SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

DECEMBER 2024 - VOL.3

The News

IN THE NEWS THIS WEEK

Microsoft Teams Vishing Spreads DarkGate RAT

The DarkGate remote access Trojan (RAT) has a new attack vector: A threat actor targeted a Microsoft Teams user via a voice call to gain access to their device.
The attack adds to the other methods for spreading the RAT, which previously has been propagated using phishing emails, malvertising, hijacking of Skype and Teams messages, and search engine optimization (SEO) poisoning, researchers said.

READ MORE

Hackers Leak Partial Cisco Data from 4.5TB of Exposed Records

On Monday, December 16, 2024, hackers leaked what they referred to as “partial data” belonging to technology and cybersecurity giant Cisco. The leak occurred on the cybercrime and data breach platform Breach Forums, where IntelBroker, a notorious hacker and the forum’s owner, released 2.9 GB of data for download.
The leaked data is part of a 4.5TB dataset that was allegedly left unprotected by Cisco in October 2024.

READ MORE

OTHER NEWS HIGHLIGHTS

Over 25,000 SonicWall VPN Firewalls exposed to critical flaws

Patch Alert: Critical Apache Struts Flaw Found, Exploitation Attempts Detected

Rspack npm Packages Compromised with Crypto Mining Malware in Supply Chain Attack

Sophos Issues Hotfixes for Critical Firewall Flaws: Update to Prevent Exploitation

Romanian Netwalker ransomware affiliate sentenced to 20 years in prison

The News

TOP OF THE NEWS THIS WEEK

Fortinet warns of FortiWLM bug giving hackers admin privileges

Fortinet has disclosed a critical vulnerability in Fortinet Wireless Manager (FortiWLM) that allows remote attackers to take over devices by executing unauthorized code or commands through specially crafted web requests.

FortiWLM is a centralized management tool for monitoring, managing, and optimizing wireless networks. It's used by government agencies, healthcare organizations, educational institutions, and large enterprises.

The flaw, tracked as CVE-2023-34990, is a relative path traversal flaw rated with a score of 9.8.

Horizon3 researcher Zach Hanley discovered and disclosed the vulnerability to Fortinet in May 2023. However, the flaw remained unfixed ten months later, and Hanley decided to disclose information and a POC it on March 14, 2024 in a technical writeup about other Fortinet flaws he discovered.

READ MORE

TOP RELATED ARTICLES

Critical Vulnerability in FortiWLM Grants Hackers Administrative Control

Fortinet Warns of Critical FortiWLM Flaw That Could Lead to Admin Access Exploits

CVE-2023-34990

FortiWLM Security Alert Critical Remote Code Execution Flaw Discovered

Geo-Politics

NEWS FROM AROUND THE WORLD

390,000 WordPress accounts stolen from hackers in supply chain attack

A threat actor tracked as MUT-1244 has stolen over 390,000 WordPress credentials in a large-scale, year-long campaign targeting other threat actors using a trojanized WordPress credentials checker.
Researchers at Datadog Security Labs, who spotted the attacks, say that SSH private keys and AWS access keys were also stolen from the compromised systems of hundreds of other victims, believed to include red teamers, penetration testers, security researchers, as well as malicious actors.

READ MORE

Ireland fines Meta $264 million over 2018 Facebook data breach

The Irish Data Protection Commission (DPC) fined Meta €251 million ($263.6M) over General Data Protection Regulation (GDPR) violations arising from a 2018 personal data breach impacting 29 million Facebook accounts.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

APT29 Hackers Target High-Value Victims Using Rogue RDP Servers and PyRDP

Hackers Use Microsoft MSC Files to Deploy Obfuscated Backdoor in Pakistan Attacks

Ukrainian Minors Recruited for Cyber Ops and Reconnaissance in Russian Airstrikes

American private equity firm buys Israeli spyware company Paragon

Breaches

SECURITY BREACHES THIS WEEK

Rhode Island confirms data breach after Brain Cipher ransomware attack

TRhode Island is warning that its RIBridges system, managed by Deloitte, suffered a data breach exposing residents' personal information after the Brain Cipher ransomware gang hacked its systems.
RIBridges is a modern integrated eligibility system (IES) used in Rhode Island to manage and deliver public assistance programs, helping streamline the administration of various social services.

READ MORE

Texas Tech University System data breach impacts 1.4 million patients

The Texas Tech University Health Sciences Center and its El Paso counterpart suffered a cyberattack that disrupted computer systems and applications, potentially exposing the data of 1.4 million patients.
The organization is a public, academic health institution that is part of the Texas Tech University System, which educates and trains healthcare professionals, conducts medical research, and provides patient care services.

READ MORE

OTHER SECURITY BREACHES

ClOp Ransomware Exploits Cleo Vulnerability, Threatens Data Leaks

Cicada3301 Ransomware Claims Attack on French Peugeot Dealership

New fake Ledger data breach emails try to steal crypto wallets

Namibia's state telecom provider says hackers leaked data after it refused to pay ransom

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-35250 - Windows Kernel-Mode Driver Elevation of Privilege Vulnerability (CVSS 7.8)

CVSS SCORE 7.8

CVE-2024-53677 Apache Struts File Upload Vulnerability (CVSS 9.5)

CVSS SCORE 9.5

LAST WEEKS RECAP

CVE-2014-2120 - Cisco Adaptive Security Appliance WebVPN Login Page Cross-Site Scripting Vulnerability (CVSS 4.3)

CVE-2024-12053 - Google Chrome V8 Type Confusion Vulnerability (CVSS 8.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

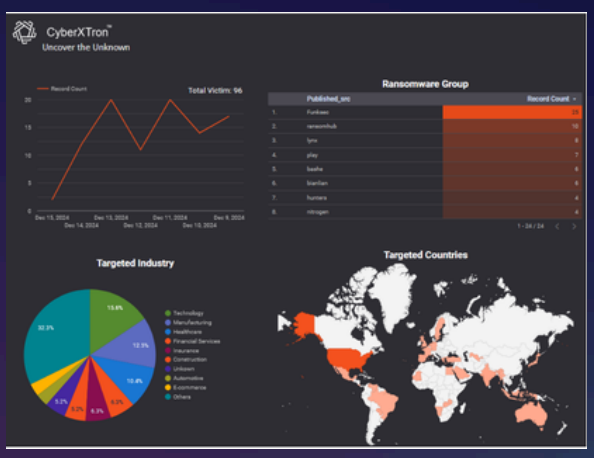
This week for ransomware, the 'Funksec' group claimed the most victims with 25 out of 96.

TARGET INDUSTRIES

This week saw the most ransomware attacks against the Manufacturing and Technology industries

TARGET COUNTRY

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



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

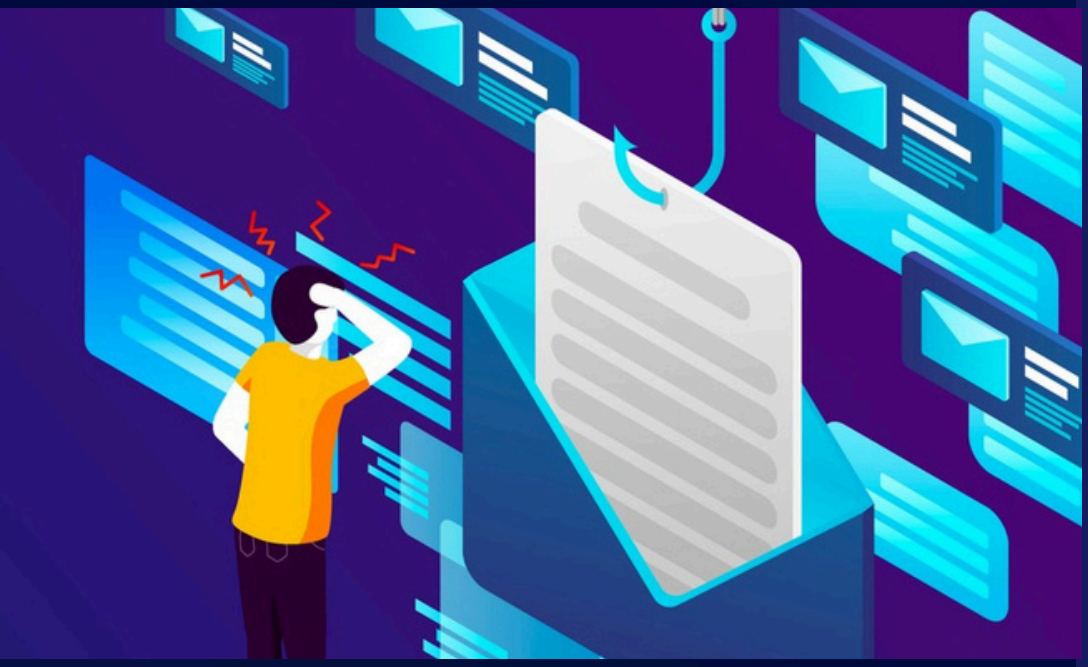
BlackBasta is a ransomware operator and Ransomware- as-a-Service criminal enterprise that first emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world.

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



Phishers cast wide net with spoofed Google Calendar invites

Criminals are spoofing Google Calendar emails in a financially motivated phishing expedition that has already affected about 300 organizations with more than 4,000 emails sent over four weeks, according to Check Point researchers.

The crims modify sender email headers so the messages appear to be legitimate Google Calendar invites sent from someone the victim knows. It's a good lure, from the fraudsters' perspective, because more than 500 million people use Google Calendar.

The phishing emails usually include a [.]ics calendar file with a link to Google Forms or Google Drawings. Once the recipient clicks on the link, they are prompted to click on another one, which Check Point notes is typically disguised as a reCAPTCHA or support button.

Spoiler alert: it's fake. Once the victim clicks the malicious link, they land on what looks like a cryptocurrency mining or Bitcoin support page.

READ MORE

OTHER PHISHING ARTICLES

Critical Infrastructure Under Siege: 42% Spike in Ransomware Attacks on Utilities

HubPhish Exploits HubSpot Tools to Target 20,000 European Users for Credential Theft

AI-Powered Investment Scams Surge: How 'Nomani' Steals Money and Data

DarkGate Malware Distributed Via Microsoft Teams Voice Phishing