Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 9, 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

- Senators call for investigation of DOD's comms following Chinese telecom breach
- Maryland Activates Traffic Management Platform To Combat Gridlock
- New NIST Guidance Offers Update on Gauging Cyber Performance
- Cloudflare's Developer Domains Increasingly Abused By Threat Actors
- Pro-Russian Hacktivists Launch Branded Ransomware Operations
- Ransomware Payments Are Now A Critical Business Decision
- Why Simulating Phishing Attacks Is the Best Way to Train Employees

Emerging Threats & Vulnerabilities

- Repeat Offenders Drive Bulk Of Tech Support Scams Via Google Ads
- Spyloan Android Malware On Google Play Installed 8 Million Times
- Corrupted Word Files Fuel Sophisticated Phishing Campaign
- Critical Vulnerability Found in Zabbix Network Monitoring Tool
- Horns&Hooves campaign delivers NetSupport RAT and BurnsRAT

Attacks, Breaches, & Leaks

- Kash Patel, Trump's Pick To Lead Fbi, Has Been Targeted In An Iranian Hack, Sources Say
- Chemonics International Data Breach Impacts 260,000 Individuals
- Researchers Uncover 4-Month Cyberattack on U.S. Firm Linked to Chinese Hackers
- 8Base ransomware group hacked Croatia's Port of Rijeka

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

Senators call for investigation of DOD's comms following Chinese telecom breach
Next Gov, 12/4/2024

A bipartisan pair of senators is calling for the Pentagon's top watchdog to investigate the Department of Defense's "failure to secure its unclassified telephone communications from foreign espionage" following a Chinese state-backed hacking group's penetration into U.S. telecom networks. In a Wednesday letter to DOD Inspector General Robert Storch, Sens. Eric Schmitt, R-Mo., and Ron Wyden, D-Ore., said the extensive spying campaign launched by the group — dubbed Salt Typhoon — underscored the national security concerns of the Pentagon's reliance on unsecured networks. https://www.nextgov.com/cybersecurity/2024/12/senators-call-investigation-dods-comms-following-chinese-telecom-breach/401431/

Maryland Activates Traffic Management Platform To Combat Gridlock
State Scoop, 12/4/2024

The Maryland Department of Transportation on Wednesday announced it's deployed a new traffic management platform that uses artificial intelligence to help combat gridlock, improve traffic flow and enhance public safety at key intersections throughout the state. The system is from NoTraffic, which has locations in Kansas and Israel, and retrofits intersections with traffic signals using AI-powered sensors to reduce congestion in real time by identifying private vehicles, public transit, emergency services and pedestrians. The statewide launch builds off the platform's success in the City of Baltimore, which last October installed the system at five intersections to better manage traffic surges after the Francis Scott Key bridge collapse in March. https://statescoop.com/maryland-notraffic-traffic-management-platform-2024/

New NIST Guidance Offers Update on Gauging Cyber Performance
Government Technology, 12/4/2024

The National Institute of Standards and Technology (NIST) continues to hone the guidance it offers to government organizations around cybersecurity. NIST on Wednesday released an update to its directives for government agencies, which it is calling NIST Special Publication (SP) 800-55. The document, which is organized in two volumes, is designed to help government organizations measure the effectiveness of their cybersecurity efforts. The first volume, known as "Identifying and Selecting Measures," focuses on how to implement a cybersecurity program so that it can be both measured and analyzed "to identify the adequacy of in-place security policies, procedures, and controls," according to the document. It also explains evaluating measures and prioritizing them.
https://www.govtech.com/security/new-nist-guidance-offers-update-on-gauging-cyber-performance

Cloudflare's Developer Domains Increasingly Abused By Threat Actors
Bleeping Computer, 12/3/2024

Cloudflare's 'pages.dev' and 'workers.dev' domains, used for deploying web pages and facilitating serverless computing, are being increasingly abused by cybercriminals for phishing and other malicious activities. According to cybersecurity firm Fortra, the abuse of these domains has risen between 100% and 250% compared to 2023. The researchers believe the use of these domains is aimed at improving the legitimacy and effectiveness of these malicious campaigns, taking advantage of Cloudflare's trusted branding, service reliability, low usage costs, and reverse proxying options that complicate detection. https://www.bleepingcomputer.com/news/security/cloudflares-developer-domains-increasingly-abused-by-threat-actors/

Pro-Russian Hacktivists Launch Branded Ransomware Operations
Infosecurity Magazine, 11/27/2024

A pro-Russian hacktivist group has launched its own ransomware-as-a-service (RaaS) operations to advance its causes. Researchers from SentinelLabs has observed the CyberVolk hacktivist collective advertise its branded ransomware since June, 2024, and has claimed responsibility for multiple ransomware attacks between June and October. The hacktivist group, which originated in India, has also promoted and shared tools with other ransomware families. The analysis highlights the growing blurring of the lines between hacktivism, cybercrime and nation-state activity. https://www.infosecurity-magazine.com/news/russian-hacktivists-branded/

Ransomware Payments Are Now A Critical Business Decision
Help Net Security, 11/28/2024

Despite the efforts of law enforcement agencies to stop and bring to justice those responsible for ransomware attacks, the situation is not improving. While authorities do not recommend making a ransomware payment, some companies are forced to make that choice in order to continue their operations. In this article, we present some important statistics about the ransom demands that companies are facing. 34% of organizations that experience ransomware attacks pay the ransom every time, 21% pay the ransom only some of the time, and 45% never pay the ransom. 83% of respondents who paid the ransom at least once saying they have worked with a ransomware broker. https://www.engineerlive.com/content/digital-rail-solutions-are-more-vital-ever

Why Simulating Phishing Attacks Is the Best Way to Train Employees
Hack Read, 12/1/2024

Despite advancements in cybersecurity tools, human vulnerability remains the weakest link, with phishing among the most dangerous forms of social engineering. The FBI's Internet Crime Complaint Center (IC3) identifies phishing as the most commonly reported type of cybercrime, with around 300,000 incidents in 2023 alone resulting in financial losses exceeding $18.23 million. Even employees are aware of these risks, even if they lag when it comes to actually ensuring the integrity of their data and access credentials. A recent industry survey found that 71% of working adults have admitted to risky behaviour, which can include reusing or sharing a password, clicking on links from unverified sources, or giving credentials to untrustworthy websites or apps. https://hackread.com/why-simulating-phishing-attacks-best-train-employees/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Repeat Offenders Drive Bulk Of Tech Support Scams Via Google Ads -*** Of all the different kinds of malicious search ads we track, those related to customer service are by far the most common. Brands such as PayPal, eBay, Apple or Netflix are among the most coveted ones as they tend to drive a lot of online searches. https://www.malwarebytes.com/blog/scams/2024/12/repeat-offenders-drive-bulk-of-tech-support-scams-via-google-ads
- ***Spyloan Android Malware On Google Play Installed 8 Million Times*** - A new set of 15 SpyLoan Android malware apps with over 8 million installs was discovered on Google Play, targeting primarily users from South America, Southeast Asia, and Africa. https://www.bleepingcomputer.com/news/security/spyloan-android-malware-on-google-play-installed-8-million-times/
- ***Corrupted Word Files Fuel Sophisticated Phishing Campaign –*** A new phishing campaign has been observed corrupting Microsoft Word documents to bypass email security systems and trick users into sharing sensitive information. https://www.infosecurity-magazine.com/news/corrupted-word-files-fuel-phishing/
- ***Critical Vulnerability Found in Zabbix Network Monitoring Tool –*** Zabbix has warned of a critical-severity vulnerability in its open source enterprise networking monitoring solution that could allow attackers to inject arbitrary SQL queries and compromise data or the system. https://www.securityweek.com/critical-vulnerability-found-in-zabbix-network-monitoring-tool/
- ***Horns&Hooves campaign delivers NetSupport RAT and BurnsRAT*** **-** Recent months have seen a surge in mailings with lookalike email attachments in the form of a ZIP archive containing JScript scripts. The script files – disguised as requests and bids from potential customers or partners – bear names such as “Запрос цены и предложения от Индивидуального предпринимателя <ФИО> на август 2024. https://securelist.com/horns-n-hooves-campaign-delivering-netsupport-rat/114740/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Kash Patel, Trump's Pick To Lead Fbi, Has Been Targeted In An Iranian Hack, Sources Say -*** Kash Patel, President-elect Donald Trump's pick to run the FBI, was recently informed by the bureau that he had been targeted as part of an Iranian hack, two sources familiar with the matter told CNN. Hackers are believed to have accessed at least some of Patel's communications, according to one of the sources. https://www.cnn.com/2024/12/03/politics/kash-patel-targeted-iran-hack/index.html
- ***Chemonics International Data Breach Impacts 260,000 Individuals*** - Chemonics International is notifying over 260,000 individuals that their personal information was compromised in a year-old data breach. https://www.securityweek.com/chemonics-international-data-breach-impacts-260000-individuals/
- ***Researchers Uncover 4-Month Cyberattack on U.S. Firm Linked to Chinese Hackers -*** A suspected Chinese threat actor targeted a large U.S. organization earlier this year as part of a four-month-long intrusion. According to Broadcom-owned Symantec, the first evidence of the malicious activity was detected on April 11, 2024 and continued until August. However, the company doesn't rule out the possibility that the intrusion may have occurred earlier. https://thehackernews.com/2024/12/researchers-uncover-4-month-cyberattack.html
- ***8Base ransomware group hacked Croatia's Port of Rijeka*** - The 8Base ransomware group attacked Croatia's Port of Rijeka, stealing sensitive data, including contracts and accounting info. https://securityaffairs.com/171779/cyber-crime/8base-ransomware-croatias-port-of-rijeka.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. go1.22 - https://www.suse.com/support/update/announcement/2024/suse-ru-20244260-1
2. Linux Kernel - https://www.suse.com/support/update/announcement/2024/suse-su-20244268-1

Gentoo Security Advisories

1. R - https://security.gentoo.org/glsa/202412-01
2. Cacti - https://security.gentoo.org/glsa/202412-02
3. Asterisk - https://security.gentoo.org/glsa/202412-03
4. Mozilla Firefox - https://security.gentoo.org/glsa/202412-04
5. Chromium, Google Chrome, Microsoft Edge. Opera - https://security.gentoo.org/glsa/202412-05
6. Mozilla Thunderbird - https://security.gentoo.org/glsa/202412-06
7. OpenJDK - https://security.gentoo.org/glsa/202412-07
8. icinga2 - https://security.gentoo.org/glsa/202412-08
9. Salt - https://security.gentoo.org/glsa/202412-09
10. Dnsmasq - https://security.gentoo.org/glsa/202412-10
11. OATH Toolkit - https://security.gentoo.org/glsa/202412-11
12. PostgreSQL - https://security.gentoo.org/glsa/202412-12
13. Spidermonkey - https://security.gentoo.org/glsa/202412-13
14. HashiCorp Consul - https://security.gentoo.org/glsa/202412-14

Fedora Security Advisories

1. Chromium - https://lwn.net/Articles/1001399
2. python3.11 - https://lwn.net/Articles/1001401
3. uv -
    a. https://lwn.net/Articles/1001402
    b. https://lwn.net/Articles/1001403
4. Chromium - https://lwn.net/Articles/1001400

Mageia Security Advisories

1. mesa, rust-bindgen, meson - http://advisories.mageia.org/MGAA-2024-0236.html
2. nvidia-newfeature - http://advisories.mageia.org/MGAA-2024-0237.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Check Point Security Advisories

1. Microsoft - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1133.html
2. Trihedral VTScada - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2016-1340.html
3. CyberPanel - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1139.html
4. VMware - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2020-4216.html

Cisco Advisories and Alerts

1. Cisco NX-OS Software Image Verification Bypass - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-image-sig-bypas-pQDRQvjL?vs_f=Cisco%20Security%20Advisory%26vs_cat=Security%20Intelligence%26vs_type=RSS%26vs_p=Cisco%20NX-OS%20Software%20Image%20Verification%20Bypass%20Vulnerability%26vs_k=1

Red Hat Security Advisories

1. postgresql:13 - https://access.redhat.com/errata/RHSA-2024:10879
2. firefox - https://access.redhat.com/errata/RHSA-2024:10880
3. postgresql - https://access.redhat.com/errata/RHSA-2024:10882

Ubuntu Security Notices

1. Tinyproxy - https://ubuntu.com/security/notices/USN-7140-1
2. WebKitGTK - https://ubuntu.com/security/notices/USN-7142-1
3. RabbitMQ - https://ubuntu.com/security/notices/USN-7143-1
4. Linux kernel - https://ubuntu.com/security/notices/USN-7144-1

Zero Day Initiative Advisories & Updates

1. Epic Games - https://www.zerodayinitiative.com/advisories/ZDI-24-1646/