Egregor – Prolock: Fraternal Twins ?

By Equipe CERT

Published: 2020-11-12 · Archived: 2026-04-05 17:21:35 UTC

CERT Intrinsec has faced since the beginning of September several cases involving Egregor and Prolock ransomwares. This article aims at presenting Egregor and Prolock techniques, tactics and procedures, as well as sharing indicators of compromise and highlighting actions of the threat actor operating both ransomwares, according to collected intelligence and TTPs analysis.

On one hand, Egregor has a similar strategy to other ransomwares, as it exfiltrates data, encrypts files and publishes them on its website in order to make victims pay the ransom. It is active since the beginning of September 2020 and impacts many sectors from insurance to transport. Its goal is lucrative.

On the other hand, Prolock, successor of PwndLocker, is active since March 2020. As many other ransomwares, it targets big companies with ransoms going from 35 to 255 bitcoins (400 000 to 3 000 000 $). Its goal is, as far as we know, only lucrative. Prolock is active mainly in Northern America and in Europe and impacts several sectors, such as health, construction, finance, legal, etc.

Kill chain

Egregor ransomware analysis

Initial access

We were not able to find identified specific initial accesses, we found traces of Qakbot during investigations but we could not identify how it was dropped on information systems. We observed many potential intrusion vectors on patient 0 (many malwares were found on the machine).

Internal reconnaissance

Prior to privilege escalation, Egregor proceeds to Active Directory reconnaissance using tools such as Sharphound or AdFind. These tools are used to gather information about users, groups, computers, and so on. They aim as well at finding the best compromission paths.

Privilege escalation

During investigations, Egregor compromises Active Directory in order to become domain admin.

Lateral movement

Egregor moves laterally on information systems using CobaltStrike SMB beacons. This feature allows an attacker to use SMB named pipes (logical connections between a client and a server) to communicate commands through the information system revealing C2 IP address.

The following command line is a service created by CobaltStrike and can be found in Windows Event Logs (event id 7045). It runs an encoded powershell command.

CobaltStrike service execution

It is possible to deobfuscate CobaltStrike payloads (base64, gunzip and XOR operations) using CyberChef[1]:

CobaltStrike payload deobfuscation

C2 Communication

Once settles on victim's information systems, Egregor communicates with its Command and Control servers via HTTPS protocol so as to drop scripts or dynamic link libraries on infected hosts. You can find the list of C2 identified during investigations in **section "IP Addresses"**.

Data exfiltration

Egregor masquerades *svchost.exe* process to launch an *RClone* client in order to exfiltrate data. *RClone* aims at managing files in cloud, it deals with multiple systems and protocols. The *RClone* configuration file, in plain text, is dropped by the attacker with the binary. Based on investigations and OSINT, we know that Egregor used at least three different configurations to exfiltrate data.

RClone Configuration File (WebDav)

RClone Configuration File (sFTP)

RClone Configuration File (DropBox)

Defense evasion

To evade protections, Egregor create a Group Policy Object to disable Windows Defender and try to takedown any anti-virus console prior to ransomware execution:

```
 Display name: New Group Policy Object
Version: 1
registry.pol content:
-       Key path: Software\Policies\Microsoft\Windows Defender
-       Data name: DisableAntiSpyware
-       Value type: 0x04 (REG_DWORD)
-       Data value: 0x01
```

Ransomware execution

Egregor downloads custom dynamic link libraries (b.dll, q.dll, etc) using bitsadmin and execute them on victim's systems to encrypt data.

DLL download and execution

Prolock ransomware analysis

Initial Access

One of the intrusion vectors is malspam. Indeed, **Emotet** is used to initiate infection on several user workstations and to drop **Qakbot**. Emotet used legitimate documents after taking control of some user's email accounts. These documents contain a payload which tries to download a binary file from different URLs, as following. On infected systems, after the execution of the binary retrieved by Emotet code, few files are created (typical Qakbot operation):

- \AppData\Roaming\Microsoft\Jfayae\vatgrcxt.exe
- \koyxogldypnalvvlyxpw.exe
- \AdFind.exe

Code embedded in the malicious document

Powershell payload (decoded from base64)

Deobfuscated powershell code (used to download F889k6.exe)

Unfortunately, we were not able to retrieve *F889k6.exe* neither from compromised systems nor from URLs, which were already down by that time.

Internal reconnaissance

Prolock proceeds to Active Directory reconnaissance AdFind tool to gather information about users, groups, computers so as to prepare exfiltration and ransomware execution.

Privilege escalation

During investigations, Prolock compromises Active Directory in order to become domain admin.

Lateral movement

Prolock uses batch scripts to enable RDP on targeted hosts. We found the script below during one of our cases. The same script has already be found on Prolock cases.

Following actions are performed by the script:

- Enable Remote Desktop connections by setting fDenyConnections to 0.
- Start Microsoft Protection Service.
- Set a rule in Windows firewall to activate RDP service.
- Modify RDP-Tcp registry key.

rdp.bat script (enable RDP connections)

Data exfiltration

We did not see any use of *RClone* during incident responses involving Prolock.

Ransomware execution

Prolock uses different scripts and files to encrypt victim's data. **It retrieves all these files from 185.238.0[.]233, the latter hosting as well Egregor dynamic link libraries.** The first script *wmi_md.bat* (*wmi_u.bat* works the same way) proceeds the following actions on each host whose IP address is in the file *list_md.txt* (or *list_u.txt*):

- Connect to the host using a compromised account
- Drop *connect.bat* and *office.txt* on the host
- Execute connect.bat using WMI command-line
- Write host IP address in log.dat file
- Cancel the network connection

Script deploying ransomware on information system (wmi_md.bat)

In addition, we found a script that uses bitsadmin to download *office.txt* and *connect.bat* from 185.238.0[.]233.

Code from eb1.bat

The script *connect.bat* contains the following encoded powershell payload.

Powershell payload from connect.bat

After decoding and deobfuscating it, we got to know that it is used to load office.txt in memory and execute it.

Decoded and deobfuscated payload

Office.txt analysis is not yet complete, but we believe that it is the ransomware, based on system events correlation.

Relations between Egregor & Prolock

During recent investigations, we observed common indicators of compromise and techniques between Egregor and Prolock. These common points are presented below:

- The IP address 185.238.0[.]233 hosts both Egregor's dynamic link libraries and Prolock files (especially scripts used to run the ransomware). You can find more information about Prolock TTP in the next section.
- Both *WIN-799RI0TSTOF* and *WIN-4K804V6ADVQ* hostnames of potential VPS have been seen during Prolock and Egregor cases.
- *list_md.txt* and *list_u.txt* files were involved in both Egregor and Prolock cases (of course, their content depends on the victim's information system).
- The use of bitsadmin in eb*.bat scripts to download dll (Egregor) or scripts (Prolock) is another common point between these threat actors.
- *md.exe* binary has been seen on both Egregor and Prolock cases.
- Even if we did not notice exfiltration using *RClone* in our Prolock cases, we know that this threat actor uses it[2].

Timeline of incident responses involving Prolock and Egregor insisting on common indicators of compromise

Indicators of compromise

Incident response

Binaries

File	Size (bytes)	MD5	SHA1	SHA256
md.exe	4516928 4183104	5ed9fb5fc74c6fdb3537629e9b23437a N/A	67424175620be87fd3b2810ba5eba0d9e0bee49f 7e0018e18f6bd230366a2b6f031c52ee8899f8dc	fec51f04710e N/A
svchost.exe	42043904	4a97c4345aabf9dd922d29687c95ac66	f54bf6a4c6f7c3d0077d152a094e3c7738cf0bd1	5bc506b9f61
main_target1.exe	4516416	a3e1ea9438e293ec8fae62c39ea3f0e4	e9581cb5161f10f5e99e0cb6c30c201e6e844676	089bb9d18b3
b.dll	808960	a654b3a37c27810db180822b72ad6d3e	d2d9484276a208641517a2273d96f34de1394b8e	4c9e3ffda0e6
q.dll	784896	520ee511034717f5499fb66f9c0b76a5	3a33de9a84bbc76161895178e3d13bcd28f7d8fe	a5989c480ec
qymrkrr.exe	N/A	N/A	N/A	N/A
fxmgwk.exe	N/A	N/A	N/A	N/A
cthwiilhz.exe	N/A	N/A	N/A	N/A
erkftj.exe	N/A	N/A	N/A	N/A
c6d7790.exe	N/A	N/A	N/A	N/A
c6d7790.exe	N/A	N/A	N/A	N/A
a31b29b.exe	N/A	N/A	N/A	N/A
ed53e67.exe	N/A	N/A	N/A	N/A
3f2eb85.exe	N/A	N/A	N/A	N/A

Scripts

File	Size (bytes)	MD5	SHA1	SHA256
e.bat	156 157	7375083934dd17f0532da3bd6770ab25 N/A	ac6d919b313bbb18624d26745121fca3e4ae0fd3 1be22505a25f14fff1e116fafcaae9452be325b1	f0adfd3f89c9268953 N/A
eb.bat	58	N/A	9dacb159779d5e57798632bac74ae5b880cf1ec8	N/A
eb1.bat	253	3872e7caaede9ee1ce8f37435dcaf836	8f166dfeb2fd8780de0e3dbdb25d0fdb373f58de	c9df055f380100a730
connect.bat	7004	6cebf3c01844520e8b27023d8f47a0ed	f5b14cc494303c91456bb50e7816358b6766a5b8	bd1dba49596c04677
wmi_u.bat	421	9deca294973f6d52f9506240b104079c	f098e6931eb32f9d28f681ad6fd2716a65b7f140	87a699923f3edeb6ce
wmi_md.bat	416	463d45502447c7aa58538159eccc1a1a	4bad78fccfc69f4f9ac619dd9a8a9f70c3cc3ed0	a9d3c1d779550b003
rdp.bat	329	dc1aafc01b5068eef6c2ed4cfd6864ed	eb43350337138f2a77593c79cee1439217d02957	ac49c114ef137cc198

Other files

File	Size (bytes)	SHA1
svchost.conf	155	bae4323aa7fa3e4de9ab021d72ecd84de795351b
office.txt	30608	4769a775fd4a2c29b433736a59dc4277354a54f2
list_u.txt	4560 9269	3b59fdff922497dc24d7cec0b219e93334e81221 33c776f25ed3bb6011bfe96c13467815fb993289

list_md.txt	4773 9633	1a3c149a2720f001a0a475ae978114090f3ed720 aaf4374400c63b0dae41f67bd90cd2ebb2c159db
list3.txt	4560	3b59fdff922497dc24d7cec0b219e93334e81221
[HOW TO RECOVER FILES].TXT	1085	620311402640b1547d59722b63f19fab082a57af
RECOVER-FILES.txt	N/A	N/A

C2 Domain names

- amajai-technologies[.]network
- amajai-technologies[.]industries

IP adresses

- *IP addresses hosting dll and scripts:*
  - 185.238.0[.]233
  - 45.153.242[.]129
- *Server using for potential data exfiltration*
  - 93.190.140[.]75
- *IP addresses communicating with infected systems through CobaltStrike*
  - 23.254.229[.]82
  - 192.236.209[.]151
- *Potential VPS IP addresses*
  - 217.138.219[.]138
  - 185.212.170[.]158
  - 23.106.215[.]67

Potential VPS Hostnames

- WIN-799RI0TSTOF
- WIN-4K804V6ADVQ
- DESKTOP-LHC2KTF
- DESKTOP-93VHU8M

Threat Intelligence

Using IOC collected during incident responses, we hunted some other Egregor files, especially from 185.238.0[.]233. We found similar dynamic link libraries (a.dll, p.dll, etc), as well as the RClone configuration file we presented in section "**Data Exfiltration**".

File	Size (bytes)	SHA1
b.dll	808960	d2d9484276a208641517a2273d96f34de1394b8e
hnt.dll	498688	38c88de0ece0451b0665f3616c02c2bad77a92a2
kk.dll	498176	09d8c91ccefd699fb5ac1aaebeeebee25170fe1a
p.dll	784896	8768cf56e12a81d838e270dca9b82d30c35d026e
p.dll	500224	fafd32e972ebb33b187bfb1ebf1a6ecb1d2d7239
sed.dll	806400	b7170443ea2b73bca3d16958712ee57cb4869d5b

- CobaltStrike C2 Domain names[3]

- atakai-technologies[.]space
- atakai-technologies[.]website
- atakai-technologies[.]host
- atakai-technologies[.]online
- atakai-technologies[.]work
- akamai-technologies[.]host

- akamai-technologies[.]site
- akamai-technologies[.]space
- akamai-technologies[.]digital
- akamai-technologies[.]website
- akamai-technologies[.]online
- amajai-technologies[.]host
- amajai-technologies[.]website
- amajai-technologies[.]network
- amajai-technologies[.]digital
- amajai-technologies[.]space
- amajai-technologies[.]tech
- amajai-technologies[.]industries
- amamai-tecnologies[.]space
- amamai-tecnologies[.]cloud
- amamai-tecnologies[.]digital
- amatai-technologies[.]website
- amatai-technologies[.]digital
- amatai-technologies[.]space
- amatai-technologies[.]site

MITRE ATT&CK

Prolock

Tactic	Technique
Initial Access	Phishing (T1566): Spearphishing attachment (T1566.001)
Execution	User Execution (T1204): Malicious File (T1204.002) Windows Management Instrumentation (T1047)
Persistence	Scheduled Task/Job (T1053): Scheduled Task (T1053.005) Valid Accounts (T1078)
Discovery	Account Discovery (T1087) Domain Trust Discovery (T1482) Permission Groups Discovery (T1069): Domain Groups (T1069.001)
Lateral Movement	Remote Services (T1021): Remote Desktop Protocol (T1021.001) Valid Accounts (T1078)
Command and Control	Ingress Tool Transfert (T1105)
Impact	Data encrypted for impact (T1486)

Egregor

Tactic	Technique
Execution	Scheduled Task/Job (T1053): Scheduled Task (T1053.005) Services Execution (T1569): Service Execution (T1569.002) Windows Management Instrumentation (T1047)
Persistence	Create or modify system process (T1543): Windows Service (T1543.003)
Defense Evasion	Impair Defenses (T1562): Disable or modify tools (T1562.001)
Discovery	Account Discovery (T1087) Domain Trust Discovery (T1482) Permission Groups Discovery (T1069): Domain Groups (T1069.001)
Lateral Movement	Remote Services (T1021): SMB/Windows Admin Shares (T1021.002)
Command and Control	Application Layer Protocol (T1071)
Exfiltration	Exfiltration over web service (T1567): Exfiltration to Cloud Storage (T1567.002)
Impact	Data encrypted for impact (T1486)

References

CyberChef recipe to deobfuscate CobaltStrike payloads : [1] https://github.com/mattnotmax/cyberchef-recipes#recipe-28—de-obfuscation-of-cobalt-strike-beacon-using-conditional-jumps-to-obtain-shellcode

Article from Group-IB about Prolock : [2]https://www.group-ib.com/blog/prolock

CobaltStrike C2 List : [3]https://twitter.com/smoothimpact/status/1308033998371905538
