Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 1d7697b0 | Oct 02, 2024, 07:46 AM

Today's Headlines:

Leading Story

- Released Guidance on Principles of OT Cybersecurity for Critical Infrastructure Organizations

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- Rackspace Internal Monitoring Web Servers Hit By Zero Day
- U.K. Hacker Charged In $3.75 Million Insider Trading Scheme Using Hacked Executive Emails

Vulnerabilities & Exploits

- Researchers Sound Alarm on Active Attacks Exploiting Critical Zimbra Postjournal Flaw

Trends & Reports

- Police Arrest Four Suspects Linked to LockBit Ransomware Gang
- European Security Teams Are Understaffed and Underfunded

Privacy, Legal & Regulatory

- Evil Corp Hit with New Sanctions, BitPaymer Ransomware Charges

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas – October 29, 2024, 12:00-01:00 PM ET

    - European – October 30, 2024, 03:00-04:00 PM CET
- T-SIG Webinar for SMB Members – October 10, 2024 at 11:30 AM ET
- European Summit, Athens, Greece - October 15-17, 2024
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Additional Information

Leading Story

Released Guidance on Principles of OT Cybersecurity for Critical Infrastructure Organizations

Summary

- Cyber agencies have published a collaborative guide, Principles of Operational Technology Cybersecurity.

Analysis & Action

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and international partners released the guide Principles of Operational Technology Cybersecurity.

This guidance offers essential information for creating and maintaining a secure operational technology (OT) environment. The six principles help organizations understand how business decisions can impact OT cybersecurity and the risks involved. Following best practices and recommended actions can reduce residual risk in OT decisions.

Health-ISAC recommends members read the guidelines and assess how their implementation can improve OT security within their organization.

Data Breaches & Data Leaks

Nothing to Report.

Cyber Crimes & Incidents

Rackspace Internal Monitoring Web Servers Hit By Zero Day

Summary

- Zero-day bug exploited by threat actors in a third-party app ScienceLogic used by Rackspace.

Analysis & Action

The technology company Rackspace has addressed its customer base regarding a threat actor's ability to break into the internal monitoring and performance environment it was using. This, in turn, led to a temporary closure of the company's monitoring dashboard for its customers.

The threat actors used a zero-day vulnerability to access Rackspace's internal web servers through a ScienceLogic-powered dashboard for monitoring catered to customers. Later discoveries by the company on September 24, 2024, found remote code execution vulnerabilities that had been exploited. The company has promised its customers that it has taken immediate action, shutting down affected services and stating there is no need for external remediation. ScienceLogic has yet to release any information on the threat actor that committed the attacks and has declined to identify the software that has been exploited.

Heath-ISAC recommends heavy monitoring of third-party access to data along with suggested implementations of third-party risk management. Additionally, including third-party audits can help maintain liability and assurance regarding general security practices.

U.K. Hacker Charged In $3.75 Million Insider Trading Scheme Using Hacked Executive Emails

Summary

- A lone threat actor who made $3.75 million illegally from hacking and using executive emails has been charged.

Analysis & Action

The man faces various charges, including wire fraud, securities fraud, and computer fraud, in which he has gained roughly $3.75 million throughout his stint. The actor is believed to have followed through with these attacks from January 2019 to May 2020.

At this time, there are at least five instances in which the actor gained unauthorized access to various email accounts. These email accounts belonged to corporate executives, in which he could obtain sensitive information, including announcements regarding impending earnings. Using the

accessed information, the actor would purchase securities and sell them quickly to make profits. A total of five public companies' sensitive information was obtained ahead of the announcement of 14 earnings through the resetting of passwords. The actor attempted to cover his tracks using anonymous emails, VPN, and Bitcoin, but he was still identified through asset tracing and data analytics.

Health-ISAC recommends strong password protection practices to ensure the safety of all sensitive information. Additionally, encryption methods to further strengthen protection are encouraged to mitigate the risks of similar instances.

Vulnerabilities & Exploits

Researchers Sound Alarm on Active Attacks Exploiting Critical Zimbra Postjournal Flaw

Summary

- Cybersecurity researchers have warned about ongoing exploitation attempts targeting a newly revealed security flaw in Synacor's Zimbra Collaboration platform.

Analysis & Action

Proofpoint has observed attacks targeting security flaws in Synacor's Zimbra Collaboration platform, tracked as CVE-2024-45519, since September 28, 2024.

The flaw affects Zimbra's postjournal service, allowing unauthorized attackers to run arbitrary commands on affected systems. The flaw was addressed in patched versions released on September 4, 2024. The attacks involve spoofed Gmail emails containing fake addresses added to CC, attempting to trigger Zimbra servers to execute malicious commands. These fake addresses contain Base64 strings that are executed with the sh utility.

Health-ISAC recommends applying the provided patches to safeguard against potential exploits or considering removing the postjournal binary as a temporary workaround until patches can be applied.

Trends & Reports

Police Arrest Four Suspects Linked to LockBit Ransomware Gang

Summary

- In a coordinated global effort, authorities from 12 countries have arrested four individuals connected to the LockBit ransomware gang.

Analysis & Action

The suspects included a developer, an administrator of a bulletproof hosting service, and two others involved in LockBit's operations. The joint operation, codenamed Operation Cronos, was led by the UK's National Crime Agency (NCA) and resulted in the seizure of LockBit infrastructure servers. The investigation began in April 2022.

Among the notable arrests was a suspected LockBit developer apprehended in August 2024 in France. Additionally, the NCA arrested two individuals in the UK linked to LockBit activity, including one believed to be associated with a LockBit affiliate and another suspected of money laundering.

In a separate action, Spanish authorities arrested the administrator of a bulletproof hosting service used to protect LockBit's infrastructure. To further disrupt the gang's operations, Australia, the United Kingdom, and the United States have imposed sanctions on individuals associated with LockBit, including a prolific affiliate linked to the notorious Evil Corp ransomware group. These sanctions target individuals involved in Evil Corp's criminal activities, with the UK sanctioning 15 individuals, the US sanctioning six, and Australia targeting two.

European Security Teams Are Understaffed and Underfunded

Summary

- European IT teams are facing challenges like being understaffed, underfunded, and suffering from skills gaps.

Analysis & Action

As reported by ISACA, an international professional association focused on IT governance, European IT security teams face significant challenges, including being understaffed and underfunded and suffering from skills gaps.

A survey of over 1800 members revealed that 61% believe their team lacks sufficient staff. 19% of those surveyed said they have unfilled entry-level positions, and 48% said they are in a similar situation with vacancies for more experienced roles. Soft skills, such as communication and problem-solving, are highlighted as lacking among cybersecurity professionals, emphasizing the need for employers to prioritize both technical and soft skills when hiring. Additionally, stress levels are increasing in the industry, with 68% of professionals feeling more stressed due to a complex threat landscape and persistent talent shortages.

The cybersecurity industry must address these challenges to maintain security resilience and protect critical infrastructure.

Privacy, Legal & Regulatory

Evil Corp Hit with New Sanctions, BitPaymer Ransomware Charges

Summary

- The United States, United Kingdom, and Australia have imposed new sanctions on the notorious cybercrime syndicate Evil Corp.

Analysis & Action

The U.S. has indicted an Evil Corp member for conducting BitPaymer ransomware attacks. The latest sanctions target seven individuals and two entities associated with the group, including Maksim Yakubets' father-in-law, Eduard Benderskiy. Benderskiy, a former Russian intelligence officer and businessman, is accused of facilitating Evil Corp's ties to the Russian government.

In 2019, the U.S. sanctioned 17 individuals and seven entities linked to Evil Corp. Today's actions expanded on those efforts, with the U.K. and Australia joining the U.S. in targeting the group's members and associates.

The U.S. Treasury Department alleges that Eduard Benderskiy played a crucial role in connecting Evil Corp with the Russian state. His former affiliation with the FSB, Russia's intelligence agency, is cited as evidence of this connection.

Health-ISAC Cyber Threat Level

On September 19, 2024, 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:

The Threat Level of Blue (Guarded) is due to threats from DPRK IT fraud, elections-induced cyber activity, potential repercussions of recent activity in the Middle East, potential Ivanti Endpoint Manager exploitation, and ongoing observances of infostealer's logs being posted on Telegram.

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.

Report Source(s)

Health-ISAC

Incident Date

Oct 02, 2024, 11:59 PM

Reference | References

Bleeping Computer
CISA
The Register
The Hacker News
Bleeping Computer
Infosecurity Magazine
The Hacker News

Tags

Email Hacking Attack, Zimbra Postjournal Flaw, OT Cybersecurity, Security Teams, LockBit Ransomware, Evil Corp

---

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

Access the Health-ISAC Threat 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 Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org