CYBLE®



U.S. THREAT LANDSCAPE

BFSI SECTOR

H1 2026

TABLE OF CONTENT

Executive Summary **3**
Notable Cyber Incidents Related to the U.S. BFSI Sector **4**
Most Active Threat Actor Profiles **6**
Ransomware Attacks **8**
Dominant Groups 8
Impact Analysis 10
Notable Trends 11
Notable Data Breaches and Leaks **12**
Notable Accesses on Sale **15**
Critical Vulnerabilities Observed **17**
Known Exploited Vulnerabilities 17
Zero-Day Vulnerabilities 20
Hacktivism **22**
Industry News **23**
Conclusion **25**

© 2026 Cyble Inc. All rights reserved.

Executive Summary

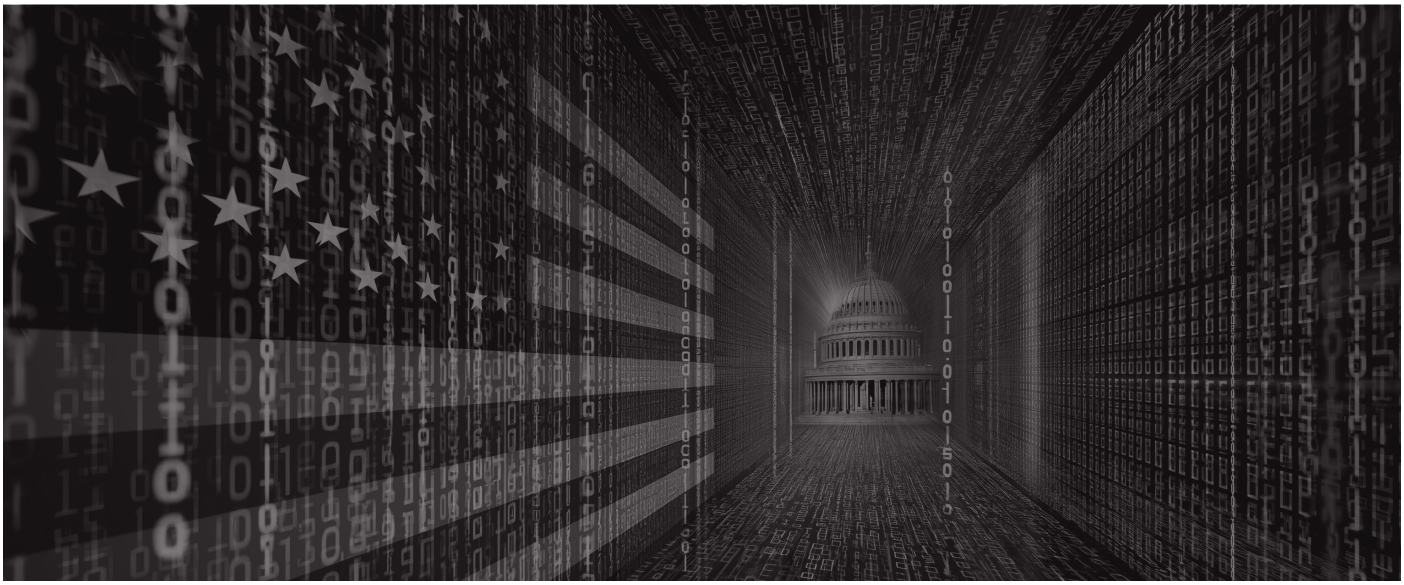
Cyble researchers analyzed the explosive cyber threat activity targeting the banking, financial services, and insurance (BFSI) sector in the United States, to date, in 2026 and found a multifaceted threat landscape characterized by persistent ransomware campaigns, extensive data compromises, and sophisticated, targeted attacks.

Prolific ransomware groups, including Qilin, Akira, and Dragonforce, were responsible for majority of the incidents, impacting a wide spectrum of financial entities from credit unions to major corporations like Fiserv and S&P Global.

Concurrently, cybercrime forums feature a continuous trade of sensitive data and network access, with threat actors advertising multi-million record databases from institutions such as Sun West Mortgage and SSN Bank.

High-impact operations include North Korean state-sponsored actors using advanced social engineering and AI to steal cryptocurrency and organized crime syndicates deploying Ploutus malware for ATM jackpotting. These intrusions are frequently enabled by the active exploitation of critical and zero-day vulnerabilities in widely deployed internet-facing infrastructure.

To mitigate these evolving threats, a security posture emphasizing accelerated patch management for known exploited vulnerabilities, robust network segmentation, and continuous monitoring is essential.



© 2026 Cyble Inc. All rights reserved.

Notable Cyber Incidents Related to the U.S. BFSI Sector

Month	Entity / Victim	BFSI Sub-sector	Threat Actor	Nature of Incident
January	**Ledger (via Global-e breach)**	Financial Technology	Unknown	Payment processor breach exposed names and contact info of ~292,000 customers; Ledger's internal systems unaffected
January	**Beacon Mutual Insurance**	Insurance	INC	Ransomware attack on Rhode Island insurer; 275 GB of internal data claimed stolen; network disconnected as precaution
February	**BridgePay Network Solutions**	Payment Processing	Unknown	Ransomware knocked US payment gateway offline; APIs, virtual terminals, and hosted payment pages disrupted for merchants and municipalities nationwide
February	**Lakeside Title Co.**	Financial Services	Play	Ransomware attack on Maryland title company; PII of customers and employees exposed; class action lawsuit filed
February	**Figure Technology Solutions**	Financial Technology	ShinyHunters	2.5 TB of data from ~967,200 accounts published after alleged refusal to pay; 900,000+ unique email addresses exposed
February	**CarGurus**	Financial Services	ShinyHunters	1.7 million account records published including finance pre-qualification data, dealer subscription info, and PII
February	**Pathstone Family Office**	Capital Markets / Investment	ShinyHunters	641,000 records including financial documents and client PII published after alleged refusal to pay ransom
February	**Catalyst RCM**	Financial Services	Everest	Compromised credentials used to access file management system; ~139,964 individuals affected; payment card and PHI data exposed
March	**Ameriprise Financial**	Financial Services	Unknown	Breach disclosed to Oregon DOJ; ~47,876 individuals affected; type of compromised data not yet confirmed

© 2026 Cyble Inc. All rights reserved.

April	**Two major US banks (unnamed, via third-party vendor)**	Banking	Everest	Both banks breached through a shared document-production vendor on the same day; posted on Everest dark web leak site April 20
April	**Belpointe Asset Management**	Capital Markets / Investment	INC Ransom	Connecticut-based financial advisory firm listed on INC Ransom leak site
May	**Sysco**	Financial Services / Supply Chain	Qilin	Internal documents including pricing lists, customer invoices, and tax records published; May 12 ransom deadline set
June	**Sysco (follow-up)**	Financial Services / Supply Chain	ShinyHunters	61 million Salesforce records claimed stolen across multiple tables including customer and employee data
June	**Madison Square Garden**	Financial / Entertainment	ShinyHunters	26 million records claimed; part of Oracle PeopleSoft zero-day exploitation campaign
June	**GIA Partners LLC**	Capital Markets / Investment	TheGentlemen	Independent minority-owned registered investment advisory firm listed on dark web leak site
June	**Houston City (finance systems)**	Banking / Government	ShinyHunters	City financial systems targeted as part of ShinyHunters Oracle PeopleSoft zero-day campaign

Table.1: Includes data of US-headquartered or US-operating entities only.

Stand out patterns

ShinyHunters was one of the most active threat actor against U.S. BFSI targets running hack and leak extortion campaigns. Remember, this TA does not necessarily use ransomware malware and thus is not considered a purely ransomware gang but a cybercriminal group. The actor/group was responsible for attacks on Figure Technology Solutions, CarGurus, Pathstone Family Office, and both the Sysco follow-up and Madison Square Garden in June — all part of an aggressive extortion campaign that escalated significantly in the second quarter.

February was the busiest month, including the BridgePay ransomware attack that caused cascading outages for merchants and municipalities across the US, and three separate ShinyHunters-linked data leaks.

The April banking incident is notable for its supply chain angle — two unnamed major US banks were both compromised through a single shared third-party vendor on the same day, which underscores how interconnected vendor infrastructure creates systemic risk across financial institutions.

June's ShinyHunters spree targeting Oracle PeopleSoft systems is worth watching closely, as that campaign was still active as of the latest reporting and claimed multiple US financial and government entities in quick succession.

© 2026 Cyble Inc. All rights reserved.

Most Active Threat Actor Profiles

Cyble observed a total of 83 threat actors including APTs, cybercriminals, ransomware groups, and more, actively targeting the U.S. BFSI sector in H1 2026. Of these, more than one-third were APT groups primarily linked to China, Iran and Russia. A further analysis revealed that 14 of these APT groups were previously tracked and attributed as state-sponsored groups.

The geo-political tensions in the Middle-East linked to the tripartite war between Iran-Israel and U.S. has led to a significant spike in cyber operations and state-sponsored activities which is evident in our observations. With the Strait of Hormuz being the bargaining chip that both Iran and U.S. are leveraging and peace agreements that keep getting pushed due to political stand-offs, these operations might just continue even if a truce is drawn.

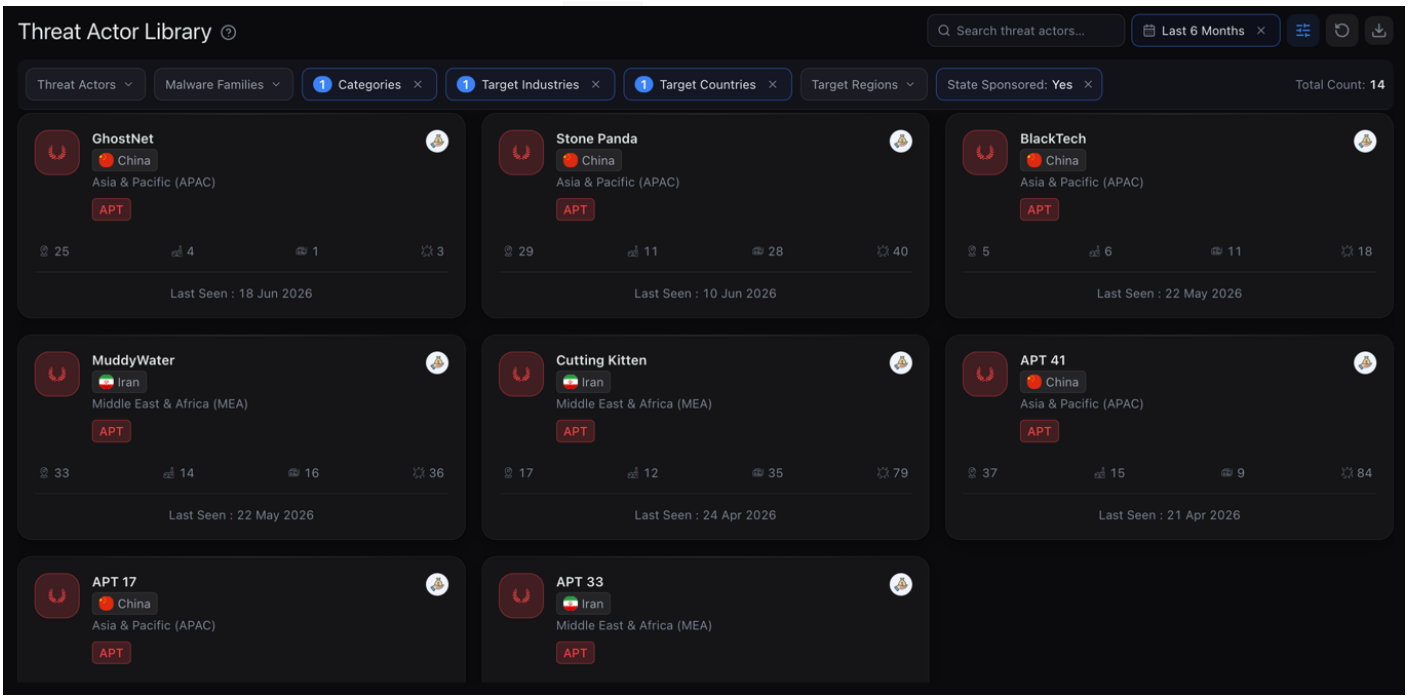


Fig.1: 14 state-sponsored APT groups were tracked targeting U.S. BFSI sector in H1 2026 (Source: Cyble Vision)

Apart from APTs, ransomware groups were the most active during the observed period with 20 different name actors. Hacktivists, who have carried out DDoS attacks, defaced websites and carried out hack and leak activities, were also seen among the most active threat actor profiles.

© 2026 Cyble Inc. All rights reserved.

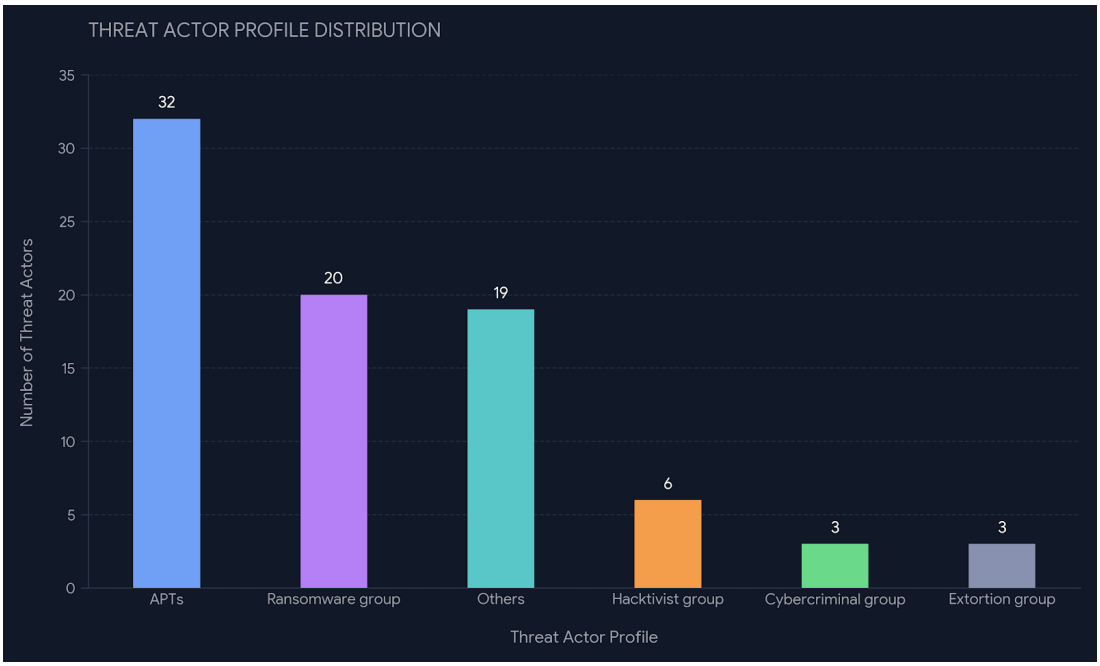


Fig.2: Threat actor profile distribution targeting U.S. BFSI sector in H1 2026 (Source: Cyble Vision)



© 2026 Cyble Inc. All rights reserved.

Ransomware Attacks

The first half of 2026 saw a persistent and significant level of ransomware activity targeting the United States' banking, financial services, and insurance sector, with 69 recorded attacks.

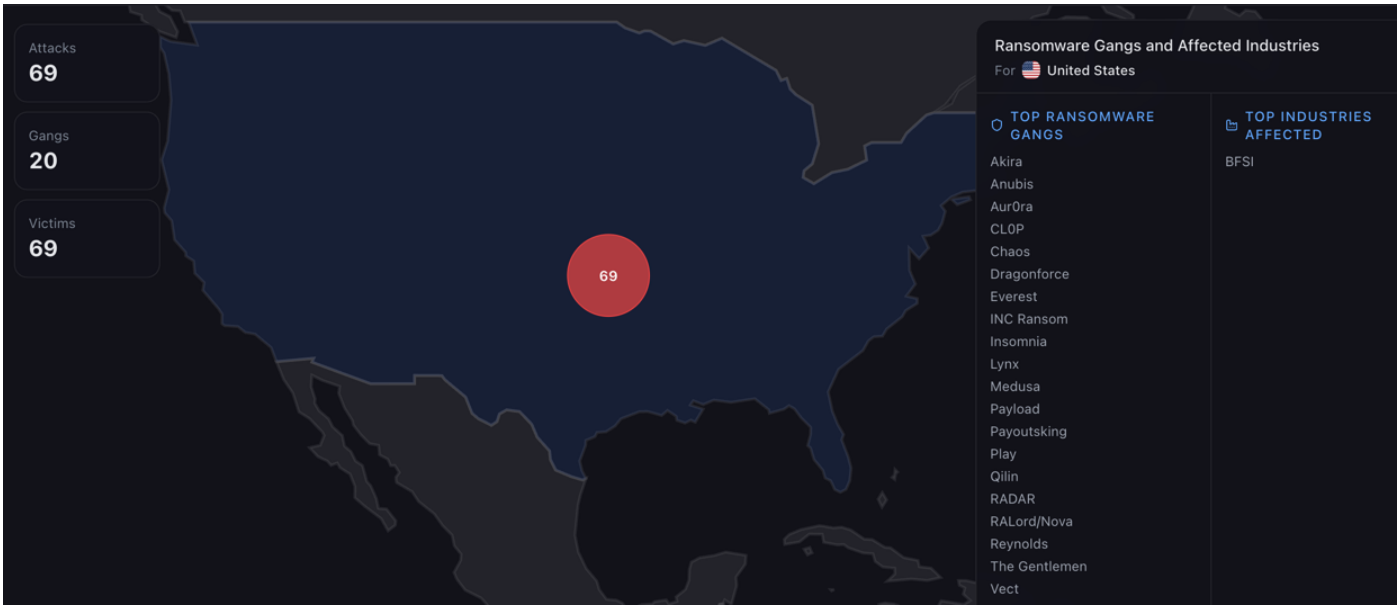


Fig.3: List of all ransomware actors that targeted BFSI sector in the U.S. – H1 2026 (Source: Cyble Vision)

This consistent volume of incidents positioned the sector as a high-value target for a diverse array of threat actors. Cyble observed a total of 20 ransomware gangs actively targeting the region (names of all gangs are in the above image in an alphabetical order).

The attacks were distributed throughout the six-month period, indicating that ransomware groups maintained a continuous operational tempo against financial institutions in the U.S.

Dominant Groups

The threat landscape was dominated by a small number of prolific ransomware groups. The triumvirate of Qilin, Akira and Dragonforce was responsible for 34 of the 69 total incidents, accounting for nearly 50% of all attacks against the sector.

© 2026 Cyble Inc. All rights reserved.

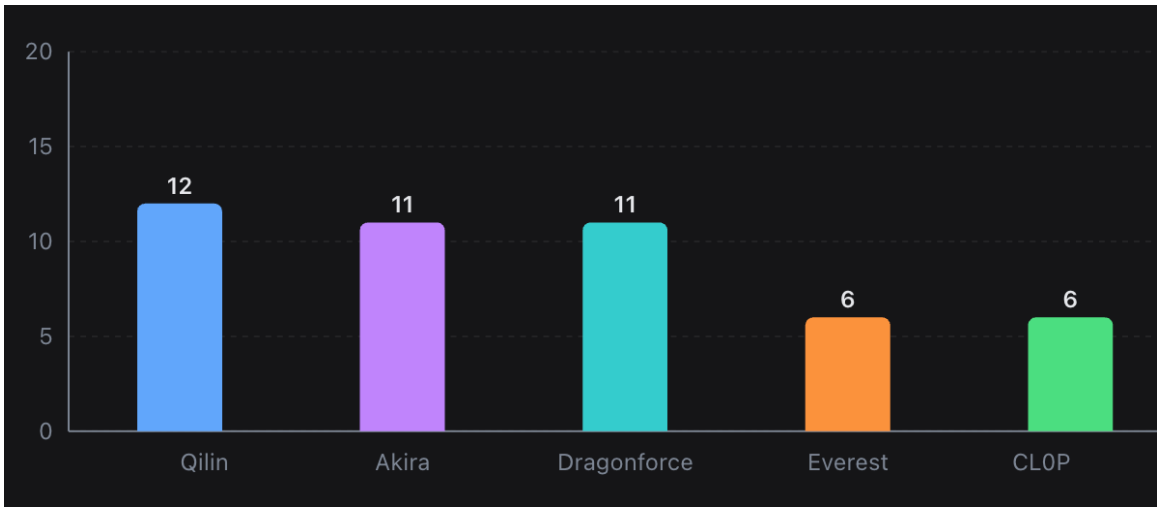


Fig.4: Top five ransomware actors targeting U.S. BFSI sector – H1 2026 (Source: Cyble Vision)

Qilin was the most active, claiming 12 victims, while Akira and Dragonforce were tied for second, each with 11 successful attacks.

Globally, Qilin targeted 28 organizations in the BFSI sector but 43% of these were from the U.S. alone.

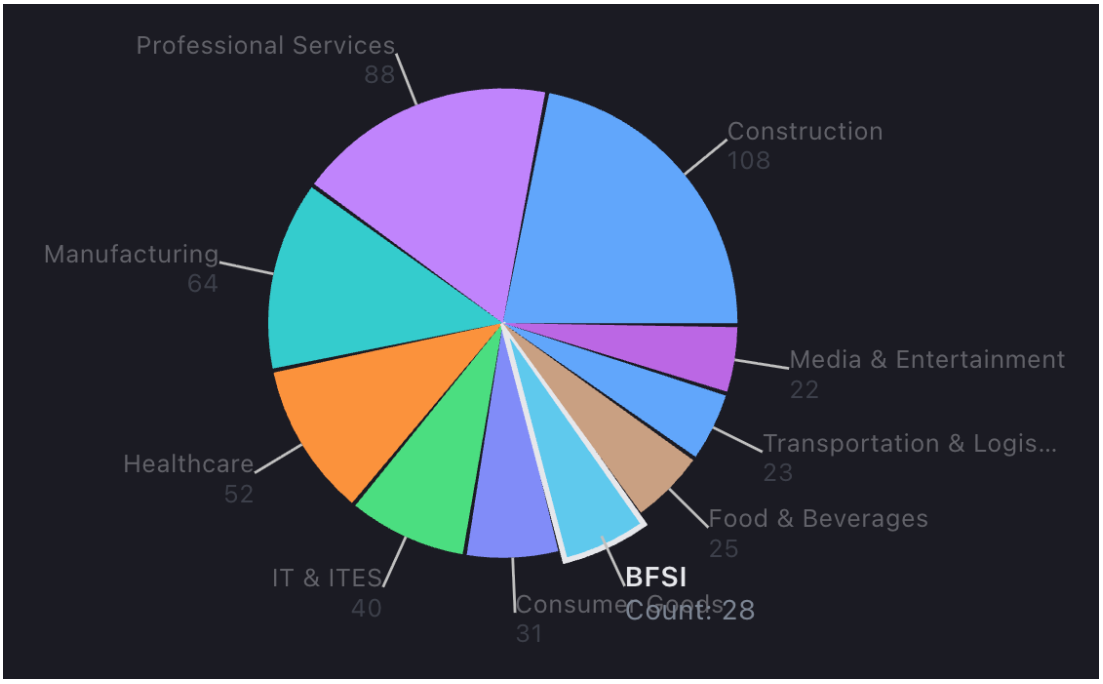


Fig.5: Qilin targeted 28 BFSI entities worldwide – H1 2026 (Source: Cyble Vision)

© 2026 Cyble Inc. All rights reserved.

A secondary tier of highly active operators included Everest, CL0P and INC Ransom, each contributing six attacks. The concentration of activity among these top six groups, which were collectively responsible for over 75% of incidents, shows their established capabilities and focus on the U.S. financial industry.

Impact Analysis

Worldwide, the BFSI sector was the sixth most targeted with 159 recorded attacks. Construction (491) sector was the most targeted in the observed period.

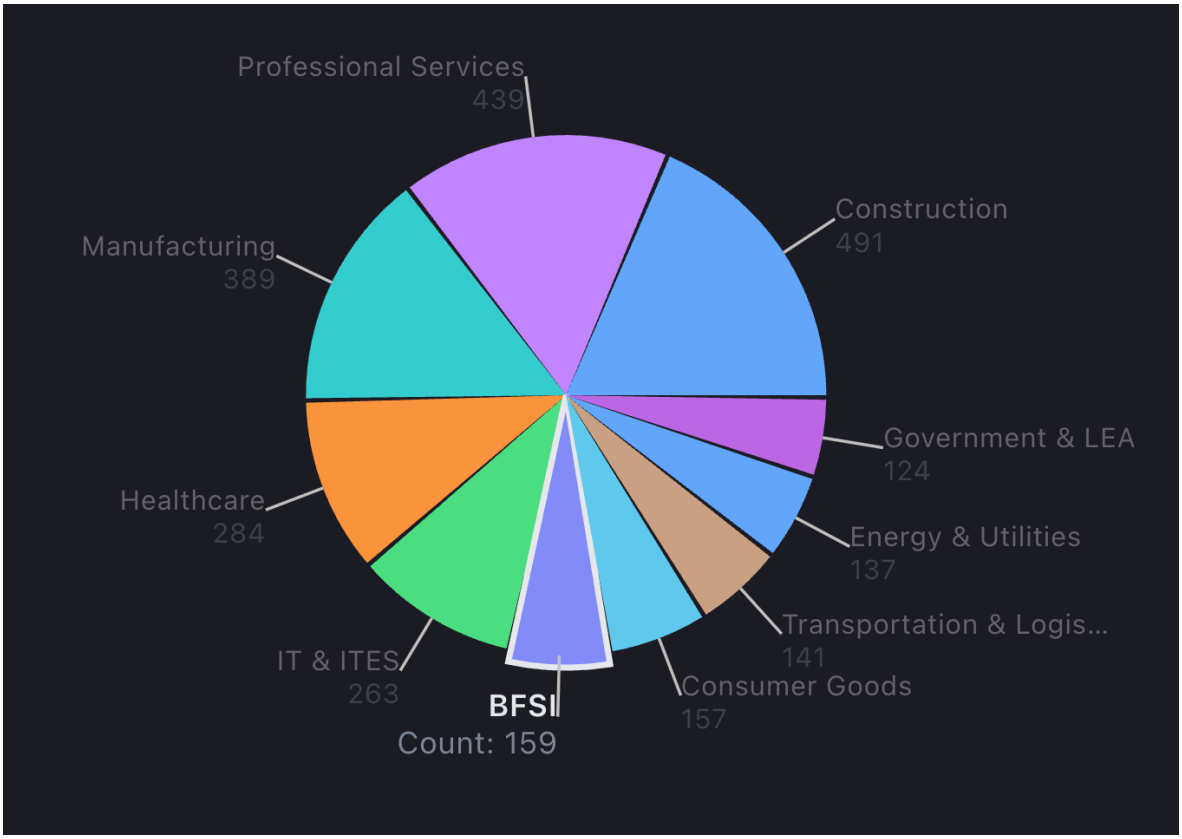


Fig.6: BFSI sixth most targeted sector worldwide – H1 2026 (Source: Cyble Vision)

But with 69 attacks, the U.S. BFSI sector was targeted 10 times more as compared to the second ranked Canada and more than 17x in comparison to the fifth ranked Singapore, a strongly emerging financial hub in South Asia.

© 2026 Cyble Inc. All rights reserved.

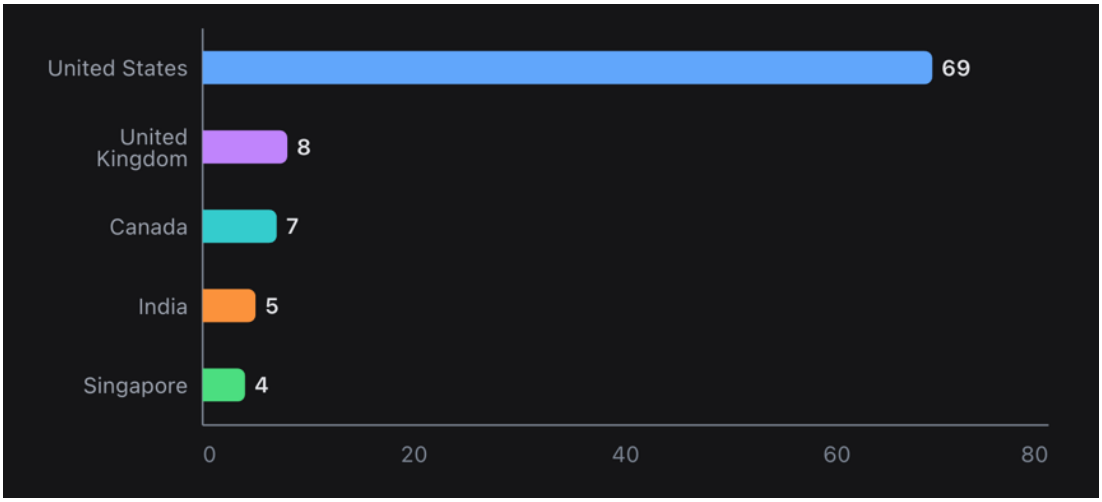


Fig.7: Five most targeted countries worldwide – H1 2026 (Source: Cyble Vision)

Ransomware attacks in this period impacted a wide spectrum of organizations across the BFSI sector, demonstrating that no sub-sector was immune. Victims ranged from regional insurance providers and credit unions to major national financial service corporations. Insurance entities such as Starr Insurance Inc., Beacon Mutual Insurance Company, and Ross & Yerger Insurance, Inc. were on the ransomware actors' victims list. Similarly, the investment and wealth management sub-sector saw significant impact, with firms like Punch & Associates Investment Management, Hudson Executive Capital, and Delbrook Capital Advisors being victimized. The attacks also reached critical financial infrastructure, with notable incidents involving major payment solutions providers.

Notable Trends

Several distinct trends emerged during this period. The Everest group, for instance, appeared to conduct a focused campaign against large, high-profile financial corporations within a two-week span. In contrast, CL0P's activity was heavily concentrated in late January and early February, a pattern consistent with the group's historical use of zero-day exploits for mass-compromise campaigns.

Beyond the top-tier operators, the landscape was highly fragmented, with 15 different ransomware groups each being responsible for a single attack. This "long tail" of threat actors, including newer or less common variants like Aur0ra and The Gentlemen, indicates a low barrier to entry and a constantly evolving ecosystem of threats.

In conclusion, the primary ransomware threat to the U.S. BFSI sector in H1 2026 stemmed from a concentrated cadre of highly active groups, led by Qilin, Akira, and Dragonforce. These actors demonstrated the ability to compromise a diverse range of financial entities, from small insurance agencies to large capital management firms, suggesting a strategy of opportunistic targeting. This was complemented by more specialized campaigns from other groups and a wide array of smaller operators, creating a complex and dynamic threat environment that demands comprehensive and adaptive security postures from all organizations within the sector.

© 2026 Cyble Inc. All rights reserved.

Notable Data Breaches and Leaks

Bank Customer Data Allegedly for Sale on Dark Web

On February 11, the threat actor ResPublica, a member of the '.zip affiliate' group, advertised a dataset on the DarkForums cybercrime forum allegedly belonging to US-based financial institutions. The actor claimed the data was compromised from a contact center and contained extensive personally identifiable information (PII) of U.S. account holders, including names, dates of birth, addresses, contact details, credit scores, routing numbers, government-issued ID information, and account numbers. ResPublica stated the breach was not yet public and that the data was recent and exclusive, providing sample records to substantiate their claims and inviting potential buyers to communicate privately.

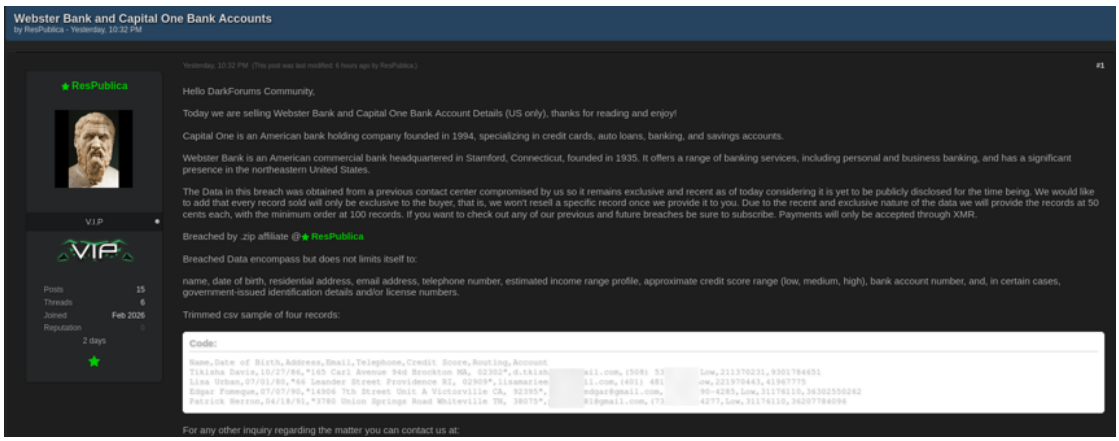


Fig.8: (Source: Cyble Vision)

252K US Payment Processor Credit Card Records Allegedly for Sale

Threat actor Lordracks advertised a database for sale on the English-language cybercrime forum darkforums[.]su. The threat actor claimed the database contained 252,784 credit card records allegedly stolen from US-based payment processors, in early June 2026. The advertised data reportedly included full payment details such as PAN, CVV2, billing addresses, Social Security Numbers, and FICO score estimates. Lordracks listed the complete dataset for US$5,000 and claimed a test sample had a 98.4% validation rate, though these assertions remained unconfirmed as no public proof was provided in the forum post.

© 2026 Cyble Inc. All rights reserved.

Alleged Database of US Fintech Firm for Sale

On January 5, the threat actor 'letsgetit' advertised a database allegedly stolen from a US-based financial technology company, on the Exploit cybercrime forum. The actor claimed to have infiltrated the company's support department using custom Remote Access Trojans (RATs) to exfiltrate several logs and databases. While a price and the total size of the data were not specified, the actor shared sample records to support their claim. The exposed data included client's personally identifiable information (PII) such as names, email addresses and phone numbers, alongside professional details, organizational data and sensitive financial information related to business funding and loan statuses.

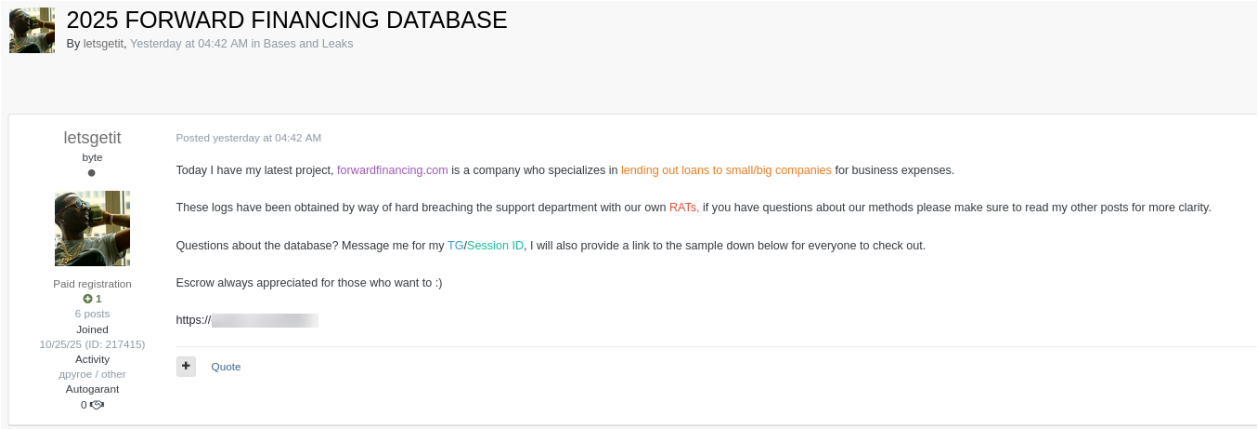


Fig.9: (Source: Cyble Vision)

Database Allegedly from US Crypto Platform Leaked on Cybercrime Forum

In early May, the threat actor 'gale_boetticher' leaked a database on the Russian cybercrime forum, Exploit. The database allegedly belongs to the firm behind a known credit card provider and contains 97,137 records. Analysis of the leaked information indicates it is likely from customer support or service-related records. It includes data such as ticket IDs, submitter email addresses, requester IDs, subjects, and timestamps associated with the credit card users.

© 2026 Cyble Inc. All rights reserved.

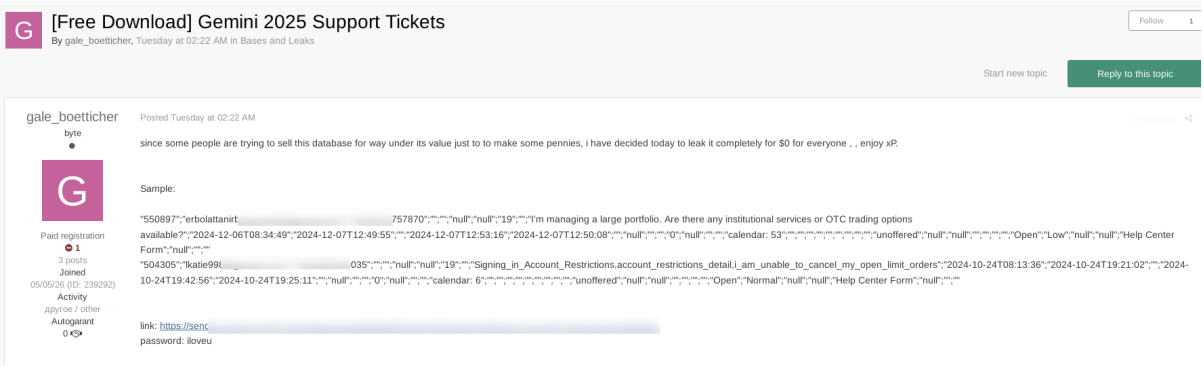


Fig.10: (Source: Cyble Vision)

Alleged Data of 24600 Bank Customers Advertised on Cybercrime Forum

On June 22, the threat actor Shadowreaper advertised a database for sale on a cybercrime forum. The actor claimed the data contained 24,600 records allegedly belonging to customers of U.S. financial institutions. The advertised information reportedly includes full names, social security numbers, addresses and live credit card details. Shadowreaper asserted the data was exfiltrated between June 14 and June 22, by exploiting misconfigured S3 buckets and API authentication bypasses. The threat actor listed the complete dataset for US$4,000 and provided redacted samples as proof, though the overall validity of the data remains unconfirmed.



© 2026 Cyble Inc. All rights reserved.

Notable Accesses on Sale

Threat Actor Advertises Alleged VM Access to US Trading Platform

In June 20, the threat actor 'Admin' posted an advertisement on the English-language cybercrime forum, spear[.]cx, offering to sell unauthorized access to a virtual machine. The post alleged that the compromised VM was part of the infrastructure of a US-based investment platform. Specific details regarding the scope of access, credentials or pricing were not publicly available as viewing the content required registration on the forum. The threat actor did not provide any visible evidence to support their claims; therefore, the assertions remained unconfirmed.

250,000 Alleged Customer Records of US Based Bank for Sale

The threat actor 'HiddenHq' advertised the sale of approximately 250,000 data leads on the English-language cybercrime forum, darkforums[.]su. The data allegedly belongs to customers of the United States-based financial institution. The compromised dataset reportedly contains a wide range of sensitive information, including full names, addresses, dates of birth, social security numbers, driver's license details, phone numbers and specific bank account information such as IBN and account numbers. To substantiate their claims, the threat actor provided a sample of the data via a JustPaste link and offered 1,000 records as a gift to forum members, with the data purportedly being updated as of June 6.

Threat Actor Offers 953 Alleged PayPal Accounts for Sale

The threat actor 'wish' advertised 953 allegedly stolen PayPal accounts on the English-language cybercrime forum, breached[.]su. The threat actor claimed the accounts belonging to the US-based financial technology company, held significant balances. The post did not specify the method of compromise, provide pricing details, or include any evidence to support the assertions, leaving the claims unconfirmed.

Alleged Mortgage Breach 6 Million Records Offered for Sale

A threat actor known as lXXXl advertised a compromised database on the PwnForums cybercrime forum, allegedly belonging to a US-based mortgage company. The actor offered a 2.3 GB SQL file containing over 6 million lines of data, purportedly from tables for mortgage leads and broker users. The exposed data reportedly includes a significant amount of personally identifiable information (PII), such as full names, phone numbers, email addresses, physical addresses, loan volumes, and National Mortgage Licensing System (NMLS) IDs. To substantiate the claim, the threat actor posted sample records while keeping the full dataset behind a paywall.

© 2026 Cyble Inc. All rights reserved.

Alleged Cryptocurrency Account Access for Sale on Cybercrime Forum

The threat actor 'wizard460' advertised unauthorized access to a single user account allegedly belonging to a United States-based cryptocurrency exchange. In a post on the English-language cybercrime forum, breached[.]su, the threat actor claimed the credentials were from an early leak but stated the data quality was low. The threat actor provided no evidence to support the claims of access, and the assertions remained unconfirmed.



© 2026 Cyble Inc. All rights reserved.

Critical Vulnerabilities Observed

Known Exploited Vulnerabilities

The first half of 2026 has been defined by a significant volume of critical, industry-agnostic, and region-agnostic vulnerabilities, with 56 CVEs scoring 9.0 or higher on the CVSSv3 scale. The U.S. Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities (KEV) Catalog for this period shows a persistent trend of threat actors targeting internet-facing enterprise platforms and network infrastructure.

A total of 127 vulnerabilities were added to the CISA KEV catalog in the first six months of the year, of which, 16 were exploited by ransomware gangs.

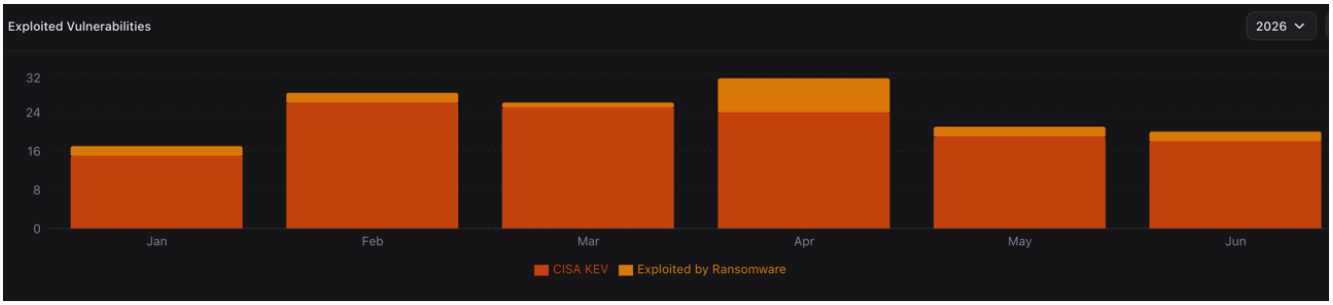


Fig.11: H1 2026 month-wise CISA KEV catalog and ransomware exploited vulnerabilities count (Source: Cyble Vision)

Notably, vendors such as SmarterTools, Solarwinds, Cisco, Microsoft, and Fortinet have had multiple products featured, indicating a concentrated risk within widely deployed technologies like mail servers, network monitoring tools, and security appliances.

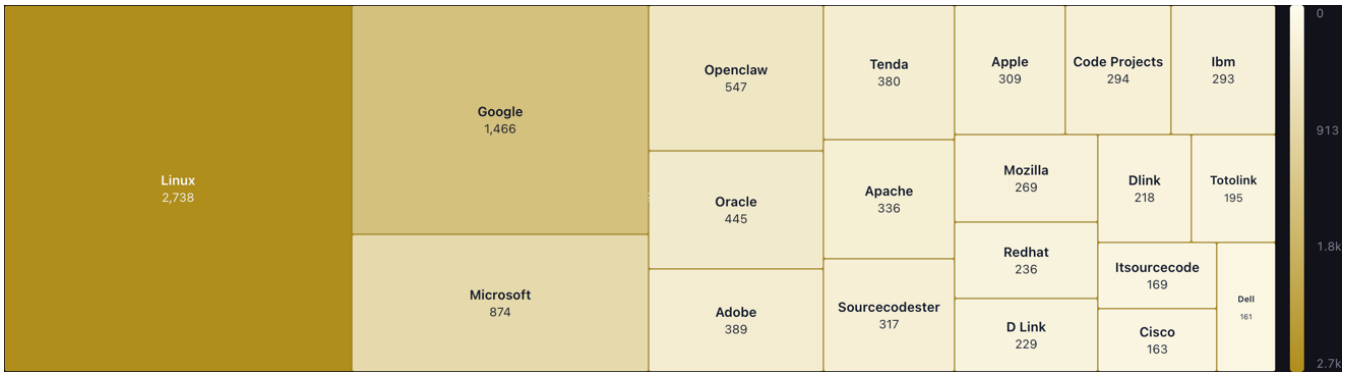


Fig.10: Top affected vendors and products in H1 2026 (Source: Cyble Vision)

© 2026 Cyble Inc. All rights reserved.

The inclusion of these CVEs in the KEV catalog signifies active and ongoing exploitation, making immediate patching a critical priority for defenders to mitigate significant operational impact.

The frequent appearance of vulnerabilities in remote access and management systems shows a continued focus by adversaries on initial access vectors that bypass perimeter defenses. Therefore, organizations are strongly advised to accelerate their patch management cycles, enhance network segmentation to limit lateral movement, and continuously monitor for signs of compromise related to these exploited vulnerabilities.

CVE ID	Product	Vendor	CVSS(V3)
CVE-2025-37164	Oneview	Hpe	9.8
CVE-2026-20045	Unified Communications Manager	Cisco	9.8
CVE-2024-37079	Cloud Foundation	Vmware	9.8
CVE-2025-52691	Smartermail	Smartertools	10
CVE-2026-24061	Inetutils	Gnu	9.8
CVE-2026-23760	Smartermail	Smartertools	9.8
CVE-2026-24858	Fortianalyzer	Fortinet	9.8
CVE-2026-1281	Endpoint Manager Mobile	Ivanti	9.8
CVE-2019-19006	Freepbx	Sangoma	9.8
CVE-2025-40551	Web Help Desk	Solarwinds	9.8
CVE-2025-11953	Metro Development Server	Metro Development Server	9.8
CVE-2026-24423	Smartermail	Smarter Tools	9.8
CVE-2025-40536	Web Help Desk	Solarwinds	9.8
CVE-2024-43468	System Center Configuration Manager	Microsoft	9.8
CVE-2026-1731	Remote Support Privileged Remote Access	Beyond Trust	9.8
CVE-2020-7796	Zimbra Collaboration Suite	Synacor	9.8
CVE-2021-22175	Gitlab	Gitlab	9.8
CVE-2026-22769	Recoverpoint For Virtual Machines	Dell	10
CVE-2026-20127	Catalyst Sd Wan Manager	Cisco	10
CVE-2017-7921	Ds 2Cd2032 I Firmware	Hikvision	9.8
CVE-2021-22681	Factorytalk Services Platform	Rockwell Automation	9.8
CVE-2025-26399	Web Help Desk	Solarwinds	9.8
CVE-2026-20963	Sharepoint Server	Microsoft	9.8
CVE-2026-20131	Secure Firewall Management Center	Cisco	10

© 2026 Cyble Inc. All rights reserved.

CVE-2025-32432	Cms	Craft	10
CVE-2025-54068	Livewire	Livewire	9.8
CVE-2026-33017	Langflow	Langflow Ai	9.8
CVE-2025-53521	Big Ip Apm	F5	9.8
CVE-2026-3055	Netscaler Application Delivery Controller	Citrix	9.8
CVE-2026-35616	Forticlientems	Fortinet	9.8
CVE-2026-1340	Endpoint Manager Mobile	Ivanti	9.8
CVE-2026-21643	Forticlientems	Fortinet	9.8
CVE-2025-32975	Kace Sma	Quest	10
CVE-2026-39987	Marimo	Marimo Team	9.8
CVE-2024-57726	Remote Support Software	Simplehelp	9.9
CVE-2024-7399	Magicinfo 9 Server	Samsung	9.8
CVE-2026-41940	Cpanel	Cpanel	9.8
CVE-2026-0300	Cloud Ngfw	Palo Alto Networks	9.8
CVE-2026-42208	Litellm	Berriai	9.8
CVE-2026-20182	Catalyst Sd Wan Manager	Cisco	10
CVE-2008-4250	Windows Server 2008	Microsoft	9.8
CVE-2026-48172	User End Cpanel Plugin	Litespeed	9.8
CVE-2026-45321	Arktype Adapter	Tanstack	9.6
CVE-2026-8398	Daemon Tools Lite	Avb Disc Soft	9.8
CVE-2026-48027	Nx Console	Nx	9.8
CVE-2026-0257	Cloud Ngfw	Palo Alto Networks	9.1
CVE-2026-45247	Full Page Cache Warmer For Magento 2	Mirasvit	9.8
CVE-2026-50751	Quantum Security Gateway	Checkpoint	9.3
CVE-2026-10520	Sentry	Ivanti	10
CVE-2026-35273	Peoplesoft Enterprise Peopletools	Oracle	9.8
CVE-2026-48907	Content Editor Extension	Joomla Content Editor	9.8
CVE-2026-20253	Cloud Platform	Splunk	9.8
CVE-2025-67038	Eds5000	Lantronix	9.8
CVE-2026-34909	Efg	Ubiquiti	10
CVE-2026-34908	Efg	Ubiquiti	10
CVE-2026-34910	Efg	Ubiquiti	10

© 2026 Cyble Inc. All rights reserved.

Zero-Day Vulnerabilities

The first half of 2026 saw 9 critically rated, industry-agnostic, and region-agnostic zero-day vulnerabilities. While Google, Ivanti and Microsoft reported two zero-day exploitations each, Notepad ++, PaloAlto Networks and TrendMicro reported one each.

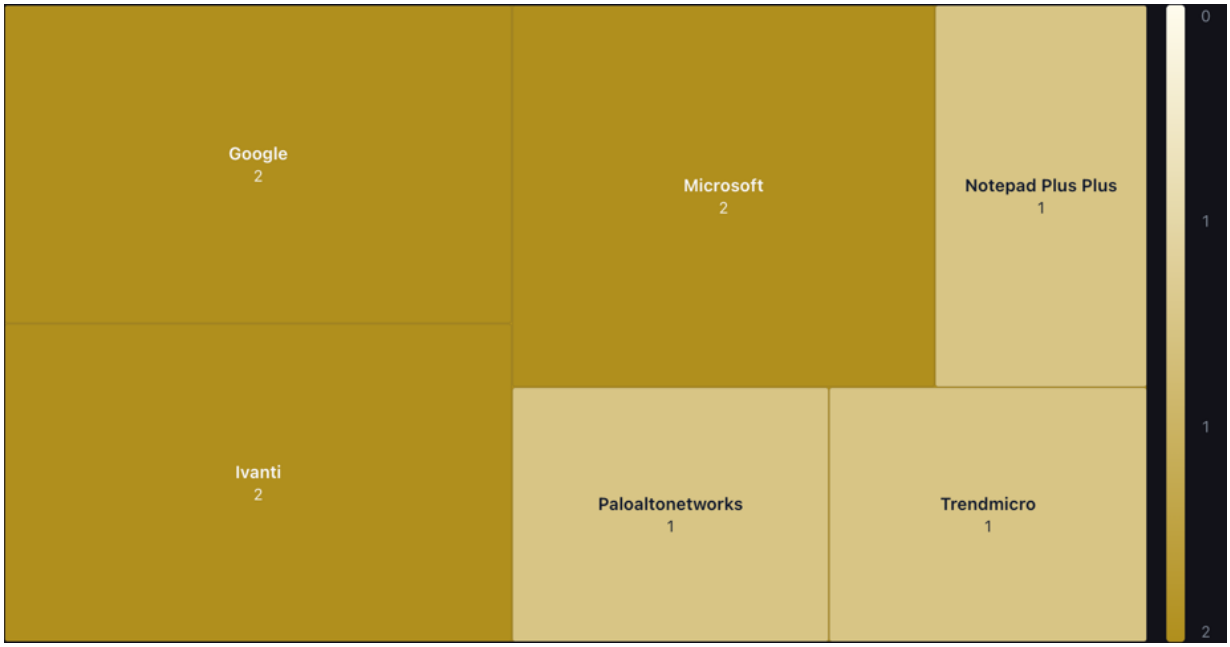


Fig.12: Zero-day affected vendors and products in H1 2026 (Source: Cyble Vision)

The active exploitation of two critical vulnerabilities, CVE-2026-1340 in Ivanti's Endpoint Manager Mobile and CVE-2026-0300 in Palo Alto Networks' Cloud NGFW, both with CVSS scores of 9.8, triggers a concerning trend of threat actors targeting edge devices and network security infrastructure. The repeated appearance of vulnerabilities in mobile management and network gateway products suggests these categories are of high interest to attackers for gaining initial access and performing lateral movement. The zero-day nature of these flaws implies a sophisticated level of threat actor capability and a compressed timeline for defenders to respond.

Organizations using these or similar public-facing applications must prioritize immediate patching where available. Furthermore, it is crucial to implement robust network segmentation and continuous monitoring to detect and contain potential compromises swiftly. The overarching trend indicates that proactive vulnerability management and a defense-in-depth strategy are essential to mitigate the growing risk from these high-impact, exploitable vulnerabilities.

© 2026 Cyble Inc. All rights reserved.

All Vulnerabilities 9

Search by CVE ID

CVE ID	CVSS (V3)	CVSS (V4)	EPSS	PRODUCT	VENDOR	IDENTIFIED ON	DESCRIPTION
CVE-2026-34926 CISA KEV ZERO DAY	6.7	0.0	12.68	trendai apex one	trendmicro	21 May 2026	A directory traversal vulnerability in the Apex One (on-premise) server could allow a pre-authenticated local attacker to modify a key table on...
CVE-2026-45498 CISA KEV ZERO DAY	7.5	0.0	63.08	defender antimalware platform	microsoft	20 May 2026	Microsoft Defender Denial of Service Vulnerability
CVE-2026-41091 CISA KEV ZERO DAY	7.8	0.0	8.37	malware protection engine	microsoft	20 May 2026	Improper link resolution before file access ('link following') in Microsoft Defender allows an authorized attacker to elevate privileges locally.
CVE-2026-6973 CISA KEV ZERO DAY	7.2	0.0	34.45	endpoint manager mobile	ivanti	07 May 2026	An Improper Input Validation in Ivanti EPMM before versions 12.6.1.1, 12.7.0.1, and 12.8.0.1 allows a remotely authenticated user...
CVE-2026-0300 CISA KEV ZERO DAY OT-ICS	9.8	9.3	36.16	cloud ngfw	paloaltonetworks	06 May 2026	A buffer overflow vulnerability in the User-ID™ Authentication Portal (aka Captive Portal) service of Palo Alto Networks PAN-OS software allows a...

Fig.13: All zero-days listed with critical indicators and patching info on Cyble Vision



© 2026 Cyble Inc. All rights reserved.



Hacktivism

During the first half of 2026, the hacktivism landscape was characterized by a consistent stream of activity driven by diverse geopolitical and ideological motivations.

Cyble Research and Intelligence Labs (CRIL) monitored threat groups and channels, with actors such as `Infrastructure Destruction Squad`, `SOLDADOS DIGITALES - UNIÓN AMERICANA`, and `Anonymous #FreeTurtleIsland` prominently featuring in the dissemination of attack claims.

The primary tactics employed by these groups included disruptive Distributed Denial-of-Service (DDoS) attacks and data exfiltration, culminating in public data leaks, with an estimated 21 distinct data dump posts identified during this period.

The scale of these operations impacted approximately 66 unique domains, demonstrating a broad targeting strategy. While this report focuses on the BFSI sector, the observed campaigns were not siloed, affecting a wide spectrum of industries including Government, Technology and Healthcare, indicating that financial institutions can be impacted both directly and as collateral damage in larger, ideologically driven campaigns.

Blazer Team Attack

Based on activity observed in the Blazer Team Attack channel, the group's primary focus was on reconnaissance and executing Layer 7 Distributed Denial-of-Service (DDoS) attacks. Their methodology involved initial information gathering, such as IP lookups and scanning for security protections on websites, followed by claims of launching DDoS attacks using various botnet command-and-control engines.

The targets were diverse and predominantly US-based, including high-profile government entities like NASA (data.nasa.gov) and major corporations such as Netflix (netflix.com).

Infrastructure Destruction Squad

The hacktivist channel 'Infrastructure Destruction Squad' demonstrated a strong anti-US focus, primarily threatening disruptive attacks against American critical infrastructure. The group issued specific threats against power grids and hospitals, promoting the use of ransomware and a tool named 'VoltRuptor' for these purposes. In one instance, the group published a detailed guide for exploiting and disabling a Network Control System, including alleged IP addresses and credentials.

© 2026 Cyble Inc. All rights reserved.

Industry News

Keylogger Found Harvesting Credentials on Top US Bank's Employee Store

Security researchers discovered a keylogger planted on the employee merchandise store of a top US bank, potentially exposing the credentials and personal data of over 200,000 employees.

The keylogger was designed to intercept login credentials, payment card numbers, and personal information. The attack utilized a sophisticated two-stage loader to evade detection. This incident highlights the vulnerability of internal portals and third-party platforms, which are often overlooked in security audits.

The stolen data was exfiltrated via an image beacon, bypassing security controls. The attack is linked to previous campaigns, including one targeting the Green Bay Packers. Standard security tools failed to detect the threat, emphasizing the need for specialized detection tools for ecommerce environments. The bank's lack of a security[.]txt file made it difficult to report the breach. The keylogger poses a significant risk to the BFSI industry.

US Charges 87 in Major ATM Jackpotting Scheme Linked to Tren de Aragua

A major international cybercrime case involving an ATM jackpotting scheme linked to the violent transnational gang Tren de Aragua (TdA) surfaced earlier this year. The indictment charged 87 individuals, highlighting the growing threat of malware-driven attacks on financial institutions in the United States. The group used Ploutus malware to hack ATMs and force cash withdrawals, with proceeds split among members. Authorities are focused on dismantling TdA's financial pipeline and stopping their funding through ATM jackpotting crimes. The gang, involved in various criminal activities, sees financial cybercrime as a key revenue stream. If convicted, defendants face significant prison terms for their roles in the scheme.

Data breach at fintech firm Betterment exposes 1.4 million accounts

In January, a data breach at fintech firm Betterment exposed 1.4 million accounts to hackers who stole email addresses and personal information. The breach involved a social engineering attack where threat actors sent fraudulent emails to customers, attempting to scam them into sending cryptocurrency. Betterment also faced a distributed denial-of-service (DDoS) attack and extortion attempts. Despite the breach, Betterment confirmed that no customer accounts were compromised, with the primary impact being on customer contact information.

BridgePay Payment Gateway Hit by Ransomware, Causing Nationwide Outages

BridgePay Network Solutions, a major U.S. payment gateway provider, experienced a ransomware attack causing a widespread outage, disrupting card processing for merchants nationwide. The attack led to degraded performance in various systems, including the Gateway.ltstgate.com

© 2026 Cyble Inc. All rights reserved.

virtual terminal and API. Despite no compromise of payment card data, core services like the BridgePay Gateway API and virtual terminals were affected. Merchants had to resort to cash-only operations, and various entities, including the City of Palm Bay and City of Frisco, faced online service disruptions. BridgePay engaged federal authorities and cybersecurity teams for recovery efforts, emphasizing customer protection.

Marquis sues firewall provider SonicWall, alleges security failings with its firewall backup led to ransomware attack

Fintech giant Marquis is suing its firewall provider SonicWall due to a breach that allowed hackers to deploy ransomware on Marquis' network. The lawsuit claims that SonicWall's security failings led to the exposure of critical security information, resulting in significant harm to Marquis. The hackers stole sensitive data, including personally identifiable information, from Marquis' network. The ransomware attack affected hundreds of banks and credit unions, impacting a significant number of individuals in the U.S. The breach was attributed to a vulnerability in SonicWall's systems, which allowed threat actors to access customer firewall configuration backup files. Marquis is seeking compensation and further information about the root cause of the breach through litigation.



© 2026 Cyble Inc. All rights reserved.



Conclusion

During the first half of 2026, the United States' Banking, Financial Services, and Insurance sector faced a severe and multi-faceted threat landscape characterized by several key trends.

A primary threat was the widespread compromise and sale of massive datasets containing sensitive customer PII and financial information on cybercrime forums, alongside offerings of unauthorized access to financial platforms.

Concurrently, the sector endured persistent ransomware attacks, with a concentrated group of threat actors, led by Qilin, Akira, and Dragonforce, accounting for nearly 50% of all incidents and impacting a wide spectrum of financial entities. These intrusions were frequently facilitated by the active exploitation of critical zero-day and known vulnerabilities in widely deployed, internet-facing enterprise and network infrastructure.

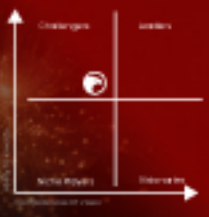
The period was also marked by highly sophisticated, state-sponsored campaigns that utilized advanced social engineering and AI-driven tactics to orchestrate significant cryptocurrency heists, resulting in substantial financial losses and underscoring a complex and dynamic risk environment for the industry.

© 2026 Cyble Inc. All rights reserved.

Industry Recognition

Gartner

Cyble Recognized as a **Challenger** in the **2026 Gartner® Magic Quadrant ™** for Cyberthreat Intelligence Technologies



QKS Group

SPARK Matrix™ 2026

LEADER

Cyble Named as a Leader in Digital Threat Intelligence Management

FROST & SULLIVAN



Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

FORRESTER®

Cyble Recognized in Forrester's **External Threat Intelligence** Service Providers Landscape, **Q1 2026 report**

Gartner

Cyble Recognized in **Three Gartner® Hype Cyble™ Reports for the Second Consecutive Year 2025, TechScape 2025 & More**

AMERICA'S BEST STARTUP EMPLOYERS | Forbes 2026

Recognized as one of America's Best Startup Employers by Forbes

WINNERS 2026

Cyble Secures Four Prestigious Honors at the 2026 Global Infosec Awards

Gartner Peer Insights.

Ranked No.1 among the top Security Threat Intelligence and Brand Protection Providers.

4.8/5



Cyble Named in America's Greatest Startup Workplaces 2025, By Newsweek



Cyble Wins Three Top InfoSec Innovator 2025 Awards



G2

Named a leader in the G2 Grid for Dark Web Monitoring and Threat Intelligence

2026 WINNER CYBER SECURITY EXCELLENCE AWARDS

Cyble Earns **36 Badges in G2 Summer 2026** Reports, Highlighting Leadership in AI-Powered Cybersecurity

SUMMER 2026 Leader

Y Combinator

Cyble featured among AI startups backed by Y Combinator (YC) 2025

OUR INVESTORS

BLACKBIRD · KING RIVER · Koogle.co · SUMMIT PEAK · innov8 · BizLabs · Y Combinator · SPIDER CAPITAL · svb Silicon Valley Bank

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067

All Rights Reserved | www.cyble.com


Stay Ahead of the Next Threat
REQUEST YOUR DEMO NOW!
Experience the power of predictive security with Cyble.