# Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : c0f5db49 Oct 11, 2023, 07:19 AM

**Today's Headlines:**

**Leading Story**

- HTTP/2 Rapid Reset: Deconstructing the Record-Breaking Attack

**Data Breaches & Data Leaks**

- Nothing to Report

**Cyber Crimes & Incidents**

- New Grayling APT Targeting Organizations in Taiwan, US
- Savvy Israel-Linked Hacking Group Reemerges Amid Gaza Fighting

**Vulnerabilities & Exploits**

- New Critical Citrix NetScaler Flaw Exposes Sensitive Data
- Microsoft Warns of Nation-State Hackers Exploiting Critical Atlassian Confluence Vulnerability

**Trends & Reports**

- Google Makes Passkeys the Default Sign-In for Personal Accounts
- North Korea's State-Sponsored APTs Organize & Align

**Privacy, Legal & Regulatory**

- Nothing to Report

**Cybersecurity Awareness Month**

- The Daily Cyber Headlines are being shared during the month of October at **TLP:WHITE** for Cybersecurity Awareness Month.

**Upcoming Health-ISAC Events**

- Americas Hobby Exercise - October 25, 2023. Registration is available here.
- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

**Additional Information**

**Leading Story**

HTTP/2 Rapid Reset: Deconstructing the Record-Breaking Attack

**Summary**

- A new record-breaking HTTP DDoS attack reached more than 201 million requests per second, nearly 3 times larger than the previous biggest attack.

**Analysis & Action**

By exploiting a new zero-day vulnerability tracked as CVE-2023-44487 and named the HTTP/2 Rapid Reset vulnerability in the HTTP/2 protocol, threat actors managed to create a botnet of 20,000 machines. This botnet conducted a Distributed Denial of Service (DDoS) attack that peaked at 201 million requests per second (rps). This represents the largest attack of its kind, with the previous largest attack being only 71 million rps.

This security incident, like many others such as Shellshock and Heartbleed has the potential to create catastrophic damage and cascading impacts. Threat actors are being made aware of this HTTP/2 vulnerability, making the race to find a patch even more important.

Members should isolate their internet facing applications to understand which ones are at risk of this new vulnerability. Members are recommended to utilize DDoS protection for layer 7 applications and layer 3 network traffic entities. To minimize the capacity for an attack to be successful, it is also recommended that members update all automation functions to avoid API abuse. To read the Health-ISAC threat bulletin, click here.

**Data Breaches & Data Leaks**

- Nothing to Report

**Cyber Crimes & Incidents**

New Grayling APT Targeting Organizations in Taiwan, US

**Summary**

- Various organizations in the United States and Asia-Pacific region are at risk of intelligence gathering operations conducted by a new advanced persistent threat (APT) actor.

**Analysis & Action**

An APT under the name Grayling has been targeting specific sectors of the manufacturing, IT, biomedical, and government sectors of numerous organizations in Taiwan and in the United States. The APT group ran intelligence-gathering campaigns against Vietnam and the United States earlier this year.

Threat actors attack these organizations by exploiting web-facing assets and performing dynamic-link library (DLL) sideloading to deploy custom malware and publicly available tools such as Havoc, Cobalt Strike, NetSpy, and Mimikatz. Threat actors have also been cited on exploiting CVE-2019-0803, a privilege escalation bug in Windows.

Members are recommended to ensure that all Windows services are updated to the latest version of the Windows operating system to remove CVE-2019-0803 from their environment.

Savvy Israel-Linked Hacking Group Reemerges Amid Gaza Fighting

**Summary**

- In the middle of the rising crisis between Israel and Palestine, an old threat actor resurfaced on the scene.

**Analysis & Action**

Predatory Sparrow, a hacking group thought to be based in Israel, has announced its return in the middle of the rising tension between Israel and Palestine.

Between 2021 and 2022, Predatory Sparrow carried several high-profile strikes on Iranian government entities. Among these incidents were attacks on the country's payment systems, petrol pump network, and steel factories. They are regarded as one of the more prolific actors to join the conflict's cyber side.

Hacktivists and possibly state-backed actors, including suspected Iranian and Chinese information operations, are now active on both sides of the conflict, and the situation is predicted to worsen.

You can read Health-ISAC's alert on the conflict and its potential impact on the healthcare sector here.

## Vulnerabilities & Exploits

### New Critical Citrix NetScaler Flaw Exposes Sensitive Data

**Summary**

- A critical vulnerability has been spotted in Citrix NetScaler ADC and NetScaler Gateway systems.

**Analysis & Action**

According to Bleeping Computer, a flaw being tracked as CVE-2023-4966 has been spotted in Citrix NetScaler ADC and NetScaler Gateway systems and is deemed to be remotely and easily exploitable.

The flaw's exploitation could lead to sensitive information being compromised. A second flaw, CVE-2023-4967, was also found that could lead to a denial of service of vulnerable devices. Current sources do not disclose what kind of sensitive information is at risk of these vulnerabilities.

Members who use Citrix NetScaler ADC and NetScaler Gateway are encouraged to upgrade their systems as soon as possible to patch up the vulnerabilities and prevent potential exploitations from threat actors.

### Microsoft Warns of Nation-State Hackers Exploiting Critical Atlassian Confluence Vulnerability

**Summary**

- Incident involving exploitation of a critical flaw in Atlassian Confluence Data Center and Server was attributed to a Chinese nation-state actor.

**Analysis & Action**

Microsoft has attributed a recent incident involving exploitation of a critical flaw in Atlassian Confluence Data Center and Server to a Chinese nation-state actor called Storm-0062 (also known as DarkShadow or Oro0lxy).

The vulnerability, tracked as CVE-2023-22515, and rated 10.0 on the CVSS severity rating system, allows remote attackers to create unauthorized administrator accounts and access servers. The flaw has been addressed in versions 8.3.3 or later, 8.4.3 or later, and 8.5.2 (Long Term Support release) or later.

Organizations that utilize Confluence applications should immediately update to the newest versions or isolate them from the rest of the network until patching is possible.

## Trends & Reports

### Google Makes Passkeys the Default Sign-In for Personal Accounts

**Summary**

- Google is making passkeys the default sign-in option across all services and platforms.

**Analysis & Action**
Google now offers passwordless sign-in on accounts and added passkey support to Chrome and Android OS. Now, Google has made the passkey their default sign-in method.

A password-less sign-in uniquely tied to each user device offers a secure alternative to passwords. They work locally and allow for the use of things like biometric sensors and PINs. Passkeys reduce the impact of a data breach because there is not a password to use to login to another account. Passkeys are also securely stored in the cloud, preventing any issues regarding being locked out if a device is lost or stolen.

Members who use Google's services are advised to create a passkey in accordance with their new sign-in recommendations. Members should continue to stay updated with any new developments regarding sign-in methods, policies, and procedures.

North Korea's State-Sponsored APTs Organize & Align

**Summary**

- Various North Korean advanced persistent threat (APT) groups have become aligned, setting the stage for aggressive, complex cyber-attacks.

**Analysis & Action**
A recent report from Mandiant revealed APTs associated with North Korea coordinating their efforts and sharing tools and information, making individual groups harder to track. This new approach makes it difficult to defend against, while allowing threat actors to move stealthily with greater speed and adaptability.

The recent collaboration that was noted is the highest since COVID-19 and it is unclear as to whether it was an intentional collaboration or one driven by necessity.

The report by Mandiant says that the ultimate takeaway is that defenders would be better served focusing on the specific nature of a particular activity rather than identifying the specific threat actor behind it. A collective response to counter APT groups tends to maximize imposed cost on threat actor rather than the victim.

The Mandiant report is available for review here.

## Privacy, Legal & Regulatory

Nothing to Report.

## Health-ISAC Cyber Threat Level

On September 20, 2023, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level at Blue (Guarded). The Threat Level of Blue (Guarded) is due to threats from concerns regarding malvertising, rogue USB drives, Async RAT, MFA Bypass, and persistent credential stuffing/spraying.

**For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.**

**You must have Cyware Access to reach the Threat Advisory System document. Contact membership@h-isac.org for access to Cyware.**

**Reference | References**

**cloudflare**
**Security Week**
**Cyberscoop**
**Bleeping Computer**
**The Hacker News**
**Bleeping Computer**
**Dark Reading**

**Tags**

Grayling, Israel-Hamas, Citrix, HTTP/2

**TLP:WHITE:** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

**Share Threat Intel:**
For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP Share Threat Intel Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

**Turn off Categories:**
For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

**Access the Health-ISAC Intelligence Portal:**
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-

isac.org for access to Cyware.

**For Questions or Comments:**

Please email us at toc@h-isac.org