Threat Brief: FireEye Red Team Tool Breach

By Unit 42

Published: 2020-12-11 · Archived: 2026-04-05 14:51:55 UTC

Executive Summary

On Dec. 8, 2020, one of the leading cybersecurity companies in the industry, FireEye, reported a breach and data exfiltration unlike any that we have seen previously. What makes this attack unique is not only the target, FireEye being a well-known cybersecurity company, but that the stolen data contains the internal, custom-crafted red-team and penetration testing tools used by the company to imitate different threat actors during customer security consultations. FireEye's blog provided a wealth of information for defenders to implement security controls and mitigations for defense against the stolen tools. This data is being used by Palo Alto Networks to help ensure our customers are protected if the attackers choose to utilize the tools for malicious purposes.

It is important to note that these custom tools were not released into the wild, they were stolen by a sophisticated threat actor and we likely will not see a sudden widespread use of them. That being said, FireEye went beyond what was required – and what companies have done in the past – in releasing detection techniques. Providing defenders access to the Yara rules, indicators of compromise (IOCs), Snort signatures and other threat data is a class act and very much appreciated by defenders and researchers at Palo Alto Networks – and surely across the industry as a whole.

Protecting Our Customers

Palo Alto Networks has been working diligently to ensure the protections released by FireEye are implemented in a timely manner. The Github repository shared by FireEye contains a list of rules and 16 vulnerability CVE identifiers. The vulnerabilities appear to have been included because sufficient protections against these can help limit the effectiveness of the red-team tools.

Palo Alto Networks has ensured the protections within our products are either already in place or are being prioritized for the provided vulnerabilities and their exploitation. These vulnerabilities range from a wide variety of products, and as always, we highly recommend our customers stay current with their updates and patch all vulnerable software.

The Github repository that provided the protections also contains rules for direct product implementation as well as hunting. Palo Alto Networks is analyzing the efficacy of and applying all stable rules to our respective products. Gap analysis and threat hunting leveraging the FireEye-provided Yara and Snort signatures have enabled Palo Alto Networks researchers to identify potential malware samples that we are now tagging, analyzing, tracking and building protections around within WildFire. Continual verdict efficacy checks of identified malware samples is ongoing within Palo Alto Networks products. Customers leveraging the Palo Alto Networks AutoFocus tool can track initially identified samples and tools under the Fireye_RedTeam_Tools, Rubeus, AndrewSpecial, KeeFarce, SafetyKatz, InveighZero, GadgetToJScript, SeatBelt, RuralBishop, SharpView, and SharpZeroLogon tags. Our

Cortex XDR Managed Threat Hunting Team (MTH) has proactively searched all Cortex XDR Pro customer logs to identify potentially impacted organizations and provide them an assessment of their risk.

Cortex XDR customers are protected using the product's WildFire integration as well as through Local Analysis, the Password theft prevention module, and the behavioral threat protection (BTP) engine. In addition, multiple Behavioural Indicators of Compromise (BIOCs) are available in XDR Server to detect malicious techniques exhibited by the stolen tools.

Threat Prevention provides protection against command and control beacons and exploitation of network vulnerabilities used by the stolen tools. The following table provides an overview of the mapping between Palo Alto Networks Universal Threat IDs (UTIDs) and the provided FireEye SIDs.

Snort Rule	PANW UTID	FireEye SID
Backdoor.HTTP.BEACON.[CSBundle Original Stager]	86215	25879
Backdoor.HTTP.BEACON.[CSBundle MSOffice POST]	86216	25889
Backdoor.HTTP.BEACON.[CSBundle USAToday GET]	86217	25892
Backdoor.HTTP.BEACON.[CSBundle MSOffice Server]	86219	25888
Backdoor.HTTP.BEACON.[CSBundle Original GET]	86220	25877
Backdoor.HTTP.GORAT.[Build ID]	86221	25850
Backdoor.HTTP.BEACON.[CSBundle Original POST]	86222	25878
Backdoor.HTTP.GORAT.[SID1]	86223	25848
Backdoor.HTTP.BEACON.[CSBundle Original Server]	86225	25874
Backdoor.HTTP.BEACON.[CSBundle Original Server 3]	86227	25876

Table 1. PANW UTIDs to FYE Signature Mapping

CVE	PANW UTID
CVE-2019-0708	55815
CVE-2017-11774	56002
CVE-2018-15961	38319
CVE-2019-19781	57570, 57497 and 57625
CVE-2019-3398	55567
CVE-2019-11580	56036

CVE-2018-13379	56365
CVE-2020-0688	57947 and 57766
CVE-2019-11510	56280
CVE-2019-0604	55411, 57462 and 56363
CVE-2020-10189	57801
CVE-2019-8394	59061
CVE-2020-1472	59336
CVE-2018-8581	55152
CVE-2016-0167	392102205
CVE-2014-1812	90128

Table 2: CVE to UTID Mapping

Conclusion

The protections in place for our customers are continually being updated for this breach and for all threats that are identified in the wild. Palo Alto Networks appreciates the information disclosure from FireEye, but we also want to emphasize that at the time this report is published, the tools, hashes of the tools and associated samples have not been disclosed to the public. From the perspective of Palo Alto Networks security researchers, the biggest threat from this breach is the actor and the techniques they were able to utilize in order to infiltrate the FireEye infrastructure. Currently, there has not been any information released on the breach or the threat actor’s tactics, techniques, and procedures (TTPs). Customers should know that Palo Alto Networks researchers are working diligently to ensure protections are in place for our entire product ecosystem.
