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

SL securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703

By Yury Namestnikov , Félix Aime on May 8, 2019. 10:00 am

On August 1, 2018, the US Department of Justice announced that it had arrested several individuals suspected of having ties to the FIN7 cybercrime rig. FIN7 operations are linked to numerous intrusion attempts having targeted hundreds of companies since at least as early as 2015. Interestingly, this threat actor created fake companies in order to hire remote pentesters, developers and interpreters to participate in their malicious business. The main goal behind its malicious activities was to steal financial assets from companies, such as debit 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.

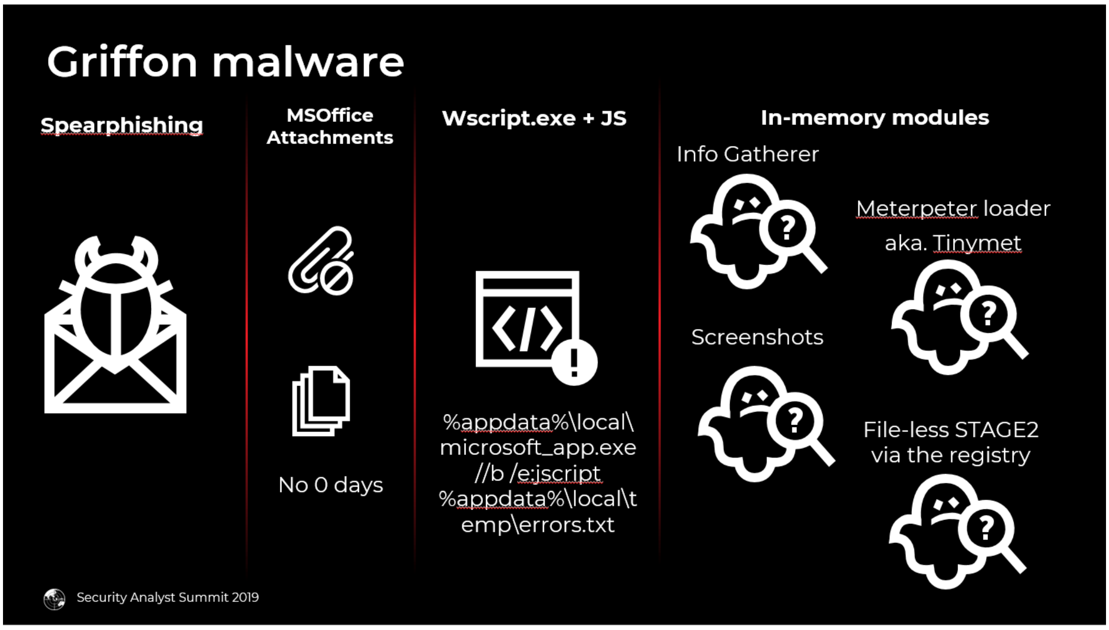
wscript.exe copy	sctasks copy	Task name	C2
byzNne10.exe	byzNne17.exe	TaskbyzNne	logitech-cdn.com
c9FGG10.exe	c9FGG17.exe	Taskc9FGG	logitech-cdn.com
zEsb10.exe	zEsb17.exe	TaskzEsb	servicebing-cdn.com

IOCs extracted from docs which use sctasks for GRIFFON persistence

Author	Company	wscript.exe copy	C2
mogjxjtvte	mogjxjtvte	mswmex44.exe	logitech-cdn[.]com
soxvremvge	soxvremvge	c9FGG10.exe	logitech-cdn[.]com
gareljtjhvd	gareljtjhvd	zEsb10.exe	servicebing-cdn[.]com

IOCs extracted from regular documents associated to GRIFFON

GRIFFON Implant



Griffon malware

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 .NET class used for taking a screenshot. The resulting screenshot is saved at "%TMP%/image.png", sent back to the attackers by the GRIFFON implant and then deleted.

Persistence module

The last retrieved module is a persistence module. If the victim appears valuable to the attackers, a GRIFFON implant installer is pushed to the victim's workstation. This module stores another instance of the GRIFFON implant inside the registry to achieve persistence. Here is a PowerLinks-style method used by the attackers to achieve persistence and execute the GRIFFON implant at each user logon. The new GRIFFON implant is written to the hard drive before each execution, limiting the "file-less" aspect of this method.

Through its light weight and modular architecture, the GRIFFON implant is the perfect validator. Even though we have been able to retrieve four different modules, it is possible that the FIN7 operators have more modules in their toolsets for achieving their objectives on the victim's workstation.

On the hunt for GRIFFON infrastructure

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

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 company seems to have been used by the FIN7 threat actor to hire new people as translators, developers and pentesters. During our research, we found various job advertisements associated with the company on freelance and remote-work websites.

In addition to that, various individuals have mentioned the company in their resumes. We believe that some of these individuals may not even be aware that they are working for a cybercrime business.

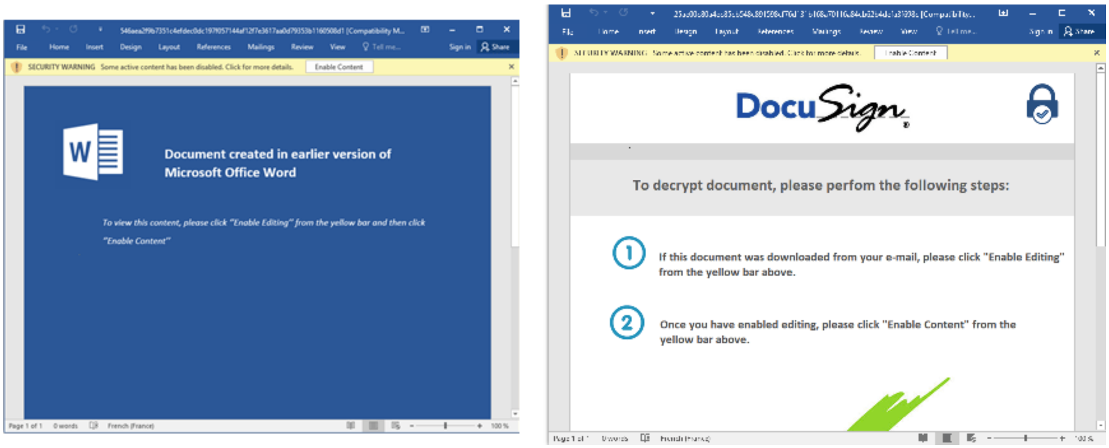
Links to other intrusion sets

While tracking numerous threat actors on a daily basis during the final days of 2018 and at the beginning of 2019, we discovered various activity clusters sharing certain TTPs associated with the FIN7 intrusion set. The link between these threat actors and FIN7 is still weak, but we decided to disclose a few hints regarding these in this blog post.

CobaltGoblin/EmpireMonkey

In his history, FIN7 has overlapped several times with Cobalt/EmpireMonkey in terms of TTPs. 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”

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).

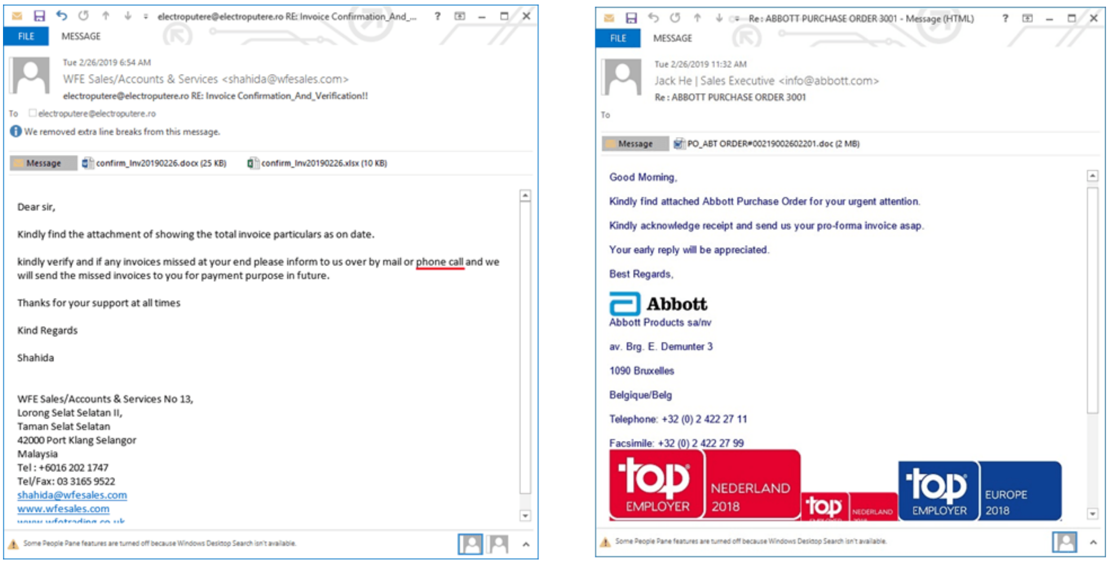
- Both executed a JScript file named “error” in %TEMP% (Errors.txt in the case of FIN7, Errors.bat for EmpireMonkey).
- Both used DocuSign decoy documents with different macros. The macros popped the same “Document decryption error” error message—even if macro code remain totally different.

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. In fact, AveMaria is a classic infostealer bot that collects all possible credentials from various types of software: browsers, email clients, messengers, etc., and can act as a keylogger. Since the beginning of 2019, we have collected more than 1300 samples and extracted more than 130 C2s.

To deliver their malware, the cyber criminals use spearphishing emails with various types of attachments: MS Office documents or spreadsheet files exploiting some known vulnerability like CVE-2017-11882, or documents with Ole2Link and SCT. They also use AutoIT droppers, password-protected EXE files and even ISO images. What is interesting, in some emails, they ask targets to phone them if they have any questions, like the FIN7 guys do.


electroputere@electroputere.ro RE: Invoice Confirmation_And_...
FILE
MESSAGE

Tue 2/26/2019 6:54 AM
WFE Sales/Accounts & Services <shahida@wfesales.com>
electroputere@electroputere.ro RE: Invoice Confirmation_And_Verification!!
To electroputere@electroputere.ro
We removed extra line breaks from this message.

Message confirm_Inv20190226.docx (25 KB) confirm_Inv20190226.xlsx (10 KB)

Dear sir,

Kindly find the attachment of showing the total invoice particulars as on date.

kindly verify and if any invoices missed at your end please inform to us over by mail or phone call and we will send the missed invoices to you for payment purpose in future.

Thanks for your support at all times

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
www.wfetrading.co.uk

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

Tue 2/26/2019 11:32 AM
Jack He | Sales Executive <info@abbott.com>
Re : ABBOTT PURCHASE ORDER 3001
To

Message PO_ABT ORDER#00219002602201.doc (2 MB)

Good Morning,

Kindly find attached Abbott Purchase Order for your urgent attention.

Kindly acknowledge receipt and send us your pro-forma invoice asap.

Your early reply will be appreciated.

Best Regards,

Abbott
Abbott Products sa/nv

av. Brg. E. Demunter 3

1090 Bruxelles

Belgique/Belg

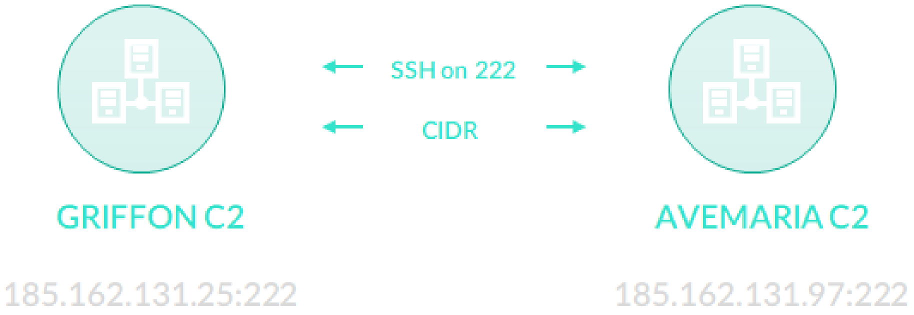
Telephone: +32 (0) 2 422 27 11

Facsimile: +32 (0) 2 422 27 99

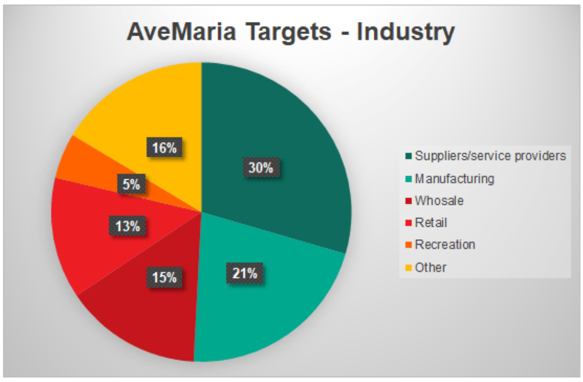
Some People Pane features are turned off because Windows Desktop Search isn't available.

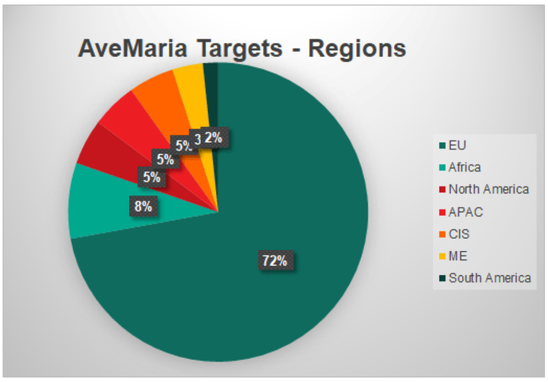
Example of AveMaria spearphing emails. Criminals suggest calling them.

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 end of 2018, while searching for new FIN7 campaigns via telemetry, we discovered a set of activity that we temporarily called “CopyPaste” from a previously unknown APT. Interestingly, this actor targeted financial entities and companies in one African country, which lead us to think that CopyPaste was associated with cybermercenaries or a training center.

This set of activity relied on open-source tools, such as Powershell Empire, and well-documented red teaming techniques, in order to get a foothold within the victim’s networks and avoid detection.

Here are the main similarities between CopyPaste and FIN7:

- Both used the same Microsoft PowerShell argument obfuscation order: “powershell.exe -NoP -NonI -ExecutionPolicy Bypass”. We have only seen FIN7 and CopyPaste use this argument list for executing their malicious Powershell Scripts.
- Both used decoy 302 HTTP redirections and typosquatting on their C2s (reminiscent of Cobalt and FIN7). The Empire C2s associated with CopyPaste had decoy redirections to Digitcert and Microsoft websites and used decoy job employment and tax websites with decoy redirections to host their payloads. FIN7 and Cobalt used decoy 302 HTTP redirections too, FIN7 on its GRIFFON C2s before January 2018, and Cobalt, on its staging servers, similar to CopyPaste.
- 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 company “Combi Security”, we are confident that they continue to create new personas for use in either targeting or recruiting under a “new” brand, “IPC”.

More information about these and related attacks is available to customers of Kaspersky Intelligence Reports. Contact: intelreports@kaspersky.com

Indicators of compromise

AveMaria

- 185.61.138.249
- tain.warzonedns[.]com
- noreply377.ddns[.]net
- 185.162.131.97
- 91.192.100.62
- server.mtcc[.]me

- 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
- 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
- yahooservices-cdn[.]com
- globaltech-cdn[.]com
- infosys-cdn[.]com
- google-services-s5[.]com
- instagram-cdn[.]com
- mse-cdn[.]com
- akamaiservice-cdn[.]com
- booking-cdn[.]com
- live-cdn2[.]com
- cloudflare-cdn-r5[.]com
- cdnj-cloudflare[.]com
- bing-cdn[.]com
- servicebing-cdn[.]com
- cdn-yahooapi[.]com
- cdn-googleapi[.]com
- googl-analytic[.]com
- 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