CylanceMDR

Release Notes

May 2024

Contents

What's new in CylanceMDR **4**

Fixed issues **5**

Known issues **6**

CylanceMDR protection enhancements **7**

Previous CylanceMDR protection enhancements 9

Legal notice **22**

What's new in CylanceMDR

What's new in the May 2024 update

- **New product name**: CylanceGUARD is now known as CylanceMDR.
- **CylanceMDR On-Demand**: The CylanceMDR On-Demand subscription is a convenient and helpful option if your organization monitors the alerts that are reported to the Cylance console. With this subscription, you can request CylanceMDR support on demand for any alerts that you think might be a threat but you need the time and expertise of a CylanceMDR analyst to help you resolve it. You can request support from an alert group in the Alerts view in the Cylance management console. CylanceMDR analysts are immediately notified with the alert details and can start their investigation and assess the threat. To follow up on the investigation (for example, to share additional details), you can log in to the CylanceMDR (CylanceGUARD) portal and find the alert in the Escalations screen.

  If you want to have dedicated CylanceMDR analysts monitoring alerts for you 24x7, consider the CylanceMDR Standard and CylanceMDR Advanced subscriptions. For more information see the CylanceMDR overview.

Fixed issues

May 2024 update

There were no fixed issues in this release.

Known issues

When trying to request on-demand assistance from the Cylance console for CylanceMDR, a "The CylanceMDR Support request could not be sent" error message appears if your CylanceMDR On Demand account setup has not been completed. Contact BlackBerry Support to complete the setup. (UES-17028)

CylanceMDR protection enhancements

Due to some emerging threats, CylanceMDR has implemented the following CylanceOPTICS rules for improved security and telemetry for analysts. These rules are already in effect and no further action is required from your organization.

Latest enhancements (April and May 2024)

Threat or vulnerability	Description
Updated rule for advanced detection of the execution of a Stager payload from PowerShell Empire	• **Rule Name**: "PowerShell Empire Stager Payload Executed" • **MITRE Techniques**: T1059, T1059.001, T1071, T1071.001 • **Description**: This rule detects the execution of a Stager related to Powershell Empire command and control activity. The rule pays attention to commonly used web requests such as /admin/get.php, /admin/news.php, and /login/process.php. PowerShell Empire is a post-exploitation framework used by security professionals and hackers to facilitate remote access and control of compromised systems through PowerShell scripts. • **Platform**: Windows • **Additional reference**: Red Team Notes • **Date added**: May 2024
Updated rule for advanced detection of the Csvde.exe export command	• **Rule Name**: "Csvde.exe Export Command" • **MITRE Techniques**: T1087, T1069, T1018, T1087.002, T1119 • **Description**: This rule detects the use of Csvde.exe for export data. Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifiers on a network that may be used for lateral movement from the current system. Cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use command line functionality to identify accounts. • **Platform**: Windows • **Additional reference**: MITRE • **Date added**: May 2024
Updated rule for advanced detection of local credential dump from NTDS, SAM or LSA using SecretsDump	• **Rule Name**: "Local Credential Dump from NTDS, SAM or LSA via SecretsDump" • **MITRE Techniques**: T1003, T1003.002, T1003.003, T1003.004, T1059, T1059.006 • **Description**: Adversaries may attempt to steal credential information from the NTDS file (%SystemRoot%\NTDS\Ntds.dit) or from the Windows Registry hives which store the Security Account Manager (SAM) database and Local Security Authority (LSA) secrets. This rule detects the usage of a tool called secretsdump.py, which can be used to locally dump the credential information like domain hashes from the NTDS.dit file, SAM, and LSA secrets from the exported registry hives. • **Platform**: Windows • **Additional reference**: Hacker Recipes NTDS, Hacker Recpies SAM & LSA • **Date added**: May 2024

Threat or vulnerability	Description
Updated rule for advanced detection of a remote credential dump from the registry hive	• **Rule Name**: “Remote Credential Dump from Registry Hive” • **MITRE Techniques**: T1003, T1003.002 • **Description**: This rule detects a Logon Type 3 event, a 'Remote Registry Service' start, and the creation of 8-character .tmp files. These are indicative of a credential dump from the registry. Threat actors can use tools like impacket to query the registry hive remotely, dump the SAM and SYSTEM hives into memory, and exfiltrate to a C2 Server. Verify user login activity and any network connections to internal/external hosts to determine if activity is malicious. • **Platform**: Windows • **Additional reference**: Medium • **Date added**: May 2024
Updated rule for enhanced investigation of system information discovery through service enumeration	• **Rule Name**: “System Information Discovery via Service Enumeration” • **MITRE Techniques**: T1082, T1007 • **Description**: This rule detects registered local system services usage of 'tasklist /svc', or 'net start' by a non-administrator user. Adversaries may obtain information about services using tools as well as OS utility commands. Adversaries may use the commands to get a list of the services on the system. • **Platform**: Windows • **Additional reference**: MITRE • **Date added**: April 2024
Updated rule for advanced detection of the extraction of the domain database (including password hashes) using ntdsutil.exe	• **Rule Name**: “Domain Database including Password Hashes Extracted via ntdsutil.exe” • **MITRE Techniques**: T1003, T1003.003 • **Description**: Adversaries may attempt to access or create a copy of the Active Directory (AD) domain database to steal credential information, as well as obtain other information about domain members such as devices, users, groups, and access rights. By default, the NTDS file is located in %SystemRoot%\NTDS\Ntds.dit of a domain controller. This rule detects the use of the built-in Windows tool, ntdsutil.exe, to extract a copy of the AD domain database (which includes the password hashes for all the users of the domain). Hashes can then be exfiltrated from the host and be used for brute force attacks offline. • **Platform**: Windows • **Additional reference**: MITRE • **Date added**: April 2024
Updated rule for advanced detection of enumeration of browser bookmarks	• **Rule Name**: “Enumeration of Browser Bookmarks" • **MITRE Techniques**: T1217, T1555, T1555.003 • **Description**: This rule detects the enumeration or discovery of web browser bookmark database files. Adversaries may enumerate browser bookmarks to discover more information about a compromised host. Browser bookmarks can show a user's personal information and information about internal network resources. • **Platform**: Linux • **Additional reference**: MITRE • **Date added**: April 2024

Threat or vulnerability	Description
Updated rule for advanced detection of Windows Defender registry key modification	• **Rule Name**: "Windows Defender Registry Key Modifications" • **MITRE Techniques**: T1562, T1562.001, T1112 • **Description**: This rule detects the modification of Windows Defender registry keys, which may be used to disable or modify security tools. • **Platform**: Windows • **Additional reference**: MITRE • **Date added**: April 2024
Updated rule for enhanced investigation of account or group discovery via dscl	• **Rule Name**: "Account or Group Discovery via dscl" • **MITRE Techniques**: T1069.002, T1087, T1087.001, T1087.002 • **Description**: This rule detects evidence of account or group discovery, according to MITRE techniques T1087 and T1069. • **Platform**: macOS • **Additional reference**: MITRE T1087, MITRE T1069 • **Date added**: April 2024
Updated rule for enhanced investigation of file and directory discovery through the Windows command line	• **Rule Name**: "File and Directory Discovery via Cmd" • **MITRE Techniques**: T1083 • **Description**: This rule detects file and directory discovery through the Windows command line (cmd). Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. • **Platform**: Windows • **Additional reference**: MITRE • **Date added**: April 2024
Updated rule for advanced detection of the ScreenConnect authentication bypass vulnerability CVE-2024-1709	• **Rule Name**: "ScreenConnect Authentication Bypass Vulnerability CVE-2024-1709" • **MITRE Techniques**: T1556 • **Description**: This rule detects potential activities associated with the successful exploitation of CVE-2024-1709. • **Platform**: Windows • **Additional reference**: Huntress • **Date added**: April 2024

Previous CylanceMDR protection enhancements

Due to some emerging threats, CylanceMDR has implemented the following CylanceOPTICS rules for improved security and telemetry for analysts. These rules are already in effect and no further action is required from your organization. To see the newest CylanceMDR rules, see CylanceMDR protection enhancements.

Threat or vulnerability	Description
Updated rule for advanced detection of payload creation via compiled HTML (.chm) file	• **Rule Name**: "Payload Creation Via Compiled HTML (CHM) File" • **MITRE Techniques**: T1218, T1218.001 • **Description**: This rule detects the creation of a possible payload like script or executable via compiled HTML files (.chm) loaded by the HTML Help executable program (hh.exe). CHM files are compressed compilations of various content such as HTML documents, images, and scripting/web related programming languages such VBA, JScript, Java, and ActiveX. Adversaries may abuse CHM files to conceal malicious code. Legitimate software may execute CHM files. • **Platform**: Windows • **Additional reference**: Lookout • **Date added**: March 2024 (update)
Updated rule for advanced detection of payload execution from Appdata\Local\Temp Directory	• **Rule Name**: "Payload Execution from Appdata Local Temp Directory" • **MITRE Techniques**: T1059, T1059.003 • **Description**: This rule detects the execution of scripts and executables from the AppData\Local\Temp directory via Windows Command Shell (cmd.exe). It is common for legitimate software to execute from this directory as well. Analysis of the script or executable is necessary to determine if it is being weaponized by a threat actor. • **Platform**: Windows • **Additional reference**: MITRE • **Date added**: March 2024
Updated rule for advanced detection of Windows Defender service shutdown via net.exe	• **Rule Name**: "Windows Defender Service Shutdown via net.exe" • **MITRE Techniques**: T1562, T1562.001, T1489 • **Description**: This rule detects if the Windows Defender service was terminated using net.exe. Adversaries may modify and/or disable security tools to avoid possible detection of their malware tools and activities. This may take many forms, such as killing security software processes or services. • **Platform**: Windows • **Additional reference**: MITRE • **Date added**: March 2024
Updated rule for advanced detection of port forwarding SSH tunnel command execution	• **Rule Name**: "Port Forwarding SSH Tunnel Command Execution" • **MITRE Technique**: T1572, T1021, T1021.004 • **Description**: This rule detects when SSH is executed using the *-N* and *-R* flags. These arguments are used to create port forwarding to a C2 server via an SSH tunnel. Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection or network filtering, and/or enable access to otherwise unreachable systems. The outbound IP address should be analyzed to determine false positives. • **Platform**: Windows • **Additional reference**: Medium • **Date added**: March 2024

Threat or vulnerability	Description
Updated rule for advanced detection of Windows Defender Antivirus Engine restored to default settings	• **Rule Name**: “Windows Defender Antivirus Engine Restored to Default” • **MITRE Technique**: T1562, T1562.001 • **Description**: This rule detects attempts to restore Windows Defender to the original default settings. Adversaries may modify and/or disable security tools to avoid possible detection of their malware tools and activities. Adversaries may also tamper with artifacts deployed and utilized by security tools. • **Platform**: Windows • **Additional reference**: MITRE • **Date added**: March 2024
Updated rule for advanced detection of obfuscated Bash History deletion	• **Rule Name**: “Bash History Deletion” • **MITRE Technique**: T1070, T1070.003 • **Description**: This rule detects the deletion of the bash_history file, which keeps track of the commands that users entered on the command line. An adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion. • **Platform**: macOS • **Additional reference**: MITRE • **Date added**: March 2024
Updated rule for advanced detection of Bash History modification and deletion	• **Rule Name**: “Bash History Modification & Deletion” • **MITRE Technique**: T1552, T1552.003, T1070, T1070.003 • **Description**: This rule detects the modification or deletion of the bash_history file. Bash keeps track of the commands that users entered on the command line with the 'history' utility. Users often enter usernames and passwords on the command line as parameters to programs, which are then saved to this file when they log out. Adversaries can abuse this by looking through the file for potential credentials. • **Platform**: macOS • **Date added**: November 2023
Updated rule for advanced detection of critical Cylance binaries moved	• **Rule Name**: “Critical Cylance Binaries Moved” • **Description**: This rule detects when CyOptics.exe, CylanceSvc.exe, and CyProtect.exe are being moved to a different directory. Adversaries may try to move the Cylance files to bypass Cylance protection and to avoid detection of their malware, tools, and activities. False positives are likely with file backup and synchronization software. • **Platform**: Windows • **Date added**: November 2023

Threat or vulnerability	Description
Updated rule for advanced detection of process execution via compiled HTML (.chm) file	• **Rule Name**: “Process Execution Via Compiled HTML (CHM) File” • **Description**: This rule detects the execution of a process via compiled HTML files (.chm) loaded by the HTML Help executable program (hh.exe). CHM files are compressed compilations of various content such as HTML documents, images, and scripting or web-related programming languages such VBA, JScript, Java, and ActiveX. Adversaries may abuse CHM files to conceal malicious code. Legitimate software may execute CHM files. • **Platform**: Windows • **Additional reference**: Lookout • **Date added**: November 2023
Updated rule for advanced detection of Svchost launching Rundll32 via scheduled task	• **Rule Name**: “Svchost Schedule Task Launches Rundll32” • **MITRE Technique**: T1053.005, T1218.011 • **Description**: This rule detects the execution of rundll32.exe through a scheduled task. Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious rundll32 exploitation. False positives are likely with legitimate software and Windows services. • **Platform**: Windows • **Additional reference**: Medium • **Date added**: November 2023
Updated rule for advanced detection of debugger registry value modification for accessibility features	• **Rule Name**: “Debugger Registry Value Modification for Accessibility Features” • **Description**: This rule detects when a registry value for Windows accessibility features has been modified to launch another program as a debugger. Windows contains accessibility features that may be launched with a key combination before a user has logged in, such as when the user is on the Windows login screen. Adversaries can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system. This can be done by using Image File Execution Options (IFEO) which enables developers to attach a debugger to an application that can be used to intercept calls to the application executable. There is no validation of whether the program listed as a debugger in the registry is legitimately a debugger, so malicious actors can leverage this to execute arbitrary payloads when specific applications (for example, sethc.exe) are executed. • **Platform**: Windows • **Additional reference**: Red Team Notes • **Date added**: November 2023

Threat or vulnerability	Description
Updated rule for advanced detection of obfuscated Base64 decoding method executed via PowerShell	• **Rule Name**: “Obfuscated Base64 Decoding Method Executed via PowerShell” • **MITRE Technique**: T1059.001, T1027.010 • **Description**: This rule detects the execution of an obfuscated 'frombase64string' method in a PowerShell payload. Adversaries can obfuscate this method by reversing the string to evade detection. This technique is most commonly associated with malware generated from the BatCloak engine. False positives are not likely. De-obfuscation of the command line is required to determine the impact. • **Platform**: Windows • **Additional reference**: SANS • **Date added**: November 2023
Updated rule for advanced detection of UAC Bypass via fodhelper.exe activity	• **Rule Name**: "UAC Bypass via Fodhelper.exe" • **MITRE Technique**: T1548.002 • **Description**: This rule detects a privilege escalation technique of bypassing UAC using PowerShell to modify registry keys for fodhelper.exe. Adversaries exploit this bypass to launch malware with administrative privileges. False positives are not likely. • **Platform**: Windows • **Additional reference**: Penetration Testing Lab • **Date added**: November 2023
Updated rule for advanced detection of payload creation via compiled HTML (CHM) file	• **Rule Name**: “Payload Creation Via Compiled HTML (CHM) File ” • **MITRE Technique**: T1218, T1218.001 • **Description**: This rule detects the creation of a possible payload like a script or executable via compiled HTML files (.chm) loaded by the HTML Help executable program (hh.exe). CHM files are compressed compilations of various content such as HTML documents, images, and scripting or web-related programming languages such VBA, JScript, Java, and ActiveX. Adversaries may abuse CHM files to conceal malicious code. Legitimate software may execute CHM files. • **Platform**: Windows • **Additional reference**: Lookout • **Date added**: November 2023

Threat or vulnerability	Description
Advanced detection of AMSI bypass through PowerShell command execution activity	• **Rule Name**: “AMSI Bypass PowerShell Command Execution” • **MITRE Technique**: T1562.001 • **Description**: This rule detects the bypassing of AMSI through PowerShell by setting amsiInitFailed to "true" or by removing the registry key in `HKLM \Software\Microsoft\AMSI`. The Windows Anti-malware Scan Interface (AMSI) is a versatile interface standard that allows your applications and services to integrate with any anti-malware product that's present on a machine. AMSI provides enhanced malware protection for your end-users and their data, applications, and workloads. Adversaries disable AMSI to avoid possible detection of their malware tools and activities. False positives are not likely. • **Platform**: Windows • **Additional references**: GitHub and GitHub • **Date added**: June 2023
Advanced detection of lateral movement through WMI and WinRM activity	• **Rule Name**: “Lateral Movement via WMI/WinRM 2” • **MITRE Techniques**: T1021.006, T1047 • **Description**: This rule detects a Logon Type 3 event and subsequent remote command execution by the user through WMI and WinRM. WMI uses WinRM to enter and control remote systems on a network. Generally, remote WMI and WinRM commands are spawned from WmiPrvSE on the target host. Threat actors can abuse WMI and WinRM to move laterally across the network. System administrators may also use WMI and WinRM for remote management. • **Platform**: Windows • **Additional reference**: Red Canary • **Date added**: June 2023
Advanced detection of Impacket SMBExec module execution activity	• **Rule Name**: “Impacket SMBExec Module Execution” • **MITRE Techniques**: T1569.002, T1021.002 • **Description**: This rule detects Impacket's SMBExec module execution where services.exe launches cmd.exe with command lines similar to "/Q /c echo 127.0.0.1". Impacket is a collection of Python classes for working with network protocols and is commonly weaponized by adversaries. Impacket's SMBExec module allows remote code execution through a semi-interactive shell by creating services that execute commands on the remote host. It is uncommon, but legitimate system admin tools may exhibit the same behavior. • **Platform**: Windows • **Additional reference**: u0041 • **Date added**: June 2023

Threat or vulnerability	Description
Advanced detection of MOVEit Transfer vulnerability (CVE-2023-34362)	• **Rule Name**: "MOVEit Transfer Vulnerability Indicators of Compromise" • **MITRE Techniques**: T1190, T1505 • **Description**: This rule detects w3wp.exe spawning csc.exe and the creation of human2.aspx files in `C:\MOVEitTransfer\wwwroot`. This may indicate exploitation of CVE-2023-34362. Adversaries can exploit this vulnerability to gain unauthenticated access to MOVEit Transfer's database. Adversaries may then be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. False positives may arise if this detection occurs around an initial MOVEit installation or software update. • **Platform**: Windows • **Additional reference**: National Vulnerability Database • **Date added**: June 2023
Advanced detection of Papercut (CVE-2023-27350, CVE-2023-27351)	• **Rule Name**: "Papercut CVE-2023-27350 CVE-2023-27351 Indicators of Compromise" • **MITRE Technique**: T1190 • **Description**: This rule detects the Papercut app spawning lolbas processes. This may indicate a threat actor is exploiting CVE-2023-27350 and/or CVE-2023-27351. False positives are not likely. • **Platform**: Windows • **Additional reference**: MITRE • **Date added**: June 2023
Advanced detection of UAC Bypass via fodhelper.exe activity	• **Rule Name**: "UAC Bypass via Fodhelper.exe" • **MITRE Technique**: T1548.002 • **Description**: This rule detects a privilege escalation technique of bypassing UAC using PowerShell to modify registry keys for fodhelper.exe. Adversaries exploit this bypass to launch malware with administrative privileges. False positives are not likely. • **Platform**: Windows • **Additional reference**: Penetration Testing Lab • **Date added**: June 2023
Advanced detection of credential dumping through comsvcs.dll activity	• **Rule Name**: "Credential dumping via comsvcs.dll" • **MITRE Technique**: T1003.001 • **Description**: This rule detects Local Security Authority Subsystem Service (LSASS) credential dumping through the "MiniDump" exported function of comsvcs.dll. Adversaries may attempt to access credential material stored in the process memory of the LSASS. False positives are not likely. • **Platform**: Windows • **Additional reference**: GitHub • **Date added**: June 2023

Threat or vulnerability	Description
Cyber actors exploiting 3CX desktop app vulnerability (CVE-2023-29059)	• **Rule Name**: “SmoothOperator 3CX Indicators of Compromise” • **MITRE Technique**: T1195.002 • **Description**: This rule detects DNS requests from the 3CX desktop app to domains associated with the "SmoothOperator" supply chain attack. • **Platform**: Windows • **Additional reference**: National Vulnerability Database • **Date added**: April 2023
Cyber actors exploiting Microsoft Outlook Vulnerability (CVE-2023-23397)	• **Rule Name**: “CVE-2023-23397 Indicators of Compromise (Process)” • **MITRE Technique**: T1212 • **Description**: This rule detects process execution behavior that is indicative of CVE-2023-23397. For example, this may indicate an attempt to steal password hashes. • **Platform**: Windows • **Additional reference**: Microsoft Security Response Center • **Date added**: March 2023
Cyber actors exploiting Microsoft Outlook Vulnerability (CVE-2023-23397) (Secondary)	• **Rule Name**: “CVE-2023-23397 Indicators of Compromise (Network)” • **MITRE Technique**: T1212 • **Description**: This rule detects outbound connections on port 445 to non-private (i.e. external) IP addresses. For example, this may indicate an attempt to steal password hashes. • **Platform**: Windows • **Additional reference**: Microsoft Security Response Center • **Date added**: March 2023
Suspicious Microsoft HTML application (Mshta) execution	• **Rule Name**: “Suspicious Mshta.exe Execution” • **MITRE Technique**: T1218.005 • **Description**: This rule detects the use of JavaScript and VBScript command line arguments, as well as remote execution of .hta files. Understanding that `mshta.exe` is a trusted utility that executes Microsoft HTML Applications (HTA), adversaries can use it to proxy execution of malicious .hta files and JavaScript or VBScript. False positives can only be determined after analyzing the command or .hta file for malicious code. • **Platform**: Windows • **Additional reference**: Cyble • **Date added**: February 2023 (update)
Microsoft Office products executing uncommon processes	• **Rule Name**: “Suspicious process execution from Microsoft Office products” • **MITRE Technique**: T1559.002, T1204.002 • **Description**: This rule detects Microsoft Office products executing uncommon processes. Uncommon processes executed from Office products may be indicative of malicious VBA or DDE code inside the offending document. • **Platform**: Windows • **Additional reference**: Cyble • **Date added**: February 2023 (update)

Threat or vulnerability	Description
Execution of suspicious disk image phishing attachment	• **Rule name**: "Suspicious Disk Image Phishing Attachment Executed" • **MITRE Techniques**: T1204.002, T1566.001 • **Description**: This rule detects the mounting of disk image attachments with malicious payloads. This is a common technique for phishing attacks. • **Platform**: Windows • **Additional reference**: GitHub • **Date added**: January 2023
Ransomware activity based on shadow copy and backup deletions	• **Rule name**: "Shadow Copy Removal Command Execution" • **MITRE Technique**: T1490 • **Description**: This rule detects when a shadow or backup catalog removal command is executed through vssadmin.exe, wbadmin.exe, wmic.exe, or PowerShell. Threat actors often delete backups to remove evidence of their presence, or to prevent recovery in ransomware attacks. • **Platform**: Windows • **Additional reference**: MITRE T1490 • **Date added**: January 2023
Lateral movement through WMI or WinRM	• **Rule name**: "Lateral Movement via WMI/WinRM" • **MITRE Techniques**: T1021.006, T1047 • **Description**: This rule detects when a user executes a remote command through WMI or WinRM, which are used to remotely take control of devices on the network. • **Platform**: Windows • **Additional reference**: Red Canary • **Date added**: January 2023
Cyber actors using malicious PowerShell Cmdlets	• **Rule name**: "PowerShell Command Execution with Identified Malicious Cmdlets" • **MITRE Techniques**: T1059.001 • **Description**: This rule detects usage of malicious PowerShell Cmdlets identified via Open-Source Intelligence (OSINT) in base64 encoded commands or plain-text commands. • **Platform**: Windows • **Additional reference**: Red Canary • **Date added**: January 2023

Threat or vulnerability	Description
Cyber actors using Base64 Encoded PowerShell Execution to evade detection (Secondary)	• **Rule Name**: “Base64 Encoded PowerShell Execution” • **MITRE Technique**: T1027 • **Description**: This rule detects the usage of Base64 encoded PowerShell commands and a long Base-64 encoded string using variations of the `-encodedCommand` argument and `Convert.FromBase64String(String)` method. Adversaries may use Base64 to encode malicious commands to evade detection. Benign usage is common with enterprise software and deployment tools • **Platform**:Windows • **Additional reference**: Medium Blog • **Date added**: January 2023 (update)
Cyber actors exploiting Microsoft Exchange (CVE-2021-34473) and Fortinet vulnerabilities (CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591)	• **Rule name**: "Fast Reverse Proxy (FRP) Tool Execution" • **MITRE Techniques**: T1588.001, T1588.002 • **Description**: This rule detects execution of the Fast Reverse Proxy (FRP) tool. FRP is an open-source tool that enables external access to an intranet PC that cannot be accessed directly. Adversaries may use FRP to expose a local server to external access, bypassing the firewall/NAT. • **Platform**: Windows • **Additional reference**: CISA article AA21-321A • **Date added**: December 2022
Jupyter infostealer	• **Rule Name**: "Jupyter Infostealer Indicators of Compromise" • **MITRE Technique**: T1059 • **Description**: This rule detects the execution of PowerShell commands indicative of the Jupyter infostealer. Jupyter is a highly modular malware that hides deep within legitimate installer packages. When executed, it can receive further malicious components via its command-and-control (C2) server to enhance its capabilities. These components can include executables and malicious PowerShell scripts. • **Platform**: Windows • **Additional reference**: BlackBerry Blog • **Date added**: December 2022
Log4Shell VMware Horizon vulnerabilities (CVE-2021-44228 and CVE-2021-45046)	• **Rule Name**: "Log4Shell VMware Horizon Indicator of Compromise " • **MITRE Technique**: T1059 • **Description** : This rule detects the execution of a PowerShell command that exploits a log4j vulnerability in VMware Horizon. • **Platform**: Windows • **Additional reference**: VMware KB article 87073 • **Date added**: December 2022

Threat or vulnerability	Description
Apache Log4J vulnerability (CVE-2021-44228)	• **Rule Name**: “Log4J Indicators of Compromise” • **MITRE Technique**: T1059 • **Description**: This rule detects common Java processes connecting to non-RFC1918 IP addresses on ports associated with Log4J. • **Platforms**: Windows, macOS, and Linux • **Additional reference**: CISA Apache Log4j Vulnerability Guidance • **Date added**: December 2022
Cyber actors using Base64 Encoded PowerShell Execution to evade detection	• **Rule Name**: “Suspicious Certutil.exe Execution” • **MITRE Techniques**: T1027, T1140, T1105 • **Description**: This rule detects the usage of the `-encode` or `-decode` arguments of `certutil.exe`. It also detects file downloads via `certutil.exe`. Adversaries may use certutil to encode and decode malicious Base64 commands to evade detection and/or to download malicious payloads. • **Platform**: Windows • **Additional reference**: GitHub (certutil) • **Date added**: December 2022
Cyber actors using Base64 Encoded PowerShell Execution to evade detection (Secondary)	• **Rule Name**: “Base64 Encoded PowerShell Execution” • **MITRE Technique**: T1027 • **Description**: This rule detects the usage of Base64 encoded PowerShell commands and a long Base-64 encoded string using variations of the `-encodedCommand` argument and `Convert.FromBase64String(String)` method. Adversaries may use Base64 to encode malicious commands to evade detection. Benign usage is common with enterprise software and deployment tools • **Platform**: Windows • **Additional reference**: Medium Blog • **Date added**: December 2022
Cyber actors decoding Base64 command and piping the output to another process to evade detection	• **Rule Name**: “Base64 String Decoded via the \"base64\" Process” • **MITRE Technique**: T1027 • **Description:**: This rule detects the usage of the `-d` or `--decode` arguments of the `base64` binary. Adversaries may decode malicious Base64 commands and pipe the output to another process to evade detection. Benign usage is common with enterprise software and deployment tools. • **Platforms**: macOS and Linux • **Additional reference** GIAC Certification Paper • **Date added**: December 2022

Threat or vulnerability	Description
Microsoft Office products executing uncommon processes	• **Rule Name**: “Suspicious process execution from Microsoft Office products” • **MITRE Technique**: T1105, T1036 • **Description**: This rule detects Microsoft Office products executing uncommon processes. Uncommon processes executed from Office products may be indicative of malicious VBA or DDE code inside the offending document. • **Platform**: Windows • **Additional reference**: Medium Blog • **Date added**: December 2022
Suspicious Microsoft HTML application (Mshta) execution	• **Rule Name**: “Suspicious Mshta.exe Execution” • **MITRE Technique**: T1218.005 • **Description**: This rule detects the use of JavaScript and VBScript command line arguments, as well as remote execution of .hta files. Understanding that `mshta.exe` is a trusted utility that executes Microsoft HTML Applications (HTA), adversaries can use it to proxy execution of malicious .hta files and JavaScript or VBScript. False positives can only be determined after analyzing the command or .hta file for malicious code. • **Platform**: Windows • **Additional reference**: MITRE T1218.005 • **Date added**: December 2022
Suspicious modification of file ownership and file permissions in macOS and Linux	• **Rule Name**: “Chmod modified Setuid and Setgid bits of file” • **MITRE Technique**: T1548 • **Description**: This rule detects the use of `chmod` to modify the `setuid` and `setgid` bits of a file. Chmod manages file and folder permissions\\security. An adversary may abuse chmod to apply `setuid` and `setgid` bits to a file in order to get code running in a privileged user/group context. • **Platforms**: macOS and Linux • **Additional reference**: MITRE T1548 • **Date added**: December 2022
Malware delivered in ISO formats	• **Rule name**: "Disk image phishing attachment downloaded and/or mounted by user T1204.002/T1566.001" • **Description**: This rule detects the creation of disk image files (.iso, .img, .vhd, or .vhdx) in common temporary directories for downloads, and the creation of shortcut files (.lnk) pointing to disk image files. The shortcut files indicate that the user recently mounted the respective disk image file. This is a common technique for phishing attacks. This can be benign on server systems but on workstations, users should rarely mount disk image files. • **Platform**: Windows • **Additional reference**: Github • **Date added**: October 2022

Threat or vulnerability	Description
ProxyNotShell vulnerabilities (CVE-2022-41040 and CVE-2022-41082)	• **Rule name**: "ProxyNotShell Indicators of Compromise. T1190/T1505.003" • **Description**: This rule detects file creation events for files with the following extensions: "dll.dll", "errorEE.aspx", "pxh4HG1v.ashx", "Xml.ashx". Files ending with these extensions may be malicious IIS webshells that indicate a ProxyNotShell exploit. • **Platform**: Windows • **Date added**: October 2022

Legal notice

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada