


ProxyShell Exchange Exploitation Now Leads To An Increasing Amount Of Cobaltstrike Backdoors

 blog.morphisec.com/proxyshell-exchange-exploitation-now-leads-to-an-increasing-amount-of-cobaltstrike-backdoors



Breach Prevention Blog

Cybersecurity news, threat research, and more from the leader in making breach prevention easy

Posted by [Morphisec Labs](#) on August 27, 2021

- [Tweet](#)
-



On approximately August 21, 2021, security researchers, cybersecurity leaders, and eventually the CISA, began voicing concerns about the inevitable threat of LockFile ransomware attacks on a wide variety of ill-informed and unprepared victims. Threat actors had been caught targeting on-premises Microsoft Exchange servers via [ProxyShell vulnerabilities](#). These vulnerabilities have been dubbed, “[worse than ProxyLogon](#)”. Patches for these vulnerabilities were made available in April & May, but many servers were still vulnerable.

That same day, [Morphisec Guard](#), our Zero Trust, Endpoint Protection Platform, successfully detected and prevented the execution of Cobaltstrike beacons, which were delivered via a ProxyShell exploit. Therefore, Morphisec actively protected the exchange servers of our customers.

Below is an example of one of the prevention events:

 Cobaltstrike beacons delivered via ProxyShell exploit

Cmd execution:

 cmd execution

Cobalt C2:

hxxp://at.miyazono[.]tk

Conclusion

Morphisec demonstrates the vital nature of a strong prevention strategy for servers. It is our hope that more enterprises will move away from faulty detection-centered strategies and move toward preventative, proactive solutions.

GET IN TOUCH TO IMPROVE YOUR VULNERABILITY MANAGEMENT

Subscribe to our blog

Stay in the loop with industry insight, cyber security trends, and cyber attack information and company updates.



Search Our Site

Recent Posts

[Contact Sales/Inquire via Azure](#)