CYBERFORCE | Q

September 14, 2023

AUGUST 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

Organizations should focus on staying up to date and addressing modern TTPs, rather than solely relying on IOCs.

Takeaway 2

Google is bringing its Safety Check feature to browser extensions, warning users when an extension has been detected as malware.

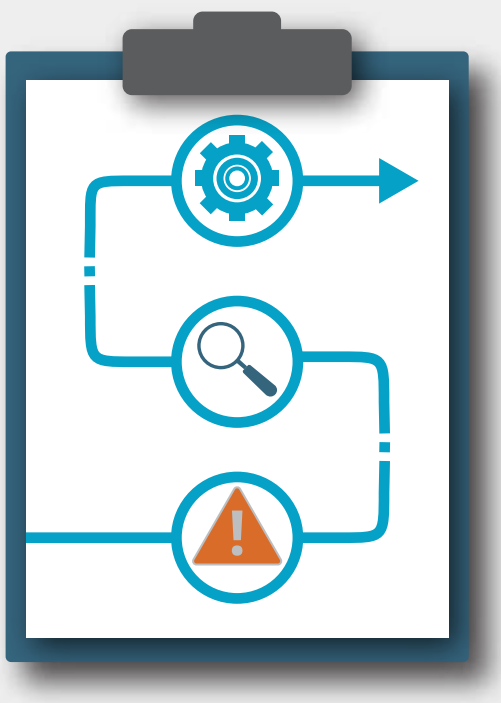
Takeaway 3

Strategically placing EDR sensors across a network ensures the SIEM solution can collect all the required data.

Case Study

Understanding the Limitations of IOCs: The Importance of Focusing on TTPs

In cyber threat intelligence, indicators of compromise (IOCs) refer to observable artifacts or traces of known malicious activity, used to indicate an intrusion or threat to a system or network. Generally, these include IP addresses, domain names, hashes of malware files, and patterns in network traffic, among others. Analyzing and tracking IOCs is an important part of detecting and responding to cyber-attacks. However, organizational focus on IOCs as part of a threat intelligence program can sometimes lead to a "whack-a-mole" approach: simply reacting to each new indicator as it appears, rather than proactively identifying and addressing tactics, techniques, and procedures (TTPs) used by threat actors.



While IOCs generally originate from external network environments, modern adversary network intrusions increasingly rely on existing technologies and utilities native to the organization's internal network environment to achieve their goals. The term TTPs is often used to refer to working within these environmental limitations. In many cases, the malicious use of these features by a threat actor is technically considered a legitimate use for them.

For instance, if a threat actor creates a remote scheduled task on an internal endpoint to periodically execute a malicious script, this scheduled task may not appear as an IOC, but rather as a legitimate task. Therefore, organizations should also focus on the abuse of legitimate operating system features, rather than solely relying on IOCs. This proactive and effective approach to threat intelligence allows for a strategy that goes beyond reacting to each new indicator as it appears. By doing so, the risk of an intrusion can be decreased, or at the very least, the time malicious activity occurs within the network can be greatly limited.

Steps To Mitigate

- Have comprehensive visibility into the organization's assets and have visibility across these assets.
- Have endpoint detection and response (EDR) sensors placed at key points across the network and ensure a SIEM solution can collect the required data.
- Increase true positive detection accuracy of threat actor behavior through robust detection analytics.
- Stay up to date on modern adversary TTPs relevant to your business area and tailor detection engineering needs to meet strategic and operational priorities.

External Trend

Google Chrome to warn when installed extensions are malware

Google is testing a feature in Chrome that will alert users if an installed extension has been removed from the Chrome Web Store, which could indicate that it is malware. The Chrome Web Store is flooded with unwanted browser extensions, created by scammers and threat actors who use them to inject ads, track search history, redirect users to affiliate pages, or steal personal information. Developers regularly create these extensions, with new ones being released as Google removes old ones from the store. Unfortunately, if a user has already installed one of these extensions, it will remain in their browser even after Google detects it as malware and removes it from the store.

To address this issue, Google is bringing its Safety Check feature to browser extensions, warning users when an extension has been detected as malware or removed from the store and prompting the user to uninstall it. The feature will be available in Chrome 117 but can be tested in Chrome 116 by enabling the browser's 'Extensions Module in Safety Check' feature.

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 assessments, 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 with our participants protecting the cyber realm.

Contact Us For More Information

248-837-1400 • solutions@cyberforceq.com

CYBERFORCE | Q