Cynet

CyOps

Monthly Cyber Threat Intelligence Report

May, 2021

CyOps Team

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

Contents

CyOps Team

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

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.

INCREASE IN RANSOMWARE ACTIVITY

In the last month, the CyOps team has identified a larger-than-usual number of incidents that involved ransomware attacks that targeted critical assets such as healthcare, first responders and national infrastructure.

The fact that this behavior is observed in different ransomware groups, raises the concern of a repetitive pattern of threat actors, completely ignoring the value of life and choose their victims recklessly.

CyOps Team

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

THREAT ANALYSIS - CONTI RANSOMWARE

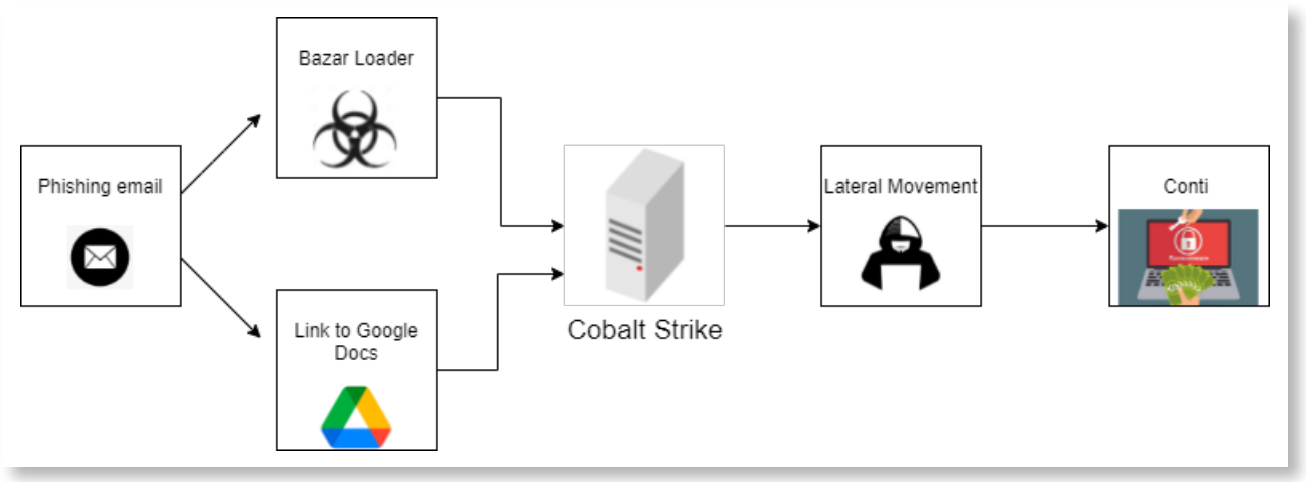
Conti ransomware is a global threat, since its first appearance in May 2020, the ransomware operators (aka. the Conti Gang) claim a vast amount of successful attacks, which estimated in millions of dollars in extortion fees.

Conti has been described as the successor to Ryuk, mainly because of their common initial infection method via phishing emails leading to a Bazar backdoor to launch an interactive attack and deploy the ransomware in turn.

Most of the Conti samples related to Cobalt strike servers in the purpose of gaining a remote control on a compromised machine, attempts to disable security products and dump the domain controller credentials.

On the next stage, the attackers exfiltrate the data, mostly to a cloud storage, and on the last stage the attackers encrypt the data or encrypt the endpoints themselves and blocking the user access.

According to the FBI, Conti ransomware was involved in 16 attacks of US healthcare and first responders in the last year.

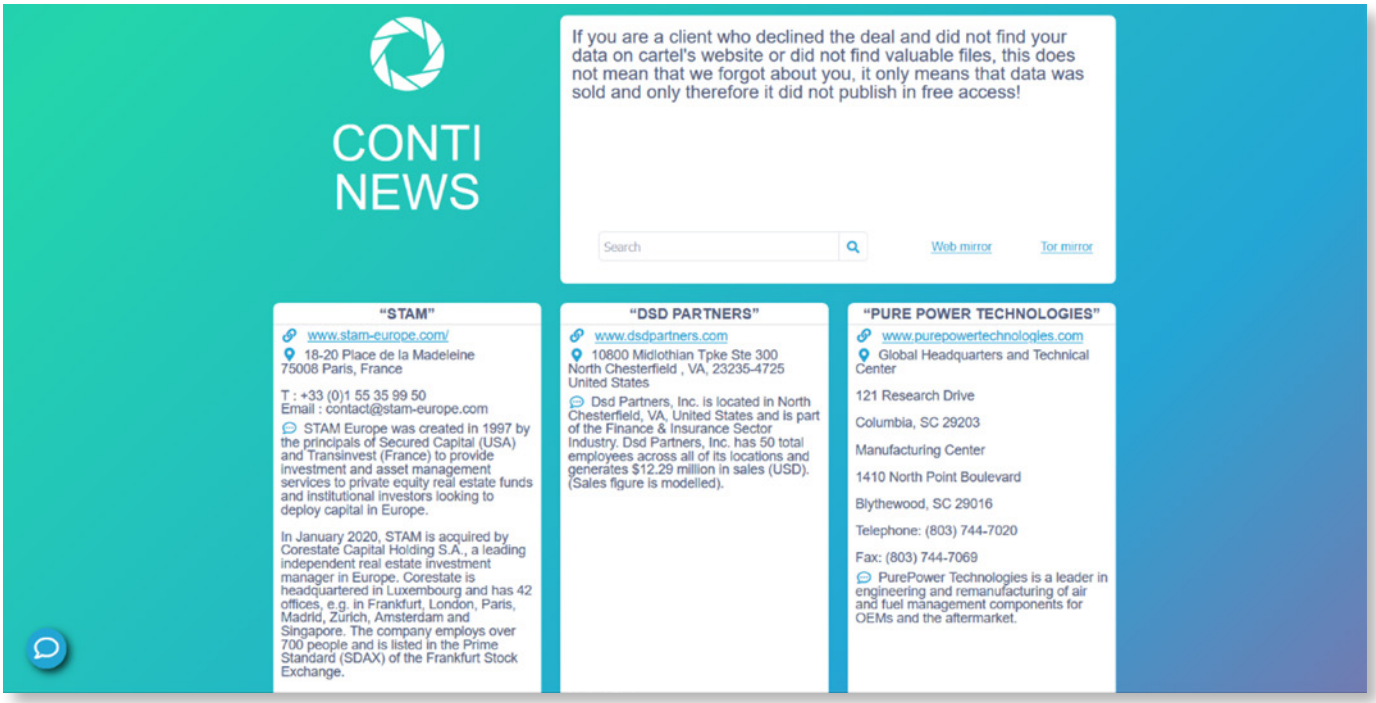


The CyOps team can locate and identify any content publication in the clear, deep, and dark web to provide 100% visibility to our customers.

CyOps Team

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

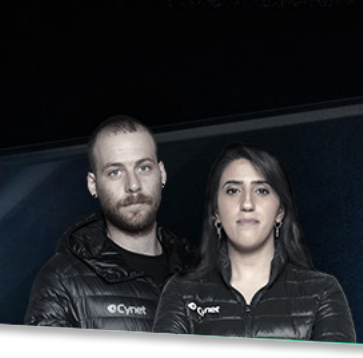
Data-Leaked Site of Conti Ransomware Group



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	DLL Side-Loading 1	Process Injection 1 1 2	Masquerading 3	OS Credential Dumping	System Time Discovery 1	Taint Shared Content 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 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	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 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	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 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	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 3	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	Regsvr32 1	LSA Secrets	File and Directory Discovery 4	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	Rundll32 1	Cached Domain Credentials	System Information Discovery 2 3	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	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Cynet has multiple detections for Conti ransomware and ransomware in general that provide several layers of protection both statically and behaviorally.



CyOps Team

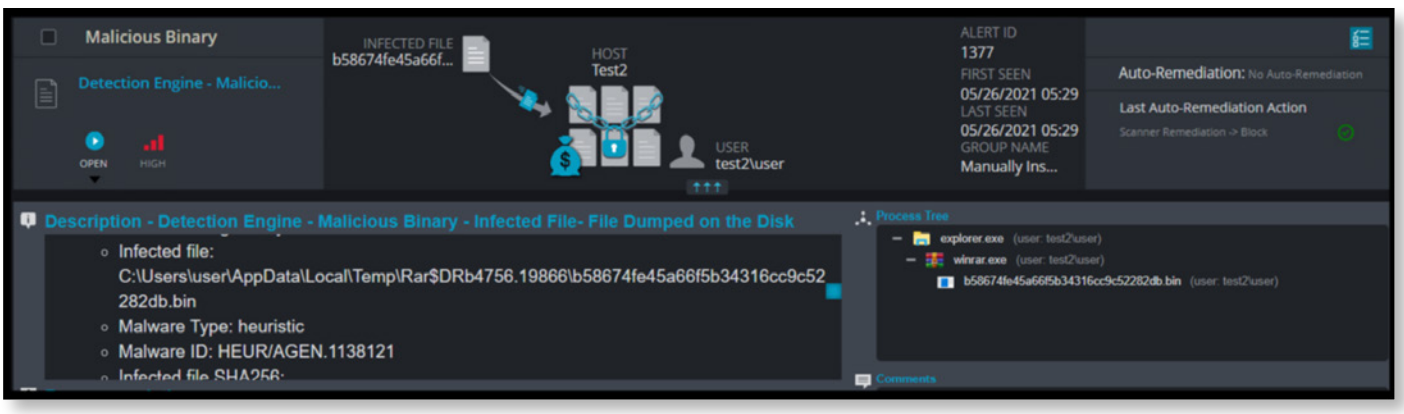
Cynet's 24/7 MDR with the latest security updates and reports

Malicious Binary

This alert triggers when Cynet detects a file that is flagged as malicious in Cynet's EPS.

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.

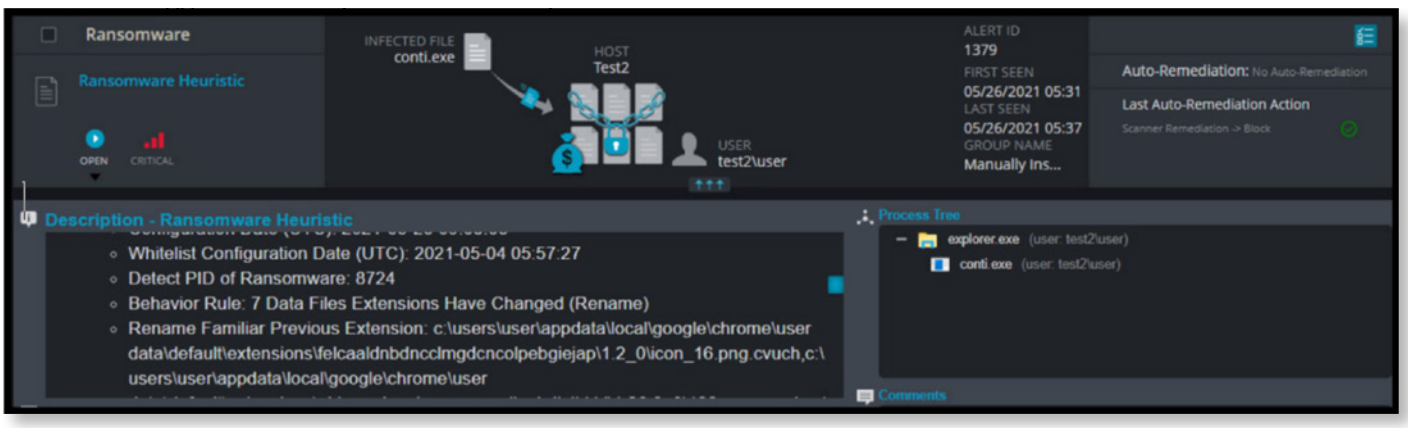


Memory Pattern

This alert triggers when Cynet detects memory strings which are associated with Ransomware.

Ransomware Heuristic

This alert triggers when Cynet detects suspicious behavior which can be associated with Ransomware.

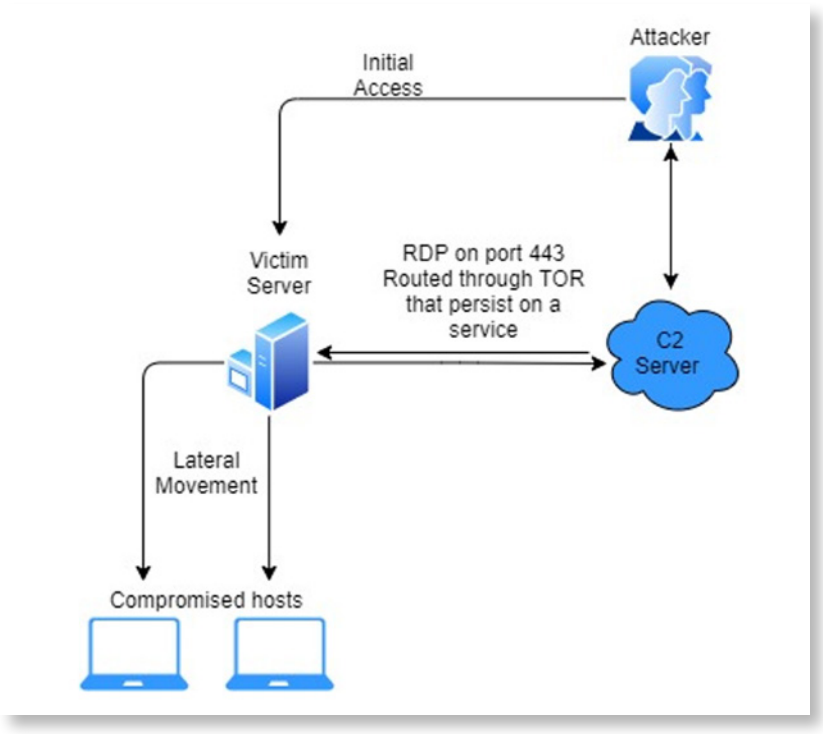


THREAT ANALYSIS - DARKSIDE RANSOMWARE

The Darkside ransomware was operated in August 2020 by professionals' Russian threat actors and become known as a professional stealthy threat targeting encryption & theft of valuable and sensitive data which in the end, provide the victims with a support web channel.

The Darkside group prefers attacking big organizations that can pay a large amount for decryption and perform financial analysis to their targeted victims and their attacks point on deep knowledge in their victim's security products & infrastructure weaknesses.

Furthermore, the group stated that they are avoiding attacking governments, schools & hospitals and their malware check the language of the device to avoid attacking Russian organizations.



On May 7, the DarkSide group has attacked the Colonial Pipeline which is one of the largest pipelines in the US that provide about 45% of the fuel for the East Coasts including military supplies.

As said before, the Darkside group avoiding targeting governments, and in this successful attack the business side was the intention but as a side effect, the operational side affected too as the company has been forced to freeze the systems and suspend the operations which define this attack from the others as it has large consequences as many government agencies including hospitals, emergency medical services, airports, military, etc. rely on the Colonial Pipeline.

After the systems were shut down for 6 days, The Colonial Pipeline confirmed it paid 4.4M$ in cryptocurrency to the Darkside group which is not a light decision.

The Darkside group announced that they are being closed following a loss of access to part of their infrastructure. The group servers were compromised, and the cryptocurrency has been transferred from the group account which uses for internal payments.

Russian OSINT

DarkSide CLOSED

Servers were seized (country not named), money of advertisers and founders was transferred to an unknown account. Ransom topics will be removed from the forums.

REvil's comment from the exp: In connection with the recent events in the USA, sorry for being straightforward, DarkSide Ransomware, a quote from the previously named PP:

Since the first version, we promised to speak honestly and openly about the problems. A few hours ago, we lost access to the public part of our infrastructure, namely: the

Blog.
Payment server.
DOS servers.

Now these servers are unavailable via SSH, the hosting panels are blocked. Hosting support, apart from information "at the request of law enforcement agencies", does not provide any other information.

Also, a few hours after the withdrawal, funds from the payment server (ours and clients') were withdrawn to an unknown address.

CyOps Team

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

Mitre Att&ck Matrix

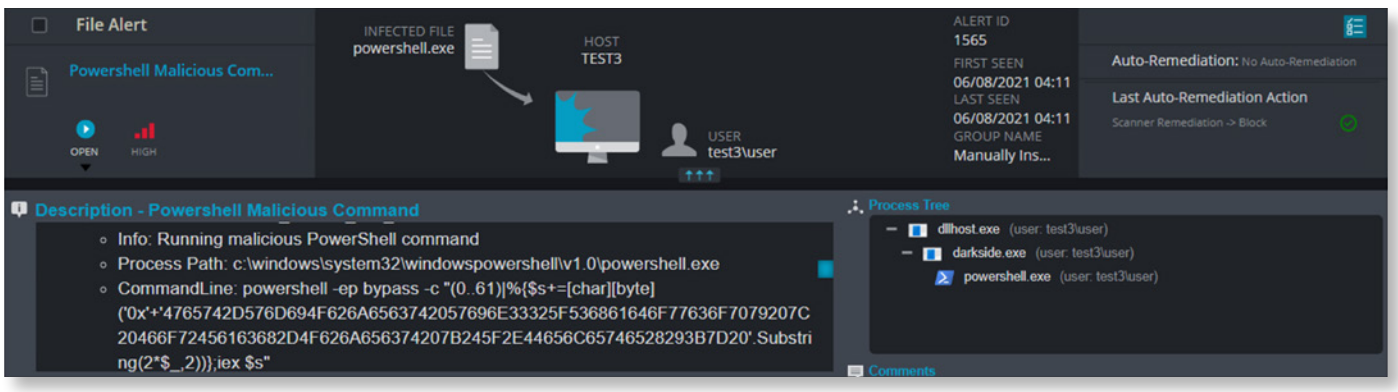
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts 2	Service Execution 1 2	Valid Accounts 2	Valid Accounts 2	Masquerading 1 1	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Data Encrypted for Impact 1
Default Accounts	Native API 1	Windows Service 1 4	Access Token Manipulation 2	Valid Accounts 2	LSASS Memory	Virtualization/Sandbox Evasion 2	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	Defacement 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Windows Service 1 4	Virtualization/Sandbox Evasion 2	Security Account Manager	Process 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	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 1 1	Access Token Manipulation 2	NTDS	Account Discovery 1	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	Process Injection 1 1	LSA Secrets	System Owner/User 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	System Service 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	Remote System 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	File and Directory Discovery 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	System Information Discovery 1 4 4	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Threat Intelligence Detection - Malicious Binary

This alert trigger when Cynet detects a file that is flagged as malicious in Cynet's internal threat intelligence database.

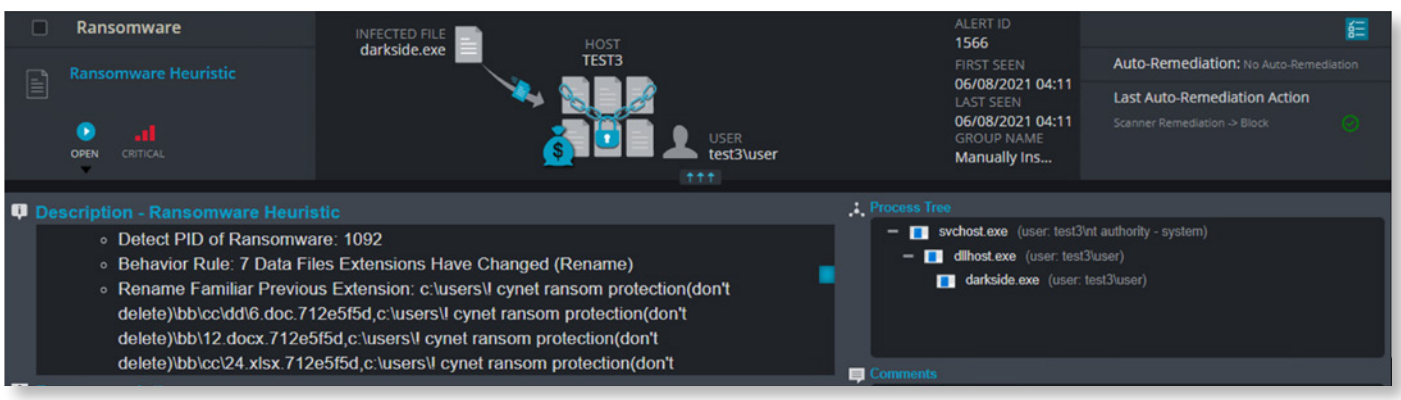
PowerShell Malicious Command

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



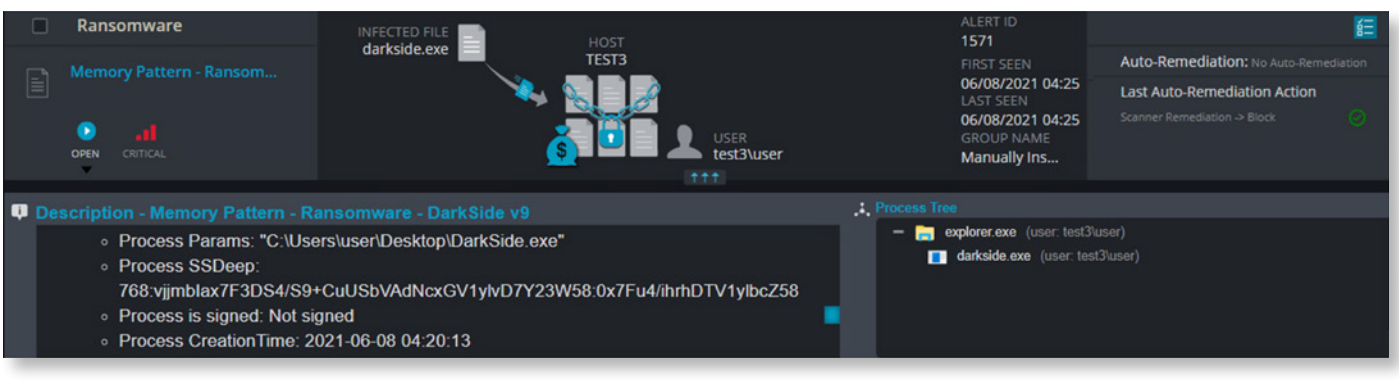
Ransomware Heuristic

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.



THREAT ANALYSIS - EPSILON RED RANSOMWARE

On the end of May, a new ransomware named Epsilon Red has revealed.

This kind of ransomware programmed in Go language.

The name came from Marvel story of the "super-soldier" Russian project which had a special ability to breathe in space, had various weapons and four tentacles.

So far, the ransomware has been observed targeting unpatched exchange servers, once the attacker gained the initial access to a victim machine, he begun to move laterally from the compromised host to other hosts using WMI which gave him the ability to install malicious components remotely.

On an early stage, the attackers used several PowerShell scripts intended to weaken the system by attempting to uninstall security products & Windows Defender, set persistence, dump credentials using VSS-Copy, block ports on firewall except RDP, and cleaning up its tracks.

This type of running scripts on a compromised network activity had been seen often on the last month as part of many ransomware variants incidents such as Conti, Ryuk & Sodinokibi in contrast to instances where the ransomware used to perform all these activities by themselves.

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 1	Path Interception	Process Injection 1 2	Masquerading 2 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	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 1 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	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 2	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	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	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 1	LSA Secrets	Remote System 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	Timestomp 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

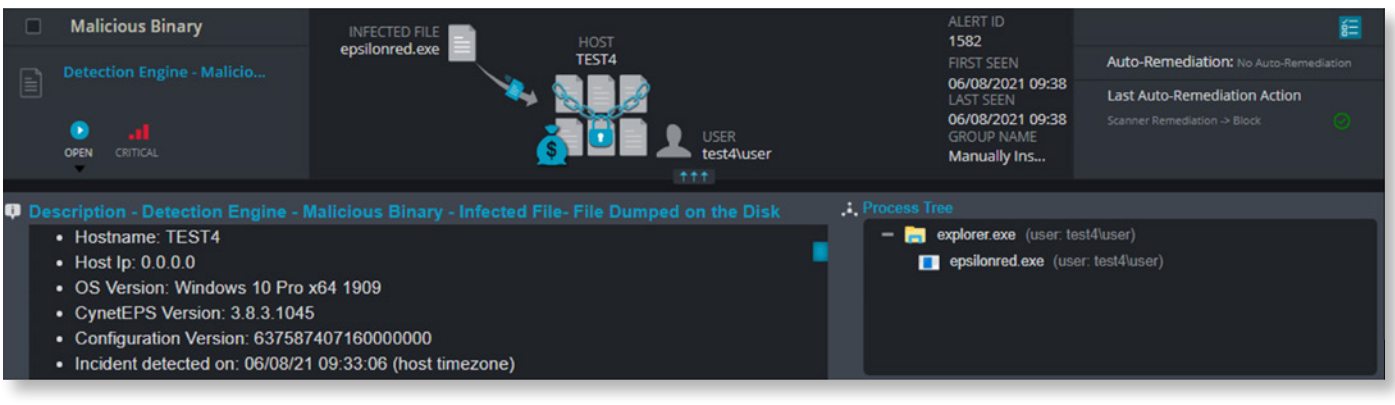
CYNET360 VS. EPSILON RED RANSOMWARE

Memory Pattern

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

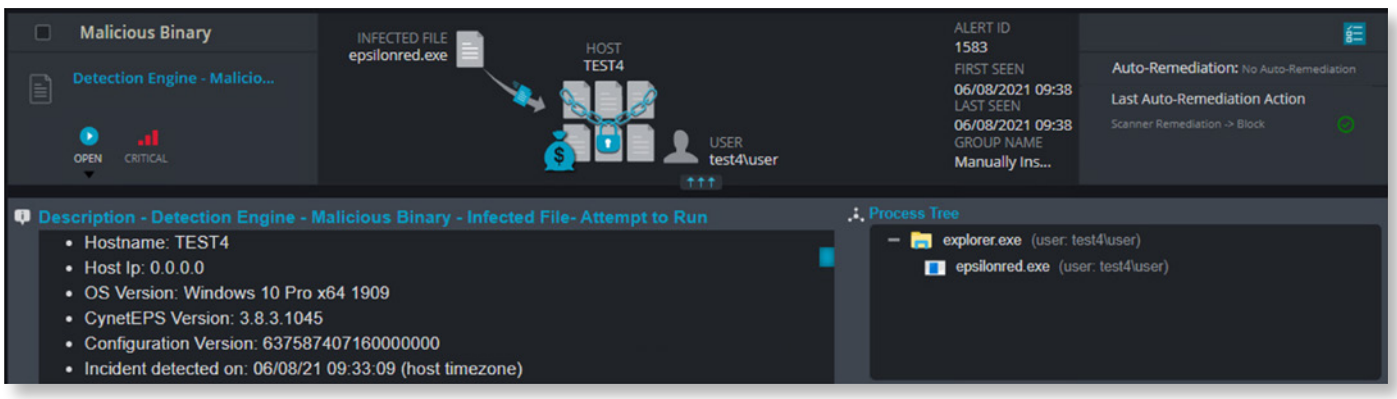
Detection Engine - Malicious Binary - Infected File- File Dumped on the Disk

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



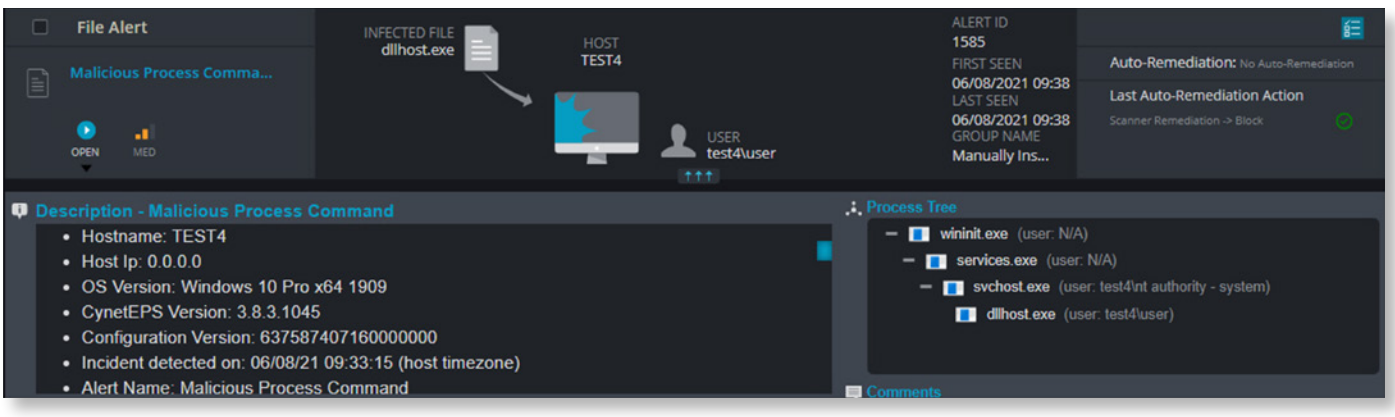
Detection Engine - Malicious Binary - Infected File- Attempt to Run

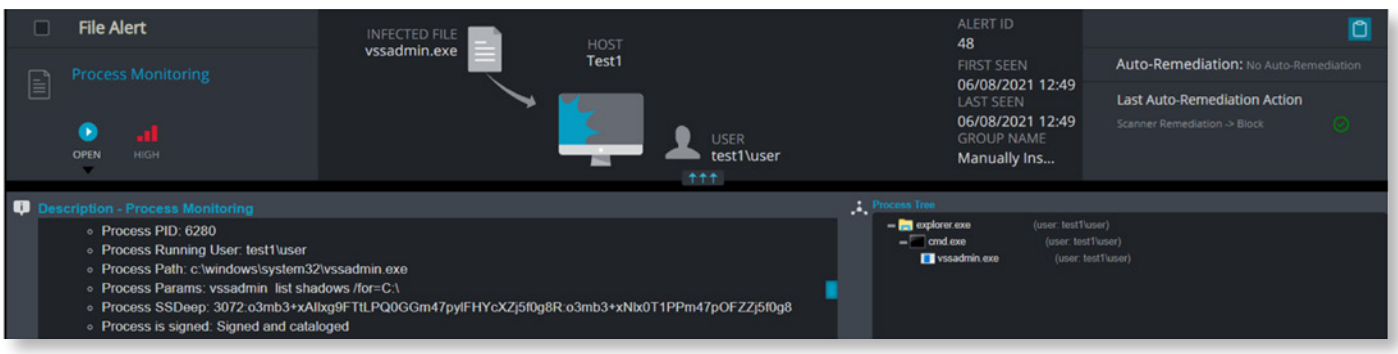
The alert trigger when Cynet's AV/AI engine detects a malicious file that was loaded to the memory.

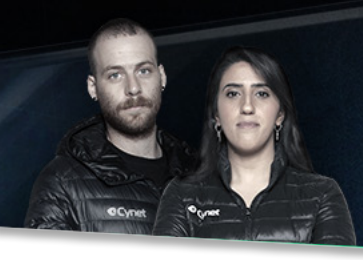


Malicious Process Command

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







CyOps Team

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

DISCLOSED VULNERABILITIES:

1. NEW VMWARE VULNERABILITY DETECTED IN VCENTER SERVER

Risk Level	
High	
Targeted Assets	**Threat Actors**
Windows and linux assets	Various
Tactic	**Technique**
Lateral movement	Exploitation of Remote Services
Mitigations	
Follow VMware recommendations	

As part of our ongoing threat intelligence efforts to discover emerging threats and vulnerabilities, the CyOps team would like to bring a new risk to your attention. The threat is associated with five vulnerable default plugins installed in VMWare vCenter Server. This vulnerability can be abused by threat actors to remotely execute arbitrary code.

1. Virtual SAN Health Check
2. vRealize Operations Manager
3. Site Recovery
4. vSphere Lifecycle Manager
5. VMware Cloud Director Availability

The vulnerabilities described above are assigned to the following CVEs:

- CVE-2021-21972 – VMSA-2021-0002 – vRealize Operations Manager Plugin
- CVE-2021-21985 – VMSA-2021-0010 – Virtual SAN Health Check Plugin
- CVE-2021-21986 – VMSA-2021-0010 – Virtual SAN Health Check, Site Recovery, vSphere Lifecycle Manager, and VMware Cloud Director Availability Plugins

All CVEs mentioned above allow a malicious actor to perform remote code execution on the hosting Operating System without privilege limitations. This can be achieved when an adversary has network access by using port 443 to infiltrate the vCenter Server.
Following VMware's instructions, below is a summary of a workaround to temporarily prevent exploitation until a patch is released:

Workaround

Important: Plugins must be set to "incompatible." Disabling a plugin from within the UI does not prevent exploitation.

The following actions must be performed on both the active and passive nodes in environments running vCenter High Availability (VCHA).

The examples documented here show the steps to disable all plugins which have been impacted by vulnerabilities disclosed by VMware. Depending on your environment and your requirements, you may only want to only disable a subset of these plugins.
Please see the VMSA-2021-0010: What You Need to Know blog to determine the plugins that are required to be disabled in your configuration.

Add the lines below to the compatibility-matrix.xml file to disable each individual plugin:

Plugin Name	Configuration Line
VMware vRops Client Plugin	`<PluginPackage id="com.vmware.vrops.install" status="incompatible"/>`
VMware vSAN H5 Client Plugin	`<PluginPackage id="com.vmware.vsphere.client.h5vsan" status="incompatible"/>`
Site Recovery	`<PluginPackage id="com.vmware.vrUi" status="incompatible"/>`
VMware vSphere Life-cycle Manager	`<PluginPackage id="com.vmware.vum.client" status="incompatible"/>`
VMware Cloud Director Availability	`<PluginPackage id="com.vmware.h4.vsphere.client" status="incompatible"/>`

Some plugins are enabled by default, and these default plugins differ from version to version.
Please refer to the table below to determine which plugin is enabled by default and which plugin requires the associated product to be installed and configured.

Apart from our recommendation to disable the mentioned plugins as described above, you can rest assured that the Cynet CyOps team is constantly monitoring your environment and will update if we observe and detect suspicious behavior or activities.

2. PulseSecure VPN

Risk Level	
Critical	
Targeted Assets	**Threat Actors**
Windows	Various Attackers
Tactic	**Technique**
Lateral movement	T1021.002 - Remote Services: SMB/Windows Admin Shares
Mitigations	
• **Upgrade to PCS Server version 9.1R.11.5** • **If upgrade is not possible at the moment – use the workaround file provided by Ivanti.**	

A new vulnerability in Pulse Secure VPN has been disclosed in 14th of May. The security advisory describes a buffer overflow bug in Windows File Resource Profiles, that enables a remote authenticated user with privileges to traverse between the SMB shares and exploit them to preform remote code execution as a high privileged user.

A malicious actor can exploit this vulnerability by inputting a long server name for SMB activities, The "smbclt" will crash in consequence of either buffer overflow or heap overflow – depending on the length of the server's name provided by the attacker.

The server will be vulnerable when a specific windows file access policy is enabled that will allows usage of regex and wildcard, so the attacker will be able to use this pattern - " * " or, by the default enabled policy in all PCS versions starting from 9.1R2 – that enables remote connections to arbitrary SMB hosts.

A remote code execution (RCE) attack will occur if a threat actor fraudulently gains access and manipulates a computer or server without authorization from its owner. Once the threat actor has compromised the server, he will execute malicious commands for further exploitation \ lateral movement \ network & assets discovery \ file encryption \ C2 communication \ payload dumping, and much more.

As of now – The company behind Pulse Secure VPN did not release an official patch to mitigate this vulnerability but has provided a workaround xml file that disables the Windows File Share Browser to cut short exploitation attempts.

3. New Dell Vulnerability Detected

Risk Level	
Critical	
Targeted Assets	**Threat Actors**
Dell Endpoints	Various
Tactic	**Technique**
Privilege escalation	Exploitation for Privilege Escalation
Mitigations	
Follow Dell's instructions and use Cynet360	

As part of our ongoing threat intelligence efforts to discover emerging threats and vulnerabilities, the CyOps team would like to bring a new risk to your attention. The risk is associated with a vulnerable file from Dell "dbutil_2_3.sys" along with 5 newly discovered vulnerabilities related to the file, a Dell driver that Dell machines install and load during the BIOS update process that is unloaded at the next reboot.

The vulnerabilities are collectively assigned to CVE-2021-21551:

- CVE-2021-21551 Local Elevation of Privileges Memory corruption
- CVE-2021-21551 Local Elevation of Privileges Memory corruption
- CVE-2021-21551 Local Elevation of Privileges Lack of input validation
- CVE-2021-21551 Local Elevation of Privileges Lack of input validation
- CVE-2021-21551 Denial of Service Code logic issue

These types of vulnerabilities are not considered critical since an attacker exploiting them needs to have previously compromised the computer. However, when successful, it allows attackers to gain persistence on infected hosts.

Following Dell's Instructions, below is a summary of steps to mitigate these vulnerabilities:

Remediation Steps:
Impacted customers must complete 2 steps as follows:

1. Immediately remove the vulnerable *dbutil_2_3.sys* driver from the affected system using one of the following options from Step 1 below: download and run a utility to remove the driver from the system (Option 1), manually remove the driver from the system (Option 2), or on or after May 10, 2021, utilize one of the Dell notification solutions to run the utility (Option 3).
2. As described in Step 2 below, obtain and run the latest firmware update utility package(s), Dell Command Update, Dell Update, Alienware Update, Dell System Inventory Agent, or Dell Platform Tags as applicable.

Step 1: Immediately remove the vulnerable *dbutil_2_3.sys* driver from the affected system using one of the options below. NOTE: If you are using the Dell System Inventory Agent you must first download the latest available version (2.6.0.0 or greater) here.

- **Option 1 (Recommended):** Download and run the Dell Security Advisory Update – DSA-2021-088 utility.
- **Option 2:** Manually remove the vulnerable *dbutil_2_3.sys* driver:

  Step A: Check the following locations for the *dbutil_2_3.sys* driver file
  - C:\Users\<username>\AppData\Local\Temp
  - C:\Windows\Temp

  Step B: Select the dbutil_2_3.sys file and hold down the SHIFT key while pressing the DELETE key to permanently delete.

CyOps Team

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

Cynet provides full visibility on Dell ".sys" drivers and enables security and IT personnel to remotely mitigate the vulnerability and delete the file via Cynet360 Console.

The following easy steps will assist in this task:

Figure 01: Enable the threat hunting module via the scan group settings.

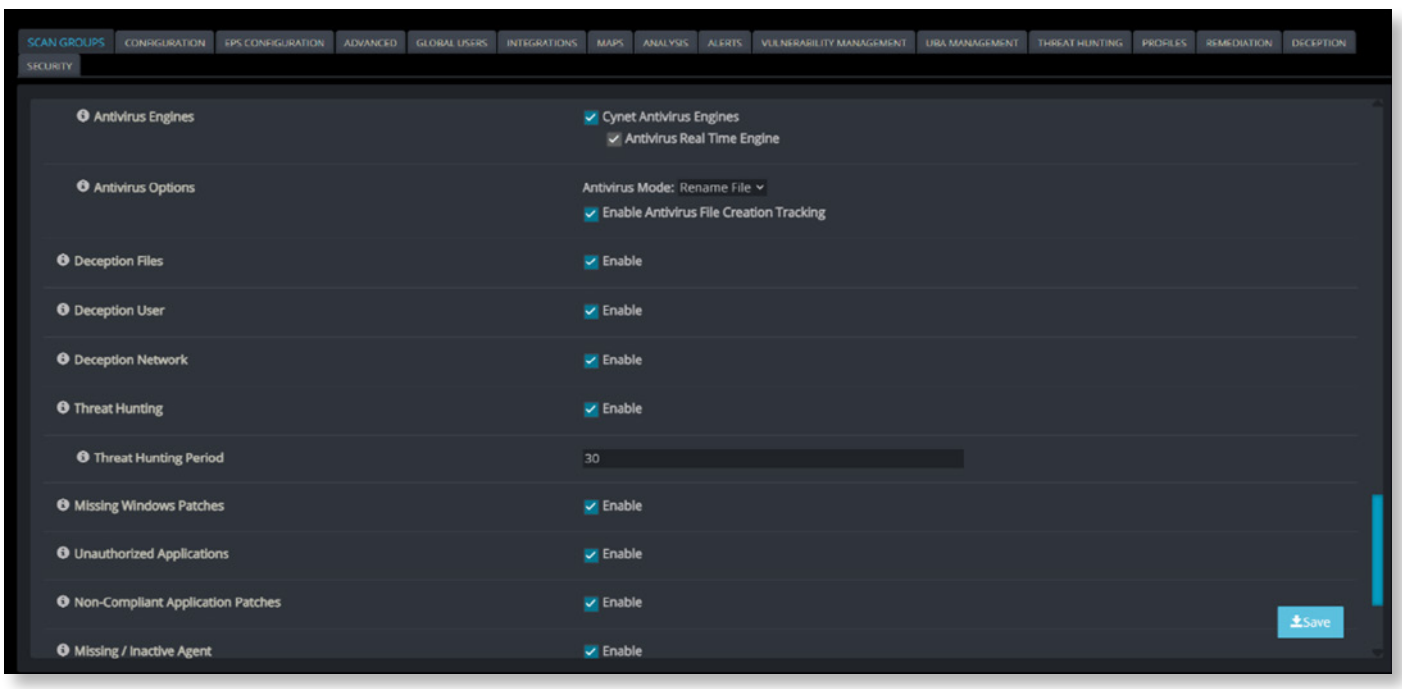


Figure 02: Using the threat hunting module to create a policy with the "dbutil_2_3.sys" value.

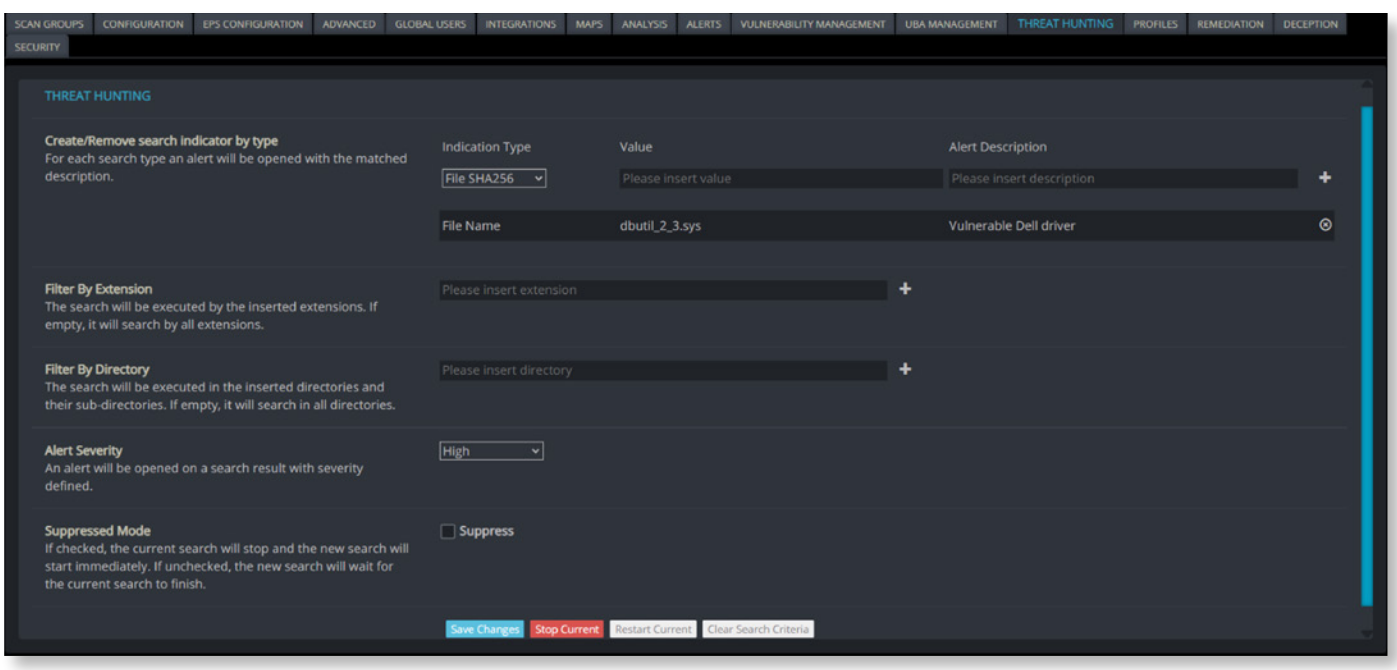


Figure 03: An alert will be triggered upon detection by the threat hunting policy.

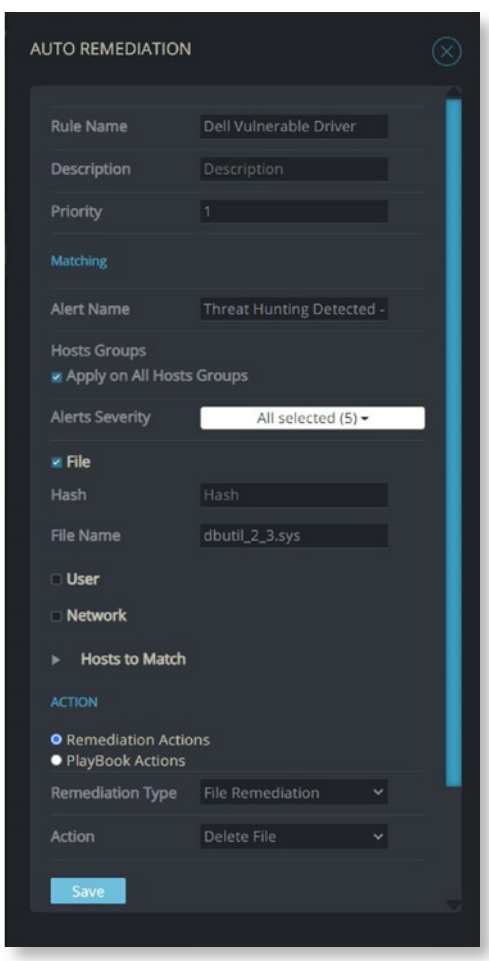


Figure 04: Create an Auto-Remediation rule to delete the vulnerable driver.

As always, we are available for any question or concerns and in any case further assistance is required.

APPENDIX:

Risk Level

Low
Medium
High
Critical

TLP Protocol

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation or operations if misused.	recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting or conversation in which it was originaly disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. in most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must beadhered to.**
TLP:GREEN Limited disclosure, restricted to community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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