CYBERFORCE | Q

October 18, 2023

SEPTEMBER 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

Identity coverage is valuable because it provides a holistic view of user activity, which can be used to detect potential threats.

Takeaway 2

Gaining access to an organization's network through a valid user account is likely to generate the least amount of system noise.

Takeaway 3

Black Cat/AlphV ransomware can lead to a breach in personal data that could end up being listed on the dark web.

Case Study

Detection in Depth and the Importance of Identity Protection

Threat identification of any kind is fundamental to safeguarding sensitive information and protecting systems from a successful compromise. More specifically, though, is the importance of identifying potentially malicious activity as early as possible. The steps in an attack chain may vary widely. However, in general, the most successful first step is achieved through compromised user credentials. Gaining access to an organization's network through a valid user account is likely to generate the least amount of system noise, because it may blur the line between legitimate and unauthorized user activity.

That being said, our team focuses on implementing new detection analytics and tuning existing ones, with a particular emphasis on monitoring identity behavior. This includes factors such as usernames and passwords, multi-factor authentication (MFA), geolocation, role-based access control (RBAC), account manipulation, user endpoint telemetry, and more. Identity coverage is valuable because it provides a holistic view of user activity, allowing us to detect anomalies and potential threats with broader granularity.

As the saying goes, "identity is the new perimeter," which is largely attributed to the shift towards a more remote-flexible workforce. With this reality facing many modern businesses, along with the ever-changing threat landscape, cyber protection must not only keep up with these trends but also stay one step ahead.

External Trend

Michigan-Based McLaren HealthCare Victim of Black Cat/AlphV Ransomware Attack

One of the largest healthcare systems in Michigan, McLaren HealthCare, is dealing with a ransomware attack after the notorious Black Cat/AlphV ransomware gang claimed responsibility and stated that they have stolen 6 TB of data, including personal data and videos of the hospitals' work.

McLaren recently detected suspicious activity on its computer network and launched an investigation. The organization determined that it experienced a ransomware event and is currently looking into reports that some data may be available on the dark web. McLaren operates 13 hospitals across Michigan and offers various medical services such as infusion centers, cancer centers, and primary and specialty care offices.

Steps To Mitigate

- User awareness training
- Implement phishing-resistant multi-factor authentication (MFA)
- Keep all systems and applications updated
- Maintain a modern security solution

CISA Launches Ransomware Vulnerability Warning Pilot Program to Address Exploited Security Flaws

CISA has launched the Ransomware Vulnerability Warning Pilot (RVWP) program to help organizations identify and address security flaws exploited by ransomware groups. The program includes two new resources: a column in the Known Exploited Vulnerabilities catalog that flags flaws associated with ransomware campaigns, and a table on the StopRansomware project's website that provides information on targeted misconfigurations and weaknesses. CISA has identified over 1,000 vulnerabilities with evidence of in-the-wild exploitation, including the recent CVE-2023-40044 flaw in Progress Software's WS_FTP server. The RVWP has identified more than 800 vulnerable systems withincritical infrastructure networks.

Through the RVWP, CISA aims to warn organizations about vulnerabilities commonly exploited by ransomware, enabling mitigation before an attack occurs. The resources provided facilitate the identification and elimination of security flaws and offer guidance on mitigation and compensation efforts. The program targets critical infrastructure entities in industries such as energy, education, healthcare, and water systems.

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