Lodestone

APRIL 2022

STATE OF CYBER

monthly newsletter

Most Targeted Industries

- Consumer and industrial products
- Manufacturing
- Real estate

Most Active Threat Actors

- LockBit 2.0 (Ransomware)
- Conti (Ransomware)
- ALPHV/BlackCat (Ransomware)
- Lapsus$ (Data Extortion)

Most Targeted Vulnerabilities

- CVE-2022-23812
- CVE-2022-0847
- CVE-2020-5722
- CVE-2022-23131
- CVE-2021-22893
- CVE-2022-20707

HINDSIGHT IS 20/20

Log management is a critical component of any organization's security posture and should be evaluated regularly as its environment changes.

Maximizing logging capabilities provides critical visibility into the events occurring in your company's environment. System and security logs can often be configured to log capture activity and detail levels. Increased visibility can also translate into more effective detection rules. While breach prevention can never be guaranteed, we can focus on minimizing Mean Times to Detection (MTTDs) and Mean Times to Respond (MTTRs) to reduce the impact of threat actors on daily operations.

Logging also facilitates incident response and threat hunting operations. Access to more historical logs enables incident response analysts like Lodestone's to reconstruct a threat actor's activities more accurately. Analytic tools can leverage this information to identify anomalous behavior for threat hunters to further investigate. Both could uncover previously unknown or undiscovered tactics, techniques, and procedures (TTPs).

In addition to the number of logs collected and the level of detail they contain, we recommend that companies also consider how long logs should be retained. It is not uncommon for threat actors to spend time carefully working within a network before taking actions that may tip off security teams to their presence. If a threat actor has been inside a network for 90 days and there are only logs for 30 days, your company could be missing out on critical information regarding threat actor TTPs and objectives. However, storage capacity limitations require some logs to be prioritized over others. Experts like Lodestone can assist with identifying which can provide the most value to your organization.

DEV-0537 CRIMINAL ACTOR TARGETING ORGANIZATIONS FOR DATA EXFILTRATION AND DESTRUCTION

Lapsus$ puts companies on notice by offering to pay insider threats for access. Microsoft, a Lapsus$ victim, provides an analysis of the group and some defense recommendations.

CISA COMPILES LIST OF FREE CYBERSECURITY TOOLS AND SERVICES

Budget constraints shouldn't prevent organizations from increasing their security capabilities, many free tools and services are available to help defend against cyber attacks.

ATTACKS ABUSING PROGRAMMING APIS INCREASED BY OVER 600% IN 2021

Organizations lacking a robust security strategy for the lifecycle of their APIs may be at increased risk of attack.

MORE ORGANIZATIONS SUFFERED SUCCESSFUL PHISHING ATTACKS IN 2021 THAN IN 2020

A surge in successful attacks stresses the importance of employees maintaining a high level of awareness regarding phishing emails.

NEW FLAWS DISCOVERED IN CISCO'S NETWORK OPERATING SYSTEM FOR SWITCHES

A vulnerability affecting Cisco Nexus switches could allow an authenticated remote attacker to execute commands with root privileges. Organizations with vulnerable devices should ensure they have applied the latest updates released by Cisco.

Contact Us: 320 East Main St, Lewisville, TX 75057. Tel: 1-203-307-4984. www.lodestone.com