November 2021

AVALON Cyber

LOCKBIT2.0 RANSOMWARE AS A SERVICE (RaaS)

Unauthorized user gains access to front-facing host(s) with no authentication required by exploiting CVEs.

1. RECON & WEAPONIZATION

CVE-2021-34473	CVE-2021-34523	CVE-2021-31207
Pre-auth path confusion leads to ACL bypass	Elevation of privilege on Exchange PowerShell	Post-auth arbitrary-file-write leads to RCE

When chained together, these CVEs are known as **ProxyShell** and target vulnerable **Microsoft Exchange** web servers.

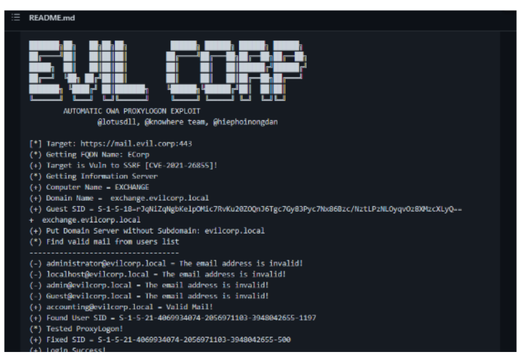
2. DELIVERY

IIS log entries for IOAs utilizing the **cttgo.aspx** file on client Exchange server:

```
2021-09-29 [IP Address] GET /aspnet_client/cttgo.aspx
-443- [IP Address] python-requests/2.25.1 -200 0 0 5000

2021-09-29 [IP Address] GET /aspnet_client/cttgo.aspx
exec_code=Response.Write%28new+ActiveXObject%28%22WScript
.Shell%22%29.Exec%28%22cmd.exe+
%2Fc+whoami%22%29.StdOut.ReadAll%28%29%29%3B 443 - [IP
Address] python-requests/2.25.1 -2000 0 562
```

While Avalon is unable to confirm with a high degree of forensic certainty, the **IOAs** identified are similar to an automated exploitation of **ProxyLogon** (Github).



README.md

```
EVIL CORP
      AUTOMATIC OWA PROXYLOGON EXPLOIT
            @lotusdll, @knowhere team, @hiephoinongdan

[*] Target: https://mail.evil.corp:443
(*) Getting FQDN Name: ECorp
(+) Target is Vuln to SSRF [CVE-2021-26855]!
(*) Getting Information Server
(+) Computer Name = EXCHANGE
(+) Domain Name =  exchange.evilcorp.local
(+) Guest SID = S-1-5-18-rJqNiZqNgbKelpOMic7RvKu20ZOQnJ6Tgc7Gy83Pyc7Nx86Bzc/NztLPzNLOyqvOz8XMzcXLyQ--
+  exchange.evilcorp.local
(+) Put Domain Server without Subdomain: evilcorp.local
(*) Find valid mail from users list
-----------------------------------
(-) administrator@evilcorp.local - The email address is invalid!
(-) localhost@evilcorp.local - The email address is invalid!
(-) admin@evilcorp.local - The email address is invalid!
(-) Guest@evilcorp.local - The email address is invalid!
(+) accounting@evilcorp.local - Valid Mail!
(+) Found User SID = S-1-5-21-4069934074-2056971103-3948042655-1197
(*) Tested ProxyLogon!
(+) Fixed SID = S-1-5-21-4069934074-2056971103-3948042655-500
(+) Login Success!
```

3. EXPLOITATION & INSTALLATION

Anomalous programs found on client Exchange server:

TightVNC

Advanced Port Scanner

PsExec64.exe

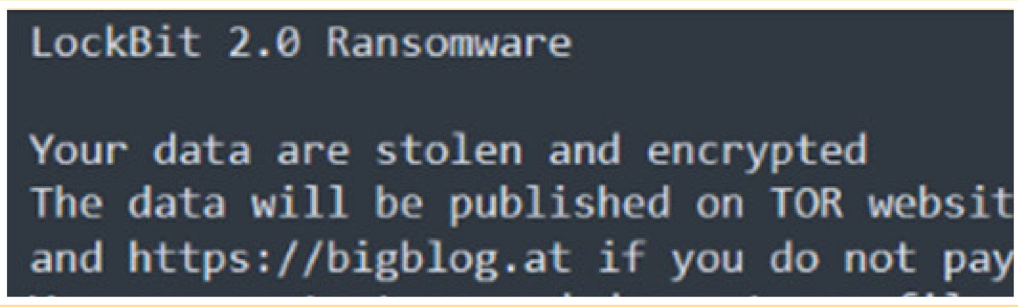
LocalRdpscan474.exe

mimikatz_trunk.zip

AnyDesk

Malicious application **ACB65E.exe** discovered on 16 hosts, which Avalon determined to be the ransomware executable **LockBit2.0.**

Appends file names with **.lockbit** extension and writes ransom note: **Restore-My-Files.txt**



```
LockBit 2.0 Ransomware

Your data are stolen and encrypted
The data will be published on TOR websit
and https://bigblog.at if you do not pay
```

4. DATA EXFILTRATION

(through examination of log/trace files)

mimikatz dump file: **bb.txt**

AnyDesk user interaction:
`app.ctrl_clip_com – Got a text offer clipbrd.capture`

Additional *.zip files removed

LOCKBIT 2.0

TASK SCHEDULER
Creation of new
`*\GroupPolicy\GPUdate *\<Task_Binary>`

TASK KILL
Attempts to delete backups and silence AV

EXPANDED TASK KILL LIST FOR LOCKBIT

https://gist.github.com/whichbuffer/c6d6839de5b58a5fa5fad971c07825ab