Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Feb 13 - 19, 2024

Report Summary:

- **New Threat Detection Added** – 3 (Pikabot Malware, GandCrab Ransomware and Ivanti Connect Secure XXE Attempt (CVE-2024-22024))
- **New Threat Protections - 118**
- **New Ransomware Victims Last Week - 132**

Newly Detected Threats Added

1. Pikabot Malware

Pikabot is a new kind of harmful software. It's made up of three parts: a downloader/installer, a loader, and a backdoor component. Even though it's still new, it's showing some smart tricks to avoid detection and analysis. The loader part especially has tricky ways to hide and protect itself, drawing inspiration from a project called Al-Khaser. Pikabot also hides its payload using steganography. Plus, it has its own special way of communicating and can do lots of things like checking out a computer and injecting more bad stuff into it.

Rules Created: 03
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
Discovery	T1518.001 T1082	Security Software Discovery System Information Discovery
Command-and-Control	T1071	Application Layer Protocol
Exfiltration	T1041 T1095 T1105	Exfiltration Over C2 Channel Non-Application Layer Protocol Ingress Tool Transfer

2. GandCrab Ransomware

Since its discovery in 2018, GandCrab has evolved through five versions, causing havoc for individuals and companies. The creators are quick to adapt to defences, making it a persistent threat. The latest version, 5.1, targets global users but spares those from ex-USSR regions, identified by keyboard or language settings. This Windows-exclusive ransomware spreads through email spam or exploit kits, leading victims to a TOR website after encrypting files. Restoring data often requires paying a ransom, ranging from $1000 to $3000, though some victims report demands as high as $700,000. GandCrab operates as Ransomware-as-a-Service, allowing distribution to clients who customise ransom notes and share proceeds with the creators.

Rules Created: 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	T1129	Shared Modules
Defence Evasion	T1027	Obfuscated Files or Information
	T1027.005	Indicator Removal from Tools
	T1140	Deobfuscate/Decode Files or Information
	T1222	File and Directory Permissions Modification
	T1497.001	System Checks
	T1564.003	Hidden Window
Discovery	T1012	Query Registry
	T1033	System Owner/User Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1087	Account Discovery

3. Ivanti Connect Secure XXE Attempt (CVE-2024-22024)

An XML external entity or XXE vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and ZTA gateways which allow an attacker to access certain restricted resources without authentication.

Rules Created: 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: Attempted-admin
Kill Chain:

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

Known exploited vulnerabilities (Week 3 February 2024):

Vulnerability	CVSS	Description
CVE-2023-43770	6.1 (Medium)	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability
CVE-2024-21412	8.1 (High)	Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability
CVE-2024-21351	7.6 (High)	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability
CVE-2020-3259	7.5 (High)	Cisco ASA and FTD Information Disclosure Vulnerability
CVE-2024-21410	9.8 (Critical)	Microsoft Exchange Server Privilege Escalation Vulnerability

Updated Malware Signatures (Week 3 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: 132

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 132 new ransomware victims or updates on previous victims across 22 different industries spanning 28 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

The LockBit3.0 ransomware group stands out as the most prolific, having updated a significant number of victims (46) distributed across multiple countries. In comparison, Hunter and Alphv ransomware groups updated 14 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	0.76%
8Base	2.27%
Abyss-Data	2.27 %
Akira	2.27%
Alphv	8.33%
Bianlian	5.30%
Black Suit	1.52%
Blackbasta	6.06%
Cactus	2.27%
Clop	0.76%
Hunters	10.61%
Inc Ransom	0.76%
Lockbit3	34.85%
Medusa	2.27%
Meow	3.03%
Mydata	0.76%
Play	6.82%
Qilin	3.79%
Ransomhub	0.76%
Rhysida	0.76%
Stormous	1.52%
Trigona	1.52%
Werewolves	0.76%

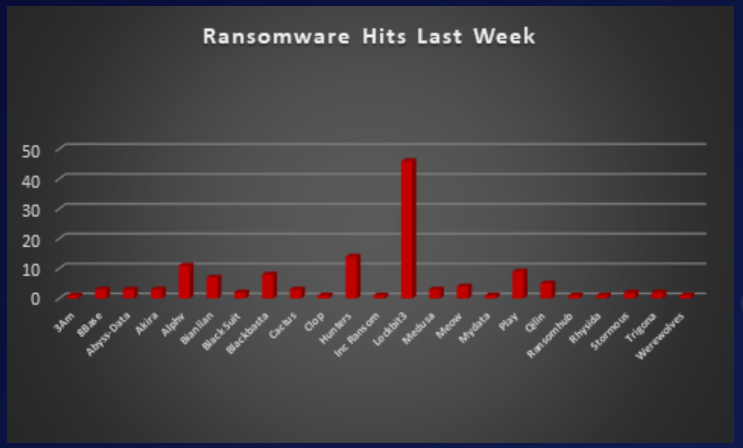

Figure 1: Ransomware Group Hits Last Week

In a comprehensive analysis of ransomware victims across 28 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 82 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
Argentina	0.76%
Australia	0.76%
Belgium	1.52%
Brazil	0.76%
Canada	4.55%
Denmark	0.76%
France	0.76%
Germany	1.52%
Guatemala	0.76%
India	0.76%
Indonesia	0.76%
Italy	3.03%
Japan	0.76%
Lebanon	0.76%
Luxembourg	0.76%
Mexico	0.76%
Netherlands	0.76%
Poland	2.27%
Slovakia	0.76%
South Africa	0.76%
Spain	1.52%
Switzerland	0.76%
Taiwan	0.76%
Thailand	1.52%
Tunisia	0.76%
UAE	3.03%
UK	5.30%
USA	62.12%

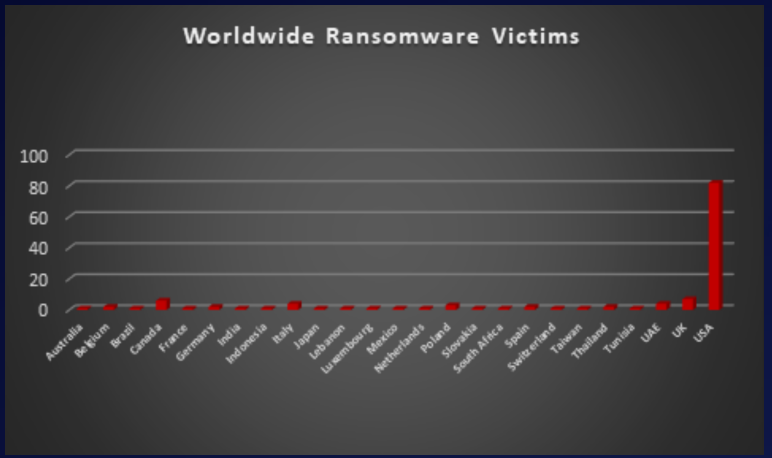

Figure 2: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 22 different industries worldwide. Notably, the Manufacturing and Retail sectors bore the brunt of the attacks in the past week, accounting for 26 and 14 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	0.76%
Business Services	9.85%
Cities, Towns & Municipalities	0.76%
Construction	9.09%
Consumer Services	2.27%
Education	4.55%
Energy, Utilities & Waste Treatment	2.27%
Finance	3.03%
Government	2.27%
Healthcare	4.55%
Hospitality	3.79%
Insurance	1.52%
IT	2.27%
Legal Services	5.30%
Manufacturing	19.70%
Media & Internet	0.76%
Metals & Mining	0.76%
Organisations	6.82%
Real Estate	1.52%
Retail	10.61%
Telecom	2.27%
Transportation	5.30%

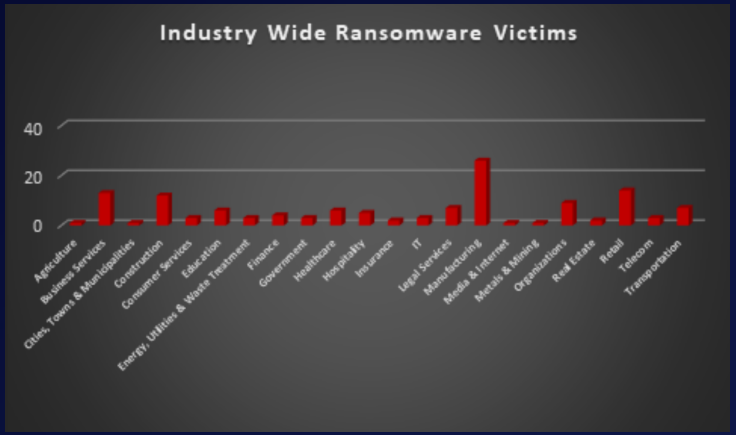

Figure 3: Industry-wide Ransomware Victims