IstroSec

THREAT LANDSCAPE DIGEST 10/2026

Date: 02/11/2026

TLP: **CLEAR**

Author: **IstroSec**

TABLE OF CONTENTS

EXECUTIVE SUMMARY **3**
LATEST RANSOMWARE INTELLIGENCE **4**
ATTACKED COMPANIES *7*
Distributed Denial of Service (DDoS) Attacks Detected in October **9**
VULNERABILITY INTELLIGENCE **11**

EXECUTIVE SUMMARY

In October 2026, the threat landscape recorded 182 ransomware victims in the European Union (EU), driven primarily by the dominant threat actor groups Qilin and The Gentlemen with 28 and 25 victims, respectively. Germany was the most targeted country with 53 ransomware victims, while Manufacturing led all impacted sectors with 42 victims. Concurrent distributed denial of service activity comprised 27 attacks targeting European Union countries, all attributed to NoName057 (16), with France absorbing 16 attacks and the Government sector receiving 16 attacks. Temporal DDoS activity peaked on October 5, 2026, with six recorded attacks. Meanwhile, the volume of actively exploited vulnerabilities declined to 36 additions, representing a 16.3% decrease from the 43 additions recorded in September 2026. Within these vulnerability additions, Plex Media Server emerged as the most affected product with four vulnerabilities, followed by Ivanti Connect Secure with three vulnerabilities.

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

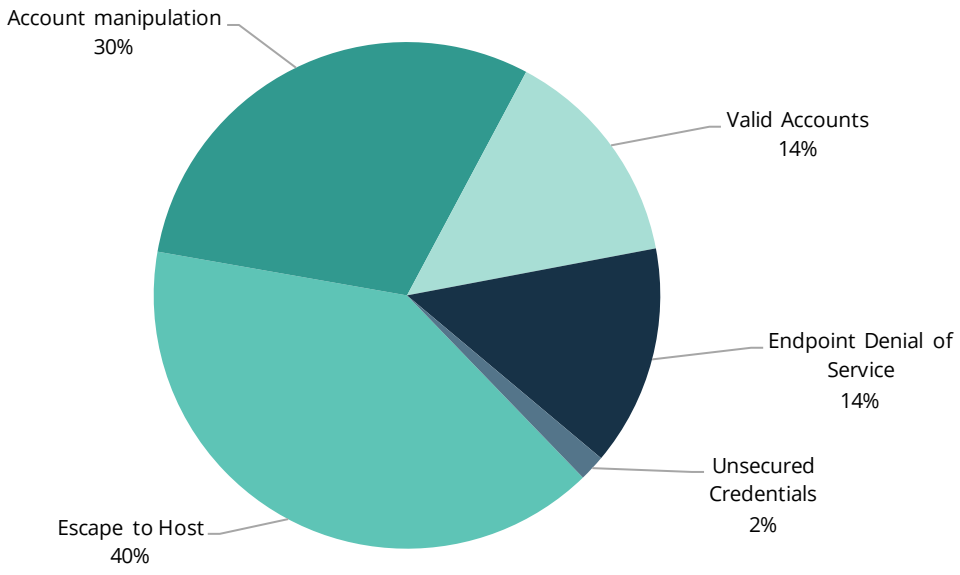


Figure 1: Most Frequently Observed ATT&CK Techniques in October

LATEST RANSOMWARE INTELLIGENCE

In October 2026, ransomware activity affected 182 victims, with Qilin and The Gentlemen emerging as the most dominant threat actor groups with 28 and 25 victims, respectively. Germany was the most targeted country with 53 victims, followed by Italy with 27, Spain with 24, France with 16, and Sweden with 15. Manufacturing accounted for 42 victims, followed by Professional Services with 22 and Technology with 14, while the sector was unspecified or not reported for 44 victims. Within the predefined countries of interest, Slovakia recorded one incident involving duhaas.sk, which was attacked by Safepay on October 5, 2026. Czechia recorded three incidents: www.kres.cz attacked by Krybit on October 2, 2026; Machine s.r.o. attacked by The Gentlemen on October 6, 2026; and Sladek Partners attacked by The Gentlemen on October 14, 2026.

Most Active Ransomware Groups in October

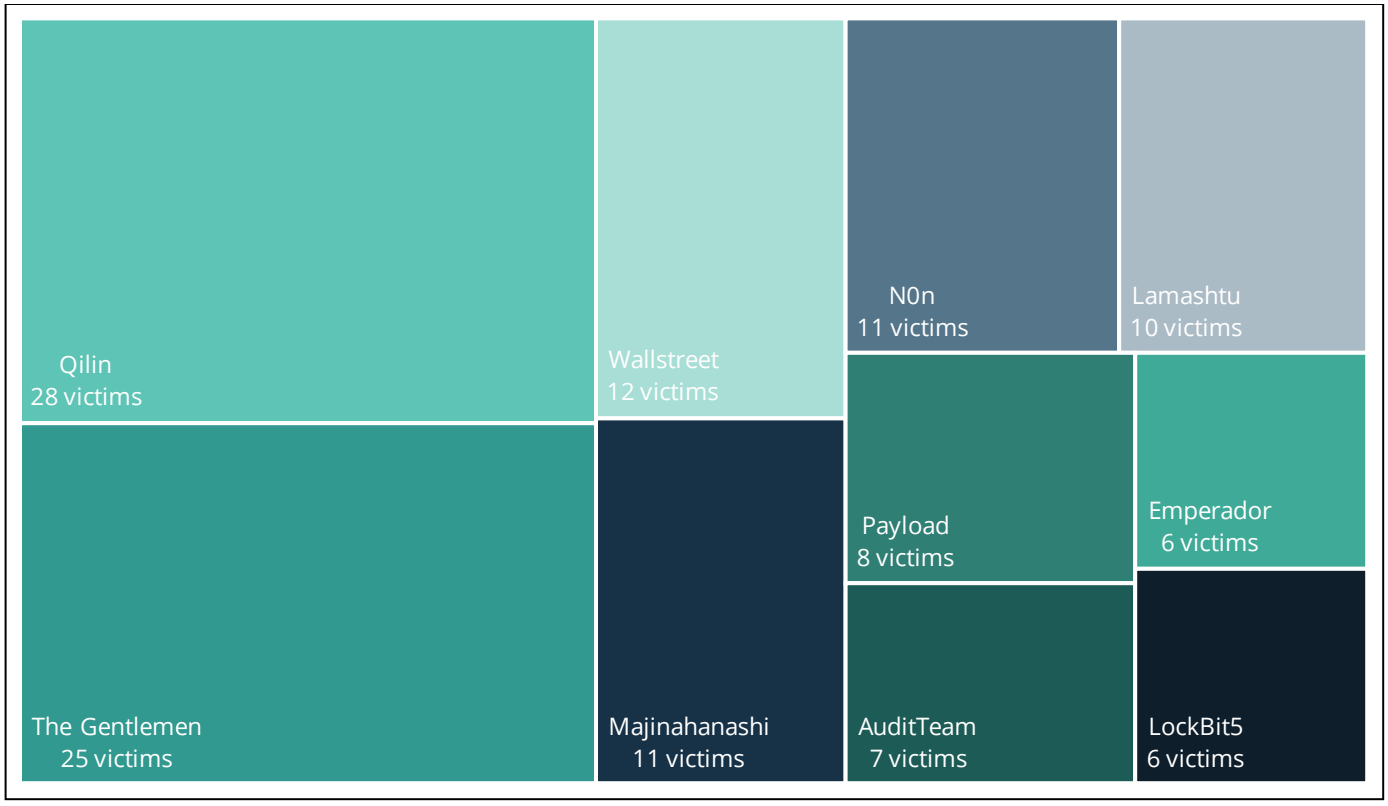


Figure 2: Most Active Ransomware Groups in October and Number of their Victims

The Most Affected EU Countries in October

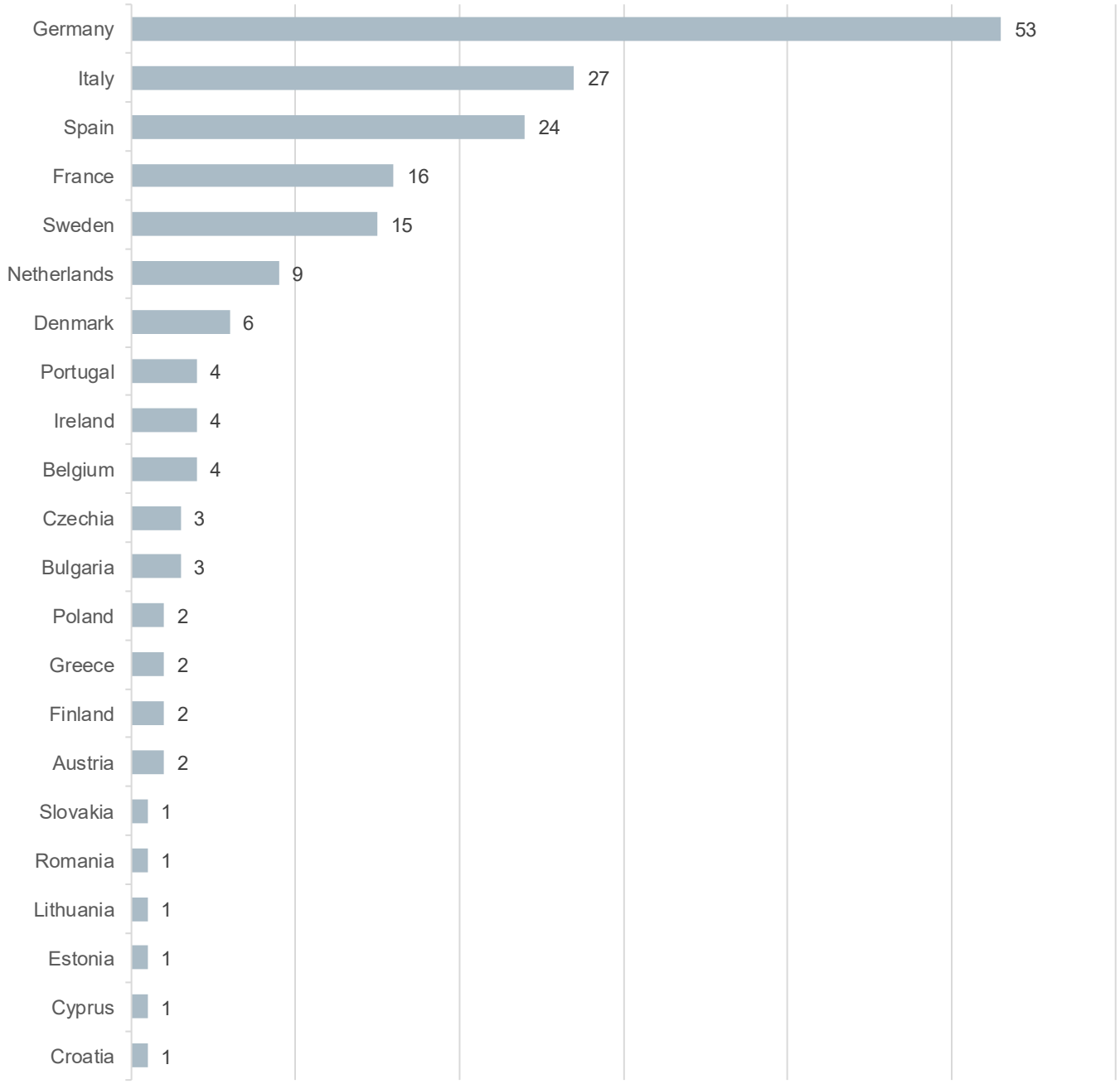


Figure 3: Most Affected EU Countries by Ransomware

The Most Affected Sectors in October

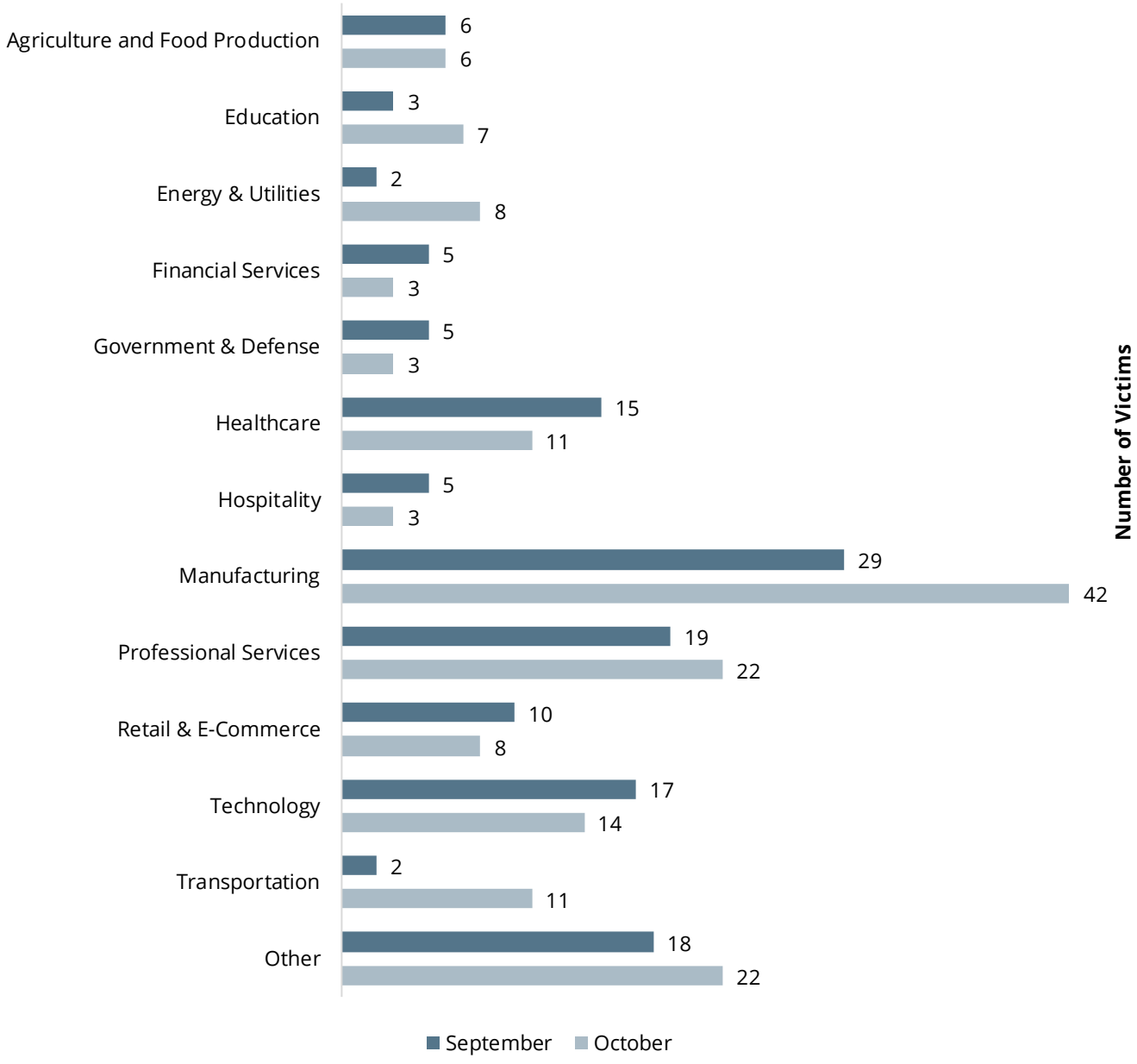


Figure 4: Most Affected Sectors in the EU

ATTACKED COMPANIES

Slovakia

duhaas.sk

Published by **Safepay** on **2026-10-05**.

Description: DUHA is a construction and engineering company based in Slovakia, specializing in civil structures, infrastructure, and environmental building projects.

Sector: Construction and Engineering

Czechia

Sladek Partners

Published by **The Gentlemen** on **2026-10-14**.

Description: Sladek Partners is a law firm based in Prague, Czechia. It specializes in real estate transactions, family law, and attorney escrow services.

Sector: Professional Services

Machine s.r.o.

Published by **The Gentlemen** on **2026-10-06**.

Description: K2 Machine s.r.o. is a Czech company that designs and builds special-purpose machinery, automated production lines, and robotic systems.

Sector: Manufacturing

www.kres.cz

Published by **Krybit** on **2026-10-02**.

Description: KRES is a Czech company that sells and services power tools, electric motors, and pumps. It operates both a retail store and an online shop.

Sector: Retail & E-Commerce

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 OCTOBER

During October 2026, 27 DDoS attacks targeted EU countries, all attributed to the threat actor NoName057 (16). France was the most targeted country with 16 attacks, followed by Italy with seven attacks, the Czech Republic with three attacks, and Spain with one attack. The Government sector absorbed the majority of targeting with 16 attacks, while Information Technology and Internet received three attacks and Financial Services received two attacks. Single attacks also impacted the Construction, Transportation, Education, Telecommunications, Adult Content, and other sectors. Temporal activity peaked on October 5, 2026, with six attacks, followed by October 11, 2026, with five attacks. Additional daily activity spikes of three attacks occurred on October 3, October 9, and October 19, 2026.

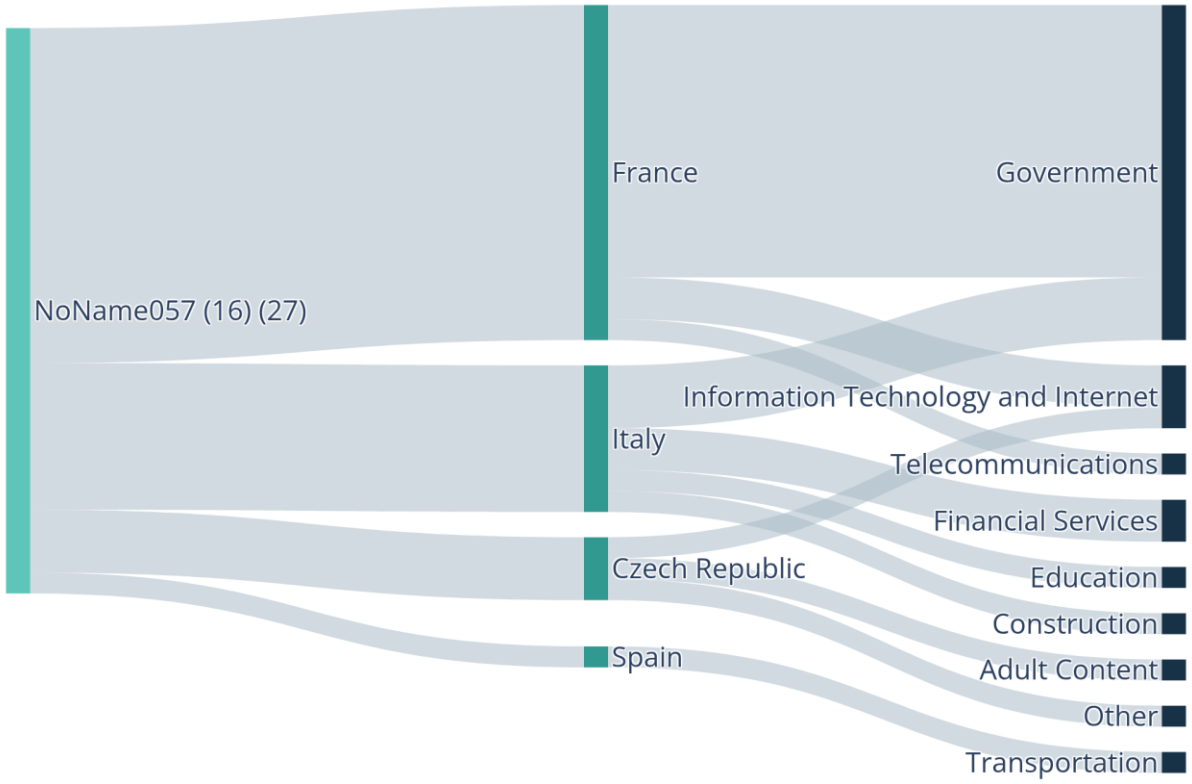


Figure 5: Diagram Showing Attacking Group → Targeted Country → Targeted Sector

Histogram of DDoS Attacks

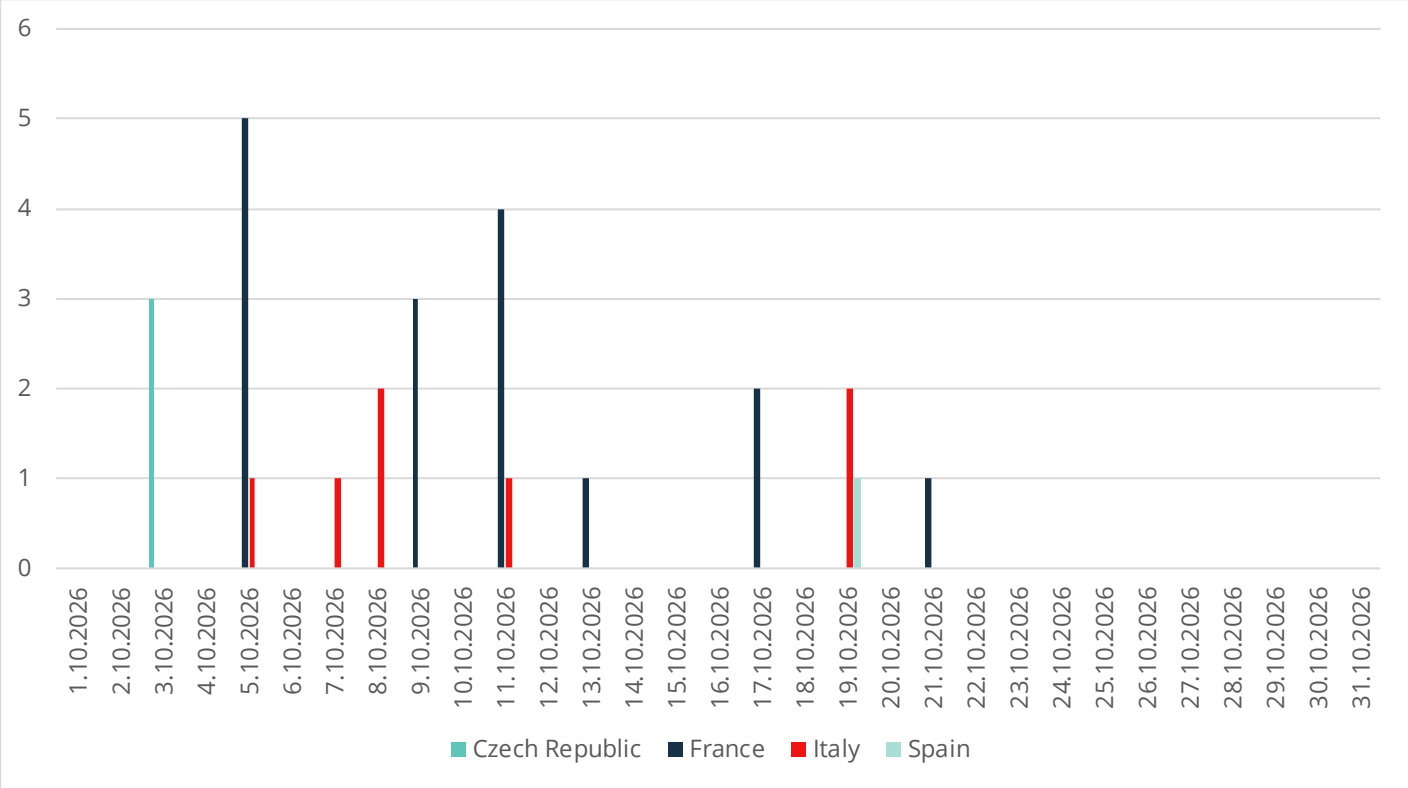


Figure 6: Histogram of Detected DDoS Attacks

VULNERABILITY INTELLIGENCE

In October, we registered 36 actively exploited vulnerabilities, a 16.3% decrease from last month. Plex Media Server was the most affected product on the KEV list, with 4 vulnerabilities reported. Ivanti Connect Secure saw the second-highest number of additions, totaling 3 vulnerabilities during the month. Several products registered 2 vulnerabilities each, including PHP Group PHP, Ahsay AhsayCBS, and Zammad GmbH Zammad. The remaining affected software, comprising ISC BIND, ProFTPD, Atlassian Multiple Products, Apache Struts, and Google Brotli, each accounted for 1 vulnerability.

Number of Known Exploited Vulnerabilities Over Months

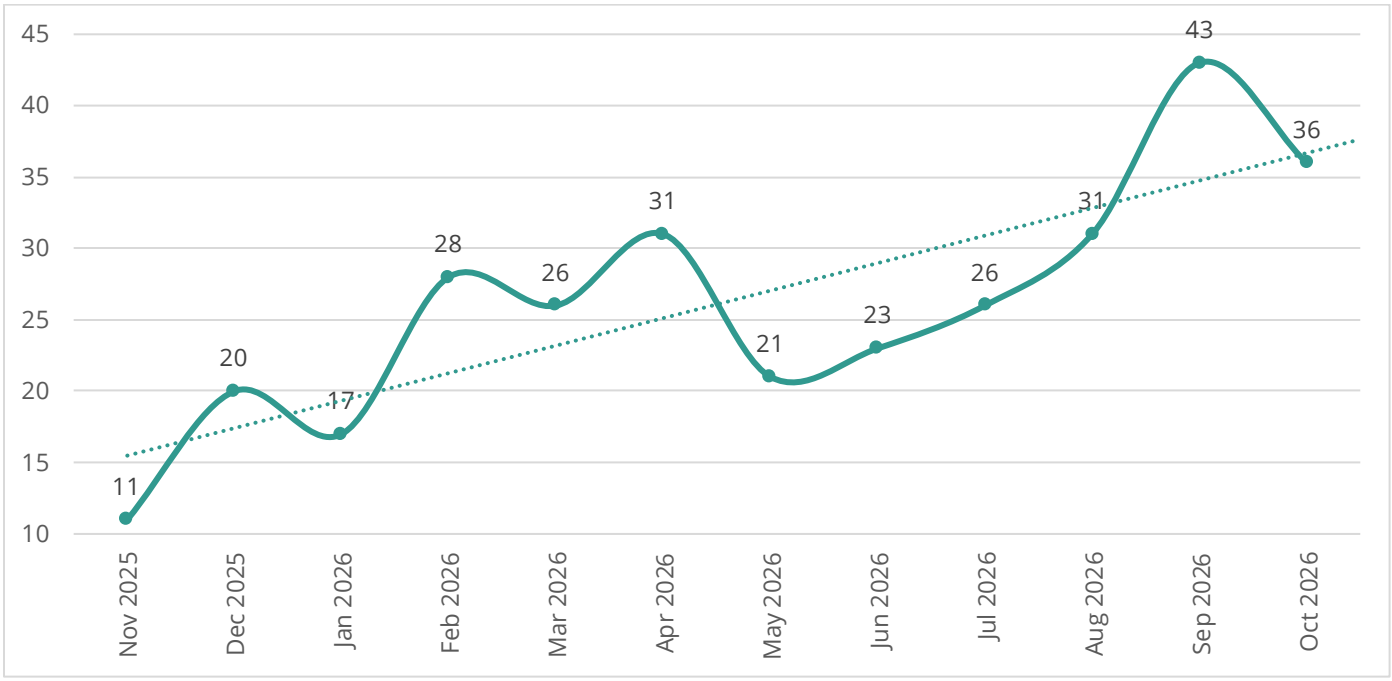


Figure 7: Number of CISA KEVs Published per Month

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

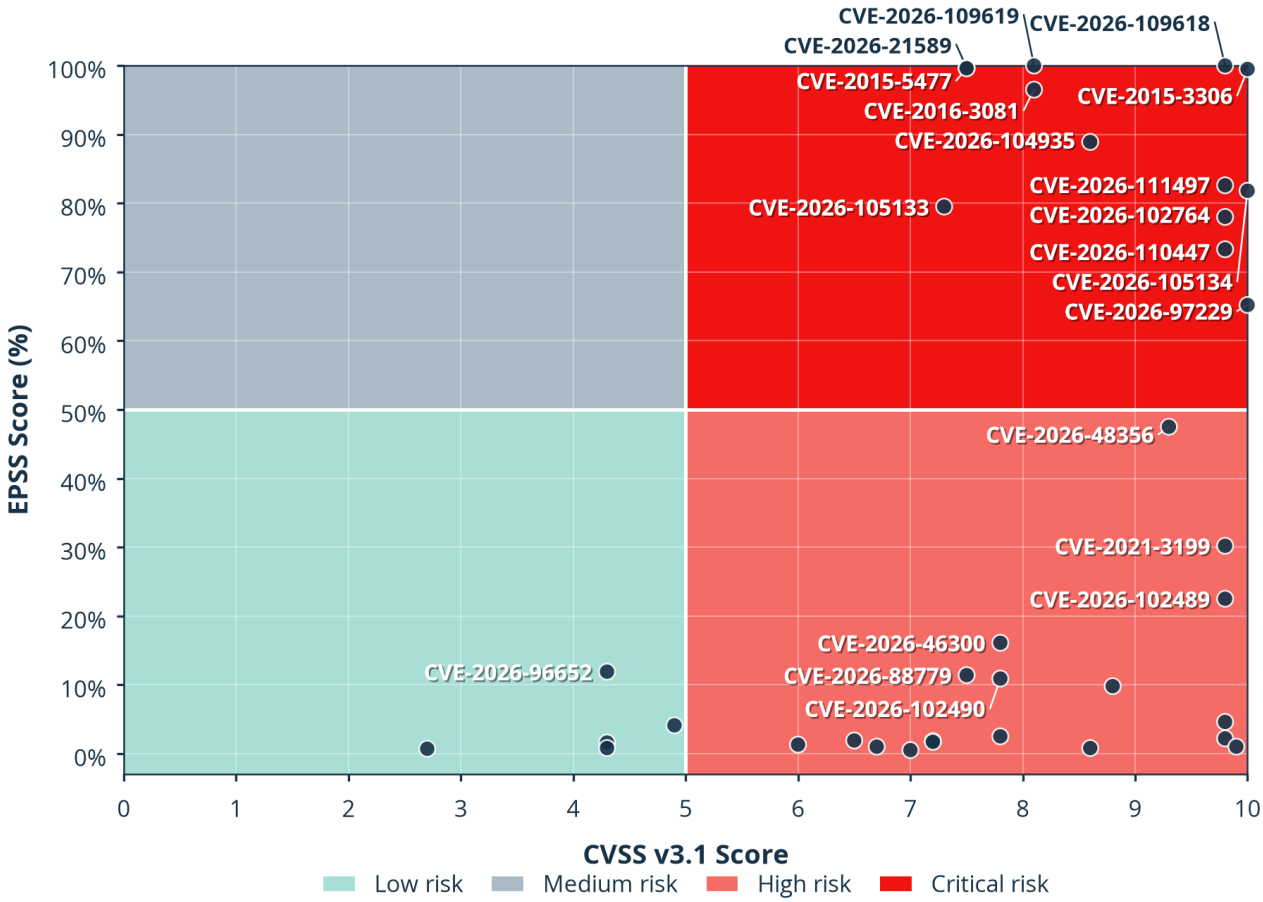


Figure 8: EPSS x CVSS Matrix of Actively Exploited Vulnerabilities

We strongly recommend reviewing the list, sorting criticality, and prioritizing immediate patching for any vulnerabilities affecting systems within your infrastructure. Timely patching is critical to reduce exploit exposure. 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 Score
CVE-2026-109618 CVE-2026-109619	PHP contains an out-of-memory corruption vulnerability that allows for unauthenticated remote code execution.	PHP Group	100.0%
CVE-2026-21589	Multiple Atlassian products (Bitbucket Data Center ,Confluence Data Center, Jira Service Management Data Center, Jira Software Data Center, Bamboo Data Center, Crowd Data Center, Crucible and Fisheye) contain a files or directories accessible to external parties vulnerability which could allow an unauthenticated attacker to access specific files within the web application root directory in affected versions.	Atlassian Multiple Products	99.7%
CVE-2015-5477	ISC BIND contains a data processing errors vulnerability that could allow remote attackers to cause a denial of service via TKEY queries.	ISC BIND	99.6%
CVE-2015-3306	ProFTPD contains an improper access control vulnerability that could allow remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.	ProFTPD	99.5%
CVE-2016-3081	Apache Struts contains a command injection vulnerability that could allow remote attackers to execute arbitrary code via method:prefix when Dynamic Method Invocation is enabled.	Apache Struts	96.5%
CVE-2026-104935	Ivanti Connect Secure contains an authentication bypass by spoofing vulnerability that allows a remote unauthenticated attacker to execute arbitrary commands.	Ivanti Connect Secure	88.9%

CVE	Description	Affected Product	EPSS Score
CVE-2026-111497	Google Brotli contains an unchecked return value vulnerability that allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a denial of service, or potentially execute arbitrary code using a crafted Brotli-compressed stream.	Google Brotli	82.6%
CVE-2026-105134	Ahsay AhsayCBS contains a command injection vulnerability that could allow a remote attacker to execute operating system commands via manipulation of the random parameter in the Replication Receiver component's /rps/api/json/UpdateReceivers.do endpoint. This vulnerability can be chained with CVE-2026-105133.	AhsayCBS	81.8%
CVE-2026-105133	Ahsay AhsayCBS contains an improper authentication vulnerability that could allow a remote attacker to bypass authentication via manipulation of the random parameter in the API component's checkSysPwd function. This vulnerability can be chained with CVE-2026-105134.	AhsayCBS	79.5%
CVE-2026-102764	BeyondTrust Remote Support contains an authentication bypass by spoofing vulnerability that could allow a remote attacker to perform file operations on the appliance.	BeyondTrust Remote Support	78.0%
CVE-2026-110447	Collabora Collabora Online – Built-in CODE Server when used within the NextCloud platform contains an OS command injection vulnerability that allows for remote code execution when the CODE server isn't running.	Collabora Online – Built-in CODE Server	73.3%
CVE-2026-97229	GitLab Community Edition and Enterprise Edition contain a integer overflow or	GitLab Community	65.2%

CVE	Description	Affected Product	EPSS Score
	wraparound vulnerability that could allow an unauthenticated user to execute arbitrary code on the GitLab server via a specially crafted regular expression in a CI/CD configuration, due to insufficient regular expression validation.	Edition and Enterprise Edition	
CVE-2026-48356	Adobe Commerce and Magento contain an unrestricted upload of file with dangerous type vulnerability that could result in arbitrary code execution in the context of the current user, potentially gaining elevated access or control over the victim's account or session.	Adobe Commerce and Magento	47.5%
CVE-2021-3199	ONLYOFFICE Docs contains a path traversal vulnerability that can occur when JWT is used, via a /.. sequence in an image upload parameter and could allow for remote code execution.	ONLYOFFICE Docs	30.2%
CVE-2026-102489	Zammad GmbH contains a session fixation vulnerability that can lead to remote code execution as the zammad user. This vulnerability can be chained with CVE-2026-102490.	Zammad GmbH	22.5%
CVE-2026-46300	Linux Kernel contains a missing initialization of a variable vulnerability that could allow for unintended modification of page-cache-backed data via failure to preserve the shared-fragment marker during socket buffer coalescing, causing ESP input processing to decrypt shared fragments in place. This vulnerability can be chained with CVE-2026-109618 and CVE-2026-109619 to implant PHP webshells and run commands as root.	Linux Kernel	16.1%
CVE-2026-96652	Plex Media Server contains a server-side request forgery (SSRF) vulnerability which could allow an attacker using any X-Plex-Token value to include	Plex Media Server	11.9%

CVE	Description	Affected Product	EPSS Score
	a full URL in the 'protocol' parameter and force the Plex server to POST to the attacker's chosen destination. This vulnerability can be chained with CVE-2026-96654, CVE-2026-96655, and CVE-2026-96656.		
CVE-2026-88779	Citrix NetScaler ADC (formerly Citrix ADC) and Citrix NetScaler Gateway (formerly Citrix Gateway) contain an improper restriction of operations within the bounds of a memory buffer vulnerability that could allow for a denial of service.	Citrix NetScaler	11.4%
CVE-2026-102490	Zammad GmbH Zammad contains an improper privilege management vulnerability that can allow the local zammad user to escalate privileges to root. This vulnerability can be chained with CVE-2026-102489.	Zammad GmbH	10.9%
CVE-2026-96951	Microsoft Windows Shell contains a command injection vulnerability that allows an unauthorized attacker to bypass a security feature over a network.	Microsoft Windows	9.8%
CVE-2026-104286	Fortinet FortiMail contains a path traversal and an improper neutralization of NULL byte or NULL character vulnerability that may allow an unauthenticated attacker to write arbitrary files on the underlying system via crafted HTTP or HTTPS requests.	Fortinet FortiMail	4.6%
CVE-2023-22894	Strapi contains a cleartext storage of sensitive information vulnerability that could allow attackers with access to the admin panel to discover sensitive user details via the query filter. 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	Strapi	4.1%

CVE	Description	Affected Product	EPSS Score
	a supported version. This vulnerability can be chained with CVE-2023-22621 to achieve remote code execution.		
CVE-2026-106931	EG Secure Solutions SiteGuard Server Edition contains an OS command injection vulnerability which may allow an attacker to execute arbitrary OS commands with root or SYSTEM privileges on the system running the affected product.	EG Secure Solutions SiteGuard Server Edition	2.5%
CVE-2026-76519	Cisco Secure Email Gateway contains a relative path traversal vulnerability that could allow an unauthenticated, remote attacker to write arbitrary files on the underlying operating system.	Cisco Secure Email Gateway	2.2%
CVE-2026-96654	Plex Media Server contains an improper neutralization of encoded URI schemes in a web page vulnerability that could allow an attacker to call other plugins' functions and supply their own parameters. This vulnerability can be chained with CVE-2026-96652, CVE-2026-96655, and CVE-2026-96656.	Plex Media Server	1.9%
CVE-2026-96656	Plex Media Server contains an external control of file name or path vulnerability which can allow an admin user to write arbitrary files that may be executed on load. This vulnerability can be chained with CVE-2026-96652, CVE-2026-96654, and CVE-2026-96655.	Plex Media Server	1.8%
CVE-2026-0322	Palo Alto Networks PAN-OS contains a code injection vulnerability that could allow an authenticated attacker with network access to execute arbitrary code with root privileges on the firewall.	Palo Alto Networks PAN-OS	1.7%

CVE	Description	Affected Product	EPSS Score
CVE-2026-96655	Plex Media Server contains a server-side request forgery (SSRF) vulnerability that could allow an authenticated user to request arbitrary internal or external addresses via the '/video/:/transcode/universal' path parameter. This vulnerability can be chained with CVE-2026-96652, CVE-2026-96654, and CVE-2026-96656.	Plex Media Server	1.6%
CVE-2025-61624	FortiOS, FortiPAM, FortiProxy, and FortiSwitchManager contain a path traversal vulnerability that may allow an authenticated attacker with admin profile and at least read-write permissions to write or delete arbitrary files via specific CLI commands.	Fortinet Multiple Products	1.3%
CVE-2026-110936	Siemens Software Center contains an uncontrolled search path element vulnerability that could allow an authenticated local attacker to place a specially crafted DLL in a directory that the application searches, leading to arbitrary code execution with the privileges of the affected application.	Siemens Software Center	1.0%
CVE-2026-114625	Arista VeloCloud Orchestrator on-prem contains a SQL injection 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	1.0%
CVE-2026-118527	Ivanti Connect Secure contains a generation of predictable numbers or identifiers vulnerability that allows a remote authenticated attacker to upload files with attacker-controlled content to a known location on disk. This vulnerability can	Ivanti Connect Secure	0.8%

CVE	Description	Affected Product	EPSS Score
	be chained with CVE-2026-104935 and CVE-2026-111357.		
CVE-2026-76418	Cisco Secure Firewall ASA Software and Cisco Secure FTD Software contains an unchecked return value to NULL pointer dereference vulnerability that could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	Cisco Secure Firewall ASA Software and Cisco Secure FTD Software	0.8%
CVE-2026-41709	Broadcom VMWare ESX contains an insufficient logging vulnerability that could allow a malicious actor with admin access to perform certain operations without being logged.	Broadcom VMware ESX	0.7%
CVE-2026-111357	Ivanti Connect Secure contains a missing authentication for critical function vulnerability that could allow a local authenticated attacker to escalate their privileges. This vulnerability can be chained with CVE-2026-104935 and CVE-2026-118527.	Ivanti Connect Secure	0.5%

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



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.