

THREAT LANDSCAPE DIGEST

09/2026

Date: 06/10/2026

TLP: CLEAR

Author: IstroSec

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

LATEST RANSOMWARE INTELLIGENCE..... 4

ATTACKED COMPANIES 6

Distributed Denial of Service (DDoS) Attacks Detected in September 8

VULNERABILITY INTELLIGENCE 10

EXECUTIVE SUMMARY

In September 2026, the threat landscape was characterized by 156 recorded ransomware victims, with Germany emerging as the most targeted country with 38 victims, followed by Italy with 28 and France with 23. The threat actor group known as The Gentlemen was the most dominant ransomware group with 27 victims, heavily impacting the manufacturing sector which saw 29 total victims, while specific regional targets included Partners Group SK in Slovakia and three entities in Czechia. Distributed denial of service activity in the European Union comprised 42 attacks, all attributed to the threat actor NoName057 (16), which primarily targeted the government sector with 24 attacks and focused geographically on Germany, Poland, and Italy. Alongside these attacks, the actively exploited vulnerability landscape recorded 43 vulnerabilities, representing a 38.7% increase compared to the previous month. Products most affected by these vulnerabilities included Citrix NetScaler, JFrog Artifactory, MikroTik RouterOS, and the Linux Kernel, which each recorded three vulnerabilities.

Most seen Tactics, Techniques & Procedures (TTPs) in September

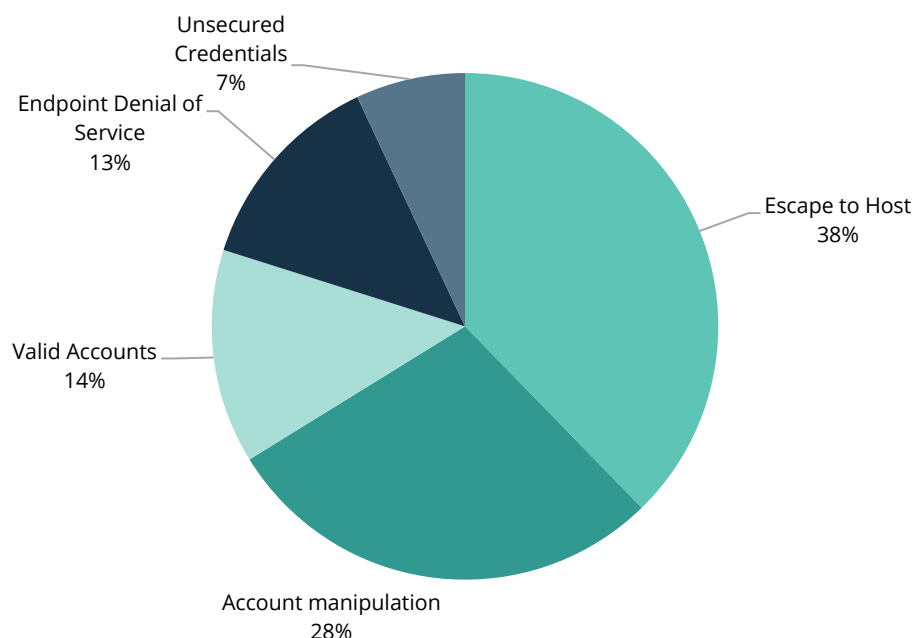


Figure 1: Most Frequently Observed ATT&CK Techniques in September

LATEST RANSOMWARE INTELLIGENCE

During September 2026, a total of 156 ransomware victims were recorded, with the threat actor group known as The Gentlemen emerging as the most dominant group with 27 victims, followed by Qilin with 16 victims and Safepay with 14 victims. Germany was the most targeted country during this period with 38 victims, followed by Italy with 28 victims and France with 23 victims. The manufacturing sector experienced the highest volume of activity with 29 victims, while the professional services and technology sectors each recorded 19 victims. Within the predefined countries of interest, Slovakia recorded a single victim, Partners Group SK, which was targeted by Qilin. Czechia saw three victims, which included sumperk.cz attacked by Safepay, Seznam targeted by MedusaLocker, and SEVENOAKS s.r.o. compromised by Emperador.

Most Active Ransomware Groups in September

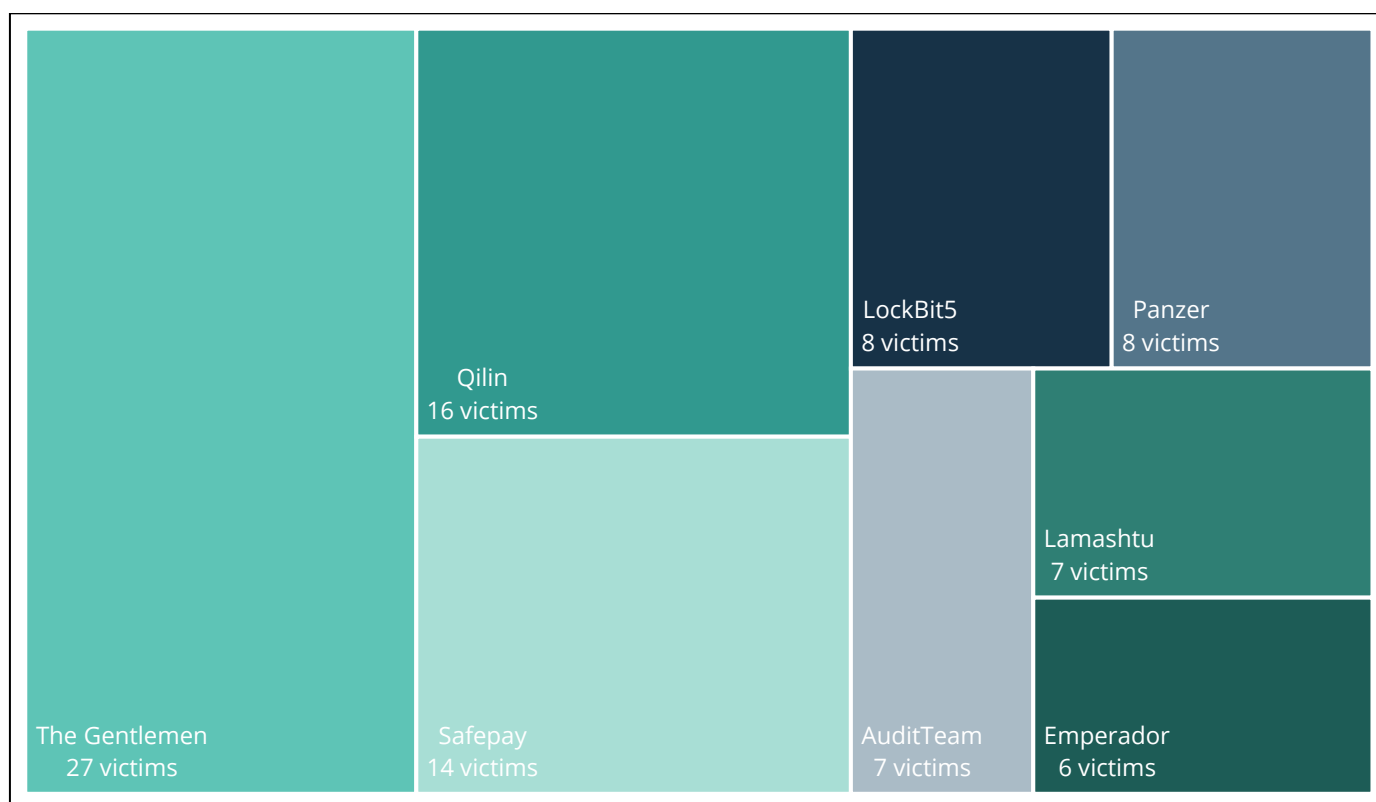


Figure 2: Most Active Ransomware Groups in September and Number of their Victims

The Most Affected EU Countries in September

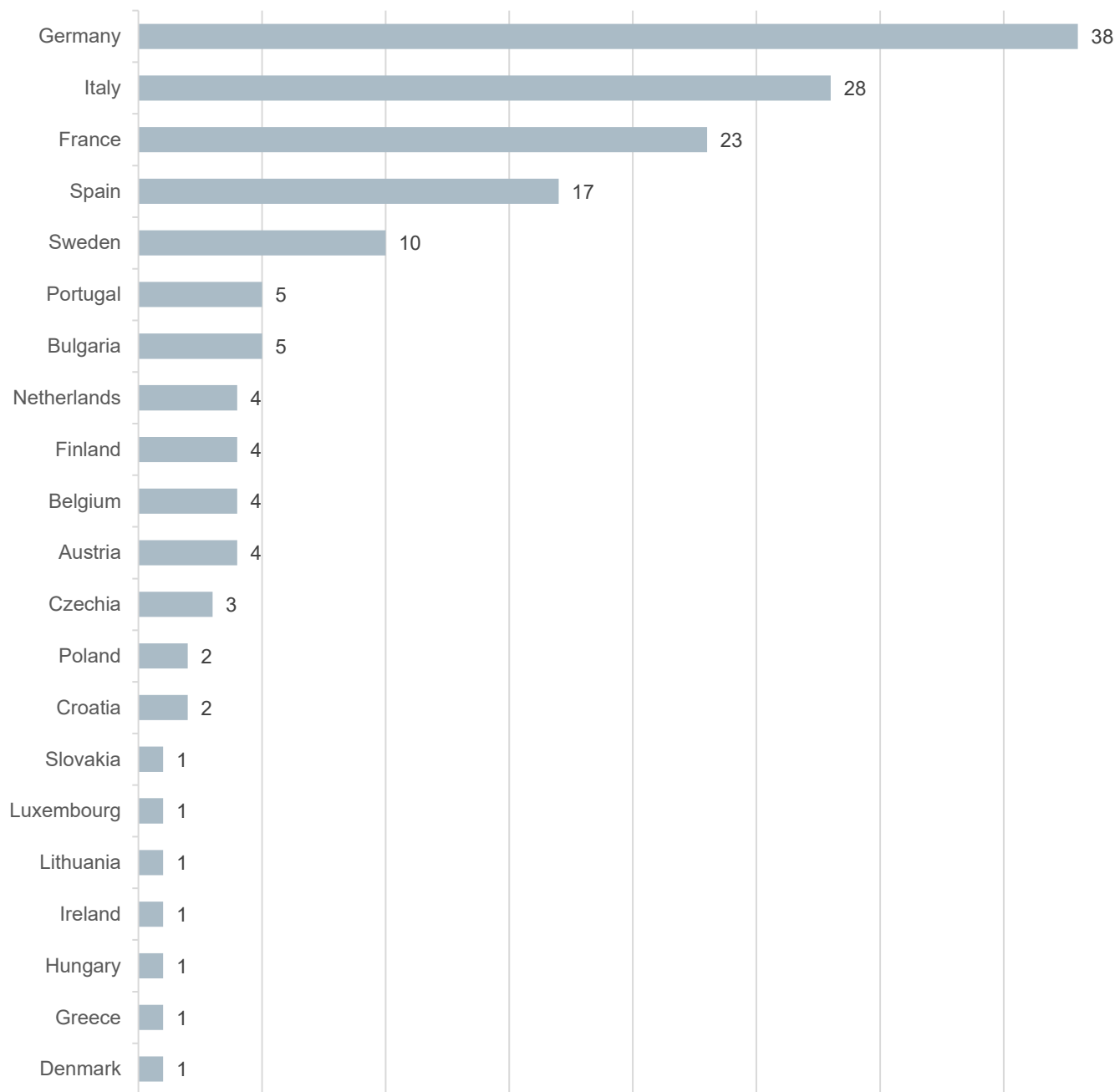


Figure 3: Most Affected EU Countries by Ransomware

The Most Affected Sectors in September

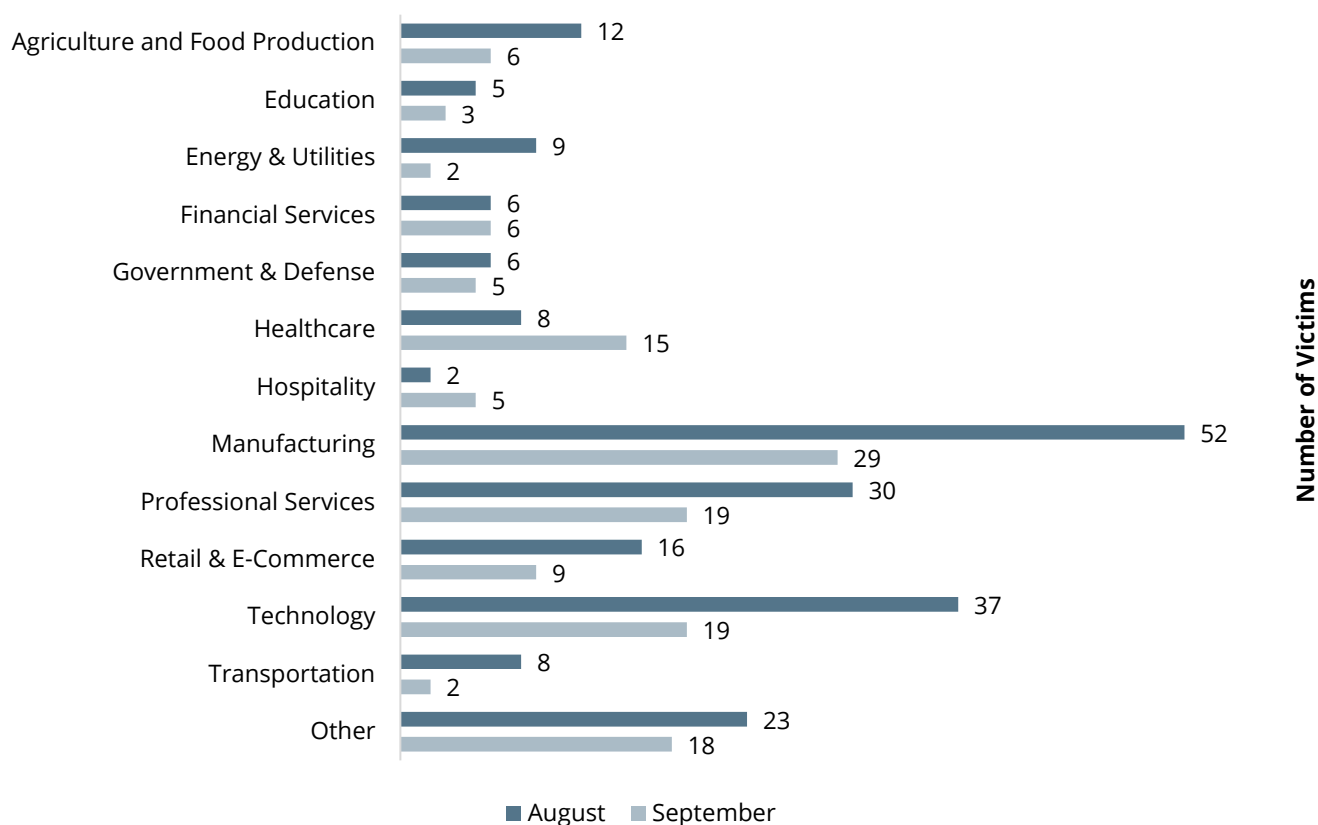


Figure 4: Most Affected Sectors in the EU

ATTACKED COMPANIES

Slovakia

Partners Group SK

Attacked by **Qilin** on **2026-09-07**.

Description: Partners Group SK is a financial services company based in Slovakia. The firm specializes in providing financial planning and investment intermediation services.

Sector: Financial Services

Czechia

sumperk.cz

Attacked by **Safepay** on **2026-09-28**.

Description: The victim is the municipal administration of Šumperk, a town located in Czechia. The organization manages local public services and community affairs for its residents.

Sector: Government

Seznam

Attacked by **MedusaLocker** on **2026-09-23**.

Description: Seznam is a Czech technology company that operates an internet portal, search engine, and digital advertising platform. The threat actors claim to have extracted email communications from the organization.

Sector: Technology

SEVENOAKS s.r.o.

Attacked by **Emperador** on **2026-09-16**.

Description: SEVENOAKS s.r.o. is an information technology and systems integration company based in Prague, Czechia. The firm provides custom software development, IT infrastructure design, and electrical installation services.

Sector: Technology

Recommendations:

In case you recognize any of your suppliers or business partners on the list above, exercise heightened vigilance against potential Business Email Compromise (BEC) attacks. Exposed victim's information may be leveraged to craft highly targeted and convincing fraudulent communications.

DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS DETECTED IN SEPTEMBER

During September 2026, a total of 42 DDoS attacks were recorded against EU countries, with all 42 of these incidents attributed to the threat actor known as NoName057 (16). Germany was the most targeted country with 15 attacks, followed by Poland with 12 attacks, Italy with 10 attacks, and the Czech Republic with 5 attacks. The government sector bore the brunt of the activity with 24 attacks, while other targeted sectors included education with 4 attacks, manufacturing with 3 attacks, transportation and telecommunications with 2 attacks each, and construction and financial services with 1 attack each, alongside 5 attacks categorized as other. Daily activity peaked on September 7, 2026, with 5 attacks, while September 8, September 12, September 13, and September 23, 2026, each saw 4 attacks.

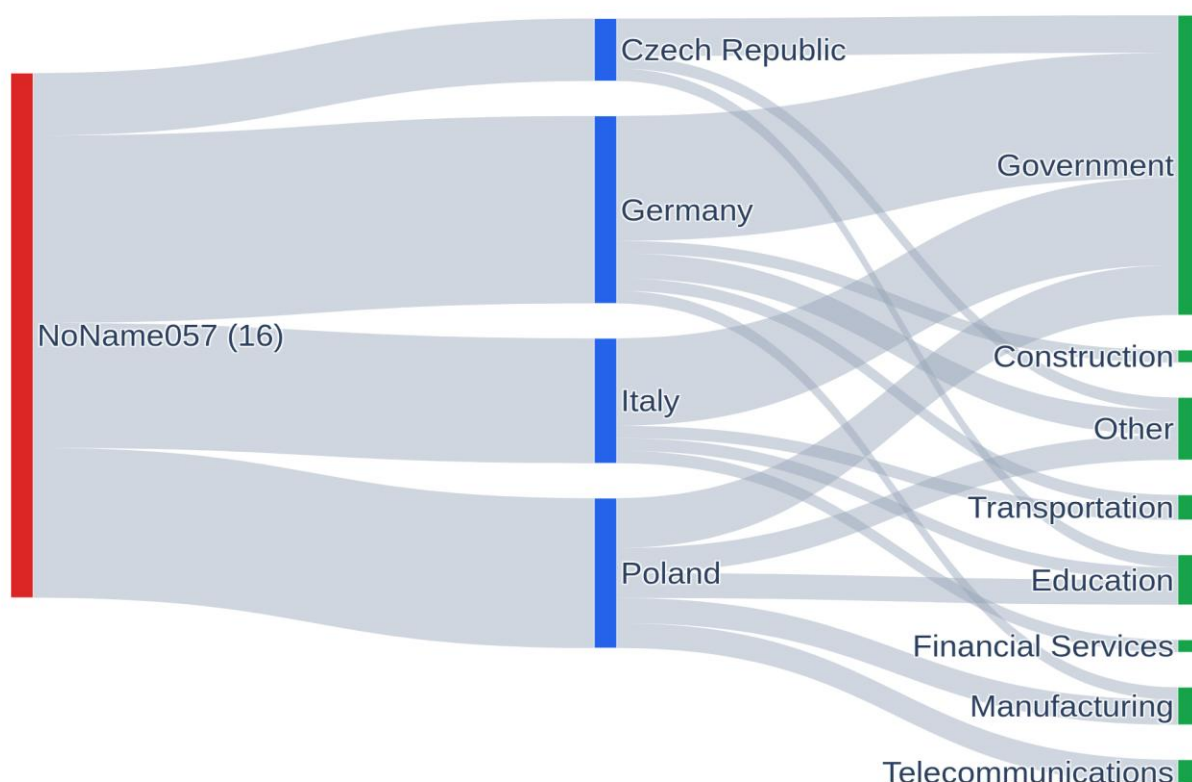


Figure 5: Diagram Showing Attacking Group à Targeted Country à Targeted Sector

Histogram of DDoS Attacks

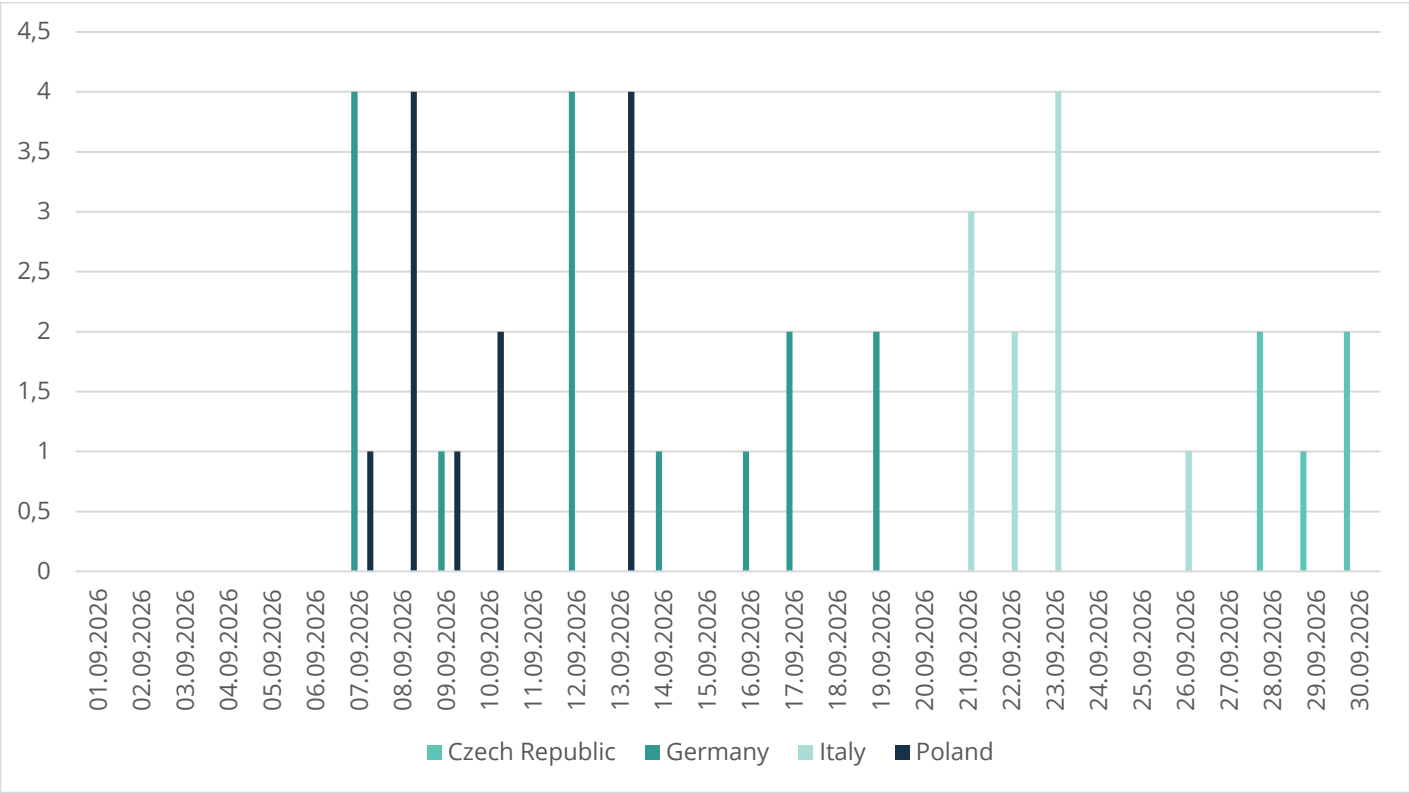


Figure 6: Histogram of Detected DDoS Attacks

VULNERABILITY INTELLIGENCE

In September we registered 43 actively exploited vulnerabilities, which represents 38.7% increase compared to last month.

In September 2026, the actively exploited vulnerability landscape recorded 43 vulnerabilities. This represents a 38.7% increase compared to the previous month, which had 31 vulnerabilities. The products most affected during this timeframe, each with three vulnerabilities, were Citrix NetScaler, JFrog Artifactory, MikroTik RouterOS, and the Linux Kernel. Products experiencing two vulnerabilities each included Adobe Commerce and Magento, Google Chromium V8, Check Point Multiple Products, SonicWall SMA1000 Appliances, and Microsoft Windows. GitLab Community Edition and Enterprise Edition was also affected, recording one vulnerability.

Number of Known Exploited Vulnerabilities Over Months

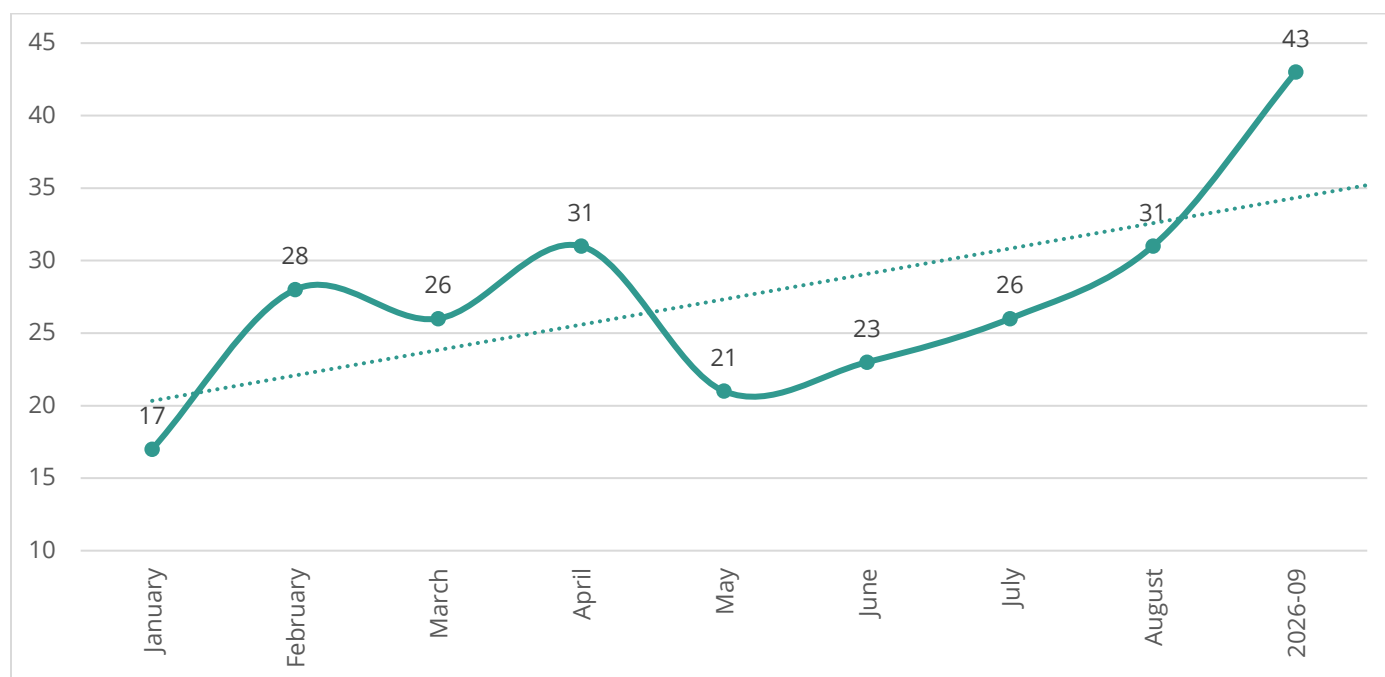


Figure 7: Number of CISA KEVs Published per Month

Below, you can find all the Known Exploited Vulnerabilities (KEV) published in September, enriched by the Exploit Prediction Scoring System (EPSS) for better clarity of what to prioritize:

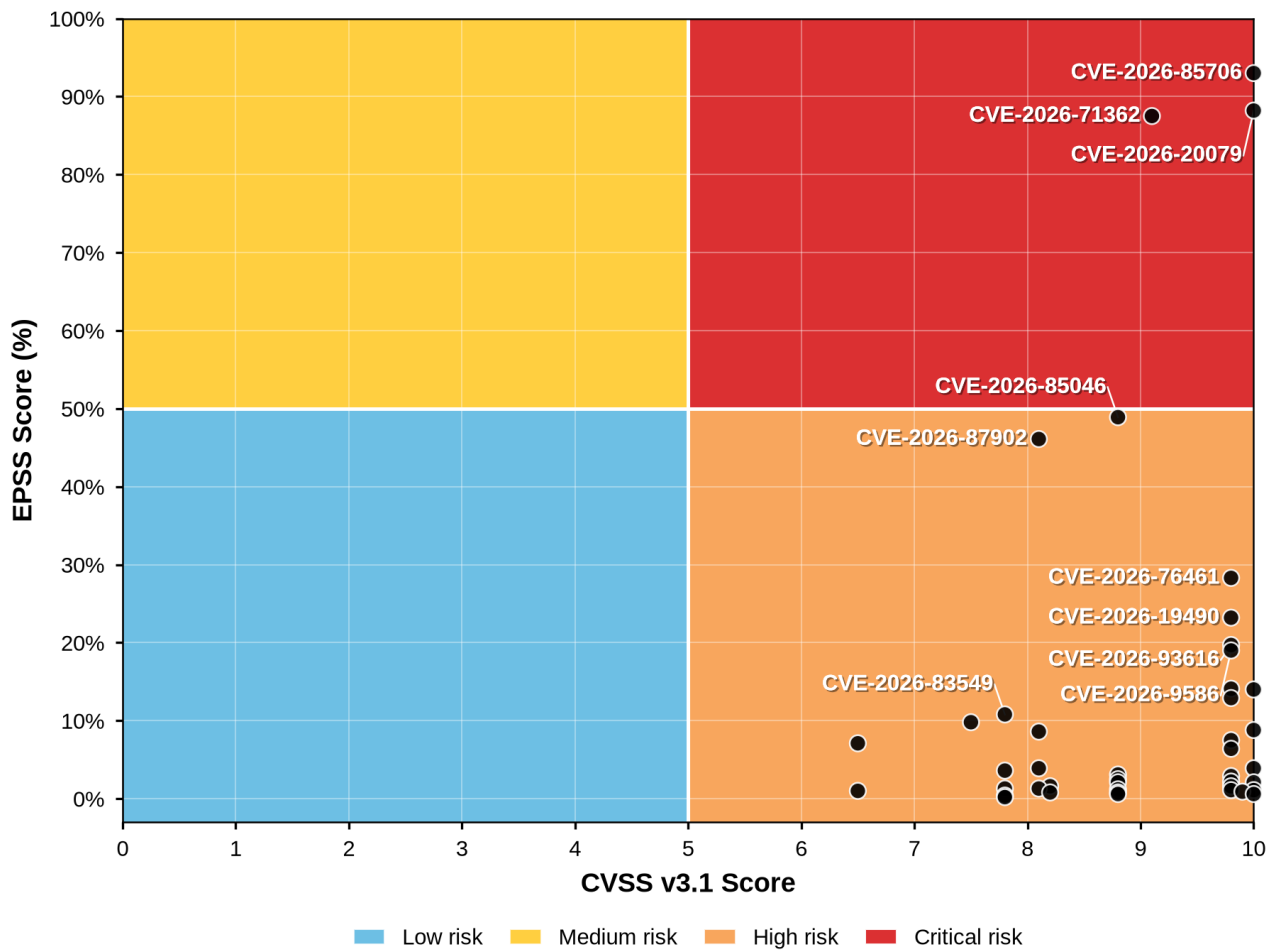


Figure 8: EPSS x CVSS Matrix of Actively Exploited Vulnerabilities

We strongly recommend reviewing the list, sorted by criticality and prioritizing immediate patching for any vulnerabilities identified as affecting systems within your infrastructure. Timely patching is critical to reduce exposure to exploits. If a patch is unavailable, isolate the affected device and follow the vendor's official guidance.

List of Actively Exploited Vulnerabilities

CVE	Description	Affected Product	EPSS %
<u>CVE-2026-85706</u>	GitLab Community Edition and Enterprise Edition contains a path traversal vulnerability that allows an unauthenticated user to read arbitrary files due to an improper path confinement and	GitLab Community	99.8%

	missing authentication enforcement in the repository commits API.	Edition and Enterprise Edition	
<u>CVE-2026-20079</u>	Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management contain an authentication Bypass using an alternate path or channel vulnerability that could allow an unauthenticated, remote attacker to bypass authentication and execute script files on an affected device to obtain root access to the underlying operating system.	Cisco Secure Firewall Management Center (FMC) and Security Cloud Control (SCC) Firewall Management	99.8%
<u>CVE-2026-71362</u>	Adobe Commerce and Magento contains an incorrect authorization vulnerability that could allow an attacker to leverage this vulnerability to gain elevated access to sensitive resources without any user interaction.	Adobe Commerce and Magento	99.8%
<u>CVE-2026-85046</u>	Google Chromium V8 contains a type confusion vulnerability that allows a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. This vulnerability could affect multiple web browsers that utilize Chromium, including, but not limited to, Google Chrome, Microsoft Edge, and Opera.	Google Chromium V8	98.8%
<u>CVE-2026-87902</u>	WordPress Core contains a remote file inclusion vulnerability which could allow an unauthenticated attacker to make page-template resolution include a chosen readable local `.php` file outside the active theme directories, leading to remote code execution.	WordPress Core	98.8%
<u>CVE-2026-76461</u>	Cisco AsyncOS software for Cisco Secure Email Gateway (SEG) contains a SQL injection vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system.	Cisco Secure Email Gateway	98.1%

<u>CVE-2026-19490</u>	Citrix NetScaler ADC and NetScaler Gateway contain an authentication-bypass vulnerability involving an alternate path or channel. When the NetScaler appliance is configured as an AAA virtual server or as a Gateway (SSL VPN, ICA Proxy, CVPN, or RDP Proxy), an unauthenticated remote threat actor may be able to bypass authentication.	Citrix NetScaler	97.7%
<u>CVE-2026-93616</u>	Check Point Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, and SmartEvent contain a path traversal vulnerability that allows an unauthenticated attacker to upload and execute arbitrary scripts.	Check Point Multiple Products	97.3%
<u>CVE-2026-9586</u>	Sangoma Switchvox contains a SQL injection vulnerability which allows an unauthenticated remote attacker to execute arbitrary SQL statements against the backend PostgreSQL database using a single crafted request, including database operations and remote code execution.	Sangoma Switchvox	97.2%
<u>CVE-2026-82329</u>	JFrog Artifactory contains an improper authentication vulnerability that under default configuration can allow an unauthenticated attacker with network access to obtain administrative privileges.	JFrog Artifactory	96.5%
<u>CVE-2026-76460</u>	Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) contain an incorrect use of privileged APIs vulnerability that could allow an unauthenticated, remote attacker to gain unauthorized access to the affected device by bypassing the web-based management interface.	Cisco Identity Services Engine	96.5%
<u>CVE-2026-86218</u>	N-able N-central contains a static code injection vulnerability that could allow for pre-authentication remote code execution.	N-able N-central	96.2%

<u>CVE-2026-83549</u>	SonicWall SMA1000 Appliances contains an OS command injection vulnerability that could enable a remote authenticated attacker as administrator to execute arbitrary OS commands, resulting in remote code execution.	SonicWall SMA1000 Appliances	95.7%
<u>CVE-2026-42018</u>	JFrog Artifactory contains an improper authentication vulnerability that could return an internal anonymous-user token to an unauthenticated caller when anonymous access is disabled, potentially exposing sensitive resources.	JFrog Artifactory	95.4%
<u>CVE-2026-83548</u>	SonicWall SMA1000 Appliances contains a server-side request forgery vulnerability that could allow a remote unauthenticated attacker to gain unauthorized access to sensitive functionality and perform unauthorized operations.	SonicWall SMA1000 Appliances	95.0%
<u>CVE-2026-42016</u>	JFrog Artifactory contains an incorrect authorization vulnerability that leads to a privilege escalation attack due to a validation check of the token signature/issuer and not the token's scope.	JFrog Artifactory	95.0%
<u>CVE-2026-85102</u>	Check Point Security Gateway and Check Point Spark Firewall using Site to Site VPN or Remote Access VPN contain an improper certificate validation vulnerability which could allow an unauthenticated remote attacker to execute arbitrary code on the Gateway.	Check Point Multiple Products	94.3%
<u>CVE-2026-48710</u>	Kludex Starlette contains a HTTP request/response smuggling vulnerability that could allow attackers to inject paths into the host part, prepending the actual path leading to issues such as authentication bypass when the authentication depends on the reconstructed URL's path. This vulnerability could be chained with CVE-2026-42271.	Kludex Starlette	94.0%

<u>CVE-2026-86060</u>	MikroTik RouterOS contains an improper neutralization of argument delimiters in a command vulnerability which allows an attacker to change the trusted RouterOS policy mask, leading to privilege escalation.	MikroTik RouterOS	93.5%
<u>CVE-2025-25249</u>	Fortinet FortiOS, FortiSwitchManager, and FortiSASE contain a heap-based buffer overflow vulnerability that allows an attacker to execute unauthorized code or commands via specially crafted packets.	Fortinet Multiple Products	89.9%
<u>CVE-2026-75650</u>	Adobe Commerce and Magento Open Source contain an improper neutralization of special elements used in a template engine vulnerability that could allow an attacker to execute arbitrary code.	Adobe Commerce and Magento	90.1%
<u>CVE-2026-85880</u>	Microsoft Windows Advanced Local Procedure Call contains a heap-based buffer overflow vulnerability that allows an attacker to elevate privileges locally.	Microsoft Windows	89.2%
<u>CVE-2026-87491</u>	Google Chromium V8 contains an out of bounds write vulnerability that allows a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. This vulnerability could affect multiple web browsers that utilize Chromium, including, but not limited to, Google Chrome, Microsoft Edge, and Opera.	Google Chromium V8	87.5%
<u>CVE-2025-39682</u>	Linux Kernel contains an improper check for unusual or exceptional conditions vulnerability in the TLS receive path which allows a zero-length record retrieved from the rx_list to bypass the intended recvmmsg() record-type handling, potentially causing subsequent TLS records to be processed using incorrect zero-copy and queuing assumptions. The impacted product(s) could be end-of-life (EoL) and/or end-of-service (EoS).	Linux Kernel	86.4%

	Users are advised to discontinue use and/or transition to a supported version.		
<u>CVE-2026-7273</u>	Zyxel GS1900 series switches contain a stack-based buffer overflow vulnerability in the CGI program which could allow a LAN-based, unauthenticated attacker to exploit the flaw and potentially execute OS commands via a crafted HTTP request.	Zyxel GS1900 Series Switches	84.2%
<u>CVE-2026-94127</u>	F5 BIG-IP APM contains a heap-based buffer overflow vulnerability when access policy and an OAuth profile are configured on a virtual server. This vulnerability could allow an unauthenticated attacker to perform remote code execution.	F5 BIG-IP APM	82.1%
<u>CVE-2026-49869</u>	Kestra OSS contains an OS command injection vulnerability that could allow an unauthenticated remote attacker to create and execute arbitrary workflows without credentials.	Kestra Kestra OSS	81.0%
<u>CVE-2026-65660</u>	Microsoft SharePoint contains a code injection vulnerability which could allow an authorized attacker to execute code over a network.	Microsoft SharePoint	81.1%
<u>CVE-2026-67277</u>	MikroTik RouterOS contains a missing authentication for critical function vulnerability which allows kernel memory disclosure and denial of service in the btest service.	MikroTik RouterOS	74.4%
<u>CVE-2026-76504</u>	Cisco Catalyst SD-WAN Manager contains a hex encoding vulnerability that could allow an unauthenticated, remote attacker to access an affected system with privileges of the admin user due to improper handling of URI encoding in an HTTP request.	Cisco Catalyst SD-WAN Manager	74.6%
<u>CVE-2025-39964</u>	Linux Kernel contains a race condition vulnerability which allows concurrent writes to the same AF_ALG socket causing data to be	Linux Kernel	68.9%

	unpredictably interleaved and creating inconsistencies in the socket's internal state.		
<u>CVE-2026-88772</u>	Citrix NetScaler ADC and NetScaler Gateway contain an improper restriction of operations within the bounds of a memory buffer vulnerability that could allow for remote code execution or denial of service	Citrix NetScaler	69.5%
<u>CVE-2026-86950</u>	Apple iOS, macOS, and iPadOS contain an out-of-bounds write vulnerability in CoreGraphics that may lead to arbitrary code execution.	Apple Multiple Products	68.2%
<u>CVE-2026-88771</u>	Citrix NetScaler ADC and NetScaler Gateway contain an improper input validation vulnerability that could allow an unauthenticated attacker to execute arbitrary commands.	Citrix NetScaler	64.0%
<u>CVE-2026-93952</u>	Arista VeloCloud Orchestrator (VCO) on-prem contains an improper input validation vulnerability that may allow a remote attacker to access privileged internal functionality and impact the VCO host. Successful exploitation may compromise the confidentiality, integrity, and availability of the orchestrator and data managed by the orchestrator.	Arista VeloCloud Orchestrator	63.4%
<u>CVE-2026-67279</u>	Mikrotik RouterOS contains an improper enforcement of behavioral workflow vulnerability that could allow an unauthenticated client to open a session channel and send an exec request. This vulnerability can be chained to achieve unauthenticated exploitation of CVE-2026-86060.	MikroTik RouterOS	62.4%
<u>CVE-2026-84869</u>	ConnectWise ScreenConnect contains both an improper privilege management and missing authorization vulnerability that may allow an attacker to transfer and execute files through an	ConnectWise ScreenConnect	59.1%

	active remote session without authorization or host confirmation.		
<u>CVE-2026-53266</u>	Linux Kernel contains an out-of-bounds write vulnerability in the ebttables SNAT target which allows an ARP sender hardware address rewrite to write directly into a nonlinear socket-buffer fragment backed by a splice-imported file page. The impacted product(s) could be end-of-life (EoL) and/or end-of-service (EoS). Users are advised to discontinue use and/or transition to a supported version.	Linux Kernel	56.0%
<u>CVE-2026-59822</u>	BerriAI LiteLLM contains an improper authentication vulnerability in the MCP Streamable HTTP endpoint that could allow an unauthenticated attacker to establish an authenticated MCP session using an arbitrary Bearer token.	BerriAI LiteLLM	56.3%
<u>CVE-2026-5430</u>	WSO2 API Control Plane, API Manager, Traffic Manager & Universal Gateway contain a path traversal vulnerability that could allow for unrestricted file upload and lead to remote code execution.	WSO2 Multiple Products	46.3%
<u>CVE-2026-58704</u>	Google Pixel devices contain an improper authorization vulnerability in the cellular modem. A logic error may allow an attacker to bypass permission checks and escalate privileges.	Google Pixel	46.4%
<u>CVE-2026-81963</u>	Microsoft Windows Update Stack contains a link following vulnerability that allows a local attacker to escalate privileges locally up to SYSTEM.	Microsoft Windows	31.2%
<u>CVE-2026-87886</u>	Acronis Backup plugin for cPanel & WHM and extension for Plesk contains an incorrect default permissions vulnerability that could allow for privilege escalation.	Acronis Backup	12.9%

We are Here to Help

IstroSec is a trusted European cybersecurity vendor, combining proprietary R&D and global technology alliances to deliver advanced defense, respond and offensive services, strengthening organizational resilience against complex threats with innovation, measurable protection, and strategic trust. Whether you need to prevent, detect or respond to a cyber threat, contact us to find out how we can help protect your organization.

CONTACT US

 www.istrosec.com  [@IstroSec](https://www.linkedin.com/company/istrosec)



DIGITAL FORENSIC & INCIDENT RESPONSE

Incident (IR) Preparedness
Recovery (IR) Readiness
Incident (IR) Response
Retainer



MANAGED DEFENSE

IstroMDR & IstroSOC
Defensive Intelligence
Threat Hunting



OFFENSIVE SECURITY

Continuous Threat
Exposure Monitoring
Threat Intel Led Pen Testing
Cyber Resilience Testing



ADVISORY

vCISO & Trusted Advisor
Regulatory Compliance
Awareness and Trainings

Disclaimer: This digest is compiled exclusively from publicly available, open-source information. It intentionally does not include intelligence from private threat feeds, non-public incident reports, or attacks that were never publicly disclosed or claimed. As such, the figures and trends presented here should be understood as a partial view of the threat landscape rather than a complete or authoritative account. The actual volume and scope of incidents during this period may be materially higher than what is reflected in publicly available sources.