THREAT ALERT: Aggressive Qakbot Campaign and the Black Basta Ransomware Group Targeting U.S. Companies

cybereason.com/blog/threat-alert-aggressive-qakbot-campaign-and-the-black-basta-ransomware-group-targeting-u.s.-companies

Written By
Cybereason Global SOC Team

November 23, 2022 | 11 minute read

The Cybereason Global SOC (GSOC) team is investigating Qakbot infections observed in customer environments related to a potentially widespread ransomware campaign run by Black Basta. The campaign is primarily targeting U.S.-based companies.

Black Basta is a ransomware group that emerged in April 2022 and specifically targets organizations in the United States, Canada, United Kingdom, Australia, and New Zealand. The group is known for using double-extortion tactics: they steal sensitive files and information from victims and later use it to extort victims by threatening to publish the data unless the victim pays the ransom.

In this latest campaign, the Black Basta ransomware gang is using QakBot malware to create an initial point of entry and move laterally within an organization's network. QakBot, also known as QBot or Pinkslipbot, is a banking trojan primarily used to steal victims' financial data, including browser information, keystrokes, and credentials. Once QakBot has successfully infected an environment, the malware installs a backdoor allowing the threat actor to drop additional malware—namely, ransomware.

In this threat alert, the Cybereason team describes one attack scenario that started from a QBot infection, resulting in multiple key machines loading Cobalt Strike, which finally led to the global deployment of Black Basta ransomware. To make the recovery more difficult, the threat actor also locked the victim out of the network by disabling DNS services. We observed this tactic used on more than one victim.

The creation of this threat alert was motivated by the large number of organizations whose IT infrastructures were impacted by this recent Qakbot campaign and by the aggressiveness of the threat actor behind it, often leading to ransomware (Black Basta in our case, but it could lead to other ransomware strains).

KEY OBSERVATIONS

Threat actor moves extremely fast: In the different cases of compromise we identified, the threat actor obtained domain administrator privileges in less than two hours and moved to ransomware deployment in less than 12 hours.

High Severity: The Cybereason GSOC assesses the threat level as **HIGH** given the potentially widespread campaign being run by Black Basta.

- **Widespread QBot campaign targeting U.S.-based companies**: Threat actors leveraging the QBot loader casted a large net targeting mainly on U.S.-based companies and acted quickly on any spear phishing victims they compromised. In the last two weeks, we observed more than 10 different customers affected by this recent campaign.
- **Network lockout**: Among the many Qakbot infections we identified, two allowed the threat actor to deploy ransomware and then lock the victim out of its network by disabling the victim's DNS service, making the recovery even more complex.
- **Black Basta deployment**: One particularly fast compromise we observed led to the deployment of Black Basta ransomware. This allowed us to tie a link between threat actors leveraging Qakbot and Black Basta operators.

Given all of these observations, we recommend that security and detection teams keep an eye out for this campaign, since it can quickly lead to severe IT infrastructure damage.

ANALYSIS

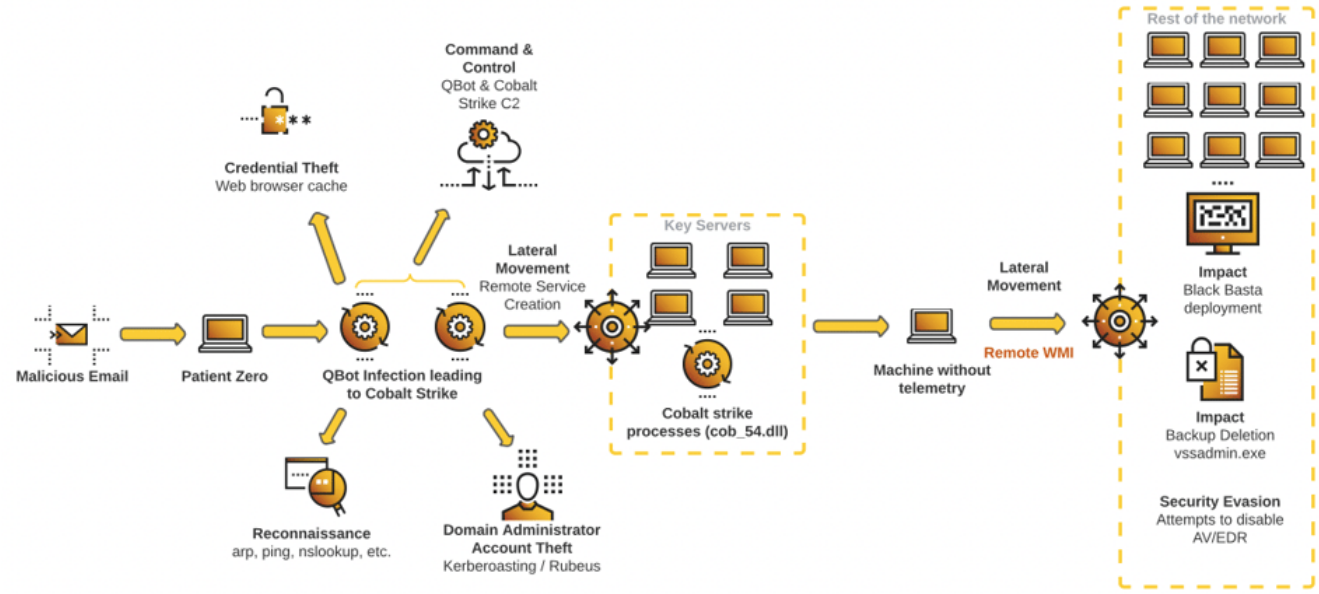
The Cybereason Managed Services team observed multiple infections of Black Basta using QakBot beginning on November 14, 2022. These QakBot infections began with a spam/phishing email containing malicious URL links. Qakbot was the primary method Black Basta used to maintain a presence on victims' networks.

That said, we also observed the threat actor using Cobalt Strike during the compromise to gain remote access to the domain controller. Finally, ransomware was deployed and the attacker then disabled security mechanisms, such as EDR and antivirus programs.

This Threat Alert is broken down into three main parts:

- **Infection Vector**, related to QBot deployment and post-exploitation on the patient zero machine
- **Lateral Movement**, related to the key machines the threat actor leveraged to complete the domain compromise
- **Global Ransomware Deployment**, related to the large-scale deployment of the Black Basta ransomware, along with attempts to deactivate security mechanisms

This attack diagram summarizes the actions carried out by Black Basta affiliates:

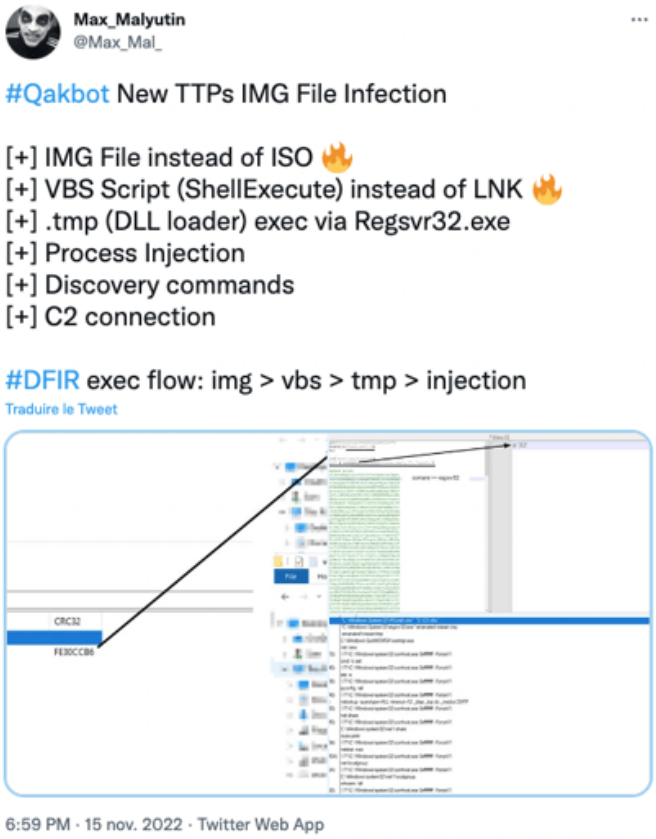


Attack Scenario Diagram

Infection Vector

QBot Deployment

Recently, security researchers have observed aggressive QBot campaigns, and the Cybereason team was able to map the identified activity to public CTI posts:



Source: Twitter

(https://twitter.com/Max_Mal_/status/1592577982912425984)

Using this source to infer the original phishing vector, we concluded that the attacker uses an IMG file (Disk Image File, similar to the ISO format) as the initial compromise vector. We also identified other QBot infection vectors starting from ISO files, depending on the campaign. Prior to Microsoft patch regarding MOTW (Mark of the web), files inside of these types of image files (ISO/IMG) were not marked properly with Mark of The Web, a system to allow Windows to flag a file with metadata such as download URL, and warn users prior to opening the file. After this patch fixed the bug, the threat actors have moved to a zero day for MOTW that allows a user to bypass the Microsoft security flags with a malformed signature inside the malicious files.

Additionally, QBot recently changed the way it is loading its malicious payload from JavaScript to VBS.

The malicious VBS file is delivered via an image file mounted to the D: drive. The regsvr32.exe process then executes another randomly named file from the same mount, in a randomly named folder–in this case “\inducted\aficionado.tmp”. The subsequent regsvr32.exe child process contains the Qbot module most commonly seen in recent attacks: fwpolicyiomgr.dll.

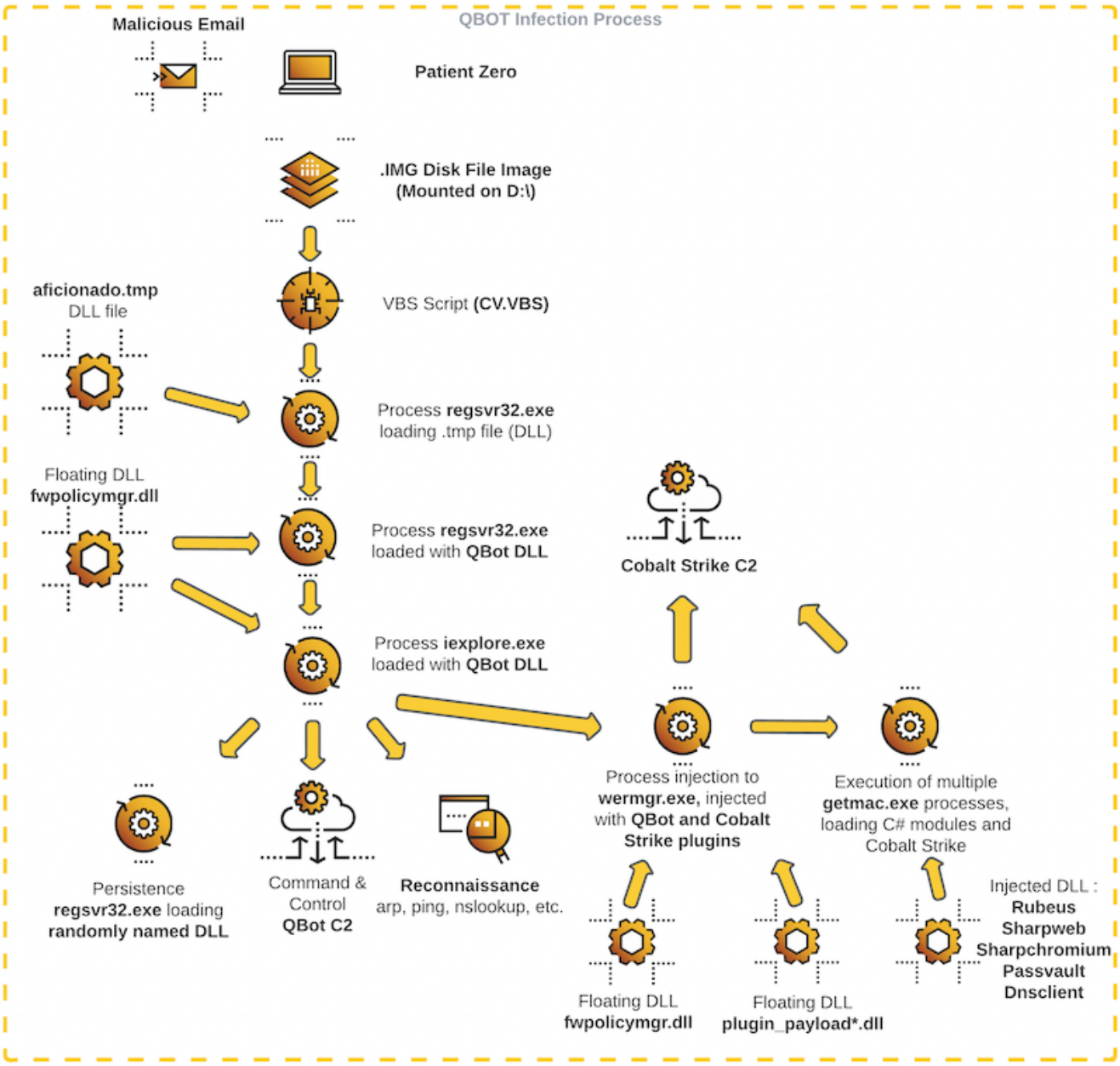
This file is named after a legitimate Windows file normally located in “C:\Windows\System32\FWPolicyIOMgr.dll”, but crucially in the case of Qbot, it is loaded as floating code without an image file on disk.

QBot full infection process tree, as seen from the Cybereason Defense Platform

In the example above:

- The processes included in the process tree from wscript.exe to wermgr.exe are related to QBot.
- The processes included in the process tree from wermgr.exe to getmac.exe are related to Cobalt Strike.

This diagram explains the infection vector:



QBot Infection Process

Subsequently, the fwpolicyiomgr.dll module is injected into the iexplore.exe process which connects to a multitude of Qbot C2 servers, many of which see no significant data sent/transferred. There are also connections to many legitimate websites such as yahoo.com, xfinity.com, irs.gov, and more. For a full list of Qbot C2 servers, refer to “Associated IPs” below.

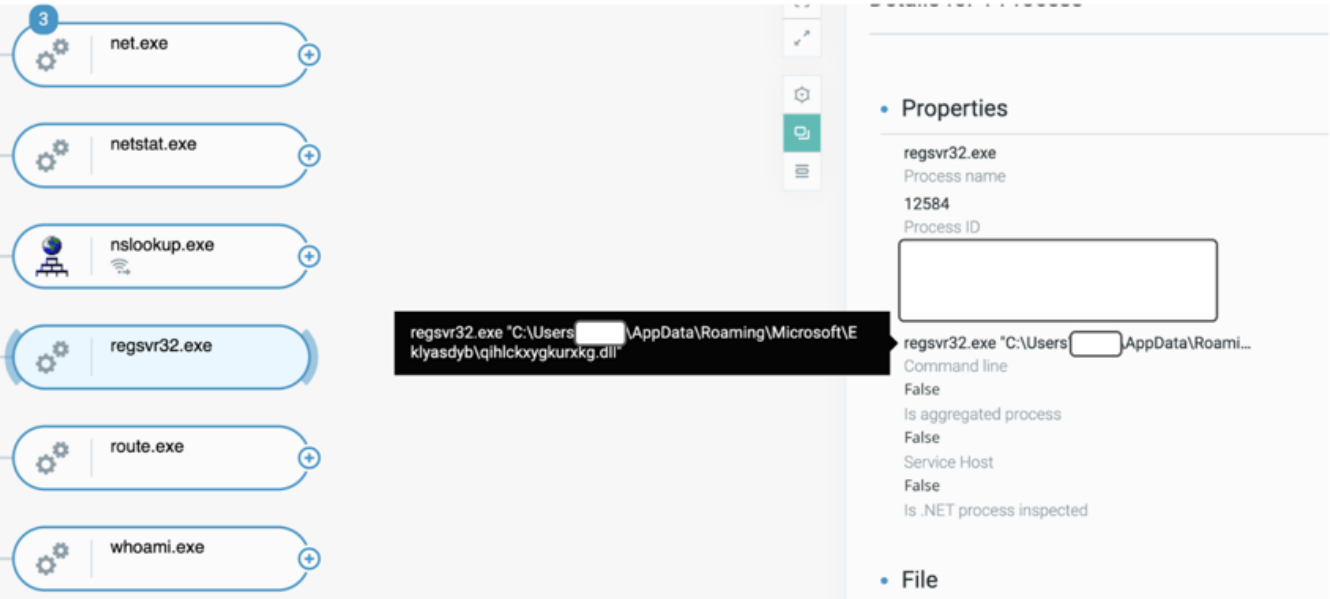
Port type	Owner proce...	Received...	Server addre...	DNS query	Transmitted bytes
HTTP	iexplore.exe	5 MB	74.6.143.25	yahoo.com > 74.6....	
Service	iexplore.exe	5 MB	172.90.139.138	172.90.139.138 > 1...	
HTTP	iexplore.exe	3 MB	74.6.143.26	www.yahoo.com > ...	
HTTP	iexplore.exe	2 MB	68.47.128.161		
HTTP	iexplore.exe	1387 KB	184.50.221.203	www.xfinity.com > ...	
HTTP	iexplore.exe	1104 KB	94.63.65.146	94.63.65.146 > 94....	
HTTP	iexplore.exe	936 KB	184.31.138.127	www.xfinity.com > ...	

List of domain/IP addresses that iexplore.exe communicates with, including legitimate and QBot C2s

The iexplore.exe process executes Qbot discovery commands as follows:

- net view
- cmd /c set
- arp -a
- ipconfig /all
- nslookup -querytype=ALL -timeout=12 _ldap._tcp.dc._msdcs.{Domain}
- net share
- route print
- netstat -nao
- net localgroup
- whoami /all

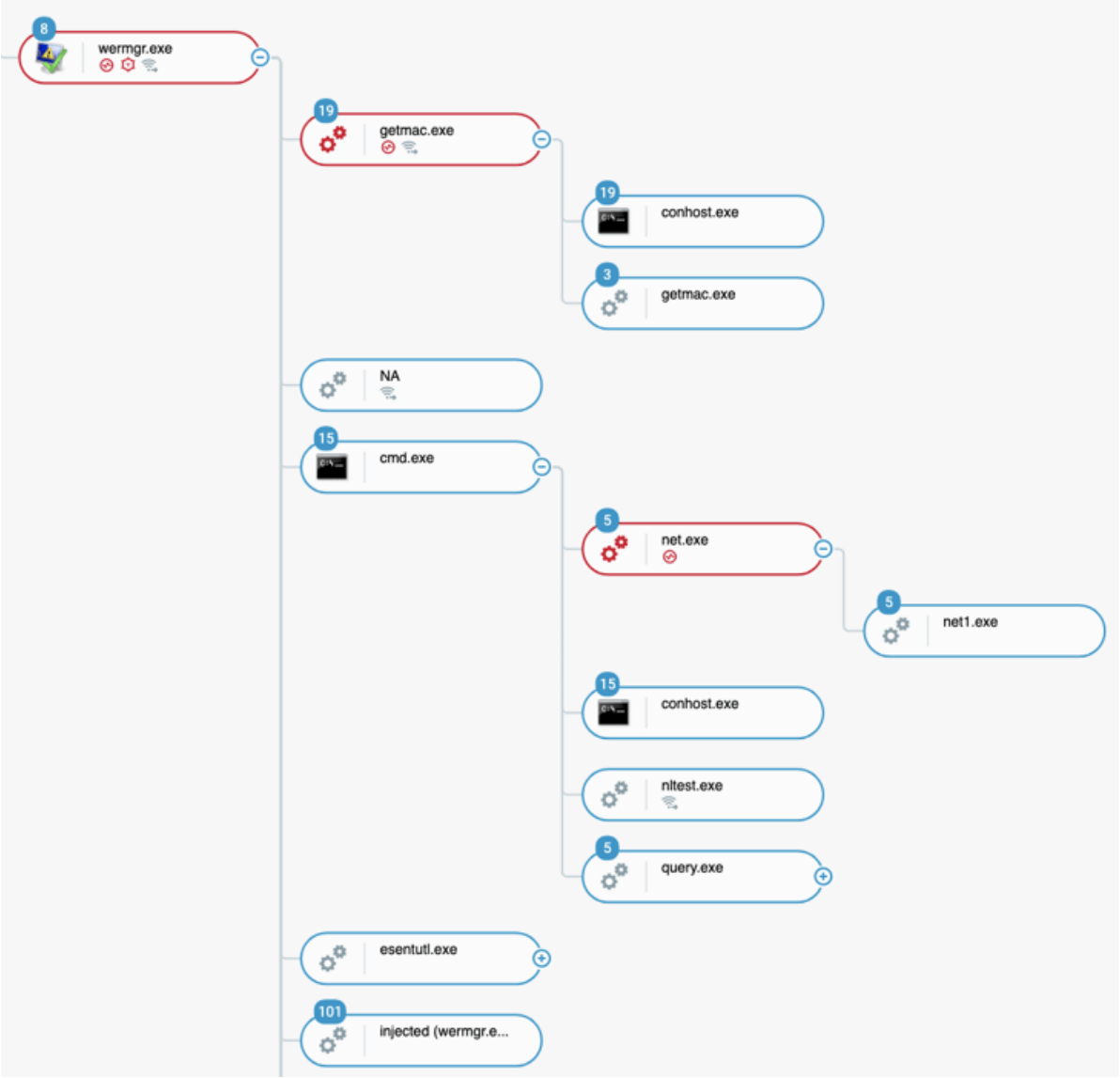
Additionally, iexplore.exe spawns another instance of Qbot through regsvr32.exe, which in that case failed to load:



Regsvr32.exe trying to load a DLL

This activity, Regsvr32.exe trying to load a DLL, is most likely related to QBot persistence mechanisms.

The Wermgr.exe process then starts and loads the Qbot module fwpolicyiomgr.dll, along with two new floating payloads (plugin_payload54.dll and plugin_payload55.dll). It also connects to the C2 domain jesofidiwi[.]com.



Full process tree as seen from the Cybereason Platform after QBot loading

The Jesofidiwi[.]com domain is the main domain used by the threat actor to persist on the network, and the Cybereason team noticed that it is embedded in recent Bumblebee samples.

Malware Configuration File

Family

CobaltStrike

C2urls

http://108.177.235.29:443/preserve/somebody/UIOOT18Z

Extract from
https://www.virustotal.com/gui/file/4a2e23d604d2d2774df43b5c539f9726c6033db55b483c49e4e84314265f6f6e/details

According to the VirusTotal information, this C2address relates to Cobalt Strike, which we will confirm in the next part of this report.

The Wermgr.exe process injects into the getmac.exe process, a Windows binary used for getting MAC addresses and network adapter information.

Getmac.exe loads a number of open source C# frameworks for stealing browser credentials, Kerberos interaction, password management, compression libraries along with .NET namespaces, and more.

Loading the frameworks helps the threat actors remain fileless to accomplish their goal in-memory.

The full list of loaded modules includes:

sharpweb {FLOATING}

sharpchromium {FLOATING}

passvault {FLOATING}

rubeus {FLOATING}

processes {FLOATING}

goc {FLOATING}

dnsclient {FLOATING}

commandline {FLOATING}

newtonsoft.json {FLOATING}

abc {FLOATING}

system.threading.tasks.dataflow {FLOATING}

- *icsharpcode.sharpziplib {FLOATING}*
- *system.buffers {FLOATING}*

Getmac.exe with network scanning suspicions

The cmd.exe process is executed with various reconnaissance and clean-up commands based on what was discovered during the discovery phase, including users and machines that were later compromised:

- C:\WINDOWS\system32\cmd.exe /C del *.txt
- C:\WINDOWS\system32\cmd.exe /C del OTllMzNkZjMtZTZhMi00NzhkLTgyZjAtZjlkOTZmYTU4ODY0.bin
- C:\WINDOWS\system32\cmd.exe /C net accounts /domain
- C:\WINDOWS\system32\cmd.exe /C net group "Domain Admins" /do
- C:\WINDOWS\system32\cmd.exe /C net group "domain controllers" /domain
- C:\WINDOWS\system32\cmd.exe /C net user {user} /domain
- C:\WINDOWS\system32\cmd.exe /C net user {user} /domain
- C:\WINDOWS\system32\cmd.exe /C nltest /dclist:{domain}
- C:\WINDOWS\system32\cmd.exe /C query user /server:{IP}

PowerShell is used to query information against Active Directory Domain Services with the System.DirectoryServices.DirectorySearcher class. The results are then saved as ccccOUT.csv.

```
powershell -nop -exec bypass -EncodedCommand $so = New-Object
System.DirectoryServices.DirectorySearcher; $so.filter = "(&(samAccountType=805306369))"; $so.FindAll() |
Select -Property @{N='Name'; E={$_.properties.samaccountname}},@{N='OS'; E=
{$_.properties.operatingsystem}},@{N='Descr'; E={$_.properties.description}},@{N='LastTime'; E={;
[datetime]::FromFileTime($_.properties.lastlogontimestamp -as [string]).ToString('yyyy-MM-dd
HH:mm')}},@{N='IP'; E={$_.properties.ipv4address}},@{N='ManagedBy'; E=
{$_.properties.managedby}},@{N='primarygroup'; E={$_.properties.primarygroup}} | Export-csv ccccOUT.csv -
encoding utf8
```

credential Harvesting

The below esentutl.exe command is used to get the victim's internet history data by combining separate log, database, and system files to form a cohesive history for later use. The file that will contain the history data is WebCacheV01.dat.

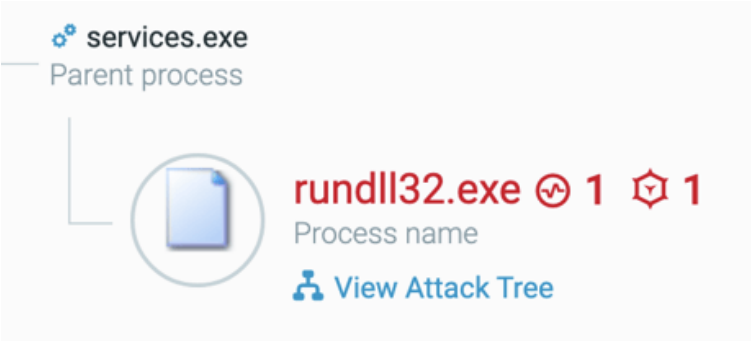
```
esentutl.exe /r V01 /l"C:\Users\[REDACTED]\AppData\Local\Microsoft\Windows\WebCache" /s"C:\Users\
[REDACTED]\AppData\Local\Microsoft\Windows\WebCache" /d"C:\Users\
[REDACTED]\AppData\Local\Microsoft\Windows\WebCache"
```

Lateral Movement

The attackers were able to compromise a domain admin account, which was possibly used to drop a Cobalt Strike payload to several servers, including a domain controller, in the customer environment.

This was done by placing the Cobalt Strike payload in the public folder and executing it with the rundll32.exe SetVolume commands through remote services deployed from the initial machine.

```
C:\Windows\SysWOW64\rundll32.exe C:\users\public\cob_54.dll,SetVolume
```



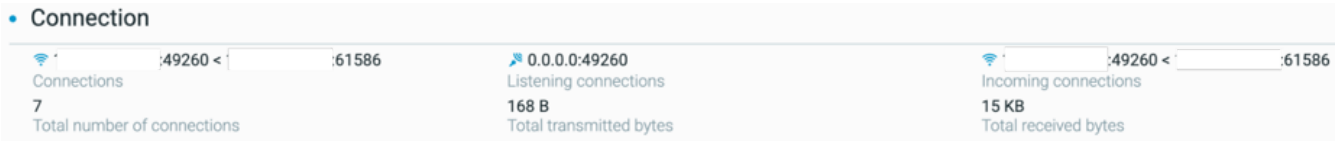
Rundll32.exe Malop with services.exe parent

MS-SCMR RStartServiceW 44		2 processes	367abb81-9844-3...	TCP x43, LRPC x1	Success x44
MS-SCMR RStartServiceW		getmac.exe	367abb81-9844-3...	TCP	Success
MS-SCMR RStartServiceW		getmac.exe	367abb81-9844-3...	TCP	Success

Getmac.exe sending StartService Remote Procedure Call to one of the compromised servers

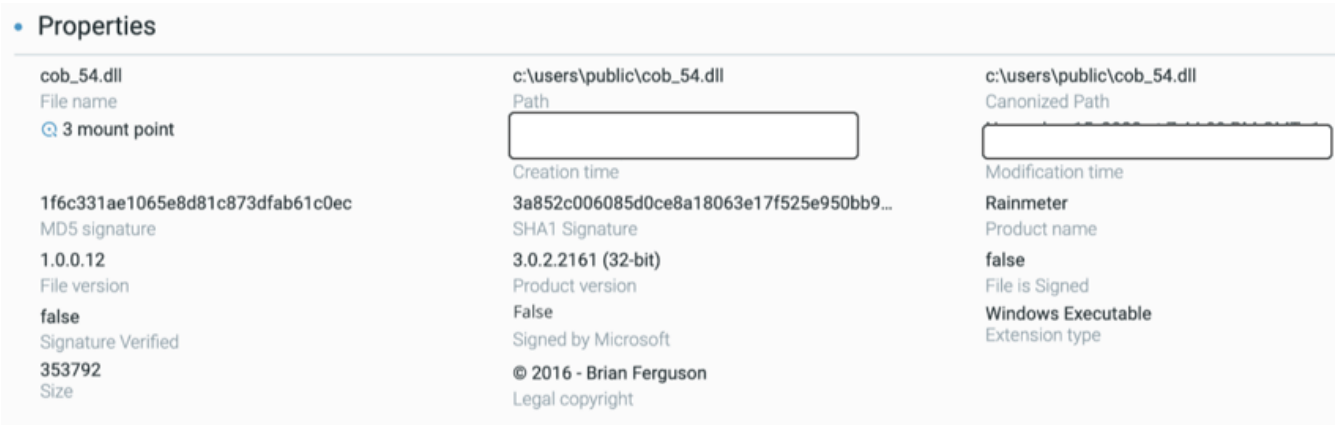
Direction	Owner machine	Owner proce...	Remote port	Port type	Received bytes
Outgoing		getmac.exe	135	Service	280 B

Outgoing connection to the compromised server over port 135 (RPC).



The connection being received by the services.exe process on the compromised server

A quick analysis of the DLL files shows that the application masquerades as the Rainmeter program:



DLL File Property of cob_54.dll

In another case, we identified what seems to be the x86 version of this DLL, named cob_56.dll.

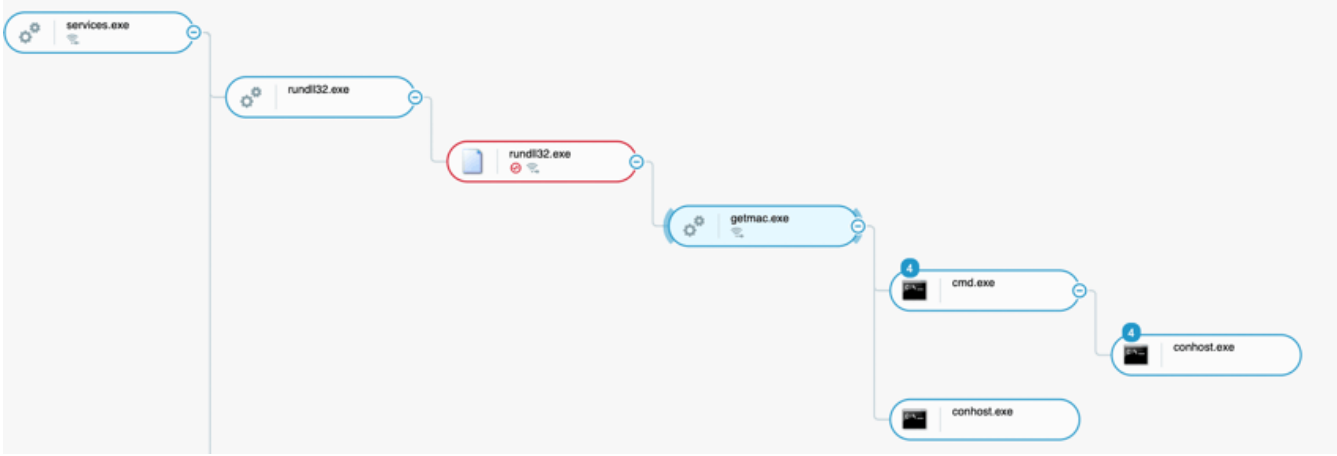
Finally, affected rundll32.exe processes actively communicated with their C2 server,

tevokaxol[.]com and jesofidiwi[.]com:

Direction	Server addre...	Server port	Port type	Received bytes	Transmitted bytes	Remote addr...	T1043 - Commo...	Owner machi...	Owner proce...	DNS query
Outgoing x1	108.177.235.29	443	HTTP x1	542 KB	12 KB		False x1		rundll32.exe	108.177.235.29 > 108.177.235.29
Outgoing x1	108.177.235.29	443	HTTP x1	538 KB	9 KB		False x1		rundll32.exe	jesofidiwi.com > 108.177.235.29
Outgoing x1	108.62.118.197	443	HTTP x1	536 KB	9 KB		False x1		rundll32.exe	tevokaxol.com > 108.62.118.197
Outgoing x1	108.62.118.197	443	HTTP x1	541 KB	12 KB		False x1		rundll32.exe	tevokaxol.com > 108.62.118.197
Outgoing x1	108.62.118.197	443	HTTP x1	554 KB	7 KB		False x1		rundll32.exe	tevokaxol.com > 108.62.118.197
Outgoing x1	108.177.235.29	443	HTTP x1	537 KB	10 KB		False x1		rundll32.exe	jesofidiwi.com > 108.177.235.29
Outgoing x1	108.62.118.197	443	HTTP x1	546 KB	14 KB		False x1		rundll32.exe	tevokaxol.com > 108.62.118.197
Outgoing x1	108.62.118.197	443	HTTP x1	534 KB	8 KB		False x1		rundll32.exe	108.62.118.197 > 108.62.118.197

Communication from the rundll32.exe process to their C2

This process is used to deploy more floating code into the getmac.exe process, as seen on patient zero:



Rundll32.exe with the malicious Cobalt Strike modules, spawning getmac.exe as well as injecting code into the process

Global Deployment of Black Basta

The final phase of the attack was to infect as many machines as possible, using the information and credentials gathered during the first two initial infection phases.

This chapter describes the different steps the threat actor took to globally deploy the Black Basta ransomware.

Identifying Security Mechanisms

The Cybereason team identified the threat actor looking for the EDR installed on the machine, through the wmic.exe executable.

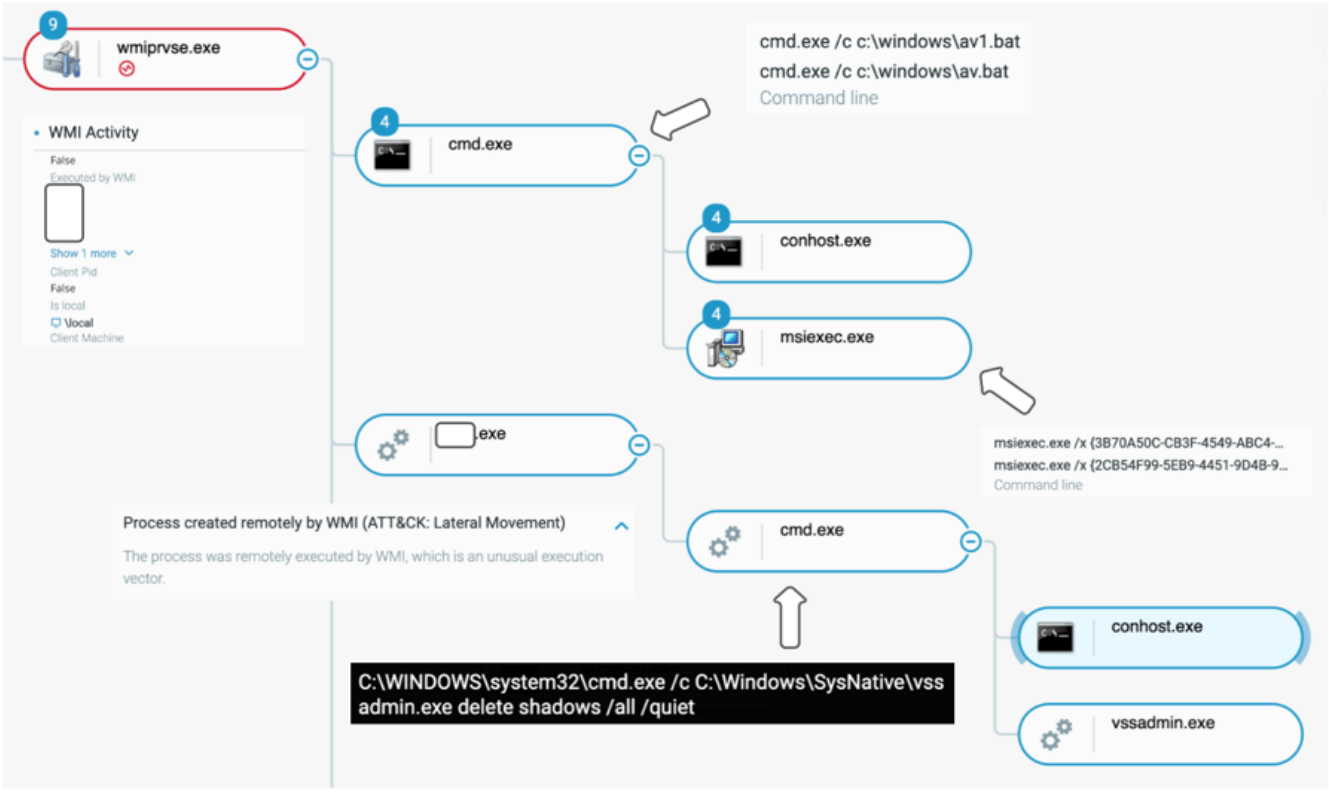
The Cybereason team identified the threat actor manually spawning a cmd.exe process on one server, looking for the presence of Cybereason EDR:

Process tree showing the threat actor launching cmd.exe then wmic.exe to identify the presence of Cybereason

It is likely the threat actor was looking for machines without a sensor to deploy additional malicious tools without being detected.

Spreading through WMI

Through the investigation, the Cybereason team identified that the threat actor moved laterally on many machines through Windows Management Instrumentation (WMI):



Process created through remote WMI

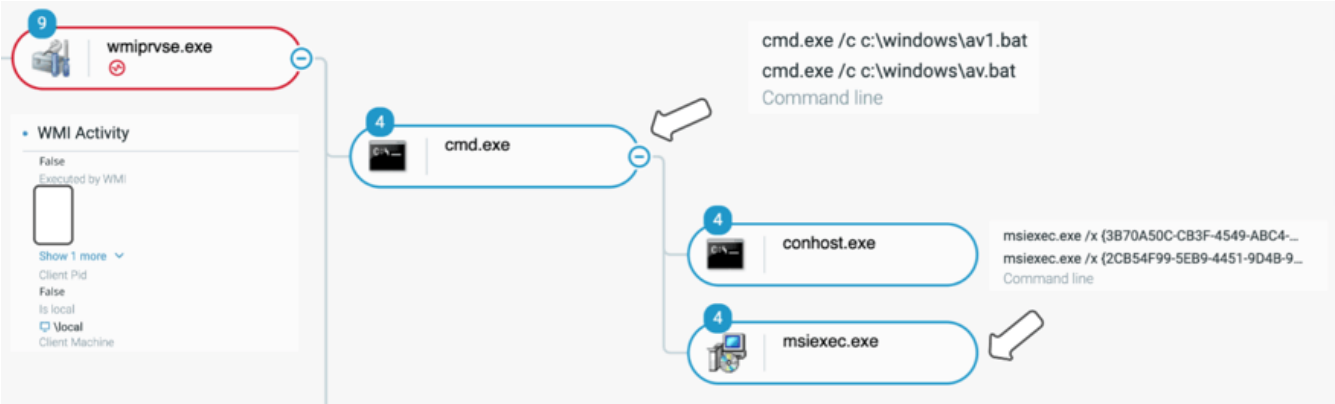
WMI is leveraged to execute the malicious commands and the ransomware [REDACTED].exe. (We redacted the file name to maintain customer confidentiality.)

The threat actor deployed the ransomware through what we call a pivot machine, a machine that didn't have a sensor. In that case, that machine was obsolete and had access to every other machine in the network.

The Cybereason team identified many connections to TCP port 135 from this pivot machine, designed to map the internal network for potential targets.

Attempts to Disable Security Mechanisms

At this point, the threat actor was targeting most of the machines it could reach and made its first attempts to disable the EDR sensor and antivirus software using two scripts, av.bat and av1.bat.



Process tree showing a remote WMI call to launch 2 bat files, av.bat and av1.bat

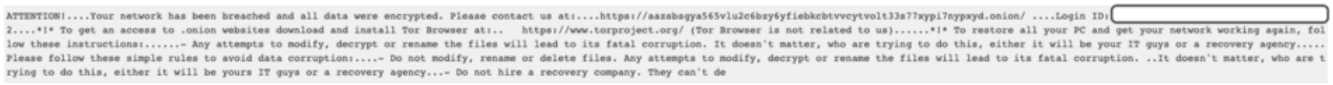
As seen on the capture above, the script calls the msiexec.exe, trying to uninstall the corresponding package of the EDR/antivirus.

Data Encryption: Black Basta

This threat alert mostly focuses on the deployment of the ransomware, rather than on the analysis of the ransomware binary itself, which explains the short size of this subchapter.

Creating the Ransom Note

Black Basta generates the ransom note file, named readme.txt, in each folder Black Basta reaches on the machine. The image below shows what the content of the file looks like:



Preview from the dropped ransom note

The embedded TOR address links clearly to Black Basta, on the analyzed sample:

hxxps://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd[.]onion

Encrypting the Files

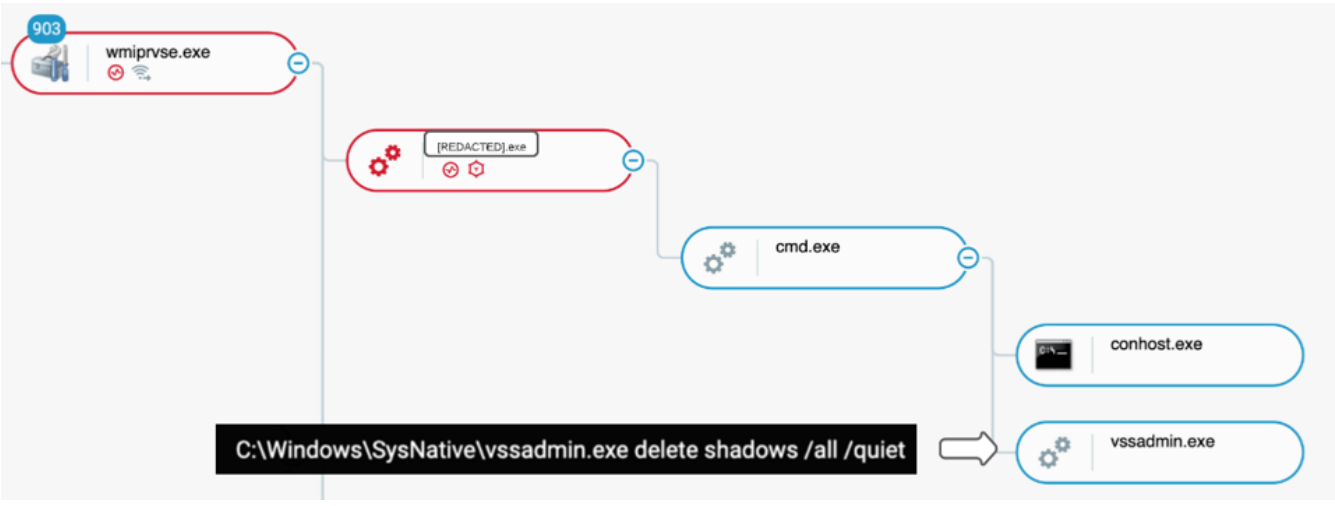
After creating the ransom note, the actual file encryption process ignites. Black Basta encrypts the files on the machine and adds a random extension to each file.

On top of that, Black Basta replaces the desktop wallpaper and avoids some specific folders like C:\Windows or the Recycle Bin.

Volume Shadow Copy Deletion

In order to delete the machine's shadow copies, Black Basta executes the process vssadmin.exe with the command line :*Vssadmin delete shadows /all /quiet*

As seen in the process tree below, the process [REDACTED].exe spawns a cmd.exe process right after the launch begins.



Cybereason process tree showing [REDACTED].exe launching cmd.exe which calls vssadmin.exe

On the observed machine, encryption did not have time to trigger because the process was prevented immediately after its launch.

CYBEREASON RECOMMENDATIONS

The Cybereason Defense Platform can detect and prevent Qakbot post-exploitations and Black Basta impact. Cybereason recommends the following actions:

- **Enhance Cybereason sensor policies**: Set the **Cybereason Anti-Ransomware protection mode to Prevent**. More information for Cybereason customers can be found on the NEST.
- **Enable Variant Payload Protection (VPP) in your Cybereason sensor policy**: Upgrade to a version that has VPP and enable it, as this will completely prevent Black Basta ransomware execution. VPP is supported in version 21.2.100 and above (Beta, and disabled by default) and 22.1.183 and above (GA, and enabled by default). More information can be found on the NEST.
- **Block compromised users**: Block users whose machines were involved in the attack, in order to stop or at least slow down attacker propagation over the network.
- **Identify and block malicious network connections**: Identify network flows toward malicious IPs or domains identified in the reports and block connections to stop the attacker from controlling the compromised machines.
- **Reset Active Directory access**: If Domain Controllers (DCs) were accessed by the attacker and potentially all accounts have been stolen, it is recommended that, when rebuilding the network, all AD accesses are reset. Important note: krbtgt account needs to be reset twice and in a timely fashion.
- **Engage Incident Response**: It is important to investigate the actions of the attacker thoroughly to ensure you've not missed any activity and you've patched everything that needs to be patched.
- **Cleanse compromised machines:** Isolate and re-image all infected machines, to limit the risk of a second compromise or the attacker getting subsequent access to the network.
- **Hunt proactively:** Use the Investigation screen in the Cybereason Defense Platform and the queries in the **Hunting Queries section of the NEST version of this article** to search for assets that have potentially been exploited. Based on the search results, take further remediation actions, such as isolating the infected machines, and deleting the payload file.
- **Add IOCs**: Add the aforementioned IoCs to the custom reputation with "**Block and Prevent**."
- **Disable disk image file auto-mounting**: To prevent this infection technique from succeeding, consider disabling auto-mounting of disk image files (primarily .iso, .img, .vhd, and .vhdx) globally through GPOs.

    This can be achieved by modifying the registry values related to the Windows Explorer file associations in order to disable the automatic Explorer "Mount and Burn" dialog for these file extensions. (This will not deactivate the mount functionality itself.)

IOCs

We recommend blocking the following domains and IP addresses using your network infrastructure:

Associated Domains:

- jesofidiwi[.]com (Cobalt Strike C2)
- dimingol[.]com (Cobalt Strike-related domain used for DNS exfiltration)
- tevokaxol[.]com (Cobalt Strike C2)
- vopaxafi[.]com (Cobalt Strike C2)

Associated IPs:

- 108.177.235.29

- 144.202.42.216
- 108.62.118.197

Qakbot C2 addresses

Server address	Port Number
94.70.37.145	2222
172.90.139.138	2222
70.50.3.214	2222
90.89.95.158	2222
200.93.14.206	2222
142.161.27.232	2222
82.127.174.33	2222
92.207.132.174	2222
92.189.214.236	2222
24.64.114.59	2222
82.31.37.241	443
87.223.80.45	443
76.9.168.249	443
174.115.87.57	443
82.41.186.124	443
131.106.168.223	443
75.98.154.19	443
170.253.25.35	443

86.133.237.3	443
73.88.173.113	443
84.209.52.11	443
180.151.104.143	443
105.184.161.242	443
24.49.232.96	443
157.231.42.190	443
75.143.236.149	443
70.64.77.115	443
137.186.193.226	3389
91.165.188.74	50000

Add the following hashes to the blocklist in your Cybereason environment:

Associated Hashes (SHA1):

- 75b2593da627472b1c990f244e24d4e971c939e7 (aficionado.tmp)
- 3a852c006085d0ce8a18063e17f525e950bb914c (cob_54.dll)
- 4202bf2408750589e36750d077746266176ac239 (cob_56.dll)

Hunt for the following files (those are also mentioned in the Hunting Queries chapter):

Associated file names:

- Aficionado.tmp (Qbot loader)
- fwpolicyiomgr.dll (Qbot module)
- plugin_payload54.dll
- Plugin_payload55.dll
- cob_54.dll

These indicators can be used for threat hunting purposes.

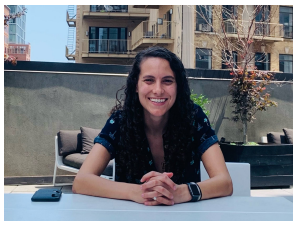
ABOUT THE RESEARCHERS

Loïc Castel, IR Security Analyst, Cybereason IR Team 

Loïc Castel is a Security Analyst with the Cybereason IR team. Loïc analyses and researches critical incidents and cybercriminals, in order to better detect compromises. In his career, Loïc worked as a security auditor in well-known organizations such as ANSSI (French National Agency for the Security of Information Systems) and as Lead Digital Forensics & Incident Response at Atos. Loïc loves digital forensics and incident response, but is also interested in offensive aspects such as vulnerability research.

Joakim Kandefelt, Blue Team Security Analyst, Cybereason Blue Team 

Joakim Kandefelt is a Blue Team Investigator with the Cybereason Global SOC team. He has been with Cybereason for more than 5 years, starting as an analyst within the APAC GSOC specializing in Reverse Engineering and Threat Hunting, and venturing into CTI and IR. As part of his current, more advanced role, he enjoys leveraging IR methodology to detect Red Team TTPs and working to ensure customers are safe. He maintains his passion for Reverse Engineering and Threat Hunting.


Danielle Frankel, GSOC AMER Security Services Account Manager, Cybereason Global SOC

Danielle Frankel is a Security Services Assurance Manager (SSAM) for the Cybereason Global SOC. As a SSAM, she serves as a focal point for services related escalations with exceptional business impact, working with customers and internal teams to resolve the issues. Previously, Danielle worked as a Customer Success Manager and as a Tier 1 SOC Analyst at Cybereason. Danielle is passionate about cybersecurity, and earned her Masters Degree in Counterterrorism and Cyber Security at Reichman University (IDC Herzeliya).

About the Author

Cybereason Global SOC Team

The Cybereason Global SOC Team delivers 24/7 Managed Detection and Response services to customers on every continent. Led by cybersecurity experts with experience working for government, the military and multiple industry verticals, the Cybereason Global SOC Team continuously hunts for the most sophisticated and pervasive threats to support our mission to end cyberattacks on the endpoint, across the enterprise, and everywhere the battle moves.

All Posts by Cybereason Global SOC Team