SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

NOVEMBER 2024 - VOL.1

The News

IN THE NEWS THIS WEEK

New FakeCall Malware Variant Hijacks Android Devices for Fraudulent Banking Calls

Cybersecurity researchers have discovered a new version of a well-known Android malware family dubbed FakeCall that employs voice phishing (aka vishing) techniques to trick users into parting with their personal information. "FakeCall is an extremely sophisticated Vishing attack that leverages malware to take almost complete control of the mobile device, including the interception of incoming and outgoing calls," Zimperium researcher Fernando Ortega said in a report published last week.

READ MORE

Malicious PyPI Package 'Fabrice' Found Stealing AWS Keys from Thousands of Developers

Cybersecurity researchers have discovered a malicious package on the Python Package Index (PyPI) that has racked up thousands of downloads for over three years while stealthily exfiltrating developers' Amazon Web Services (AWS) credentials. The package in question is "fabrice," which typosquats a popular Python library known as "fabric," which is designed to execute shell commands remotely over SSH.

READ MORE

OTHER NEWS HIGHLIGHTS

Chinese Air Fryers May Be Spying on Consumers, Which? Warns

UK Council Sites Recover Following Russian DDoS Blitz

Google Cloud to make MFA mandatory by the end of 2025

Germany drafts law to protect researchers who find security flaws

South Korea Fines Meta $15 Million for Illegally Collecting Information on Facebook Users

The News

TOP OF THE NEWS THIS WEEK

Windows infected with backdoored Linux VMs in new phishing attacks

A new phishing campaign dubbed 'CRON#TRAP' infects Windows with a Linux virtual machine that contains a built-in backdoor to give stealthy access to corporate networks.

Using virtual machines to conduct attacks is nothing new, with ransomware gangs and cryptominers using them to stealthily perform malicious activity. However, threat actors commonly install these manually after they breach a network.

A new campaign spotted by Securonix researchers is instead using phishing emails to perform unattended installs of Linux virtual machines to breach and gain persistence on corporate networks.

The phishing emails pretend to be a "OneAmerica survey" that includes a large 285MB ZIP archive to install a Linux VM with a pre-installed backdoor.

This ZIP file contains a Windows shortcut named "OneAmerica Survey.lnk" and a "data" folder that contains the QEMU virtual machine application, with the main executable disguised as fontdiag.exe.

READ MORE

TOP RELATED ARTICLES

Dangerous new phishing campaign infects Windows devices with malicious Linux VM

Hackers Deploy CRON#TRAP for Persistent Linux System Backdoors

CRON#TRAP Campaign Attacking Windows Machine With Weaponized Linux VMs

Attacker Hides Malicious Activity in Emulated Linux Environment

Geo-Politics

NEWS FROM AROUND THE WORLD

Ukraine accuses Google of revealing locations of its military systems

Ukraine is accusing Google of exposing the locations of its military sites in recent updates to its online mapping service. Andrii Kovalenko, the head of the counter-disinformation department at Ukraine's National Security and Defense Council, said the images were spotted last week and have already been “actively distributed” by Russians. He did not provide further details about what was specifically revealed or how Moscow could use the obtained data.

READ MORE

German Police Disrupt DDoS-for-Hire Platform dstat[.]cc; Suspects Arrested

German law enforcement authorities have announced the disruption of a criminal service called dstat[.]cc that made it possible for other threat actors to easily mount distributed denial-of-service (DDoS) attacks. "The platform made such DDoS attacks accessible to a wide range of users, even those without any in-depth technical skills of their own," the Federal Criminal Police Office (aka Bundeskriminalamt or BKA) said.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Canadian Suspect Arrested Over Snowflake Data Breach and Extortion Attacks

US Says Russia Behind Fake Haitian Voters Video

Social media and mobile internet restricted in Mozambique amid election protests

Canada Closes TikTok Offices, Citing National Security

Breaches

SECURITY BREACHES THIS WEEK

SelectBlinds says 200,000 customers impacted after hackers embed malware on site

More than 200,000 who shopped for blinds or window dressing this year had their credit card information and other data stolen after hackers placed malware on a major retailer's website. In breach notification documents filed this week in California and Maine, SelectBlinds said employees discovered the malware on September 28 and realized the malware had been on the company website since at least January 7.

READ MORE

Cyber-Attack on Microlise Disrupts DHL and Serco Tracking Services

A cyber-attack targeting telematics provider Microlise has disrupted tracking services for key clients like DHL and Serco while exposing some employee data. The company, which supplies asset-tracking software to large corporations, announced the breach on October 31. Following the disclosure, Microlise's stock price dropped by 16%, and the company has been working to restore its systems by the end of the week. The attack compromised "some limited employee data," according to Microlise's statement to the London Stock Exchange, although the company has indicated that customer data was not affected.

READ MORE

OTHER SECURITY BREACHES

Hackers Leak 300,000 MIT Technology Review Magazine User Records

Nokia says hackers leaked third-party app source code

Schneider Electric confirms dev platform breach after hacker steals data

Georgia hospital unable to access record system after ransomware attack

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-20418 - Cisco Unified Industrial Wireless Software for Ultra-Reliable Wireless Backhaul Access Point Command Injection Vulnerability

CVSS SCORE 10.0

CVE-2024-5910 - Palo Alto Expedition Missing Authentication Vulnerability

CVSS SCORE 9.3

LAST WEEKS RECAP

CVE-2024-23113 - Thousands of Fortinet instances vulnerable to actively exploited flaw
CVSS Score: (9.8)

CVE-2024-38178 - North Korean ScarCruft Exploits Windows Zero-Day to Spread RokRAT Malware
CVSS Score: (7.5)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

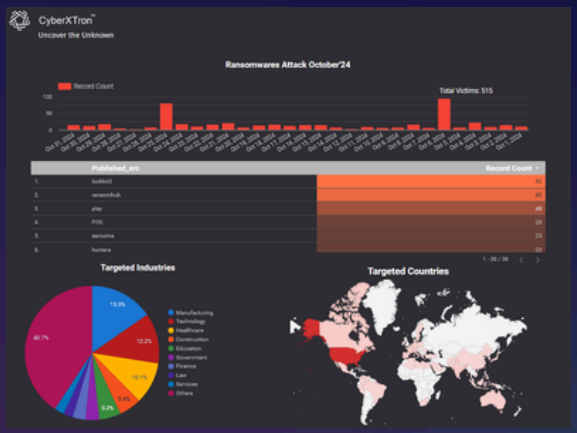
Throughout October 2024, lockbit3 claimed the most ransomware victims with 92 out of 515 (18%).

TARGET INDUSTRIES

Last month 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

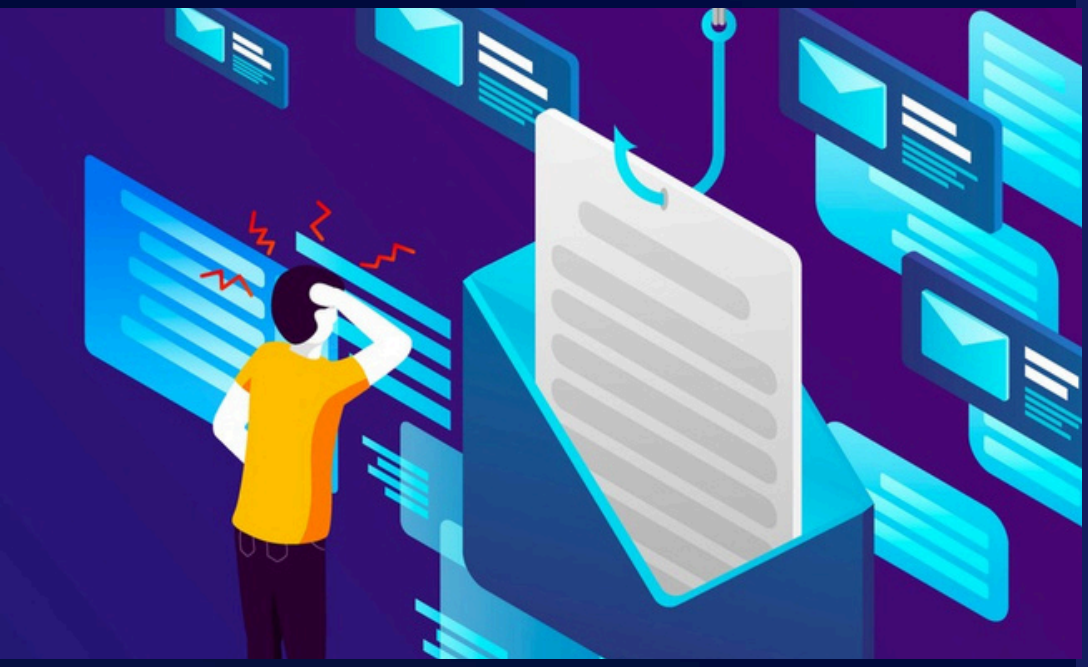
BlackBasta is a ransomware operator and Ransomware- as-a-Service criminal enterprise that first emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world.

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



Fake Copyright Infringement Emails Spread Rhadamanthys

Hundreds of companies worldwide have been targeted with spear-phishing emails claiming copyright infringement that actually deliver an infostealer.

Starting in July, Check Point Research began to track the emails as they spread across the Americas, Europe, and Southeast Asia, coming from a new domain each time. Hundreds of its customers have been targeted, indicating that the real reach of the campaign may be far greater still.

The goal of the emails is to bait guilt-riddled victims into downloading Rhadamanthys, a sophisticated infostealer equally capable of pilfering nation-state intelligence or, in this case, cryptocurrency wallet passphrases.

No two emails in the campaign that researchers have dubbed "CopyR(ight)hadamantys" come from the same address, indicating that there must be some kind of automation behind their distribution. This automation proves awkward in some circumstances — like when an Israeli target receives an email almost entirely in Korean — and limits the emails' ability to realistically impersonate known brands.

READ MORE

OTHER PHISHING ARTICLES

You're Invited: Rampant Phishing Abuses Eventbrite

US Sentences Nigerian to 26 Years in Prison for Stealing Millions Through Phishing

Businesses Worldwide Targeted in Large-Scale ChatGPT Phishing Campaign

How Microsoft Defender for Office 365 innovated to address QR code phishing attacks