Cynet

CyOps

Monthly Cyber Threat Intelligence Report

July, 2021

INTRO

The purpose of this document is to provide a monthly summary of observed threats, vulnerabilities, and risks relevant to Cynet's customers. Throughout this report you will find detailed information regarding specific attack groups, campaigns, malware variants, etc., As well as the relevant sectors, industries, and infrastructures being targeted. The report is comprised out of data and observations gathered from our internal sources, and it is focused mainly but not solely on sectors which comprise our customer's base.

Microsoft Monthly security update

Microsoft have published **117** security updates for different vulnerabilities:

- **44** vulnerabilities provide an attacker to gain RCE
- **32** vulnerabilities are for privilege escalation
- **14** vulnerabilities are information disclosure
- **12** vulnerabilities are Denial of Services
- **8** vulnerabilities are security feature bypass
- **7** spoofing vulnerabilities

13 of the vulnerabilities are classified as critical:

- **CVE-2021-34474** - Dynamics Business Central Remote Code Execution Vulnerability
- **CVE-2021-34473** - Microsoft Exchange Server Remote Code Execution Vulnerability
- **CVE-2021-34448** - Scripting Engine Memory Corruption Vulnerability
- **CVE-2021-33740** - Windows Media Remote Code Execution Vulnerability
- **CVE-2021-34439** - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
- **CVE-2021-34503** - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
- **CVE-2021-34494** - Windows DNS Server Remote Code Execution Vulnerability
- **CVE-2021-34450** - Windows Hyper-V Remote Code Execution Vulnerability
- **CVE-2021-34522** - Microsoft Defender Remote Code Execution Vulnerability
- **CVE-2021-34464** - Microsoft Defender Remote Code Execution Vulnerability
- **CVE-2021-34458** - Windows Kernel Remote Code Execution Vulnerability
- **CVE-2021-34497** - Windows MSHTML Platform Remote Code Execution Vulnerability
- **CVE-2021-34527** - Windows Print Spooler Remote Code Execution Vulnerability

4 of the vulnerabilities are actively exploited by threat actors as Zero-Day.

- **3** vulnerabilities were not publicly disclosed:
  - **CVE-2021-33771** - Windows Kernel Elevation of Privilege Vulnerability
  - **CVE-2021-34448** - Scripting Engine Memory Corruption Vulnerability
  - **CVE-2021-31979** - Windows Kernel Elevation of Privilege Vulnerability
- The **POrintNightmare** vulnerability was publicly disclosed:
  - **CVE-2021-34527** - Windows Print Spooler Remote Code Execution Vulnerability.

CyOps Team

Cynet's 24/7 MDR with the latest security updates and reports

Contents

Printnightmare - Windows Print Spooler Patched Vulnerability Remains Exploitable

Introduction

On June 29th, security researchers demonstrated that the patch Microsoft released for a new vulnerability in the Windows Print Spooler service – which was classified as privilege escalation, and which provides authenticated attacker with the ability to perform RCE (remote code execution) in SYSTEM context – is in fact still exploitable.

The "PrintNightmare" remote code execution (RCE) vulnerability that affects Windows Print Spooler is different from the issue addressed by Microsoft as part of its Patch Tuesday update released earlier this month while warning about exploitation attempts targeting the flaw. Microsoft is tracking the security weakness under the identifier CVE-2021-34527.

CVE-2021-1675, originally classified as an elevation of privilege vulnerability and later revised to RCE, was remediated by Microsoft on June 8, 2021.

Microsoft noted in its advisory that PrintNightmare is distinct from CVE-2021-1675 since the latter resolves a separate vulnerability in RpcAddPrinterDriverEx() and that the attack vector is different.

On July 15th, Microsoft shared a security update guide on another vulnerability affecting the Windows Print Spooler service – CVE-2021-34481. This vulnerability can be exploited to achieve elevated privileges on the local machine.

Vulnerability overview

PrintNightmare" – CVE-2021-34527 is a vulnerability that allows an attacker with a low-privilege domain user account to take control over a server running the Windows Print Spooler service, which is running by default on all Windows servers and clients.

The Print Spooler service is vulnerable due to the fact that it fails to restrict access to the RpcAddPrinterDriverEx() function, which can allow a remote authenticated attacker to execute malicious code with SYSTEM privileges.

You can find a proof-of-concept exploit here.

In contrast to the recently patched 'PrintNightmare' vulnerability, the new shared vulnerability (CVE-2021-34481) is focused on gaining elevated privileges locally.

The privilege elevation vulnerability can be exploited once the Windows Print Spooler service inappropriately performs a privileged file operation. Prior to the exploit, the attacker must have access to the local machine to take advantage of this vulnerability. From the moment the attacker manages to successfully exploit this vulnerability, they can run arbitrary code with SYSTEM privileges. They could then view, change or delete data, install programs, or create new accounts with full user rights.

Vulnerability Patch

MSRC has released a patch that fixes the RCE "PrintNightmare" vulnerability. You can find the patch here.

As of now, MSRC hasn't released an official patch for the CVE-2021-34481 vulnerability. You may follow our recommendations to mitigate this vulnerability through Cynet360 Console.

Cynet Protection and Recommendations Protection

The Cynet research team already deployed new detection rules aimed to detect and prevent exploitation attempts of this vulnerability, and is currently working on additional detections to increase the visibility around it.

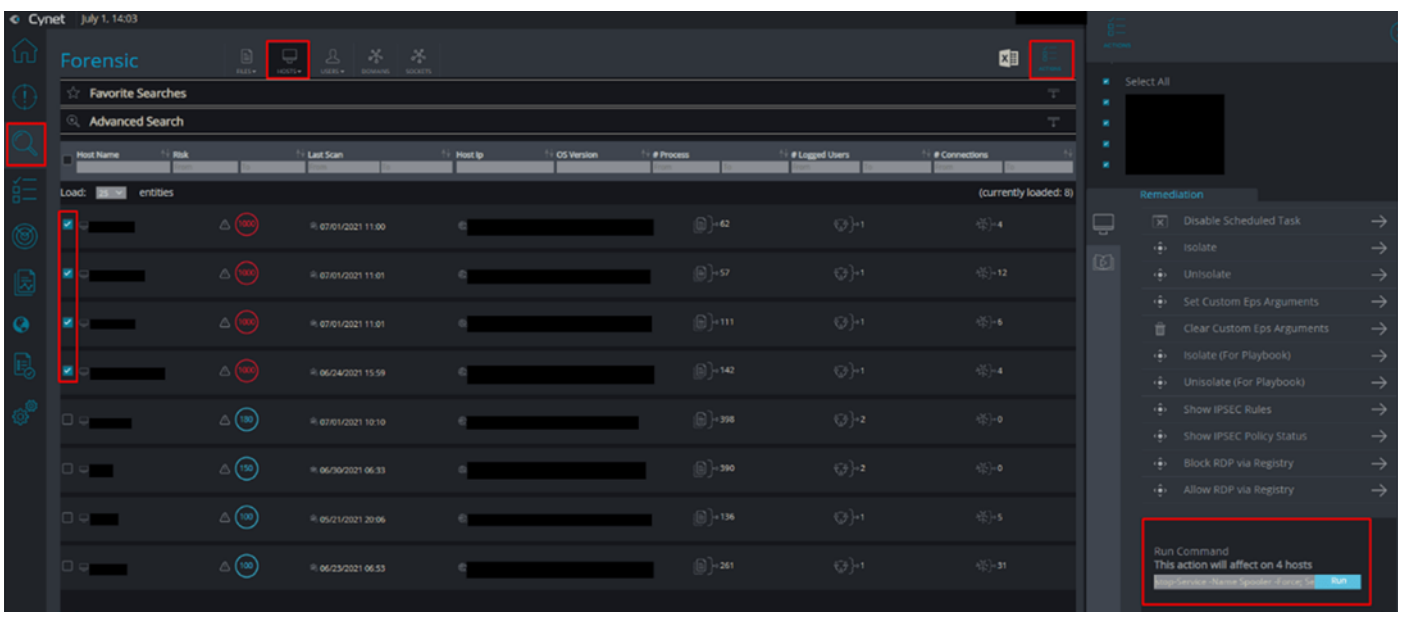
The CyOps team monitors our customers' environments 24/7 and will be in contact in case any indicators of this vulnerability are detected in your environment.

Recommendations

We highly recommend **disabling the Print Spooler service on all domain controllers (DC)** within the organization. Additionally, we recommend disabling this service on assets where it's not essential to maintain regular business operations.

Please follow these simple steps:

Forensics → Hosts → Tick all domain controllers → Actions → Run Command →
Powershell.exe Stop-Service -Name Spooler -Force; Set-Service -Name Spooler -StartupType Disabled



Forensics

Cynet360 Forensics can search for artifacts that can provide strong indicators of exploitation attempts of this vulnerability based on the POCs observed in the wild. The following path has been observed while using the POCs as a part of the exploit. The path can be used to store malicious dll's which in turn are being loaded by spoolsv.

Please follow these steps to find artifacts using Cynet360:

Figure 01: **Forensic → Files → Advanced Search → Common Path → Contains → \spool\drivers\x64\3\old\ → Save Policy/Search**

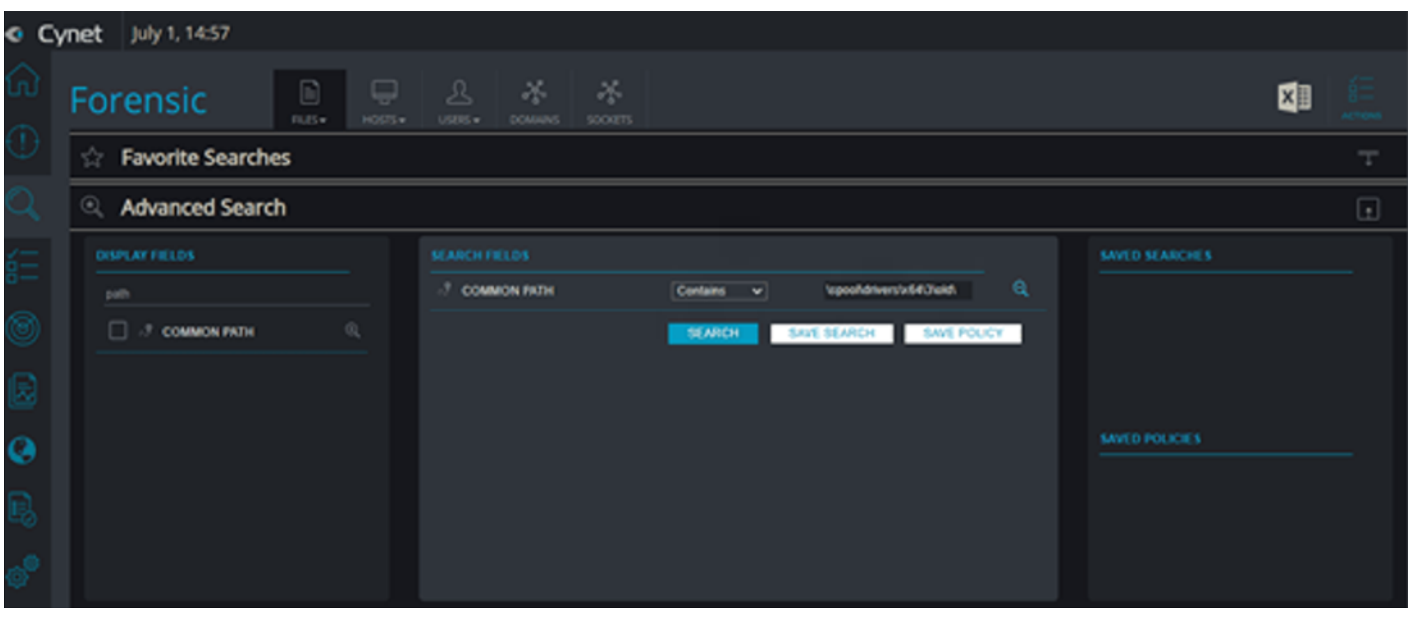


Figure 02: **Fill in the fields as shown below: Policy name: CVE-2021-1675 –PrintNightmare**

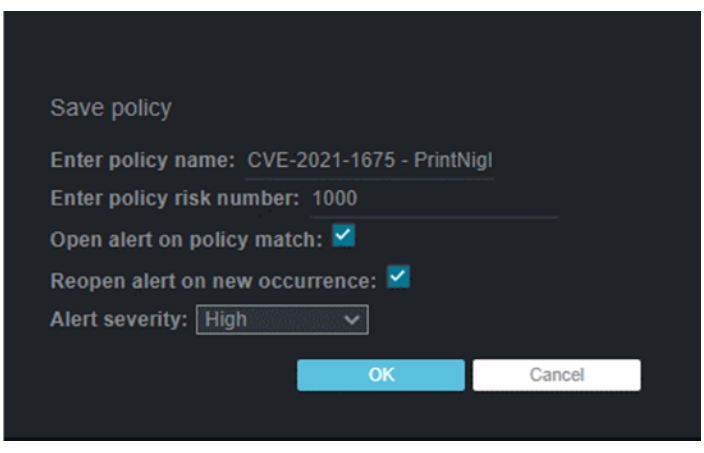
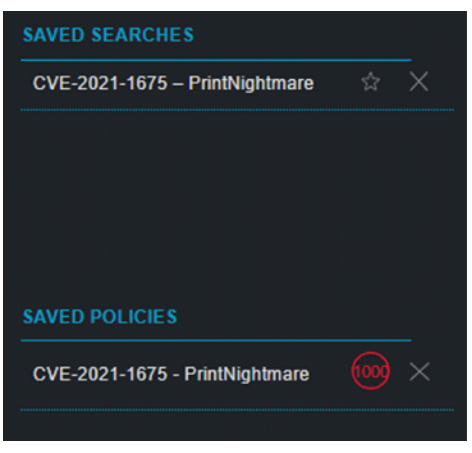
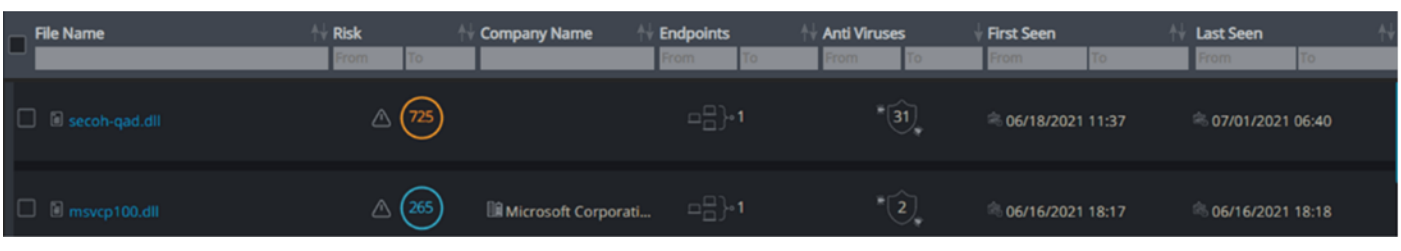


Figure 03: **You can find the saved policy/search in the Advanced Search of the Forensic:**



Cynet360 allows you to automatically investigate the dll's by presenting the risk score, company name and the number of vendors which classified it as malicious in VT (presented under the "Anti Viruses" field, the shied icon is clickable and allows you to navigate to the virustotal website).



If one of the detected dll's do not exist in VT or have a high-risk score and are unfamiliar to you, please feel free to contact the CyOps team.

Petitpotam NTLM Relay Aattack

On July 23rd, 2021, a new NTLM Relay PoC was published under the name PetitPotam which allows a remote Windows server authentication.

The PetitPotam attack allows threat actors to send SMB requests to remote victim machines, establish the authentication procedure and share authentication certificates or NTLM authentication details.
PetitPotam exploits Windows Servers where the Active Directory Certificate Services (AD CS) is not configured with protections for NTLM Relay Attacks.

Your environment is vulnerable to PetitPotam Attack if NTLM authentication is enabled in your domain, and you are using Active Directory Certificate Services (AD CS) with one of the following services:

- Certificate Authority Web Enrollment
- Certificate Enrollment Web Service

Mitigation

If your environment is vulnerable, we recommend following one of the mitigation steps published by Microsoft:

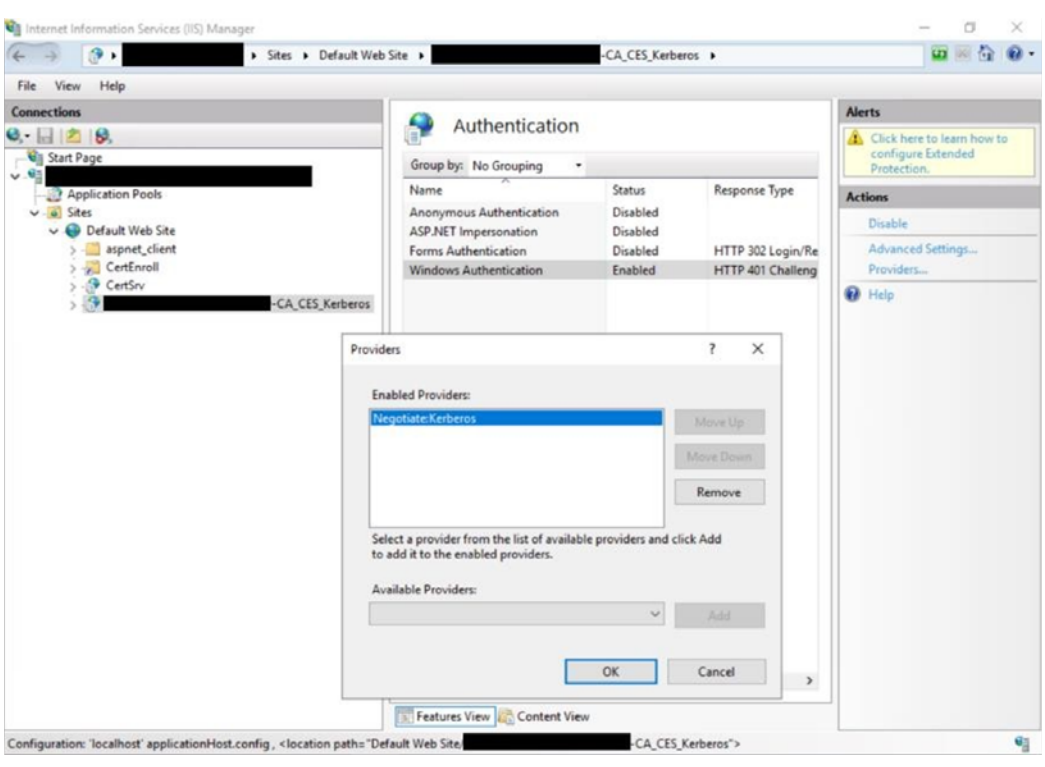
Preferred mitigation: we recommend you disable NTLM authentication on your Windows domain controller as the simplest mitigation. This can be accomplished by following the documentation in Network security: Restrict NTLM: NTLM authentication in this domain.

Other Mitigations: If you are unable to disable NTLM on your domain for compatibility reasons, you can do one of the following. They are listed in order of more secure to less secure:

- Disable NTLM on any AD CS Servers in your domain using the group policy Network security: Restrict NTLM: Incoming NTLM traffic. To configure this GPO, open Group Policy and go to Computer Configuration ⟶ Windows Settings ⟶ Security Settings ⟶ Local Policies ⟶ Security Options and set "Network security: Restrict NTLM: Incoming NTLM traffic" to "Deny All Accounts" or "Deny All domain accounts". If needed you can add exceptions as necessary using the setting "Network security: Restrict NTLM: Add server exceptions in this domain."

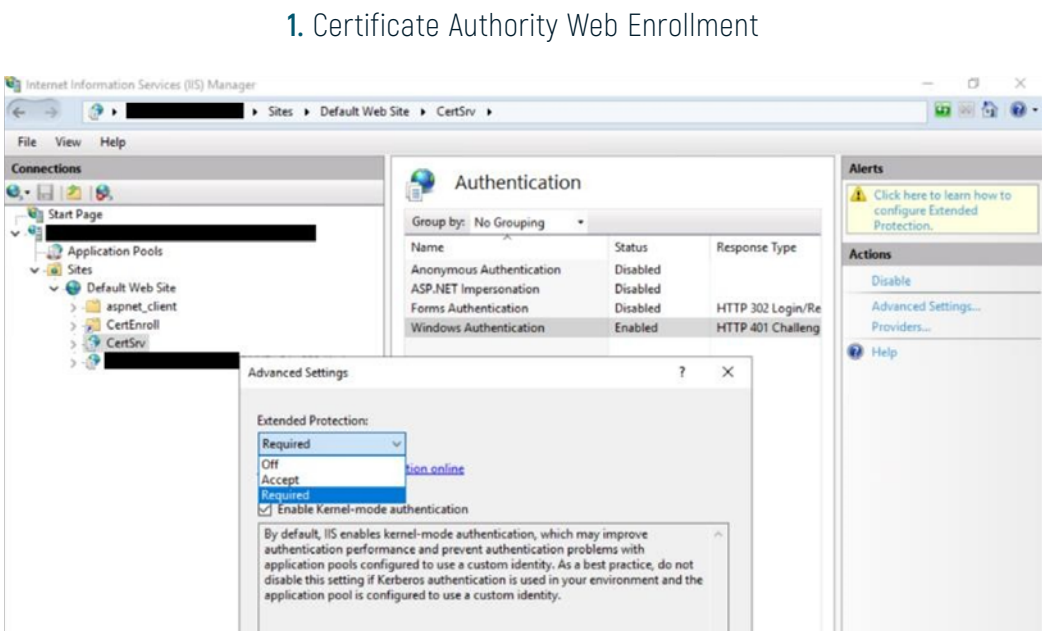
- Disable NTLM for Internet Information Services (IIS) on AD CS Servers in your domain running the "Certificate Authority Web Enrollment" or "Certificate Enrollment Web Service" services.

To do so open IIS Manager UI, set Windows authentication to "Negotiate:Kerberos":

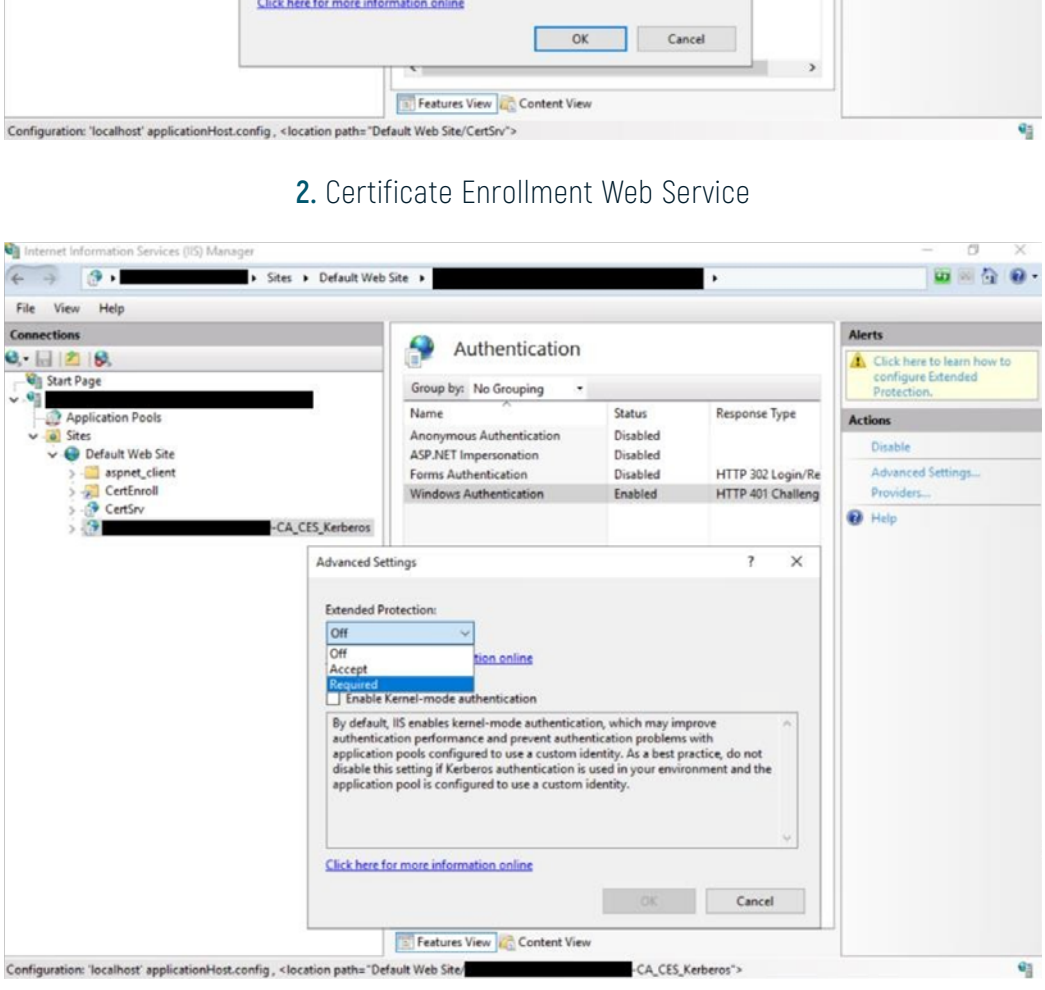


- However, if you can't disable NTLM outright then we recommend enabling EPA on AD CS services. This is achieved by:

1. Certificate Authority Web Enrollment



2. Certificate Enrollment Web Service



3. After enabling EPA in the UI, the Web.config file created by CES role at "**<%windir%>\systemdata\CES\<CA Name>_CES_Kerberos\web.config**" should also be updated by adding <extendedProtectionPolicy> element with either "WhenSupported | Always" value based on the Extended Protection option selected in above IIS UI. For more information on the options available for extendedProtectionPolicy, see <transport> of <basicHttpBinding>. The settings most likely to be used are as follows:

```
<binding name="TransportWithHeaderClientAuth">

<security mode="Transport">

<transport clientCredentialType="Windows">

<extendedProtectionPolicy policyEnforcement="Always" />

</transport>
```

For more information, please see Microsoft Security Advisory ADV210003

Additional Recommendations

Cynet360 can detect complex post-exploitation attempts and malicious behavior on endpoints as long the detection mechanisms are enabled.

Besides applying the Microsoft mitigation steps we recommend enabling all the detections and remediations mechanisms to maximize environmental protection and visibility.

SeriousSam Vulnerability

On July 20th, 2021, Microsoft disclosed vulnerability **CVE-2021-36934**, dubbed SeriousSAM or HiveNightmare.

CVE-2021-36934 A local privilege escalation vulnerability in Windows – allows users with low-level privileges (non-admins) to access the C:\Windows\System32\Config directory that stores the SAM, SYSTEM and SECURITY critical files. These files contain system secrets, local users, computer-hashed passwords, and additional sensitive credential information. Accessing these files gives threat actors with low-level privileges the ability to potentially carry out a local privilege escalation attack.

The vulnerability affects versions of Windows 10 released after 2018, as well as Windows 11 due to overly permissive Access Control Lists (ACLs) on multiple system files, including the Security Accounts Manager (SAM) database which is particularly vulnerable.

Cynet protects its customers from a wide range of credential access and theft techniques relevant to the Security Accounts Manager (SAM) by utilizing several different detection and prevention mechanisms. Moreover, we always work on adding new detections as new techniques are being researched.

Furthermore, as mentioned in the Microsoft publication, an attacker must have the ability to execute code on a victim's system prior to any attempts to exploit this vulnerability. Cynet360 will detect these pre-exploitation activities and trigger the relevant alerts according to the detected activity and, based on enabled prevention capabilities, will deny the attacker attempts to exploit this vulnerability.

In addition to Microsoft and the US-CERT workaround suggestions, you can utilize Cynet360 for that purpose by executing the PowerShell commands via Cynet360 user interface.
Keep in mind that in case you choose to do so, you should make sure to have a proper backup as deleting the shadow copies will affect your ability to restore any lost data.

Kaseya Supply-Chain Attack

Executive Summary

Kaseya VSA is a unified RMM solution that lets MSPs maintain, automate, collect information, and patch IT equipment via a remote centralized interface.

On Friday afternoon, July 2nd, the REvil group leveraged the 4th of July celebrations and upcoming long weekend to launch a large-scale attack involving Kaseya VSA. Because of the impending holiday, most of the IT staff were away from the office, a prime opportunity for a threat group to strike. Over 200 businesses have been hit by ransomware attacks, and Kaseya VSA has issued an emergency notice to its customers to immediately shutdown the VSA server until further notice.

We have reason to believe the Russian threat group REvil's attack is connected to the tensions between the U.S. and Russia in recent weeks.

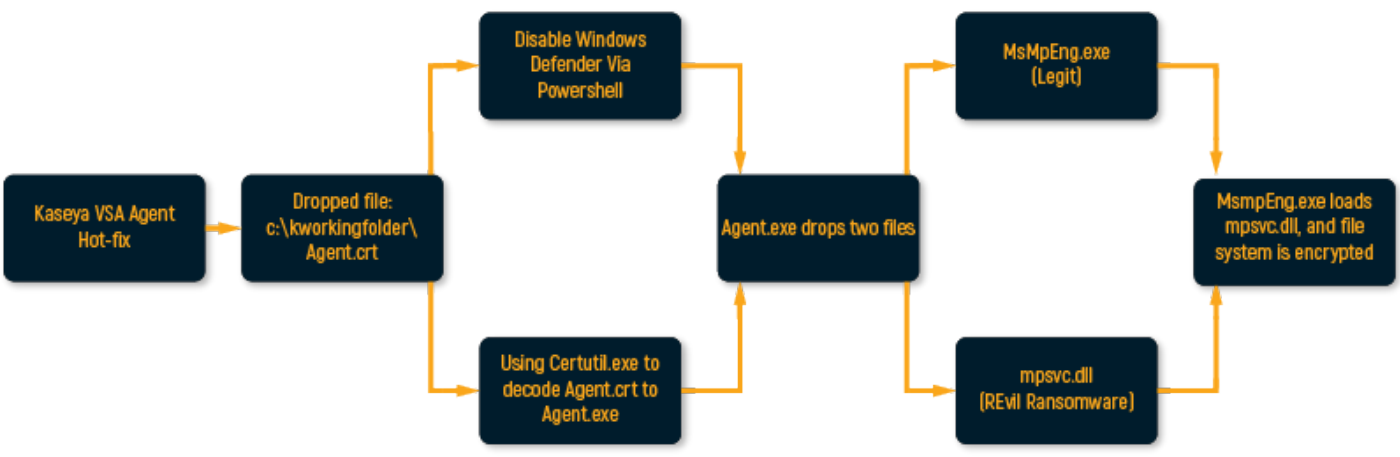
On June 17, U.S. President Joe Biden "warned Russian president Vladimir Putin that the US has significant cyber capability as he looked to pressure his counterpart over cyber-attacks.". Just a day prior, Biden had warned that the U.S. would retaliate to Russia's continued cyber strikes.

We have found some artifacts within the recent REvil attack that could indicate a political motivation. The threat actors used "**DTrump4ever**" and "**blacklivesmatter**" strings as part of the attack. Additionally, the REvil attack launched a day before the fourth of July (U.S. Independence Day).

REvil Ransomware (AKA Sodinokibi) threat actors are one of the most active RaaS gangs recently. They have been operating since April 2019, right after the demise of "GandCrab". REvil operators are believed to be of Russian nationality and are involved in attacks against US targets. In addition, they also have a reputation for large ransomware demands and targeting high-profile corporate targets.

The Threat actors have exploited what seems to be a security flaw in Kaseya VSA that allowed them to inject malicious files via the software's update mechanism. That gave the attackers a vast attack surface of around eight managed service providers that opened the door to 200 businesses with countless endpoints to encrypt.

Attack Flow



History Repeats Itself

Unfortunately, this is not the first time the same attack group has leveraged the Kaseya supply-chain vulnerability. On June 21st, 2019, Bleepingcomputer published an article ("Sodinokibi Ransomware Spreads Wide via Hacked MSPs, Sites, and Spam") about how REvil group appeared to have used the MSP's Kaseya VSA console to push a file .bat file to endpoints and execute it. Once executed, it would then execute a ransomware. Additionally, Cynet has also published an article about this incident and a new wave of Sodinokibi.

Mitre Att&ck Matrix

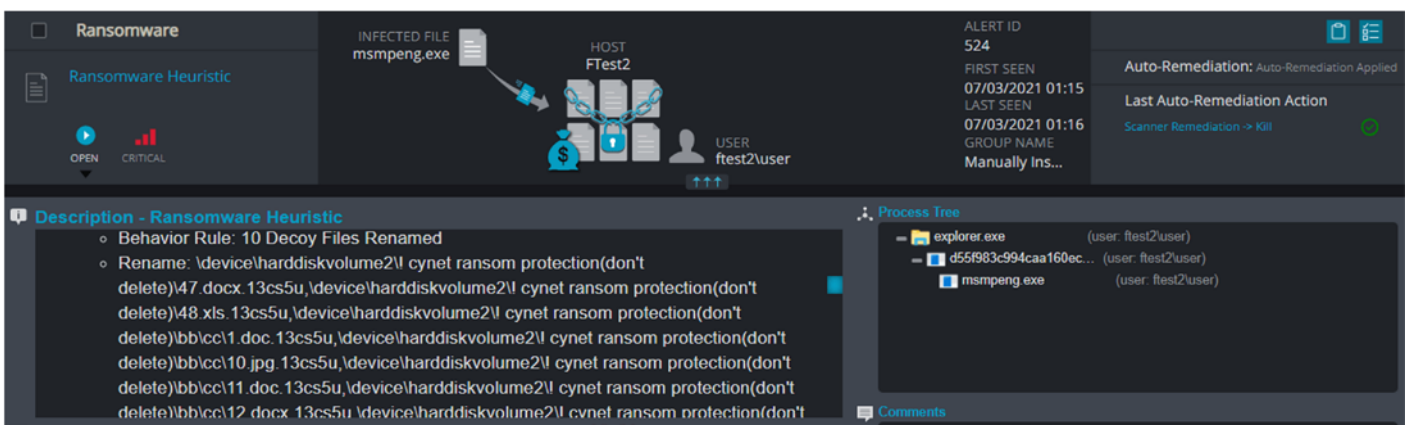
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media 1	Windows Management Instrumentation 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2	OS Credential Dumping	Peripheral Device Discovery 1 1	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Data Encrypted for Impact 1
Default Accounts	Service Execution 1	Windows Service 1	Windows Service 1	Obfuscated Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	System Shutdown/Reboot 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 2	DLL Side-Loading 1	Security Account Manager	System Service Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Defacement 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 3	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Proxy 1	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2	LSA Secrets	System Information Discovery 2 5	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 2	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Security Software Discovery 2 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Virtualization/Sandbox Evasion 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Application Window Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

Cynet vs. REvil Ransomware – Detection and Prevention

Cynet Customers are protected against this ransomware by several detection mechanisms:

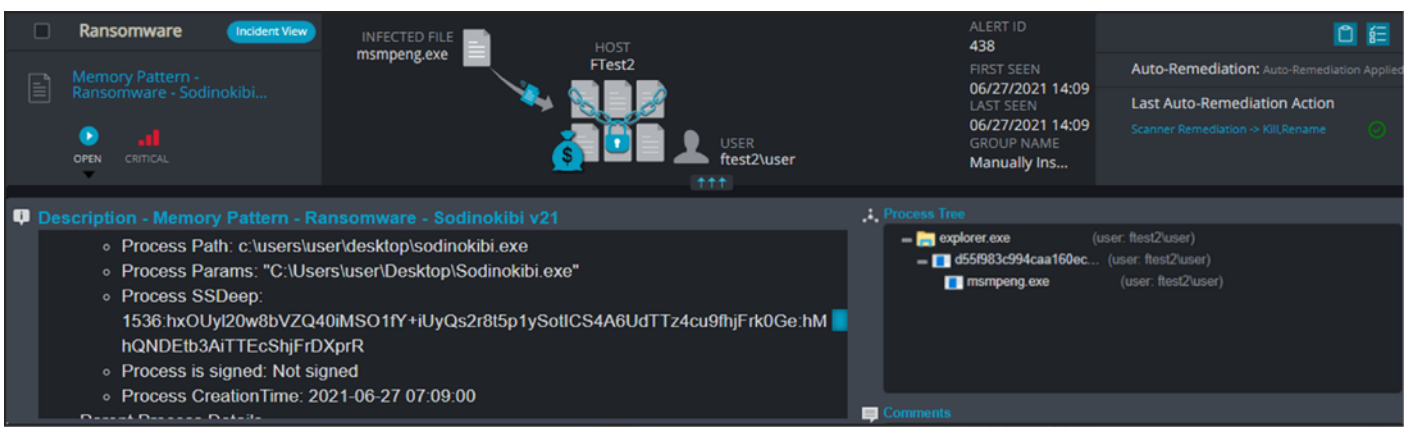
Ransomware Heuristic

This alert triggers when Cynet detects suspicious behavior which can be associated with Ransomware (such as changing file extensions to ".Lock").



Memory Pattern

This alert trigger when Cynet detects memory strings which are associated with Malware or with malicious files.



CyOps Team

Cynet's 24/7 MDR with the latest security updates and reports

Serv-U Remote Memory Escape Vulnerability

Microsoft recently discovered a new zero-day RCE vulnerability (**CVE-2021-35211**) in SolarWinds Serv-U products that is currently being exploited in the wild. This vulnerability has already been patched by SolarWinds (Serv-U version 15.2.3 hotfix (HF) 2).

The vulnerable versions are:

Software Version	Upgrade Paths
Serv-U 15.2.3 HF1	Apply Serv-U 15.2.3 HF2, available in your Customer Portal
Serv-U 15.2.3	Apply Serv-U 15.2.3 HF1, then apply Serv-U 15.2.3 HF2, available in your Customer Portal
All Serv-U versions prior to 15.2.3	Upgrade to Serv-U 15.2.3, then apply Serv-U 15.2.3 HF1, then apply Serv-U 15.2.3 HF2, available in your Customer Portal

An attacker that successfully exploits this vulnerability can execute code remotely with high privileges. Using RCE, they can remove or install programs, modify and exfiltrate data, and run dropped executables.

SolarWinds has officially addressed this matter on their website. You can find more information at the following link: https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211

Installing this update will fully mitigate the vulnerability and we highly recommend appliyng the patch as soon as possible.

Threat Analysis - HelloKitty

HelloKitty ransomware was first spotted in 2020. The ransomware is less sophisticated and easier to spot than the more infamous REvil and Conti but has successfully breached major targets. These include CEMIG0 and the successful attack against video games developer CD Projekt Red, which claimed to have stolen many games' source code, including The Witcher 3, Cyberpunk 2077 and Gwent.

Earlier this month, vulnerable SonicWall devices were exploited as part of a HelloKitty ransomware attack. The security vulnerability was found in SonicWall SMA100 series and SRA products which were patched previously following the successful deployment of FiveHands ransomware.

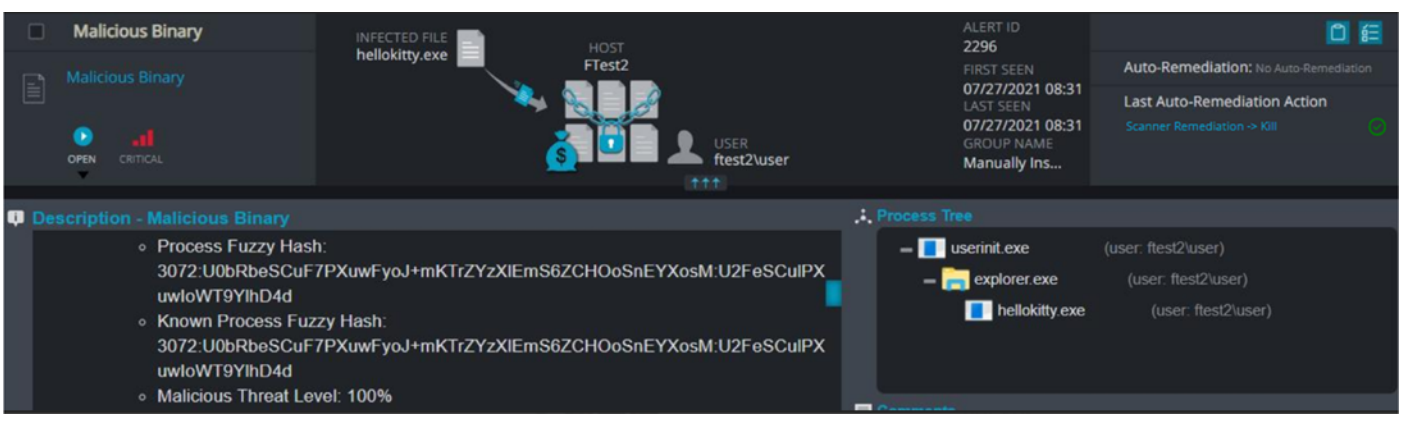
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1	Process Injection 2	Virtualization/Sandbox Evasion 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Data Encrypted for Impact 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Process Injection 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Proxy 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Virtualization/Sandbox Evasion 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 2 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Cynet 360 VS HelloKitty

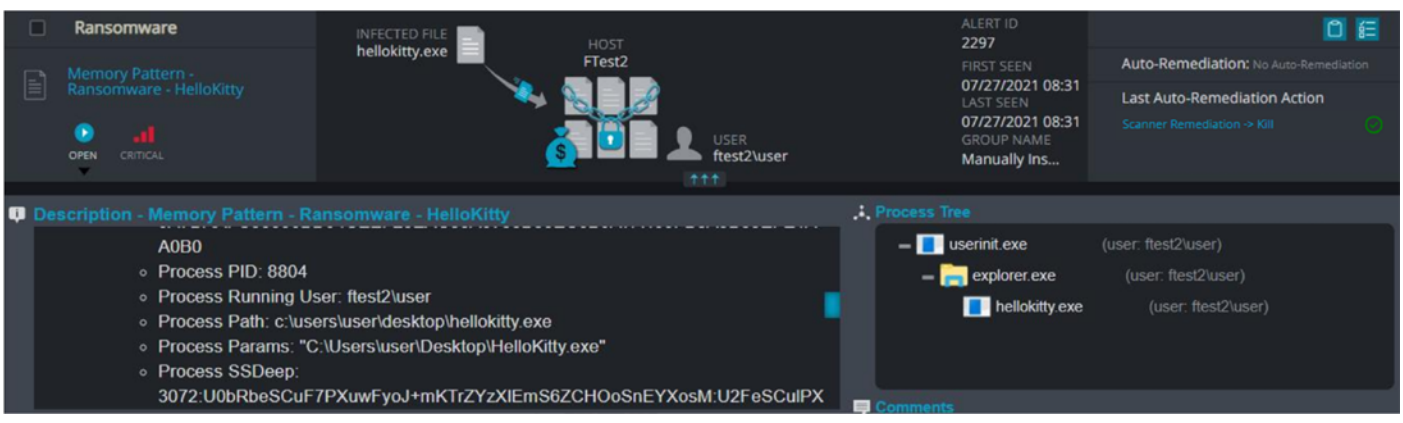
Malicious Binary

This alert triggers when Cynet detects a file flagged as malicious in Cynet's EPS (endpoint scanner) built-in threat intelligence database. This database contains only critical IoCs (such as ransomware, hacking tools, etc.).



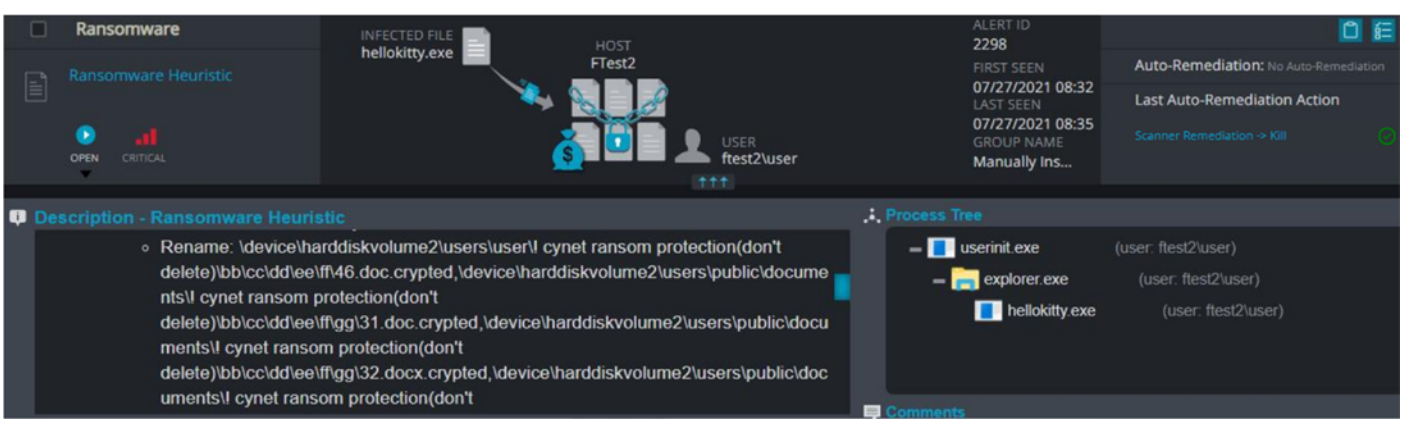
Memory Pattern

This alert triggers when Cynet detects memory strings associated with malware or with malicious files.



Ransomware Heuristic

This alert triggers when Cynet detects suspicious behavior which can be associated with Ransomware (such as changing file extensions to ".Lock").



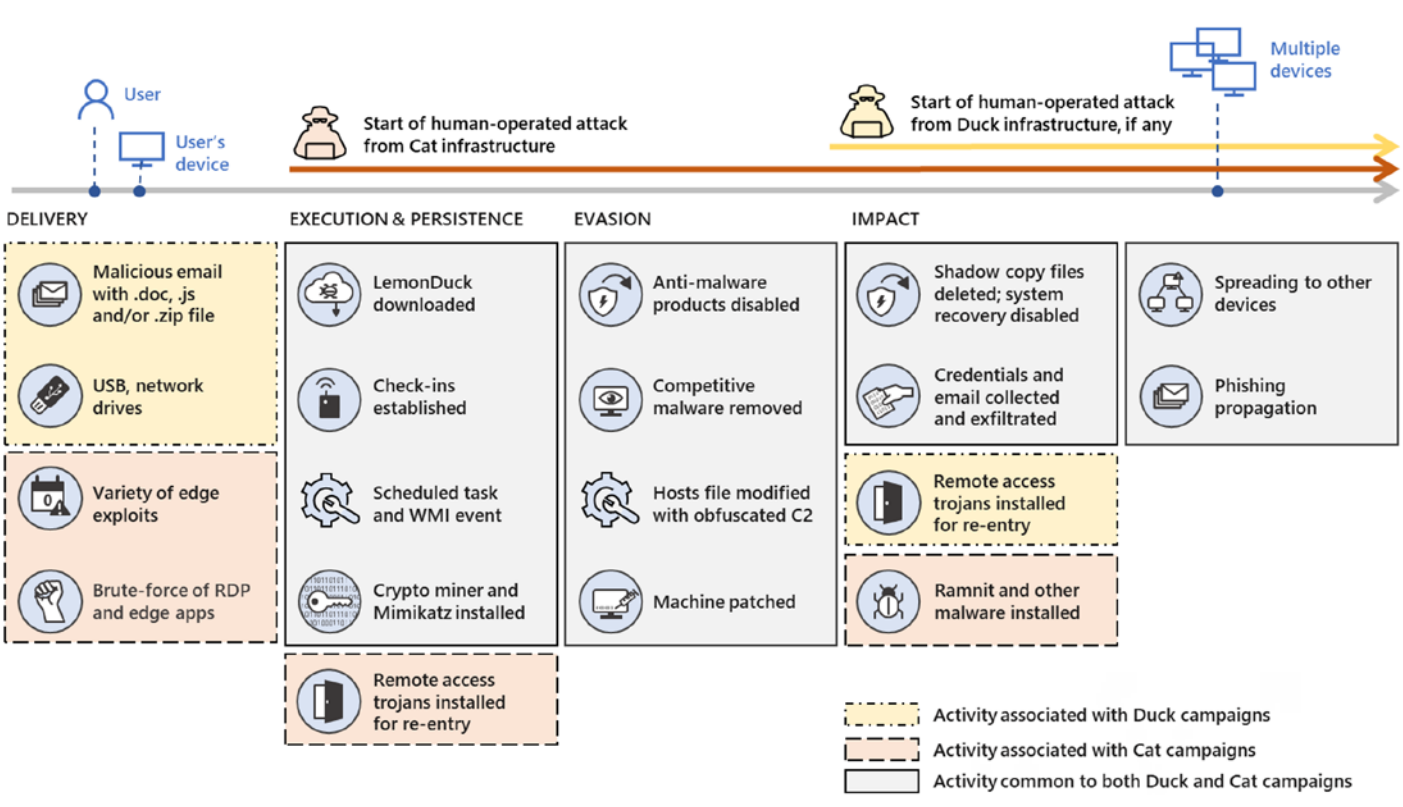
Threat Analysis - Lemon Duck

Lemon Duck and LemonCat are active, constantly upgrading, cross-platform modular bots that first surfaced in the wild in May 2019. The bots contain a mining payload for Monero cryptocurrency and automated infection capabilities. Both bots carry several infection vectors, including:

- SMB password brute force and PassTheHash
- Email with malicious attachment
- RDP password bruteforce
- XMRig
- RDP BlueKeep
- Mshta.exe
- Startup folder
- MSSQL
- SMBGHOST
- Mimikatz
- MS Exchange vulnerability

The infection always begins with the execution of a PowerShell script retrieved from another infected host or the C2 server. Once this is accomplished, the botnets continue to spread to more endpoints using one of the infection vectors specified above, and a Monero coin miner is installed on each infected host. Once complete, the infection cycle starts again.

The Attack is described in the flowchart below:



Mitre Att&ck Matrix

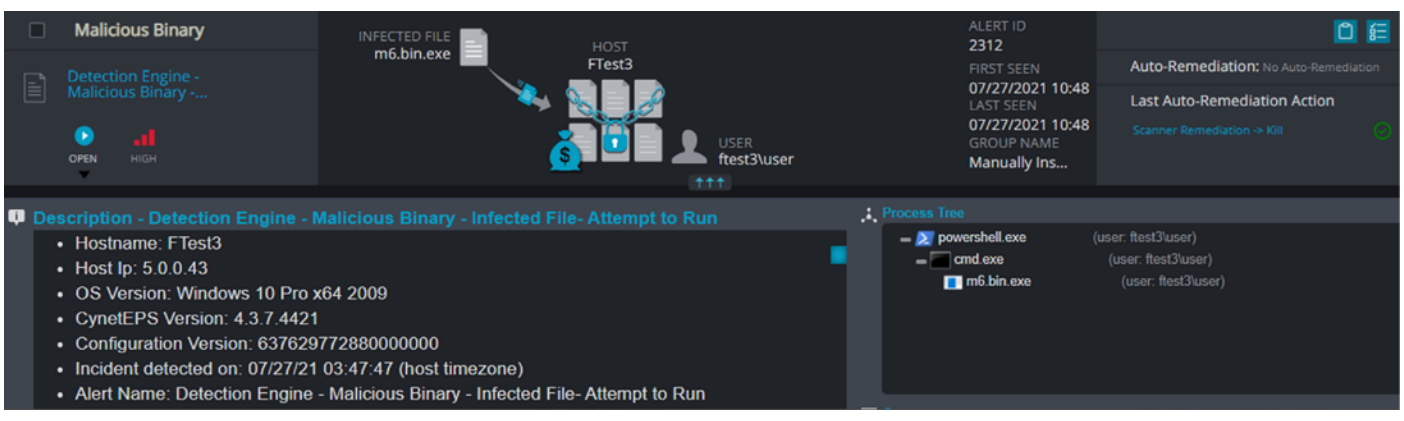
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation 4 1	Windows Service 1	Windows Service 1	Masquerading 1 3 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Command and Scripting Interpreter 1 1	Boot or Logon Initialization Scripts	Process Injection 1 2	Virtualization/Sandbox Evasion 3 4	LSASS Memory	Security Software Discovery 4 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	Scripting 1	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	Service Execution 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	PowerShell 2 1	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Cynet 360 VS Lemon Duck

Cynet Customers are protected from LemonDuck as we detect the malware in its first stage – either by the downloaded payload or the PowerShell command:

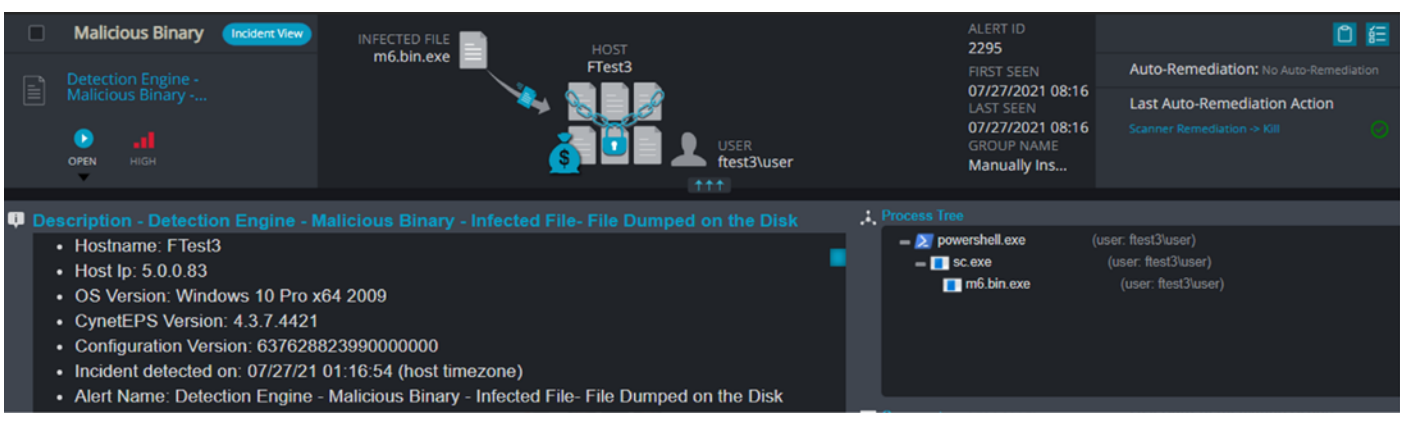
Detection Engine - Malicious Binary - Infected File- Attempt to Run

The alert triggers when Cynet's AV/AI engine detects a malicious file that was loaded to the memory.



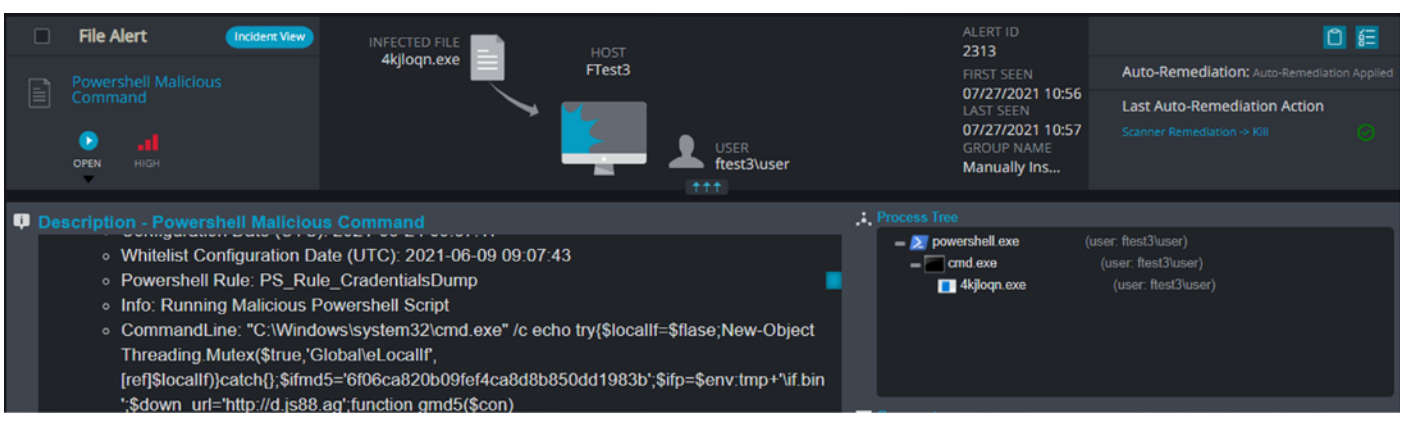
Detection Engine - Malicious Binary - Infected File - File Dumped on the Disk

This alert triggers when Cynet's AV/AI engine detects a malicious file that was dumped on the disk.



Powershell Malicious Command

This alert triggers when Cynet detects a PowerShell process which executes a command that contains suspicious arguments or a command which is associated with malicious patterns.



Contact Cynet CyOps
(Cynet Security Operations Center)

The Cynet CyOps available to clients for any issues 24/7, questions or comments related to Cynet 360. For additional information, you may contact us directly at:

CyOps Mailbox
soc@cynet.com

CyOps Team Leader
sivanc@cynet.com

CyOps Manager
shirang@cynet.com

+1 (347) 474-0048
+44 2032-909051
+972 72-3369736