Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Feb 06 - 12, 2024

Report Summary:

- **New Threat Detection Added** – 4 (PennyWise Stealer, XWorm RAT, FormBook Malware and Ivanti Multiple Products SSRF (CVE-2024-21893))
- **New Threat Protections - 93**
- **New Ransomware Victims Last Week - 85**

Newly Detected Threats Added

1. PennyWise Stealer

The PennyWise stealer has re-emerged in the cyber landscape with its updated version, v1.2, distributed through the #PureCrypter downloader. This malicious software is designed to pilfer sensitive information from infected computers, including login credentials, credit card details, social security numbers, and personal data. Once infiltrated, PennyWise may target online accounts, such as email, social media, and banking, compromising usernames and passwords. It can also harvest credit card information, birthdates, and home addresses. This malware may record keystrokes, monitor browsing history, and collect system data. Stolen information facilitates identity theft, financial fraud, and unauthorised access to personal accounts. Users should exercise caution, especially with email attachments, malicious links, and software downloads, to prevent malware infections.

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:

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
Defence Evasion	T1140	Deobfuscate/Decode Files or Information
	T1497	Virtualisation/Sandbox Evasion
	T1055.012	Process Injection: Process Hollowing
Credential Access	T1555	Credentials from Password Stores
	T1539	Steal Web Session Cookies
	T1552	Unsecured Credentials
	T1528	Steal Application Access Token
Collection	T1113	Screen Capture
Discovery	T1518	Software Discovery
	T1124	System Time Discovery
	T1007	System Service Discovery
Command-and-Control	T1071	Application Layer Protocol
Exfiltration	T1041	Exfiltration Over C2 Channel

2. XWorm RAT

Researchers have identified a malicious email campaign deploying the XWorm RAT, a .Net-based malware. The campaign employs embedded URLs as entry points, redirecting to a multilayer distribution with obfuscated PowerShell codes. This leads to the delivery of XWorm, utilising both "XWormV2.1" and "XWormV3.1" malware. One payload involves cryptocurrency coin hijacking, replacing legitimate addresses with fraudulent ones, and facilitating theft. The crypto ID used matches a 2021 AgentTesla campaign, suggesting the same threat actors. XWorm RAT exhibits capabilities for both crypto theft and ransomware attacks, employing a sophisticated distribution method seen in past campaigns. Robust security measures are crucial against such persistent threats.

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:

Tactic	Technique ID	Technique Name
Execution	T1047	Windows Management Instrumentation
	T1106	Native API
	T1129	Shared Modules
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1027	Obfuscated Files or Information
	T1140	Deobfuscate/Decode Files or Information
	T1497	Virtualisation/Sandbox Evasion
	T1055	Process Injection
Credential Access	T1056	Input Capture
	T1056.001	Keylogging
Discovery	T1010	Application Window Discovery
	T1018	Remote System Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1497	Virtualisation/Sandbox Evasion
	T1056	Input Capture
Collection	T1056.001	Keylogging
	T1115	Clipboard Data
	T1560	Archive Collected Data
Command-and-Control	T1071	Application Layer Protocol
	T1095	Non-Application Layer Protocol
	T1571	Non-Standard Port

3. FormBook Malware

FormBook, discovered in 2016, is an infostealer malware with a broad range of capabilities. It pilfers data from infected systems, including browser-cached credentials, screenshots, and keystrokes. Additionally, it functions as a downloader, allowing the retrieval and execution of more malicious files. Operating as Malware as a Service (MaaS), FormBook is available for purchase by cybercriminals at a relatively low cost, providing them easy access to its destructive functionalities. This malware poses a significant threat due to its versatility and accessibility, highlighting the ongoing challenges in combating cyber threats. Users should remain vigilant to safeguard their systems against potential FormBook attacks.

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:

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059	Command and Scripting Interpreter
Persistence	T1574.002	DLL Side-Loading
Privilege Escalation	T1055	Process Injection
	T1134	Access Token Manipulation
Defence Evasion	T1027	Obfuscated Files or Information
	T1055	Process Injection
	T1112	Modify Registry
	T1134	Access Token Manipulation
	T1497	Virtualisation/Sandbox Evasion
Credential Access	T1003	OS Credential Dumping
Discovery	T1010	Application Window Discovery
	T1082	System Information Discovery
Collection	T1005	Data from Local System
	T1114	Email Collection
	T1115	Clipboard Data
	T1125	Video Capture
Command-and-Control	T1071	Application Layer Protocol
	T1095	Non-Application Layer Protocol
Impact	T1529	System Shutdown/Reboot

4. Ivanti Multiple Products SSRF (CVE-2024-21893)

A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.

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: Attempted-admin
Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application

Known exploited vulnerabilities (Week 2 February 2024):

Vulnerability	CVSS	Description
CVE-2024-21762	9.8 (Critical)	Fortinet FortiOS Out-of-Bound Write Vulnerability

Updated Malware Signatures (Week 2 February 2024)

Threat	Description
Valyria	A Microsoft Word-based malware which is used as a dropper for second-stage malware.
LokiBot	An information-stealer malware used to gather data from victims' machines such as stored account credentials, banking information and other personal data.
DarkKomet	A remote access trojan that can take full control over an infected machine.
Qakbot	A malware designed to acquire valuable data such as banking credentials and is also capable of stealing FTP credentials and spreading across a network by utilising SMB.

New Ransomware Victims Last Week: 85

The Red Piranha Team actively collects information on organisations globally affected by ransomware attacks from various sources, including the Dark Web. In the past week alone, our team uncovered a total of 85 new ransomware victims or updates on previous victims across 20 different industries spanning 24 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

LockBit3.0 ransomware group stands out as the most prolific, having updated a significant number of victims (24) distributed across multiple countries. In comparison, Play and 8Base ransomware groups updated 13 and 11 victims, respectively, in the past week. The following list provides the victim counts in percentages for these ransomware groups and a selection of others.

Name of Ransomware Group	Percentage of new Victims last week
3Am	1.18%
8Base	12.94%
Abyss Data	2.35%
Akira	7.06%
Alphv	2.35%
Bianlian	8.24%
Black Suit	3.53%
Blackbasta	1.18%
Cactus	3.53%
Clop	1.18%
Cuba	1.18
Hunters	1.18%
Knight	3.53%
Lockbit3	28.24%
Medusa	1.18%
Meow	1.18%
Play	15.29%
Qilin	1.18%
Ransomhouse	2.35%
Stormous	1.18%

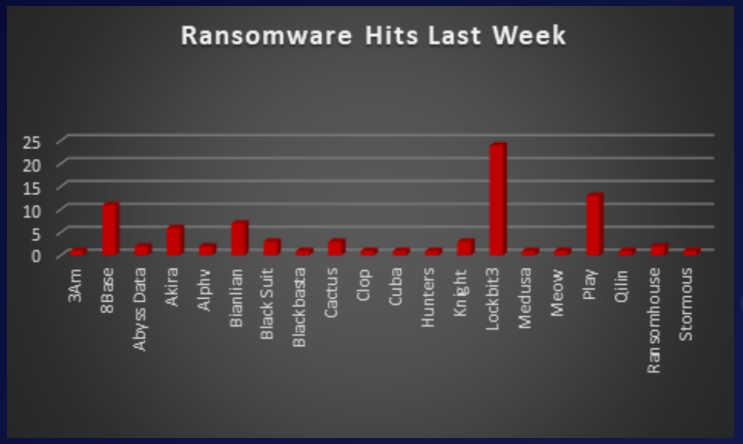

Figure 1: Ransomware Group Hits Last Week

In a comprehensive analysis of ransomware victims across 24 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 43 victim updates in the past week. The following list provides a breakdown of the number and percentage of new ransomware victims per country, underscoring the persistent and concerning prevalence of ransomware attacks, with the USA particularly susceptible to these cybersecurity threats.

Name of the affected Country	Number of Victims
Australia	1.18%
Austria	2.35%
Belgium	1.18%
Bolivia	1.18%
Brazil	1.18%
Canada	2.35%
Colombia	1.18%
Cyprus	1.18%
Egypt	1.18%
France	3.53%
Germany	3.53%
India	1.18%
Islands	1.18%
Italy	3.53%
Mexico	1.18%
Netherlands	1.18%
New Zealand	1.18 %
Portugal	1.18%
Singapore	1.18%
Spain	3.53%
Trinidad and Tobago	1.18%
UAE	1.18%
UK	11.76%
USA	50.59%

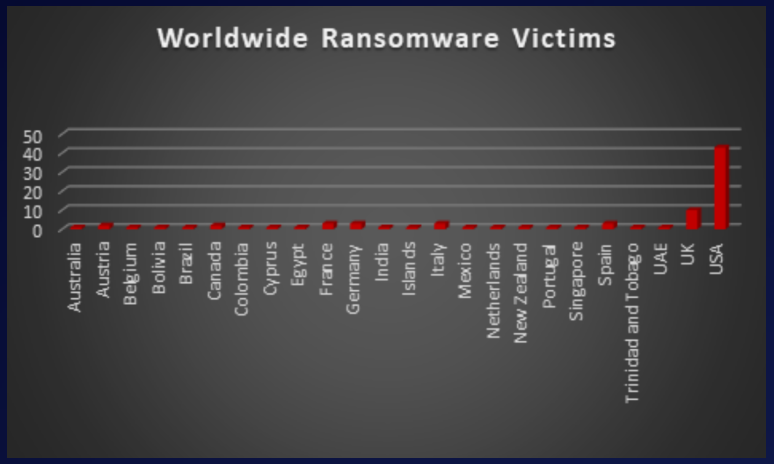

Figure 2: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 20 different industries worldwide. Notably, the Manufacturing and Business Services sectors bore the brunt of the attacks in the past week, accounting for 24% and 12% of the total ransomware victims, respectively. The table below delineates the most recent ransomware victims, organised by industry, shedding light on the sectors grappling with the significant impact of these cyber threats.

Industry	Victims Count (%)
Agriculture	1.18%
Business Services	12.94%
Cities, Towns & Municipalities	1.18%
Construction	10.59%
Consumer Services	2.35%
Education	1.18%
Energy, Utilities & Waste Treatment	1.18%
Finance	1.18%
Government	1.18%
Health Care	3.53%
Hospitality	4.71%
Insurance	1.18%
IT	1.18%
Legal Services	9.41%
Manufacturing	24.71%
Metals & Mining	1.18%
Organisations	1.18%
Retail	10.59%
Telecom	4.71%
Transportation	4.71%

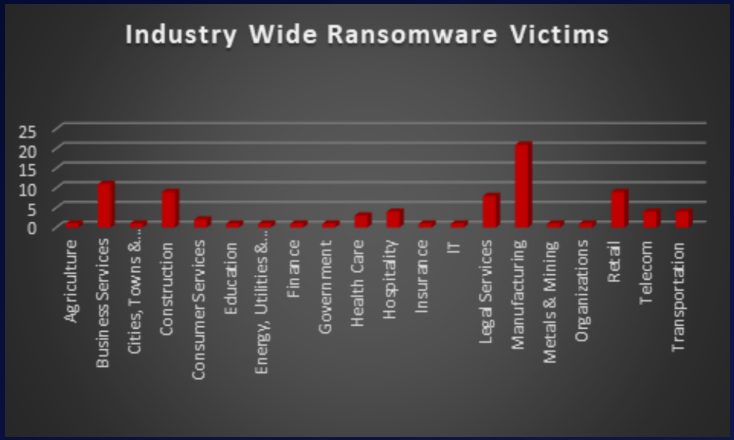

Figure 3: Industry-wide Ransomware Victims