TLP:AMBER

MSS-INT REPORT

ORGANO JUDICIAL

September 02, 2026

TLP AMBER
MSS-INT REPORT

Sobre este reporte

Se trata de un informe SKYWATCH que presenta la información más actualizada del MSS-INT tal y como se muestra en el panel de control del servicio.

MSS-INT

Active High-Severity Items

49

0

Executive Action Required

▲

10 items pending executive awareness or decision

Threat Relevance Score (TRS)

71
→ 0

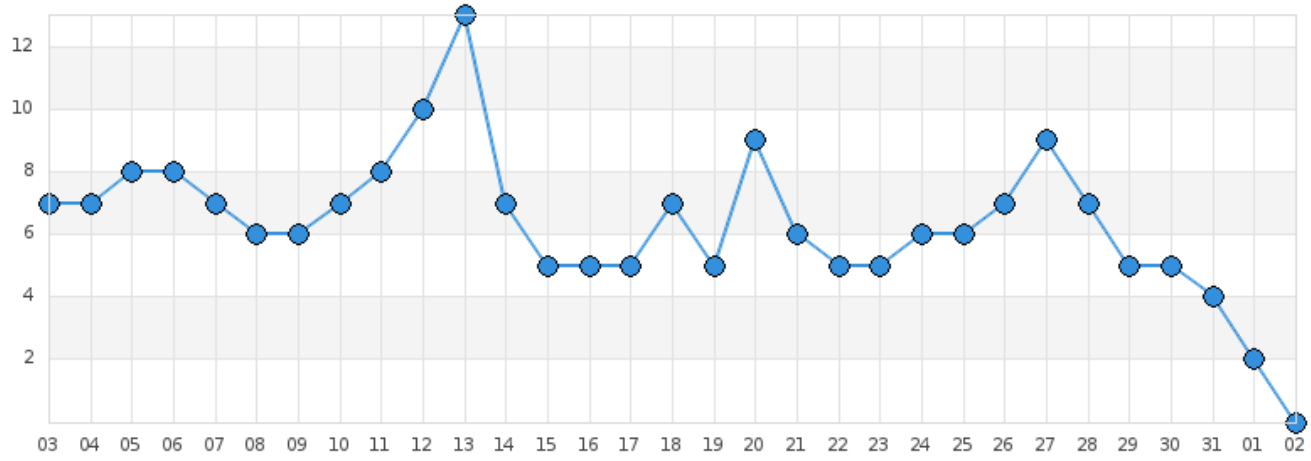
Risk Score (RS)

77
▼ -1

MSS-INT REPORT

Organo Judicial 09/02/2026

Threat Landscape – Feed Volume



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

TLP:AMBER

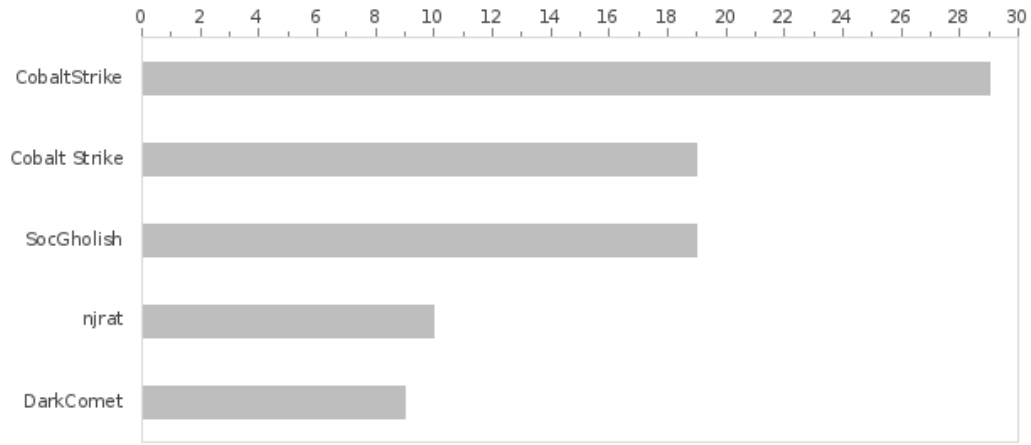
MSS-INT REPORT

Organo Judicial 09/02/2026

Threat Headlines

Date	Threat Headline	Actor	Malware	Sector	Why Relevant
Aug 31, 2,026	OTX [Mini Shai-Hulud]: Real-time Open Source Software Supply Chain Security	Mini Shai-Hulud	-	Government	Sector + Region
Aug 28, 2,026	OTX [APT28]: Open Directory Exposes Moobot Source Code and Ongoing Activity Post 2,024 Court-Authorized Disruption	apt28	Moobot	Government	Sector + Region
Aug 27, 2,026	OTX [APT28]: Defense and Diplomacy Targeted with HOOKEDGE	apt28	HOOKEDGE	Government	Sector + Region
Aug 26, 2,026	OTX [Tortoiseshell]: Expands Toolset With New Backdoor, SSH Tunnel	Tortoiseshell	TWOSTROKE	Government	Sector + Region
Aug 24, 2,026	OTX [Vanilla Tempest]: A ClickFix cluster: Observed activity from recent ClickFix campaigns	Vanilla Tempest	Lorem Ipsum	Government	Sector + Region
Aug 20, 2,026	OTX [Kimsuky]: Inside Kimsuky's Abuse of Legitimate Remote Control Tools Across Northeast Asia	kimsuky	-	Government	Sector + Region
Aug 20, 2,026	OTX [APT29]: Distinct Clusters Target Individuals of Interest to Russia	APT29	Vidar	Government	Sector + Region
Aug 20, 2,026	OTX [UAT-10147]: Chinese-speaking adversary integrates agentic AI into post-compromise operations	UAT-10147	BADIIS	Government	Sector + Region
Aug 20, 2,026	OTX [SilkParasite]: SilkParasite: Tracking a China-Nexus APT Across Central Asia	SilkParasite	DriveSilkRAT	Government	Sector + Region
Aug 19, 2,026	OTX [Balonx Sistema]: Balonx Sistema: The Face Behind the PhaaS Affecting Mexican Banking	Balonx Sistema	Spyroid	Government	Sector + Region

Relevant Top Malware Families



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

TLP:AMBER

MSS-INT REPORT

Organo Judicial 09/02/2026

Relevant Top Threat Actors

ThreatActor	client	count
teampcp	Organo Judicial	2
the gentlemen	Organo Judicial	2
agent tesla	Organo Judicial	1
black cat	Organo Judicial	1
blitz brigantine	Organo Judicial	1

Persistence of Blocked Attacks to Organization's Perimeter

	1.1.1.1	195.134.236.240	195.134.248.240	195.134.250.240	40.79.167.10	77.239.124.253	80.251.153.178	82.165.160.26
190.34.182.228	822 (74%)	0 (0%)	0 (0%)	1 (0%)	293 (26%)	0 (0%)	0 (0%)	0 (0%)
190.61.124.251	71 (23%)	0 (0%)	0 (0%)	0 (0%)	232 (77%)	0 (0%)	0 (0%)	0 (0%)
200.46.13.2	0 (0%)	725 (38%)	509 (27%)	656 (35%)	2 (0%)	2 (0%)	0 (0%)	0 (0%)
200.46.13.6	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	35 (90%)	4 (10%)	0 (0%)
200.46.13.9	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	33 (100%)	0 (0%)	0 (0%)
200.46.13.41	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	98 (100%)	0 (0%)	0 (0%)
200.46.65.189	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	36 (1%)	1147 (40%)	1668 (59%)
200.46.126.115	0 (0%)	0 (0%)	0 (0%)	0 (0%)	89 (100%)	0 (0%)	0 (0%)	0 (0%)

Ongoing cases

Case #	Service	Priority	Hours	Status
42479 Notable Event Alert: InstallFix Campaign Uses Fake Claude AI Installer Pages	MSS-INT	Medium	0	Answered
42589 Organo Judicial TEVR 051426	MSS-INT	High	0	Answered
42597 CASE – Validación de Exposición Linux Relacionada a CVE-2026-46300 / Fragnesia-ORGANO JUDICIAL	MSS-INT	High	0	Answered
43813 Notable Event Alert: New TrickMo Variant Device Take Over malware targeting Banking Fintech Wallet Auth apps	MSS-INT	High	0	Answered
43814 Notable Event Alert: RVTools Leveraged In Multiple Attack Campaigns	MSS-INT	High	0	Answered
43817 Notable Event Alert: Vibe Hacking Two AI-Augmented Campaigns Target Government and Financial Sectors in Latin America	MSS-INT	High	0	Answered
43820 Notable Event Alert: New Maoloa Ransomware Variant	MSS-INT	High	0	Answered
43899 Notable Event Alert: Kimsukys Advanced Attack Techniques JSONPing Webex Spoofing and a New HttpSpy Variant	MSS-INT	High	0	Answered
43900 Notable Event Alert: Trellix Telemetry - Remus Stealer Infection Via Malicious Driver Update	MSS-INT	High	0	Answered
43901 Notable Event Alert: Attack Campaign Compromises Red Hat Cloud Services Packages	MSS-INT	High	0	Answered

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

Cybersecurity News

Title	Categories	Industries
FBI Probes Service Selling 153M+ Drivers Licenses	Cyber Attacks, Malware	Government, Healthcare, Banking and Financial, Hospitality, Transportation, Telecommunication
Breeze Comet Executes Hundreds of Fraudulent Transactions via Brazilian Payment Systems	Cyber Attacks, Malware	Government, Banking and Financial, Utilities
Hackers abuse Faronics Deploy admin tool to install ScreenConnect	Cyber Attacks	Government
Aesto Health says data breach affects over 9.5 million patients	Cyber Attacks, Compliance	Government, Healthcare, Banking and Financial, Education, Insurance
Nearly 22,000 Microsoft Exchange servers vulnerable to hijack attacks	Cyber Attacks, Vulnerabilities, Malware	Government, Legal Services
Massive Microsoft 365 outage causes auth issues, service failures	Cyber Attacks	Government

MSS-INT-V

Immediate Threat Intelligence Assessment

Threat	Status	Weakness	Tactic	Technique	APT	Rules of Engagement	related_countries	related_industries
Atomic macOS Stealer Infection Through Malicious Terminal Commands	Partial Blocked	Web Gateway Not Prevented 4/34	Initial Access	Drive-by Compromise	N/A	Countries: N/A | Industries: N/A		
CNCMachineRMS The Undocumented RAT At the End of a BabaDeda Chain	Blocked | Not Blocked	Antivirus Prevented 4/4 | Web Gateway Not Prevented 4/4	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
DeadLock Ransomware Employs Decentralized Recovery Infrastructure	Blocked | Not Blocked	Antivirus Prevented 2/2 | Web Gateway Not Prevented 6/6	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
DoubleCup ClickFix Loader Delivers CountLoader And DeviceManager RATs	Blocked | Partial Blocked	Antivirus Prevented 8/8 | Web Gateway Not Prevented 28/66	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		

MSS-INT REPORT

Organo Judicial 09/02/2026

Threat	Status	Weakness	Tactic	Technique	APT	Rules of Engagement	related_countries	related_industries
Fortinet Vulnerability CVE-2026-35616 and EKZ Stealer Attacking Obfuscating Compilers with Binary Ninja Workflows	Blocked | Partial Blocked	Antivirus Prevented 2/2 | Web Gateway Not Prevented 2/4	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
GenieLocker Ransomware Targets Windows ESXi And Linux Systems	Blocked | Partial Blocked	Antivirus Prevented 6/6 | Web Gateway Not Prevented 6/8	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
GhostDesk Chrome Spyware Installed Through Fake CCleaner	Blocked | Partial Blocked	Antivirus Prevented 10/10 | Web Gateway Not Prevented 10/12	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
GitHub Actions Abused To Exploit cPanel And WHM Servers	Blocked	Web Gateway Prevented 16/16	Initial Access	Drive-by Compromise	N/A	Countries: N/A | Industries: N/A		
Grandoreiro goes north From Brazil to Mexico with a new DLL sideloading campaign	Not Blocked | Partial Blocked	Antivirus Not Prevented 4/36 | Web Gateway Not Prevented 36/36	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
Gunra Ransomware-as-a-Service Targets Critical Infrastructure Worldwide AA26-222A	Blocked | Partial Blocked	Antivirus Prevented 4/4 | Web Gateway Not Prevented 4/16	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
Kimsuky Group Impersonates Diplomats Using PebbleDash And PrxClient	Blocked | Partial Blocked	Antivirus Prevented 6/6 | Web Gateway Not Prevented 6/24	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
Kynx Stealer Targets Crypto Wallets Gaming Platforms And AI Tools	Partial Blocked	Antivirus Not Prevented 2/38 | Web Gateway Not Prevented 40/46	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		

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

MSS-INT REPORT

Organo Judicial 09/02/2026

Threat	Status	Weakness	Tactic	Technique	APT	Rules of Engagement	related_countries	related_industries
Midnight Blizzard Targets Travelers In CaptiveCrunch Campaign	Blocked | Partial Blocked	Antivirus Prevented 4/4 | Web Gateway Not Prevented 4/28	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
Mirage Kitten Deploys NightLedger Backdoor And Tunneling Tools	Blocked | Partial Blocked	Antivirus Prevented 2/2 | Web Gateway Not Prevented 10/32	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
Operation Dream Job Exploits Zero-Day In Targeted Attack	Blocked | Partial Blocked	Antivirus Prevented 22/22 | Web Gateway Not Prevented 24/28	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
PhantomStealer Phishing Campaign Exploits Vulnerable Drivers And UAC Bypass	Blocked | Not Blocked	Antivirus Prevented 4/4 | Web Gateway Not Prevented 6/6	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
Phishing Campaign Delivers ScreenConnect Via Fake Transaction Receipts	Not Blocked | Partial Blocked	Antivirus Not Prevented 4/4 | Web Gateway Not Prevented 4/6	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
Project CAV3RN Uses Google Apps Script For Stealthy C2	Blocked | Partial Blocked	Antivirus Prevented 10/10 | Web Gateway Not Prevented 10/28	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
Russian State-Supported Cyber Actors Target Zimbra Collaboration Suite AA26-204A	Not Blocked | Partial Blocked	Antivirus Not Prevented 8/8 | Web Gateway Not Prevented 16/58	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		

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

MSS-INT REPORT

Organo Judicial 09/02/2026

Threat	Status	Weakness	Tactic	Technique	APT	Rules of Engagement	related_countries	related_industries
StopRansomware: Medusa Ransomware 2,026	Blocked | Partial Blocked	Antivirus Prevented 4/4 | Web Gateway Not Prevented 2/18	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
Striking gold Inside the GoldDigger Android malware	Not Blocked	Antivirus Not Prevented 6/6 | Web Gateway Not Prevented 6/6	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
TAG-195 Upgrades MaaS Ecosystem With Modular Tools	Blocked | Partial Blocked	Antivirus Prevented 56/56 | Web Gateway Not Prevented 56/74	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
Technical Analysis Of Modular Abyssos RAT	Blocked | Partial Blocked	Antivirus Prevented 4/4 | Web Gateway Not Prevented 4/8	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
The Gentlemen Affiliate Deploys EtherRAT Across Windows Networks Using Ethereum Smart Contract C2	Partial Blocked	Antivirus Not Prevented 2/4 | Web Gateway Not Prevented 4/30	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
npm Worm Poisons Hundreds Of Packages Across Multiple Organizations	Blocked | Partial Blocked	Antivirus Prevented 6/6 | Web Gateway Not Prevented 6/14	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

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

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