Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

June 18, 2024

Extracted from multiple sources by PT and OTRB, and ST ISAC analysts for the purpose of supporting ISAC member cybersecurity awareness, protection, and mitigation.

Recipients may share this report only within their own immediate organization. No further dissemination is authorized.

AT-A-GLANCE

Executive News

- UK Man Suspected of Being 'Scattered Spider' Leader Arrested
- Decade-Old Cyber Advice From Gao Remains Unimplemented, Watchdog Says
- China-Linked Hackers Infiltrate East Asian Firm for 3 Years Using F5 Devices
- North Korea's Moonstone Sleet Widens Distribution of Malicious Code
- Report Reveals Record Exploitation Rate For Load Balancers
- Analysis Of User Password Strength
- Malware Peddlers Love This One Social Engineering Trick!

Emerging Threats & Vulnerabilities

- Operation Celestial Force Employs Mobile And Desktop Malware To Target Indian Entities
- Fortinet Patches Code Execution Vulnerability in FortiOS
- Arid Viper Launches Mobile Espionage Campaign with AridSpy Malware
- TellYouThePass Ransomware Group Exploits Critical PHP Flaw
- WithSecure Reveals Mass Exploitation of Edge Software and Infrastructure Appliances

Attacks, Breaches, & Leaks

- Keytronic Says Personal Information Stolen in Ransomware Attack
- Kansas City Kansas Police Department
- Insurance Giant Globe Life Investigating Web Portal Breach
- Cyber Attack Takes Richland, Wash., Schools Offline

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

UK Man Suspected of Being 'Scattered Spider' Leader Arrested
Security Week, 6/17/2024

Spanish news website Murcia Today reported on June 14 that an unnamed British man had been arrested in Palma de Mallorca as he was trying to board a flight to Italy. The arrest was the result of collaboration between Spanish police and the FBI. The FBI announced in May that it had been seeking to charge members of the Scattered Spider cybercrime group, whose members are largely believed to be from the US and western countries, and some from eastern Europe. One alleged member of the group, a 19-year-old from Florida, was arrested in January. Active since early 2022, Scattered Spider is also known as Starfraud, UNC3944, Scatter Swine, and Muddled Libra. Its financially motivated operations have targeted organizations in customer relationship management (CRM), business-process outsourcing (BPO), telecoms and the technology sectors. https://www.securityweek.com/uk-man-suspected-of-being-scattered-spider-leader-arrested/

Decade-Old Cyber Advice From Gao Remains Unimplemented, Watchdog Says
NextGov, 6/13/2024

Nearly 570 out of 1,610 cybersecurity recommendations for federal agencies remain unimplemented as of May 2024, hindering the government's ability to protect its sensitive systems, critical infrastructure and sensitive data from hackers, according to a report from the Government Accountability Office. As of last month, agencies have implemented 1,043 of GAO's recommendations made since 2010 in an effort to fix "challenge areas" involved in protecting government systems, but 567 of them remain unaddressed. "This increases the risk that the nation will be unprepared to respond to the cyber threats that can cause serious damage to public safety, national security, the environment, and economic well-being," GAO auditors said in the paper, released as part of the watchdog's High Risk series that focuses on programs needing swift cost overhaul, new management or transformation.
https://www.nextgov.com/cybersecurity/2024/06/decade-old-cyber-advice-gao-remains-unimplemented-watchdog-says/397356/

China-Linked Hackers Infiltrate East Asian Firm for 3 Years Using F5 Devices
The Hacker News, 6/17/2024

A suspected China-nexus cyber espionage actor has been attributed as behind a prolonged attack against an unnamed organization located in East Asia for a period of about three years, with the adversary establishing persistence using legacy F5 BIG-IP appliances and using it as an internal command-and-control (C&C) for defense evasion purposes. Cybersecurity company Sygnia, which responded to the intrusion in late 2023, is tracking the activity under the name Velvet Ant, vulnerabilities. https://thehackernews.com/2024/06/china-linked-hackers-infiltrate-east.html

North Korea's Moonstone Sleet Widens Distribution of Malicious Code
Dark Reading, 6/13/2024

A newly identified North Korean threat actor has widened its distribution of malicious node package manager (npm) code to public registries. And it's differentiating itself from other state-sponsored groups as it ramps up activity to threaten the software supply chain by poisoning open source code repositories. Moonstone Sleet first appeared on the scene late last month, when Microsoft revealed that the threat group concurrently was engaged in espionage and financial cyberattacks using a grab bag of attack techniques against aerospace, education, and software organizations and developers. Among those techniques was to try to get hired for remote tech jobs with real companies and, in the process, spread malicious npm packages on LinkedIn and freelancer websites.
https://www.darkreading.com/cyberattacks-data-breaches/north-koreas-moonstone-sleet-widens-distribution-of-malicious-code-packages

Report Reveals Record Exploitation Rate For Load Balancers
InfoSecurity Magazine, 6/18/2024

Threat actors are increasingly targeting edge devices known as load balancers, according to new data from Action1 which revealed a record exploitation rate for the category over a three-year period. The security vendor assessed various categories of products from 2021-2023, using NVD and cvedetails.com data to calculate the ratio of exploited vulnerabilities to total vulnerabilities. It found that while load balancers overall were fairly secure, they were disproportionately targeted by threat actors – leading to a record 17% exploitation rate over the period. This rose to 100% for NGINX and 57% for Citrix products. “Vulnerabilities in load balancers pose significant risks, as a single exploit in these systems can provide broad access or disruption capabilities against targeted networks,” the report warned.
https://www.infosecurity-magazine.com/news/record-100-exploitation-rate-load/

Analysis Of User Password Strength
SecureList, 6/18/2024

The processing power of computers keeps growing, helping users to solve increasingly complex problems faster. A side effect is that passwords that were impossible to guess just a few years ago can be cracked by hackers within mere seconds in 2024. For example, the RTX 4090 GPU is capable of guessing an eight-character password consisting of same-case English letters and digits, or 36 combinable characters, within just 17 seconds. Our study of resistance to brute-force attacks found that a large percentage of passwords (59%) can be cracked in under one hour.
https://securelist.com/passworde-brute-force-time/112984/

Malware Peddlers Love This One Social Engineering Trick!
HelpNet Security, 6/17/2024

Getting users to install malware on their computers was always a matter of finding the right lure and bypassing security protections. As the latter get better (and broader) and users' awareness of attackers' usual tricks increases, threat actors must adapt their tactics. One method that is getting increasingly popular is the fake error message, whether displayed by a website or when opening an HTML document delivered as an email attachment. If the desire or need to see the webpage/document is great, many users will go through the outlined steps to "install the root certificate", "resolve the issue", "install the extension", or "update the DNS cache manually". https://www.helpnetsecurity.com/2024/06/17/social-engineering-malware-installation/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Operation Celestial Force Employs Mobile And Desktop Malware To Target Indian Entities -*** Cisco Talos is disclosing a new malware campaign called "Operation Celestial Force" running since at least 2018. It is still active today, employing the use of GravityRAT, an Android-based malware, along with a Windows-based malware loader we track as "HeavyLift." https://blog.talosintelligence.com/cosmic-leopard/
- ***Fortinet Patches Code Execution Vulnerability in FortiOS -*** The most severe of the issues is CVE-2024-23110 (CVSS score of 7.4), which collectively tracks multiple stack-based buffer overflow security defects in the platform's command line interpreter. https://www.securityweek.com/fortinet-patches-code-execution-vulnerability-in-fortios/
- ***Arid Viper Launches Mobile Espionage Campaign with AridSpy Malware*** - The threat actor known as Arid Viper has been attributed to a mobile espionage campaign that leverages trojanized Android apps to deliver a spyware strain dubbed AridSpy. https://thehackernews.com/2024/06/arid-viper-launches-mobile-espionage.html
- ***TellYouThePass Ransomware Group Exploits Critical PHP Flaw -*** A threat group is exploiting a critical, easily exploitable PHP bug for remote code execution (RCE) in living-off-the-land style ransomware attacks that target businesses and individuals running both Windows and Linux systems. https://www.darkreading.com/vulnerabilities-threats/tellyouthepass-ransomware-exploits-critical-php-flaw
- ***WithSecure Reveals Mass Exploitation of Edge Software and Infrastructure Appliances -*** Vulnerabilities in edge services and infrastructure devices are being increasingly exploited by cyber threat actors, according to a new report by WthSecure. https://www.infosecurity-magazine.com/news/withsecure-exploitation-edge/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Keytronic Says Personal Information Stolen in Ransomware Attack*** **-** Printed circuit board assembly (PCBA) manufacturing firm Keytronic has disclosed a data breach after a ransomware gang published information allegedly stolen from its network. https://www.securityweek.com/keytronic-says-personal-information-stolen-in-ransomware-attack/
- ***Kansas City Kansas Police Department*** **-** The Kansas City, Kansas Police Department is a premiere law enforcement agency. https://www.breachsense.com/breaches/great-lakes-international-trading-data-breach/
- ***Insurance Giant Globe Life Investigating Web Portal Breach*** **-** American financial services holding company Globe Life says attackers may have accessed consumer and policyholder data after breaching one of its web portals. https://www.bleepingcomputer.com/news/security/insurance-giant-globe-life-investigating-web-portal-breach/
- ***Cyber Attack Takes Richland, Wash., Schools Offline*** **-** Richland School District was without phones and Internet for at least three days this week, with grades and the district's enrollment portal inaccessible, after someone gained unauthorized access to the network. https://www.govtech.com/education/k-12/cyber-attack-takes-richland-wash-schools-offline

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT Alerts and Advisories

1. RAD DATA Communications - https://www.cisa.gov/news-events/ics-advisories/icsa-24-170-01

SUSE Security Updates

1. trento-agent - https://www.suse.com/support/update/announcement/2024/suse-ru-20242048-1
2. Trento - https://www.suse.com/support/update/announcement/2024/suse-fu-20242049-1
3. Podman - https://www.suse.com/support/update/announcement/2024/suse-su-20242050-1
4. openssl-1_1 - https://www.suse.com/support/update/announcement/2024/suse-su-20242051-1
5. cosign - https://www.suse.com/support/update/announcement/2024/suse-su-20241486-2
6. bouncycastle - https://www.suse.com/support/update/announcement/2024/suse-su-20241539-2
7. ghostscript - https://www.suse.com/support/update/announcement/2024/suse-su-20241590-2
8. python-Werkzeug - https://www.suse.com/support/update/announcement/2024/suse-su-20241591-2
9. libaom - https://www.suse.com/support/update/announcement/2024/suse-su-20242056-1
10. less - https://www.suse.com/support/update/announcement/2024/suse-su-20242060-1
11. MozillaFirefox - https://www.suse.com/support/update/announcement/2024/suse-su-20242061-1
12. Booth - https://www.suse.com/support/update/announcement/2024/suse-su-20242062-1
13. webkit2gtk3 - https://www.suse.com/support/update/announcement/2024/suse-su-20242065-1
14. xdg-desktop-portal - https://www.suse.com/support/update/announcement/2024/suse-su-20242067-1
15. python-requests - https://www.suse.com/support/update/announcement/2024/suse-su-20242068-1

Fedora Security Advisories

1. mariadb - https://lwn.net/Articles/978774/
2. ghostscript - https://lwn.net/Articles/978773/
3. galera - https://lwn.net/Articles/978772/

Check Point Security Advisories

1. Microsoft - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36884

2. PHP - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0377.html
3. Foxit Reader - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0357.html
4. Dynamic Linq - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1754.html
5. Gitlab - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1589.html

Red Hat Security Advisories

1. Firefox - https://access.redhat.com/errata/RHSA-2024:3972
2. Flatpack - https://access.redhat.com/errata/RHSA-2024:3979

Oracle Linux Security Update

1. Firefox –
    a. https://lwn.net/Articles/978780/
    b. https://lwn.net/Articles/978781/
    c. https://lwn.net/Articles/978778/
    d. https://lwn.net/Articles/978779/
2. Flatpak - https://lwn.net/Articles/978783/

Other

1. Events2 - https://typo3.org/security/advisory/typo3-ext-sa-2024-003
2. friendlycaptcha_official - https://typo3.org/security/advisory/typo3-ext-sa-2024-004
3. aimeos - https://typo3.org/security/advisory/typo3-ext-sa-2024-005
4. Chrome OS - https://chromereleases.googleblog.com/2024/06/stable-channel-update-for-chromeos.html