Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 19 - 25, 2023

Report Summary:

- **New Threat Detection Added** – 3 (Sandman APT, Stately Taurus APT, and Earth Lusca APT)
- **New Threat Protections - 6**
- **New Ransomware Victims Last Week - 105**

Newly Detected Threats Added

1. Sandman APT

Researchers observed a new threat activity cluster in August 2023 targeting the telecommunication sector. The activities were carried out by a threat actor of unknown origin using a novel modular backdoor based on the LuaJIT platform. The threat actor and the backdoor were dubbed Sandman and LuaDream, respectively, about the suspected internal name – DreamLand client. The observed activities were characterized by strategic lateral movement to specific targeted workstations and minimal engagement, suggesting a deliberate approach to achieve objectives while minimising detection risk. LuaDream's implementation and architecture suggested a maintained, versioned project under active development. It is a modular, multi-protocol backdoor with core functionalities including exfiltrating system and user information and managing attacker-provided plugins for extended features. Identifying 36 distinct LuaDream components and support for multiple C2 communication protocols indicated a considerable-scale project. The LuaDream staging chain was designed to evade detection and thwart analysis by deploying malware directly into memory, leveraging the LuaJIT platform to make malicious Lua script code hard to detect.

Threat Protected: 03
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 T1129 - Defence Evasion T1027/T1497 - Discovery T1018/1082/T1497

2. Stately Taurus APT

A cyber espionage group, likely Stately Taurus, carried out persistent attacks on a Southeast Asian government from mid-2021 to late 2023. They infiltrated networks, stealing sensitive documents and files. We are moderately to highly confident that this activity is linked to the Chinese cyber espionage group Stately Taurus, also known as Mustang Panda, BRONZE PRESIDENT, TA416, RedDelta, and Earth Preta. It has previously observed this group targeting Southeast Asia. This attribution is supported by their use of unique, rarely seen tools like the ToneShell backdoor, not associated with any other known threat actor.

Threat Protected: 02
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: Execution T1129 - Defence Evasion T1622 - Discovery T1622

3. Earth Lusca APT

Throughout the initial part of 2023, the Earth Lusca APT group has concentrated their assaults on nations in the Southeast Asia, Central Asia, and extending to countries in Latin America and Africa. The group is primarily focused on governmental entities engaged in foreign affairs, technology, and telecommunications. They have escalated their efforts honing in on the exposed servers of its targets. There is a noticeable trend of them consistently exploiting 0-day vulnerabilities in servers.

The SprySOCKS Trojan incorporates various conventional backdoor commands. These include gathering system information, initiating an interactive shell, enumerating network connections, establishing a SOCKS proxy, as well as uploading and downloading files. It also supports fundamental file operations such as listing, deleting, renaming, and creating directories.

Threat Protected: 01
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 T1190 - Execution T1059 - Collection T1005 - Command-and-Control T1090

Known exploited vulnerabilities (Week 4 September 2023):

Vulnerability	Description
CVE-2022-31463	Owl Labs Meeting Owl Improper Authentication Vulnerability
CVE-2022-31462	Owl Labs Meeting Owl Use of Hard-coded Credentials Vulnerability
CVE-2022-31461	Owl Labs Meeting Owl Missing Authentication for Critical Function Vulnerability
CVE-2022-31459	Owl Labs Meeting Owl Inadequate Encryption Strength Vulnerability
CVE-2021-3129	Laravel Ignition File Upload Vulnerability
CVE-2017-6884	Zyxel EMG2926 Routers Command Injection Vulnerability
CVE-2014-8361	Realtek SDK Improper Input Validation Vulnerability
CVE-2022-22265	Samsung Mobile Devices Use-After-Free Vulnerability
CVE-2023-28434	MinIO Security Feature Bypass Vulnerability
CVE-2023-41179	Trend Micro Apex One and Worry-Free Business Security Remote Code Execution Vulnerability

Updated Malware Signatures (Week 4 September 2023)

Threat	Description
Bifrost	A remote access trojan that enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
HawkEye	A trojan and keylogger used to steal various account credentials.

New Ransomware Victims Last Week: 105

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 115 new ransomware victims or updates in a few past victims from 20 distinct industries across 31 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 (30) updates spread across various countries. Ciphbit and AlphV updated 13 & 11 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
3AM	8.57%
8Base	0.95%
Akira	1.90%
AlphV	10.48%
Bianlian	1.90%
BlackByte	0.95%
Cactus	3.81%
Ciphbit	12.38%
Donutleaks	1.90%
Everest	0.95%
Inc Ransom	2.86%
Karakurt	0.95%
Knight	0.95%
LockBit3.0	28.57%
Medusa	2.86 %
Monti	1.90%
Noescape	4.76%
Play	5.71 %
Ransomhouse	1.90%
Rhysida	0.95%
Snatch	2.86%
Trigona	1.90%

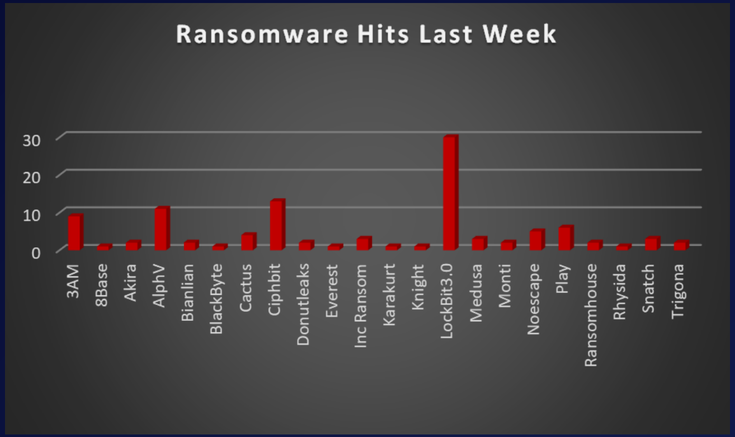

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 31 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 50 victims reported last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Angola	0.95%
Australia	1.90%
Austria	0.95%
Belgium	0.95%
Brazil	0.95%
Bulgaria	0.95%
Canada	4.76%
China	0.95%
Czech Republic	0.95%
France	1.90%
Germany	6.67%
India	0.95%
Indonesia	0.95%
Israel	3.81%
Japan	0.95%
Mexico	0.95%
New Zealand	1.90%
Norway	0.95%
Poland	0.95%
Portugal	0.95%
Saudi Arabia	0.95%
Singapore	1.90%
Slovakia	0.95%
South Africa	0.95%
South Korea	0.95%
Spain	2.86%
Switzerland	0.95%
Turkey	2.86 %
UAE	1.90%
UK	3.81%
USA	47.62%

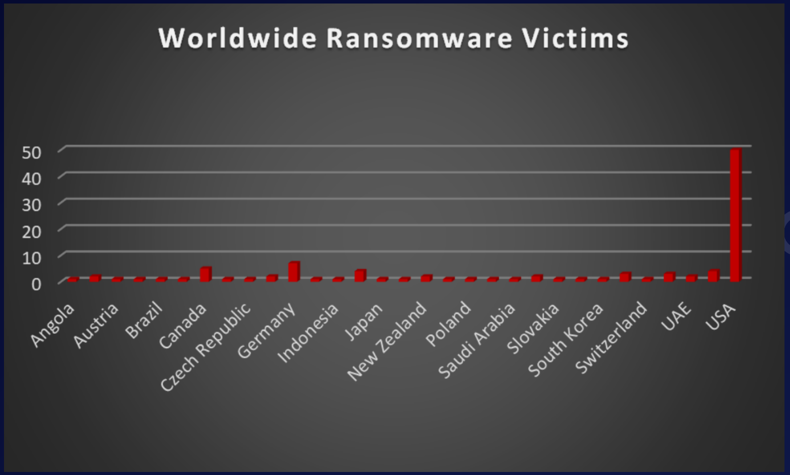

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 20 industries globally. Last week, the Manufacturing and Construction sectors were hit particularly hard, with 18% 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 (%)
Agriculture	0.95%
Business Services	6.67%
Construction	15.24%
Consumer Services	1.90%
Education	5.71%
Electricity, Oil & Gas	0.95%
Finance	6.67%
Government	3.81%
Healthcare	3.81%
Hospitality	4.76%
IT	0.95%
Legal Services	5.71%
Manufacturing	18.10%
Media & Internet	2.86%
Metals & Mining	0.95%
Organisation	0.95%
Real Estate	1.90%
Retail	10.48%
Telecom	3.81%
Transportation	3.81%

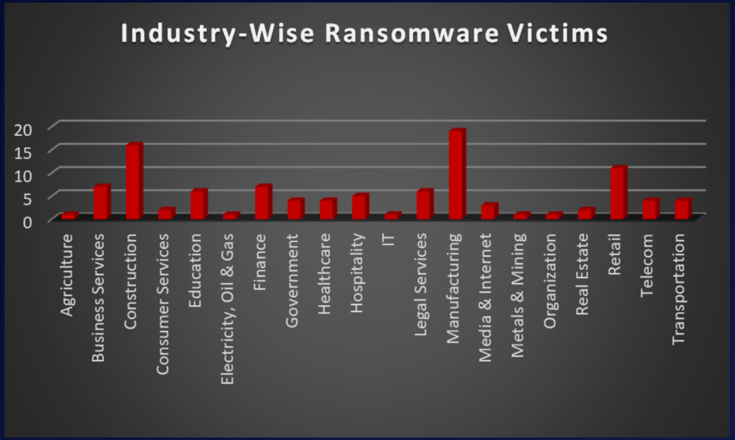

Figure 3: Industry-wise Ransomware Victims