CrowdStrike Falcon Endpoint Protection Evaluated Against GOTHIC PANDA (APT3)

About this evaluation: *MITRE's Leveraging External Transformational Solutions (LETS) program evaluates the effectiveness of cyber tools being used or considered for use across government. MITRE identifies government users who are evaluating, piloting, or deploying cyber technologies that we believe to be innovative and impactful. Then we provide subject matter expertise to help companies articulate their products' functionality and effectiveness. Full reports are releasable only to the U.S. Government.*

This evaluation is for informational purposes only and is not an endorsement. For more information, please email LETS@mitre.org.

Description

The MITRE LETS team evaluated CrowdStrike Falcon Endpoint Protection Platform to assess the tool's ability to detect an Advanced Persistent Threat (APT). We focused on post-exploit detection of attack techniques employed by GOTHIC PANDA, also known as APT3. No weaponized document or actual exploit was used as part of this effort.

Process

The MITRE team evaluated CrowdStrike Falcon by emulating GOTHIC PANDA, an advanced threat group that employs techniques described in the MITRE ATT&CK™ framework. This group does not typically employ sophisticated scripting techniques, leveraging exploits after initial access, or use anti-endpoint sensing capabilities such as rootkits or bootkits. GOTHIC PANDA emulation provides an initial bounded evaluation for basic Endpoint Detection and Response (EDR) capabilities, thus making it an appropriate choice for these initial MITRE evaluations.

Results

Overall, CrowdStrike Falcon detected the majority of GOTHIC PANDA's post-exploit attack techniques. CrowdStrike uses a collaboration of machine and human, bringing together both proprietary APT detecting software (Falcon Insight) and Managed Threat Hunting Service operators (Falcon OverWatch) to identify malicious activity. Combining both products, along with CrowdStrike Falcon's user interface, assisted in the detection and investigation of GOTHIC PANDA attack techniques emulated by the LETS team.

-Continued-

CrowdStrike Falcon Endpoint Protection Evaluated Against GOTHIC PANDA (APT3)

Results as tested in the MITRE ATT&CK Framework

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Application Shimming	Audio Capture	Automated Exfiltration	Commonly Used Port
AppInit DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Exploitation of Vulnerability	Command-Line Interface	Automated Collection	Data Compressed	Communication Through Removable Media
Application Shimming	AppInit DLLs	Bypass User Account Control	Create Account	File and Directory Discovery	Logon Scripts	Execution through API	Clipboard Data	Data Encrypted	Connection Proxy
Component Object Model Hijacking	Application Shimming	Code Signing	Credential Dumping	Network Service Scanning	Pass the Hash	Execution through Module Load	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
DLL Search Order Hijacking	Bypass User Account Control	Component Firmware	Credentials in Files	Network Share Discovery	Pass the Ticket	Graphical User Interface	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
External Remote Services	DLL Injection	Component Object Model Hijacking	Exploitation of Vulnerability	Peripheral Device Discovery	Remote Desktop Protocol	InstallUtil	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
File System Permissions Weakness	DLL Search Order Hijacking	DLL Injection	Input Capture	Permission Groups Discovery	Remote File Copy	PowerShell	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Hidden Files and Directories	Exploitation of Vulnerability	DLL Search Order Hijacking	Network Sniffing	Process Discovery	Remote Services	Process Hollowing	Email Collection	Exfiltration Over Physical Medium	Fallback Channels
Hypervisor	File System Permissions Weakness	Disabling Security Tools	Private Keys	Query Registry	Replication Through Removable Media	Regsvcs/Regasm	Input Capture	Scheduled Transfer	Multi-Stage Channels
Local Port Monitor	Local Port Monitor	Exploitation of Vulnerability	Two-Factor Authentication Interception	Remote System Discovery	Shared Webroot	Regsvr32	Screen Capture		Multiband Communication
Logon Scripts	New Service	File Deletion		Security Software Discovery	Taint Shared Content	Rundll32	Video Capture		Multilayer Encryption
Modify Existing Service	Path Interception	File System Logical Offsets		System Information Discovery	Third-party Software	Scheduled Task			Remote File Copy
New Service	Scheduled Task	Hidden Files and Directories		System Network Configuration Discovery	Windows Admin Shares	Scripting			Standard Application Layer Protocol
Redundant Access	Service Registry Permissions Weakness	Regsvcs/Regasm		System Network Connections Discovery	Windows Remote Management	Service Execution			Standard Cryptographic Protocol
Registry Run Keys / Start Folder	Valid Accounts	Regsvr32		System Owner/User Discovery		Third-party Software			Standard Non-Application Layer Protocol
Scheduled Task	Web Shell	Rootkit		System Service Discovery		Trusted Developer Utilities			Uncommonly Used Port
Shortcut Modification		Rundll32				Windows Remote Management			
System Firmware		Scripting							
Valid Accounts		Software Packing							
Web Shell		Timestomp							
Windows Management Instrumentation Event Subscription		Trusted Developer Utilities							
Winlogon Helper DLL		Valid Accounts							

CrowdStrike Falcon-to-ATT&CK Mapping – colored cells considered relevant for Gothic Panda/APT3: Gray – not tested; Green – tested, detected; Yellow – tested, detection possible; Red – capability gaps

MITRE