Microsoft Exchange Vulnerabilities – After Action Review and Outlook

MS Exchange Aftermath – Now What?

Over the last week, there has been an influx of updated information regarding the critical ProxyLogon vulnerabilities which have impacted Microsoft Exchange Servers globally. Estimates of vulnerable and impacted servers number in the tens of thousands with new adversaries, tactics, and tools being observed targeting these systems.

In the aftermath of yet another wide-spread hack here are the top 5 concerns and assessments Fidelis Threat intelligence team would like our customers and industry intelligence teams to know and consider as of 10 March 2021.

1. This is no longer a patch/update issue, but an incident response issue
2. This is not isolated to just one adversary group's indicators or behaviors, and attacks started even prior to Microsoft's disclosure
3. Adversaries taking advantage have been seen using older or open-source tactics and tools during post-compromise activity
4. Assessing the breadth and depth of this situation is still on-going
5. Exploit proof of concept code was temporarily publicly available, which may pose a greater risk

Continue reading for more information about this top 5 list and what you should know now.

After Action Review and Outlook

1. The ProxyLogon (name given to the recent set of 0day-vulnerabilities for MS Exchange Server) threat is no longer a patch/update issue but is now an incident response issue.

- Attacks are estimated to have begun since early January with some assessments suggesting attacks may have started as early as December 2020
- This suggests that the exploit and shells used during the later-stages of initial research, discovery and private disclosure to the vendor were somehow obtained (inadvertently leaked, actively/offensively obtained) and abused by adversaries for several weeks before public disclosure and acknowledgement of the 0-days in March 2021

2. Attacks and campaigns are not isolated to only one adversary group, but rather a plethora of different campaigns with varying post-compromise intent and payloads

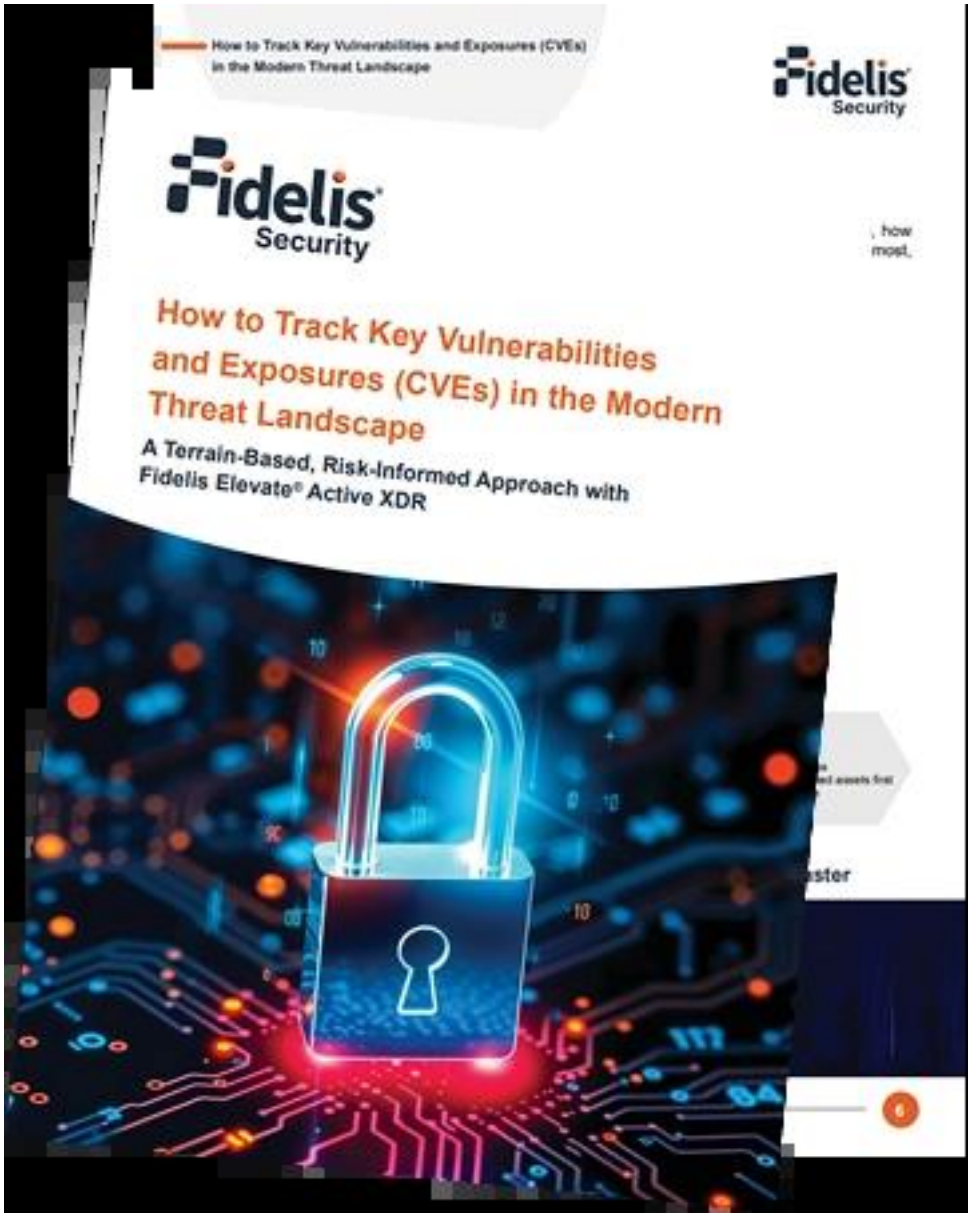
- Post-compromise attacks include varying strains of webshells, credential discovery and dumping techniques, DLP/file exfiltration, crypto-currency miners, and deployment of other malware frameworks like Cobalt Strike

How to Track Key Vulnerabilities and Exposures (CVEs) in the Modern Threat Landscape

- The Evolving Risk of CVEs
- Risk-Based, Terrain-Aware Defense

- From Visibility to Risk: Prioritizing CVEs

[Download the Whitepaper Now!]



3. Some adversaries named in ongoing attempts against ProxyLogon exploitation have been observed reusing older or open-sourced tactics or tools

- Mimikatz, PowerCat, AntSword, and ChinaChopper, observed used by the Hafnium threat group and others, have been open-source projects on GitHub for many years
- Both AntSword and ChinaChopper webshells were observed to be used in previous campaigns targeting critical-level vulnerabilities in MS Exchange (CVE-2019-0604)
- Indicators for AntSword, specifically the user-agent, show that default settings were used. This suggests that other than exploiting 0days, many post-compromise tactics were not necessarily novel or requiring bespoke tactics

4. Although response and clean-up take precedence over attribution of named adversary groups at this time, the breadth and depth of access and compromise requires review of possible adversary courses of actions based off past activity

- Fidelis TRT Intel has previously assessed a shift in state-sponsored/executed campaigns using destructive (e.g.: ransomware, wiper) malware as a Most Dangerous Course of Action (MDCOA).
- LuckyMouse (aka: APT27, Emissary Panda), identified by ESET as exploiting ProxyLogon since February 2021, has been reported to deploy ransomware in financial driven campaigns in late-2020, as opposed to expected espionage
- Webshells provide persistence and access; access-brokerage constitutes a significant portion of the cyber-criminal economy; although the practice of access swapping/sale is not confirmed between state-sponsored group, several state-affiliated/sponsored groups that have been named may have a significant amount of access into enterprise environments that could be leveraged for further attacks, such as ransomware, or contracted out to proxy actors.

5. In-depth technical reports and exploit proof of concept (POC), which was released to GitHub and subsequently removed by Microsoft, may exasperate the risk against MS Exchange Servers

Despite the available POC, detections and prevention will require an in-depth approach.

1. Endpoint – new file creation such as *.aspx files and credential harvesting behaviors leveraging or targeting procdump, lsass, and NTDS files.
2. Network – DLP rules, IIS log monitoring, suspected inbound traffic related to webshell activity (e.g.: PHP Post traffic, suspicious or default user-agents for webshells)

Conclusion and Analyst Comments

While not every single environment or organization is confirmed to be impacted or targeted, Fidelis TRT assesses that that attempted exploitation or interrogation of your environments for these vulnerabilities should be considered as a Most Likely Course of Action (MLCOA) due to the length of time the threats have been present as well as recent public release of the exploit’s POC.

It is important to consider that exploitation of the 0-day ProxyLogon vulnerabilities does not necessarily constitute a full compromise. There are several steps and processes that were involved beyond the initial compromise of vulnerable Microsoft Exchange Servers in order to achieve varying levels of access, persistence, discovery and execution or exfiltration.

Previous major breaches have also proved that failures at multiple levels of defense and detection, not just the initial compromise or vulnerability exploitation, resulted in major impact of confidentiality, integrity, and/or availability. A defense in depth and risk-focused approach is an important consideration to ensure known and future threats are mitigated where possible.