Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 15 - 21, 2023

Report Summary:

- **New Threat Detection Added** – 4 (Duke Malware, NetSupport RAT, JanelaRAT, and QwixxRAT)
- **New Threat Protections**
- **New Ransomware Victims Last Week - 126**

Newly Detected Threats Added

1. Duke Malware

Duke, a malware toolkit used by the APT29 group, also known as The Dukes, Cloaked Ursa, CozyBear, Nobelium, and UNC2452. APT29 is a Russian state-sponsored actor linked to SVR RF, engaging in politically motivated cyber espionage. Duke malware includes backdoors, loaders, data stealers, and disruptors. In 2023, The Dukes used malicious PDFs posing as German embassy invitations in a spam campaign targeting NATO-aligned Foreign Affairs ministries.

Threat Protected: 05
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain: Execution T1047- Defence Evasion TA0005/T1036 - Credential Access TA0006 -Discovery T1018 - Collection T1005 - Command-and-Control TA0011

2. NetSupport RAT

Experts found an ongoing scheme that tricks people with fake Chrome updates, getting them to install a tool called NetSupport Manager. Bad actors then misuse this tool to steal data and control victims' computers. This scheme is somewhat similar to the earlier SocGholish campaign, possibly linked to Russian threats. But the connection to SocGholish is not certain, and they are using different tools.

Threat Protected: 04
Rule Set Type:

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

Class Type: Trojan- Activity
Kill Chain: Initial Access T1566 - Execution T1059 - Collection T1119/T1005/T1185 - Command-and-Control T1132 - Exfiltration T1041

3. JanelaRAT

A targeted threat campaign named JanelaRAT has been recently discovered. It appears to be aimed at FinTech users in the LATAM region. Employing tactics like DLL side-loading, dynamic C2 infrastructure, and a multi-stage approach, the campaign utilises a customised BX RAT variant, leading to the naming of the malware as JanelaRAT. Notably, JanelaRAT focuses on harvesting financial data in LATAM, incorporates a Windows titles sensitivity feature, employs dynamic socket configuration, exploits legitimate sources for DLL side-loading evasion, and exhibits Portuguese-language indicators, highlighting the origin of the threat actor.

The initiation of the attack chain is executed through a VBScript, enclosed within ZIP archives. The VBScript undertakes two primary actions: retrieving a ZIP archive from the attackers' server and depositing a BAT file on the targeted endpoint to prime the system for the subsequent infection stage. Enclosed within the ZIP archive are two components responsible for orchestrating the ensuing stages of infection, facilitating DLL side-loading.

JanelaRAT is designed to gather and transmit data regarding the compromised host to the attacker.

Threat Protected: 01
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain: Execution T1059 - Persistence T1574 - Command-and-Control T1095 - Exfiltration T1041

4. QwixxRat

A new threat has emerged under the name QwixxRAT, posing risks to both enterprises and individual users. This Trojan enters systems discreetly, extending its reach to extract a wide array of data. It was seen in early August 2023. The malicious tool is being extensively propagated by the threat actor through platforms like Telegram and Discord.

Upon successful installation on victim Windows devices belonging to, the RAT adeptly gathers sensitive information, which is subsequently dispatched to the attacker's Telegram bot, granting unauthorised access to the victim's confidential data.

To elude detection by antivirus software, the RAT utilises command and control capabilities through a Telegram bot. This mechanism empowers the attacker to remotely oversee the RAT's actions and administer its functions.

Threat Protected: 01
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain: Initial Access T1190 - Execution T1059 - Command-and-Control T1102/T1071

Known exploited vulnerabilities (Week 3 August 2023):

Vulnerability	Description
CVE-2023-24489	Citrix Content Collaboration ShareFile Improper Access Control Vulnerability

Updated Malware Signatures (Week 3 August 2023)

Threat	Description
Valyria	A Microsoft Word-based malware which is used as a dropper for second-stage malware.
Tofsee	A malware that is used to send spam emails, conduct click frauds as well as cryptomining.
Ramnit	A banking trojan used to steal online banking credentials
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
XtremeRAT	A remote access trojan interacts with the infected machine via a remote shell, uploads/downloads files, and records from a webcam/microphone.

New Ransomware Victims Last Week: 126

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 126 new ransomware victims from 21 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.

Clop, a specific ransomware, has affected the largest number of new victims (41) spread across various countries. LockBit3.0 and Blackbasta hit 22 & 20 new 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	3.17%
Akira	3.97%
AlphV	3.97%
Bianlian	1.59%
Blackbasta	15.87%
Clop	32.54%
Clop Torrents	3.17%
Everest	1.59%
INC Ransom	0.79%
LockBit3.0	17.46%
Medusa	2.38%
Metaencryptor	8.73%
Noescape	3.97%
Rhysida	0.79%

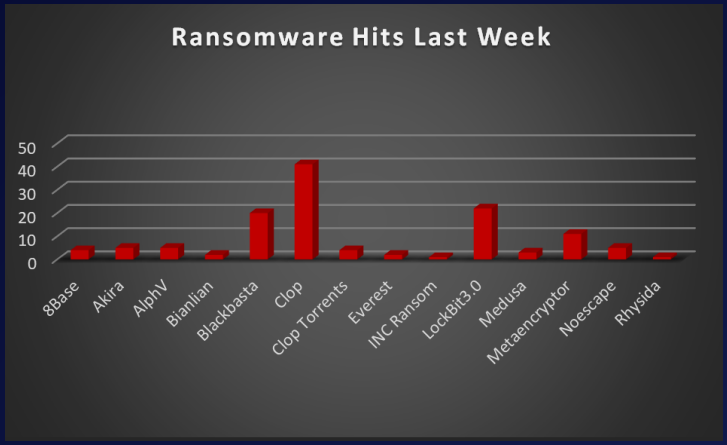

Figure 1: Ransomware Group Hits Last Week

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 71 new victims reported last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Argentina	0.79%
Australia	2.38%
Austria	1.59%
Belgium	2.38%
Brazil	1.59%
Canada	3.17%
China	0.79%
France	0.79%
Germany	9.52%
Hong Kong	0.79%
Ireland	0.79%
Italy	2.38%
Japan	0.79%
Luxembourg	0.79%
Netherlands	2.38%
Portugal	1.59%
Qatar	0.79%
South Africa	1.59%
Thailand	1.59%
UAE	1.59%
UK	5.56%
USA	56.35%

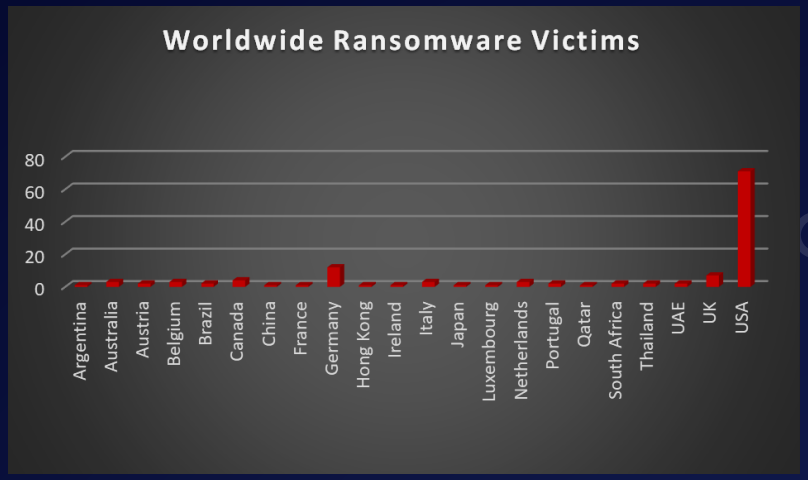

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 21 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with 17% and 15% 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 (%)
Banking	1.59%
Business Services	15.87%
Construction	7.94%
Consumer Services	2.38%
Education	6.35%
Electricity, Oil & Gas	1.59%
Energy, Utilities & Waste Treatment	0.79%
Finance	6.35%
Government	2.38%
Healthcare	2.38%
Hospitality	0.79%
Insurance	4.76%
IT	9.52%
Legal Services	2.38%
Manufacturing	17.46%
Media & Internet	2.38%
Organisation	3.17%
Real Estate	0.79%
Retail	6.35%
Telecom	3.17%
Transportation	1.59%

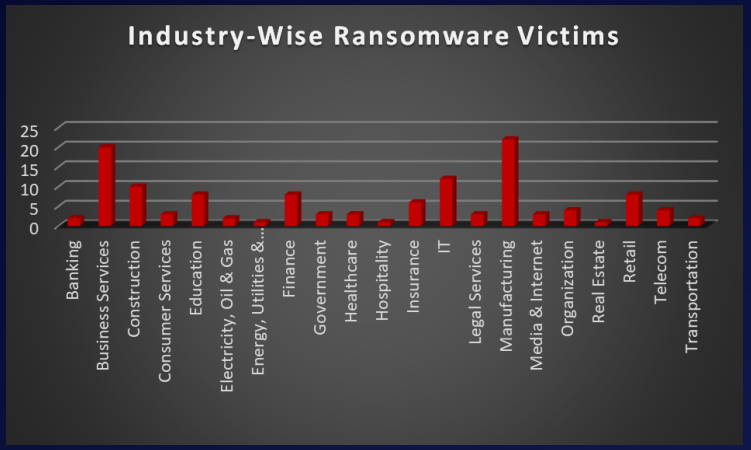

Figure 3: Industry-wise Ransomware Victims