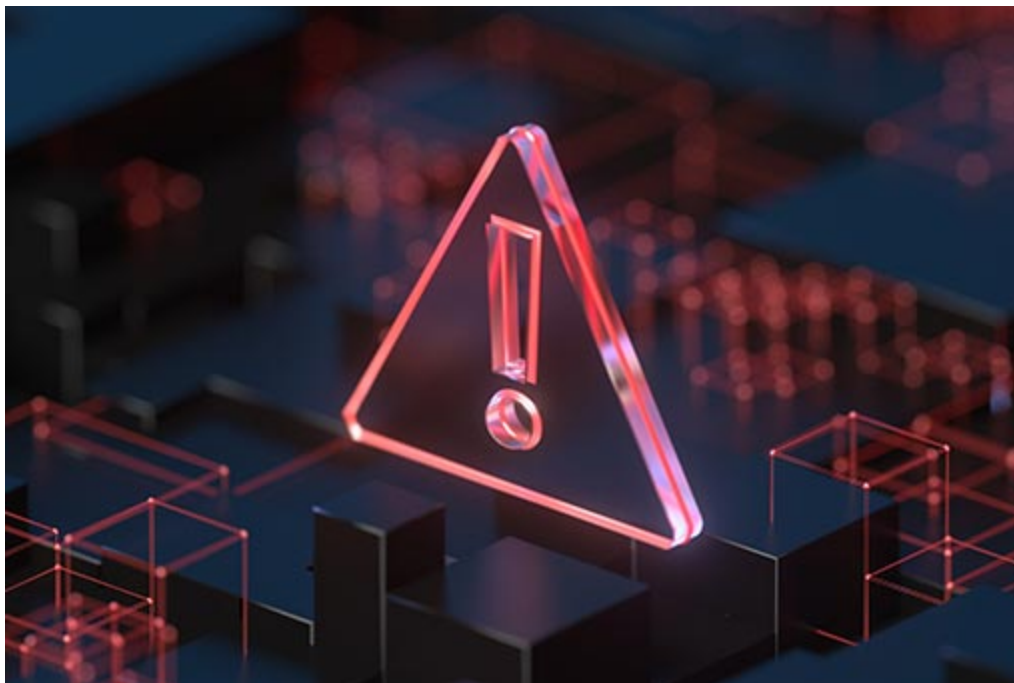


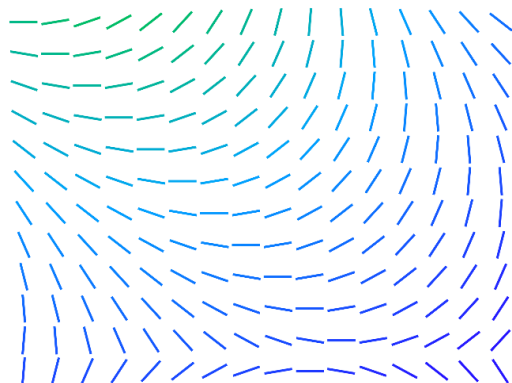
Trellix Global Defenders: Analysis and Protections for RagnarLocker Ransomware

trellix.com/en-us/about/newsroom/stories/threat-labs/analysis-and-protections-for-ragnarlocker-ransomware.html



Stories

The latest cybersecurity trends, best practices, security vulnerabilities, and more



Trellix

**Threat
Intelligence**

By [Taylor Mullins](#) · February 28, 2022

The United States Federal Bureau of Investigation (FBI) has released a Flash Alert warning that the RagnarLocker ransomware gang has breached the networks of at least fifty-two organizations from multiple critical infrastructure sectors across the United States. This is the second FBI alert released for the RagnarLocker Ransomware variant, the last alert was released in November 2020.

The following FBI flash alerts will focus on providing indicators of compromise (IOCs) that organizations can use to detect and block RagnarLocker ransomware attacks.

[March 2022 FBI Alert \(PDF\) - RagnarLocker Ransomware Indicators of Compromise](#)

[November 2020 FBI Alert \(PDF\) - RagnarLocker Ransomware Indicators of Compromise](#)

RagnarLocker ransomware first appeared in the wild at the end of December 2019 as part of a campaign against compromised networks targeted by its operators. The actors behind RagnarLocker will perform reconnaissance on the targeted network, exfiltrate sensitive information, encrypt files, and then notify the victim the stolen files will be released to the public if the ransom is not paid. The threat actor behind the malware is known in previous attacks to ask for millions of dollars in payment and creates a ransom note that includes the company name. The ransomware enumerates all running services on the infected host and stops services that contain a specific string. Ragnar is small compared to other malware and is written in the C/C++ programming language.



Figure 1. Global Detections and Observed Sectors for RagnarLocker Ransomware. Source: MVISION Insights

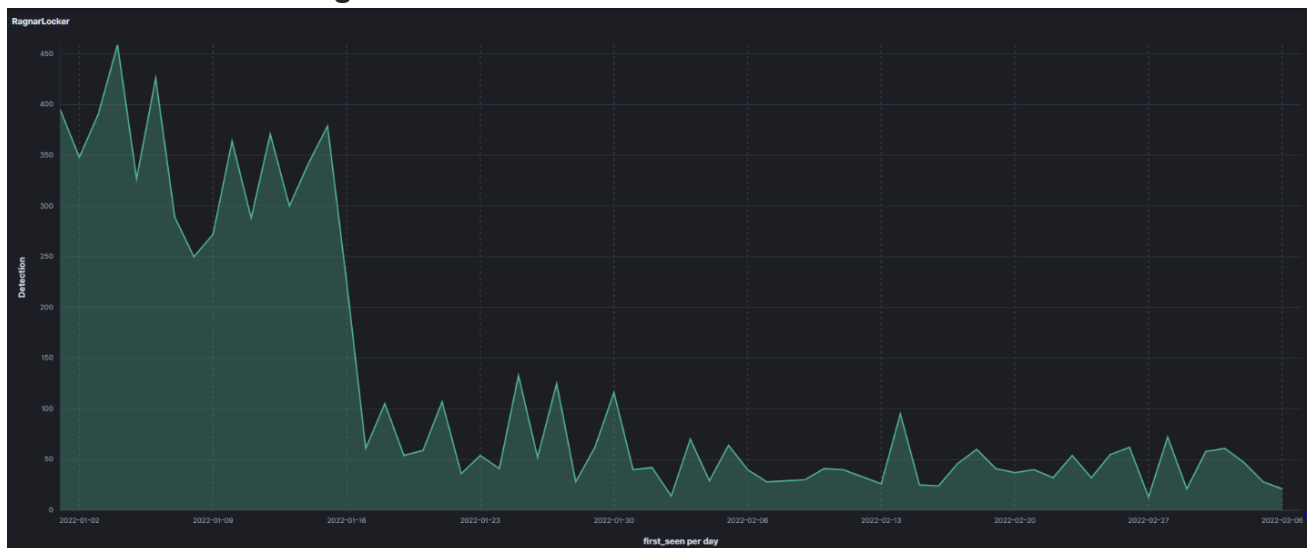


Figure 2. Last 60 days of detections for RagnarLocker Ransomware. Source: Trellix APG Team

Recommended Steps to Prevent Initial Access

The threat actors behind the RagnarLocker attacks often gain entry by compromising the company's network via the RDP service, using brute force attacks to guess weak passwords or with stolen credentials purchased on the Dark Web.

- After gaining access the exploitation of [CVE-2017-0213](#) is used to elevate privileges, patching of this CVE is critical.
- Reviewing the CVEs for all Public Facing Systems – CISA regularly updates and maintains a full list of CVEs that are known to be exploited: [CISA: KNOWN EXPLOITED VULNERABILITIES CATALOG](#)
- Over 90% of successful cyber-attacks begin with a phishing email and has been a technique used by RagnarLocker, it is critical to continually monitor for spearphishing campaigns with malicious attachments and links.
 - Communication – Along with monitoring, educating end users on what they could be receiving in their email can help them spot phishing campaigns before they click or download.
- Review Indicators of Compromise in FBI alerts and block the malicious IP addresses observed in previous attacks.

Trellix Protections and Global Detections

Trellix Global Threat Intelligence (GTI) is currently detecting all known analyzed indicators for this campaign across their products that use the GTI threat feed.



Figure 3. Trellix

Products detecting this threat globally. Source: MVISION Insights

Blocking RagnarLocker Attacks with Endpoint Security

Trellix ENS is currently detecting RagnarLocker Indicators of Compromise (IOCs) with signature detections and the malware behavior associated with RagnarLocker Ransomware attacks. The following Adaptive Threat Protection Rules in ENS have shown success in stopping the techniques associated with RagnarLocker. Trellix always recommends testing in Report Only Mode before blocking to confirm no false positives are detected by this behavioral rule.

Coverage

Minimum AMCore Content: 4217

Adaptive Threat Protection Rule ID 239: Identify suspicious command parameter execution (Mitre-T1059: Identifies the suspicious execution of an application through command line parameters).

Adaptive Threat Protection Rule ID 341: Identify and block patterns being used in Ransomware attacks in security rule group assignments.

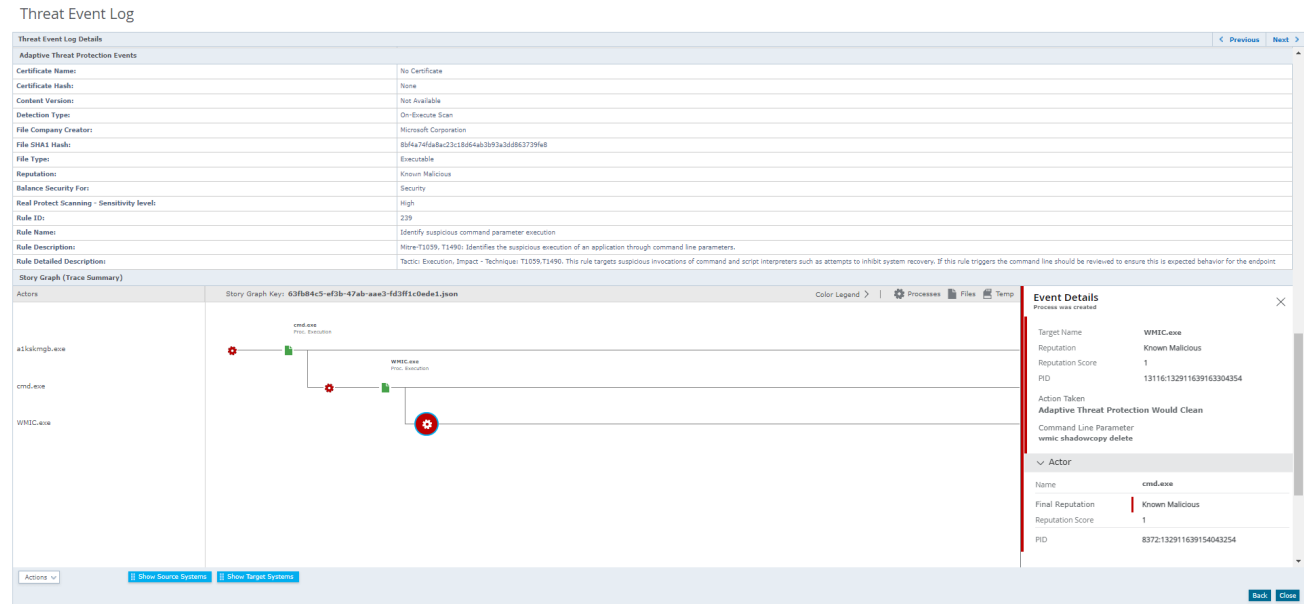


Figure 4. Story Graph and Adaptive Threat Protection Detection for Rule ID 239 in ePolicy Orchestrator/MVISION ePO

Threat Event Log

The screenshot displays the Threat Event Log interface. The top section, 'Adaptive Threat Protection Events', provides details for Rule ID 341, including its name, certificate information, file hashes, and reputation. The 'Rule Description' states it identifies and blocks patterns used in ransomware attacks. Below this is a 'Story Graph (Trace Summary)' showing a sequence of processes: mftoprep32.exe, mftoprep32.exe, mftoprep32.exe, mftoprep32.exe, mftoprep32.exe, System.Cm..., System.Cm..., System.Cm..., System.Cm..., G4P.exe, G4P.exe, G4P.exe, and cmd.exe. A red star icon indicates a threat detection event on the cmd.exe process. An 'Event Details' panel on the right shows the target name as cmd.exe, its reputation as 'Known Malicious', and the action taken: 'Adaptive Threat Protection Would Clean'.

Figure 5. Story Graph and Adaptive Threat Protection Detection for Rule ID 341 in ePolicy Orchestrator/MVISION ePO

The screenshot shows the 'Threats' section in MVISION Insights. It lists five detections of RagnarLocker ransomware, each with a 'HIGH' severity. The threats are categorized as 'Ransomware' and have a description stating that ransomware demands payment to regain access to a computer. The threats are: RagnarLocker.MKIMTB, RagnarLocker.B, RagnarLocker.MSR, RagnarLocker.php, and RagnarLocker.BMIMSR.

Figure 6. Threat detections for RagnarLocker Ransomware shown in MVISION Insights

RagnarLocker Threat Intelligence from the Trellix Advanced Threat Research Team and MVISION Insights

MVISION Insights will provide the current threat intelligence and known indicators for RagnarLocker Ransomware. MVISION Insights will alert to detections and Process Traces that have been observed and systems that require additional attention to prevent widespread infection. MVISION Insights will also include Hunting Rules for threat hunting and further intelligence gathering of the threat activity and adversary.

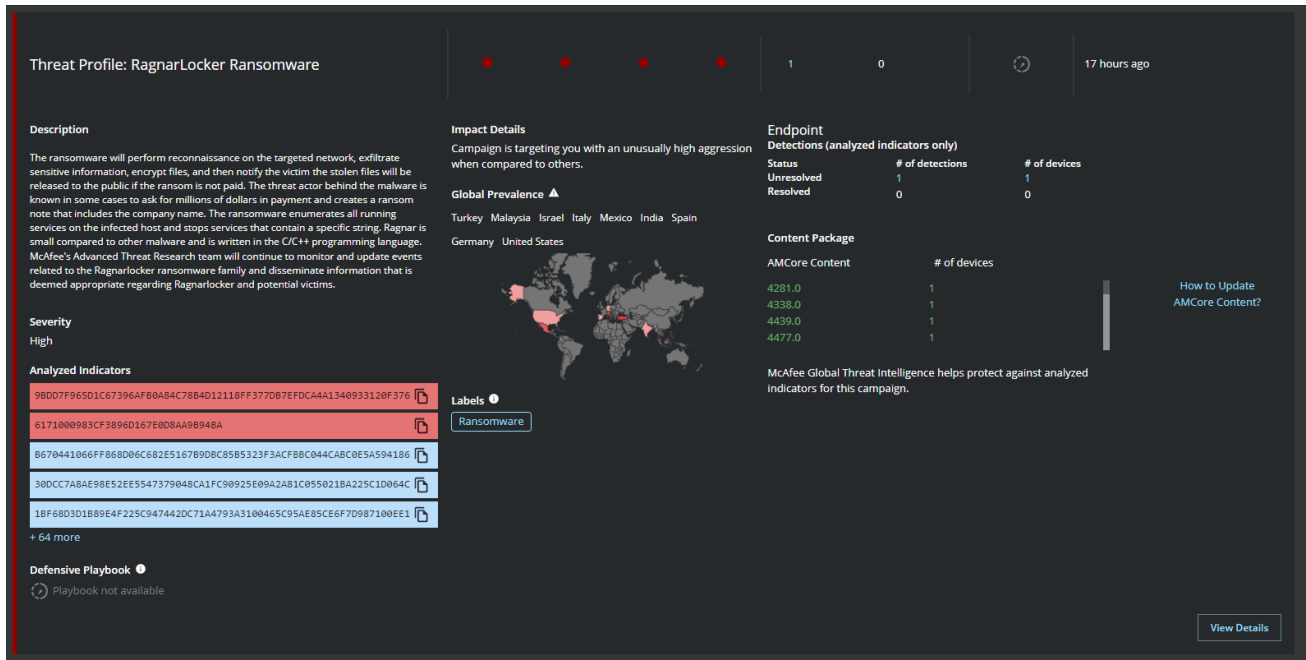


Figure 7. Campaign Details, Analyzed Indicators of Compromise, and Detections

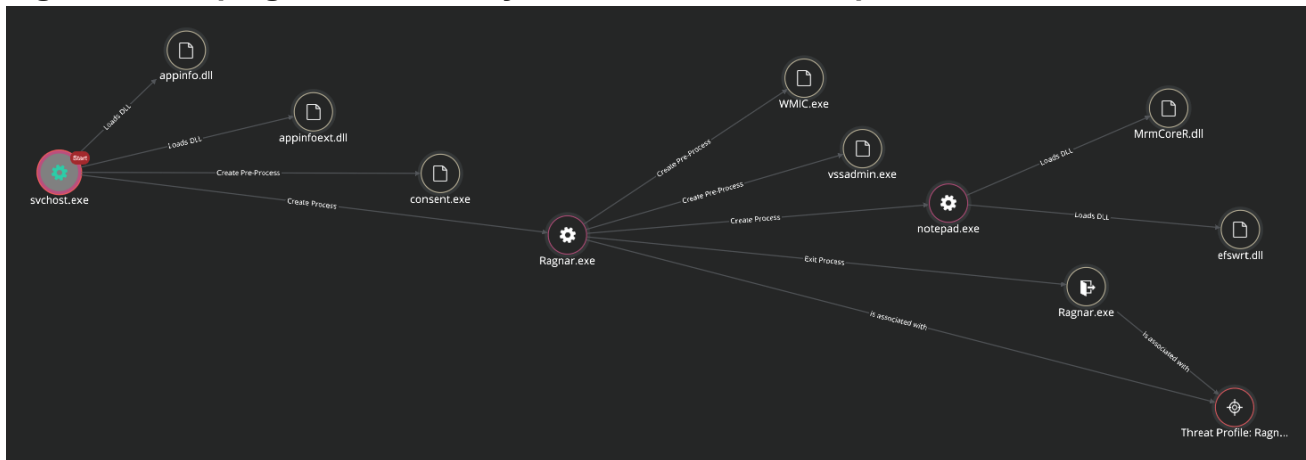


Figure 8. Process Trace for RagnarLocker Ransomware activity in MVISION Insights

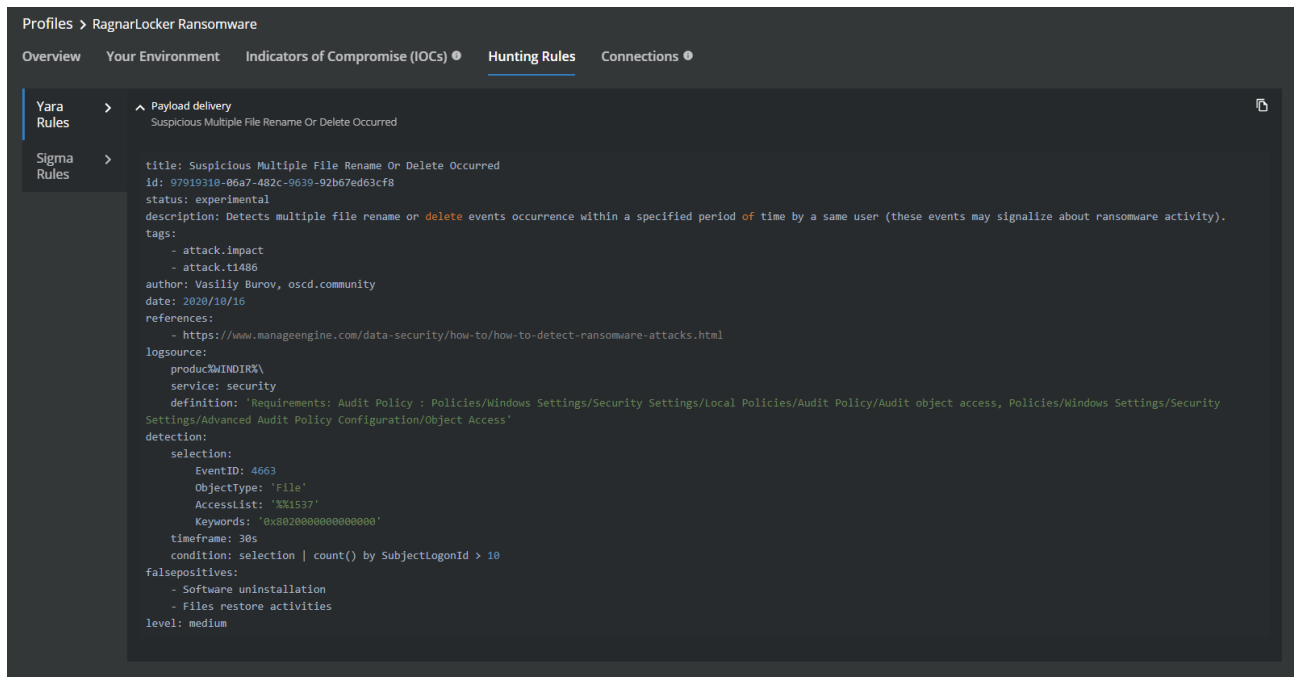


Figure 9. Hunting Rules for RagnarLocker Ransomware in MVISION Insights

Detecting Malicious Activity with MVISION EDR

MVISION EDR is currently monitoring for the activity associated with RagnarLocker Ransomware and will note the MITRE techniques and any suspicious indicators related to the adversarial activity. Analysis of RagnarLocker malware samples note the usage of native Windows APIs, Microsoft Connection Manager Profile Installer (CMSTP.exe), and the deletion of Shadow Copy to inhibit system recovery.

Techniques Observed(7)	MITRE ATT&CK® Matrix	Suspicious Indicators(10)	
Application Window Discovery T1010 (Discovery)		Executed COM Elevation Monitor (potential UAC bypass)	
Remote System Discovery T1018 (Discovery)		Detected binary doing window discovery	
Native API T1106 (Execution)		Detected suspicious binary doing window application discovery	
Malicious File T1204.002 (Execution)		Ran Microsoft Connection Manager Profile Installer	
CMSTP T1218.002 (Defense Evasion)		Suspicious file would have been blocked by Endpoint Protection (in observe mode)	
Process Activity			
Table View			
Filter events by Filter by keyword Showing 6 of 195 events			
Date	Event Type	Actor	Summary
Mar 7, 2022 3:37:34 PM	Process started	> PID: 13472 -- svchost.exe	Command line: "C:\Users\McAfee\Downloads\RagnarLocker.exe" Domain name: DLPLCLT.02 User name: McAfee
Mar 7, 2022 3:37:36 PM	API Call	> PID: 11640 -- RagnarLocker.exe	API name: GetWindowLong Arguments: Result: 113311744 Module: -
Mar 7, 2022 3:37:35 PM	Process started	> PID: 11640 -- RagnarLocker.exe	Command line: "c:\windows\system32\cmstp.exe" /au C:\Windows\temp\3c3ddays.inf Domain name: DLPLCLT.02 User name: McAfee
Mar 7, 2022 3:37:35 PM	API Call	> PID: 1148 -- cmstp.exe	API name: GetWindowLong Arguments: Result: 2348810240 Module: -
Mar 7, 2022 3:37:36 PM	API Call	> PID: 1148 -- cmstp.exe	API name: CoGetObject Arguments: Result: 0 Module: -
Mar 7, 2022 3:37:36 PM	API Call	> PID: 1148 -- cmstp.exe	API name: GetWindowInfo Arguments: Result: 1 Module: -

Figure 10. Interaction with the native OS application programming interface (API) to execute behaviors.

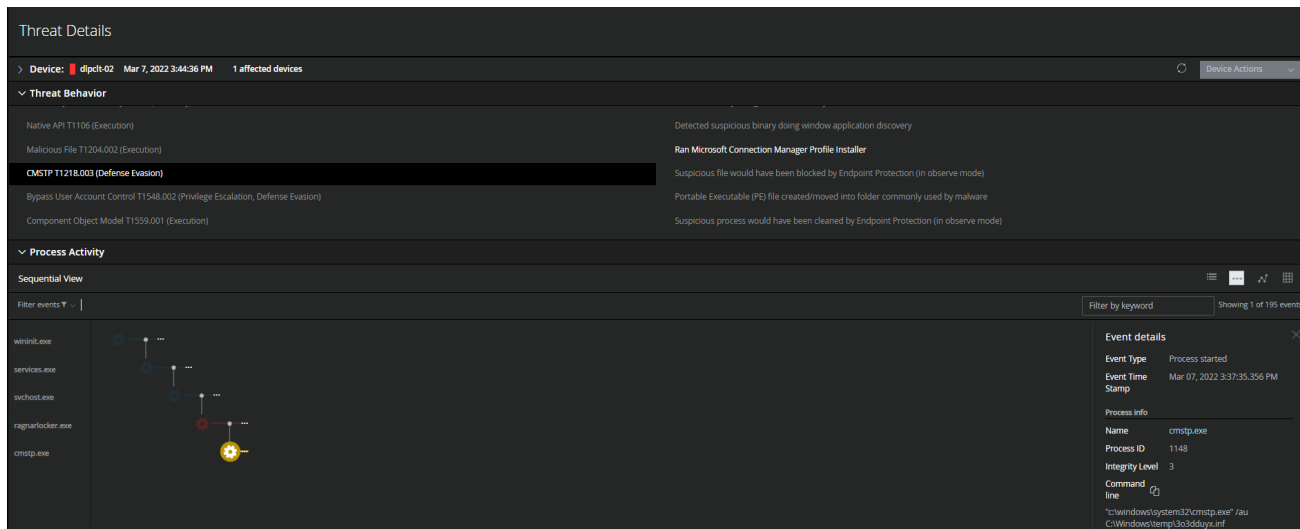


Figure 11. T1218.003 – Adversaries may abuse CMSTP to proxy execution of malicious code. The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles.

Device: dlpcit-03 | Detection window: 24h before - 24h after | Detection date: Mar 7, 2022 3:57:20 PM

Include: Exact | Exclude: Exact | Search | Export All

Date	PID	Process Name	Command Line	User	Tactics	Technique	Suspicious Indicator
Mar 7, 2022 3:53:54 PM	8124	WMIC.exe	wmic.exe shadowcopy delete	McAfee	Discovery, Execution	Application Window Discovery, Remote Sy...	Detected binary doing wind...
Mar 7, 2022 3:53:53 PM	12200	vssadmin.exe	vssadmin delete shadows /all /quiet	McAfee	Execution	Malicious File	Suspicious process would h...
Mar 7, 2022 3:53:53 PM	12200	vssadmin.exe	vssadmin delete shadows /all /quiet	McAfee	Execution		Process reputation was do...
Mar 7, 2022 3:53:53 PM	12200	vssadmin.exe	vssadmin delete shadows /all /quiet	McAfee	Defense Evasion, Impact	File Deletion, Inhibit System Recovery	EPP Detection: Identify and ...
Mar 7, 2022 3:53:53 PM	12200	vssadmin.exe	vssadmin delete shadows /all /quiet	McAfee	Defense Evasion, Impact	File Deletion, Inhibit System Recovery	Removed shadow copies fr...
Mar 7, 2022 3:53:53 PM	8124	WMIC.exe	wmic.exe shadowcopy delete	McAfee	Execution		Process reputation was do...
Mar 7, 2022 3:53:53 PM	8124	WMIC.exe	wmic.exe shadowcopy delete	McAfee	Execution	Malicious File	Suspicious process would h...
Mar 7, 2022 3:53:53 PM	8124	WMIC.exe	wmic.exe shadowcopy delete	McAfee	Execution	Windows Command Shell	EPP Detection: Identify sus...
Mar 7, 2022 3:53:53 PM	8124	WMIC.exe	wmic.exe shadowcopy delete	McAfee	Execution, Impact	Windows Management Instrumentation, L...	Removed shadow copy/stor...

Figure 12. Native Windows utilities utilized by adversaries to disable or delete system recovery.

Additional Resources

[Trellix Labs: RagnarLocker Ransomware Threatens to Release Confidential Information](#)

[McAfee KB92601 - MVISION Insights: RagnarLocker ransomware](#)

[McAfee Labs Threat Advisory - Ransom-Ragnar](#)

Featured Content

PERSPECTIVES

Our CEO On Living Security

By [Bryan Palma](#) · January 19, 2022

Trellix CEO, Bryan Palma, explains the critical need for security that's always learning.

[Read More](#)

XDR

Time to Drive Change by Challenging the Challengers

By [Michelle Salvado](#) · January 19, 2022

Dynamic threats call for dynamic security – the path to resiliency lies in XDR.

[Read More](#)

THREAT LABS

2022 Threat Predictions

By [Trellix](#) · January 19, 2022

What cyber security threats should enterprises look out for in 2022?

[Read More](#)

Get the latest

We're no strangers to cybersecurity. But we are a new company.
Stay up to date as we evolve.

Please enter a valid email address.

Zero spam. Unsubscribe at any time.