CYBERFORCE|Q

November 15, 2023

OCTOBER 2023 MONTHLY BULLETIN

CyberForce|Q continues to work diligently to detect the latest threats of the cyber landscape. Our monthly bulletin covers the most prominent security incidents of the past month and provides insights into emerging trends and tactics used by threat actors, so you can stay informed.

Key Takeaways

Takeaway 1

When implementing geo-blocking measures, thorough risk assessments and regular monitoring should be conducted.

Takeaway 2

Microsoft identified unsecured remote desktop protocol (RDP) and virtual private networks (VPN) as the primary tools leveraged by adversaries in breaching external remote services.

Takeaway 3

Human-operated ransomware attacks have seen a significant increase of over 200% since September 2022.

Case Study

Attack Surface Management: Geo-Blocking

In one client environment, we noticed a significant increase in network traffic from specific countries outside of the United States over the past month. When trends emerge that go beyond blocking known malicious network infrastructure as indicators of compro+ mise (IOCs), teams should conduct further analysis and explore more suitable measures to safeguard the network. One measure is to consider geo-blocking.

Geo-blocking is the practice of restricting access to or from external resources based on their country of origin. This is typically done by enforcing firewall policies that deny connection attempts to or from specific countries. In certain cases, organizations may require employees to travel outside of their usual areas of operation to fulfill business needs. As a result, organizations must carefully consider the potential impact of geo-blocking on legitimate business activities. It is important to strike a balance between network security and operational requirements. When implementing geo-blocking measures, thorough risk assessments and regular monitoring should be conducted to ensure that the desired security outcomes are achieved without unnecessarily hindering business operations.

When geo-blocking is effective, organizations experience benefits such as a decreased risk of malicious network traffic. This is accom+ plished by analyzing geographical trends using both internal and external threat intelligence sources. Such analysis helps improve network performance, alleviate congestion, and cut costs, while enhancing operational efficiency. These advantages are particularly evident when the country or countries in question generate a significant volume of network traffic. Additionally, this reduces the time and resource allocation by security teams to monitor and investigate reoccurring incidents, allowing them to focus on other security priorities. However, it is important to note that geo-blocking is not a foolproof solution and should be considered as one part of a comprehensive network security strategy.

External Trend

Microsoft: Human-operated ransomware attacks tripled over past year

Human-operated ransomware attacks have seen a significant increase of over 200% since September 2022, according to a report by Microsoft. The rise in these attacks suggests a shift in the cybercrime landscape, with individual ransomware hackers seeking to maximize their profits by collaborating with various criminal groups. Unlike automated attacks delivered through phishing documents, human-operated attacks involve the active abuse of remote monitor+ ing and management (RMM) tools, allowing hackers to leave behind less evidence. These attacks often target unmanaged devices, com+ monly used under "bring your own device" policies, as they typically have fewer security controls and defenses.

The report, spanning from July 1, 2022, to June 30, 2023, revealed that human-operated attacks accounted for 40% of all ransomware incidents by the end of that period. Microsoft predicts that the number of human-operated attacks will continue to grow in 2024. In response, hackers are evolving their tactics to circumvent defensive measures implemented by Microsoft and other companies.

Despite the alarming increase in attacks, the report observed that most ransomware attempts failed to encrypt any data, with only 2% of attacks progressing to successful ransomware deployment. The majority of attacks could be traced back to three points of compro+ mise: breaching external remote services, abusing valid accounts, and compromising public-facing applications.

Microsoft identified unsecured remote desktop protocol (RDP) and virtual private networks (VPN) as the primary tools leveraged by adversaries in breaching external remote services. Furthermore, attackers who gained legitimate account credentials were most commonly able to log in via Citrix.

Steps To Mitigate

Configure firewalls and proxies to limit outgoing traffic to remote access tool sites.

To detect unapproved RMM tools, analyze installed applications and observed executables for outliers.

Monitor host firewall rules for unexpected changes indicating unauthorized application installations.

How CyberForce|Q Can Help

For over 27 years, CyberForce|Q has been a trusted name in advancing cybersecurity programs. Our expertise lies in designing and executing measurable cybersecurity strategies tailored to organizations of all sizes. With a track record of proven results, we offer services such as customized security assess-ments, robust security operations centers, and comprehensive strategic guidance. Let us assist your organization in prioritizing its goals, elevating your cybersecurity capabilities, and providing meaningful measurements of progress. Our participants are innovative leaders who share optimal strategies to implement and advance a proven cybersecurity program. CyberForce|Q together, we protect the cyber realm.

Contact Us For More Information

248-837-1400 • solutions@cyberforceq.com

CYBERFORCE|Q