Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

May 10, 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. Releases International Cyberspace Strategy
- BTC-e Operator Pleads Guilty to Money Laundering Conspiracy
- Supply Chain Breaches Up 68% Year Over Year, According to DBIR
- Selfie Spoofing Becomes Popular Identity Document Fraud Technique
- RSAC: Law Enforcement Takedowns Force Ransomware Affiliates to Diversify
- Exploits And Vulnerabilities In Q1 2024
- Confronting Quantum Computers' Cryptanalysis Concerns

Emerging Threats & Vulnerabilities

- Attackers May Be Using TunnelVision To Snoop On Users' VPN Traffic (CVE-2024-3661)
- New BIG-IP Next Central Manager Bugs Allow Device Takeover
- LLMjacking: Stolen Cloud Credentials Used in New AI Attack
- 'The Mask' Espionage Group Resurfaces After 10-Year Hiatus
- Citrix Warns Customers To Update Putty Version Installed On Their Xencenter System Manually

Attacks, Breaches, & Leaks

- Dell Discloses Data Breach Impacting Millions Of Customers
- Poland says Russian military hackers target its govt networks
- 500,000 Impacted by Ohio Lottery Ransomware Attack
- IntelBroker Hacker Leaks Alleged HSBC & Barclays Bank Data
- LockBit Claims Wichita as Its Victim 2 Days After Ransomware Attack

EXECUTIVE NEWS

U.S. Releases International Cyberspace Strategy
Security Week, 5/7/2024

The US Department of State on Monday announced its international cyberspace strategy, aimed at fostering collaboration for a more secure, inclusive, safe, and equitable world. Developed in collaboration with other federal agencies, the strategy revolves around the idea of digital solidarity, calling rights-respecting users of digital technologies to work together to become more secure, resilient, and prosperous. The International Cyberspace and Digital Policy Strategy provides guidance on international engagement in technology diplomacy and advancing the US's security and cybersecurity strategies, while encouraging partners to work together on shared goals, supporting each other, and on building capacity. "The concept of digital solidarity rests on efforts to build digital and cyber capacity so that partners are not only better able to build a defensible and resilient digital ecosystem over the long term but are also able to respond and recover quickly when incidents happen and to hold criminal and malign actors accountable," the State Department said.
https://www.securityweek.com/us-releases-international-cyberspace-strategy/

BTC-e Operator Pleads Guilty to Money Laundering Conspiracy
Department of Justice, 5/3/2024

A Russian national pleaded guilty today to conspiracy to commit money laundering related to his role in operating the cryptocurrency exchange BTC-e from 2011 to 2017. According to court documents, Alexander Vinnik, 44, was one of the operators of BTC-e, which was one of the world's largest virtual currency exchanges. From its inception in or around 2011 until it was shut down by law enforcement in or around July 2017 contemporaneous with Vinnik's arrest, BTC-e processed over $9 billion-worth of transactions and served over one million users worldwide, including numerous customers in the United States. "Today's result shows how the Justice Department, working with international partners, reaches across the globe to combat cryptocrime," said Deputy Attorney General Lisa Monaco. "This guilty plea reflects the Department's ongoing commitment to use all tools to fight money laundering, police crypto markets, and recover restitution for victims."
https://www.justice.gov/opa/pr/btc-e-operator-pleads-guilty-money-laundering-conspiracy

Supply Chain Breaches Up 68% Year Over Year, According to DBIR
Dark Reading, 5/6/2024

Breaches resulting from a third party were up 68% last year, primarily due to software vulnerabilities exploited in ransomware and extortion attacks. Supply chain breaches have been on the rise for some time now. According to Verizon's latest Data Breach Investigations Report (DBIR), that rise has been extra steep in recent months. Some 15% of all breaches in 2023 involved a third party, a marked

increase from 9% in 2022. Those figures have as much to do with accounting as attacking, though. In this year's DBIR, Verizon Business expanded its definition of "supply chain breach" to include not just compromises through vendors (e.g., Target in 2013), data custodians (MOVEit), and software updates (SolarWinds), but also vulnerabilities in third-party software.
https://www.darkreading.com/cyber-risk/supply-chain-breaches-up-68-yoy-according-to-dbir

Selfie Spoofing Becomes Popular Identity Document Fraud Technique
Help Net Security, 5/10/2024

Document image-of-image was the most prevalent identity (ID) document fraud technique in 2023, occurring in 63% of all IDs that were rejected, according to Socure. Document image-of-image occurs when the user takes a photograph or uses a screenshot image of an ID, rather than providing a live capture of the document. Document headshot tampering takes place when a user purposefully manipulates facial imagery. And, selfie spoofing entails taking a picture of an image on a computer screen, printed on a piece of paper or even an actual headshot on a different document – often carried out to steal identities or fraudulently access systems. The report assesses document verification-related account openings across a variety of industries including online gaming, marketplaces, lending, and credit cards. https://www.helpnetsecurity.com/2024/05/10/identity-document-selfie-spoofing/

RSAC: Law Enforcement Takedowns Force Ransomware Affiliates to Diversify
Infosecurity Magazine, 5/6/2024

The recent wave of law enforcement operations against ransomware gangs led to short-term decreased ransomware payments and activities, forcing ransomware affiliates to diversify. This is one of the findings of a new report by dark web research firm Chainalysis, published during the RSA Conference on May 6. In the report, Chainalysis recorded evidence of a decrease in ransomware operations' profitability following recent law enforcement takedowns against ransomware groups, such as QakBot, ALPHV/BlackCat and LockBit. However, it also found that the persistence of ransomware affiliates challenges the lasting effectiveness of these measures.
https://www.infosecurity-magazine.com/news/law-enforcement-takedowns/

Exploits and Vulnerabilities in Q1 2024
Secure List, 5/7/2024

…In this report, we present a series of insightful statistical and analytical snapshots relating to the trends in the emergence of new vulnerabilities and exploits, as well as the most prevalent vulnerabilities being used by attackers. Additionally, we take a close look at several noteworthy vulnerabilities discovered in Q1 2024… Although vendors often fail to register vulnerabilities, and the CVE list cannot be considered exhaustive, it does allow us to track certain trends. We analyzed data on registered software vulnerabilities and compared their quantities over the past five years… Firstly, the growing popularity of bug bounty platforms and vulnerability discovery competitions have provided a major impetus to

research in the field. As a result, vulnerability discoveries have been on the rise. This also leads to more vendors registering the discovered vulnerabilities, resulting in a growing number of CVEs.
https://securelist.com/vulnerability-report-q1-2024/112554/

Confronting Quantum Computers' Cryptanalysis Concerns
Beta News, 5/7/2024

The race to successfully build quantum computers is on. With the potential to solve all manner of problems for humanity, players across the globe -- from tech companies to academic institutions to governments -- have been busy investing significant resources into quantum computing initiatives for some years now. But what are they exactly? A traditional (digital) computer processes zeros and ones, so called bits. These, to a first order approximation, are represented as on/off electrical signals. Quantum computers, on the other hand, leverage quantum mechanics to process information using quantum-bits or qubits, which can represent multiple states simultaneously. And it's this capability that enables quantum computers to tackle computational tasks that are currently out of the question for classical computers - think factoring large numbers, simulating quantum systems, optimizing complex systems or solving certain types of optimization and machine learning problems.
https://betanews.com/2024/05/07/confronting-quantum-computers-cryptanalysis-concerns/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Attackers may be using TunnelVision to snoop on users' VPN traffic (CVE-2024-3661)*** – Researchers have brought to light a new attack method – dubbed TunnelVision and uniquely identified as CVE-2024-3661 – that can be used to intercept and snoop on VPN users' traffic by attackers who are on the same local network. https://www.helpnetsecurity.com/2024/05/08/tunnelvision-cve-2024-3661/
- ***New BIG-IP Next Central Manager bugs allow device takeover*** - F5 has fixed two high-severity BIG-IP Next Central Manager vulnerabilities, which can be exploited to gain admin control and create hidden rogue accounts on any managed assets. Next Central Manager allows administrators to control on-premises or cloud BIG-IP Next instances and services via a unified management user interface. https://www.bleepingcomputer.com/news/security/new-big-ip-next-central-manager-bugs-allow-device-takeover/
- ***LLMjacking: Stolen Cloud Credentials Used in New AI Attack*** – The Sysdig Threat Research Team (TRT) recently observed a new attack that leveraged stolen cloud credentials in order to target ten cloud-hosted large language model (LLM) services, known as LLMjacking. The credentials were obtained from a popular target, a system running a vulnerable version of Laravel (CVE-2021-3129). https://sysdig.com/blog/llmjacking-stolen-cloud-credentials-used-in-new-ai-attack/
- ***'The Mask' Espionage Group Resurfaces After 10-Year Hiatus*** - An advanced persistent threat (APT) group that has been missing in action for more than a decade has suddenly resurfaced in a cyber-espionage campaign targeting organizations in Latin America and Central Africa. The group, called "Careto" or "The Mask", began operations in 2007 and then seemingly wafted into thin air in 2013. https://www.darkreading.com/cyberattacks-data-breaches/-the-mask-espionage-group-resurfaces-after-10-year-hiatus
- ***Citrix Warns Customers To Update Putty Version Installed On Their Xencenter System Manually*** - Versions of XenCenter for Citrix Hypervisor 8.2 CU1 LTSR used PuTTY, a third-party component, for SSH connections to guest VMs. However, PuTTY inclusion was deprecated with XenCenter version 8.2.6, and any versions after 8.2.7 will not include PuTTY. https://securityaffairs.com/162953/security/citrix-manually-update-putty-ssh-client.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Dell Discloses Data Breach Impacting Millions Of Customers*** – IT giant Dell suffered a data breach exposing customers' names and physical addresses, the company notified impacted individuals. The company launched an investigation into the incident that involved a Dell portal, which contains a database with limited types of customer information related to purchases from IT firm. The company downplayed the risk for the impacted individuals given the type of information involved. https://securityaffairs.com/162942/cyber-crime/dell-data-breach-2.html
- ***Poland says Russian military hackers target its govt networks*** - Poland says a state-backed threat group linked to Russia's military intelligence service (GRU) has been targeting Polish government institutions throughout the week. https://www.bleepingcomputer.com/news/security/poland-says-russian-military-hackers-target-its-govt-networks/
- ***500,000 Impacted by Ohio Lottery Ransomware Attack*** – The incident came to light in late December 2023, after the Ohio Lottery announced shutting down some systems in an effort to contain the breach. At around the same time, a seemingly new ransomware group named DragonForce took credit for the attack. https://www.securityweek.com/500000-impacted-by-ohio-lottery-ransomware-attack/
- ***IntelBroker Hacker Leaks Alleged HSBC & Barclays Bank Data*** – The infamous IntelBroker hacker claims to have breached a third-party contractor and stolen sensitive data belonging to two prominent banks in the United Kingdom: HSBC and Barclays. The hacker has already leaked a substantial portion of the alleged compromised information on Breach Forums, a notorious hub for cybercriminal activity, and the data is now circulating on several prominent Russian-language forums, Hackread.com can confirm. https://www.hackread.com/intelbroker-hacker-hsbc-barclays-data-breach/
- ***LockBit Claims Wichita as Its Victim 2 Days After Ransomware Attack*** - LockBit ransomware group says it is responsible for a ransomware attack on the City of Wichita. The attack occurred over the weekend and disrupted the city's networks and services. Much of the area has been affected, including the airport, water service, and public transit. The city was forced to switch to a cash-based system, where applicable, until systems become fully operational again. https://www.darkreading.com/cyberattacks-data-breaches/lockbit-claims-wichita-as-its-victim-two-days-after-ransomware-attack

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. Rockwell Automation –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-130-01
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-107-03
2. Delta Electronics InfraSuite Device Master - https://www.cisa.gov/news-events/ics-advisories/icsa-24-130-03
3. alpitronic Hypercharger EV Charger - https://www.cisa.gov/news-events/ics-advisories/icsa-24-130-02

SUSE Security Updates

1. less - https://www.suse.com/support/update/announcement/2024/suse-su-20241598-1/
2. Kernel –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20241596-1/
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20241582-1/
3. Ghostscript - https://www.suse.com/support/update/announcement/2024/suse-su-20241590-1/

Fedora Security Advisories

1. Pypy –
    a. https://lwn.net/Articles/973184/
    b. https://lwn.net/Articles/973185/
2. Kernel - https://lwn.net/Articles/973183/
3. freerdp2 - https://lwn.net/Articles/973033/

Debian Security Advisories

1. Chromium - https://lists.debian.org/debian-security-announce/2024/msg00092.html
2. Wordpress - https://lists.debian.org/debian-security-announce/2024/msg00093.html
3. dav1d - https://lists.debian.org/debian-security-announce/2024/msg00096.html
4. webkit2gtk - https://lists.debian.org/debian-security-announce/2024/msg00095.html

UBUNTU SECURITY NOTICES

1. Glib - https://ubuntu.com/security/notices/USN-6768-1
2. Fossil - https://ubuntu.com/security/notices/USN-6770-1
3. libspreadsheet-parsexlsx-perl - https://ubuntu.com/security/notices/USN-6769-1

TOOL NEWS & UPDATES

TOOLS & INITIATIVES

- AIDE 0.18.7 - https://packetstormsecurity.com/files/178466/aide-0.18.7.tar.gz
- RansomLord Anti-Ransomware Exploit Tool 3 - https://packetstormsecurity.com/files/178491/RansomLord-3.zip
- Zed Attack Proxy 2.15.0 Cross Platform Package - https://packetstormsecurity.com/files/178523/ZAP_2.15.0_Crossplatform.zip
- I2P 2.5.1 - https://packetstormsecurity.com/files/178524/i2psource_2.5.1.tar.bz2