
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Sept 26 - Oct 02, 2023

Report Summary:

- **New Threat Detection Added** – 2 (Lu0Bot Malware and AtlasAgent Malware)
- **New Threat Protections - 7**
- **New Ransomware Victims Last Week - 147**

Newly Detected Threats Added

1. Lu0Bot Malware

Cybersecurity experts recently examined a Lu0Bot malware sample based on Node.js, which completely hijacks a victim's computer. This Node.js malware, initially, believed to be a basic DDOS bot, turned out to be more complex. Node.js is a runtime environment used in modern web apps. Lu0Bot first appeared in February 2021 as a GCleaner second-stage payload, acting as a bot that awaits commands from a C2 server and sends encrypted system data. While its activity is limited, its creative use of Node.js makes it stand out, potentially posing risks if its campaign expands and the server becomes active.

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 1053/T1059/T1064/T1106/T1129 - Persistence T1053 - Privilege Escalation T1053/T1134 - Defence Evasion T1006/T1064 - Discovery T1012/T1016 - Collection T1560 - Command-and-control T1071/T1095 - Impact T1529

2. AtlasAgent Malware

AtlasAgent is a Trojan with a sinister agenda – it is designed to infiltrate a host system, gather sensitive data, impede the concurrent operation of multiple programs, inject specific shellcodes, and fetch files from Command-and-Control servers. This malicious software is built as a DLL application using the C++ programming language. Once inside a system, AtlasAgent becomes an information scavenger, hunting for details like the computer's Guid number, local computer name, adapter specifics, network card info, operating system version, local IP address, and process ID. It then takes action based on instructions from a control terminal, often executing shellcode to carry out various tasks. These actions can have dire consequences, including data theft, system compromise, performance issues, and privacy invasion, making AtlasAgent a significant cybersecurity menace.

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: Initial Access T1190 - Execution T1059 - Collection T1005 - Command-and-Control T1090

Known exploited vulnerabilities (Week 5 September 2023):

Vulnerability	Description
CVE-2023-41993	Apple Multiple Products WebKit Code Execution Vulnerability
CVE-2023-41992	Apple Multiple Products Kernel Privilege Escalation Vulnerability
CVE-2023-41991	Apple Multiple Products Improper Certificate Validation Vulnerability
CVE-2018-14667	Red Hat JBoss RichFaces Framework Expression Language Injection Vulnerability

Updated Malware Signatures (Week 5 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.
Upatre	Upatre is also a malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.
Ramnit	A banking trojan used to steal online banking credentials.

New Ransomware Victims Last Week: 147

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 147 new ransomware victims or updates in a few past victims from 21 distinct industries across 23 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LostTrust, a specific ransomware group, has affected the largest number of victims (53) updates spread across various countries. Alphv and Ransomed ransomware groups updated 16 & 12 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	0.68%
8Base	5.44%
Akira	2.72%
Alphv	10.88%
Bianlian	2.72%
Cactus	2.72%
Clop	0.68%
Dunghill	2.04%
Inc Ransom	0.68%
Karakurt	0.68%
Knight	0.68%
Lockbit3	4.76%
LostTrust	36.05%
Mallox	0.68%
Medusa	2.72%
Noescape	4.08%
Play	6.80%
Qilin	0.68%
Ragnarlocker	2.72%
Ransomed	8.16%
Rhysida	2.04%
Stormous	1.36%

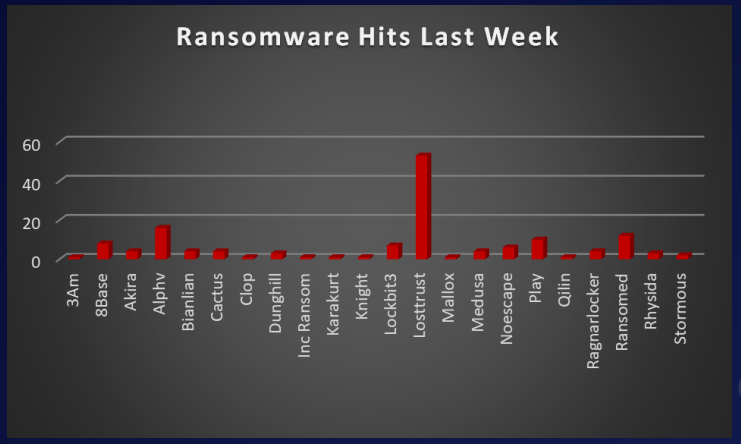

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 23 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 87 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	0.68%
Bulgaria	4.76%
Canada	4.08%
Colombia	0.68%
Florida	0.68%
France	2.04%
Germany	2.72%
Italy	4.08%
Japan	2.72%
Kuwait	0.68%
Mexico	0.68%
Netherlands	2.04%
Peru	0.68%
Philippines	1.36%
Poland	0.68%
Portugal	0.68%
Romania	0.68%
Spain	0.68%
Sweden	1.36%
Thailand	0.68%
UAE	0.68%
UK	7.48%
USA	59.18%

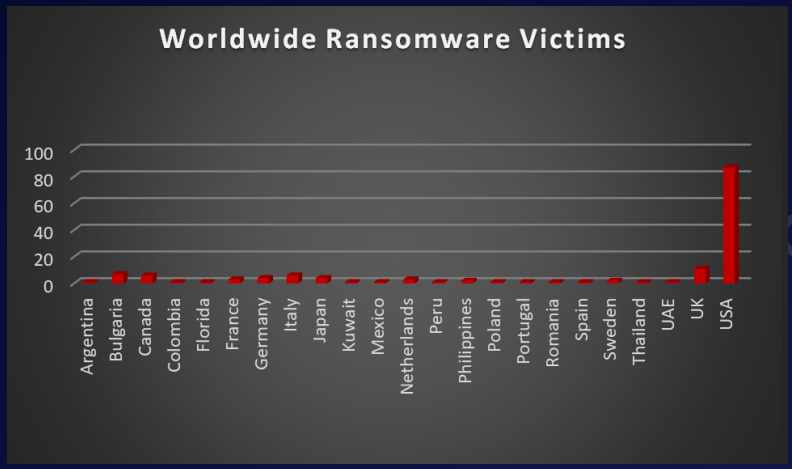

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 21 industries globally. Last week, the Business Services and Manufacturing sectors were hit particularly hard, with 14% and 13% 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	1.36%
Business Services	14.97%
Construction	12.24%
Consumer Services	4.76%
Education	4.76%
Electricity, Oil & Gas	0.68%
Energy, Utilities & Waste Treatment	0.68%
Finance	2.04%
Government	3.40%
Healthcare	5.44%
Hospitality	4.08%
Insurance	0.68%
IT	2.04%
Legal Services	4.76%
Manufacturing	13.61%
Media & Internet	0.68%
Organisations	4.08%
Real Estate	2.04%
Retail	10.88%
Telecom	1.36%
Transportation	5.44%

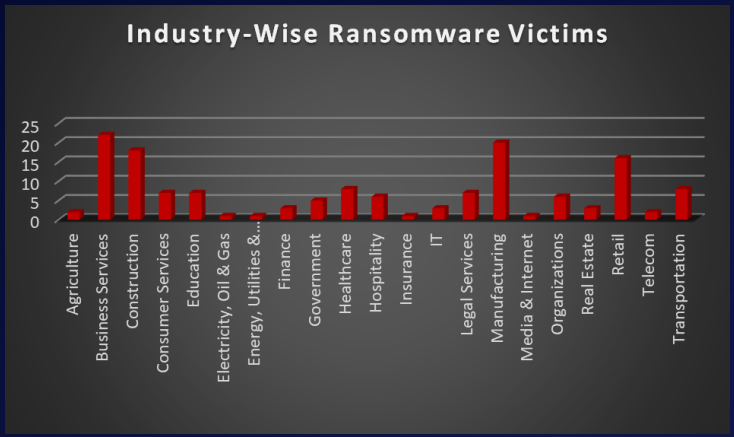

Figure 3: Industry-wise Ransomware Victims