Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 10 - 16, 2023

Report Summary:

- **New Threat Detection Added** – 4 (Atlassian Confluence CVE-2023-22515, Cytrox Predator Spyware, MataDoor Malware, and Ursnif Malware)
- **New Threat Protections - 8**
- **New Ransomware Victims Last Week - 76**

Newly Detected Threats Added

1. Atlassian Confluence CVE-2023-22515

Atlassian has received reports from a few customers regarding a Broken Access Control Vulnerability issue in publicly accessible Confluence Data Centre and Server instances. This vulnerability may have been exploited by external attackers to create unauthorised administrator accounts and gain access to Confluence instances. An update reveals that a known nation-state actor is actively exploiting the identified vulnerability (CVE-2023-22515), prompting Atlassian to collaborate closely with partners and customers for a thorough investigation and response.

Threat Protected: 02
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Alert	Alert
Security	Alert	Alert
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Attempted-recon
Kill Chain: Reconnaissance T1595 - Initial Access T1190

2. Cytrox Predator Spyware

A threat actor who has been sending links believed to contain Predator malware through social media replies, particularly on Twitter or X posts made by officials, journalists, and members of civil society has been discovered. They have been identified as REPLYSPY. It is strongly believed that REPLYSPY included Cytrox Predator infection links in replies to various US and international officials and others.

If a user were to click on one of these links and pass a validation procedure, their device would likely be infected with Cytrox's Predator spyware, potentially through a series of undiscovered vulnerabilities (zero-day exploits). Cytrox is a subsidiary of the surveillance conglomerate Intellexa. Some of the validation steps include Process Checks, Checking for Log Monitoring, Location Check, Developer Mode Check, Jailbreak detection, and Proxy Check.

Threat Protected: 02
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity
Kill Chain: Initial Access T1189/T1566 - Execution T1623/T1575 - Command-and-Control T1437 - Exfiltration T1639

3. MataDoor Malware

In October 2022, while investigating an incident at a Russian industrial enterprise, new and sophisticated malware came to light. Named MataDoor, this complex modular backdoor was uncovered, and designed for covert, long-term operations. The initial attack likely originated from a phishing email with an attached DOCX document, exploiting the CVE-2021-40444 vulnerability. Similar emails targeting Russian defence industry enterprises were sent in August-September 2022, all designed to lure recipients into enabling document editing. Attributing these attacks is challenging, as the Dark River group customises each campaign for specific targets, employing a separate network infrastructure for each attack. The MataDoor backdoor is a central tool, that is demonstrating advanced development. Russian defence industry entities remain prime targets, facing increasingly intricate espionage and data theft attempts, exemplified by the Dark River group's activities.

Threat Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity
Kill Chain: Initial Access T1566.001 - Execution T1106/T1129 - Persistence T1543.003 - Defence Evasion T1622/T1140 - Collection T1005 - Command-and-Control T1071/T1132

4. Ursnif Malware

Ursnif, also known as Gozi, Gozi-ISFB, Dreambot, Papras, or Snifula, is a notorious banking trojan and spyware. In 2020, it ranked as the second-most active malware strain, responsible for over 30% of detections. This malware's history dates to 2000, making it one of the oldest in existence. Frequent public disclosures have led to numerous variants. It is a top concern for the US government's CISA. Ursnif gains initial access via email attachments, malicious sites, or trojanised apps. An ingenious tactic involves using stolen email credentials to inject malicious attachments into ongoing conversations. Once triggered, Ursnif steals credentials, connects to a command-and-control server, and downloads additional modules. Recent Ursnif versions employ Living Off the Land Binaries (LOLBins) and Google Drive URLs for stealth. It encrypts its payload in password-protected ZIP files.

Capabilities include:

a. Gathering data and credentials from email, browsers, and FTP clients
b. Stealing keystrokes, screenshots, and clipboard data
c. Modifying browser traffic for credential theft
d. Uploading and downloading files
e. Establishing remote desktop access
f. Dynamic domain generation to avoid detection and blocking

Threat Protected: 03
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity
Kill Chain: Initial Access T1566.001 - Execution T1547.001/T1543.003/T1047 - Persistence T147.001/T1543.003 - Privilege Escalation T1055.004/T1055.004 - Collection T1115 - Command-and-Control T1071.001 - Exfiltration T1041

Known exploited vulnerabilities (Week 2 October 2023):

Vulnerability	Description
CVE-2023-44487	HTTP/2 Rapid Reset Attack Vulnerability
CVE-2023-36563	Microsoft WordPad Information Disclosure Vulnerability
CVE-2023-41763	Microsoft Skype for Business Privilege Escalation Vulnerability
CVE-2023-20109	Cisco IOS and IOS XE Group Encrypted Transport VPN Out-of-Bounds Write Vulnerability
CVE-2023-21608	Adobe Acrobat and Reader Use-After-Free Vulnerability

Updated Malware Signatures (Week 2 October 2023)

Threat	Description
Zusy	Zusy, alternatively referred to as TinyBanker or Tinba, is a trojan specifically designed to engage in man-in-the-middle attacks with the intention of pilfering banking data. Upon execution, it inserts itself into legitimate Windows processes like "explorer.exe" and "winver.exe." As the user visits a banking site, Zusy deceitfully presents a fraudulent form, aiming to deceive the user into providing personal information.
Gh0stRAT	Gh0stRAT is a widely recognised group of remote access trojans strategically crafted to grant an assailant full authority over a compromised system. Its functionalities encompass monitoring keystrokes, capturing video via the webcam, and deploying subsequent malware. The source code of Gh0stRAT has been openly accessible on the internet for an extended period, substantially reducing the hurdle for malicious actors to adapt and employ the code in fresh attack endeavours.
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
Tofsee	A malware that is used to send spam emails, conduct click frauds as well as cryptomining.

New Ransomware Victims Last Week: 76

Red Piranha proactively gathers information about organisations impacted by ransomware attacks through various channels, including the Dark Web. In the past week, our team identified a total of 76 new ransomware victims or updates in the few past victims from 19 distinct industries across 22 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

Alphv, a specific ransomware, has affected the largest number of victims (10) updates spread across various countries. NoEscape and Play ransomware groups updated 8 & 7 victims, respectively. Below are the victim counts (%) for these ransomware groups and a few others.

Name of Ransomware Group	Percentage of new Victims last week
8Base	5.26%
Akira	1.32%
Alphv	13.16%
Arvinclub	1.32%
Bianlian	3.95%
Black Suit	1.32%
Blackbasta	3.95%
Cactus	1.32%
Cuba	1.32%
Inc Ransom	3.95%
Knight	5.26%
Lockbit3	9.21%
Medusa	3.95%
Money Message	1.32%
Monti	1.32%
NoEscape	10.53%
Play	9.21%
Qilin	1.32%
Ragnarlocker	2.63%
Ransomed	11.84%
Ransomhouse	1.32%
Rhysida	1.32%
Snatch	1.32%
Trigona	2.63%

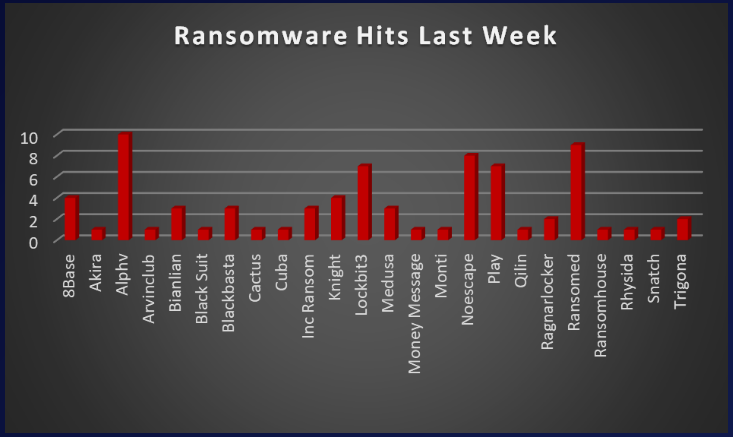

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 22 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 30 victims updates last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Argentina	1.32%
Australia	1.32%
Austria	1.32%
Belgium	1.32%
Brazil	3.95%
Bulgaria	7.89%
Canada	6.58%
France	2.63%
Germany	1.32%
India	2.63%
Israel	1.32%
Italy	6.58%
Norway	1.32%
Peru	1.32%
Shiraz	1.32%
Somalia	1.32%
South Africa	2.63%
Spain	2.63%
Turkey	2.63%
UAE	1.32%
UK	7.89%
USA	39.47%

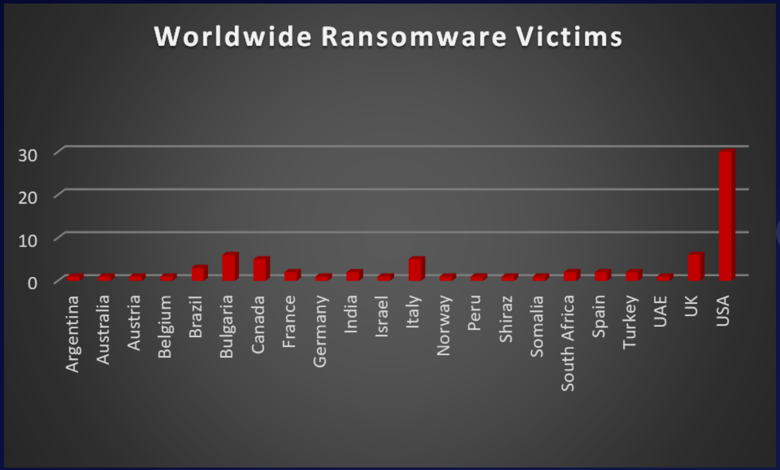

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 19 industries globally. Last week, the Manufacturing and Hospitality sectors were hit particularly hard, with 16% and 12% of the total ransomware victims belonging to each of those sectors respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Business Services	10.53%
Construction	3.95%
Consumer Services	1.32%
Cultural	1.32%
Education	7.89%
Finance	1.32%
Government	2.63%
Healthcare	5.26%
Hospitality	5.26%
Insurance	1.32%
IT	6.58%
Legal Services	3.95%
Manufacturing	23.68%
Metals & Mining	1.32%
Organizations	2.63%
Real Estate	3.95%
Retail	11.84%
Telecom	1.32%
Transportation	3.95%

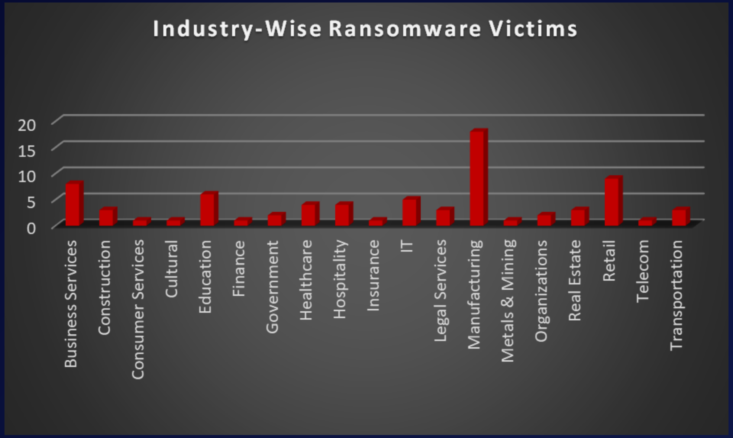

Figure 3: Industry-wise Ransomware Victims