72%) were in the EU.





CopyPaste

At the er

of activi

this acto

think tha

This set

docume

avoid de

Here are

- Both
NoP
argur
- Both
Coba
Digit
decc
redir
serve
- Quite recently, FIN7 threat actors typosquatted the brand “Digicert” using the domain name digicert-cdn[.]com, which is used as a command and control server for their GRIFFON implants. CopyPaste, in turn, also typosquatted this brand with their domains digicertweb[.]com and digi-cert[.]org, both used as a Powershell Empire C2 with decoy HTTP 302 redirects to the legitimate Digicert website.

The links between CopyPaste and FIN7 are still very weak. It is possible that the CopyPaste operators were influenced by open-source publications and do not have any ties with FIN7.

Conclusions

During 2018, Europol and DoJ announced the arrest of the leader of the FIN7 and Carbanak/CobaltGoblin cybercrime groups. It was believed that the arrest of the group leader will have an impact on the group’s operations. However, recent data seems to indicate that the attacks have continued without significant drawbacks. One may say CobaltGoblin and FIN7 have even extended the number of groups operating under their umbrella. We observe, with various level of confidence, that there are several interconnected groups using very similar toolkits and the same infrastructure to conduct their cyberattacks.

The first of them is the well-known FIN7, which specializes in attacking various companies to get access to financial data or PoS infrastructure. They rely on a Griffon JS backdoor and Cobalt/Meterpreter, and in recent attacks, Powershell Empire. The second one is CobaltGoblin/Carbanak/EmpireMonkey, which uses the same toolkit, techniques and similar infrastructure but targets only financial institutions and associated software/services providers.

We link the AveMaria botnet to these two groups with medium confidence: AveMaria's targets are mostly suppliers for big companies, and the way AveMaria manages its infrastructure is very similar to FIN7. The last piece is the newly discovered CopyPaste group, who targeted financial entities and companies in one African country, which lead us to think that CopyPaste was associated with cybermercenaries or a training center. The links between CopyPaste and FIN7 are still very weak. It is possible that the operators of this cluster of activity were influenced by open-source publications and do not have any ties with FIN7.

All of the aforementioned groups greatly benefit from unpatched systems in corporate environments. They thus continue to use effective spearphishing campaigns in conjunction with well-known MS Office exploits generated by the framework. So far, the groups have not used any zero-days.

FIN7/Cobalt phishing documents may seem basic, but when combined with their extensive social engineering and focused targeting, they are quite successful. As with their previous fake compan

use in ei

More inf

Intelligen

Indic

AveMa

- 185.6
- tain.w
- norep
- 185.16
- 91.192
- serve
- doddyfire.dyndns[.]org
- 212.8.240.116
- 168.167.45.162
- toekie.ddns[.]net
- warmaha.warzonedns[.]com

CopyPaste

- digi-cert[.]org
- somtelnetworks[.]com
- geotrusts[.]com
- secureclientupdate[.]com
- digicertweb[.]com
- sport-pesa[.]org
- itaxkenya[.]com
- businessdailyafrica[.]net

IN THE SAME CATEGORY

Beyond the Surface: the evolution and expansion of
roup

n Latin

ew
s on
ions in

2024

w APT

- infotrak-research[.]com
- nairobiwired[.]com
- k-24tv[.]com

FIN7/GRIFFON

- hpservice-cdn[.]com
- realtek-cdn[.]com
- logitech-cdn[.]com
- pci-cdn[.]com
- appleservice-cdn[.]com
- servicebing-cdn[.]com
- cisco-cdn[.]com
- facebook77-cdn[.]com
- yahooservices-cdn[.]com
- globaltech-cdn[.]com
- infos
- goog
- insta
- mse-
- akam
- book
- live-
- clou
- cdnj-
- bing-
- servi
- cdn-
- cdn-
- goog
- mse-cdn[.]com
- tw32-cdn[.]com
- gmail-cdn3[.]com
- digicert-cdn[.]com
- vmware-cdn[.]com
- exchange-cdn[.]com
- cdn-skype[.]com
- windowsupdatemicrosoft[.]com
- msdn-cdn[.]com
- testing-cdn[.]com
- msdn-update[.]com

EmpireMonkey/CobaltGoblin

In order to preserve the privacy of the potential victims, we stripped the targeted entities from the domain names.

- (entity)-corporate[.]com
- (entity)-cert[.]com
- (entity)-no[.]org
- (entity)-fr[.]org
- (entity)-acquisition[.]org
- (entity)-trust[.]org
- riscomponents[.]pw
- nlscdn[.]com

APT FINANCIAL MALWARE MALWARE DESCRIPTIONS POWERSHELL SOCIAL ENGINEERING SPEAR PHISHING

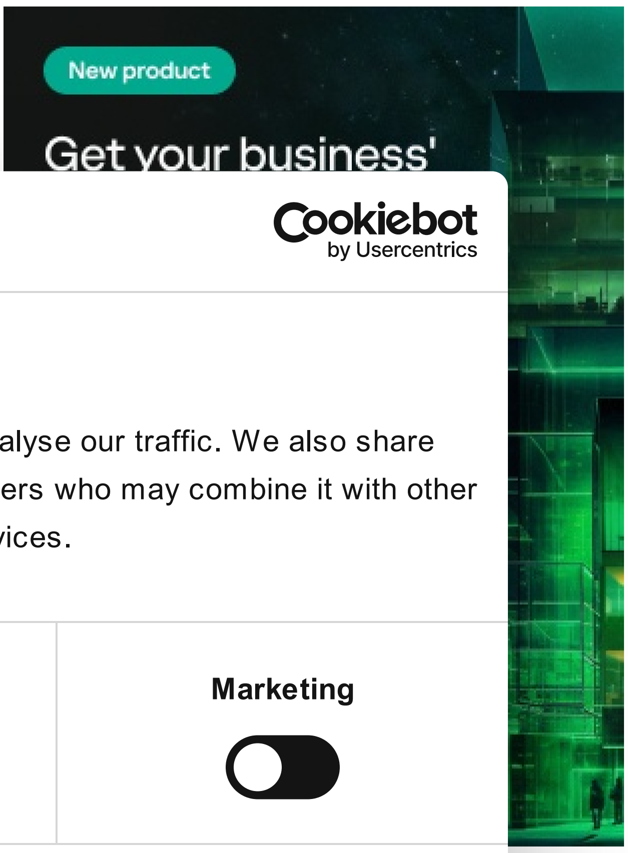
FIN7.5: the infamous cybercrime rig "FIN7" continues its activities

Your email address will not be published. Required fields are marked *

Type y

Name *

Com



Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
●	○	○	○

Show details >

// LA

SAS

The Crypto Game of Lazarus APT: Investors vs. Zero-days

BORIS LARIN, VASILY BERDNIKOV

MALWARE DESCRIPTIONS

Grandoreiro, the global trojan with grandiose goals

GREAT

CRIMEWARE REPORTS

Stealer here, stealer there, stealers everywhere!

GREAT

CRIMEWARE REPORTS

Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia

KASPERSKY

// LATEST WEBINARS

THREAT INTELLIGENCE AND IR

04 SEP 2024, 5:00PM 60 MIN

Inside the Dark Web: exploring the human side of cybercriminals

ANNA PAVLOVSKAYA

TECHNOLOGIES AND SERVICES

13 AUG 2024, 5:00PM 60 MIN

The Cybersecurity Buyer’s Dilemma: Hype vs (True) Expertise

OLEG GOROBETS, ALEXANDER LISKIN

CYBERTHREAT TALKS

16 JUL 2024, 5:00PM 60 MIN

Cybersecurity’s human factor – more than an unpatched vulnerability

OLEG GOROBETS

TRAININGS AND WORKSHOPS

09 JUL 2024, 4:00PM 60 MIN

Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

// REPORTS

Beyond the Surface: the evolution and expansion of the SideWinder APT group

Kaspersky analyzes SideWinder APT’s recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

BlindEagle flying high in Latin America

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Kaspersky has identified a new EastWind campaig using Cl APT27 t

APT trends report Q2 2024

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility

// SU MAILS

The hott

cribe

Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary	Preferences	Statistics	Marketing

Show details ›

kaspersky

THREATS

- APT (Targeted attacks)
- Secure environment (IoT)
- Mobile threats
- Financial threats
- Spam and phishing
- Industrial threats
- Web threats
- Vulnerabilities and exploits
- All threats

CATEGORIES

- APT reports
- Malware descriptions
- Security Bulletin
- Malware reports
- Spam and phishing reports
- Security technologies
- Research
- Publications
- All categories

OTHER SECTIONS

- Archive
- All tags
- Webinars
- APT Logbook
- Statistics
- Encyclopedia
- Threats descriptions
- KSB 2023

Privacy Policy | License Agreement | Cookies