SCC DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

NOVEMBER 2024 - VOL.4

The News

IN THE NEWS THIS WEEK

Critical WordPress Anti-Spam Plugin Flaws Expose 200,000+ Sites to Remote Attacks

Two critical security flaws impacting the Spam protection, Anti-Spam, and FireWall plugin WordPress could allow an unauthenticated attacker to install and enable malicious plugins on susceptible sites and potentially achieve remote code execution.

The vulnerabilities, tracked as CVE-2024-10542 and CVE-2024-10781, carry a CVSS score of 9.8 out of a maximum of 10.0. They were addressed in versions 6.44 and 6.45 released this month.

READ MORE

British hospital group declares ‘major incident’ following cyberattack

The NHS Trust responsible for a group of hospitals in northwest England has declared a “major incident” following a cyberattack, invoking the crisis management status for events that pose a serious risk to public health.

A statement on the website for Wirral University Teaching Hospital NHS Foundation Trust says: “A major incident has been declared at the Trust for cyber security reasons.”

READ MORE

OTHER NEWS HIGHLIGHTS

XML-RPC npm Library Turns Malicious, Steals Data, Deploys Crypto Miner

Appeals court overturns Treasury sanctions against crypto mixer Tornado Cash

Tor needs 200 new WebTunnel bridges to fight censorship

Microsoft Fixes AI, Cloud, and ERP Security Flaws; One Exploited in Active Attacks

Over Two Dozen Flaws Identified in Advantech Industrial Wi-Fi Access Points – Patch ASAP

The News

TOP OF THE NEWS THIS WEEK

Cloudflare says it lost 55% of logs pushed to customers for 3.5 hours

Internet security giant Cloudflare announced that it lost 55% of all logs pushed to customers over a 3.5-hour period due to a bug in the log collection service on November 14, 2024.

Cloudflare offers an extensive logging service to customers that allows them to monitor the traffic on their site and filter that traffic based on certain criteria.

These logs allow customers to analyze traffic to their hosts to monitor and investigate security incidents, troubleshooting, DDoS attacks, traffic patterns, or to perform site optimizations.

For customers who wish to analyze these logs using external tools, Cloudflare offers a "logpush" service that collects logs from its various endpoints and pushes them out to external storage services, such as Amazon S3, Elastic, Microsoft Azure, Splunk, Google Cloud Storage, etc.
These logs are generated at a massive scale, as Cloudflare processes over 50 trillion customer event logs daily, of which around 4.5 trillion logs are sent to customers.

READ MORE >

TOP RELATED ARTICLES

Cloudflare incident on November 14, 2024, resulting in lost logs

Cloudflare broke its logging-a-service service, causing customer data loss

Bug causes Cloudflare to lose customer logs

Cloudflare Improves Systems After Data Loss Incident

Geo-Politics

NEWS FROM AROUND THE WORLD

Chinese hackers breached T-Mobile's routers to scope out network

T-Mobile says the Chinese "Salt Typhoon" hackers who recently compromised its systems as part of a series of telecom breaches first hacked into some of its routers to explore ways to navigate laterally through the network.
However, the company says its engineers blocked the threat actors before they could spread further on the network and access customer information.

READ MORE >

GLASSBRIDGE: Google Blocks Thousands of Pro-China Fake News Sites

Google's Threat Intelligence Group (TAG), in collaboration with its cybersecurity firm Mandiant, has discovered a large-scale network of fake news websites operated by four different public relations (PR) firms spreading propaganda aligned with the interests of the Chinese government.

READ MORE >

HIGHLIGHTS FROM AROUND THE WORLD

Chinese Hackers Use GHOSTSPIDER Malware to Hack Telecoms Across 12+ Countries

North Korean Hackers Steal $10M with AI-Driven Scams and Malware on LinkedIn

Russian Hackers Deploy HATVIBE and CHERRYSPY Malware Across Europe and Asia

Attack Group APT-C-60 Targets Japan Using Trusted Platforms

Breaches

SECURITY BREACHES THIS WEEK

Ransomware Attack on Blue Yonder Hits Starbucks, Supermarkets

A disruptive ransomware attack on Blue Yonder, a supply chain management software provider for major retailers, consumer product companies, and manufacturers, highlights the heightened risk organizations face during the busy holiday season.
A Nov. 21 attack on Blue Yonder affected infrastructure that the company uses to host a variety of managed services for customers

READ MORE

Hackers exploit ProjectSend flaw to backdoor exposed servers

Threat actors are using public exploits for a critical authentication bypass flaw in ProjectSend to upload webshells and gain remote access to servers. The flaw, tracked as CVE-2024-11680, is a critical authentication bug impacting ProjectSend versions before r1720, allowing attackers to send specially crafted HTTP requests to 'options.php' to change the application's configuration.
Successful exploitation allows the creation of rogue accounts, planting webshells, and embedding malicious JavaScript code.

READ MORE

OTHER SECURITY BREACHES

Malicious Actors Exploit ProjectSend Critical Vulnerability

Russian Hackers Exploit Firefox and Windows 0-Days to Deploy Backdoor

RansomHub gang says it broke into networks of Texas city, Minneapolis agency

China’s Salt Typhoon hackers target telecom firms in Southeast Asia with new malware

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2020-26073 - Cisco SD-WAN vManage Software Directory Traversal Vulnerability

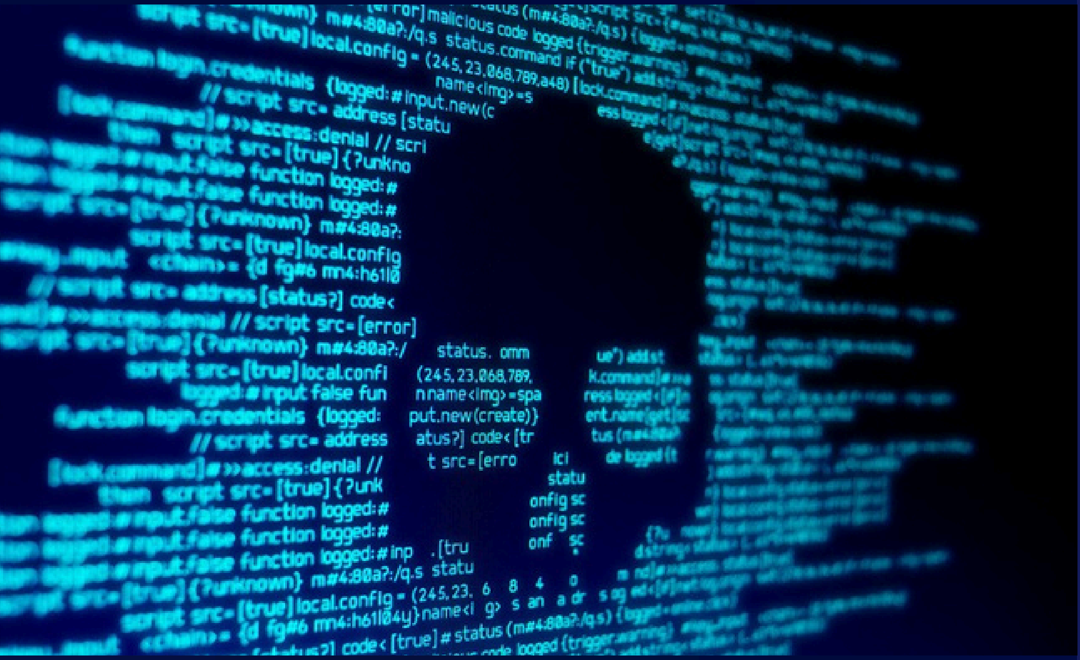
CVSS SCORE 7.8

LAST WEEKS RECAP

CVE-2024-0012 PAN-OS: Authentication Bypass in the Management Web Interface (PAN-SA-2024-0015)
CVSS Score: (9.3)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS



OVERVIEW

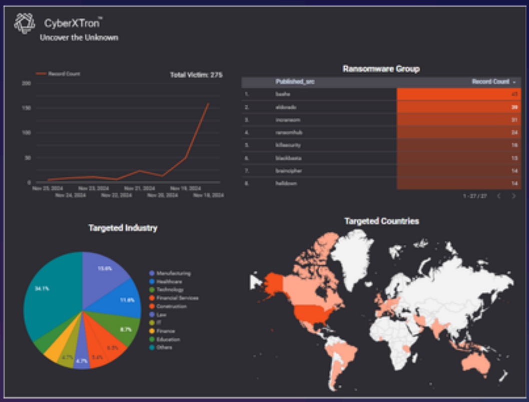
This week the ransomware group who had performed the most attacks was bashe who performed 45 out of 275

TARGET INDUSTRIES

Last week saw the most ransomware attacks against the Manufacturing and healthcare

TARGET COUNTRY

The United States has consistently held the top position as the primary target.



Ransomware Group

	Published_src	Record Count
1.	bashe	45
2.	eldorado	39
3.	incransom	31
4.	ransomhub	24
5.	killsecurity	16
6.	blackbasta	15
7.	braincipher	14
8.	helldown	14

1 - 27 / 27

Dive into this interactive report to uncover hidden trends HERE!

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

TOP THREAT ACTORS

LockBit

LockBit is a ransomware-as- a-service (RaaS) group that has been active since September 2019. LockBit has developed several variants of ransomware products to perform encryption

RansomHub

RansomHub, a new Ransomware-as-a-Service (RaaS) that has rapidly become one of the largest ransomware groups currently operating, is very likely an updated and rebranded version of the older Knight ransomware.

BlackBasta

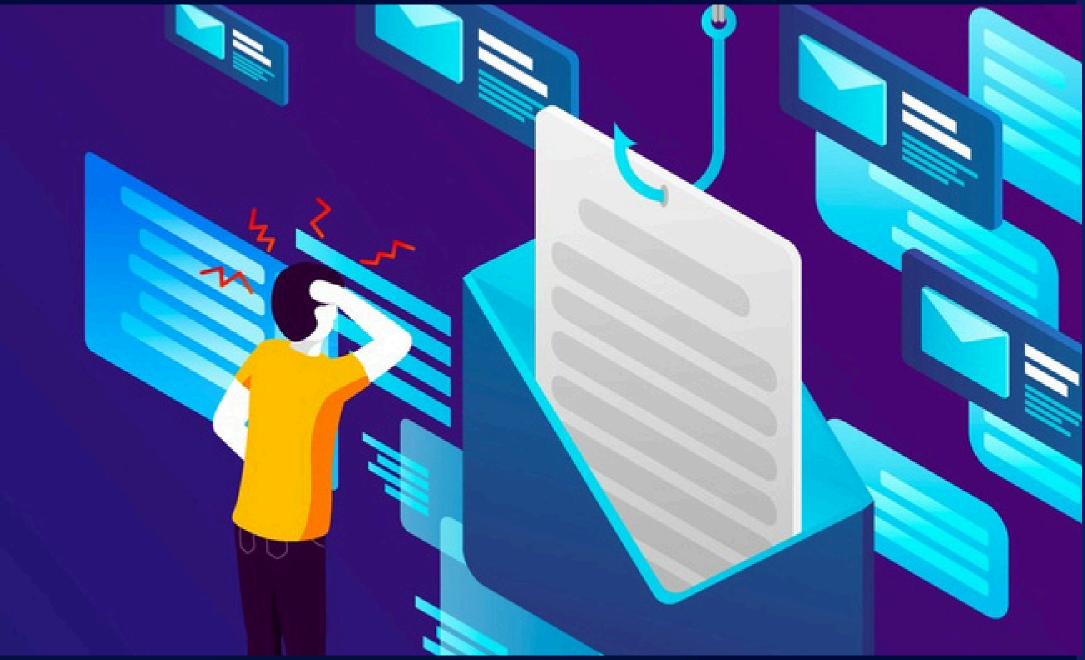
BlackBasta is a ransomware operator and Ransomware- as-a-Service criminal enterprise that first emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world.

Play

The group focuses on multi- extortion in that they encrypt target organizations’ data, but also threaten to post the data to their public TOR-based sites.

Phishing

PHISHING NEWS THIS WEEK



Bangkok busts SMS Blaster sending 1 million scam texts from a van

The Thailand police located a van and arrested its driver for using an SMS blaster device to spam over 100,000 SMS phishing texts an hour to people living in Bangkok.

The device, which reportedly had a range of approximately three kilometres (10,000 feet), could send out messages at a rate of 100,000 every hour.

Over three days, the scammers sent almost one million SMS text messages to mobile devices in range that stated, "Your 9,268 points are about to expire! Hurry up and redeem your gift now."

The text messages contained a link to a phishing website that contained the string 'aisthailand,' impersonating Advanced Info Service (AIS), Thailand's largest mobile phone operator.

Users who clicked on the phishing URL were taken to a page requesting their credit card information, which is then sent back to the scammers to perform unauthorized transactions in other countries.

READ MORE >

OTHER PHISHING ARTICLES

Latest Multi-Stage Attack Scenarios with Real-World Examples

Woman loses £50k in WhatsApp investment scam

Nearly Every Hacker Believes AI Tools Have Created a New Attack Vector

Chinese Threat Actor Targets Black Friday Shoppers With Phishing Campaign