Trellix Global Defenders: Analysis and Protections for BlackByte Ransomware

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

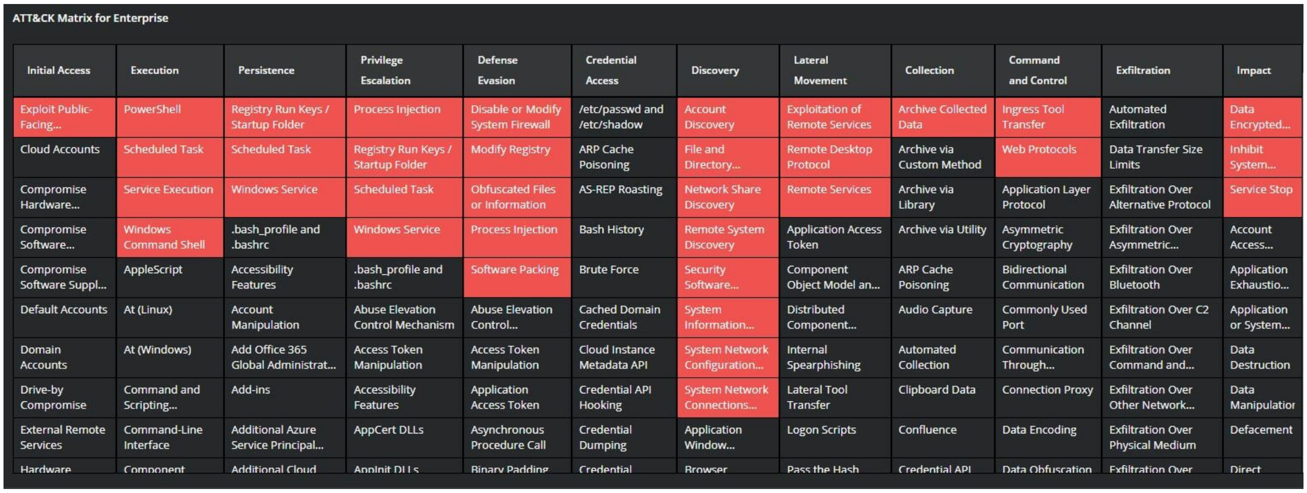
Stories

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

By Taylor Mullins · February 28, 2022

BlackByte Ransomware has been in the news of late due to a successful attack against a National Football League (NFL) Franchise and a Joint Cybersecurity Advisory by the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USSS) warning on breaches to the networks of at least three organizations from US critical infrastructure sectors in the last three months. BlackByte Ransomware is currently being offered to threat actors as a Ransomware-as-a-Service (RaaS) and makes use of PowerShell and Windows CLI commands to carry out various tasks such as network discovery, task scheduling and to create and disable Windows and security services.

BlackByte Ransomware makes files inaccessible by encrypting them and generates a ransom note (the "BlackByte_restoremyfiles.hta" file) that contains instructions on how to contact the attackers for data decryption and other details. Also, BlackByte appends the ".blackbyte" extension to the names of encrypted files. BlackByte does have worming capabilities and can infect additional endpoints on the same network.



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing...	PowerShell	Registry Run Keys / Startup Folder	Process Injection	Disable or Modify System Firewall	/etc/passwd and /etc/shadow	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Ingress Tool Transfer	Automated Exfiltration	Data Encrypted...
Cloud Accounts	Scheduled Task	Scheduled Task	Registry Run Keys / Startup Folder	Modify Registry	ARP Cache Poisoning	File and Directory...	Remote Desktop Protocol	Archive via Custom Method	Web Protocols	Data Transfer Size Limits	Inhibit System...
Compromise Hardware...	Service Execution	Windows Service	Scheduled Task	Obfuscated Files or Information	AS-REP Roasting	Network Share Discovery	Remote Services	Archive via Library	Application Layer Protocol	Exfiltration Over Alternative Protocol	Service Stop
Compromise Software...	Windows Command Shell	.bash_profile and .bashrc	Windows Service	Process Injection	Bash History	Remote System Discovery	Application Access Token	Archive via Utility	Asymmetric Cryptography	Exfiltration Over Asymmetric...	Account Access...
Compromise Software Suppl...	AppleScript	Accessibility Features	.bash_profile and .bashrc	Software Packing	Brute Force	Security Software...	Component Object Model an...	ARP Cache Poisoning	Bidirectional Communication	Exfiltration Over Bluetooth	Application Exhaustio...
Default Accounts	At (Linux)	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control...	Cached Domain Credentials	System Information...	Distributed Component...	Audio Capture	Commonly Used Port	Exfiltration Over C2 Channel	Application or System...
Domain Accounts	At (Windows)	Add Office 365 Global Administrat...	Access Token Manipulation	Access Token Manipulation	Cloud Instance Metadata API	System Network Configuration...	Internal Spearphishing	Automated Collection	Communication Through...	Exfiltration Over Command and...	Data Destruction
Drive-by Compromise	Command and Scripting...	Add-ins	Accessibility Features	Application Access Token	Credential API Hooking	System Network Connections...	Lateral Tool Transfer	Clipboard Data	Connection Proxy	Exfiltration Over Other Network...	Data Manipulatior
External Remote Services	Command-Line Interface	Additional Azure Service Principal...	AppCert DLLs	Asynchronous Procedure Call	Credential Dumping	Application Window...	Logon Scripts	Confluence	Data Encoding	Exfiltration Over Physical Medium	Defacement
Hardware	Component	Additional Cloud	AppInit DLLs	Binary Padding	Credential	Browser	Pass the Hash	Credential API	Data Obfuscation	Exfiltration Over	Direct

Figure 1. MITRE ATT&CK Framework for BlackByte Ransomware

Recommended Steps to Prevent Initial Access

The Joint Cybersecurity Advisory provides several recommendations to secure your environment against BlackByte that were gathered from their analysis of malware samples discovered in the wild.

- BlackByte operators have been observed exploiting the following CVEs to gain initial access, patching is recommended to prevent exploitation.
    - CVE-2021-34473 - Microsoft Exchange Server Remote Code Execution Vulnerability
    - CVE-2021-34523 - Microsoft Exchange Server Elevation of Privilege Vulnerability
    - CVE-2021-31207 - Microsoft Exchange Server Security Feature Bypass Vulnerability

- Blocking IP Addresses known to download additional payloads in BlackByte attacks prior to encryption: **185.93.6.31** and **45.9.148.114.**
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs for any unusual activity.
- After gaining access to the service accounts some adversaries have utilized AnyDesk for lateral movement, monitoring for AnyDesk activity can be an early indicator of compromise if AnyDesk is not utilized or allowed by your organization.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Disable hyperlinks in received emails.

Joint Cybersecurity Advisory: Indicators of Compromise Associated with BlackByte Ransomware

Trellix Protections and Global Detections

Trellix Global Threat Intelligence is currently detecting all known analyzed indicators for this campaign.

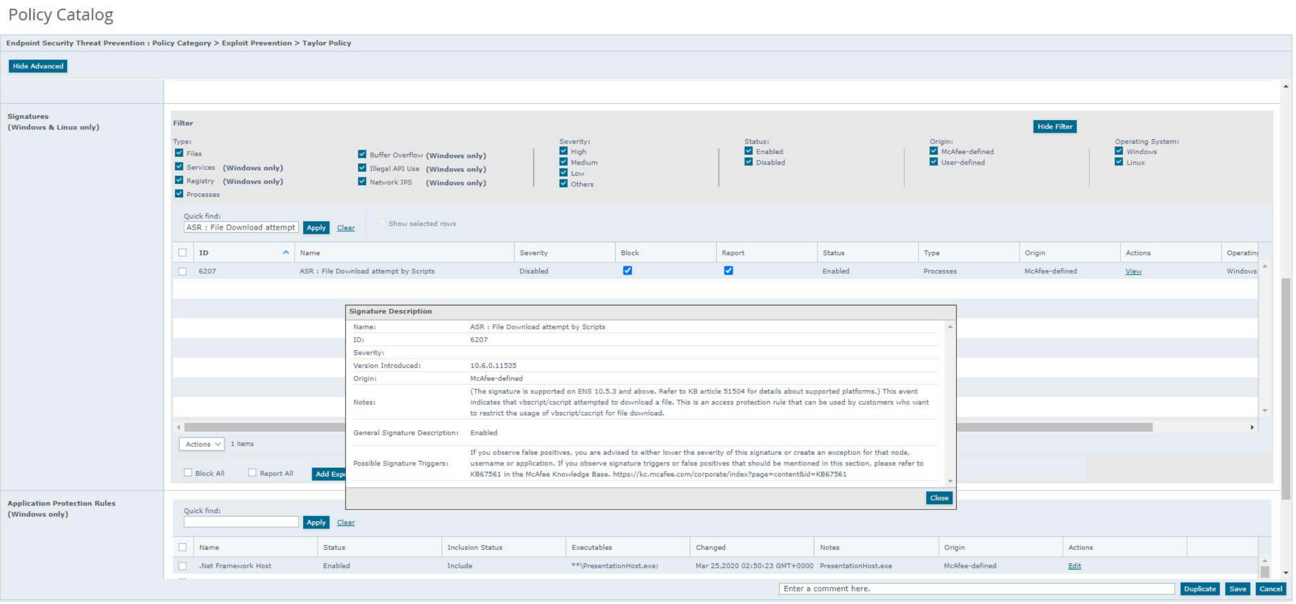
McAfee Products detecting this threat globally
BY PRODUCTS
ENS SCANNERS
ENS 10.7

Figure 2. Trellix Products detecting this threat globally. Source: MVISION Insights

Blocking BlackByte Attacks with Endpoint Security

Trellix ENS is currently detecting BlackByte Indicators of Compromise (IOCs) from the standpoint of signature detections and the malware behavior associated with BlackByte Ransomware attacks. The following Exploit Prevention Rule in ENS has shown success in stopping BlackByte samples due to BlackByte being Script-based. Trellix always recommends testing in Report Only Mode before blocking to confirm no false positives are being detected by this signature rule.

Exploit Prevention Signature ID 6207: ASR : File Download attempt by Scripts



Policy Catalog

Endpoint Security Threat Prevention : Policy Category > Exploit Prevention > Taylor Policy

Signatures (Windows & Linux only)

Filter

Type:
☑ Files
☑ Services (Windows only)
☑ Registry (Windows only)
☑ Processes
☑ Buffer Overflow (Windows only)
☑ Illegal API Use (Windows only)
☑ Network IPS (Windows only)

Severity:
☑ High
☑ Medium
☑ Low
☑ Others

Status:
☑ Enabled
☑ Disabled

Origin:
☑ McAfee-defined
☑ User-defined

Operating System:
☑ Windows
☑ Linux

Quick find: ASR : File Download attempt

□	ID	Name	Severity	Block	Report	Status	Type	Origin	Actions	Operatin
□	6207	ASR : File Download attempt by Scripts	Disabled	☑	☑	Enabled	Processes	McAfee-defined	View	Windows

Signature Description

Name:	ASR : File Download attempt by Scripts
ID:	6207
Severity:	
Version Introduced:	10.6.0.11535
Origin:	McAfee-defined
Notes:	(The signature is supported on ENS 10.5.3 and above. Refer to KB article 51504 for details about supported platforms.) This event indicates that vbscript/cscript attempted to download a file. This is an access protection rule that can be used by customers who want to restrict the usage of vbscript/cscript for file download.
General Signature Description:	Enabled
Possible Signature Triggers:	If you observe false positives, you are advised to either lower the severity of this signature or create an exception for that node, username or application. If you observe signature triggers or false positives that should be mentioned in this section, please refer to KB67561 in the McAfee Knowledge Base. https://kc.mcafee.com/corporate/index?page=content&id=KB67561

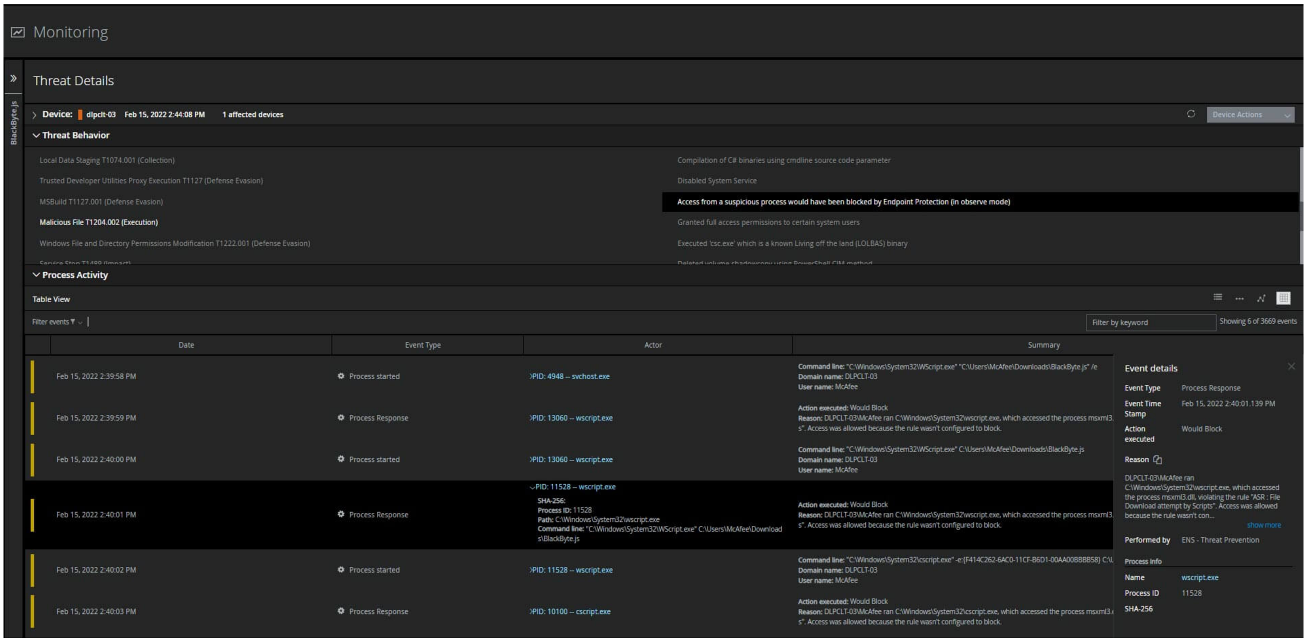
Application Protection Rules (Windows only)

Quick find:

□	Name	Status	Inclusion Status	Executables	Changed	Notes	Origin	Actions
□	.Net Framework Host	Enabled	Include	**\PresentationHost.exe:	Mar 25,2020 02:50:23 GMT+0000	PresentationHost.exe	McAfee-defined	Edit

Enter a comment here.

Figure 3. Exploit Prevention Rule in ePolicy Orchestrator/MVISION ePO



Monitoring

Threat Details

Device: dlpclt-03 Feb 15, 2022 2:44:08 PM 1 affected devices

Threat Behavior

Local Data Staging T1074.001 (Collection)	Compilation of C# binaries using cmdline source code parameter
Trusted Developer Utilities Proxy Execution T1127 (Defense Evasion)	Disabled System Service
MSBuild T1127.001 (Defense Evasion)	Access from a suspicious process would have been blocked by Endpoint Protection (in observe mode)
Malicious File T1204.002 (Execution)	Granted full access permissions to certain system users
Windows File and Directory Permissions Modification T1222.001 (Defense Evasion)	Executed 'csc.exe' which is a known Living off the land (LOLBAS) binary
Service Stop T1489 (Impact)	Deleted volume shadowcopy using PowerShell CIM method

Process Activity

Table View

Filter events

Filter by keyword

Showing 6 of 3669 events

Date	Event Type	Actor	Summary
Feb 15, 2022 2:39:58 PM	Process started	›PID: 4948 -- svchost.exe	**Command line:** "C:\Windows\System32\WScript.exe" "C:\Users\McAfee\Downloads\BlackByte.js" /e **Domain name:** DLPCLT-03 **User name:** McAfee
Feb 15, 2022 2:39:59 PM	Process Response	›PID: 13060 -- wscript.exe	**Action executed:** Would Block **Reason:** DLPCLT-03\McAfee ran C:\Windows\System32\wscript.exe, which accessed the process msxml3. s". Access was allowed because the rule wasn't configured to block.
Feb 15, 2022 2:40:00 PM	Process started	›PID: 13060 -- wscript.exe	**Command line:** "C:\Windows\System32\WScript.exe" C:\Users\McAfee\Downloads\BlackByte.js **Domain name:** DLPCLT-03 **User name:** McAfee
Feb 15, 2022 2:40:01 PM	Process Response	⌄PID: 11528 -- wscript.exe **SHA-256:** **Process ID:** 11528 **Path:** C:\Windows\System32\wscript.exe **Command line:** "C:\Windows\System32\WScript.exe" C:\Users\McAfee\Downloads\BlackByte.js	**Action executed:** Would Block **Reason:** DLPCLT-03\McAfee ran C:\Windows\System32\wscript.exe, which accessed the process msxml3. s". Access was allowed because the rule wasn't configured to block.
Feb 15, 2022 2:40:02 PM	Process started	›PID: 11528 -- wscript.exe	**Command line:** "C:\Windows\System32\cscript.exe" -e:{F414C262-6AC0-11CF-B6D1-00AA00BBBB58} C:\U **Domain name:** DLPCLT-03 **User name:** McAfee
Feb 15, 2022 2:40:03 PM	Process Response	›PID: 10100 -- cscript.exe	**Action executed:** Would Block **Reason:** DLPCLT-03\McAfee ran C:\Windows\System32\cscript.exe, which accessed the process msxml3. s". Access was allowed because the rule wasn't configured to block.

Event details

Event Type	Process Response
Event Time Stamp	Feb 15, 2022 2:40:01.139 PM
Action executed	Would Block

Reason

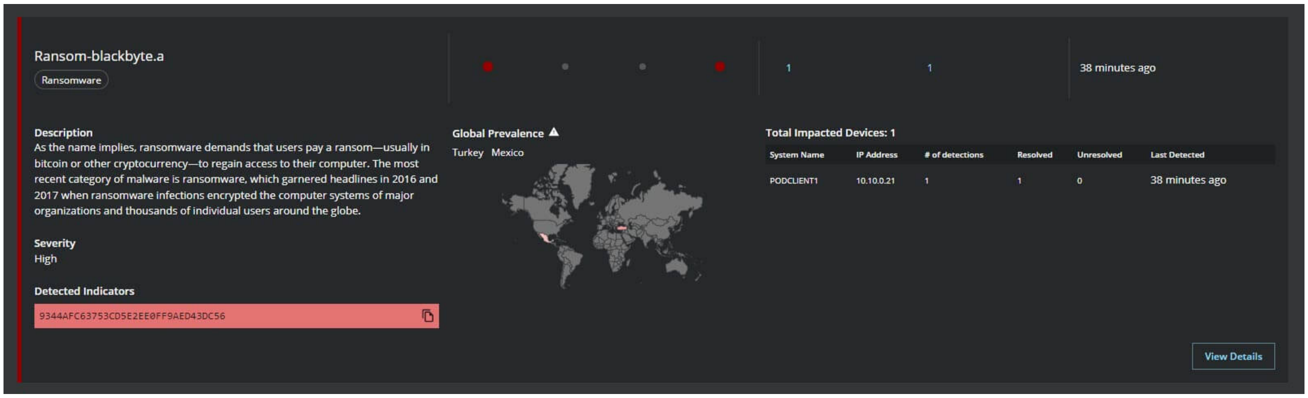
DLPCLT-03\McAfee ran C:\Windows\System32\wscript.exe, which accessed the process msxml3.dll, violating the rule "ASR : File Download attempt by Scripts". Access was allowed because the rule wasn't con...

Performed by	ENS - Threat Prevention

Process info

Name	wscript.exe
Process ID	11528
SHA-256	

Figure 4. MVISION EDR noting where Endpoint Protection (ENS) could have stopped specific techniques


Ransom-blackbyte.a

Ransomware

1 1 38 minutes ago

Description

As the name implies, ransomware demands that users pay a ransom—usually in bitcoin or other cryptocurrency—to regain access to their computer. The most recent category of malware is ransomware, which garnered headlines in 2016 and 2017 when ransomware infections encrypted the computer systems of major organizations and thousands of individual users around the globe.

Severity

High

Detected Indicators

9344AFC63753CD5E2EE0FF9AED43DC56

Global Prevalence

Turkey Mexico

Total Impacted Devices: 1

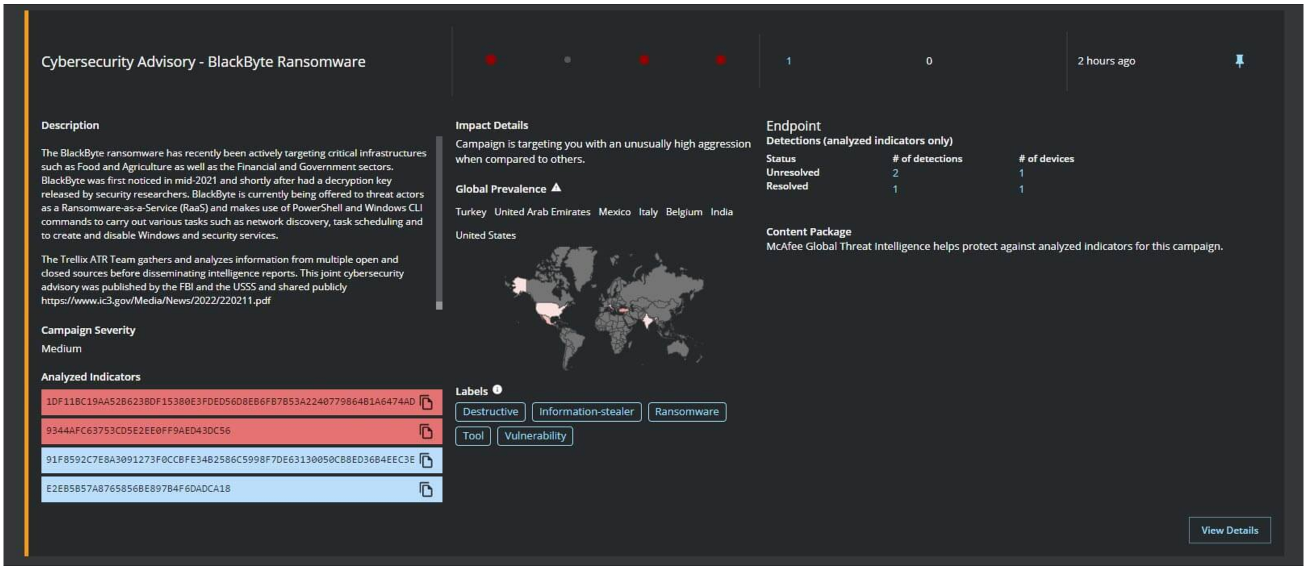
System Name	IP Address	# of detections	Resolved	Unresolved	Last Detected
PODCLIENT1	10.10.0.21	1	1	0	38 minutes ago

Figure 5. Ransomware Detection Name and Observed Detections noted in MVISION Insights

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

MVISION Insights will provide the current threat intelligence and known indicators for BlackByte 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.

MVISION Insights Campaign Names: Cybersecurity Advisory - BlackByte Ransomware and JavaScript Malware Threat Landscape


Cybersecurity Advisory - BlackByte Ransomware

1 0 2 hours ago

Description

The BlackByte ransomware has recently been actively targeting critical infrastructures such as Food and Agriculture as well as the Financial and Government sectors. BlackByte was first noticed in mid-2021 and shortly after had a decryption key released by security researchers. BlackByte is currently being offered to threat actors as a Ransomware-as-a-Service (RaaS) and makes use of PowerShell and Windows CLI commands to carry out various tasks such as network discovery, task scheduling and to create and disable Windows and security services.

The Trellix ATR Team gathers and analyzes information from multiple open and closed sources before disseminating intelligence reports. This joint cybersecurity advisory was published by the FBI and the USSS and shared publicly https://www.ic3.gov/Media/News/2022/220211.pdf

Campaign Severity

Medium

Analyzed Indicators

1DF11BC19AA52B623BDF15380E3FDED56D8EB6FB7B53A2240779864B1A6474AD

9344AFC63753CD5E2EE0FF9AED43DC56

91F8592C7E8A3091273F0CCBFE34B2586C5998F7DE63130050CB8ED36B4EEC3E

E2EB5B57A8765856BE897B4F6DADCA18

Impact Details

Campaign is targeting you with an unusually high aggression when compared to others.

Global Prevalence

Turkey United Arab Emirates Mexico Italy Belgium India United States

Labels

Destructive Information-stealer Ransomware Tool Vulnerability

Endpoint

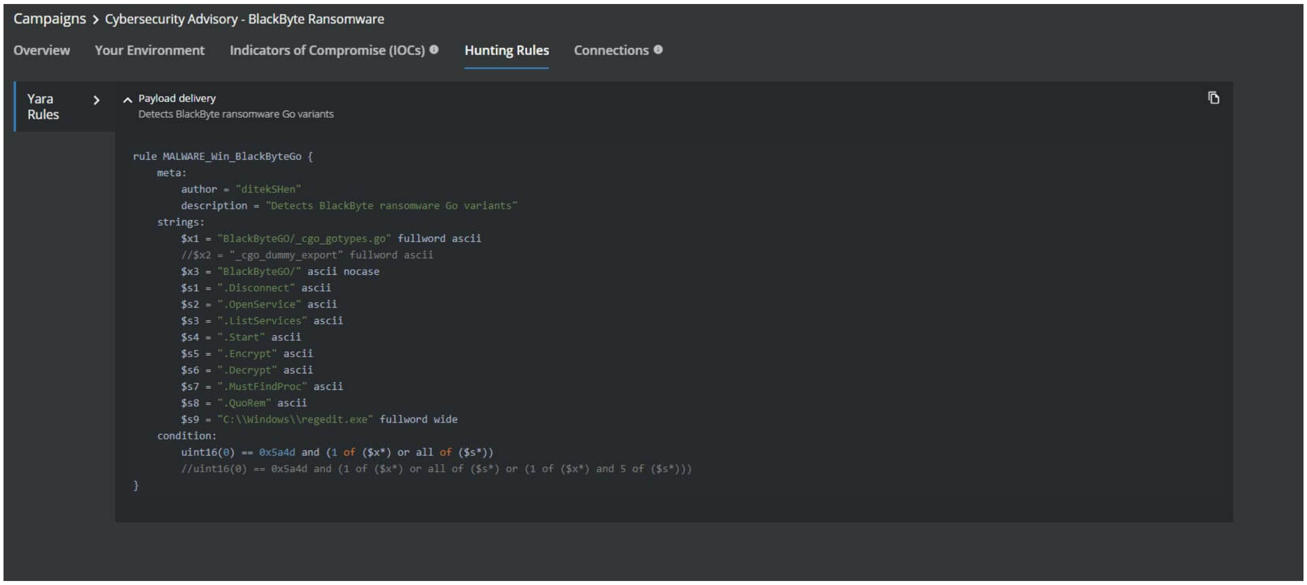
Detections (analyzed indicators only)

Status	# of detections	# of devices
Unresolved	2	1
Resolved	1	1

Content Package

McAfee Global Threat Intelligence helps protect against analyzed indicators for this campaign.

Figure 6. Campaign Details, Analyzed Indicators of Compromise, and Detections


Campaigns > Cybersecurity Advisory - BlackByte Ransomware
Overview
Your Environment
Indicators of Compromise (IOCs)
Hunting Rules
Connections
Yara Rules

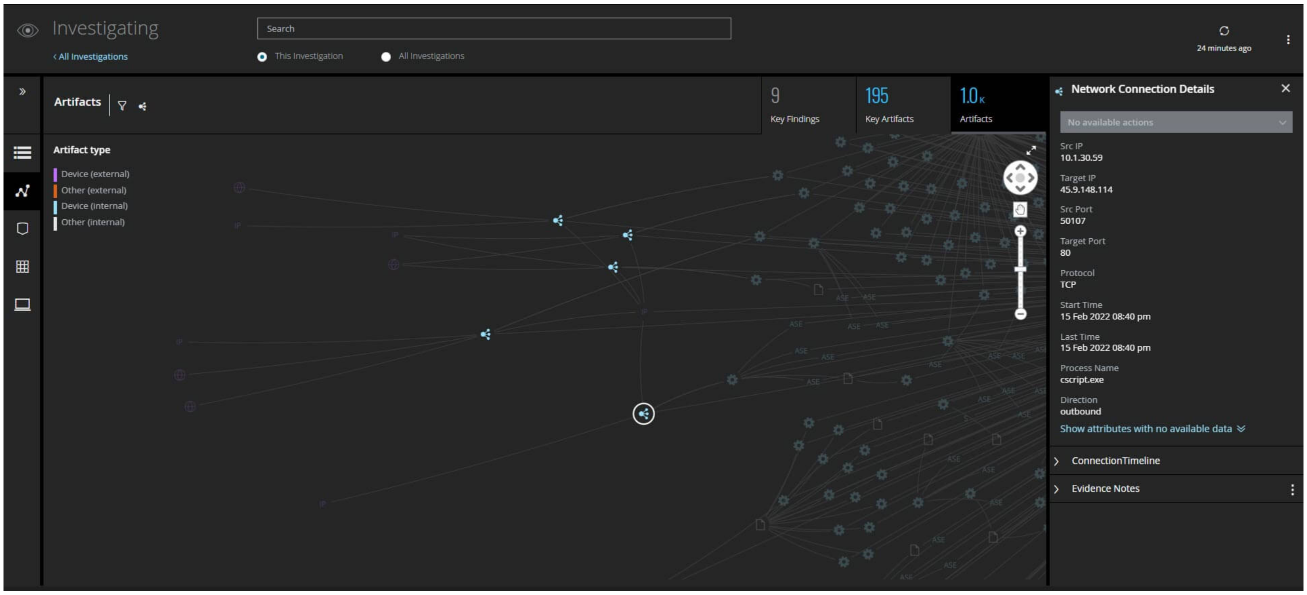
Payload delivery
Detects BlackByte ransomware Go variants

```
rule MALWARE_Win_BlackByteGo {
    meta:
        author = "ditekSHen"
        description = "Detects BlackByte ransomware Go variants"
    strings:
        $x1 = "BlackByteGO/_cgo_gotypes.go" fullword ascii
        //$x2 = "_cgo_dummy_export" fullword ascii
        $x3 = "BlackByteGO/" ascii nocase
        $s1 = ".Disconnect" ascii
        $s2 = ".OpenService" ascii
        $s3 = ".ListServices" ascii
        $s4 = ".Start" ascii
        $s5 = ".Encrypt" ascii
        $s6 = ".Decrypt" ascii
        $s7 = ".MustFindProc" ascii
        $s8 = ".QuoRem" ascii
        $s9 = "C:\\Windows\\regedit.exe" fullword wide
    condition:
        uint16(0) == 0x5a4d and (1 of ($x*) or all of ($s*))
        //uint16(0) == 0x5a4d and (1 of ($x*) or all of ($s*) or (1 of ($x*) and 5 of ($s*)))
}
```

Figure 7. Hunting Rules for BlackByte Ransomware in MVISION Insights

Detecting Malicious Activity with MVISION EDR

MVISION EDR is currently monitoring for the activity associated with BlackByte Ransomware and will note the MITRE techniques and any suspicious indicators related to the adversarial activity. Several of the techniques outlined in the Joint Advisory that are observed with BlackByte are noted below, monitoring for this type of activity can point to activity associated with the Tactics, techniques, and procedures (TTPs) for BlackByte.



Network Connection Details

Src IP
10.1.30.59

Target IP
45.9.148.114

Src Port
50107

Target Port
80

Protocol
TCP

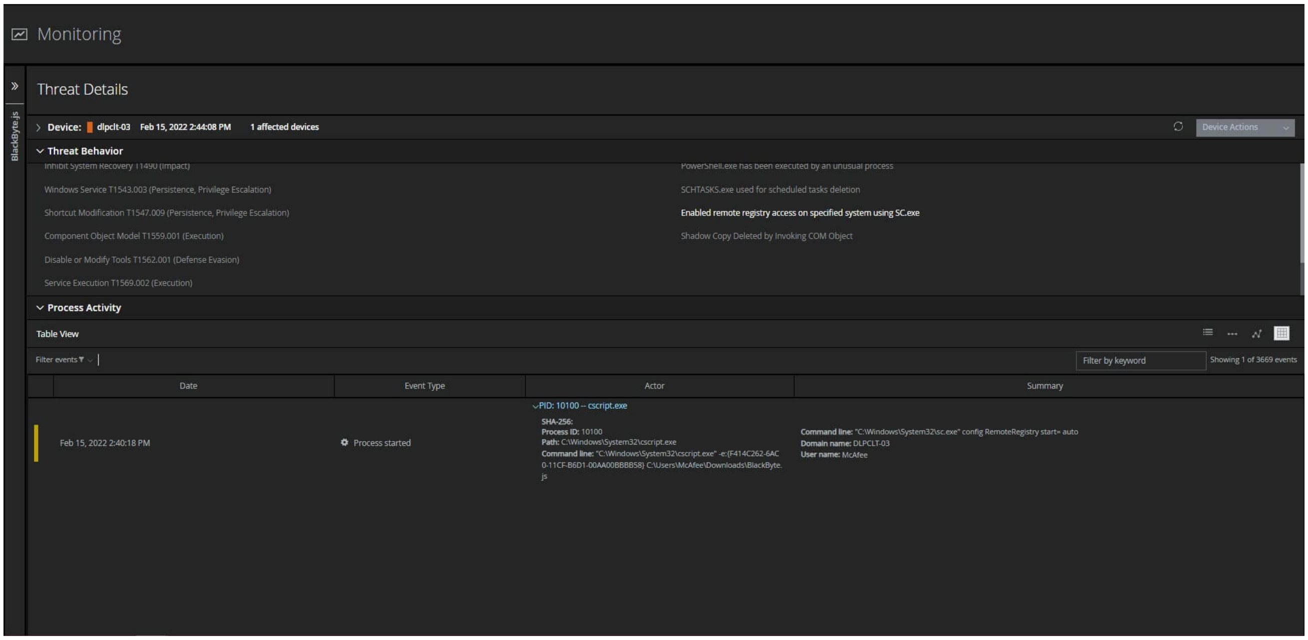
Start Time
15 Feb 2022 08:40 pm

Last Time
15 Feb 2022 08:40 pm

Process Name
cscript.exe

Direction
outbound

Figure 8. Network Connection to Known Malicious IP Address Associated with BlackByte



Threat Details

Device: dlpclt-03 Feb 15, 2022 2:44:08 PM 1 affected devices

Threat Behavior

Inhibit System Recovery T1490 (Impact)	PowerShell.exe has been executed by an unusual process
Windows Service T1543.003 (Persistence, Privilege Escalation)	SCHTASKS.exe used for scheduled tasks deletion
Shortcut Modification T1547.009 (Persistence, Privilege Escalation)	Enabled remote registry access on specified system using SC.exe
Component Object Model T1559.001 (Execution)	Shadow Copy Deleted by Invoking COM Object
Disable or Modify Tools T1562.001 (Defense Evasion)	
Service Execution T1569.002 (Execution)	

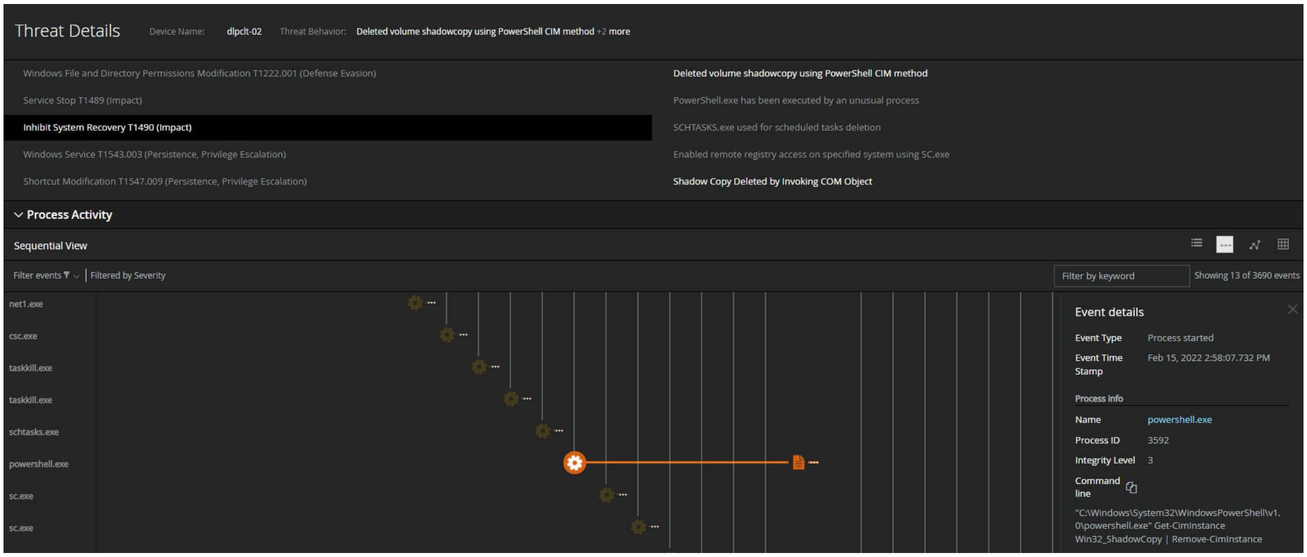
Process Activity

Table View

Filter events | Filter by keyword | Showing 1 of 3669 events

Date	Event Type	Actor	Summary
Feb 15, 2022 2:40:18 PM	Process started	PID: 10100 -- cscript.exe SHA-256: Process ID: 10100 Path: C:\Windows\System32\cscript.exe Command line: "C:\Windows\System32\cscript.exe" -e:{F414C262-6AC0-11CF-B6D1-00AA00BBBB58} C:\Users\McAfee\Downloads\BlackByte.js	Command line: "C:\Windows\System32\sc.exe" config RemoteRegistry start= auto Domain name: DLPCLT-03 User name: McAfee

Figure 9. Enabling of remote registry for possible preparation of Lateral Movement



Threat Details Device Name: dlpclt-02 Threat Behavior: Deleted volume shadowcopy using PowerShell CIM method +2 more

Windows File and Directory Permissions Modification T1222.001 (Defense Evasion)	Deleted volume shadowcopy using PowerShell CIM method
Service Stop T1489 (Impact)	PowerShell.exe has been executed by an unusual process
Inhibit System Recovery T1490 (Impact)	SCHTASKS.exe used for scheduled tasks deletion
Windows Service T1543.003 (Persistence, Privilege Escalation)	Enabled remote registry access on specified system using SC.exe
Shortcut Modification T1547.009 (Persistence, Privilege Escalation)	Shadow Copy Deleted by Invoking COM Object

Process Activity

Sequential View

Filter events | Filtered by Severity | Filter by keyword | Showing 13 of 3690 events

Event details

Event Type	Process started
Event Time Stamp	Feb 15, 2022 2:58:07.732 PM

Process Info

Name	powershell.exe
Process ID	3592
Integrity Level	3
Command line	

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Get-CimInstance Win32_ShadowCopy | Remove-CimInstance

Figure 10. Deletion of Shadow Copy to inhibit system recovery

Trellix offers Threat Intelligence Briefings along with Cloud Security and Data Protection workshops to provide customers with best practice recommendations on how to utilize their existing security controls to protect against adversarial and insider threats, please reach out if you would like to schedule a workshop with your organization.

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.