






2024

May 4th week

CYBER SECURITY NEWS

CONTACT US

-  www.qualysec.com
-  +91 865 866 3664
-  contact@qualysec.com



Japan To Launch Active Cyber Defense System To Prevent Cyber Attacks

Japan is creating a consultative body to implement an active cyber defense system to improve its ability to counter cyberattacks on critical infrastructure. The government will tap railways, electricity, and telecommunications operators for their expertise.

This collaboration will likely involve information sharing on cyber risks and potential countermeasures, including an analysis of international cyberattacks. The new system is expected to function as a centralized command post for gathering intelligence and coordinating defensive actions.

A new organization is being formed to improve cybersecurity defense capabilities, including potential successors to the National Center for Incident Readiness and Strategy for Cybersecurity (NISC) and critical infrastructure operators like electricity and telecom companies.

The model is based on the US Cybersecurity and Infrastructure Security Agency's Joint Cyber Defense Collaborative (JCDC), a similar information-sharing group comprising various organizations, including telecoms, that share confidential cyber threat data and develop collaborative defense strategies.

Japan is updating its cybersecurity strategy to address the rising prevalence of hybrid warfare strategies that combine physical attacks with cyberattacks on critical infrastructure, and the NISC will establish a new centralized command post to gather and analyze threat data and tailor countermeasures.



Ransomhub Attacking Industrial Control Systems To Encrypt And Exfiltrate Data

Ransomhub, a new ransomware group, has targeted the SCADA system of a Spanish bioenergy plant, Matadero de Gijón, which highlights the critical security risks associated with Industrial Control Systems (ICS) across various industries.

Since 2022, numerous cyberattacks have exploited vulnerabilities in ICS, causing significant disruptions to operations and infrastructure. This highlights the need for robust security measures to safeguard ICS environments.

The Ransomhub ransomware group claimed unauthorized access to Gijón's Bio-Energy Plant's Supervisory Control and Data Acquisition (SCADA) system, which is critical for industrial process control.

The group provided screenshots as evidence, showcasing their ability to manipulate the plant's Digester and Heating system controls.

While the exact size of the data breach remains unclear (varying between 15 GB and 400 GB), the compromised SCADA system poses a significant risk to the plant's operations.

Ransomhub, a RaaS operation first advertised in February 2024, utilizes Golang and C++ for its locker component and leverages asymmetric cryptography (x25519) and a combination of symmetric algorithms (aes256, chacha20, and xchacha20) to encrypt victim data while achieving faster encryption speeds.



Chinese Hackers Using ORB Proxy Networks For Stealthy Cyber Attacks

Researchers found that cyber espionage groups with ties to China are increasingly using complicated proxy networks called Operational Relay Box (ORB) networks.

These networks are made up of mesh networks made from hacked devices and commercially leased virtual private servers (VPS).

Unlike traditional botnets, ORBs can be a hybrid of both, offering threat actors a constantly evolving infrastructure that's difficult to track by reporting details of the framework developed by Mandiant to map these ORBs, allowing defenders to identify potential infiltration attempts.

One such network, ORB3 (also known as SPACEHOP), has been linked to the well-known Chinese APT (Advanced Persistent Threat) groups APT5 and APT15.

At the same time, SPACEHOP is believed to be used for tasks like initial reconnaissance and vulnerability exploitation.

It has been highlighted that while using proxy networks for espionage isn't new, the scale and sophistication of ORBs employed by Chinese actors are a significant development.

By leveraging ORBs, Chinese APT groups can mask the origin of their malicious traffic, making it harder for defenders to identify and block communication between the attackers' command and control (C2) infrastructure and the targeted victim's network.

Source : <https://cybersecuritynews.com/chinese-orb-network-attacks/>



Sharp Dragon Hackers Attacking Government Entities Using Cobalt Strike & Custom Backdoors

The activities of the Chinese threat actor group known as Sharp Dragon (formerly Sharp Panda) have been meticulously documented.

Since 2021, this group has been involved in highly targeted phishing campaigns, primarily focusing on Southeast Asia.

However, recent developments indicate a significant shift in their operations, with the group now targeting governmental organizations in Africa and the Caribbean.

Historical Context

Checkpoint Blog [shows](#) Sharp Dragon has a history of deploying various payloads, including VictoryDLL and the Soul framework, through sophisticated phishing emails. Their modus operandi has remained consistent, with a focus on high-profile targets. However, the group's recent activities mark a notable expansion in their geographical focus.

Shift to Africa and the Caribbean

Starting in November 2023, Sharp Dragon began targeting governmental entities in Africa and the Caribbean.

This shift was facilitated by exploiting previously compromised entities in Southeast Asia.

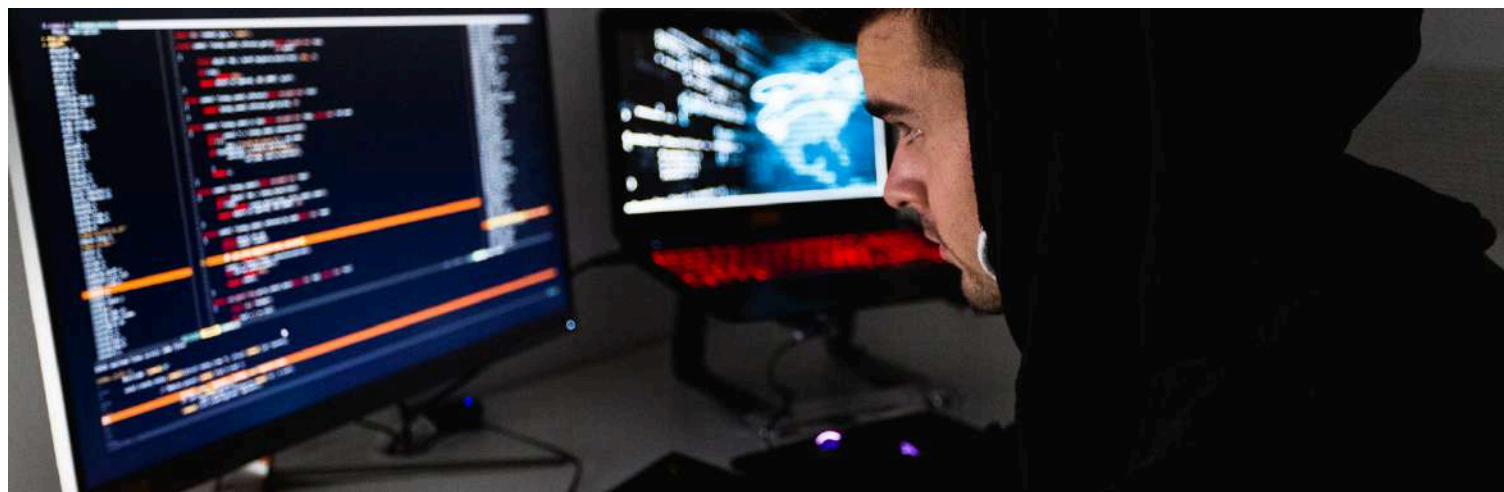
The group used highly tailored lures related to intergovernmental relations to establish footholds in these new regions.

Cyber Activities in Africa

The first identified phishing attack targeting Africa was sent from a Southeast Asian country to an African country in November 2023.

The lure document, which appeared to be an authentic correspondence about industrial relations, was used to deploy the Cobalt Strike Beacon.

Source : <https://cybersecuritynews.com/sharp-dragon-hackers-attacking/>



GenAI Bots Can Be Tricked by Anyone To Leak Company Secrets

The introduction and widespread use of generative AI technologies such as ChatGPT has shown a new era for the world but comes with some unexplored cybersecurity risks.

Prompt injection attacks are one form of manipulation that can happen with LLMs, wherein threat actors can manipulate bots into giving away sensitive data, generating offensive content, or generally disrupting computer systems. Such threats will rise as more GenAIs are adopted before fully understanding their cyber-security.

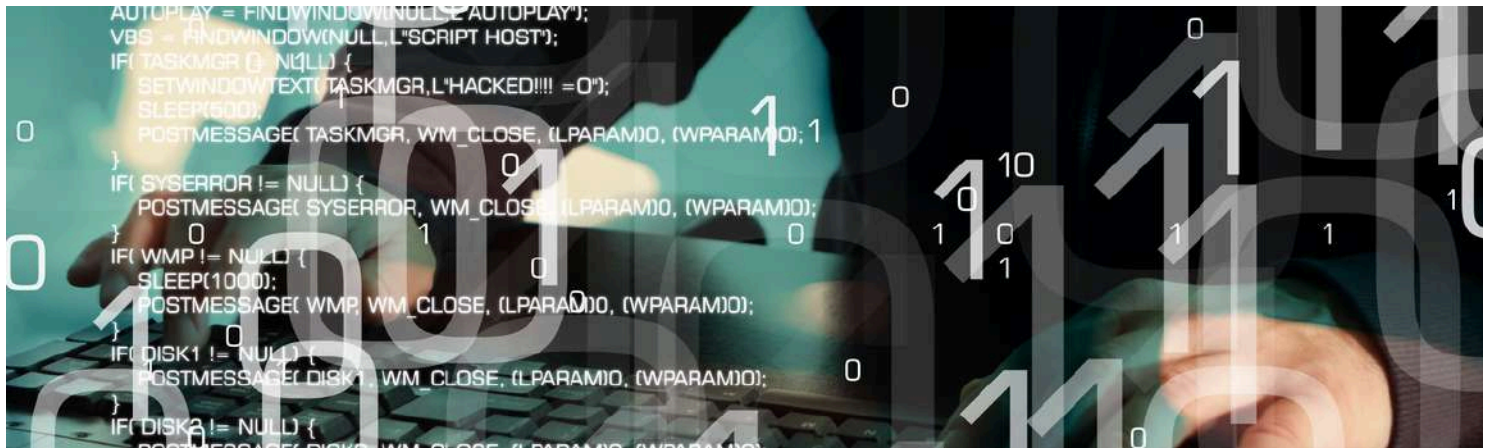
If nothing is done about it, widespread exploitation similar to botnets could occur, just as what happened with IoT default password exploitation, leading to new attack types.

Cybersecurity researchers at Immersive Labs recently discovered that anyone can trick GenAI bots into leaking company secrets.

GenAI Bots Leak Company Secrets

The research was based on anonymized, aggregated data from an interactive experience where users attempted prompt injection attacks to trick a GenAI bot into disclosing passwords through 10 progressively difficult levels.

This challenge tested the ability to outwit the AI system by exploiting vulnerabilities through carefully crafted prompts.



New DoS Attack 'DNSBomb' Exploiting DNS Queries & Responses

Cybersecurity researchers have unveiled a new and potent Denial of Service (DoS) attack, dubbed "DNSBomb."

This attack leverages the inherent mechanisms of the Domain Name System (DNS) to create a powerful pulsing DoS attack that poses a significant threat to internet infrastructure.

Exploiting DNS Mechanisms

DNSBomb capitalizes on several widely implemented DNS mechanisms, including timeout, query aggregation, and fast-returning response.

These mechanisms, designed to ensure availability, security, and reliability, are ingeniously transformed into malicious attack vectors.

By accumulating DNS queries sent at a low rate and amplifying them into large-sized responses, DNSBomb concentrates all DNS responses into short, high-volume periodic bursts.

This overwhelming pulse can simultaneously cripple target systems, leading to complete packet loss or severe service degradation across various connection types, including TCP, UDP, and QUIC.

The researchers extensively evaluated DNSBomb on 10 mainstream DNS software, 46 public DNS services, and approximately 1.8 million open DNS resolvers.

The findings were alarming: all DNS resolvers tested could be exploited to conduct more practical and powerful DNSBomb attacks than previous pulsing DoS attacks.

Small-scale experiments demonstrated that the peak pulse magnitude could approach 8.7Gb/s, with a bandwidth amplification factor exceeding 20,000x.

Source : <https://cybersecuritynews.com/new-dos-attack-dnsbomb-exploiting/>



Ransomware Attacks Targeting VMware ESXi Infrastructure Adopt New Pattern

Cybersecurity professionals at Sygnia have noted a notable change in the strategies used by ransomware groups that are aiming at virtualized environments, specifically VMware ESXi infrastructure, in relation to development.

The incident response team has noted a steady increase in these attacks, with threat actors exploiting misconfigurations and vulnerabilities in virtualization platforms to maximize their impact.

Sygnia's analysis reveals that notorious ransomware groups such as LockBit, HelloKitty, BlackMatter, RedAlert (N13V), Scattered Spider, Akira, Cactus, BlackCat, and Cheerscrypt frequently leverage this attack vector.

These threat actors have adopted a new attack pattern, focusing on data exfiltration before encrypting the targeted systems.

The modus operandi of these ransomware attacks involves gaining initial access to the virtualized environment, escalating privileges, and conducting extensive reconnaissance to identify valuable data.

The threat actors then exfiltrate this data, enabling them to encrypt the existing files and release the stolen information publicly to inflict additional reputational damage on the targeted organizations.

One of the most alarming aspects of these attacks is the unique actions taken by the threat actors during the ransomware execution phase.

Source : <https://cybersecuritynews.com/ransomware-attacks-targeting-vmware-esxi-infrastructure-adopt-new-pattern/>



Hackers Can Abuse Apple's Wi-Fi Positioning System to Track Users Globally

A recent study by security researchers has revealed a major privacy vulnerability in Apple's Wi-Fi Positioning System (WPS) that allows hackers to track the locations of Wi-Fi access points and their owners globally.

Researchers from the University of Maryland published their findings, which reveal that an unprivileged attacker can exploit Apple's crowdsourced location tracking system to amass a worldwide database of Wi-Fi access point locations and track devices' movements over time.

Apple's WPS relies on the company's vast network of iPhones, iPads, and MacBooks to collect the geolocation of Wi-Fi access points based on their unique Basic Service Set Identifier (BSSID).

When an Apple device uses GPS to determine its location, it periodically reports nearby Wi-Fi BSSIDs and their GPS coordinates to Apple's servers. This allows other Apple devices to query the WPS with visible BSSIDs to estimate their location, even without GPS connectivity.

The researchers found that Apple's WPS can be abused by repeatedly querying the service with BSSIDs derived from the IEEE's public database of Organizationally Unique Identifiers (OUIs) assigned to device manufacturers.

Researchers said that by systematically scanning the allocated OUI space, an attacker with no prior knowledge can quickly discover the location of millions of Wi-Fi access points worldwide

Source : <https://cybersecuritynews.com/apples-wi-fi-positioning-system/>



Threat Actor Claiming Access to AWS, Azure, MongoDB & Github API Keys

A threat actor has claimed to have gained unauthorized access to API keys for major cloud service providers, including Amazon Web Services (AWS), Microsoft Azure, MongoDB, and GitHub.

The announcement was made via a post on the social media platform X by the account DarkWebInformer.

The tweet has raised alarms within the cybersecurity community, prompting immediate investigations by the affected companies and security experts worldwide.

Potential Impact

Unauthorized access to API keys poses a severe risk as these keys can be used to access sensitive data, manipulate cloud resources, and potentially disrupt services.

API keys are essentially digital keys that allow applications to interact with cloud services, and if compromised, they can lead to data breaches and financial losses.

Security experts warn that the exposure of these keys could lead to:

- Unauthorized access to sensitive data stored in cloud databases.
- Manipulation or deletion of cloud resources.
- Potential for large-scale data breaches affecting millions of users.



LastPass is Encrypting URLs Used within Password Vaults

LastPass, a widely used password manager trusted by millions of consumers and businesses globally, has announced an upgrade to its security measures, the encryption of URLs within its password vaults.

This development is part of LastPass's ongoing mission to protect customer data while maintaining a seamless user experience.

The Evolution of URL Encryption

When LastPass was launched in 2008, the technology landscape was vastly different.

Decrypting URLs was a resource-intensive process that could slow down performance on low-powered PCs and mobile devices.

To ensure a smooth user experience, LastPass opted not to encrypt URLs within its vaults.

Over the years, additional URL-matching functionalities, such as the equivalent domains feature, were built on this logic.

However, technological advancements have made it feasible to encrypt all URL-related fields without compromising performance.

Modern devices can efficiently handle the encryption and decryption processes, allowing LastPass to enhance security without affecting the user experience.

URLs can contain sensitive information about the nature of the accounts associated with stored credentials, such as banking, email, and social media accounts.

Source : <https://cybersecuritynews.com/lastpass-is-encrypting-urls/>



“It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications”, concludes the researchers.

It's a fact that cybercrime is on the rise and it's more important than ever to protect your business from cyber threats.

But the good news is that you don't have to navigate the complex world of cybersecurity alone. Our team of experts is here to help you cyber security testing services need to protect your application or business.

Don't wait for a cyber attack to happen. Contact us now to learn more about how we can help secure your business and give you peace of mind.

Contact now and protect your business with our expert cyber security services.

CONTACT US AT