CYBERINT WEEKLY >REPORT

CRYPTO PLATFORM ACCESS OFFERED FOR SALE

Cyberint Argos has identified an initial access broker offering system admin panel access to a crypto platform. This access is priced significantly higher than usual, at $50,000.

EXCLUSIVE | CRYPTO | ACCESS

UPSTOX.COM Data leak - Reposted

In April 2021, Indian brokerage firm Upstox suffered a data breach. The incident exposed extensive personal information on over 100,000 customers, including names, genders, dates of birth, physical addresses, banking information, and passwords stored as bcrypt hashes.

EXCLUSIVE | LEAK | INDIA

Police seize over 100 malware loader servers, arrest four cybercriminals

An international law enforcement initiative dubbed 'Operation Endgame' has dismantled over 100 servers used by major malware loader operations, including IcedID, Pikabot, Trickbot, Bumblebee, Smokeloader, and SystemBC.

SIEZE | MALWARE | GLOBAL

Cybercriminals pose as "helpful" Stack Overflow users to push malware

Cybercriminals are leveraging Stack Overflow to spread malware by answering user questions and promoting a malicious PyPi package named 'pytoileur.' This package, part of the known 'Cool package' campaign, masquerades as an API management tool but installs Windows information-stealing malware.

SOCIAL | CAMPAIGN | GLOBAL

Threat Actor 888 Allegedly Leaks Shell Data, Impacting 80,000 Individuals

Cyberint Argos has detected that a threat actor named '888' has allegedly leaked data belonging to Shell, the prominent British multinational oil and gas corporation. The disclosed database purportedly contains around 80,000 entries

888 | LEAK | SHELL

Threat Actor Allegedly Selling Unauthorized Citrix Access to American Insurance Company

A threat actor named ‘proper12’ from Exploit forum, claims to be selling unauthorized Citrix access to a major American insurance company with an annual revenue of $10 billion.

PROPER12 | ACCESS | INSURANCE

DMM Bitcoin warns that threat actors stole $300 million in Bitcoin

Japanese crypto exchange DMM Bitcoin has reported the theft of 4,502.9 Bitcoin (BTC), valued at approximately $308 million (48.2 billion yen) , marking the most significant cryptocurrency heist of 2024. The unauthorized transfer was detected on May 31, 2024

DMM | CRYPTO | BREACH

ShinyHunters - Snowflake - Breach

In April and May of 2024, Snowflake, a cloud data warehousing company, became the victim of a data breach when a threat actor named "ShinyHunters" gained access to its systems using stolen employee credentials. According to the threat actor, customer data of 400 companies using Snowflake's services was extracted.

SHINYHUNTERS | SNOWFLAKE | BREACH

Mysterious Cyber Attack Took Down 600,000+ Routers in the U.S.

Over 600,000 small office/home office (SOHO) routers have been rendered inoperable following a cyber attack by unidentified actors, disrupting internet access for many users in the U.S.

CAMPAIGN | U.S. | DISRUPTION

Threat Actor Claims to Have Leaked Riyadh Airport Employee Database

A threat actor (”888”) from Breachforums, claims to have leaked sensitive employee data from Riyadh Airport, potentially exposing the personal information of hundreds of employees.

888 | RIYADH AIRPORT | BREACH

NEW WEEKLY VULNERABILITIES

CVE-2024-24919

CHECK POINT

CVSS: 8.6

On May 28, 2024, Check Point released an advisory for CVE-2024-24919, a high-severity information disclosure vulnerability affecting Check Point Security Gateway devices configured with the “IPSec VPN” or “Mobile Access” software blade. They reported observing in-the-wild exploitation of this vulnerability since April 30, 2024. Threat actors have been using it to enumerate and extract password hashes for all local accounts, including those connected to Active Directory. Additionally, adversaries have been seen moving laterally and extracting the “ntds.dit” file from compromised customers' Active Directory servers within hours of the initial attack on a vulnerable Check Point Gateway.

CVE-2024-3820

WORDPRESS

CVSS: 10.0

A vulnerability was found in wpDataTables Plugin up to 6.3.1 on WordPress. It has been declared as critical. The plugin for WordPress is vulnerable to SQL Injection via the 'id_key' parameter of the wdt_delete_table_row AJAX action in all versions up to and including 6.3.1. This is due to insufficient escaping of user-supplied parameters and inadequate preparation of existing SQL queries. This vulnerability allows unauthenticated attackers to append additional SQL queries to existing ones, potentially extracting sensitive information from the database. It is important to note that this issue only affects the plugin's premium version.

CVE-2024-5035

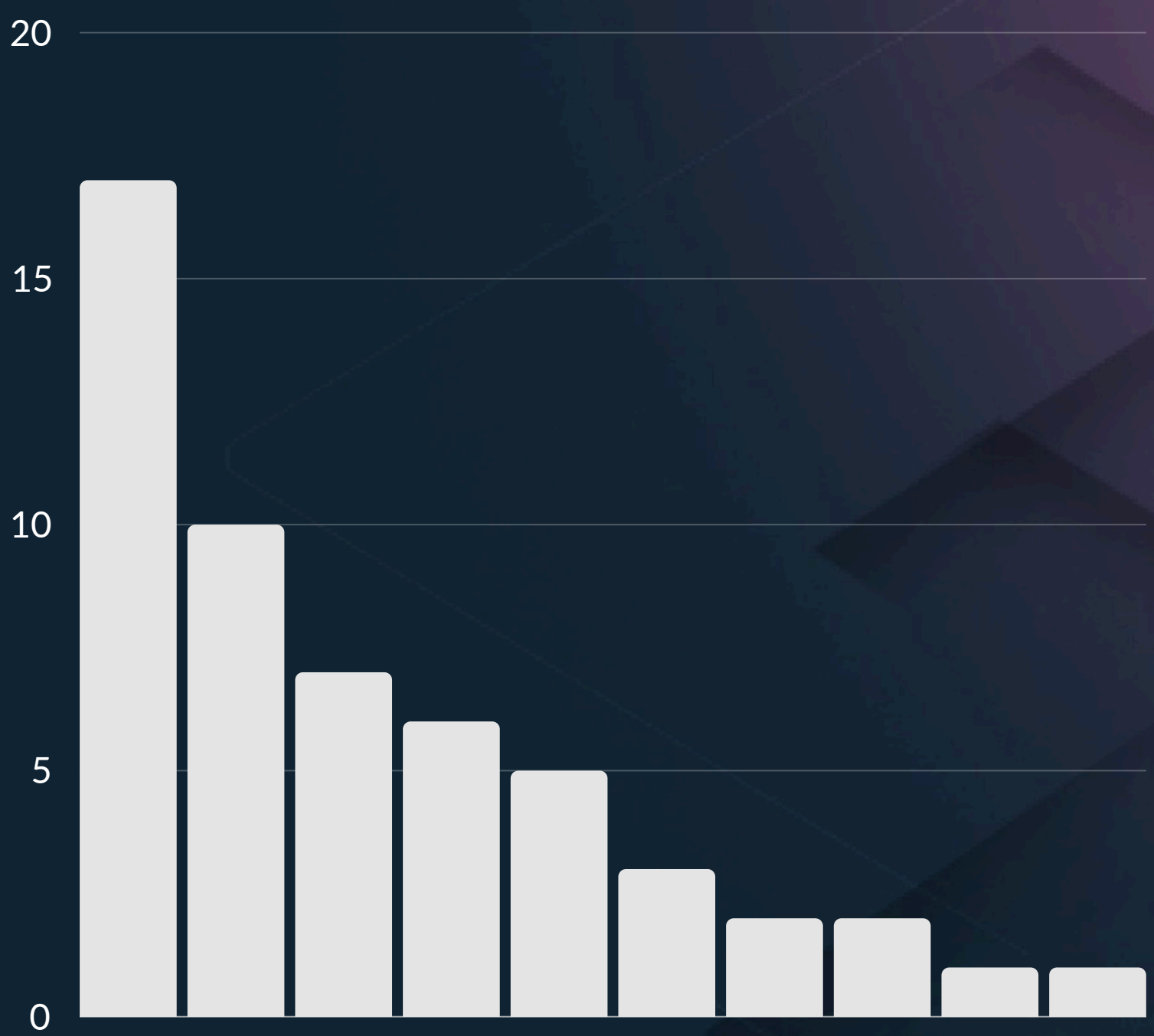
TP-LINK

CVSS: 9.8

A critical security flaw has been identified in the TP-Link Archer C5400X gaming router, potentially leading to remote code execution through specially crafted requests. Exploiting this flaw allows remote unauthenticated attackers to execute arbitrary commands on the device with elevated privileges.
The vulnerability lies in the "rftest" binary related to radio frequency testing, which is launched at startup and listens on TCP ports 8888, 8889, and 8890. This exposure permits remote unauthenticated attackers to achieve code execution. Although the network service is supposed to accept only commands starting with "wl" or "nvram get," ONEKEY discovered that this restriction can be easily bypassed by injecting commands after shell meta-characters like ; , & , or | (e.g., "wl;id;").

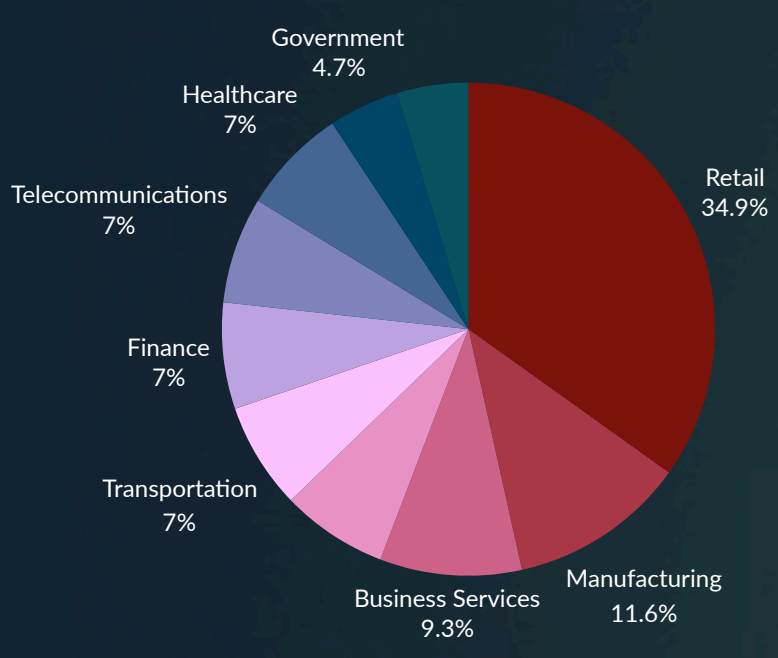
WEEKLY RANSOMWARE STATS

WEEKLY TOP RANSOMWARE FAMILIES



- LOCKBIT3.0 LEADING THE RANSOMWARE INDUSTRY THIS WEEK WITH 17 NEW VICTIMS.
- AKIRA IN SECOND PLACE THIS WEEK WITH 10 NEW VICTIMS.
- 8BASE ARE THIRD THIS WEEK WITH SEVEN NEW VICTIMS

TOP 10 TARGETED SECTORS DISTRIBUTION



TOP 10 TARGETED COUNTRIES DISTRIBUTION