Date of Publication
November 28, 2022

Hive Pro

WEEKLY

THREAT DIGEST

Actors, Threats, and Vulnerabilities

21 to 27 NOVEMBER 2022

Summary

Threat Actors

Hive Pro discovered that one Actor has been active in the last week. **Earth Preta**, a Chinese threat actor group popular for Information theft and espionage, was spotted carrying out a large-scale cyber espionage campaign. For further details, see the key takeaway section for Actors.

Attacks

We also discovered five new malware strains have been active over the last week. **Aurora** Botnet a Malware-as-a-Service (MaaS) has been transformed into a stealer. To target Arab countries, several types of malware were employed, including **Emotet**, Qakbot, Formbook, and QuadAgent. Novel **Royal ransomware** has affected more than 50 victims. To exploit US businesses, the Black Basta ransomware gang utilized **QakBot** malware. The new variation **RansomExx** has been rewritten using the Rust programming language. For further details, see the key takeaway section for Attacks.

Vulnerabilities

We discovered two Vulnerabilities organizations should Prioritize last week. These 2 vulnerabilities affected Atlassian products. For further details, see the key takeaway section for Vulnerabilities.

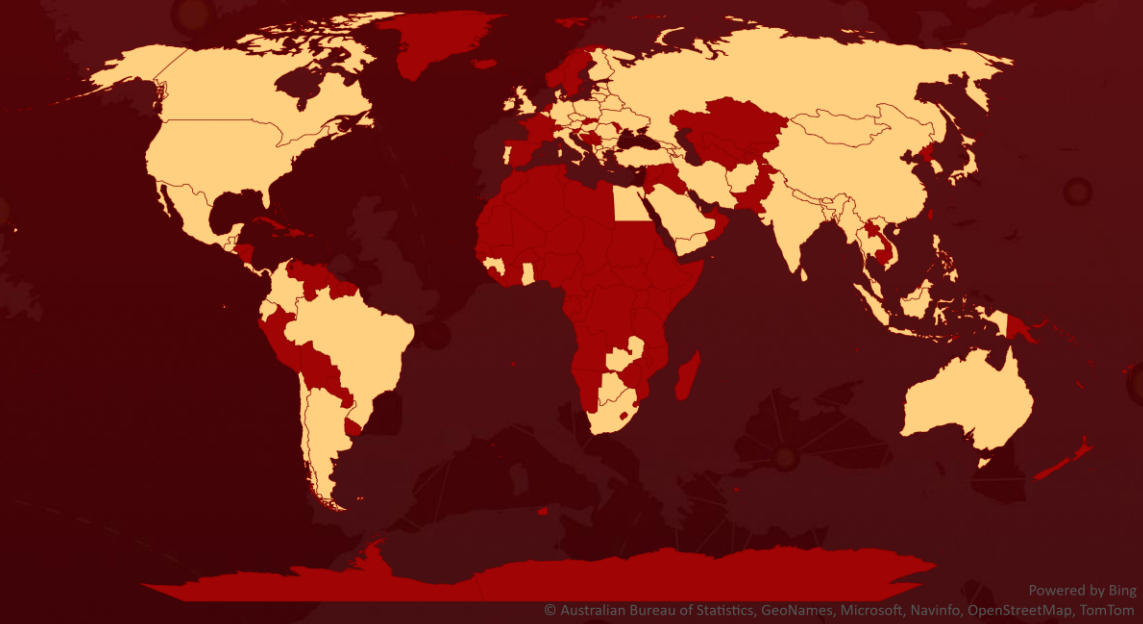
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Threat Actors

Earth Preta (Mustang Panda)
Earth Preta, an APT gang, conducted a large-scale cyber espionage campaign employing the malware families TONEINS, TONESHELL, and PUBLOAD, which were distributed via spear-phishing.

Actor Map



Actor Details

ICON	NAME	ORIGIN	MOTIVE
	Earth Preta	China	Information theft and espionage

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Attacks

Aurora (Cheshire)

Aurora Botnet, a Malware-as-a-Service (MaaS), has been repurposed into a stealer and supplied by Cheshire, a threat actor. Aurora distributes via phishing and executes several instructions through WMIC.

Multiple Malware (Oilrig)

Multiple malware families, including Emotet, Qakbot, Formbook, and QuadAgent, use the Oilrig actor in World Cup-themed phishing campaigns targeting specific companies partnered with the tournament in the Middle East.

Royal ransomware (DEV-0569)

The Royal Ransomware is the latest strain of ransomware operated by DEV-0569 that has infected over 50 victims via phishing attachments containing BATLOADER masquerading as legitimate installers for Microsoft Teams or Zoom.

QakBot (Black Basta Ransomware)

The QakBot malware is used by the Black Basta ransomware to acquire initial access and migrate laterally through an organization's network via spear-phishing operations.

RansomExx (Gold Dupont)

RansomExx is a ransomware variation that uses a ransomware-as-a-service (RaaS) model reconstructed in the Rust programming language, which reduces the likelihood of detection by antivirus software.

TOP MITRE ATT&CK TTPS:

T1082 System Information Discovery	**T1566** Phishing	**T1059** Command and Scripting Interpreter	**T1562** Impair Defenses	**T1140** Deobfuscate/ Decode Files or Information

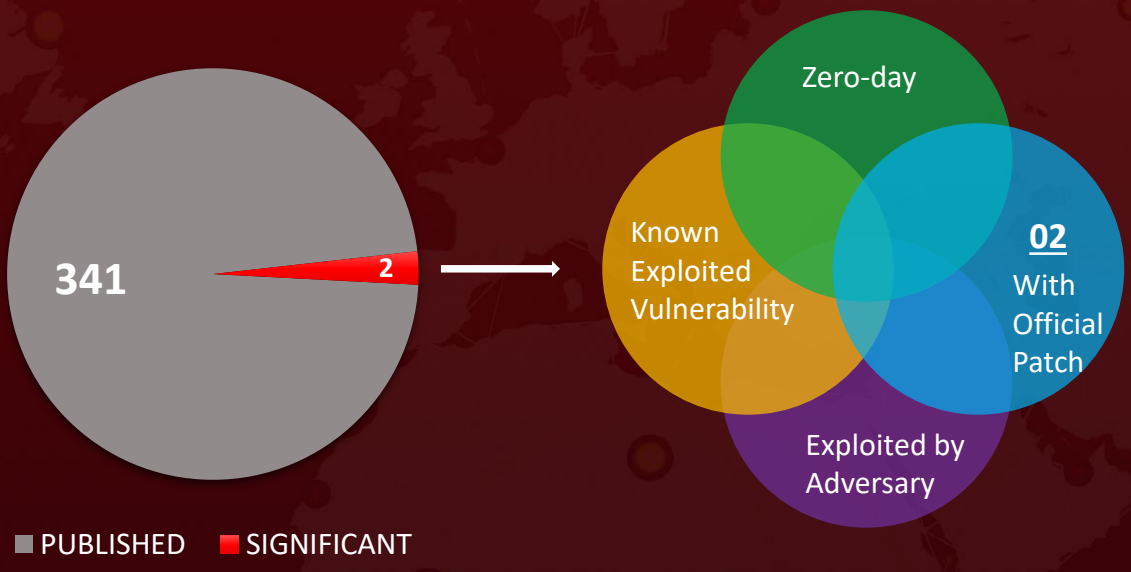
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

2 Notable Mentions

When exploited, the CVE-2022-43782 vulnerability in Atlassian provides privileged access to the Crowd API endpoints and the CVE-2022-43781 command injection vulnerability in Bitbucket Server and DataCenter.



*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **2 significant vulnerabilities** and block the indicators related to the threat actor **Earth Preta** and malware **Aurora**, **Emotet**, **Qakbot**, **Formbook**, **QuadAgent**, **Royal ransomware**, and **RansomExx**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **2 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to **Earth Preta** and malware **Aurora**, **Emotet**, **Qakbot**, **Formbook**, **QuadAgent**, **Royal ransomware**, and **RansomExx** in Breach and Attack Simulation(BAS)

Threat Advisories

Check out the links below for more extensive remediation and security precautions

Chinese APT Earth Preta runs spearphishing campaigns

Atlassian Addresses Issues in Crowd and Bitbucket Products

Aurora Botnet evolves into a Stealer

Arab countries are being targeted by multiple malware families

Rise in new Royal Ransomware attacks

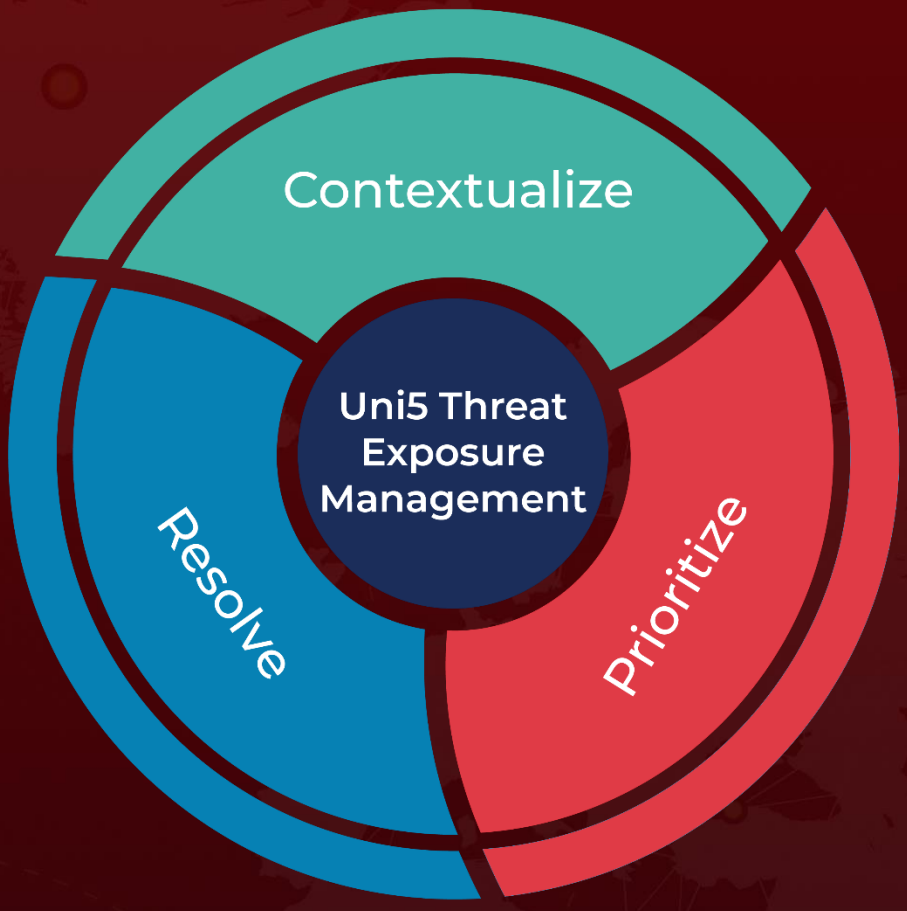
Black Basta Ransomware Invades US Firms with Qakbot Malware

A new RansomExx ransomware strain revised in Rust

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 28, 2022 . 2:10 AM

More at www.hivepro.com