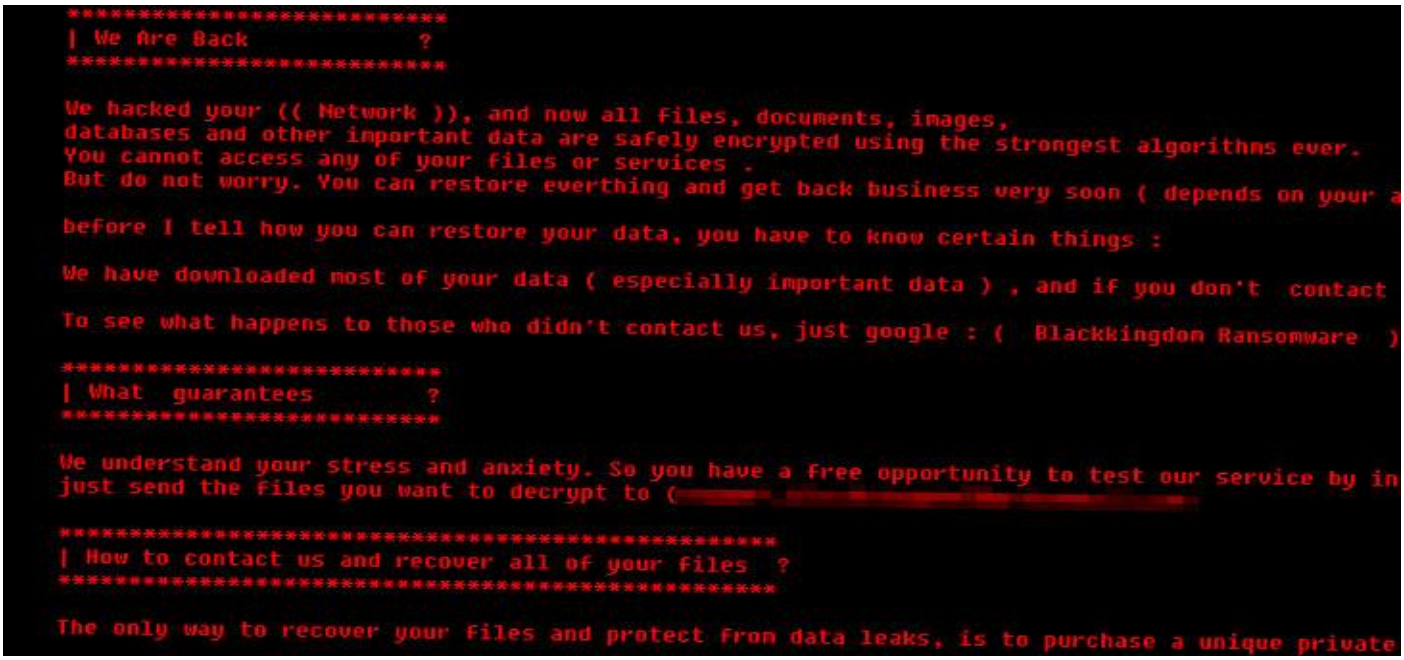
Black Kingdom Ransomware Hunting Unpatched Microsoft Exchange Servers



More than a week after Microsoft released a one-click mitigation tool to mitigate cyberattacks targeting on-premises Exchange servers, the company disclosed that patches have been applied to 92% of all internet-facing servers affected by the ProxyLogon vulnerabilities.

The development, a 43% improvement from the previous week, caps off a whirlwind of espionage and malware campaigns that hit thousands of companies worldwide, with as many as 10 advanced persistent threat (APT) groups opportunistically moving quickly to exploit the bugs.

According to telemetry data from RiskIQ, there are roughly 29,966 instances of Microsoft Exchange servers still exposed to attacks, down from 92,072 on March 10.

While Exchange servers were under assault by multiple Chinese-linked state-sponsored hacking groups prior to Microsoft's patch on March 2, the release of public proof-of-concept exploits fanned a feeding frenzy of infections, opening the door for escalating attacks like ransomware and hijacking web shells planted on unpatched Microsoft Exchange servers to deliver cryptominers and other malware.

"To make matters worse, proof-of-concept automated attack scripts are being made publicly available, making it possible for even unskilled attackers to quickly gain remote control of a vulnerable Microsoft Exchange Server," cybersecurity firm F-Secure noted in a write-up last week.

In the weeks since Microsoft first released its patches, at least two different strains of ransomware have been discovered as leveraging the flaws to install "DearCry" and "Black Kingdom."

Cybersecurity firm Sophos' analysis of Black Kingdom paints the ransomware as "somewhat rudimentary and amateurish in its composition," with the attackers abusing the ProxyLogon flaw to deploy a web shell, utilizing it to issue a PowerShell command that downloads the ransomware payload, which encrypts the files and demands a bitcoin ransom in exchange for the private key.

"The Black Kingdom ransomware targeting unpatched Exchange servers has all the hallmarks of being created by a motivated script-kiddie," Mark Loman, director of engineering at Sophos, said. "The encryption tools and techniques are imperfect but the ransom of $10,000 in bitcoin is low enough to be successful. Every threat should be taken seriously, even seemingly low-quality ones."

The volume of attacks even before the public disclosure of ProxyLogon has prompted experts to investigate if the exploit was shared or sold on the Dark Web, or a Microsoft partner, with whom the company shared information about the vulnerabilities through its Microsoft Active Protections Program (MAPP), either accidentally or purposefully leaked it to other groups.

Exchange On-premises Mitigation Tool (EOMT)

This is the most effective way to help quickly protect and mitigate your Exchange Servers prior to patching. We recommend this script over the previous ExchangeMitigations.ps1 script. The Exchange On-premises Mitigation Tool automatically downloads any dependencies and runs the Microsoft Safety Scanner. This a better approach for Exchange deployments with Internet access and for those who want an attempt at automated remediation. We have not observed any impact to Exchange Server functionality via these mitigation methods. EOMT.ps1 is completely automated and uses familiar mitigation methods previously documented. This script has three operations it performs:

- Mitigate against current known attacks using CVE-2021-26855 via a URL Rewrite configuration
- Scan the Exchange Server using the Microsoft Safety Scanner
- Attempt to remediate compromises detected by the Microsoft Safety Scanner.

This a better approach for Exchange deployments with Internet access and for those who want an attempt at automated remediation. We have not observed any impact to Exchange Server functionality via these mitigation methods nor do these mitigation methods make any direct changes that disable features of Exchange.

Requirements to run the Exchange On-premises Mitigation Tool

- External Internet Connection from your Exchange server (required to download the Microsoft Safety Scanner and the IIS URL Rewrite Module).
- PowerShell script must be run as Administrator.

System Requirements

- PowerShell 3 or later
- IIS 7.5 and later
- Exchange 2013, 2016, or 2019
- Windows Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019

References:

- https://thehackernews.com/2021/03/black-kingdom-ransomware-hunting.html
- https://blog.f-secure.com/microsoft-exchange-proxylogon/
- https://thehackernews.com/2021/03/use-this-one-click-mitigation-tool-from.html
- https://github.com/microsoft/CSS-Exchange/tree/main/Security#exchange-on-premises-mitigation-tool-eomt
- https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download