TLP:AMBER

MSS-INT REPORT

GLESEC

March 10, 2026

TLP AMBER
MSS-INT REPORT

About this report

This is a SKYWATCH report that presents the most up-to-date information for the MSS-INT as displayed in the service dashboard.

MSS-INT

Active High-Severity Items

0

0

Executive Action Required

No executive action required today

Threat Relevance Score (TRS)

57
→ 0

Risk Score (RS)

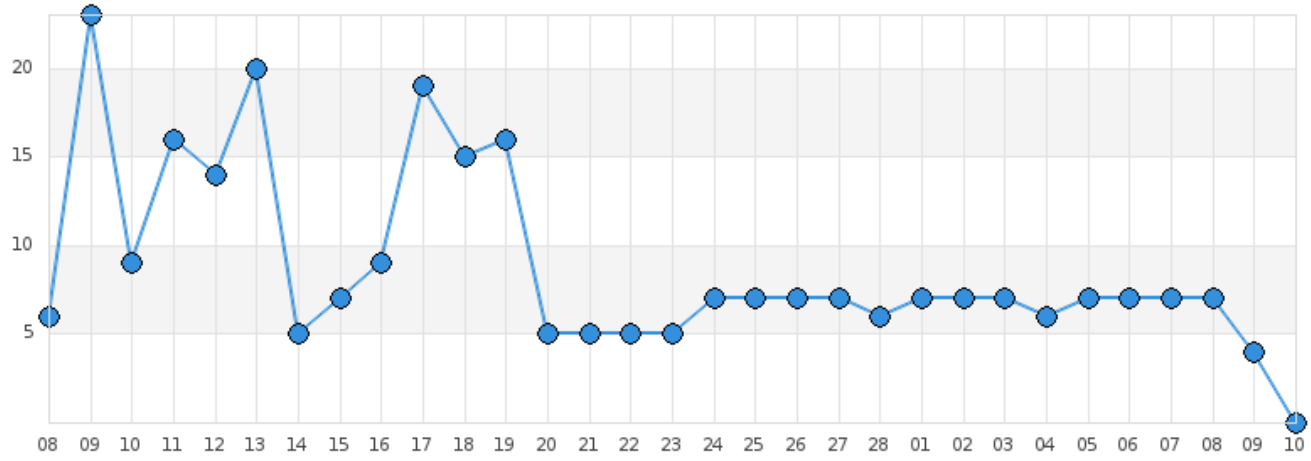
53
→ 0

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

MSS-INT REPORT

GLESEC 03/10/2026

Threat Landscape – Feed Volume



Threat Headlines

Date	Threat Headline
Feb 24, 2,026	GLESEC CVE Enrichment - EPSS Scores 2026-02-24
Feb 24, 2,026	GLESEC CVE Enrichment - CISA KEV 2026-02-24
Feb 25, 2,026	GLESEC CVE Enrichment - CISA KEV 2026-02-25
Feb 25, 2,026	GLESEC CVE Enrichment - EPSS Scores 2026-02-25
Feb 26, 2,026	GLESEC CVE Enrichment - CISA KEV 2026-02-26
Feb 26, 2,026	GLESEC CVE Enrichment - EPSS Scores 2026-02-26
Feb 27, 2,026	GLESEC CVE Enrichment - CISA KEV 2026-02-27
Feb 27, 2,026	GLESEC CVE Enrichment - EPSS Scores 2026-02-27
Feb 28, 2,026	GLESEC CVE Enrichment - CISA KEV 2026-02-28
Mar 1, 2,026	GLESEC CVE Enrichment - CISA KEV 2026-03-01

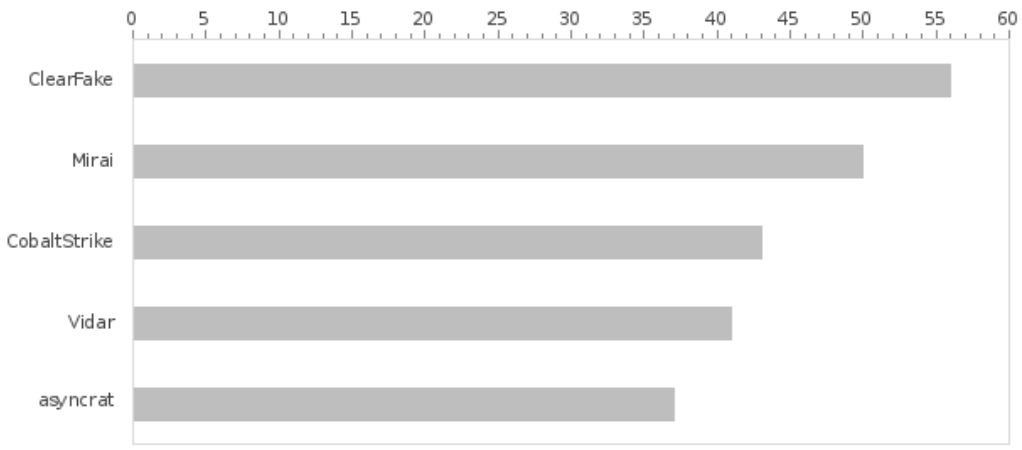
LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

MSS-INT REPORT

GLESEC 03/10/2026

Relevant Top Malware Families



Persistence of Blocked Attacks to Organization's Perimeter

	10.10.10.14	10.4.0.60	100.101.2.103	162.142.125.254	172.110.223.22	172.20.1.124	172.20.2.114	172.20.2.86	185.243.5.22	51.79.77.159
100.64.0.227	0	0	0	0	0	11245	0	0	0	0
192.168.51.15	162	0	0	0	0	0	563	1520	0	0
192.168.50.114	102	0	0	0	0	0	657	1007	0	0
192.168.100.202	0	0	17	19	73	0	0	0	38	27
3.219.2.182	0	170	0	0	0	0	0	0	0	0
192.168.100.30	0	0	17	16	72	0	0	0	38	27
3.86.141.192	0	167	0	0	0	0	0	0	0	0
3.209.246.195	0	159	0	0	0	0	0	0	0	0
192.168.100.13	0	0	17	17	68	0	0	0	38	27
54.158.84.126	0	151	0	0	0	0	0	0	0	0

Ongoing cases

Case #	Service	Priority	Hours	Status

Cybersecurity News

Title	Categories	Industries
Microsoft Teams phishing targets employees with A0Backdoor malware	Cyber Attacks, Malware	Banking and Financial
Dutch govt warns of Signal, WhatsApp account hijacking attacks	Cyber Attacks, Data Breaches	Government, Telecommunication, Military
President Trump's Cyber Strategy for America: What It Means for the U.S. and Why It Matters Globally	Cyber Attacks, Vulnerabilities, Malware	Government, Banking and Financial, Education, Transportation, Telecommunication, Blockchain

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Title	Categories	Industries
President Trump's Cyber Strategy for America: What It Means for the U.S. and Why It Matters Globally	Cyber Attacks, Vulnerabilities, Malware	Government, Banking and Financial, Education, Transportation, Telecommunication, Blockchain
Google: Cloud attacks exploit flaws more than weak credentials	Cyber Attacks, Data Breaches, Vulnerabilities, Malware	Government, Banking and Financial, Legal Services, Military, Blockchain
Google: Cloud attacks exploit flaws more than weak credentials	Cyber Attacks, Data Breaches, Vulnerabilities, Malware	Government, Banking and Financial, Legal Services, Military, Blockchain

MSS-INT-V

Immediate Threat Intelligence Assessment

Threat_Name	Endpoint_Target	Summary	Tags	Attack_Vector_Score	Category_Pct	Last_Seen
Unknown					0.00	2026-03-09 19:30:07
APT28 - In-the-Wild Exploit of CVE-2026-21513	GOC-PANAMA5	On February 2,026s Patch Tuesday Microsoft patched CVE-2026-21513 a security features bypass vulnerability within MSHTML framework. The vulnerability affects all Windows versions is actively exploited in the wild and carries a CVSS score of 8.8. Using PatchDiff-AI Akamai researchers performed automated root cause analysis of the patch and correlated it with an observed in-the-wild exploit attributed to the Russian state-sponsored threat actor APT28. Related Countries: Russian Federation Related Industries: Government, Defense & Aerospace, IT Services	Bypass, Exploit, Government, Vulnerability		33.30	2026-03-05 19:06:42

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

MSS-INT REPORT

GLESEC 03/10/2026

Threat_Name	Endpoint_Target	Summary	Tags	Attack_Vector_Score	Category_Pct	Last_Seen
StegaBin 26 Malicious npm Packages Use Pastebin Steganography to Deploy Multi-Stage Credential Stealer	GOC-PANAMA5	Sockets AI-powered threat detection systems identified 26 malicious npm packages published over a two-day period that deploy a multi-stage credential and secret harvesting operation targeting developers. The packages use a Pastebin-based dead-drop resolver that hides C2 infrastructure inside seemingly benign text using character-level steganography. We are referring to this campaign as StegaBin due to its use of steganographic Pastebin dead-drop resolvers. After resolving infrastructure hosted across 31 Vercel deployments the infection chain retrieves platform-specific shell payloads that ultimately install a Remote Access Trojan (RAT) and automatically deploys a nine-module infostealer toolkit. The modules target developer environments directly including VSCode configuration SSH keys git repositories browser credential stores clipboard data and locally stored secrets. Independent researcher Kieran Miyamoto disclosed 17 related packages earlier on February 26 2,026 including a detailed walkthrough of the steganographic Pastebin decoder. At the time of his disclosure Sockets threat research team was already investigating the same cluster after our threat detection engine flagged the packages for malicious install-script behavior and obfuscated payload delivery. Socket flagged the first package within two minutes of publication and all 26 were detected in under six minutes each. Our analysis identified nine additional related packages and by simulating a compromised host connecting to the live C2 infrastructure captured the full automated post-exploitation payload suite delivered to victims. Related Industries: Education, Technology, Transportation	Exploit, RAT, Steganography, Trojan		50.00	2026-03-05 19:04:41
Henry IV Hotspur Hal and hallucinations	GOC-PANAMA5	This article draws parallels between Shakespeares Henry IV and modern cybersecurity challenges particularly focusing on the adoption of AI. It emphasizes the importance of taking calculated risks learning from failures and surrounding oneself with knowledgeable peers. The piece also highlights a new campaign by UAT-10027 using the Dohdoor backdoor which leverages DNS-over-HTTPS for stealthy communications and targets education and healthcare sectors in the US. The author encourages security teams to stay vigilant update detection tools and monitor for unusual activities to combat sophisticated threats. Related Countries: United States Related Industries: Health Care, Education, Defense & Aerospace, Telco, IT Services	Backdoor		50.00	2026-03-05 19:01:41
Trellix Telemetry - Sophisticated PowerShell Backdoor Infection Discoverd In LATAM	GOC-PANAMA5	Trellix identified a sophisticated PowerShell backdoor targeting government entities in Latin America that likely originated from infected USB devices. The intrusion began when a user executed a malicious JavaScript file disguised as a tax notification which utilized a sequence of legitimate Windows processes including WScript and mshta to deploy the final payload. Once established the backdoor granted unauthorized actors full remote control via a command and control infrastructure allowing for the execution of arbitrary commands and the deployment of additional malware. To maintain access and avoid detection the campaign leveraged a variety of advanced techniques such as system binary proxy execution registry modifications and scheduled tasks while facilitating data exfiltration through standard web protocols. Related Countries: US Related Industries: Government, Technology	Backdoor, Exfiltration, Government, Malware, PowerShell		12.50	2026-03-05 16:43:20

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

MSS-INT REPORT

GLESEC 03/10/2026

Threat_Name	Endpoint_Target	Summary	Tags	Attack_Vector_Score	Category_Pct	Last_Seen
New malicious npm package ambar-src targets developers with open source malware	GOC-PANAMA5	A malicious npm package named "ambar-src" reached 50,000 downloads in days before being removed from the registry. It uses a preinstall script to execute malicious code during installation targeting Windows Linux and macOS systems. The package employs detection evasion techniques and deploys powerful open-source malware variants. It abuses npms preinstall script hook to trigger the payload without explicit invocation. The malware fetches additional payloads from remote servers and uses Yandex Cloud for command and control. Affected systems should be considered fully compromised requiring immediate incident response actions. The attack highlights the speed at which supply chain risks can propagate and confirms that npm install is a high-risk action. Related Industries: IT Services	Cloud, Malware		45.50	2026-03-05 16:39:37
From Extension to Infection An In-Depth Analysis of the Evelyn Stealer Campaign Targeting Software Developers	GOC-PANAMA5	The Evelyn Stealer campaign targets software developers through weaponized Visual Studio Code extensions employing a multistage delivery of information-stealing malware. The attack chain involves a downloader disguised as a legitimate Lightshot DLL an injector that uses process hollowing to inject the final payload and the Evelyn Stealer itself. The malware implements sophisticated anti-analysis techniques collects sensitive information including browser credentials and cryptocurrency data and exfiltrates the stolen data via FTP. This campaign highlights the increasing threat to developer communities and the need for enhanced security measures in development environments. Related Industries: Real Estate / Property Management, Technology, Defense & Aerospace, Transportation	Credentials, Cryptocurrency, FTP, Malware		50.00	2026-01-28 12:27:40
Trellix Telemetry - ClickFix Campaign Targets Canadian Users With PowerShell	GOC-PANAMA5	The ClickFix infection campaign demonstrated sophisticated living off the land techniques targeting Canadian entities. The attack began with social engineering that led to the execution of a malicious forfiles.exe command initiating a chain of events using legitimate Windows binaries. The operation leveraged multiple techniques including PowerShell abuse command obfuscation and system binary proxy execution through mshta. The multi-stage attack chain demonstrated advanced operational security through its use of legitimate tools and obfuscation techniques. Related Countries: Canada Related Industries: Defense & Aerospace	PowerShell		50.00	2026-01-28 11:58:44
Malicious NexShield Extension Delivers ModeloRAT Through CrashFix Campaign	GOC-PANAMA5	KongTukes CrashFix campaign discovered in January 2,026 demonstrates sophisticated social engineering through a malicious Chrome extension (NexShield) that impersonates uBlock Origin Lite. The attack uses delayed execution intentional browser crashes and fake security warnings to trick users into executing malicious commands. The campaign implements multiple layers of defense evasion including AES-256 and XOR encryption DGA domains and system fingerprinting to detect analysis environments. Domain-joined machines receive ModeloRAT a full-featured Python RAT with RC4-encrypted C2 communications while non-domain machines follow a separate infection chain. The attack leverages LOLBins like finger.exe for payload delivery and establishes persistence through Windows Registry modifications showing particular focus on compromising corporate environments. Related Industries: Transportation, Defense & Aerospace, Telco	Python, RAT		54.50	2026-01-28 11:27:13

MSS-INT REPORT

GLESEC 03/10/2026

Threat_Name	Endpoint_Target	Summary	Tags	Attack_Vector_Score	Category_Pct	Last_Seen
PureLogs Infostealer Hides Malware In PNG Files	GOC-PANAMA5	Swiss Post Cybersecurity revealed a PureLogs infostealer campaign operating through a four-stage infection chain. The attack begins with a phishing email containing a JScript dropper that downloads a weaponized PNG from archive.org. The malware employs multiple evasion techniques including steganography process hollowing of CasPol.exe and completely fileless execution. Despite being a commodity malware available for $150/month it implements sophisticated techniques like DPAPI bypass 3DES encryption and extensive credential stealing capabilities targeting browsers cryptocurrency wallets and various applications. The campaign demonstrates how modern malware combines legitimate infrastructure abuse multi-stage payloads and in-memory execution to evade detection while maintaining scalability for mass deployment. Related Industries: IT Services	Bypass, Cryptocurrency, Dropper, Fileless, Malware, Phishing, Steganography		58.30	2026-01-28 10:57:28
Critical HPE OneView RCE Vulnerability Under Active Exploitation CVE-2025-37164	GOC-PANAMA5	Check Point Research uncovered a major exploitation campaign targeting CVE-2025-37164 a critical RCE vulnerability in HPE OneView. The vulnerability in the executeCommand REST API endpoint allows unauthenticated remote code execution. Initially disclosed on December 16 2,025 exploitation attempts began December 21 before dramatically escalating on January 7 2,026 with over 40,000 automated attacks by the RondoDox botnet in a single day. The attacks leveraged RondoDox botnet techniques for DDoS and crypto mining operations. Related Industries: Education	Botnet, Exploit, Vulnerability		75.00	2026-01-23 01:57:36
VoidLink Advanced Cloud-Native Linux Malware Framework Discovered	GOC-PANAMA5	VoidLink is a cloud-native Linux malware framework discovered in December 2,025 featuring modular architecture with 37+ plugins advanced rootkit capabilities and adaptive stealth mechanisms. Written in Zig it specifically targets cloud environments with detection and exploitation capabilities for major providers containers and Kubernetes clusters. The framework employs multiple C2 channels mesh networking and environment-based risk scoring to adjust its behavior. Developed by Chinese-affiliated actors it includes a comprehensive operator dashboard and plugin API similar to Cobalt Strike. While showing commercial-grade development no real-world infections have been observed yet. Related Countries: China Related Industries: Real Estate / Property Management, IT Services, Architecture & Engineering	Cloud, Exploit, Kubernetes, Malware, RootKit		100.00	2026-01-22 12:44:18
Analyzing the MonetaStealer macOS Threat	GOC-PANAMA5	Security researchers discovered a suspicious Mach-O binary masquerading as a Windows .exe file named MonetaStealer. This PyInstaller-compiled malware targets macOS systems and is believed to be in early development. MonetaStealer focuses on stealing Chrome browser data cryptocurrency wallet information Wi-Fi credentials keychain items financial documents SSH private keys and clipboard content. It uses deceptive naming conventions and targets specific file paths to gather sensitive information. The malware employs various techniques to extract data including querying SQLite databases using regex patterns and executing system commands. Exfiltration is attempted via Telegram although researchers did not observe successful file uploads. A Windows variant was also identified but contained non-functional code. The threat highlights the ongoing prevalence of stealers in the macOS landscape. Related Industries: Technology, IT Services, Defense & Aerospace, Finance, Real Estate / Property Management	Credentials, Cryptocurrency, Exfiltration, Keychain, Malware, Telegram		62.50	2026-01-22 04:11:00

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

MSS-INT REPORT

GLESEC 03/10/2026

Threat_Name	Endpoint_Target	Summary	Tags	Attack_Vector_Score	Category_Pct	Last_Seen
CastleLoader Malware Targets Government Sector Through Process Hollowing	GOC-PANAMA5	CastleLoader is a stealthy malware loader that emerged in early 2,025 primarily targeting government entities and critical infrastructure in the US and Europe. It employs a sophisticated multi-stage execution chain using Inno Setup AutoIt and an uncommon process hollowing technique that maintains the original memory area of jsc.exe. The loader delivers information stealers and RATs enabling credential theft and persistent access. Technical analysis revealed C2 communication to 94.159.113.32 and successfully decoded encrypted configuration data. The malwares evasion techniques include heavy obfuscation API resolution by hash and ensuring the final payload only exists in memory after process modification. One campaign impacted 469 devices demonstrating its effectiveness as an initial access threat. Related Countries: United States Related Industries: Technology, IT Services, Government	AutoIt, Government, Loader, Malware		33.30	2026-01-22 04:07:37
Operation Covert Access Weaponized LNK-Based Spear-Phishing Targeting Argentinas Judicial Sector to Deploy a Covert RAT	GOC-PANAMA5	A sophisticated spear-phishing campaign targeting Argentinas judicial sector has been uncovered. The operation uses a multi-stage infection chain to deploy a stealthy Remote Access Trojan (RAT). Attackers exploit trust in court communications by using authentic-looking judicial decoy documents. The campaign employs a weaponized LNK file a BAT-based loader script and a covert Rust-based RAT to establish persistent access within judicial environments. The malware performs extensive anti-VM and anti-debug checks collects system information and establishes resilient C2 connections. It supports various malicious activities including persistence file transfer data harvesting encryption and privilege escalation. The campaign demonstrates high operational sophistication and aims to gain long-term access to sensitive legal and institutional data. Related Industries: Legal, Technology, IT Services, Telco	Exploit, Loader, Malware, Phishing, RAT, Trojan		50.00	2026-01-22 04:06:45
Sicarii Ransomware Group Masquerades As Israeli Operation	GOC-PANAMA5	Sicarii Ransomware emerged as a ransomware service operation that combines functional extortion capabilities with unusual Israeli/Jewish branding likely as a false flag operation. The malware demonstrates sophisticated technical features including anti-VM detection geo-fencing credential harvesting and AES-GCM encryption alongside destructive capabilities. However operational patterns linguistic analysis and behavioral indicators suggest the groups claimed identity is inauthentic with evidence pointing to Russian-speaking operators rather than Israeli origins. The operation emerged in late 2,025 and shows signs of being an experimental or immature ransomware group rather than an established criminal enterprise. Related Countries: Israel, Russian Federation	Extortion, Malware, Ransomware		50.00	2026-01-22 03:42:34

TLP:AMBER

MSS-INT REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500