Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 29, 2023

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.

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) MONTH

Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)

ICT is integral for the daily operations and functionality of U.S. critical infrastructure. If vulnerabilities in the ICT supply chain—composed of hardware, software, and managed services from third-party vendors, suppliers, service providers, and contractors—are exploited, the consequences can affect all users of that technology or service. Protecting your organization's information in a digitally connected world requires understanding not only your organization's immediate supply chain, but also the extended supply chains of third-party vendors, service providers, and customers. Additional information and resources to assist with managing supply chain risks and building an effective SCRM practice are available at: https://www.cisa.gov/information-and-communications-technology-supply-chain-risk-management

Additional Resources:

- ICT Supply Chain Resource Library: https://www.cisa.gov/ict-supply-chain-library
- Internet of Things (IoT) Acquisition Guidance: https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_1.pdf

EXECUTIVE NEWS

Cyber Scam Organization Disrupted Through Seizure of Nearly $9M in Crypto
Department of Justice, 11/21/2023

The Justice Department announced today the seizure of nearly $9 million worth of Tether, a cryptocurrency pegged to the U.S. dollar. These seized funds were traced to cryptocurrency addresses allegedly associated with an organization that exploited over 70 victims through romance scams and cryptocurrency confidence scams, which are widely known as "pig butchering…" According to court

documents, criminal actors worked together to target victims and convince them to make cryptocurrency deposits by fraudulently representing that the victims were making investments with trusted firms and cryptocurrency exchanges. In reality, the purported firms and cryptocurrency exchanges were non-existent trading platforms. Agents and analysts from the U.S. Secret Service (USSS) were able to trace those victim deposits and observed that the funds were quickly laundered through dozens of cryptocurrency addresses and exchanged for several different cryptocurrencies, a money laundering technique often referred to as "chain hopping."
https://www.justice.gov/opa/pr/cyber-scam-organization-disrupted-through-seizure-nearly-9m-crypto

Municipal Water Authority of Aliquippa Hacked by Iranian-Backed Cyber Group
CBS News, 11/26/2023

The Municipal Water Authority of Aliquippa said on Saturday that one of their booster stations had been hacked by an Iranian-backed cyber group. Matthew Mottes, the chairman of the board of directors for the Municipal Water Authority of Aliquippa, confirmed to KDKA-TV that the cyber group, known as Cyber Av3ngers, took control of one of the stations. An alarm went off as soon as the hack had occurred. Mottes added that the station, located on the outskirts of town, monitors and regulates pressure for Raccoon and Potter Townships and stressed that there is no known risk to the drinking water or water supply. The machine that was hacked uses a system called Unitronics, which Mottes says is software or has components that are Israeli-owned. https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/

Secure by Design Alert: How Software Manufacturers Can Shield Web Management Interfaces from Malicious Cyber Activity
Cybersecurity and Infrastructure Security Agency, 11/29/2023

This guidance was created to urge software manufacturers to proactively prevent the exploitation of vulnerabilities in web management interfaces by designing and developing their products using SbD principles: Take Ownership of Customer Security Outcomes. Embrace Radical Transparency and Accountability. By implementing these two principles in their software design process, software manufactures can help their customers avoid exploitation of vulnerabilities in web management interfaces at scale. How Software Manufacturers Can Shield Web Management Interfaces From Malicious Cyber Activity is the first in a new Secure by Design Alert Series that focuses on how vendor decisions can reduce harm at a global scale. https://www.cisa.gov/resources-tools/resources/secure-design-alert-how-software-manufacturers-can-shield-web-management-interfaces-malicious-cyber

Researchers Want More Detail on Industrial Control System Alerts
Cyber Scoop, 11/22/2023

At the beginning of July, Rockwell Automation released a security advisory about a vulnerability in one of its products. Working with the U.S. government, the company said it had become aware that a state-

backed hacking unit had developed the ability to run malicious code on the communication modules of an industrial controller. The company wouldn't identify who had this ability to attack its products and an accompanying advisory from the Cybersecurity and Infrastructure Security Agency said there were no known instances of the vulnerability being exploited in the wild. It's rare that vulnerabilities affecting industrial control systems that are targeted by hackers working on behalf of nation states are discovered before they are exploited. By publicly revealing the vulnerability and urging customers to patch their system, Rockwell may have effectively burned the ability of a foreign intelligence agency to attack U.S. critical infrastructure systems. https://cyberscoop.com/industrial-control-system-alerts/

Atomic Stealer Malware Strikes macOS via Fake Browser Updates
Bleeping Computer, 11/25/2023

The 'ClearFake' fake browser update campaign has expanded to macOS, targeting Apple computers with Atomic Stealer (AMOS) malware. The ClearFake campaign started in July this year to target Windows users with fake Chrome update prompts that appear on breached sites via JavaScript injections. In October 2023, Guardio Labs discovered a significant development for the malicious operation, which leveraged Binance Smart Chain contracts to hide its malicious scripts supporting the infection chain in the blockchain. Via this technique, dubbed "EtherHiding," the operators distributed Windows-targeting payloads, including information-stealing malware like RedLine, Amadey, and Lumma. https://www.bleepingcomputer.com/news/security/atomic-stealer-malware-strikes-macos-via-fake-browser-updates/#google_vignette

Mideast Oil & Gas Facilities Could Face Cyber-Related Energy Disruptions
Dark Reading, 11/22/2023

Middle East oil and gas operators will need to be vigilant about the risk of cyberattacks as the Israel-Gaza conflict continues, security experts warn, or else risk energy supply disruption globally. A recent report by S&P Global Ratings found that the Middle East's gas industry was at greater risk of physical attacks than its oil counterparts, but the threat of cyberattacks affects both industry sectors. There is the potential for the impact of cyberattacks in the region to be felt further afield, according to Paul Laudanski, director of security research at Onapsis. "The repercussions of these digital battles extend far beyond the confines of local geopolitics," Laudanski cautions. "In recent years, we have witnessed the strain on global supply chains and energy systems, prompting governments to fortify their reserves and establish crisis protocols for the world economy." https://www.darkreading.com/ics-ot-security/mideast-oil-gas-facilities-could-face-cyber-related-energy-disruptions

Cybercriminals Turn to Ready-Made Bots for Quick Attacks
Help Net Security, 11/23/2023

Bots and human fraud farms were responsible for billions of attacks in the H1 of 2023 and into Q3, according to Arkose Labs. These attacks comprised 73% of all website and app traffic measured. In other

words, almost three-quarters of traffic to digital properties is malicious. Researchers assessed the attacks across three primary attack vectors: basic bots, intelligent bots, and human fraud farms. Fraudsters use these vectors to launch attack types such as SMS toll fraud, web scraping, card testing, credential stuffing, and more. The analysis found bot attacks overall increased 167% in the H1 of 2023, weighted heavily by a 291% increase in intelligent bots. These smart bots are capable of complex, context-aware interactions. In Q2 2023, there was a 202% increase in bots attempting to take over consumer financial accounts, and a 164% increase in bots attempting to establish fake new bank accounts. This trend continued going into Q3, which experienced a 30% increase over the second quarter in fake new bank accounts. https://www.helpnetsecurity.com/2023/11/23/bot-attacks-h1-2023/

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***UK and South Korea: Hackers use zero-day in supply-chain attack*** – The National Cyber Security Centre (NCSC) and Korea's National Intelligence Service (NIS) warn that the North Korean Lazarus hacking group breaches companies using a zero-day vulnerability in the MagicLine4NX software to conduct supply-chain attacks. MagicLine4NX is a security authentication software developed by the South Korean company Dream Security, used for secure logins in organizations. https://www.bleepingcomputer.com/news/security/uk-and-south-korea-hackers-use-zero-day-in-supply-chain-attack/
- ***ISRAEL-HAMAS WAR SPOTLIGHT: SHAKING THE RUST OFF SYSJOKER*** – Check Point Research is actively tracking the evolution of SysJoker, a previously publicly unattributed multi-platform backdoor, which we asses was utilized by a Hamas-affiliated APT to target Israel. Among the most prominent changes is the shift to Rust language, which indicates the malware code was entirely rewritten, while still maintaining similar functionalities. https://research.checkpoint.com/2023/israel-hamas-war-spotlight-shaking-the-rust-off-sysjoker/
- ***NEW INFECTEDSLURS MIRAI-BASED BOTNET EXPLOITS TWO ZERO-DAYS*** - Akamai discovered a new Mirai-based DDoS botnet, named InfectedSlurs, actively exploiting two zero-day vulnerabilities to infect routers and video recorder (NVR) devices. The researchers discovered the botnet in October 2023, but they believe it has been active since at least 2022. The experts reported the two vulnerabilities to the respective vendors, but they plan to release the fixes in December 2023. https://securityaffairs.com/154607/malware/infectedslurs-botnet.html
- ***Stealthy WailingCrab Malware misuses MQTT Messaging Protocol*** – IBM X-Force researchers have been tracking developments to the WailingCrab malware family, in particular, those relating to its C2 communication mechanisms, which include misusing the Internet-of-Things (IoT) messaging protocol MQTT. WailingCrab, also known as WikiLoader, is a sophisticated, multi-component malware delivered almost exclusively by an initial access broker that X-Force tracks as Hive0133, which overlaps with TA544. https://securityintelligence.com/x-force/wailingcrab-malware-misues-mqtt-messaging-protocol/
- ***Scattered Spider Hops Nimbly From Cloud to On-Prem in Complex Attack*** - The group behind the high-profile MGM cyberattack in September has resurfaced in yet another sophisticated ransomware attack, in which the actor pivoted from a third-party service environment to the target organization's on-premise network in only an hour. The attack by Scattered Spider, an ALPHV/Black Cat ransomware affiliate, sealed the group's position as a formidable adversary for large enterprises with a nimble ability to target the enterprise through their cloud service providers, according to a report by ReliaQuest published on Nov. 22. https://www.darkreading.com/threat-intelligence/scattered-spider-hops-nimbly-from-cloud-to-on-prem-in-complex-attack

ATTACKS, BREACHES & LEAKS

- ***UT Health East Texas on divert status*** – After a potential security incident caused a network outage, UT Health East Texas enters a divert status. According to UT Health East Texas officials, a potential security incident caused a network outage. In a statement to KETK, officials said UT Health East Texas entered a divert status while they work to bring their systems back online. https://www.ketk.com/news/local-news/network-outage-at-ut-health-east-texas-causes-the-hospital-to-enter-divert-status/
- ***Fidelity National Financial ransomware incident impacts real estate closings*** – Fidelity National Financial (FNF) is the nation's largest group of title companies and underwriters in the country. They claim that collectively, they issue more title insurance policies than any other firm in the United States. On Wednesday, while many Americans were getting ready for Thanksgiving, AlphV (BlackCat) threat actors announced that they had attacked FNF. https://www.databreaches.net/fidelity-national-financial-ransomware-incident-impacts-real-estate-closings/
- ***WELLTOK DATA BREACH IMPACTED 8.5 MILLION PATIENTS IN THE U.S.*** – Welltok is a company that specializes in health optimization solutions. It provides a platform that leverages data-driven insights to engage individuals in their health and well-being. The platform aims to personalize and optimize health programs for individuals, employers, health plans, and other organizations. https://securityaffairs.com/154663/data-breach/welltok-data-breach-11m-patients.html
- ***Microsoft: Lazarus hackers breach CyberLink in supply chain attack*** - Microsoft says a North Korean hacking group has breached Taiwanese multimedia software company CyberLink and trojanized one of its installers to push malware in a supply chain attack targeting potential victims worldwide. According to Microsoft Threat Intelligence, activity suspected to be linked with the altered CyberLink installer file surfaced as early as October 20, 2023. https://www.bleepingcomputer.com/news/security/microsoft-lazarus-hackers-breach-cyberlink-in-supply-chain-attack/
- ***Enterprise software provider Tmax leaks 2TB of data*** - A Korean IT company developing and selling enterprise software has leaked over 50 million sensitive records. The 2 TB-strong Kibana dashboard has been exposed for over two years. Cybernews researchers discovered it back in January 2023, noting the set of data was first spotted in June 2021. Our team attributed the dashboard to tmax.co.kr – a website owned by TmaxSoft, one of the Tmax brand companies. https://cybernews.com/security/tmax-data-leak/

SENSITIVE & PROPRIETARY INFROMATION - NOT FOR PUBLIC DISSEMINATION

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

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT ALERTS AND ADVISORIES

1. Delta Electronics InfraSuite Device Master - https://www.cisa.gov/news-events/ics-advisories/icsa-23-331-01
2. Franklin Electric Fueling Systems Colibri - https://www.cisa.gov/news-events/ics-advisories/icsa-23-331-02
3. Mitsubishi Electric GX Works2 - https://www.cisa.gov/news-events/ics-advisories/icsa-23-331-03
4. BD FACSChorus - https://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-331-01

SUSE SECURITY UPDATES

1. selinux-policy –
   a. https://www.suse.com/support/update/announcement/2023/suse-ru-20234605-1/
   b. https://www.suse.com/support/update/announcement/2023/suse-ru-20234604-1/
   c. https://www.suse.com/support/update/announcement/2023/suse-ru-20234603-1/
2. python-apache-libcloud - https://www.suse.com/support/update/announcement/2023/suse-ru-20234606-1/
3. python3-Twisted –
   a. https://www.suse.com/support/update/announcement/2023/suse-su-20234607-1/
   b. https://www.suse.com/support/update/announcement/2023/suse-su-20234608-1/
4. suseconnect-ng –
   a. https://www.suse.com/support/update/announcement/2023/suse-ru-20234601-1/
   b. https://www.suse.com/support/update/announcement/2023/suse-ru-20234602-1/

FEDORA SECURITY ADVISORIES

1. python-geopandas –
   a. https://lwn.net/Articles/953212/
   b. https://lwn.net/Articles/953213/
   c. https://lwn.net/Articles/953214/
2. Libcap - https://lwn.net/Articles/953208/
3. nats-server –
   a. https://lwn.net/Articles/953209/
   b. https://lwn.net/Articles/953210/
4. golang-github-nats-io-streaming-server –

   a. https://lwn.net/Articles/953207/
   b. https://lwn.net/Articles/953206/

5. Openvpn - https://lwn.net/Articles/953211/

Debian Security Advisories

1. Gimp - https://lists.debian.org/debian-lts-announce/2023/11/msg00015.html
2. gnutls28 - https://lists.debian.org/debian-lts-announce/2023/11/msg00016.html
3. firefox-esr - https://lists.debian.org/debian-lts-announce/2023/11/msg00017.html
4. strongswan - https://lists.debian.org/debian-lts-announce/2023/11/msg00018.html
5. symphony - https://lists.debian.org/debian-lts-announce/2023/11/msg00019.html
6. freeimage - https://lists.debian.org/debian-lts-announce/2023/11/msg00020.html

Drupal Security Advisories

1. Xsendfile - https://www.drupal.org/sa-contrib-2023-053

Red Hat Security Advisories

1. postgresql:13 –
   a. https://access.redhat.com/errata/RHSA-2023:7581
   b. https://access.redhat.com/errata/RHSA-2023:7580
   c. https://access.redhat.com/errata/RHSA-2023:7579
2. Squid –
   a. https://access.redhat.com/errata/RHSA-2023:7578
   b. https://access.redhat.com/errata/RHSA-2023:7576
3. Firefox –
   a. https://access.redhat.com/errata/RHSA-2023:7569
   b. https://access.redhat.com/errata/RHSA-2023:7573
   c. https://access.redhat.com/errata/RHSA-2023:7577
4. Thunderbird - https://access.redhat.com/errata/RHSA-2023:7574

Ubuntu Security Notices

1. AFFLIB - https://ubuntu.com/security/notices/USN-6518-1
2. Kernel –
   a. https://ubuntu.com/security/notices/USN-6520-1

   b. https://ubuntu.com/security/notices/USN-6502-3
3. EC2 hibagent –
   a. https://ubuntu.com/security/notices/USN-6519-1
   b. https://ubuntu.com/security/notices/USN-6519-2
4. GIMP - https://ubuntu.com/security/notices/USN-6521-1
5. FreeRDP - https://ubuntu.com/security/notices/USN-6522-1
6. u-boot-nezha - https://ubuntu.com/security/notices/USN-6523-1

OTHER

1. Google Chrome –
   a. https://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html
   b. https://chromereleases.googleblog.com/2023/11/extended-stable-channel-update-for_28.html
   c. https://chromereleases.googleblog.com/2023/11/chrome-for-android-update_0449462503.html
2. Tor Browser 13.5a2 - https://blog.torproject.org/new-alpha-release-tor-browser-135a2/

***** FAIR USE NOTICE*****

This message contains copyrighted material whose use has not been specifically authorized by the copyright owner. The ST-ISAC is making it available to ISAC members who have expressed a prior interest in receiving information to advance their understanding of threat activities in the interest of protecting the national infrastructure of the United States. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.