Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

May 2, 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

- Pro-Russia Hacktivists Attacking Vital Tech In Water And Other Sectors, Agencies Say
- Finnish Hacker Gets Prison for Accessing Thousands of Psychotherapy Records and Demanding Ransoms
- Millions of Malicious 'Imageless' Containers Planted on Docker Hub Over 5 Years
- Thousands of Qlik Sense Servers Open to Cactus Ransomware
- Vulnerabilities In Employee Management System Could Lead To Remote Code Execution, Login Credential Theft
- Deepfakes and AI-Driven Disinformation Threaten Polls
- Ransom Payments Surge By 500% To An Average Of $2M

Emerging Threats & Vulnerabilities

- 'Cuttlefish' Zero-Click Malware Steals Private Cloud Data
- New Latrodectus Malware Attacks Use Microsoft, Cloudflare Themes
- New "Goldoon" Botnet Targets D-Link Routers With Decade-Old Flaw
- ZLoader Malware Evolves with Anti-Analysis Trick from Zeus Banking Trojan
- Wpeeper Android Trojan Uses Compromised WordPress Sites to Shield Command-and-Control Server

Attacks, Breaches, & Leaks

- Panda Restaurant Group Disclosed A Data Breach
- Play Ransomware Victim: Axip Energy Services
- School Officials: Cyberattack Causes Internet, Phone Outage At Mineola Public Schools
- Dropbox Discloses Breach of Digital Signature Service Affecting All Users
- French Hospital CHC-SV Refuses To Pay Lockbit Extortion Demand

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

Pro-Russia Hacktivists Attacking Vital Tech In Water And Other Sectors, Agencies Say
Cyber Scoop, 5/1/2024

Pro-Russia hacktivists are compromising technology that keeps facilities safe and operational in the water, wastewater, energy, dam, food and agriculture sectors, federal and international agencies said in an advisory released Wednesday. The hacks exploited common weaknesses in cyber defenses, the agencies said, and in some cases the attacks pose physical threats. The advisory, focused on hacktivist activity in those sectors in North America and Europe, provides guidance on defending operational technology (OT) devices and industrial control systems (ICS), which are involved in the maintenance, monitoring or controlling of industrial processes.
https://cyberscoop.com/pro-russia-hacktivists-attacking-vital-tech-in-water-and-other-sectors-agencies-say

Finnish Hacker Gets Prison for Accessing Thousands of Psychotherapy Records and Demanding Ransoms
SecurityWeek, 4/30/2024

A Finnish court on Tuesday sentenced a 26-year-old man to six years and three months in prison for hacking thousands of patient records at a private psychotherapy center and seeking ransom from some patients over the sensitive data. The case has caused outrage in the Nordic nation, with a record number of people — about 24,000 — filing criminal complaints with police. In February 2023, French police arrested well-known Finnish hacker Aleksanteri Kivimäki, who was living under a false identity near Paris. He was deported to Finland. His trial ended last month. https://www.securityweek.com/finnish-hacker-gets-prison-for-accessing-thousands-of-psychotherapy-records-and-demanding-ransoms/

Millions of Malicious 'Imageless' Containers Planted on Docker Hub Over 5 Years
The Hacker News, 4/30/2024

Cybersecurity researchers have discovered multiple campaigns targeting Docker Hub by planting millions of malicious "imageless" containers over the past five years, once again underscoring how open-source registries could pave the way for supply chain attacks. "Over four million of the repositories in Docker Hub are imageless and have no content except for the repository documentation," JFrog security researcher Andrey Polkovnichenko said in a report shared with The Hacker News. What's more, the documentation has no connection whatsoever to the container. Instead, it's a web page that's designed to lure users into visiting phishing or malware-hosting websites.
https://thehackernews.com/2024/04/millions-of-malicious-imageless.html

Thousands of Qlik Sense Servers Open to Cactus Ransomware
Dark Reading, 4/26/2024

Nearly five months after security researchers warned of the Cactus ransomware group leveraging a set of three vulnerabilities in Qlik Sense data analytics and business intelligence (BI) platform, many organizations remain dangerously vulnerable to the threat. Qlik disclosed the vulnerabilities in August and September. The company's August disclosure involved two bugs in multiple versions of Qlik Sense Enterprise for Windows tracked as CVE-2023-41266 and CVE-2023-41265. The vulnerabilities, when chained, give a remote, unauthenticated attacker a way to execute arbitrary code on affected systems.
https://www.darkreading.com/cyber-risk/more-than-3-000-qlik-sense-servers-vuln-to-cactus-ransomware-attacks

Vulnerabilities In Employee Management System Could Lead To Remote Code Execution, Login Credential Theft
Cisco Talos Blog, 5/1/2024

Cisco Talos' Vulnerability Research team has disclosed more than a dozen vulnerabilities over the past three weeks, five in a device that allows employees to check in and out of their shifts, and another that exists in an open-source library used in medical device imaging files. The Peplink Smart Reader contains several vulnerabilities, including one issue that could allow an adversary to obtain the administrator's login credentials and the MD5-hashed version of their password. Talos also recently helped to responsibly disclose and patch other vulnerabilities in the Foxit PDF Reader and two open-source libraries that support the processing and handling of DICOM files.
https://blog.talosintelligence.com/vulnerability-roundup-may-1-2024/

Deepfakes and AI-Driven Disinformation Threaten Polls
Trend Micro, 5/2/2024

I've participated in many elections over the years, both pre-Internet and post-Internet, and the last few elections have seen massive shifts in how citizens get their information and news. With 2024 having many elections occurring around the world, and the US looking at a Presidential election in November, we're already seeing some concerning aspects of what is to come. In my opinion, misinformation/disinformation campaigns are the most significant challenges we will have as citizens trying to figure out what news is real or fake. The technological advances over the past few years have allowed anyone worldwide to post information on the Internet about any topic they want.
https://www.trendmicro.com/en_us/research/24/e/poll-security.html

Ransom Payments Surge by 500% to an Average of $2M
InfoSecurity Magazine, 4/30/2024

Average ransom payments surged by 500% in the past year to reach $2m per payment, according to Sophos' The State of Ransomware 2024 report. This compares to an average payment of $400,000 calculated by Sophos in its 2023 study, demonstrating that ransomware operators are seeking increasingly large payoffs from victims. Nearly two thirds (63%) of ransom demands made in the past year were $1m or more, with 30% of demands demanding over $5m. This is despite a reduction in the

rate of organizations being hit by ransomware in the past year, at 59%, which compares to 66% in Sophos' State of Ransomware 2023 report. https://www.infosecurity-magazine.com/news/ransom-payments-surge-500/

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***'Cuttlefish' Zero-Click Malware Steals Private Cloud Data*** The newly discovered malware, which has so far mainly targeted Turkish telcos and has links to HiatusRat, infects routers and performs DNS and HTTP hijacking attacks on connections to private IP addresses. https://www.darkreading.com/cloud-security/cuttlefish-zero-click-malware-steals-private-cloud-data
- ***New Latrodectus Malware Attacks Use Microsoft, Cloudflare Themes -*** Latrodectus malware is now being distributed in phishing campaigns using Microsoft Azure and Cloudflare lures to appear legitimate while making it harder for email security platforms to detect the emails as malicious. https://www.bleepingcomputer.com/news/security/new-latrodectus-malware-attacks-use-microsoft-cloudflare-themes/
- ***New "Goldoon" Botnet Targets D-Link Routers With Decade-Old Flaw*** - A never-before-seen botnet called Goldoon has been observed targeting D-Link routers with a nearly decade-old critical security flaw with the goal of using the compromised devices for further attacks. https://thehackernews.com/2024/05/new-goldoon-botnet-targets-d-link.html
- ***ZLoader Malware Adopts Anti-Analysis Techniques from Zeus Trojan*** - The ZLoader malware has evolved, incorporating anti-analysis tricks from the infamous Zeus banking trojan. This development makes ZLoader more elusive and dangerous, enhancing its ability to steal financial data without detection. https://thehackernews.com/2024/05/zloader-malware-evolves-with-anti.html
- ***Wpeeper Trojan Uses WordPress Sites for Stealth*** - The Wpeeper Android trojan exploits compromised WordPress sites to mask its command-and-control server. This tactic increases its stealth and complicates efforts to track and mitigate the malware. https://www.securityweek.com/wpeeper-android-trojan-uses-compromised-wordpress-sites-to-shield-command-and-control-server/

ATTACKS, BREACHES & LEAKS

- ***Panda Restaurant Group Reports Data Breach*** – Panda Restaurant Group has disclosed a data breach affecting an undisclosed number of customers. Sensitive personal information was compromised, prompting urgent calls for affected individuals to monitor for fraudulent activity. https://securityaffairs.com/162633/data-breach/panda-restaurant-group-data-breach.html

- ***Axip Energy Services Hit by Play Ransomware*** - Axip Energy Services has fallen victim to Play ransomware, leading to significant data encryption and operational disruptions. This incident is part of a larger pattern of ransomware attacks targeting energy sector companies. https://www.redpacketsecurity.com/play-ransomware-victim-axip-energy-services/
- ***Mineola Public Schools Suffer Cyberattack*** – A cyberattack on Mineola Public Schools resulted in a complete outage of internet and phone services, affecting daily operations and highlighting vulnerabilities in school IT systems. https://longisland.news12.com/school-officials-cyberattack-causes-internet-phone-outage-at-mineola-public-schools
- ***Dropbox Breach Affects Digital Signature Service*** - Cloud storage services provider Dropbox on Wednesday disclosed that Dropbox Sign (formerly HelloSign) was breached by unidentified threat actors, who accessed emails, usernames, and general account settings associated with all users of the digital signature product. https://thehackernews.com/2024/05/dropbox-discloses-breach-of-digital.html
- ***French Hospital CHC-SV Defies LockBit Ransom Demand*** - The French hospital CHC-SV has refused to pay a ransom demand by the LockBit cybercriminal group, despite threats. The hospital is exploring other recovery options and reinforcing its cybersecurity defenses against future attacks. https://www.bleepingcomputer.com/news/security/french-hospital-chc-sv-refuses-to-pay-lockbit-extortion-demand/

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT Alerts and Advisories

1. CyberPower - https://www.cisa.gov/news-events/ics-advisories/icsa-24-123-01
2. Delta Electronics - https://www.cisa.gov/news-events/ics-advisories/icsa-24-123-02
3. Chirp Systems - https://www.cisa.gov/news-events/ics-advisories/icsa-24-067-01

SUSE Security Updates

1. cosign - https://www.suse.com/support/update/announcement/2024/suse-su-20241486-1
2. aaa_base - https://www.suse.com/support/update/announcement/2024/suse-ru-20241487-1
3. chrony - https://www.suse.com/support/update/announcement/2024/suse-ru-20241488-1

Fedora Security Advisories

1. et - https://lwn.net/Articles/972176/
2. python-openapi-core - https://lwn.net/Articles/972181/
3. tpm2-tools - https://lwn.net/Articles/972183/

4. python-aiohttp - https://lwn.net/Articles/972180/
5. thunderbird - https://lwn.net/Articles/972182/
6. php-tcpdf - https://lwn.net/Articles/972177/

Debian Security Advisories

1. chromium - https://lists.debian.org/debian-security-announce/2024/msg00085.html

Check Point Security Advisories

1. TrendNet TEW-820AP - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1676.html
2. VMware Spring Framework - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2022-1731.html
3. TRENDnet TEW-815DAP - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0219.html
4. NETGEAR Orbi RBR750 - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1678.html

Red Hat Security Advisories

1. OpenShift Container Platform
    a. https://access.redhat.com/errata/RHSA-2024:2049
    b. https://access.redhat.com/errata/RHSA-2024:2054
    c. https://access.redhat.com/errata/RHSA-2024:2047
    d. https://access.redhat.com/errata/RHSA-2024:2071
    e. https://access.redhat.com/errata/RHSA-2024:2068
2. Libxml2 - https://access.redhat.com/errata/RHSA-2024:2679
3. Kernal - https://access.redhat.com/errata/RHSA-2024:2674

Ubuntu Security Notices

1. Firefox - https://ubuntu.com/security/notices/USN-6747-2
2. GNU C Library - https://ubuntu.com/security/notices/USN-6762-1
3. PHP - https://ubuntu.com/security/notices/USN-6757-2

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

If you have any questions about this document please contact the ISAC at 866-ST-ISAC1 (866.784.7221) or email st-isac@surfacetransportationisac.org