CYBERFORCE | Q

December 13, 2023

NOVEMBER 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

Participants in our program have the opportunity to experience proven tactics that are customized to their specific technologies and workflows.

Takeaway 2

Google has issued a warning about threat actors using native cloud tools to conceal their malicious activities.

Takeaway 3

CyberForce|Q's collective approach helps organizations share strategies and quantifiable results.

Case Study

Collective Innovation: Empowering Cybersecurity Through CyberForce|Q's Comprehensive Services and Collaborative Approach

CyberForce|Q is a collective force for good in the cybersecurity realm. Our brand promise is to provide proven cybersecurity program advancement, offering a range of services and benefits to individuals and organizations. The best cybersecurity leaders work in the collective to share strategies and quantifiable results. Participants in our program have the opportunity to experience proven tactics that are customized to their specific technologies and workflows. This allows individuals to acquire valuable skills in cybersecurity while organizations rely on us to operationalize their cybersecurity capabilities, effectively protecting them from various threats.

One of the key aspects of our mission is our commitment to providing strategic and tactical guidance that is aligned with the client's objectives and leveraged with the current state of their cybersecurity program. This ensures that the efforts put in place are focused on achieving the desired outcomes. Another important aspect of our offering is our emphasis on measurable risk reduction. We provide a methodology, scoring system, and proof through our platform and reporting, allowing clients to track and monitor the progress made in reducing their cybersecurity risks. This data-driven approach helps organizations make informed decisions and adapt their cybersecurity strategies accordingly.

In addition to these services, we also facilitate collective knowledge sharing among its participants. We provide a network and a cadence for collaboration, allowing cybersecurity professionals to learn from each other, exchange ideas, and inform their cybersecurity plans. By harnessing the collective wisdom and expertise of the community, we ensure that our participants are equipped with the latest insights and best practices in the field.

External Trend

Google Warns of "Google Calendar RAT" Exploit Using Calendar Events for C2 Purposes

Google has issued a warning about threat actors using native cloud tools to conceal their malicious activities. In its recent Threat Horizons report, Google highlighted a proof-of-concept exploit called "Google Calendar RAT," which repurposed Google Calendar events for command-and-control purposes. Although Google has not seen it in real-world deployments, multiple users have shared it on cybercriminal forums, indicating some level of interest. Google has since implemented a fix to block this tool, but similar malware may be on the horizon.

The Google Calendar RAT significantly reduces the infrastructure required for command-and-control purposes. Threat actors only need to set up a Google service account, obtain its credentials.json file, create a new Google calendar, and share it with the service account. By editing the script and executing commands through the event description field, the RAT checks for commands on infected machines and returns the output in the same field. Notably, the Google Cloud RAT operates entirely over legitimate cloud infrastructure, making it challenging to identify and prevent.

Steps To Mitigate

Architect systems with a defense-in-depth approach to reduce risk if threat actors bypass controls by evading detection such as when using valid cloud services.

Segment networks to reduce the impact of adversaries gaining access to additional resources in your environment.

Develop baselines for network traffic and monitor for connections to user facing cloud services to help identify low prevalence and/or anomalous behavior.

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