TLP: Clear - Unlimited disclosure, this information can be shared publicly with everyone.

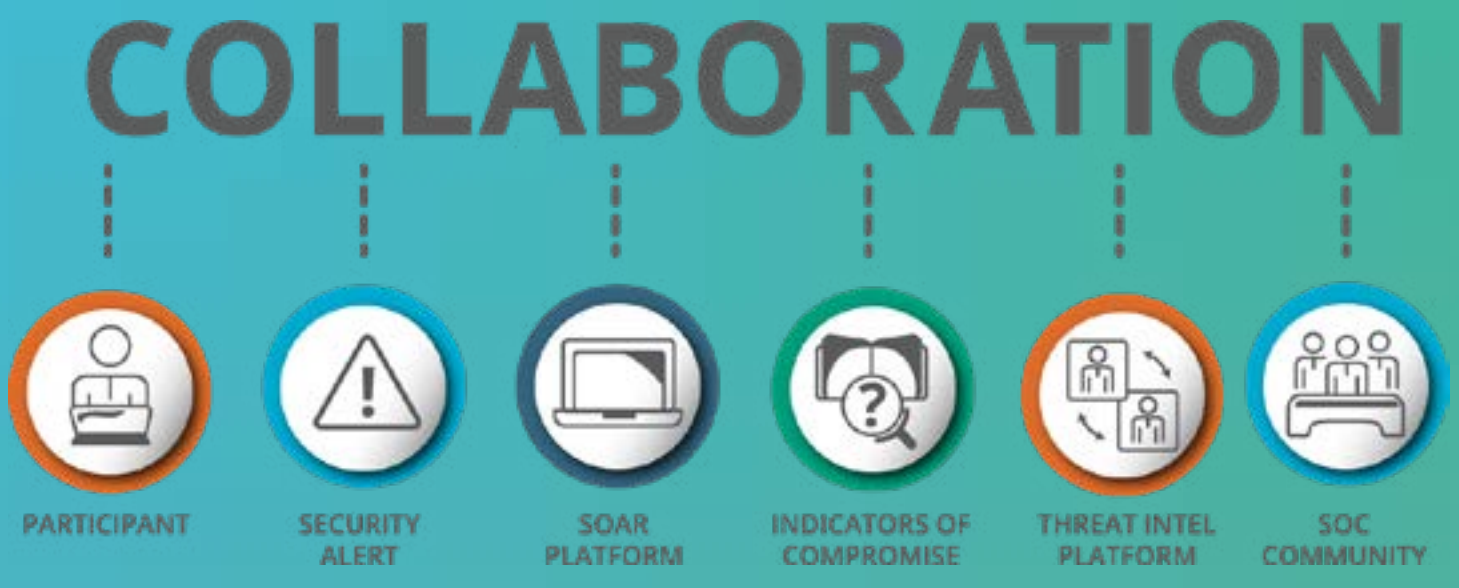
MARCH 2023 MONTHLY BULLETIN

CyberForce|Q continues to work diligently to detect the latest threats of the cyber landscape. Cyber criminals work around the clock to steal your personal information. At CyberForce|Q we work to stay ahead of the cyber criminals. 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.

01 Executive Summary

Our collaborative and information sharing efforts have grown stronger, despite the threat landscape remaining consistent. This is beneficial for our organizations as it allows them to access a wider range of expertise and resources, which can enhance their ability to detect and respond to potential cyber incidents, thereby improving their overall security posture.

By staying informed, organizations can stay ahead of the threats and keep their sensitive information and systems secure. In these monthly bulletins, we cover the most prominent security incidents of the past month and provide insights into emerging trends and tactics used by threat actors.



02 Case Study

Suspicious Process Behavior and the Importance of Thorough Threat Detection Coverage

As enterprise security solutions become better at detecting and blocking malicious files, sophisticated threat actors are increasingly using Windows operating system-native utilities for malicious purposes. These utilities, known as LOLBins (Living-off-the-Land Binaries), have trusted functionality within an organization's environment, making them attractive to threat actors. Even if one is being used maliciously to install malware, exfiltrate sensitive data, or for other objectives, the interaction may often bypass detection because of insufficient detection coverage. To help mitigate this risk, organizations are encouraged to include up-to-date and prioritized detection rules, proactive security assessments and iterative threat hunting in their asset management strategy.

In addition to detecting suspicious file behavior in client environments, we also prioritize identifying suspicious process behavior. This is crucial for providing broader coverage and visibility around an organization's assets, as it helps to identify suspicious activity and highlight unidentified blight spots. As mentioned earlier, assuming that confidential data loss or other consequences of a network compromise are most likely due to a user unintentionally downloading malware onto their device carries a significant risk. Threat actors can gain initial access to a system through various means, such as (but not limited to) a phishing email that harvests user credentials, by exploiting a security vulnerability in an asset, or by leveraging external-facing remote services.

This emphasizes the significance of understanding what an organization is protecting, having visibility into those assets, being able to detect unauthorized activity and triage accurately, and being aware of potential threat actors, as well as their capabilities.

03 External Trend Spotlight

DNS Data Shows One in 10 Organizations Have Malware Traffic on their Networks, Akamai Report

DNS, also known as the Domain Name System, is a crucial aspect of network communication, often referred to as the phonebook of the Internet. It is used by most network software, including malware, to look up domain names and find their corresponding IP addresses before establishing connections over protocols like HTTP(S) and SMTP. DNS is also available in almost all enterprise environments, even those with strict network security policies that restrict HTTP(S) traffic. As a result, DNS can be used by threat actors to tunnel communications for malicious purposes, such as command and control (C2), data infiltration, and data exfiltration. This type of malicious activity is commonly referred to as DNS Tunneling.

Last year, DNS service provider Akamai discovered that 10-16% of organizations had DNS traffic going to command-and-control (C2) servers associated with botnets and malware. More than 25% of that traffic was going to initial access brokers who sell access to other cyber-criminals. Akamai's DNS infrastructure observed up to seven trillion requests per day and identified requests to malicious domains. Of the devices making DNS requests to Akamai, 9-13% attempted to visit malware-serving domains, while 4-6% tried to access known phishing sites.

The percentage of devices attempting to access C2 domains is smaller, but still significant given the number of devices generating 7 trillion DNS requests per day. A request for a C2 domain strongly suggests an active malware infection, though a request for a malware-hosting domain does not guarantee a successful compromise.

Steps to Mitigate Risk

- Monitor and review hosts that have a high volume of uncommon resource record types, such as TXT, NULL, and CNAME.
- Monitor and look for uncommon top-level domains (TLDs) such as .xyz, .me, and .biz, as well as TLDs for geographical regions where your organization does not regularly operate.
- Filter DNS application logs to list response codes with NXDOMAIN (domain does not exist) to monitor for and look for hosts with a high volume of DNS resolution failures.

Contact Us for More Info: 248-837-1400 solutions@cyberforceq.com