Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

March 26, 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

- U.S. and UK Accuse China of Cyber Operations Targeting Domestic Politics
- Idaho Man Pleads Guilty to Hacking Computers of the City of Newnan and a Griffin Medical Clinic
- Saflok Lock Vulnerability Can Be Exploited to Open Millions of Doors
- Microsoft Warns of New Tax Returns Phishing Scams Targeting You
- After LockBit, ALPHV Takedowns, RaaS Startups Go on a Recruiting Drive
- Fake Data Breaches: Countering the Damage
- Study Uncovers 27% Spike in Ransomware; 8% Yield to Demands

Emerging Threats & Vulnerabilities

- AndroxGh0st Malware Targets Laravel Apps to Steal Cloud Credentials
- India's Android Users Hit by Malware-as-a-Service Campaign
- Netgear Wireless Router Open to Code Execution After Buffer Overflow Vulnerability
- Atlassian Patches Critical Vulnerability in Bamboo Data Center and Server
- Evasive SIGN1 Malware Campaign Infects 39,000 WordPress Sites

Attacks, Breaches, & Leaks

- Ransomware Attack in Colorado Exposed Personal Information, Say Officials
- 8 Base Ransomware Victim: APS – Automotive Parts Solutions
- City of St. Cloud Responds to Ransomware Cyberattack
- Ransomware Group Takes Credit for Attack on Boat Dealer MarineMax
- 'IntelBroker' Claims Access to Database Belonging to England and Wales Cricket Board (ECB)

EXECUTIVE NEWS

U.S. and UK Accuse China of Cyber Operations Targeting Domestic Politics
CyberScoop, 3/25/2024

The U.S. government on Monday accused seven Chinese nationals and a company based in Wuhan of orchestrating a wide-ranging hacking operation targeting political targets in the United States, in what is Washington's latest attempt to curb what officials describe as increasingly aggressive cyber operations carried out by Beijing. In an indictment unsealed in the Eastern District of New York, federal prosecutors allege that the group of seven Chinese nationals conspired in a sprawling operation to breach personal devices belonging to U.S. officials, dissidents based in the United States and companies. "The Justice Department will not tolerate efforts by the Chinese government to intimidate Americans who serve the public, silence the dissidents who are protected by American laws, or steal from American businesses," Attorney General Merrick B. Garland said in a statement.
https://cyberscoop.com/china-indictments-apt31-surveillance/

Idaho Man Pleads Guilty to Hacking Computers of the City of Newnan and a Griffin Medical Clinic
U.S. Attorney's Office, Northern District of Georgia, 3/19/2024

Robert Purbeck, also known as "Lifelock," and "Studmaster," who hacked into the computer servers of the City of Newnan and a Griffin medical clinic, and then targeted at least 17 other victims across the United States – in the process stealing personal information of more than 132,000 individuals – has pleaded guilty today to federal charges of computer fraud and abuse. "Purbeck breached computer systems in our district and across the country, stole vast amounts of personal information, and aggravated his crimes by weaponizing sensitive data in an egregious attempt to extort his victims," said U.S. Attorney Ryan K. Buchanan. "Cyber-attacks on health care facilities and local governments pose a grave risk to the security of personal information. Our office is committed to tirelessly coordinating with our law enforcement partners to help safeguard the sensitive information of citizens by combatting cybercrime threats from within and outside this district…" According to U.S. Attorney Buchanan, the charges, and other information presented in court: in June 2017, Purbeck purchased access to the computer server of a Griffin, Georgia medical clinic on a darknet marketplace.
https://www.justice.gov/usao-ndga/pr/idaho-man-pleads-guilty-hacking-computers-city-newnan-and-griffin-medical-clinic

Saflok Lock Vulnerability Can Be Exploited to Open Millions of Doors
Security Week, 3/22/2024

A security vulnerability in Dormakaba's Saflok electronic locks can be exploited to forge keycards and open doors, security researchers warn. The issue, named Unsaflok, impacts more than three million locks commonly used in hotels and multi-family housing environments. A total of more than 13,000

locations across 131 countries are likely affected. Vulnerable lock models include Saflok MT and the Quantum, RT, Saffire, and Confidant series devices, which are used in combination with the System 6000, Ambiance, and Community management software. According to the security researchers who identified and reported the flaw in September 2022, an attacker could use a keycard from a property where the vulnerable locks are used to forge a keycard and unlock any door on that property. https://www.securityweek.com/saflok-lock-vulnerability-can-be-exploited-to-open-millions-of-doors/

Microsoft Warns of New Tax Returns Phishing Scams Targeting You
Hackread, 3/21/2024

Taxpayers beware! Phishing scams are on the rise again as tax season heats up. Microsoft Threat Intelligence has issued warnings about new and innovative tactics cybercriminals are using to steal your personal information and financial data. These scams don't discriminate, but they do target specific groups more heavily. New taxpayers, recent immigrants with green cards, small business owners who file themselves, and older adults are all prime targets because they might be less familiar with tax procedures. It is also worth noting that these threat actors are getting more sophisticated too. They're impersonating trusted sources like employers, tax agencies, and even payment processors. They might send emails with blurry or incomplete tax documents to create a sense of urgency and trick you into clicking on a malicious attachment. https://www.hackread.com/microsoft-tax-returns-phishing-malware-alert/

After LockBit, ALPHV Takedowns, RaaS Startups Go on a Recruiting Drive
Dark Reading, 3/20/2024

High-profile takedowns of brand-name ransomware operations are starting to have a real impact, sowing discord among hackers and causing major shifts in the cyber underground. The US and European Union governments have ramped up efforts to disrupt ransomware-as-a-service (RaaS) operations in recent months, most notably with headline-grabbing coordinated actions against the infamous LockBit and ALPHV/BlackCat groups. Police have identified ringleaders, seized malicious infrastructure and data — including information about affiliates — and even trolled adversaries with messages posted to their leak sites. Though well-intentioned, these missions tend to receive criticism when, inevitably, remnants of such large, diffuse groups pop up days or weeks after their reported demise. After all, if the threat actors aren't being eradicated, what's the point?
https://www.darkreading.com/threat-intelligence/after-lockbit-alphv-takedowns-raas-recruiting-drive

Fake Data Breaches: Countering the Damage
Help Net Security, 3/21/2024

Amid the constant drumbeat of successful cyberattacks, some fake data breaches have also cropped up to make sensational headlines. Unfortunately, even fake data breaches can have real repercussions. Earlier this year, a hacker on a criminal forum claimed to have stolen data on some 50 million Europcar

customers. After investigation, the car rental company determined that the data claimed to have been stolen was completely bogus. In February 2024, someone created a fake news story claiming a major data breach at the Maine Attorney General's office and tricked the Attorney General's office into posting it on their website. Epic Games, maker of Fortnite was a victim of a fake data breach by a cybercrime group that claimed without evidence it had absconded source code and sensitive user data. Such fabricated attacks create panic and damage business reputations.
https://www.helpnetsecurity.com/2024/03/21/fake-data-breaches/

Study Uncovers 27% Spike in Ransomware; 8% Yield to Demands
Infosecurity Magazine, 3/20/2024

New data has unveiled a 27% rise in ransomware attacks in 2023, with 8% of affected organizations resorting to paying ransoms. The figures, extracted from the 2024 Thales Data Threat Report, also suggest that less than half of organizations have established formal ransomware response plans. In addition to the surge in ransomware attacks, the report identifies malware as the fastest-growing threat, with 41% of enterprises reporting incidents in the past year. Phishing and ransomware attacks targeting cloud assets such as SaaS applications and cloud-based storage are also on the rise, posing significant challenges to organizations' data security efforts. Moreover, human error continues to be a leading cause of data breaches for the second consecutive year, highlighting the importance of employee training and awareness in maintaining data security protocols.
https://www.infosecurity-magazine.com/news/27-spike-ransomware-8-yield/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***AndroxGh0st Malware Targets Laravel Apps to Steal Cloud Credentials*** – Cybersecurity researchers have shed light on a tool referred to as AndroxGh0st that's used to target Laravel applications and steal sensitive data. "It works by scanning and taking out important information from .env files, revealing login details linked to AWS and Twilio," Juniper Threat Labs researcher Kashinath T Pattan said. https://thehackernews.com/2024/03/androxgh0st-malware-targets-laravel.html
- ***India's Android Users Hit by Malware-as-a-Service Campaign*** – A malware campaign offering malware-as-a-service (MaaS) is targeting Android users based in India. According to Broadcom, the campaign distributes malicious APK packages and seeks out banking information, SMS messages, and other sensitive information from a victim's device. https://www.darkreading.com/cyberattacks-data-breaches/hackers-target-android-users-in-india-through-maas-campaign
- ***Netgear wireless router open to code execution after buffer overflow vulnerability*** - Cisco Talos' Vulnerability Research team recently disclosed three vulnerabilities across a range of products, including one that could lead to remote code execution in a popular Netgear wireless router designed for home networks. There is also a newly disclosed vulnerability in a graphics driver for some NVIDIA GPUs that could lead to a memory leak. https://blog.talosintelligence.com/vulnerability-roundup-march-20-2024/
- ***Atlassian Patches Critical Vulnerability in Bamboo Data Center and Server*** – Atlassian on Tuesday announced patches for two dozen vulnerabilities in Bamboo, Bitbucket, Confluence, and Jira products, including a critical-severity bug that could be exploited without user interaction. Tracked as CVE-2024-1597 (CVSS score of 10) and described as an SQL injection issue, the critical-severity flaw impacts the org.postgresql:postgresql third-party dependency of Bamboo Data Center and Server. https://www.securityweek.com/atlassian-patches-critical-vulnerability-in-bamboo-data-center-and-server/
- ***Evasive Sign1 malware campaign infects 39,000 WordPress sites*** - A previously unknown malware campaign called Sign1 has infected over 39,000 websites over the past six months, causing visitors to see unwanted redirects and popup ads. https://www.bleepingcomputer.com/news/security/evasive-sign1-malware-campaign-infects-39-000-wordpress-sites/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Ransomware attack in Colorado exposed personal information, say officials*** – The Office of the Colorado State Public Defender on Friday announced that some personal client data was exposed during a ransomware attack last month, when officials shut down the office's computer network after becoming aware of malware-encrypted data on system, CBS reported. https://statescoop.com/colorado-ransomware-personal-data-february-cyberattack/
- ***8 Base Ransomware Victim: APS – Automotive Parts Solutions*** – Automotive Parts Solutions, Inc. located in the Rockville – St. Cloud area of Minnesota is a supplier of used auto parts to insurance companies, collision centers and auto repair facilities throughout Minnesota, North Dakota, South Dakota, Wisconsin, and Iowa. https://www.redpacketsecurity.com/8base-ransomware-victim-aps-automotive-parts-solutions-9/
- ***Ransomware Group Takes Credit for Attack on Boat Dealer MarineMax*** - The Rhysida ransomware group has taken credit for the recent cyberattack on boat dealer MarineMax and is offering to sell data allegedly stolen from the company for a significant amount of money. MarineMax is one of the world's largest retailers of recreational boats and yachts. The company has over 125 locations worldwide and nearly 4,000 employees, and it reported a revenue of more than $500 million in the first fiscal quarter of 2024. https://www.securityweek.com/ransomware-group-takes-credit-for-attack-on-boat-dealer-marinemax/
- ***CITY OF ST. CLOUD RESPONDS TO RANSOMWARE CYBERATTACK*** - Early this morning, the City of St. Cloud reported a cybersecurity incident involving a ransomware attack targeting its systems. Officials have swiftly initiated a coordinated response, engaging with both state and local agencies to mitigate the impact of the attack and restore affected services promptly. https://www.positivelyosceola.com/city-of-st-cloud-responds-to-ransomware-cyberattack/
- ***'IntelBroker' Claims Access to Database Belonging to England and Wales Cricket Board (ECB)*** - A cybercriminal going by the name 'IntelBroker' has asserted responsibility for an alleged data breach targeting the European Central Bank (ECB). The purported ECB data breach involved the sale of a database on the dark web forum BreachForums, spanning from 2014 to 2021. The database reportedly contained email addresses, hashed passwords, backup passwords, and tokens. However, the accuracy of these claims has not been confirmed. https://thecyberexpress.com/alleged-ecb-data-breach-claimed-by-intelbroker/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. Kernel –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20240995-1/
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20240991-1/
2. krb5 - https://www.suse.com/support/update/announcement/2024/suse-su-20240997-1/

Fedora Security Advisories

1. Webkitgtk - https://lwn.net/Articles/966666/

Debian Security Advisories

1. zfs-linux - https://lists.debian.org/debian-lts-announce/2024/03/msg00019.html
2. imagemagick - https://lists.debian.org/debian-lts-announce/2024/03/msg00020.html
3. pillow - https://lists.debian.org/debian-lts-announce/2024/03/msg00021.html
4. thunderbird - https://lists.debian.org/debian-lts-announce/2024/03/msg00022.html

Check Point Security Advisories

1. Microsoft SharePoint - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2017-1825.html
2. AirTies 5444 Firmware - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2018-2714.html
3. Fortinet –
    a. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2023-1621.html
    b. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0133.html
4. WordPress DWBooster Appointment Hour Booking Plugin - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2019-3165.html
5. Joomla! - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2015-1599.html
6. CirCarLife Scada - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2018-2729.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Red Hat Security Advisories

1. Dnsmasq - https://access.redhat.com/errata/RHSA-2024:1522
2. python-twisted - https://access.redhat.com/errata/RHSA-2024:1516
3. squid - https://access.redhat.com/errata/RHSA-2024:1515
4. libreoffice - https://access.redhat.com/errata/RHSA-2024:1514

Ubuntu Security Notices

1. Thunderbird - https://ubuntu.com/security/notices/USN-6717-1
2. Kernel –
    a. https://ubuntu.com/security/notices/USN-6707-3
    b. https://ubuntu.com/security/notices/USN-6704-3
    c. https://ubuntu.com/security/notices/USN-6701-3
    d. https://ubuntu.com/security/notices/USN-6716-1
3. Debian Goodies - https://ubuntu.com/security/notices/USN-6714-1
4. CRM shell - https://ubuntu.com/security/notices/USN-6711-1
5. PAM - https://ubuntu.com/security/notices/USN-6588-2

Other

1. Google Chrome –
    a. https://chromereleases.googleblog.com/2024/03/chrome-dev-for-desktop-update_15.html
    b. https://chromereleases.googleblog.com/2024/03/chrome-dev-for-android-update_14.html
    c. https://chromereleases.googleblog.com/2024/03/chrome-stable-for-ios-update.html
    d. https://chromereleases.googleblog.com/2024/03/early-stable-update-for-desktop.html
    e. https://chromereleases.googleblog.com/2024/03/chrome-beta-for-desktop-update_13.html
    f. https://chromereleases.googleblog.com/2024/03/chrome-beta-for-android-update_13.html