

Threat Intelligence Report April 21 to April 27, 2026

Archived: 2026-05-09 02:00:16 UTC

[Skip to main content](#)



Threat Intelligence Report April 21 - April 27 2026

New Threats Detection Added	• Atemu RAT
New Threat Protection	160
Newly Detected Threats	16

Weekly Detected Threats

The following threats were added to Crystal Eye this week:

Threat name:	Atemu RAT																	
Atemu RAT is a windows-based Remote Access Trojan (RAT) that’s primarily spread through ClickFix based attacks impersonating CloudFlare captchas to trick the user into pasting a malicious payload into PowerShell or cmd. The initial ClickFix payload uses ‘finger.exe’ to download and execute the second stage installer which contains the traditional RAT functionality. Once executed, the machine is registered on the C2 server, ‘systeminfo.exe’ and EDR/AV information is collected and exfiltrated.																		
Threat Protected:	09																	
Rule Set Type:	<table><tr><th>Ruleset</th><th>IDS: Action</th><th>IPS: Action</th></tr><tr><td>Balanced</td><td>Reject</td><td>Drop</td></tr><tr><td>Security</td><td>Reject</td><td>Drop</td></tr><tr><td>WAF</td><td>Disabled</td><td>Disabled</td></tr><tr><td>Connectivity</td><td>Alert</td><td>Alert</td></tr></table>			Ruleset	IDS: Action	IPS: Action	Balanced	Reject	Drop	Security	Reject	Drop	WAF	Disabled	Disabled	Connectivity	Alert	Alert
	Ruleset	IDS: Action	IPS: Action															
	Balanced	Reject	Drop															
	Security	Reject	Drop															
	WAF	Disabled	Disabled															
	Connectivity	Alert	Alert															

	OT	Reject	Drop
Class Type:	Trojan-activity		
Kill Chain:	Tactic	Technique (ID)	Description
	Execution	T1204.004 T1059.001 T1059.003	User Execution: Malicious Copy and Paste Command and Scripting Interpreter: PowerShell Command and Scripting Interpreter: Windows Command Shell
	Discovery	T1082	System Information Discovery
	Collection	T1119	Automated Collection
	Stealth	T1027.010 T1070.004	Obfuscated Files or Information: Command Obfuscation Indicator Removal: File Deletion
	Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols
	Exfiltration	T1041	Exfiltration Over C2 Channel

Known Exploited Vulnerabilities (Week 4 - April 2026)

For more information, please visit the Red Piranha Forum:

<https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-april-2026/657>.

Vulnerability	CVSS	Description			
D-Link DIR-823X (CVE-2025-29635)	7.2	Authenticated RCE - D-Link DIR-823X contains a command injection vulnerability that allows an authenticated attacker to execute operating system commands on the device via a HTTP request. This router is an end-of-life product and may no longer receive any further security updates.	240802 240126	N/A (End-of-Life)	
Samsung MagicINFO 9	8.8	Unauthenticated RCE - Samsung MagicINFO 9 Server contains a path	<= 21.1040.3	21.1050	

Server (CVE-2024-7399)		traversal vulnerability that can allow an unauthenticated remote attacker to upload files to an arbitrary location via a HTTP request. This can enable an attacker to upload a WebShell that gets executed with SYSTEM level privileges.			
SimpleHelp SimpleHelp (CVE-2024-57728)	7.2	Authenticated RCE - SimpleHelp contains a path traversal vulnerability that can allow an authenticated remote attacker to upload files to an arbitrary file system location via a specially crafted zip file. Exploitation can result in code execution in the context of the SimpleHelp server user.	<= 5.5.7	5.5.8	
SimpleHelp SimpleHelp (CVE-2024-57726)	9.9	Privilege Escalation - SimpleHelp contains a privilege escalation vulnerability that can allow an authenticated remote attacker to elevate their privileges to a server admin role through the creation of an API key. This vulnerability can be chained with CVE-2024-57728.	<= 5.5.7	5.5.8	
Marimo Marimo (CVE-2026-39987)	9.8	Unauthenticated RCE - Marimo contains a vulnerability that can allow an unauthenticated remote attacker to execute arbitrary operating system commands by using the WebSocket communication endpoint.	<= 0.22.5	0.23.0	
Microsoft Defender (CVE-2026-33825)	7.8	Privilege Escalation - Microsoft Defender contains a privilege escalation vulnerability that can allow an authenticated attacker to escalate their privileges to SYSTEM.	<= 4.18.26020.6	4.18.26030.3011	
Cisco Catalyst SD-WAN	5.4	Authenticated Privilege Escalation via File Overwrite - Cisco Catalyst	Check vendor advisory for affected products and versions		

Manger (CVE-2026-20122)		SD-WAN Manager contains a vulnerability that can allow an authenticated remote attacker with read-only API credentials to overwrite arbitrary files on the system. Exploitation of this vulnerability can result in escalating to vmanage user privileges.			
Cisco Catalyst SD-WAN Manager (CVE-2026-20133)	6.5	Unauthenticated Information Disclosure - Cisco Catalyst SD-WAN Manager contains an information disclosure vulnerability that can allow an unauthenticated remote attacker to access sensitive information via the API of the system.	Check vendor advisory for affected products and versions		
Kentico Kentico Xperience (CVE-2025-2749)	7.2	Authenticated RCE - Kentico Xperience contains a path traversal vulnerability that can allow an authenticated remote attacker to upload files to an arbitrary file system location. This can enable an attacker to upload a WebShell that gets executed in the context of the webserver.	<= 13.0.177	13.0.178	
PaperCut NG/MF (CVE-2023-27351)	7.5	Authentication Bypass - PaperCut NG/MF contains a vulnerability that can allow unauthenticated remote attackers to bypass authentication and gain access to the system.	15.0 - 20.1.6 21.0.0 - 21.2.10 22.0.0 - 22.0.8	20.1.7 21.2.11 22.0.9	
Synacor Zimbra Collaboration Suite (ZCS) (CVE-2025-48700)	6.1	XSS - Synacor Zimbra Collaboration Suite (ZCS) contains a cross-site scripting vulnerability within the Zimbra Classic UI that can allow an unauthenticated remote attacker to execute arbitrary JavaScript within the users session upon viewing a specially crafted email.	8.8.15 - 8.8.15p46 9.0.0 - 9.0.0p42 10.0.0 - 10.0.11 10.1.0 - 10.1.3	8.8.15p47 9.0.0p43 10.0.12 10.1.4	

Cisco Catalyst SD-WAN Manager (CVE-2026-20128)	7.5	Information Disclosure - Cisco Catalyst SD-WAN Manager contains an information disclosure vulnerability within the Data Collection Agent (DCA) functionality that can allow an authenticated local attacker to recover the passwords stored within the credential file for the DCA user. Exploitation of this vulnerability can allow an attacker to use these credentials to gain access to another system with DCA user privileges.	Check Vendor Advisory for affected products and versions		
Quest KACE Systems Management Appliance (SMA) (CVE-2025-32975)	10.0	Authentication Bypass - Quest KACE Systems Management Appliance (SMA) contains an Authentication Bypass vulnerability that can allow an unauthenticated remote attacker to impersonate another user without needing valid credentials.	Check Vendor Advisory for affected products and versions		
JetBrains TeamCity (CVE-2024-27199)	7.3	Authentication Bypass - JetBrains TeamCity contains a path traversal vulnerability that can allow an unauthenticated remote attacker to access administrative functionality without needing to authenticate. Exploitation of this vulnerability may assist an attacker in gaining further access to the system.	<= 2023.11.3	2023.11.4	
D-Link DIR-823X (CVE-2025-29635)	7.2	Authenticated RCE - D-Link DIR-823X contains a command injection vulnerability that allows an authenticated attacker to execute operating system commands on the device via a HTTP request. This router is an end-of-life product and may no longer receive any further security updates.	240802 240126	N/A	

Samsung MagicINFO 9 Server (CVE-2024-7399)	8.8	Unauthenticated RCE - Samsung MagicINFO 9 Server contains a path traversal vulnerability that can allow an unauthenticated remote attacker to upload files to an arbitrary location via a HTTP request. This can enable an attacker to upload a WebShell that gets executed with SYSTEM level privileges.	<= 21.1040.3	21.1050	
--	-----	---	--------------	---------	--

Updated Malware Signature (Week 4 - April 2026)

Threat	Description	
ErrTraffic	ErrTraffic is a self-hosted cybercrime platform that is used to automate ClickFix campaigns. It functions as a Traffic Distribution Platform (TDS) that enables threat actors to deploy custom ClickFix lures dynamically to a victim based on the browser or operating system.	
XWorm	A Remote Access Trojan (RAT) and malware loader that's commonly used in cyberattacks to give attackers full remote control over a victim's system. It's part of a growing trend of commercialised malware sold or rented on dark web forums, often under the guise of a "legitimate tool."	

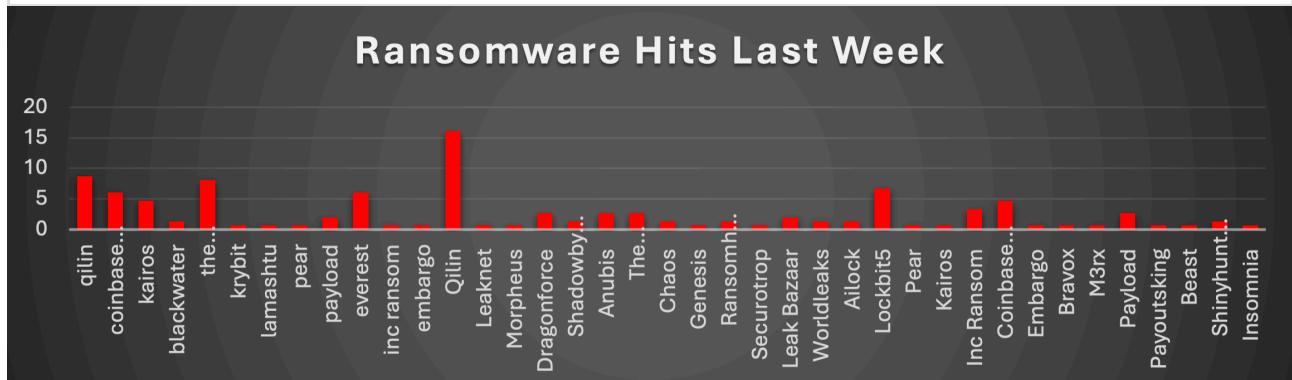
Ransomware Report

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. In the past week, our monitoring revealed multiple ransomware incidents across diverse threat groups, underscoring the persistent and widespread nature of these cyber risks. Presented below is a detailed breakdown of ransomware group activities during this period.

Ransomware Hits Last Week

[Qilin](#) led with 24.83%, followed by Coinbase Cartel at 10.74%, The Gentlemen at 10.73%, and [Lockbit5](#) at 6.71%. Everest accounted for 6.04%, Kairos 5.37%, Payload 4.69%, and Inc Ransom 4.03%. Dragonforce and Anubis each contributed 2.68%, while Leak Bazaar stood at 2.01%. Blackwater, Embargo, Pear, Shadowbyt3\$, Chaos, Ransomhouse, Worldleaks, Ailock, and Shinyhunters each recorded 1.34%.

The remaining actors - Krybit, Lamashtu, Leaknet, Morpheus, Genesis, Securotrop, Bravox, M3rx, Payoutsking, Beast, and Insomnia - each accounted for 0.67% of total ransomware hits last week.



Lamashtu Ransomware

Section 1 - Executive Summary

Lamashtu is a financially motivated data-theft and leak-site extortion group that emerged on 12–13 April 2026, the group operates a purpose-built Tor-hosted leak site – Lamashtu[.]Blog - featuring a public REST API (/API/posts), countdown-timer pressure mechanics, victim-specific Breach Impact Reports, and proof-of-life attachment thumbnails.

Within three weeks of operation, Lamashtu claimed 17 victims and totals 760+ GB across 12 size-verified victims, with the largest single theft being 250 GB from International Assistance Sdn (Malaysia).

The group's motive is financial extortion. No ransom amounts are publicly posted; negotiation is conducted privately via LamashtuSupport@onionmail.org. No encryptor binary, ransom note, file extension, cryptocurrency wallet, YARA rule, or malware sample has been identified in any open source. No ideological, hacktivist or nation-state attribution has been established. Targeting is assessed as opportunistic and broad scan based on the absence of any coherent sector or geographic focus.

Key Findings - Confirmed by Primary Sources

- Lamashtu IS a confirmed data-exfiltration operator - Apple Film Group page shows 27 GB / 51,000 files with proof samples
- 17 total victims; full roster now confirmed via /api/posts JSON - 960+ GB aggregate claimed
- 2 victims PENDING release on May 2, 2026 - active countdown timers (Malaysian NPK Fertilizer; Apple Film Group)

Section 2 - Threat Actor Description

Origin, Branding and Site Architecture

Lamashtu named after the Mesopotamian female demon - was first indexed by RansomLook on 12 April 2026 and by Ransomware.live on 13 April 2026.

These kinds of attacks are mostly initiated through one of three common entry points. The most likely is stolen credentials - groups like Lamashtu typically purchase valid account details from credential markets or prior breach dumps and use them to walk straight in through exposed RDP or VPN endpoints without triggering much noise. It is the path of least resistance for a financially motivated newcomer that has not demonstrated any known exploit specialisation.

The second likely vector is phishing - either a targeted email with a malicious attachment or a link dropping a loader - which remains the single most common initial access method across the double-extortion landscape broadly.

Third is exploitation of a public-facing application such as an unpatched VPN gateway or web portal, though this typically requires more capability than the other two and is less probable given the opportunistic, broad-scan targeting profile Lamashtu displays.

What makes the victims case particularly telling is the scope of what was taken - financial records, manufacturing data, HR files, customer data, all spanning 2023 through early 2026 across multiple departments. That kind of breadth does not happen in a quick in-and-out. It suggests the actor had quiet, persistent access for long enough to map the environment, identify where the valuable data sat, and stage it methodically before exfiltrating 27 GB across 51,000 files.

That dwell-time pattern points more toward credential-based access and deliberate lateral movement than a loud exploit-driven intrusion.

Section 3 - Attack Lifecycle and TTPs (MITRE ATT&CK)

Evidence Status Update

Exfiltration (TA0010) is now CONFIRMED by primary source. All other TTPs remain INFERRED from the generic double-extortion playbook - no malware binary, IR writeup or YARA rule has been published. The DLS API and site architecture reveal operational tradecraft (countdown timers, structured breach reports, proof-of-life thumbnails) but do not expose technical attack TTPs.

ATT&CK ID	Tactic	Technique	Evidence Status
T1567.002, T1041, T1048	Exfiltration	Exfil to web service / alt protocol / C2 channel	CONFIRMED - by DLS evidence

Data exfiltration is now the confirmed primary harm vector. The multi-department nature of Apple Film Group's stolen data (sales, accounting, QC, personnel, production, customer data across 2023–2026) implies sustained, broad-scope access to the victim environment - not a single-share smash-and-grab. This suggests dwell time sufficient for comprehensive discovery and staged exfiltration.

Section 4 - Crystal Eye 5.5 Mitigations

This section maps CE 5.5 controls to each TTP. Following the evidence upgrade - confirmed exfiltration across 960+ GB - the priority tier ranking has been revised: DLP and NDR egress detection are now Priority.

1. Enable DLP in Reject mode on all outbound channels; configure NDR 7-day baseline anomaly to alert on sustained high-volume outbound flows to MEGA/BackBlaze/Telegram CDN/Tor exits; block Tor onion routing and known file-exfil domains at SWG; run Suricata in Prevention mode with Security profile
2. Enforce O365/relay email scanning with AV, anti-phish, SPF/DKIM/DMARC reject; run Deep-mode vuln scans weekly on all external assets; enforce Entra ID SSO + MFA on all WireGuard/IPSec/OpenVPN tunnels; sinkhole new/low-rep domains via DNS.Insure
3. Enforce O365/relay email scanning with AV, anti-phish, SPF/DKIM/DMARC reject; run Deep-mode vuln scans weekly on all external assets; enforce Entra ID SSO + MFA on all WireGuard/IPSec/OpenVPN tunnels; sinkhole new/low-rep domains via DNS.Insure
4. Detect AV disable and event log clearing via EDR behavioural rules; IDPS Prevention mode drops known evasion tooling

Immediate Blocklist Actions - Apply Now

Indicator Type	Value
Tor Onion - DLS	lamashtux5j74mcm7lwwgn5yrvuwtrpxjoyendif3v3hrztjesfoayd[.]onion
Contact Email	LamashtuSupport@onionmail.org
DLS API Endpoint	lamashtu[.]blog/api/posts (clearnet access to DLS API)

Section 5 - Indicators of Compromise

Two new CONFIRMED indicators added (DLS clearnet domain + API path). All file-based IOCs remain NOT FOUND in open sources.

IOC Type	Value
Tor Onion (DLS)	lamashtux5j74mcm7lwwgn5yrvuwtrpxjoyendif3v3hrztjesfoayd[.]onion
DLS Brand Domain	lamashtu[.]blog (clearnet)
DLS API Endpoint	lamashtu[.]blog/api/posts?page=1&filter=all
Contact Email	LamashtuSupport@onionmail.org
PGP Public Key	OpenPGP v2.0.76 block (full key on DLS)
Victim (in-window)	Jesin Group (jesin[.]com[.]my) - Malaysia - Apr 18, 2026
Victim + Exfil Proof	Apple Film Group (applefilm-group[.]com) - Thailand - 27 GB / 51,000 files

Victim + Exfil Size	Malaysian NPK Fertilizer Sdn. Bhd (mnfsb[.]com[.]my) - 20 GB
Victim + Exfil Size	international-assist[.]com - Malaysia - 250 GB

← LAMASHTU.BLOG />

BLOG NEWS FAQ CONTACTS

<< APR >>

← BACK

// COMPANY

APPLE FILM GROUP

Apple Film Co., Ltd. is a leading manufacturer of high-quality plastic bags and films, specializing in Polyethylene (PE) products like HDPE, LDPE, and LLDPE.

// Company.getCustoms()

TIME REMAINING: 6d 20h 02m 47s

RELEASE DATE: May 2, 2026, 12:08 PM

// Company.getState()

// PUBLISHED: Apr 22, 2026

LOCATION: 475 Moo 6, Bangpoo Industrial Estate, Soi 1, Sukhumvit Road, Prsekke, Mueang Samut Prakes, 10280, Thailand

WEBSITE:

applefilm-group.com

PHONE:

+66-2324-0802-3

SIZE:

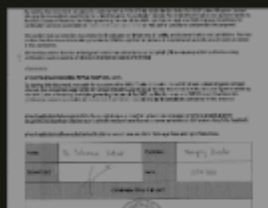
27 GB

FILES:

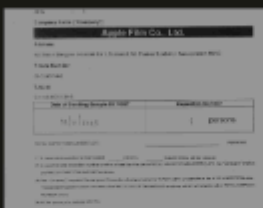
51008

// Company.getAllocations()

[4 total]



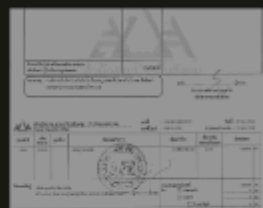
img_01



img_02



img_03



img_04

// Company.getInfo()

Breach Impact Report

SUMMARY

We obtained a substantial dataset from a Thai manufacturing organization. The archive contains tens of thousands of files spanning multiple operational departments including sales, accounting, quality control, personnel, and production. The data covers operations from 2023 through early 2026, with the bulk of materials dated 2024-2025.

The dataset represents comprehensive business operations documentation. We have financial records including invoices, profit and loss statements, budgets, ledgers, and tax documentation. Manufacturing data includes tensile testing results, production reports, and ISO 9001 quality management documentation. Personnel files contain employee records, insurance claims, and payroll documentation. Customer data includes shipping documents, complaints, and pricing information.

This is a complete operational snapshot of a plastic film and packaging manufacturer with export operations.

WHAT WE HAVE

[+ Read Full Report +](#)

// Companies.GetNavigation()

← PREV

Malaysian NPK Fertilizer Sdn. Bhd

NEXT →

Jesin Group

// RELATED.FILTER(CATEGORY)

VIEW.All() →

// LICENSE: COPYRIGHT() 2026 <LAMASHU.BLOG />



// LICENSE.COPYRIGHT() 2026 <LAMASHTU.BLOG />

<LAMASHTU.BLOG />

BLOGNEWSFAQCONTACTS

</ API >

// DISCLOSURE

SHOWCASE

A curated archive of documents from organizations with absolutely nothing to hide. These corporations welcome public scrutiny, have no fear of litigation, and stand behind every decision with complete confidence in their ethical practices. They definitely wanted you to see this.

// Companies.Filter()

ALL COMPANIES [17]

HOT COMPANIES [6]

PENDING COMPANIES [2]

// Companies.getList()

// COMPANY.PENDING()

4d 16h 40m 51s

RELEASE: May 2, 2026

// COMPANY.PENDING()

4d 16h 40m 51s

RELEASE: May 2, 2026

// COMPANY.RELEASED()

jesin.com.my

PUBLISHED: Apr 10, 2026

Melaysian NPK Fertilizer Sdn. Bhd

Apple Film Group

Jesin Group

MNFSB.COM.MY

APPLEFILM-GROUP.COM

JESIN.COM.MY

2.1k views

Apr 23, 2026

1.9k views

Apr 22, 2026

6k views

Apr 10, 2026

// COMPANY.RELEASED()

volterres.fr

PUBLISHED: Apr 14, 2026

// COMPANY.RELEASED()

biotehnos.ro

PUBLISHED: Apr 12, 2026

// COMPANY.RELEASED()

theseacarehotel.com

PUBLISHED: Apr 8, 2026

VOLTERRES

Biotehnos

The Seacare Hotel

VOLTERRES.FR

BIOTEHNOS.RO

THESEACAREHOTEL.COM

9.9k views

Apr 14, 2026

9.3k views

Apr 12, 2026

10k views

Apr 8, 2026

// Companies.Paginate()

↓ LOAD MORE [6]

// LICENSE.COPYRIGHT() 2026 <LAMASHTU.BLOG />

Page 15 of 18

CLEARWATER.BLOG >

RIDS NFWS FAQ CONTACTS

< NP1 >

< BDC

// COMPANY

BEAVER ENGINEERING

Beaver Engineering, Inc. is a Nashville-based geotechnical engineering firm founded in 1968, specializing in construction observation, materials testing, and sinkhole investigation throughout the southeastern United States.

// Company.GetStats()

// PROJECTS: Mar 30, 2026

LOCATION: 757B Cockrell Bend Blvd, Nashville, Tennessee, 37209-1066, USA.

WEBSITE:

beaverengineering.com

PHONE:

N/A

CITY:

SO TN

FILES:

20260

// Company.GetTasksView()

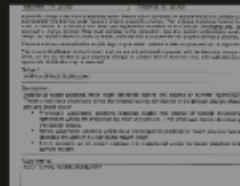
[0 files]



img_01



img_02



img_03



img_04

// Company.GetInfo()

BREACH IMPACT REPORT SUMMARY

We obtained a comprehensive dataset from a US-based geotechnical engineering firm. The archive contains tens of thousands of files spanning over three decades of operations, from 1992 through 2023. The dataset encompasses the full scope of corporate operations: financial records, project documentation, client contracts, employee files, and technical engineering data.

The breadth of this dataset is substantial. We have tens of thousands of invoices, several thousand proposals, over a thousand contracts, and extensive correspondence dating back to the early 2000s. The dataset includes QuickBooks company files, payroll import files, database exports, and technical engineering documentation covering well testing, soil analysis, and construction inspection reports.

Dozens of named individuals and entities are identified throughout the records. The data reveals operational details across municipal projects, commercial developments, and petroleum industry work.

WHAT WE HAVE

[+ Read Full Report +](#)

// Company.GetFormUrl()

magnet:?xt=urn:btih:6B73wSd610B5w1ASd2w7w31wsc110Dsc5P1dbw6d
subbeaverengineering

copy

Password: JBwG6xy1B8Tj4cT0V4JQ18A71k2w-Y0

copy

Use a torrent client to download.

// Companies.GetNavigation()

< Prev

ClientSolution EPO Service Srl Logitech Srl
Safety

Next >

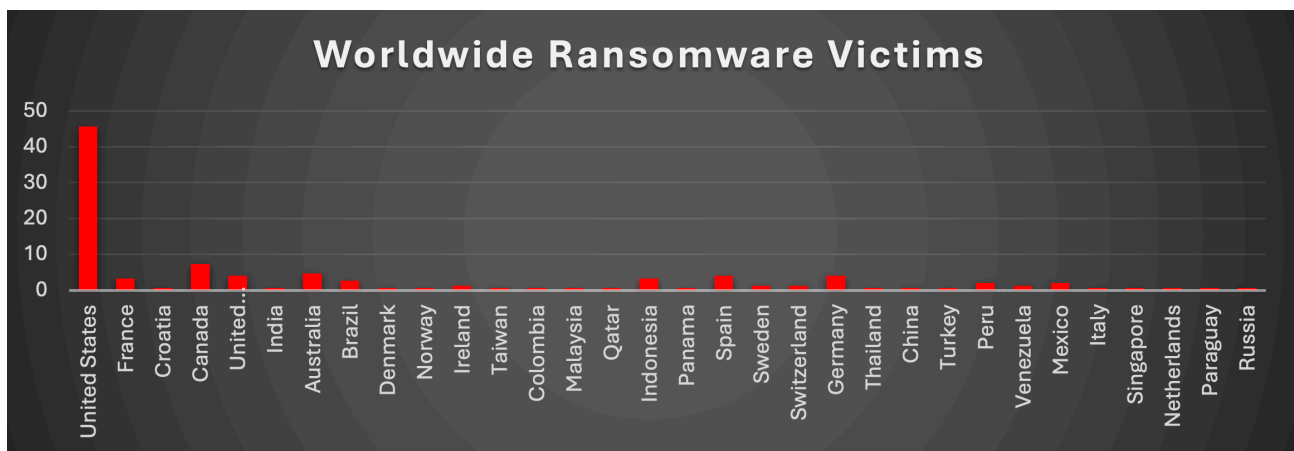
ELIAB

// RELATVS.FILTER(CATGORY)

VIEW ALL >

Worldwide Ransomware Victims

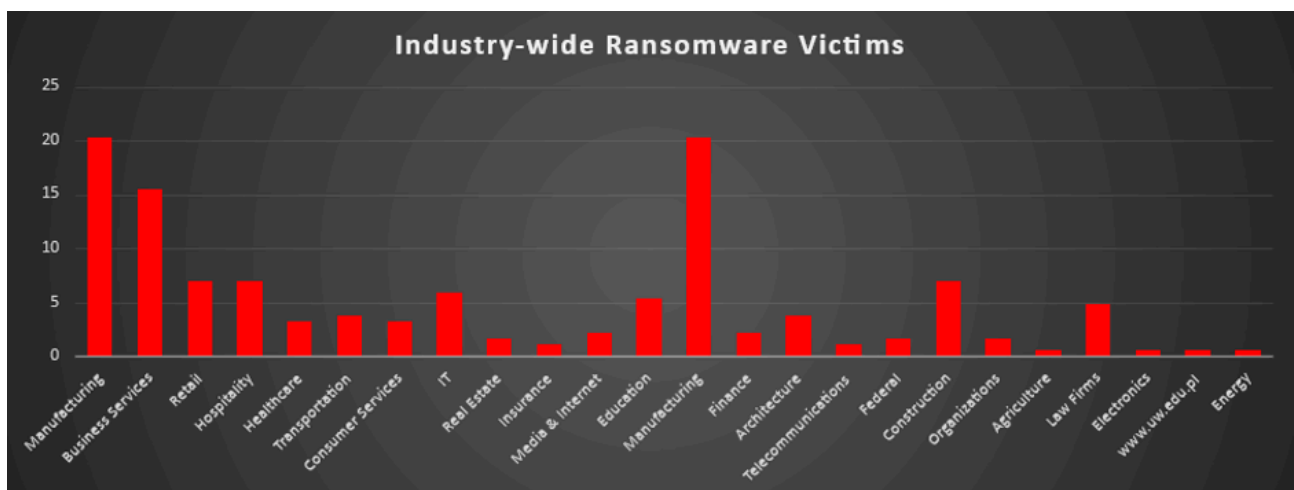
The remaining nations - Croatia, India, Denmark, Norway, Taiwan, Colombia, Malaysia, Qatar, Panama, Thailand, China, Turkey, Italy, Singapore, Netherlands, Paraguay, and Russia - each represented 0.67% of total global ransomware victims recorded last week.



Industry-wide Ransomware Impact

Business Services and Manufacturing jointly led with 16.11% each, followed by Retail at 10.07% and Law Firms at 8.72%. Healthcare accounted for 7.38%, while IT stood at 6.04%. Transportation recorded 5.37%, with Finance and Construction each at 4.70%. Organizations contributed 4.03% and Federal agencies 3.36%.

Architecture, Education, and Energy each accounted for 2.68%, while Hospitality, Media & Internet, and Consumer Services each recorded 1.34%. Real Estate and Electronics each represented 0.67% of total industry-wide ransomware victims last week.



Source: <https://redpiranha.net/news/threat-intelligence-report-april-21-april-27-2026>