Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 431ec492 | Oct 22, 2024, 08:17 AM

Today's Headlines:

Leading Story

- Bumblebee Malware Returns After Recent Law Enforcement Disruption

Data Breaches & Data Leaks

- Cisco Confirms Security Incident After Hacker Offers to Sell Data

Cyber Crimes & Incidents

- ESET Distributor's Systems Abused To Deliver Wiper Malware
- Has BlackCat Returned As Cicada3301? Maybe.

Vulnerabilities & Exploits

- Atlassian Patches Vulnerabilities in Bitbucket, Confluence, Jira
- Roundcube Webmail Vulnerability Exploited in Government Attack

Trends & Reports

- Cyber Threats In Manufacturing Report Show Alarming Cybersecurity Trends In Industry

Privacy, Legal & Regulatory

- Nothing to Report

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 – November 14, 2024 at 11:30 AM ET
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Additional Information

Leading Story

Bumblebee Malware Returns After Recent Law Enforcement Disruption

Summary

- Previously disrupted in May, the Bumblebee malware loader has resurfaced in recent attacks.

Analysis & Action

The Bumblebee malware loader was originally assessed to be developed as a replacement for the Bazarloader backdoor to enable ransomware operations to gain access to victim networks. Typically, the malware is delivered via tactics including phishing, malvertising, and SEO poisoning, leveraging commonly used software as lures. Oftentimes, an infection leveraging the Bumblebee malware loader dropped Cobalt Strike beacons, infostealer malware, and different ransomware strains.

In May, a global law enforcement operation dubbed Operation Endgame disrupted several malware loader operations, including Bumblebee, by seizing over 100 servers. Despite their disappearance after Operation Endgame, security researchers have recently observed new Bumblebee activity associated with the malware, indicating its return.

Newly observed activity regarding Bumblebee malware loader begins with a phishing email that tricks victims into downloading a malicious ZIP file. The ZIP file contains a shortcut that triggers PowerShell to retrieve a malicious MSI executable disguised as a legitimate update. The MSI file is silently executed, and the malware is dropped into the memory. It is important that organizations continue to educate end-users, employ email security, and implement endpoint protection measures to help defend enterprise networks against the use of malware.

Data Breaches & Data Leaks

Cisco Confirms Security Incident After Hacker Offers to Sell Data

Summary

- Cisco acknowledges some of its files were stolen in a recent cyberattack after the data was offered up for sale.

Analysis & Action

On October 14, 2024, the cybercriminal group IntelBroker claimed to have stolen sensitive information from Cisco in a data breach.

The stolen data includes GitHub and SonarQube projects, source code, hardcoded credentials, certificates, confidential documents, Jira tickets, API tokens, AWS private buckets, encryption keys, and other types of information. Additionally, IntelBroker claimed to have stolen source code from major companies, including Microsoft, AT&T, Verizon, Chevron, BT, SAP, T-Mobile, and Bank of America.

After learning about the threat actors' claims of having gained access to management interfaces, internal documents, and customer data, Cisco launched an ongoing investigation and determined their systems were not breached. However, Cisco disclosed that the threat actor obtained data from a public-facing DevHub environment. To prevent data breaches, DevHub users should regularly update their platforms, enforce strong access controls, and avoid storing sensitive information in publicly accessible environments.

Cyber Crimes & Incidents

ESET Distributor's Systems Abused To Deliver Wiper Malware

Summary

- Official product distributor ESET was abused to deliver wiper malware, launching investigations by the company.

Analysis & Action

Analysis done by ESET's Advanced Threat Defense team announced that the targeting users have since been informed via email. The emails contained information on the government-backed threat actors and their attempts to compromise their devices.

Further research found that the threat actor's malicious emails could get through DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) checks. Included was a link to an ESET Israel store, which pointed to a ZIP file with an executable called setup.exe deploying wiper malware on targeted victims' systems. ESET has since come out, confirming their awareness of the incident and stating the campaign had been blocked within 10 minutes. ESET was not compromised by the campaign as it continues to monitor and investigate the situation further.

As malicious phishing attempts become common for threat actors, the importance of following best practices remains evident. Heath-ISAC recommends that its members implement anti-phishing tools and remain vigilant about suspicious emails.

Has BlackCat Returned As Cicada3301? Maybe.

Summary

- Cicada3301, a similar iteration to BlackCat, a top malware type in 2022, has emerged, indicating the malware type's return.

Analysis & Action

During their activity, the ransomware group consistently made the top ten list of threat actors, being the first Rust-written piece of ransomware.

Upgraded versions of the ransomware known as Sphinx utilized common encryption lines, preventing security teams from accessing their code. Additionally, the threat actor used custom malware named ExMatter to automate their data exfiltration; once complete, the tool would self-delete to avoid detection. The threat actor targeted entities, including government agencies, energy providers, and educational institutions.

The threat actor is now believed to have returned after selling its Ransomware-as-a-Service source code for $5 million and being on hiatus for six months, taking on the name Cicada3301. Cicada3301 has begun targeting small and medium-sized businesses using easy-to-crack passwords or stolen

credentials. These events lead officials to believe that malware can be in the development process as these more small-scale attacks continue to take place.

Health-ISAC recommends issuing the latest patches and limiting file sharing to mitigate risks of malware attacks. Additionally, including trusted antimalware and antivirus software can help defend against ransomware attacks, detecting and responding to any malicious threat.

Vulnerabilities & Exploits

Atlassian Patches Vulnerabilities in Bitbucket, Confluence, Jira

Summary

- Security patches have been released to address vulnerabilities affecting several Atlassian products.

Analysis & Action

Atlassian released patches for several products, including Bitbucket, Confluence, and Jira Service Management. For Bitbucket Data Center and Server, Atlassian released an update for a critical vulnerability, tracked as CVE-2024-21147, which affects the Java Runtime Environment (JRE). This vulnerability could allow unauthorized access to and tampering with sensitive data.

Patches for this security flaw followed Oracle's release of fixes, which Atlassian included in Bitbucket Data Center and Server versions 9.2.1, 8.19.10, and 8.9.20.

Atlassian released Confluence Data Center and Server updates to address four high-severity vulnerabilities. These vulnerabilities include two publicly disclosed path traversal and ReDoS issues in an open-source JavaScript library, a cross-site scripting flaw, and an Apache Commons Configuration bug. Updates for these vulnerabilities are available in Confluence Data Center and Server versions 7.19.26, 8.0.0, 8.5.11, 8.9.3, and all versions greater than 9.0.0.

Lastly, Atlassian released security updates for the Jira Service Management Data Center and Server to address a vulnerability tracked as CVE-2024-7254. The vulnerability stems from a Protobuf buffer overflow flaw that can allow threat actors to disrupt service availability. Updates for this vulnerability are available in versions 5.12.14, 5.17.4, and 10.1.1.

Health-ISAC recommends patching affected instances to the latest version to mitigate risks of exploitation.

Roundcube Webmail Vulnerability Exploited in Government Attack

Summary

- A threat actor was recently observed targeting a governmental organization by exploiting a vulnerability affecting Roundcube Webmail.

Analysis & Action

The vulnerability, tracked as CVE-2024-37383, is a cross-site scripting (XSS) security flaw affecting how Roundcube handles SVG animate attributes. Updates for the vulnerability were released on May 19, 2024, and are available in versions 1.5.7 and 1.6.7.

Cybersecurity firm Positive Technologies discovered that a governmental organization in a Commonwealth of Independent States (CIS) country was targeted via exploitation activity against the vulnerability. The attack involved a malicious email containing distinctive tags attached, allowing the threat actor to bypass Roudcube's security checks and execute nefarious code.

Further analysis of the attack revealed that the executed code intended to save the malicious attachment, steal emails, and harvest user credentials. Health-ISAC recommends updating affected Roundcube Webmail instances to the latest versions to prevent similar targeted activity.

Trends & Reports

Cyber Threats In Manufacturing Report Show Alarming Cybersecurity Trends In Industry

Summary

- As cyber threats continue to evolve, recent reports evaluate cybersecurity trends within the manufacturing industry

Analysis & Action

Further analysis of the state of the manufacturing industry regarding cyber attacks has led to reports claiming that manufacturing is the most vulnerable, accounting for over 25% of incidents.

With manufacturing being a top 10 industry, it has become a target for threat actors to administer their attacks. Researchers confirm that 45% of cyberattacks in these top 10 industries are malware attacks, pressing more concerns about the imposing risks to these industries. With manufacturing growing more reliant on both IT and OT systems, vulnerabilities only seem to be increasing. Training is being provided to combat these threats so that recognition of threat actor methods like phishing and social engineering can be found early. Recent attacks have come about across Europe, North America, Asia, and Oceania, as protecting the manufacturing industry highlights the need for defenses against cyber threats.

As cyber threats become more experienced and robust in their methods of attacking various industries, preventative strategies become even more important. Health-ISAC recommends that its members issue the latest patches to all systems and limit file sharing to mitigate the risks of malware attacks.

Privacy, Legal & Regulatory

- Nothing to Report.

Health-ISAC Cyber Threat Level

On October 17, 2024, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to raise the Cyber Threat Level to Yellow (Elevated). The Threat Level of Yellow (Elevated) is due to threats from:

The Threat Level of Yellow (Elevated) is due to threats from elections-related smishing campaigns, DPRK remote worker activity, potential repercussions of recent activity in the Middle East, commodity malware, and a recent uptick in ransomware events.

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 22, 2024, 11:59 PM

Reference | References

cnhinews
Security Week
Security Week
Security Week
Security Intelligence
Security Week
Bleeping Computer

Tags

Cicada3301, BlackCat, Bumblebee, ESET, Cisco

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 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