Executive Summary

On the 8th December, Cybersecurity firm FireEye released a statement (FireEye, 2020) announcing that a sophisticated state-sponsored attack against them had resulted in the theft of their "red team" tools, a toolset used by their penetration test teams to exploit vulnerabilities in corporations' estates.

The good news: Microsoft's Jeff Jones has praised FireEye for their disclosure and collaboration (TechCrunch, 2020), with the cybersecurity firm releasing helpful information on the hacking tools stolen, along with a repository of useful countermeasures to help combat the use of their tools in the wild (FireEye, FireEye Red Team Tool Countermeasures, 2020).

FireEye have stated that none of the exploits stolen were "zero-day" and provided a list of CVEs for all targeted vulnerabilities. For each of these documented vulnerabilities (a mixture of remote code executions, privilege escalations, and methods to circumvent security controls), we have broken down the various mitigations and remediations to stop FireEye's tools being used on your estate. This advisory contains several actionable steps our team suggests and further recommendations for security mechanisms to help manage/prevent these attacks.

Continue reading:

Products Effected

- Microsoft Exchange, SharePoint, Remote Desktop, and Active Directory servers (numerous versions spanning from Windows 10/Server 2019 all the way back to Vista/Server 2003)
- Microsoft Outlook
- ZoHo ManageEngine Desktop Central and ServiceDesk Plus (numerous versions)
- Both Pulse Secure SSL VPNs and Fortinet FortiGate SSL VPNs
- Citrix Application Delivery Controller (ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway
- Atlassian Confluence and Crowd/Crowd Data Center Servers
- Adobe ColdFusion

Mitigation Steps

- Microsoft has folded patches for these CVEs into their standard update lifecycle, so carrying out regular updates to all Windows Server products will ensure you are protected.
    - Microsoft have also supplied some manual mitigations (such as registry changes and enabling Network Level Authentication) that can be found through the links at the bottom of the page.
- Ensure that endpoints have the latest version/update of Microsoft Outlook installed.
- ZoHo ManageEngine Desktop Central should be updated to version 10.0.479 or later.
- ZoHo ManageEngine ServiceDesk Plus should be updated to build 10012 or later.
- Atlassian Confluence and Crowd/Crowd Data Center need to be updated to the latest versions.
- Adobe ColdFusion 2018, 2016 and 11 need to be updated to the latest available versions.
- FortiOS should be upgraded to versions 5.4.13, 5.6.8, 6.0.5 or 6.2.0 and above.
- Pulse Policy Secure and Pulse Connect Secure should be upgraded to the latest versions if possible, or at a minimum, the corresponding builds for your current versions that contain the fixes listed here.

Security Mechanisms to Help Manage/Prevent These Attacks

User Behavioural Analytics / Credential Access Management:

Several of the FireEye tools utilize Windows credential exploits and manipulate vulnerable mechanisms to either steal credentials or impersonate other users. A privilege access management solution can help control access to and usage of these credentials within an estate, crippling the usefulness of such exploits.

Additionally, user behavioural monitoring can help detect strange usage of credentials so you can respond quickly to these attacks before a threat actor can use the credentials to inflict damage.

Endpoint Detect Protect Respond (EDPR):

Many of the tools targeting Microsoft vulnerabilities involve exploiting mechanisms on the vulnerable servers themselves, using tools and on-endpoint techniques. Endpoint protection tools such as SentinelOne can help detect suspicious indicators and protect from these attacks, even when the vulnerability is new and undocumented.

Network Intrusion Detection Systems (NIDS):

The tools designed to attack servers often utilize specially crafted network connections to exploit vulnerable services within estates.

Network Intrusion Detection Systems can detect indicators of malicious network traffic, potentially even using "Yara rules" provided by FireEye themselves specially for the identification and detection of the network traffic generated by these tools.

Relevant Articles

Vulnerability	Effect Products	Mitigation Documentations
CVE-2019-11510	Numerous Pulse Secure Products (including connect secure and policy secure)	https://nvd.nist.gov/vuln/detail/CVE-2019-11510
CVE-2018-13379	Numerous Fortinet Systems (including versions of FortiOS)	https://nvd.nist.gov/vuln/detail/CVE-2018-13379
CVE-2020-1472	Microsoft Active Directory (numerous versions of windows server)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472
CVE-2018-15961	Adobe Cold Fusion (numerous versions)	https://helpx.adobe.com/security/products/coldfusion/apsb18-33.html
CVE-2019-0604	Microsoft SharePoint (numerous versions of windows server)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604
CVE-2019-0708	Windows Remote Desktop Services	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0708
CVE-2019-11580	Atlassian Crowd/Crowd Data Center	https://jira.atlassian.com/browse/CWD-5388
CVE-2019-19781	Citrix Application Delivery Controller (ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway	https://support.citrix.com/article/CTX267027
CVE-2020-10189	ZoHo ManageEngine Desktop Central	https://www.manageengine.com/products/desktop-central/remote-code-execution-vulnerability.html
CVE-2014-1812	Numerous Versions of Windows including Vista, 7, 8, 8.1, Server 2008, Server 2012	https://support.microsoft.com/en-us/help/2962486/ms14-025-vulnerability-in-group-policy-preferences-could-allow-elevati

Vulnerability	Effect Products	Mitigation Documentations
CVE-2019-3398	Atlassian Confluence (numerous versions)	https://jira.atlassian.com/browse/CONFSERVER-58102
CVE-2020-0688	Microsoft Exchange (numerous versions)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0688
CVE-2016-0167	Numerous Older Versions of Windows (Windows 10 1511 and Older + Windows 8.1 or earlier)	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-039
CVE-2017-11774	Microsoft Outlook (numerous older versions)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-11774
CVE-2018-8581	Microsoft Exchange Server (numerous versions)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-8581
CVE-2019-8394	ZoHo ManageEngine ServiceDesk Plus, build 10012 or older	https://www.exploit-db.com/exploits/46413

Bibliography

FireEye. (2020, December 8). FireEye Red Team Tool Countermeasures. Retrieved from GitHub: https://github.com/fireeye/red_team_tool_countermeasures

FireEye. (2020, December 8). FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community. Retrieved from FireEye Stories: https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

TechCrunch. (2020, December 8). FireEye Says It Was Hacked By A Nation State. Retrieved from TechCrunch: https://techcrunch.com/2020/12/08/cybersecurity-firm-fireeye-says-it-was-hacked-by-a-nation-state