BLANKROME

Cybersecurity & Data Privacy

JUNE 8, 2020 • NO. 10

Enhanced Threat of Human-Operated Ransomware Tied to COVID-19

To "bend the curve" and slow the spread of the coronavirus, most businesses across the country have transitioned to remote working arrangements. Recently, Microsoft issued its first-ever targeted ransomware alert regarding the significantly enhanced threat of human-operated ransomware campaigns, which have increased precipitously as cyber criminals seek to exploit the range of security vulnerabilities that exist with remote working. Companies should review this guidance carefully and, where feasible, implement the risk mitigation strategies offered by Microsoft to protect from these attacks that can prevent access to critical systems, cause downtime, and steal sensitive information.

The Noteworthy Threat Posed by Human-Operated Ransomware

The COVID-19 pandemic, and the switch to remote working in particular, has brought about a range of cyber vulnerabilities that ordinarily do not exist with traditional office work environments. Cyber criminals have taken note and responded by upping the frequency of their human-operated ransomware campaigns to take advantage of this opportunity to penetrate organizational networks and deliver their attacks.

Human-operated ransomware attacks are a cut above run-of-the-mill commodity ransomware campaigns. They employ human-operated attack methods to target organizations that are most vulnerable to disruption—those that have not had time or resources to double-check their security hygiene like installing the latest patches, updating firewalls, and checking the health and privilege levels of users and endpoints—therefore increasing the probability of payoff. In addition, current attacks tied to COVID-19 are also employing sophisticated social engineering tactics tailored to prey on people's fears about the pandemic and their urgent need for health-related information, further increasing the likelihood that these attacks will prove successful.

Consequently, businesses need to take proactive measures to protect themselves from this sizeable threat.

Measures to Mitigate Ransomware Threats That Exploit Gateways and VPN Vulnerabilities

Since the COVID-19 pandemic began, ransomware operators have focused primarily on targeting network devices like gateway and virtual private network ("VPN") appliances to gain a foothold in the systems and networks of target organizations. In doing so, attackers are actively scanning the Internet for vulnerable systems, using the updater features

of VPN clients to deploy malware payloads, and tailoring exploits to take advantage of remote workers.

Microsoft provides a number of action steps that can be implemented to guard against this threat of ransomware attacks that exploit gateways and VPN vulnerabilities, including the following:

- apply all available security updates for VPN and firewall configurations;
- monitor and pay special attention to your remote access infrastructure and immediately investigate any detections from security products or anomalies found in event logs; in the event of a compromise, ensure that any account used on impacted devices has a password reset, as the credentials may have been exfiltrated;
- turn on attack surface reduction rules, including rules that block credential theft and ransomware activity; and
- to address malicious activity initiated through weaponized Microsoft Office documents, use rules that block advanced macro activity, executable content, process creation, and process injection initiated by Office applications.

Measures to Strengthen Networks Against All Types of Cyber-Attacks

In addition, to further mitigate risk of cyber-attacks generally, Microsoft recommends that businesses consider implementing the following additional measures:

- harden Internet-facing assets and ensure they have the latest security updates;
- use threat and vulnerability management to audit these assets regularly for vulnerabilities, misconfigurations, and suspicious activity;
- secure remote desktop connections/gateways using solutions like multi-factor authentication ("MFA") or network-level authentication ("NLA");
- practice the principle of least privilege and maintain credential hygiene;
- enforce strong randomized, just-in-time local administrator passwords;
- monitor for brute-force attempts and check excessive failed authentication attempts;
- monitor for clearing of event logs; and
- utilize firewalls to prevent communication among endpoints whenever possible to limit lateral movement and other attack activities.

Conclusion

Human-operated ransomware campaigns pose a significant and growing threat to businesses, and represent one of the most impactful trends in cyber-attacks today. Combating and preventing attacks of this nature requires a shift in mindset—one that focuses on comprehensive protection required to slow and stop hackers before they can succeed. Cyber criminals will continue to take advantage of security weaknesses to deploy destructive human-operated attacks—especially during the ongoing COVID-19 pandemic, which has made it much easier for hackers to penetrate organizational networks as employees continue to work remotely. Consequently, now more than ever businesses must consistently and aggressively apply security best practices to their networks to manage and defend against this burgeoning threat.

As part of its COVID-19 Task Force, Blank Rome's Cybersecurity & Data Privacy team can assist in providing key counseling and guidance with respect to any issues or concerns relating to the risk of ransomware attacks, as well the necessary policies, procedures, and protocols that are needed to fully mitigate this significant security threat. And if your organization suffers any type of security incident during the COVID-19 pandemic, Blank Rome's data breach incident response team is available 24/7 and can provide immediate assistance with rapid response and crisis management following any type of breach or security event.

For additional information, please contact:

David J. Oberly, Cincinnati Office
Associate, Cybersecurity & Data Privacy, Privacy Class Action Defense
513.362.8711 | doberly@blankrome.com