MORPHISEC

THREAT PROFILE

AN ANALYSIS OF THE EGREGOR RANSOMWARE

INTRODUCTION

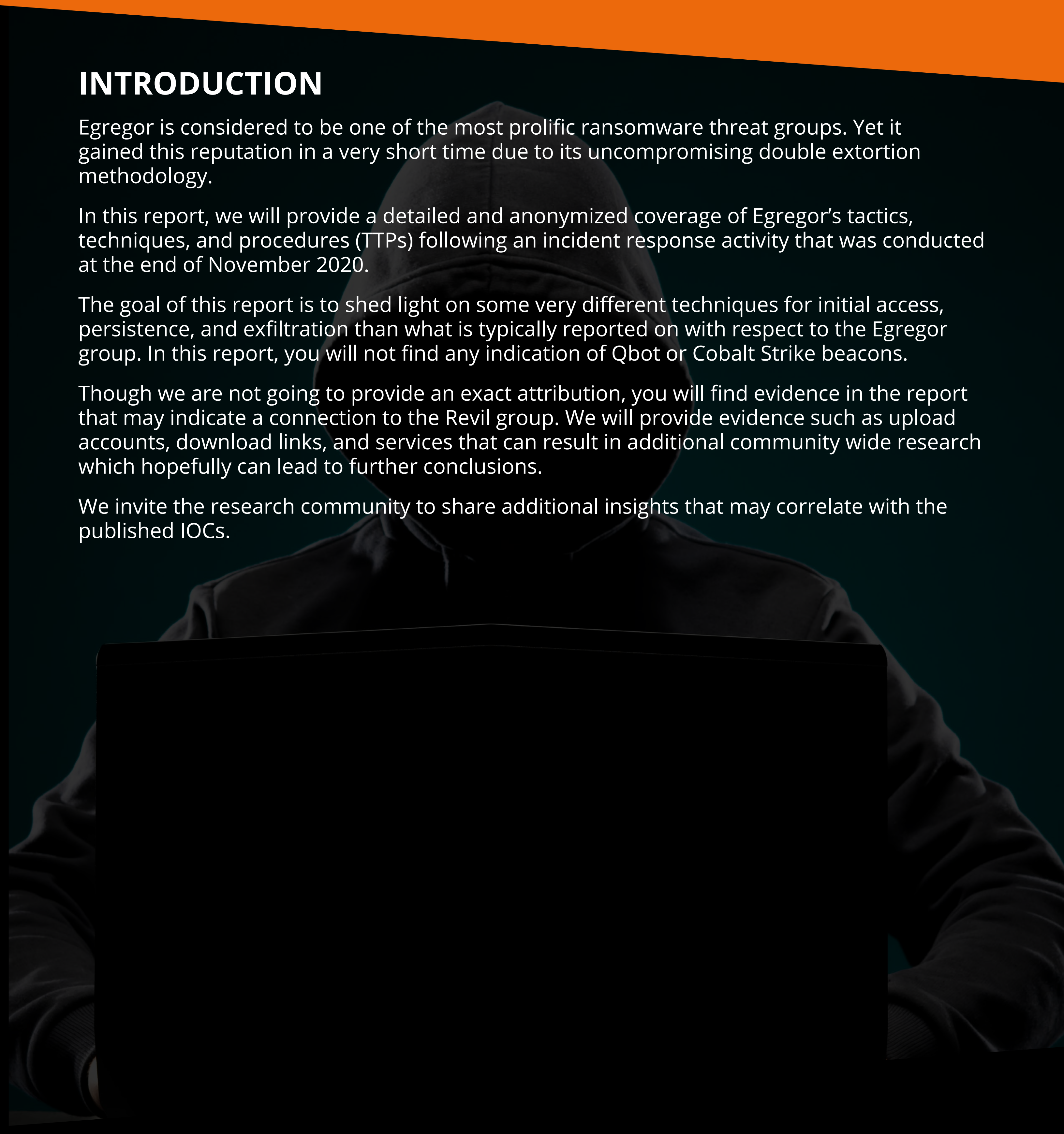
Egregor is considered to be one of the most prolific ransomware threat groups. Yet it gained this reputation in a very short time due to its uncompromising double extortion methodology.

In this report, we will provide a detailed and anonymized coverage of Egregor's tactics, techniques, and procedures (TTPs) following an incident response activity that was conducted at the end of November 2020.

The goal of this report is to shed light on some very different techniques for initial access, persistence, and exfiltration than what is typically reported on with respect to the Egregor group. In this report, you will not find any indication of Qbot or Cobalt Strike beacons.

Though we are not going to provide an exact attribution, you will find evidence in the report that may indicate a connection to the Revil group. We will provide evidence such as upload accounts, download links, and services that can result in additional community wide research which hopefully can lead to further conclusions.

We invite the research community to share additional insights that may correlate with the published IOCs.



TECHNICAL INTRODUCTION

Any incident response involving business compromise usually starts with the end - the impact. When the impact is ransomware, incident investigation is particularly difficult as it is done in parallel to containment activities.

This investigation wasn't different from most that involve ransomware;

- The AD is compromised and the ransomware is deployed directly from the AD.
- A search and mapping of suspicious connections to the AD are correlated to legitimate activities and connections of privileged users. RDP, pass the hash, and other techniques are taken into account.
- Compromised credentials or/and a lateral movement chain is established and patient zero is identified. Obviously, if logs exist, SIEM, event viewers, VPN, AV, and other logs are considered.
- In the case of ransomware, the customer would usually like to know what was exfiltrated to be able to calculate business continuity risks.
- In the last stage, victims like to have a recommendation report for corrective actions that can be applied to the network.

Our incident investigation revealed that the Egregor threat group most probably exploited a VPN vulnerability to access the internal network from a Tor exit node. The attackers then scanned the network while looking for a vulnerable server. They quickly identified and exploited a second vulnerability on an old 2003 application server. This application server became our patient zero. The attackers then moved laterally between file share, application, virtualization, update, and secondary AD servers until they infiltrated to the AD. Next, they exfiltrated data through known services such as MegaUpload directly from the AD. As a final step, they encrypted the network.

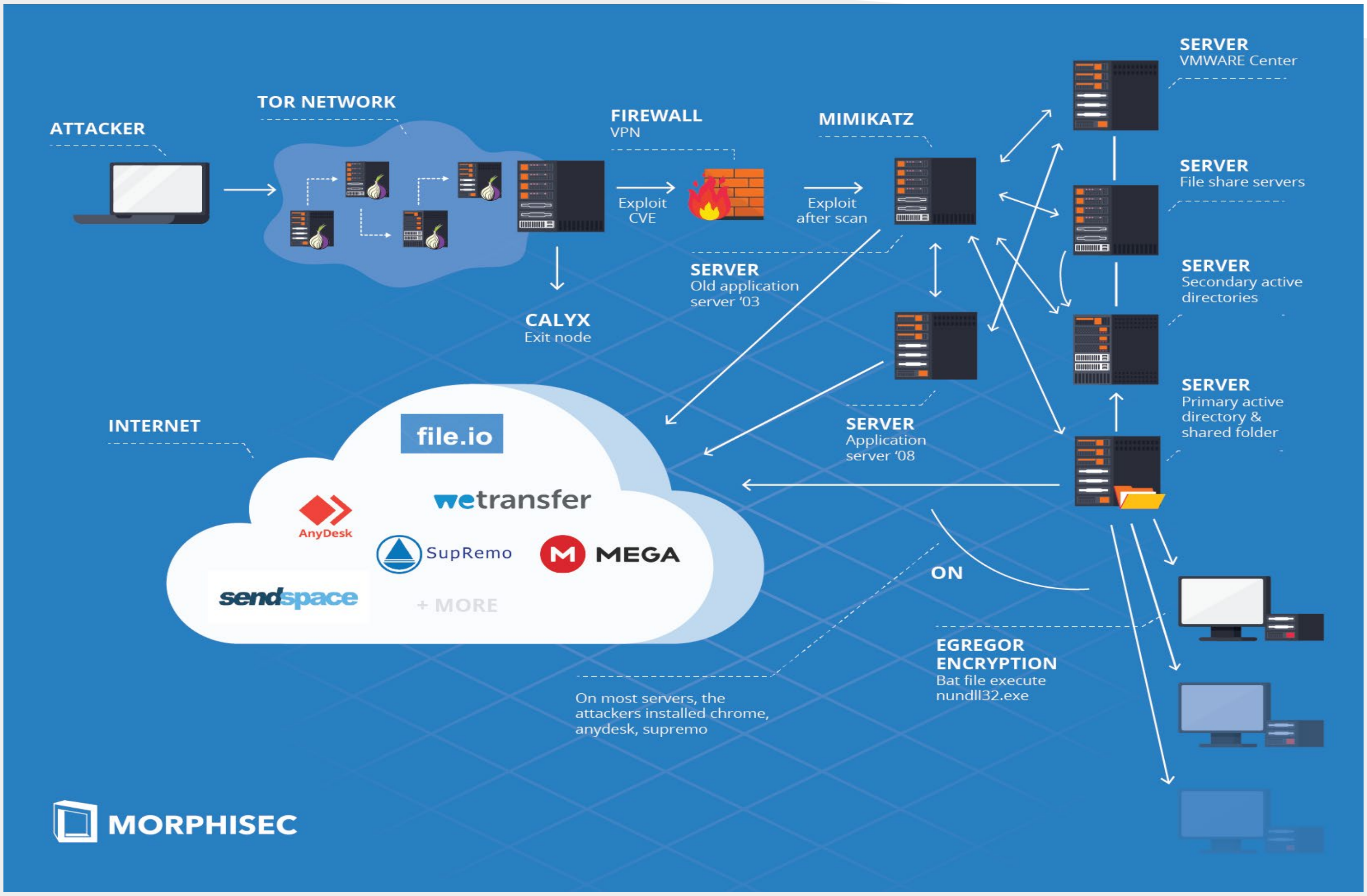


Figure 1: The Egregor attack chain

A number of interesting and unique details will be mentioned in this report:

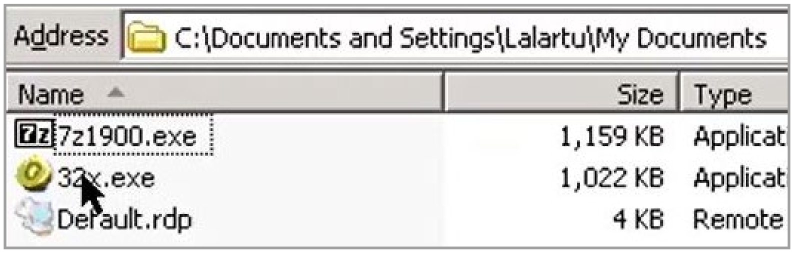
- The upload account credentials and the additional file share services
- Persistence through known legitimate remote control services
- Download multiple versions of the ransomware while bypassing enterprise AV solution
- The use of AES.ONE for ransomware download
- Connection to Revil through Lalartu

INITIAL ACCESS

The current assumption is that the adversaries successfully exploited a non-patched VPN as no SSL login event was registered while the attackers had been assigned with a local IP. The local IP was assigned to a Tor exit node; **162.247.74.74** which belongs to a Calyx Institute. Immediately following an assignment of the local IP, the adversaries initiated a standard network scan as part of a discovery process. Though different users, passwords, and domains were used, we successfully identified the attacker machine VM:

Device name: MAVERIK-PC, Client OS version: Microsoft Windows 7 Ultimate Edition Service Pack 1, 64-bit

As soon as the adversaries identified an older unpatched server (2003), they exploited a second vulnerability which allowed them to log in as a new user "***Lalartu***". Lalartu immediately triggered our suspicion of a possible connection to the Revil and GandCrab groups. At first the attackers tried to exploit other servers in the network using the same username.

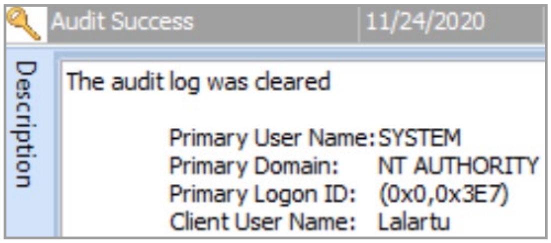


Address C:\Documents and Settings\Lalartu\My Documents

Name	Size	Type
7z1900.exe	1,159 KB	Applicat
32x.exe	1,022 KB	Applicat
Default.rdp	4 KB	Remote

Figure 2: The vulnerable application server.

The vulnerable application server became our patient zero, and our goal was to identify as much as possible by correlating indicators from within and outside the server. This became extra difficult as the attackers wiped the logs from the server.



Audit Success 11/24/2020

Description

The audit log was cleared

```
Primary User Name:SYSTEM
Primary Domain:    NT AUTHORITY
Primary Logon ID:  (0x0,0x3E7)
Client User Name:  Lalartu
```

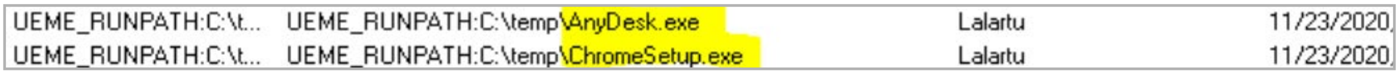
Figure 3: Lalartu is used.

Nevertheless, we succeeded to rebuild the timeline and identify most of the artifacts that were used by the attackers. We assume that at least 3 attackers were working on this environment in parallel.

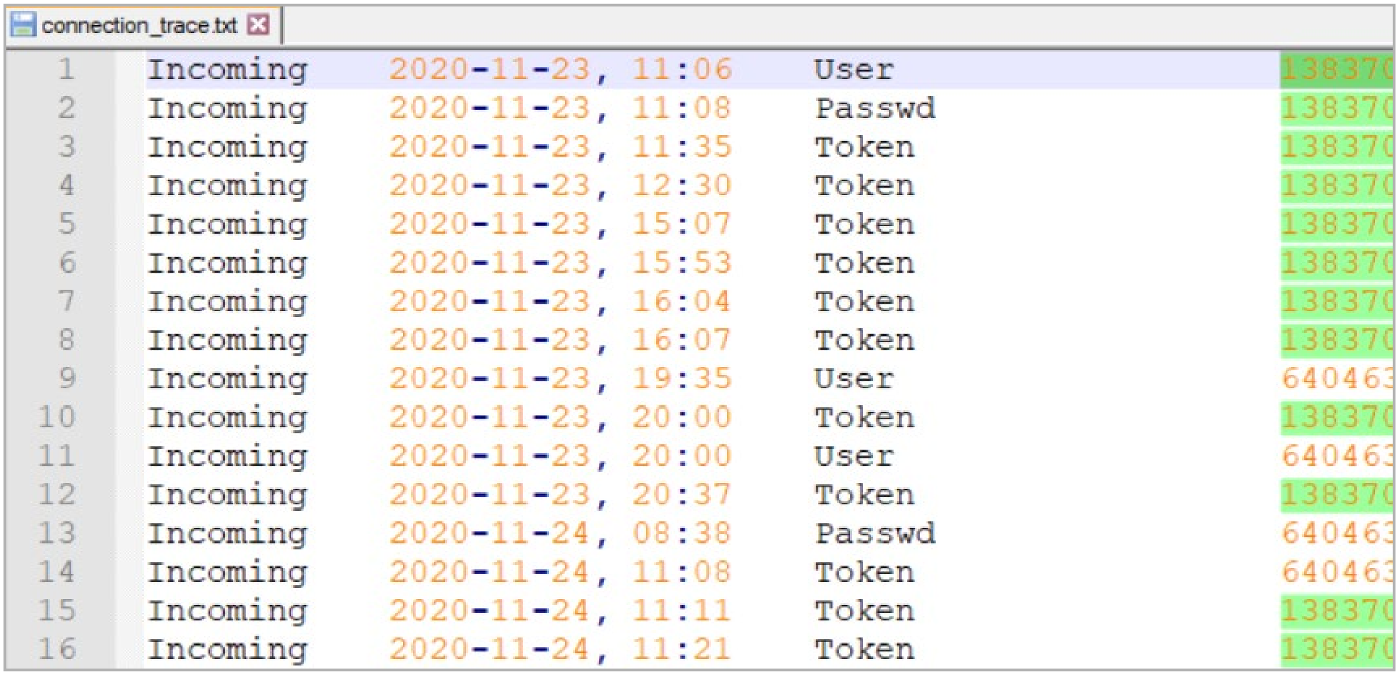
PERSISTENCE & BACKDOORS

As with most similar attack chains, the adversaries needed to maintain access to the servers in case they would lose the connection. They surely needed to avoid the re-exploitation of the network. Due to an opened outbound connection to the internet, they were able to install legitimate remote connection software:

- **AnyDesk -** was dropped on the first login on almost every server that has been compromised



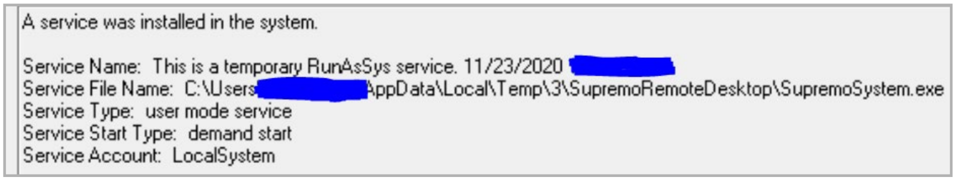
```
UEME_RUNPATH:C:\t...   UEME_RUNPATH:C:\temp\AnyDesk.exe          Lalartu      11/23/2020
UEME_RUNPATH:C:\t...   UEME_RUNPATH:C:\temp\ChromeSetup.exe      Lalartu      11/23/2020
```



```
Incoming    2020-11-23, 11:06    User      13837
Incoming    2020-11-23, 11:08    Passwd    13837
Incoming    2020-11-23, 11:35    Token     13837
Incoming    2020-11-23, 12:30    Token     13837
Incoming    2020-11-23, 15:07    Token     13837
Incoming    2020-11-23, 15:53    Token     13837
Incoming    2020-11-23, 16:04    Token     13837
Incoming    2020-11-23, 16:07    Token     13837
Incoming    2020-11-23, 19:35    User      64046
Incoming    2020-11-23, 20:00    Token     13837
Incoming    2020-11-23, 20:00    User      64046
Incoming    2020-11-23, 20:37    Token     13837
Incoming    2020-11-24, 08:38    Passwd    64046
Incoming    2020-11-24, 11:08    Token     64046
Incoming    2020-11-24, 11:11    Token     13837
Incoming    2020-11-24, 11:21    Token     13837
```

Figure 4: Anydesk dropped

- **SupRemo (supremocontrol.com) -** was installed in parallel to AnyDesk and was used as a backup.



```
A service was installed in the system.

Service Name:  This is a temporary RunAsSys service. 11/23/2020 [redacted]
Service File Name:  C:\Users[redacted]AppData\Local\Temp\3\SupremoRemoteDesktop\SupremoSystem.exe
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

Figure 5: SupRemo installed

In addition to having a remote control using the mentioned applications, the attacker logged in through VPN using legitimate domain administrator credentials as soon as they were gathered from the servers.

DOWNLOADED TOOLS

As most communication has been outgoing from within the target business, attackers needed a way to download the ransomware and the tools they would use for discovery and lateral movement without leaving any trace of the C2 IP.

Just after installing Chrome, they downloaded a 7zip installer and a net scanner from known sources:

- https://www.7-zip.org/download.html
- https://www.softperfect.com/download/files/netscan_portable.zip
  (have been also downloaded under different names such as old.exe)

In other cases, the attackers downloaded Mimikatz and PowerTool executables:

- **Mimikatz** used for credential collection was downloaded only on the “patient” zero server (2003).
- PowerTool was downloaded on a small number of servers under different names with slight executable modifications (e.g. 777.exe and kaav32.exe). This was to identify and tamper with already installed and running security solutions.

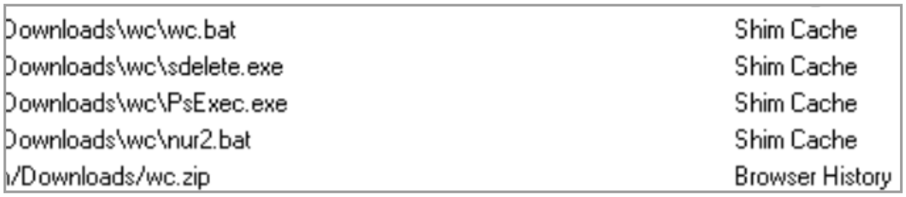
File.io

Most of the tools have been downloaded using the file.io file share service with a one time download link.

E.g. hxxps://file[.]io/WmCH77xcKmbJ

7zip archive was downloaded through file.io, the archive included:

- PsExec (SysInternals)
- Sdelete.exe (SysInternals)
- BAT file to execute the ransomware (described later in the report)
- BAT file to deploy / distribute the ransomware (described later in the report)



Downloads\wc\wc.bat	Shim Cache
Downloads\wc\sdelete.exe	Shim Cache
Downloads\wc\PsExec.exe	Shim Cache
Downloads\wc\nur2.bat	Shim Cache
/Downloads/wc.zip	Browser History

Figure 6: The downloaded tools.

AES.ONE

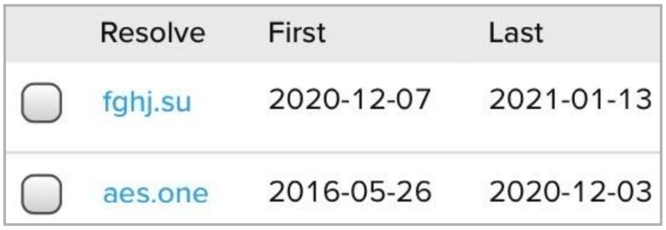
Attackers also used an intriguing backup option for file sharing. Once the first variant of the ransomware was detected by an installed leading AV solution, attackers turned to a less popular and highly questionable AES. ONE file sharing solution. They specifically used it to download only the ransomware component with the other described tools in a previous bullet.

hxxps://aes[.]one/files/d/p43/r1jv9967jd1i3kik9knctlok5/35f35ecea4d8a142/ hxxps://aes[.]one/files/d/pc3/2iopi0o8coob22n8s60pn6b7ps/b6bbf78b901c1fdf/

salsa.7z Downloads

Figure 7: The downloaded ransomware component.

AES.ONE was previously associated with Russian campaigns within the US and conveniently vanished and was replaced by fghj.su on **December 3 through December 7** (10 days after the massive attacks). Some fghj.su links still point back to aes. one.



	Resolve	First	Last
□	fghj.su	2020-12-07	2021-01-13
□	aes.one	2016-05-26	2020-12-03

Figure 8: fghj.su and AES.ONE

EXFILTRATION

As the attackers had access to multiple servers including file share servers and ADs we have established a partial timeline for exfiltration of memory dumps and files. We identified exfiltration attempts mainly from the primary AD following a successful share of folders from the file share servers with the AD.

File share services - lsass dump

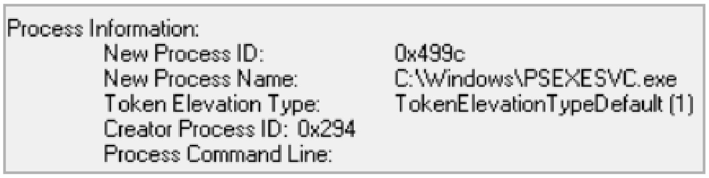
As soon as the attackers compromised the primary AD, they installed Chrome and decided to generate lsass memory dump using PowerShell and exfiltrate it through known sharing services;

- https://wetransfer.com/
- https://www.sendspace.com/

Further evidence that this group could be associated with other Russian based attacks is the misspelling of the word "space" in Google a search that one of the attackers made, typing "*sendspase*."

Unfortunately for the attacker, the network was extremely slow and the upload broke the existing connection to the AD.

During the next couple of hours, attackers tried to reconnect to the AD using all available domain administrator's credentials both through RDP and through PSEXEC service which eventually worked.



```
Process Information:
        New Process ID:             0x499c
        New Process Name:           C:\Windows\PSEXESVC.exe
        Token Elevation Type:       TokenElevationTypeDefault (1)
        Creator Process ID: 0x294
        Process Command Line:
```

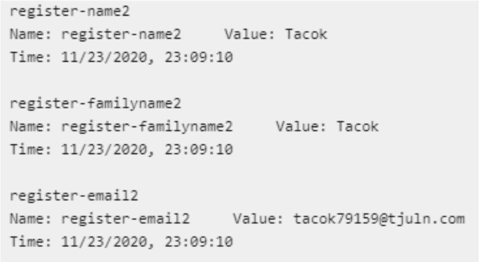
Figure 9: Attackers tried to reconnect.

This led the attacker to execute a speed test while trying to identify the issue and then to install a MegaUpload service on the AD.

MegaUpload

The decision to install a MegaUpload service required the attackers to register a new user for this service (MEGAsyncSetup64.exe).

Luckily we were able to recover the user "Tacok" and his temp email by tjuln.com. "Tjuln" mail is handled by mail.mailerhost.net, a known shared service that is hosted on AWS. This is why the IP can not be blacklisted. This is also likely the reason the attackers used the email.



```
register-name2
Name: register-name2     Value: Tacok
Time: 11/23/2020, 23:09:10

register-familyname2
Name: register-familyname2     Value: Tacok
Time: 11/23/2020, 23:09:10

register-email2
Name: register-email2     Value: tacok79159@tjuln.com
Time: 11/23/2020, 23:09:10
```

Figure 10: The Tacok user and email.

Additional investigation of the email domain revealed a high abuse rate on the same date of the attack. This could indicate that the attackers executed the same attack on multiple targets at the same time.

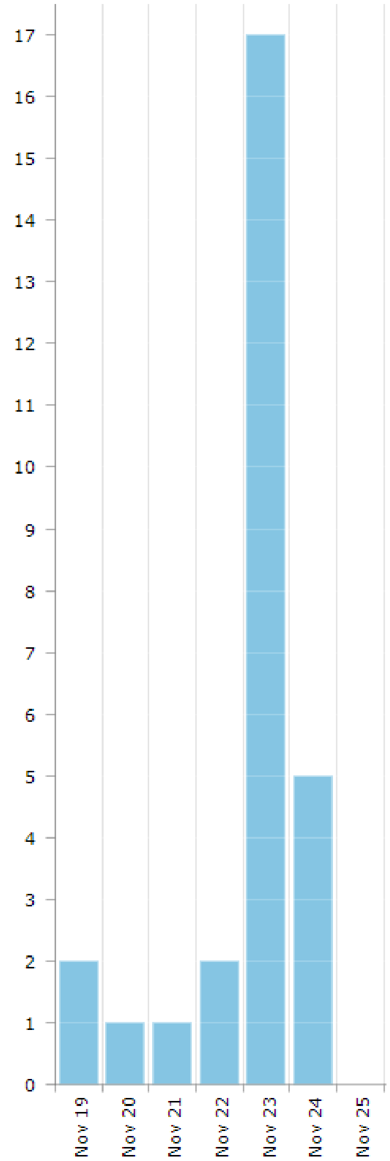
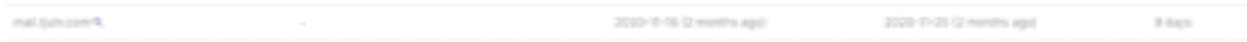
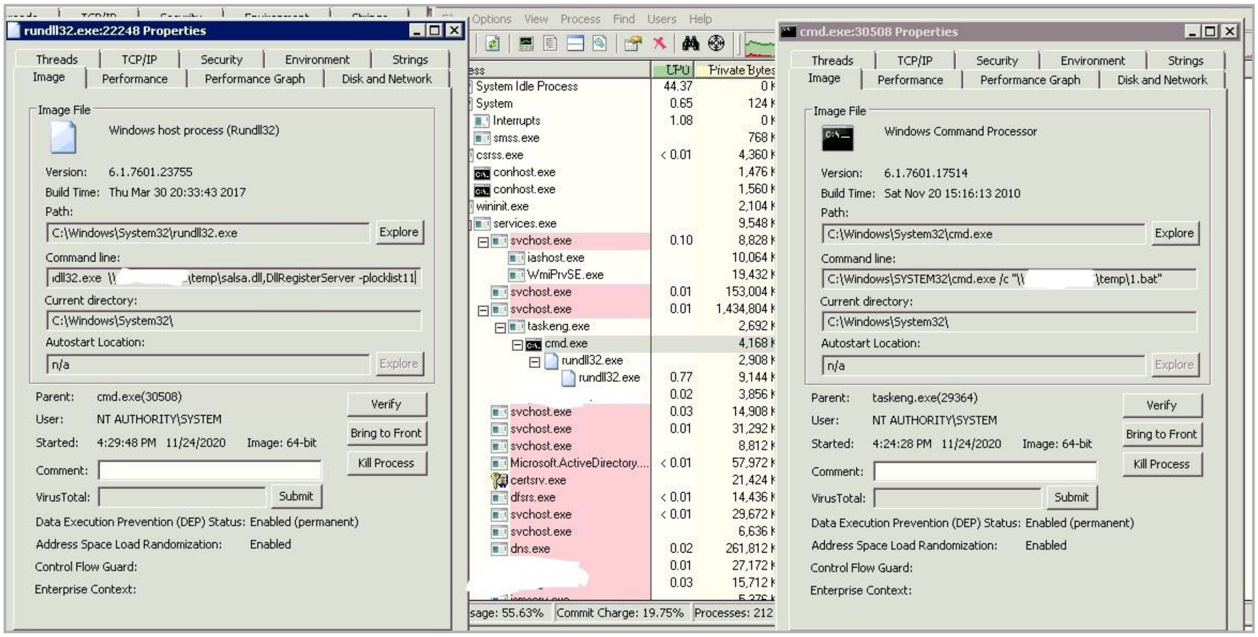


Figure 11: A high abuse rate of Tjuln email domain from StopForumSpam.



RANSOMWARE

Following a successful exfiltration, ransomware was deployed from an AD shared folder. We succeeded in identifying many of the scripts, but not all as many of the artifacts have been either overwritten by sdelete or re-encrypted by the ransomware itself.



Windows host process (Rundll32)

Version: 6.1.7601.23755
Build Time: Thu Mar 30 20:33:43 2017
Path: C:\Windows\System32\rundll32.exe
Command line: ıdll32.exe \\[redacted]\temp\salsa.dll,DllRegisterServer -plocklist11
Current directory: C:\Windows\System32\
Autostart Location: n/a
Parent: cmd.exe(30508)
User: NT AUTHORITY\SYSTEM
Started: 4:29:48 PM 11/24/2020 Image: 64-bit
Comment:
VirusTotal:
Data Execution Prevention (DEP) Status: Enabled (permanent)
Address Space Load Randomization: Enabled
Control Flow Guard:
Enterprise Context:

```
ess                              CPU     Private Bytes
System Idle Process              44.37          0 K
System                            0.65        124 K
Interrupts                        1.08          0 K
smss.exe                                      768 K
csrss.exe                       < 0.01      4,360 K
conhost.exe                                 1,476 K
conhost.exe                                 1,560 K
wininit.exe                                 2,104 K
services.exe                                9,548 K
  svchost.exe                     0.10      8,828 K
      iashost.exe                          10,064 K
      WmiPrvSE.exe                         19,432 K
    svchost.exe                   0.01    153,004 K
  svchost.exe                     0.01  1,434,804 K
      taskeng.exe                           2,692 K
        cmd.exe                             4,168 K
          rundll32.exe                      2,908 K
            rundll32.exe          0.77      9,144 K
[redacted]                        0.02      3,856 K
    svchost.exe                   0.03     14,908 K
    svchost.exe                   0.01     31,292 K
    svchost.exe                             8,812 K
    Microsoft.ActiveDirectory.... < 0.01     57,972 K
    certsrv.exe                            21,424 K
    dfsrs.exe                   < 0.01     14,436 K
    svchost.exe                 < 0.01     29,672 K
    svchost.exe                             6,636 K
    dns.exe                       0.02    261,812 K
[redacted]                        0.01     27,172 K
                                  0.03     15,712 K
sage: 55.63%   Commit Charge: 19.75%   Processes: 212
```

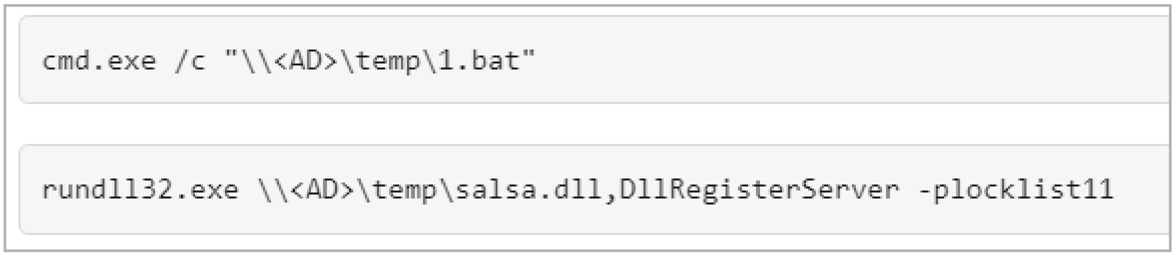
Windows Command Processor

Version: 6.1.7601.17514
Build Time: Sat Nov 20 15:16:13 2010
Path: C:\Windows\System32\cmd.exe
Command line: C:\Windows\SYSTEM32\cmd.exe /c "\\[redacted]\temp\1.bat"
Current directory: C:\Windows\System32\
Autostart Location: n/a
Parent: taskeng.exe(29364)
User: NT AUTHORITY\SYSTEM
Started: 4:24:28 PM 11/24/2020 Image: 64-bit
Comment:
VirusTotal:
Data Execution Prevention (DEP) Status: Enabled (permanent)
Address Space Load Randomization: Enabled
Control Flow Guard:
Enterprise Context:

Figure 12: The ransomware scripts.

The attackers deployed the ransomware in 3 ways depending on the endpoint environment - the differentiator is usually the deployment BAT file (nur.bat, nur2.bat, nur3.bat):

- Nur3.bat - direct execution of local BAT file that executes the ransomware locally (on a set of selected targets such as file shares)
- Nur.bat - Task scheduler with remote execution of the ransomware (most servers)



```
cmd.exe /c "\\<AD>\temp\1.bat"
```

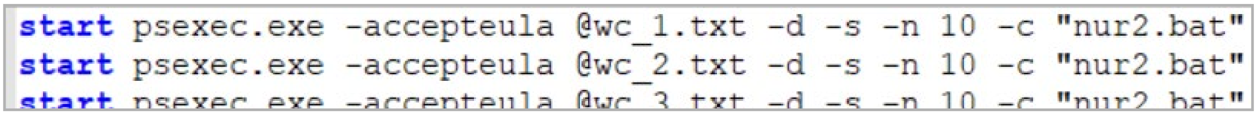
```
rundll32.exe \\<AD>\temp\salsa.dll,DllRegisterServer -plocklist11
```

Figure 13: Deployment of the ransomware.

- Nur2.bat - most endpoints - direct remote psexec with remote BAT execution from remote (AD) share (will be described below)

wc.bat

The Egregor deployment script is a .bat file that **remotely** executes Egregor in chunks using psexec (about 20 local IPs per execution line). Every command is executed with a connection timeout of 10 seconds.

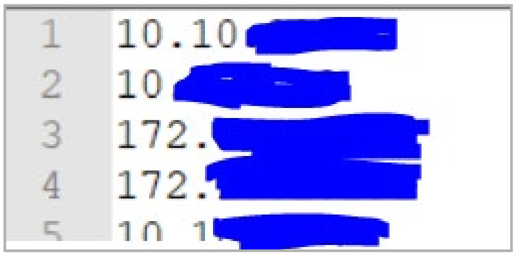


```
start psexec.exe -accepteula @wc_1.txt -d -s -n 10 -c "nur2.bat"
start psexec.exe -accepteula @wc_2.txt -d -s -n 10 -c "nur2.bat"
start psexec.exe -accepteula @wc_3.txt -d -s -n 10 -c "nur2.bat"
```

Figure 14: The Egregor deployment script.

wc_1.txt

As mentioned above, every execution line has a unique input file that contains about 20 unique local IP addresses that were previously identified through the netscan tool.

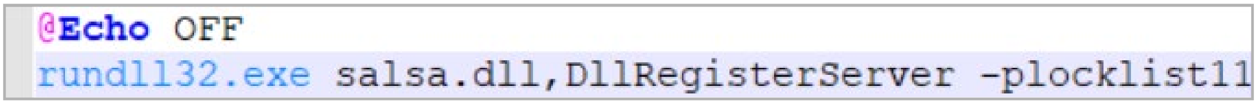


```
10.10[redacted]
10[redacted]
172.[redacted]
172.[redacted]
10.1[redacted]
```

Figure 15: Unique local IP addresses

Nur2.bat

The command that is executed on a remote machine, Salsa.dll, is the Egregor ransomware that requires a decoding password for its successful execution. As mentioned above (the Downloaded Tools section) we have identified more than a single version of the ransomware dropped on the servers due to a previous detection of the first variant.

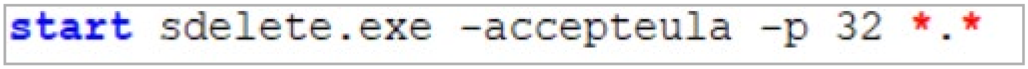


```
@Echo OFF
rundll32.exe salsa.dll,DllRegisterServer -plocklist11
```

Figure 16: The Salsa.dll file.

s.bat

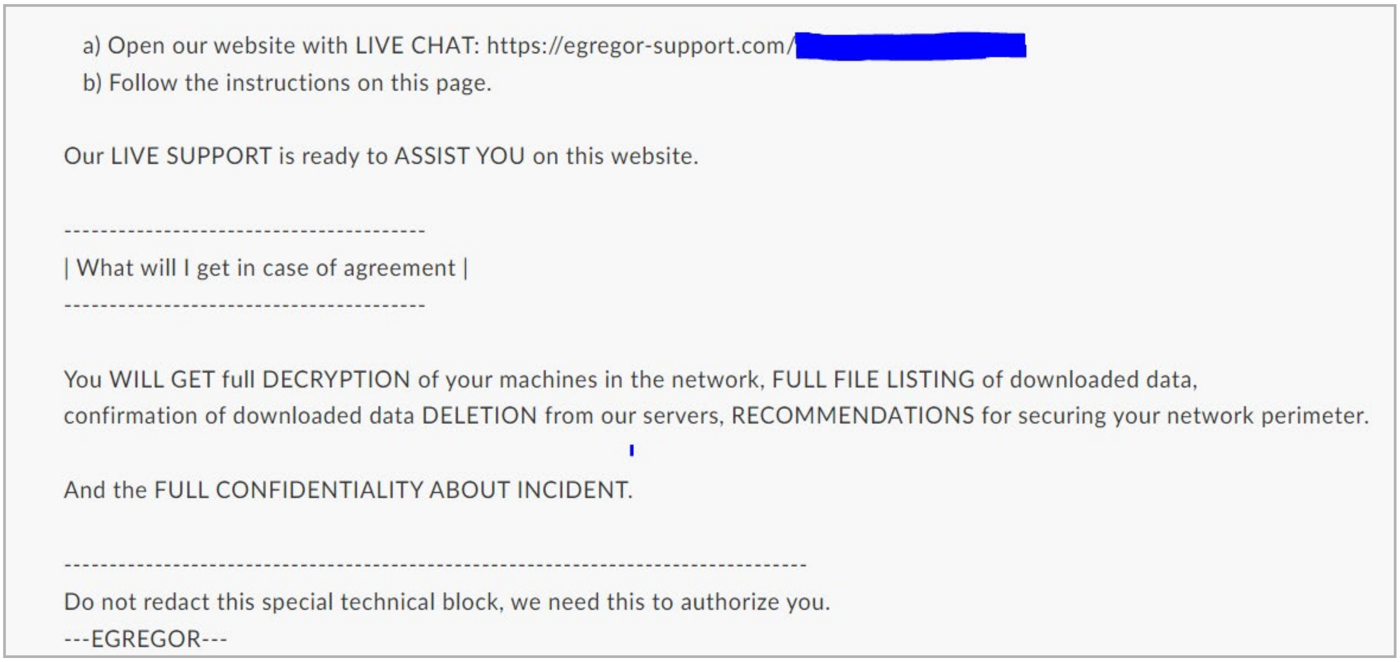
To remove the attacker traces, sdelete was used to overwrite the trace files (32 overwrites).



```
start sdelete.exe -accepteula -p 32 *.*
```

Figure 17: Sdelete

As we already know, the Egregor group threatens to leak sensitive data as part of their double extortion attempts where they actually release chunks of exfiltrated information to the public. Their demands are also extremely high and can lead to more than $40 million.



```
   a) Open our website with LIVE CHAT: https://egregor-support.com/[redacted]
   b) Follow the instructions on this page.

Our LIVE SUPPORT is ready to ASSIST YOU on this website.


---------------------------------------
| What will I get in case of agreement |
---------------------------------------


You WILL GET full DECRYPTION of your machines in the network, FULL FILE LISTING of downloaded data,
confirmation of downloaded data DELETION from our servers, RECOMMENDATIONS for securing your network perimeter.

And the FULL CONFIDENTIALITY ABOUT INCIDENT.


--------------------------------------------------------------------------------
Do not redact this special technical block, we need this to authorize you.
---EGREGOR---
```

Figure 18: An Egregor ransom note.

CONCLUSIONS AND RECOMMENDATIONS

As can be seen from the latest waves of ransomware campaigns; extortion, human-operated propagation, exploitation of VPN applications, and meteoric encryption are a landmark change in the current attack landscape.

Enterprises must adhere to the zero trust principles in order to minimize the risk of exposure to a ransomware attack, basic recommendations would be:

- Deny network communication to all and from all, allow only on demand (minimize the risk for backdoors).
- Apply MFA to minimize lateral movement risk.
- Deploy runtime zero trust preventive technology such as Morphisec to keep your runtime applications safe.
- Minimize administrator privileges.
- Implement basic attack surface reduction rules such as script prevention and psexec prevention.
- Isolate your backups and test those regularly.

IOCS

Salsa.dll (Egregor)	D0AB713F502D01DDF73694276F0199DB	-plocklist11
Salsa.dll (Egregor)	D20CD3F8F0ECC34FA400EDF72687B215	
32x.exe	(mimikatz)	
777.exe	3FADBE9038C51C12014818F172E43A7D	PowerTool v2 x64
kaav32.exe		PowerTool x86

Tools used:

AnyDesk.exe	365AA18CADC5B80A9B5CA5950690C7F8	
Supremo.exe	00283740140DBE5C227BD15733D7A3B6	
MEGAsyncSetup64.exe	B04F9B4FEAC14CFF959718B69B7BBEAF	
Netscan.exe (old.exe)		https://www.softperfect.com/download/files/netscan_portable.zip

Chromesetup.exe	7AF4A442683662B020FD391E26666958	
7z1900.exe	FABE184F6721E640474E1497C69FFC98	https://www.7-zip.org/download.html
PsExec.exe	27304B246C7D5B4E149124D5F93C5B01	Sysinternals
sdelete.exe	F41A1AFC4CFB95F35CD92DA98D90C27B	Sysinternals

Emails and URLs:

tacok79159@tjuln.com
hxxps://aes[.]one/files/d/p43/r1jv9967jd1i3kik9knctlok5/35f35ecea4d8a142/
hxxps://aes[.]one/files/d/pc3/2iopi0o8coob22n8s60pn6b7ps/b6bbf78b901c1fdf/
hxxps://file[.]io/WmCH77xcKmbJ
162.247.74[.]74

ABOUT MORPHISEC

Morphisec delivers an entirely new level of innovation to customers with its patented Moving Target Defense technology – placing defenders in a prevent-first posture against the most advanced threats to the enterprise, including APTs, zero-days, ransomware, evasive fileless attacks and web-borne exploits. Morphisec provides a crucial, small footprint zero trust memory-defense layer that easily deploys into a company's existing security infrastructure to form a simple, highly effective, cost-efficient prevention stack that is truly disruptive to today's existing cybersecurity model.