TLP:AMBER

MSS-BAS IMTHREAT REPORT

ORGANO JUDICIAL

September 02, 2026

TLP AMBER
MSS-BAS IMTHREAT REPORT

Sobre este reporte

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

Cymulate Score

19%

Percent Penetrated

162%

Simulation Summary

Penetrated: 162 / Total: 430

Immediate Threats Campaigns

assessmentName	Risk	Penetrated_Events	Affected_Controls
TAG-195 Upgrades MaaS Ecosystem With Modular Tools	3	28	□ Web Gateway
Kynx Stealer Targets Crypto Wallets Gaming Platforms And AI Tools	3	21	□ Web Gateway | □ EDR / Endpoint
Grandoreiro goes north From Brazil to Mexico with a new DLL sideloading campaign	3	20	□ Web Gateway | □ EDR / Endpoint
DoubleCup ClickFix Loader Delivers CountLoader And DeviceManager RATs	3	14	□ Web Gateway
Operation Dream Job Exploits Zero-Day In Targeted Attack	3	12	□ Web Gateway
Russian State-Supported Cyber Actors Target Zimbra Collaboration Suite AA26-204A	3	12	□ Web Gateway | □ EDR / Endpoint
Striking gold Inside the GoldDigger Android malware	3	6	□ Web Gateway | □ EDR / Endpoint
GhostDesk Chrome Spyware Installed Through Fake CCleaner	3	5	□ Web Gateway

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

MSS-BAS IMTHREAT REPORT

Organo Judicial 09/02/2026

assessmentName	Risk	Penetrated_Events	Affected_Controls
Mirage Kitten Deploys NightLedger Backdoor And Tunneling Tools	3	5	Web Gateway
Project CAV3RN Uses Google Apps Script For Stealthy C2	3	5	Web Gateway
Phishing Campaign Delivers ScreenConnect Via Fake Transaction Receipts	3	4	Web Gateway	EDR / Endpoint
GenieLocker Ransomware Targets Windows ESXi And Linux Systems	3	3	Web Gateway
PhantomStealer Phishing Campaign Exploits Vulnerable Drivers And UAC Bypass	3	3	Web Gateway
The Gentlemen Affiliate Deploys EtherRAT Across Windows Networks Using Ethereum Smart Contract C2	3	3	Web Gateway	EDR / Endpoint
DeadLock Ransomware Employs Decentralized Recovery Infrastructure	3	3	Web Gateway
Kimsuky Group Impersonates Diplomats Using PebbleDash And PrxClient	3	3	Web Gateway
npm Worm Poisons Hundreds Of Packages Across Multiple Organizations	3	3	Web Gateway
Atomic macOS Stealer Infection Through Malicious Terminal Commands	3	2	Web Gateway
CNCMachineRMS The Undocumented RAT At the End of a BabaDeda Chain	3	2	Web Gateway
Gunra Ransomware-as-a-Service Targets Critical Infrastructure Worldwide AA26-222A	3	2	Web Gateway
Midnight Blizzard Targets Travelers In CaptiveCrunch Campaign	3	2	Web Gateway
Technical Analysis Of Modular Abyssos RAT	3	2	Web Gateway
Fortinet Vulnerability CVE-2026-35616 and EKZ Stealer Attacking Obfuscating Compilers with Binary Ninja Workflows	3	1	Web Gateway
StopRansomware: Medusa Ransomware 2,026	3	1	Web Gateway

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-BAS IMTHREAT 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