CyberProof

Advanced Threat Hunting

CyberProof Guidelines for Threat Hunting

July 2021

UNCLASSIFIED

Table of Contents

Session Stakeholders **3**
Hunting Via the SIEM Platform 3
Hunting Via the EDR Platform 3
Cuba Ransomware **4**
Threat Explained 4
Correlated MITRE Techniques 4
Operational Hunting Workflows 5
Hunting Via the SIEM Platform 6
Network Activity (Relevant Data Sources: Firewall, Proxy) 6
Processes (Relevant Data Sources: Security Event Logs, Sysmon) 6
Services (Relevant Data Sources: Security Event Logs, Sysmon) 6
Email Gateway (Relevant Data Sources: Email Gateway) 7
Hunting Via the EDR Platform 7
Filenames 7
Hashes 7
Network Activity 8
Services 8
Mitigation 8
Yara Rule 9
Microsoft PrintNightmare Vulnerability **10**
Threat Explained 10
Correlated MITRE Techniques 10
Operational Hunting Workflows 11
Hunting Via the SIEM Platform 11
Event Logs (Relevant Data Sources: Security Event Logs, PrintService Logs, Sysmon) 11
Hunting Via the EDR Platform 12
Executions 12
Mitigation 12
Appendix **15**
List of Services Terminated by Cuba Ransomware 16
List of Processes Terminated by Cuba Ransomware 16
References **17**

Session Stakeholders

This report was created for threat hunters and security analysts with highly technical skills – skills that can be used to identify threats by developing hypotheses, locating infection evidence across environments, and providing indicators for attack detection. These guidelines should provide the logic for hunting malware samples or malicious techniques and can be converted into detection rules or mitigation strategies as well.

Hunting Via the SIEM Platform

Security information and event management (SIEM) is a software solution that aggregates and analyzes activity from various log sources across an entire IT infrastructure. SIEM platforms collect security data from network devices, servers, domain controllers, and more. CyberProof's guidelines assume that environmental data is collected into the SIEM platform, but if there is no SIEM platform (or the relevant data is not gathered), you should develop guidelines in order to limit the hunt to the relevant data sources.

Hunting Via the EDR Platform

Endpoint Detection and Response (EDR) refers to a category of tools used to detect and investigate threats on endpoints. EDR tools typically provide detection, investigation, threat hunting, and response capabilities.

For additional malware review, please refer to CyberProof's weekly CTI report or to the Appendix at the end of this document.

For more details or assistance regarding hunting workflows, please contact the CyberProof Threat Hunting team at TH_Mailbox@cyberproof.com.

Cuba Ransomware

Threat Explained

Cuba ransomware is written in C++ and is used as the final-stage payload in double extortion campaigns. Operators use Cuba ransomware in conjunction with a leak site that publishes data extracted from compromised systems prior to encryption. Cuba has affected organizations in North America, South America, and Europe. It has also affected various sectors, including pharmaceutical, manufacturing, and logistics. Recently, it has been delivered by the Hancitor downloader in spam email campaigns.

While Cuba ransomware has purportedly been active for a few years, they have only recently gained notoriety, primarily for publishing leaked documents from infected companies that resisted their blackmail attempts.

Correlated MITRE Techniques

Tactic	Technique	Description
Initial Access	Spear Phishing (T1566)	Cuba ransomware being delivered by phishing
Execution	Command and Scripting Interpreter: PowerShell (T1059.001)	Threat actors are using PowerShell payloads to drop Cuba ransomware
Execution	System Services: Service Execution (T1569.002)	Cuba ransomware executes services
Execution	Shared Modules (T1129)	Cuba ransomware links function at runtime
Execution	Command and Scripting Interpreter (T1059)	Cuba ransomware accepts command line arguments
Persistence	Create or Modify System Process: Windows Service (T1543.003)	Cuba ransomware can modify services
Privilege Escalation	Access Token Manipulation (T1134)	Cuba ransomware can adjust access privileges
Defense Evasion	File and Directory Permissions Modification (T1222)	Cuba ransomware will set file attributes

Tactic	Technique	Description
Defense Evasion	Obfuscated Files or Information (T1027)	Cuba ransomware is using XOR algorithm to encode the data
Defense Evasion	Virtualization/Sandbox Evasion: System Checks	Cuba ransomware executes anti-VM instructions
Defense Evasion	Impair Defenses: Disable or Modify System Firewall (T1562.004)	Cuba ransomware adding firewall rule
Command and Control	Non-Application Layer Protocol (T1095)	Communication over dedicated protocol
Command and Control	Application-Layer Protocol: DNS (T1071.004)	outbound network activity to the malicious domain
Discovery	File and Directory Discovery (T1083)	Cuba ransomware enumerates files
Discovery	Process Discovery (T1057)	Cuba ransomware enumerates process modules
Discovery	System Information Discovery (T1082)	Cuba ransomware can get keyboard layout, and enumerate disks
Discovery	System Service Discovery (T1007)	Cuba ransomware can query service status
Collection	Input Capture: Keylogging (T1056.001)	Cuba ransomware logs keystrokes via polling
Impact	Service Stop (T1489)	Cuba ransomware can stop services
Impact	Data Encrypted for Impact (T1486)	Cuba ransomware encrypts data

Operational Hunting Workflows

The CyberProof Threat Hunting team worked collaboratively with the Cyber Threat Intelligence (CTI) team to import the external sources of information that the hunt was based on, as described below. We categorized the hunt according to the type of platform in which the indicators need to be verified: SIEM platform or EDR platform.

The Cuba ransomware campaign started in December 2019; however, the CTI team identified additional waves of attacks in 2020 and 2021. Our threat hunting session includes all of the indicators since 2020.

Hunting Via the SIEM Platform

Network Activity (Relevant Data Sources: Firewall, Proxy)

- Adding a firewall rule[1]
  - Hunt in firewall logs for adding or modifying firewall rules to allow RDP connections over port 3389
- Malicious network communications[2]
  - Hunt in firewall logs for connections over port 5050
  - Hunt in firewall logs and in the proxy logs for communication to the malicious IP address 185.153.196[.]182
  - Hunt in proxy logs for outbound network activity to the malicious domain kurvalarva[.]com

Processes (Relevant Data Sources: Security Event Logs, Sysmon)

- Hunt for events that indicate process termination[3] for the processes list provided in the Appendix:
  - In security event logs `Event ID 4689`
  - When the Sysmon is configured as `Event ID 5`

Services (Relevant Data Sources: Security Event Logs, Sysmon)

- Hunt for events that indicate service termination[4] for the services list provided in the Appendix:
  - In system event logs `Event ID 6006`
  - When the Sysmon is configured as `Event ID 4`

---

1 (T1562.004) Impair Defenses: Disable or Modify System Firewall;
(T1071.004) Application Layer Protocol: DNS
2 (T1095) Non-Application Layer Protocol
3 (T1489) Service Stop
4 (T1489) Service Stop

Email Gateway (Relevant Data Sources: Email Gateway)

- Hunt for email gateway logs, for the following sender email addresses[5]:
  - admin@cuba-supp[.]com
  - cuba_support@exploit[.]im
  - fedelsupportagent@cock[.]li
  - helpadmin2@cock[.]li
  - helpadmin2@protonmail[.]com
  - iracomp2@protonmail[.]ch
  - under_amur@protonmail[.]ch

Hunting Via the EDR Platform

Filenames

- Hunt for the creation of the file extension ".cuba"[6]
- Hunt for the creation or execution[7] of the following filenames:
  - !!FAQ for Decryption!!.txt (Ransom note)
  - Socks1.ps1
  - 151.bat
  - 151.ps1
  - kurva.ps1
  - 182.bat
  - 182.ps1
  - Or use regex of 3 digits: \d{3}.(ps1|bat)

Hashes

- Hunt for script execution by using the SHA256 hash[8]:
  - 54627975c0befee0075d6da1a53af9403f047d9e367389e48ae0d25c2a7154bc
  - c385ef710cbdd8ba7759e084051f5742b6fa8a6b65340a9795f48d0a425fec61

5 (T1566) Phishing
6 (T1486) Data encrypted for Impact
7 (T1059.001) Command and Scripting Interpreter: PowerShell
8 (T1059) Command and Scripting Interpreter

- 40101fb3629cdb7d53c3af19dea2b6245a8d8aa9f28febd052bb9d792cfbefa6

Network Activity

- Malicious network communications[9]
  - Hunt for network communication with the malicious IP address 185.153.196[.]182
  - Hunt for outbound network activity to the malicious domain kurvalarva[.]com
  - Hunt for connections over port 5050

Services

- Service termination[10]
  - Hunt for events that indicate service termination for the services list provided in the Appendix

Mitigation

- Security awareness training is one of the most cost-effective ways to reduce your chance of suffering a ransomware attack. By training your users to avoid phishing, you can often prevent an attack before it even happens.
- Ensure that you are keeping all IT systems and servers up to date with the latest patches.
- Backups should be maintained offline or on separate networks, as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups eliminates the need to pay a ransom for data that is readily accessible to your organization.
- Add additional layers of protection to your email by using content filter software.
- Use granular network segmentation to minimize the chances that laterally spreading malware can propagate. Attackers can use a continuous network to spread throughout your entire infrastructure. You can prevent this by segmenting your network. You might also consider placing your industrial assets and IoT devices on their own segments.
- During a ransomware event, a Windows firewall policy can be configured to restrict the scope of communications permitted between common endpoints within an environment. This firewall policy can be enforced locally or centrally

9 (T1095) Non-Application Layer Protocol; (T1071.004) Application Layer Protocol: DNS
10 (T1489) Service Stop

via Group Policy. At a minimum, common ports and protocols (e.g., RDP port 3389) should be blocked between workstation-to-workstation and workstations-to-non-domain controllers and non-file servers.

Yara Rule

This ransomware has had many variants - from December 2019 to March 2021. Hunt for the latest variants of the malware using the Yara rule in the EDR platform, or the equivalent Yara scan platform. Below are the combined Yara rules for all of the previous variants of Cuba ransomware.

```
import "pe"

rule Mal_W32_Ransom_Cuba
 {
    meta:
        description = "Cuba Ransomware"
        author = "Blackberry Threat Research"
        date = "2021-04-12"

   strings:

       //Good day. All your files are encrypted. For decryption contact us.
        $x0 =
{476f6f64206461792e20416c6c20796f75722066696c6573206172652065 6e637279707465642e20466f72206465637279707469
6f6e20636f6e746163742075732e}
        //We also inform that your databases, ftp server and file server were downloaded by us to our servers.
        $x1 =
{576520616c736f20696e666f726d207468617420796f7572206461746162617365732c206674702073657276657220616e64206
6696c65207365727665722077657265726520646f
 776e6c6f6164656420627920757320746f206f75722073657276657 2732e}
        //FIDEL.CA
        $x2 = {464944454c2e4341}
        //!!FAQ for Decryption!!.txt
        $x3 =
{210021004600410051002000660 06f00720020004400650063007200790070007400690 06f006e00210021002e007400780074
00}
        //MySQL80
        $x4 = {4d007900530051004c0038003000}
        //MSSQLSERVER
        $x5 = {4d005300530051004c005300450052005600450052 00}
        //SQLWriter
        $x6 = {530051004c005700720069007400650072 00}
        //SQLBrowser
        $x7 = {530051004c00420072006f007700730065007200}
        //sqlservr.exe
        $x8 = {730071006c007300650072007600720 02e00650078006500}

   condition:
        uint16(0) == 0x5A4D and
        filesize < 3MB and
        pe.imports("mpr.dll", "WnetEnumResourceW") and
        pe.imports("mpr.dll", "WNetCloseEnum") and
```

```
        pe.imports("mpr.dll", "WNetOpenEnumW") and
        pe.imports("netapi32.dll", "NetShareEnum") and

    8 of ($x*)
}
```

Microsoft PrintNightmare Vulnerability

Threat Explained

Microsoft reported about CVE-2021-1675 (now termed CVE-2021-34527), on June 21; PrintNightmare was updated to critical severity as the potential for remote code execution was uncovered. Microsoft's patch did not successfully resolve the issue for CVE-2021-34527 PrintNightmare, but it did resolve CVE-2021-1675.

PrintNightmare allows the attacker to run any code with SYSTEM privileges (Local Privileges Escalation & Remote Code Execution). The PrintNightmare vulnerability affects the Windows Print Spooler in all versions of Windows, including the versions installed on personal computers, enterprise networks, Windows servers, and domain controllers.

Correlated MITRE Techniques

Tactic	Technique	Description
Persistence, Privilege Escalation	Boot or Logon Autostart Execution: Print Processors (T1547.012)	Identifies a print spooler adding a new printer driver
Persistence, Privilege Escalation	Boot or Logon Autostart Execution: Print Processors (T1547.012)	Detects when a new printer plug-in has failed to load
Persistence, Privilege Escalation	Boot or Logon Autostart Execution: Print Processors (T1547.012)	Detects spoolsv with a child process of rundll32.exe
Persistence, Privilege Escalation	Boot or Logon Autostart Execution: Print Processors (T1547.012)	Identifies potentially suspicious module loads into spoolsv.exe, based on a DLL loading from a specific path used by CVE-2021-34527

Tactic	Technique	Description
Privilege Escalation	Exploitation for Privilege Escalation (T1068)	Identifies suspicious process access events from Spoolsv.exe to a target process
Persistence, Privilege Escalation	Boot or Logon Autostart Execution: Print Processors (T1547.012)	Detects spoolsv.exe writing a DLL
Defense Evasion	Signed Binary Proxy Execution: rundll32 (T1218.011)	Identifies rundll32.exe with no command line arguments

Operational Hunting Workflows

The CyberProof Threat Hunting team worked collaboratively with the CTI team to import the external sources of information that the hunt was based on - as described below. We categorized the hunt according to the type of platform in which the indicators need to be verified: SIEM platform or EDR platform.

Hunting Via the SIEM Platform

Event Logs (Relevant Data Sources: Security Event Logs, PrintService Logs, Sysmon)

(*) For visibility on the following logs, please ensure that you have Microsoft-Windows-PrintService/Operational logging enabled.

- Attempts to use Remote Procedure Call (RPC)
  - Hunt for Windows Security `Event ID 5712`
- Adding a new printer driver[11]
  - Hunt for Microsoft-Windows-PrintService/ Operational `Event ID 316`
  - If you cannot enable this logging, another option is to use Sysmon logs. You can hunt for the "spoolsv.exe" process loading module using "ImageLoad" - Sysmon `Event ID 7`
- The print spooler failed to load a plug-in module
  - Hunt for Microsoft-Windows-PrintService/ Operational `Event ID 808` or `Event ID 4909`

11 (T1547.012) Boot or Logon Autostart Execution: Print Processors

Hunting Via the EDR Platform

Executions

- spoolsv.exe launching rundll32.exe[12]
  - With empty command line
  - With command line: rundll32.exe
- Creation of suspicious DLL files spawned in a dedicated folder
  - Hunt for the filename with the ".DLL" extension that was created in the folder path: C:\Windows\system32\spool\drivers\x64*\
- Execution of "spoolsv.exe" with Process Integrity Level 'SYSTEM' [13]
- spoolsv.exe launching suspicious processes (child process):
  - Hunt for Spoolsv.exe launching one of the following processes: "gpupdate.exe", "whoami.exe", "nltest.exe", "taskkill.exe", "wmic.exe", "taskmgr.exe", "sc.exe", "findstr.exe", "curl.exe", "wget.exe", "certutil.exe", "bitsadmin.exe", "accesschk.exe", "wevtutil.exe", "bcdedit.exe", "fsutil.exe", "cipher.exe", "schtasks.exe", "write.exe", or "wuauclt.exe"
- Spoolsv.exe launching suspicious processes with exceptions:
  - Hunt for spoolsv.exe executing "net.exe" where the process command line is not "start"
  - Hunt for spoolsv.exe executing "cmd.exe" and the process command line is not one of the following: ".spl", "route add," or "program files"
  - Hunt for spoolsv.exe executing "netsh.exe" and the process command line is not one of the following: "add portopening" or "rule name"
  - Hunt for spoolsv.exe executing "powershell.exe" and the process command line is not ".spl"
- Suspicious DLL creation in folder:
  - Hunt for kernelbase.dll, unidrv.dll, and any other DLL written into the subfolders of C:\Windows\System32\spool\drivers\ - in the same timeframe that spoolsv.exe was executed.

Mitigation

The most effective mitigation strategy is to disable the print spooler service itself. This should be done on all endpoints, servers, and especially domain

12 (T1218.011) Signed Binary Proxy Execution: rundll32
13 (T1068) Exploitation for Privilege Escalation

controllers. Note that disabling the print spooler service disables the ability to print both locally and remotely. Dedicated print servers could still be vulnerable if the spooler is not stopped.

Below are the options for disabling the printer service:

- Windows CLI
  - Using CMD
    - net stop spooler
    - REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\Spooler" /v "Start" /t REG_DWORD /d "4" /f
    - sc config spooler start=disabled
    - sc spooler stop
  - Using PowerShell
    - Stop-Service -Name Spooler –Force
    - Set-Service -Name Spooler -StartupType Disabled
    - Uninstall-WindowsFeature Print-Services
- Hardening Policies
  - Block RPC and SMB ports at the firewall level.
    - Blocking both RPC 135/tcp and SMB 445/tcp at the firewall level can prevent remote exploitation of this vulnerability. Note that blocking these ports on a Windows system could prevent expected capabilities from functioning properly, especially on a system that functions as a server
  - Set a warning when installing drivers for a new connection through Group Policy and the Registry key
    - Navigate to 'Computer Configuration > Administrative Templates > Printers > Point and Print Restrictions,' and set "Do not show warning on elevation prompt" under "When installing drivers for a new connection."
    - Manually set a value of 0 to the NoWarningNoElevationOnInstall registry value under HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
    - Or use CMD to execute the following command line: *"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint" /v* NoWarningNoElevationOnInstall */t REG_DWORD /d 0 /f*
  - Disable inbound remote printing through Group Policy

        - Navigate to 'Computer Configuration/Administrative Templates/Printers,' and disable the "Allow Print Spooler to accept client connections" policy to block remote attacks.

    - Restrict the installation of new unsigned printer drivers
        - Install the July 2021 out-of-band update
        - Manually set a value of 1 or any non-zero value to the RestrictDriverInstallationToAdministrators registry value under HKEY_LOCAL_MACHINE \Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint
        - Use CMD to execute the following command line: *"HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint" /v RestrictDriverInstallationToAdministrators /t REG_DWORD /d 1 /f*

Appendix

Appendix A: IOC Types

IOC Type	Event Source	Query Timeframes
IP Address	Firewall Traffic Firewall Threat Protection DNS Queries Proxy Queries Authentication Logs EDR Logs	30-60 Days
Domain	DNS Queries Proxy Queries EDR Logs	30-60 Days
URL	Firewall Threat Protection DNS Queries Proxy Queries EDR Logs	30-60 Days
HASH (MD5, SHA1, SHA265)	Firewall Threat Protection Email Threat Protection EDR Logs Anti-Virus Logs	30-60 Days
Email address	Email Gateway Email Threat Protection Authentication Logs	30-90 Days

Appendix B: List of Services Terminated by Cuba Ransomware

- MySQL
- MySQL80
- SQLSERVERAGENT
- MSSQLSERVER
- SQLWriter
- SQLTELEMETRY
- MSDTC
- SQLBrowser
- vmcompute
- vmms
- MSExchangeUMCR
- MSExchangeUM
- MSExchangeTransportLogSearch
- MSExchangeTransport
- MSExchangeThrottling
- MSExchangeSubmission
- MSExchangeServiceHost
- MSExchangeRPC
- MSExchangeRepl
- MSExchangePOP3BE
- MSExchangePop3
- MSExchangeNotificationsBroker
- MSExchangeMailboxReplication
- MSExchangeMailboxAssistants
- MSExchangeIS
- MSExchangeIMAP4BE
- MSExchangeImap4
- MSExchangeHMRecovery
- MSExchangeHM
- MSExchangeFrontEndTransport
- MSExchangeFastSearch
- MSExchangeEdgeSync
- MSExchangeDiagnostics
- MSExchangeDelivery
- MSExchangeDagMgmt
- MSExchangeCompliance
- MSExchangeAntispamUpdate

Appendix C: List of Processes Terminated by Cuba Ransomware

- sqlagent.exe
- sqlservr.exe
- sqlwriter.exe
- sqlceip.exe
- msdtc.exe
- sqlbrowser.exe
- vmwp.exe

- vmsp.exe
- outlook.exe

References

1. https://blogs.blackberry.com/en/2021/04/threat-thursday-blackberry-protect-vs-cuba-ransomware
2. https://digital.nhs.uk/cyber-alerts/2021/cc-3855#indicators-of-compromise
3. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cuba-ransomware.pdf
4. https://shared-public-reports.s3-eu-west-1.amazonaws.com/Cuba+Ransomware+Group+-+on+a+roll.pdf
5. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-cuba-ransomware-campaign/
6. https://medium.com/proferosec-osm/cuba-ransomware-group-on-a-roll-2b3d2b0e2312
7. https://blog.group-ib.com/hancitor-cuba-ransomware
8. https://shared-public-reports.s3-eu-west-1.amazonaws.com/Cuba+Ransomware+Group+-+on+a+roll.pdf
9. https://www.blumira.com/cve-2021-1675/
10. https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/tree/master/Exploits/Print%20Spooler%20RCE
11. https://www.splunk.com/en_us/blog/security/i-pity-the-spool-detecting-printnightmare-cve-2021-34527.html
12. https://www.kb.cert.org/vuls/id/383432
13. https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/07/printnightmare-0-day-can-be-used-to-take-over-windows-domain-controllers/
14. https://touchstonesecurity.com/mitigate-ransomware-attacks/