
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Oct 17 - 23, 2023

Report Summary:

- **New Threat Detection Added** – 4 (DarkWatchman RAT, MataDoor Malware, Fake Chrome Landing Pages, and Cisco IOS XE Web Server Implant (CVE-2023-20198))
- **New Threat Protections - 11**
- **New Ransomware Victims Last Week - 55**

Newly Detected Threats Added

1. DarkWatchman RAT

A phishing site mimicking the reputable Russian platform has surfaced, facilitating the distribution of the potent DarkWatchman RAT. This malware, though lightweight, grants attackers remote control over compromised devices. Initially discovered in 2021, the deceptive website primarily targets Russian users. It tricks visitors into downloading a malicious file, providing a false sense of security with a password for extraction. Unpacking reveals two executable files in Russian, implying a localised focus. The executable file drops DarkWatchman RAT, initiating various activities on the host machine. This includes depositing an encrypted keylogger, saving stolen data in the Windows registry to avoid detection, and showcasing advanced, fileless malware tactics. Protecting against such threats demands a multi-layered security approach, including firewalls, behaviour-based anti-malware tools, and endpoint security solutions.

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: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1129 - Persistence T1543 - Defence Evasion T1622 - Collection T1005 - Command-and-Control T1132

2. MataDoor Malware

In October 2022, an investigation into an incident at a Russian industrial enterprise unearthed novel malware on compromised computers. These malicious files bore names resembling legitimate software on the infected machines, with some having valid digital signatures. Themida protector was employed to obscure and toughen their detection. Further analysis revealed a sophisticated, modular backdoor named MataDoor, built for covert, long-term operations. The Dark River group employed MataDoor in targeted, difficult-to-attribute attacks, typically initiated through phishing emails with relevant DOCX documents containing CVE-2021-40444 exploits. Similar tactics were noted in prior attacks on Russian defence industry entities. This underscores the ongoing and escalating sophistication of espionage and data theft in these sectors.

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 - Execution T1543.003/T1047 - Persistence T147.001 - Privilege Escalation T1055.004 - Collection T1115 - Command-and-Control T1071.001

3. Fake Chrome Landing Pages

Red Piranha has added known domains imitating Chrome's landing pages that have been identified.

Threat Protected: 06
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

4. Cisco IOS XE Web Server Implant (CVE-2023-20198)

The implant was in "/usr/binos/conf/nginx-conf/cisco_service.conf" and consisted of two variable strings represented in hexadecimal characters. Notably, it was non-persistent, meaning it would be deleted upon a device reboot. However, the newly established local user accounts continued to remain active even after reboots, each with level 15 privileges, granting complete administrator access to the device. This elevated access to the devices and the subsequent creation of new users was designated as CVE-2023-20198.

Upon successfully exploiting CVE-2023-20198, attackers could leverage another component of the WebUI feature for command injection with elevated (root) privileges to write the implant to the file system, referring to CVE-2023-20273.

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 T1566

Known exploited vulnerabilities (Week 3 October 2023):

Vulnerability	Description
CVE-2023-20198	Cisco IOS XE Web UI Privilege Escalation Vulnerability
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability
CVE-2021-1435	Cisco IOS XE Web UI Command Injection Vulnerability

Updated Malware Signatures (Week 3 October 2023)

Threat	Description
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
Agent Tesla	AgentTesla is a remote access trojan designed to log keystrokes and make efforts to pilfer sensitive data from web browsers and other installed software applications.
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.
Tofsee	A malware that is used to send spam emails, conduct click frauds and cryptomining.
DarkKomet	A remote access trojan that can take full control over an infected machine.

New Ransomware Victims Last Week: 55

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 55 new ransomware victims or updates in the few past victims from 17 distinct industries across 14 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit3.0, a specific ransomware, has affected the largest number of victims (9) updates spread across various countries. Blackbasta and Alphv ransomware groups updated 8 & 6 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
0Mega	1.82%
Akira	9.09%
Alphv	10.91%
Arvinclub	3.64%
Bianlian	7.27%
Black Suit	1.82%
Blackbasta	14.55%
Cactus	3.64%
Inc Ransom	3.64%
Lockbit3	16.36%
Medusa	9.09%
Monti	1.82%
Noescape	5.45%
Play	1.82%
Ransomed	3.64%
Rhysida	1.82%
Snatch	3.64%

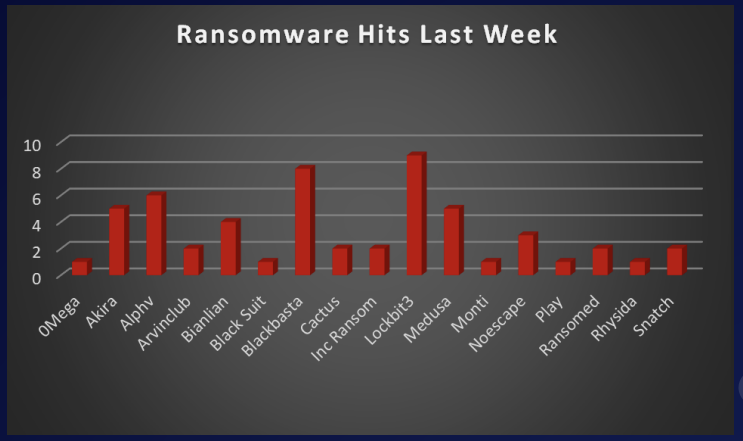

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 14 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
Belgium	1.82%
Brazil	1.82%
Canada	3.64%
China	1.82%
France	7.27%
Iran	1.82%
Italy	7.27%
Japan	1.82%
Mexico	1.82%
Norway	1.82%
Somalia	1.82%
UAE	1.82%
UK	10.91%
USA	54.55%

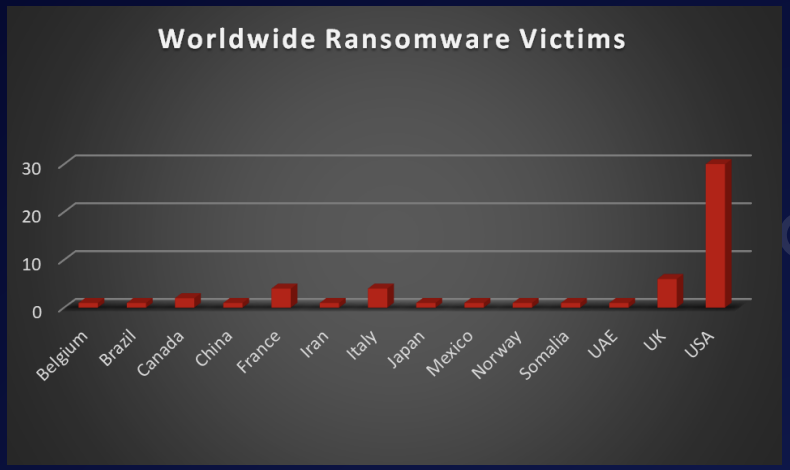

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 17 industries globally. Last week, the Business Services and Retail sectors were hit particularly hard, with 16% and 10% 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	16.36%
Construction	3.64%
Consumer Services	1.82%
Education	5.45%
Electricity, Oil & Gas	3.64%
Energy, Utilities & Waste Treatment	3.64%
Finance	1.82%
Government	1.82%
Healthcare	3.64%
Hospitality	3.64 %
IT	7.27 %
Legal Services	7.27%
Manufacturing	9.09%
Media & Internet	1.82%
Organisations	12.73%
Retail	10.91%
Telecom	5.45%

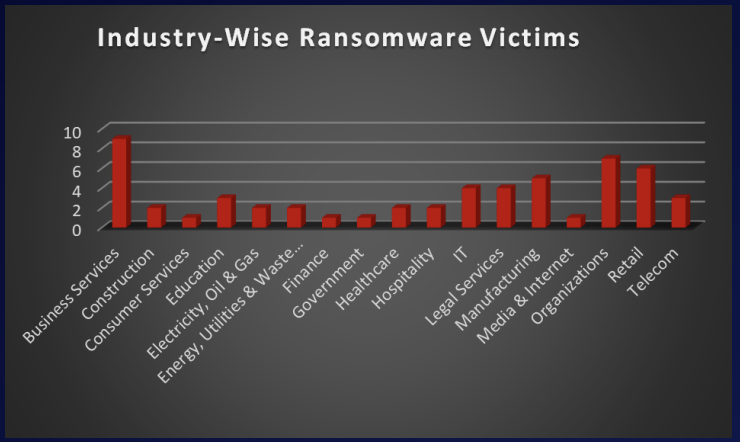

Figure 3: Industry-wise Ransomware Victims