

TLP:AMBER

MSS-INT REPORT

TROPIGAS

November 17, 2026



©2023. GLESEC. All Rights Reserved.

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

26

0

Executive Action Required

▲

10 items pending executive awareness or decision

Threat Relevance Score (TRS)

49
→ 0

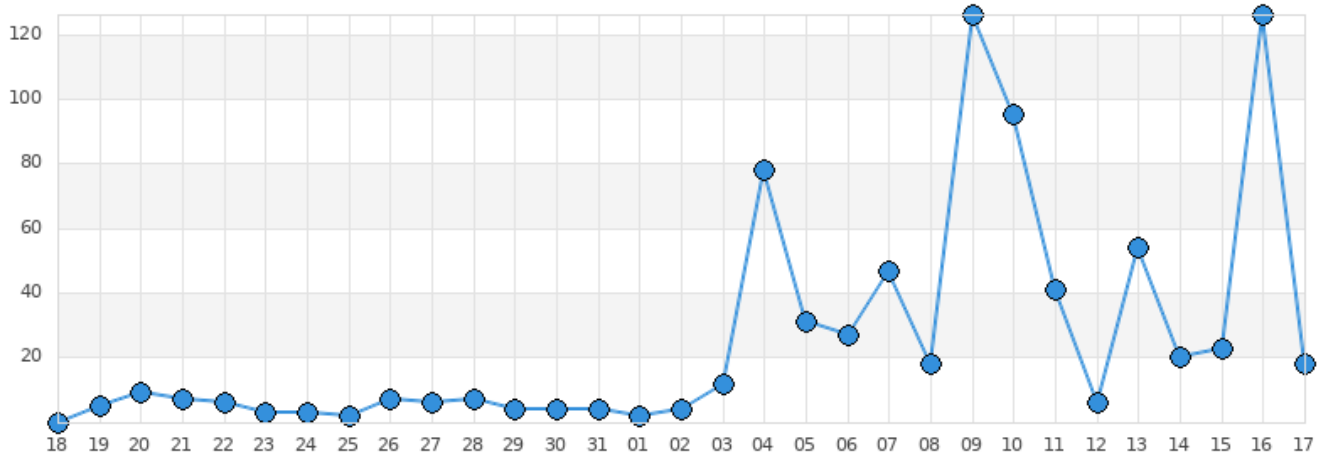
Risk Score (RS)

52
▲ +1

©2023. GLESEC. All Rights Reserved.

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

Threat Landscape – Feed Volume



©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

MSS-INT REPORT

TROPIGAS 11/17/2026

Threat Headlines

Date	Threat Headline	Actor	Malware	Sector	Why Relevant
Nov 14, 2,026	OTX [Storm-3358]: Threat Overview of ARTEX Autonomous Penetration Testing Framework	Storm-3358	BloodAlchemy	Energy	Sector + Region
Nov 11, 2,026	OTX [Citrus Ransomware]: Citrus Ransomware: tactics, techniques, procedures, and links to Toy Ghouls	Citrus Ransomware	Sn00py	Energy	Sector + Region
Nov 10, 2,026	OTX [CyberAveng3rs]: The Cold Chain on Fire: Unpatched Danfoss controllers exploited	CyberAveng3rs	-	Energy	Sector + Region
Nov 6, 2,026	OTX [Storm-0940]: ARTEX: Agentic Asbestos	Storm-0940	Cobalt Strike - S0154	Manufacturing	Sector + Region
Nov 5, 2,026	OTX [Black Owl (BO Team]: Supply chain attack: BO Team in a software developer's infrastructure	Black Owl (BO Team	Nanodump	Manufacturing	Sector + Region
Nov 5, 2,026	OTX [TraderTraitor]: Binance heist: what we know, and what we see in TraderTraitor's toolkit	TraderTraitor	FLATROOF	Manufacturing	Sector + Region
Nov 5, 2,026	OTX [APT29]: Hackers exploited iOS and Android flaws to infect phones	APT29	DarkSword	Energy	Sector + Region
Nov 4, 2,026	OTX [APT29]: Poisoned Source: APT29 Watering Holes Targets Mobile Devices	APT29	DarkSword	Energy	Sector + Region
Nov 3, 2,026	OTX [HAZY TIGER]: BITTER Expands Its Arsenal with PapRAT	HAZY TIGER	PapRAT	Energy	Sector + Region
Nov 3, 2,026	OTX [Videostrong Technology Co., Ltd.]: The Internals of a Badbox Operation	Videostrong Technology Co., Ltd.	x.cpe	Manufacturing	Sector + Region

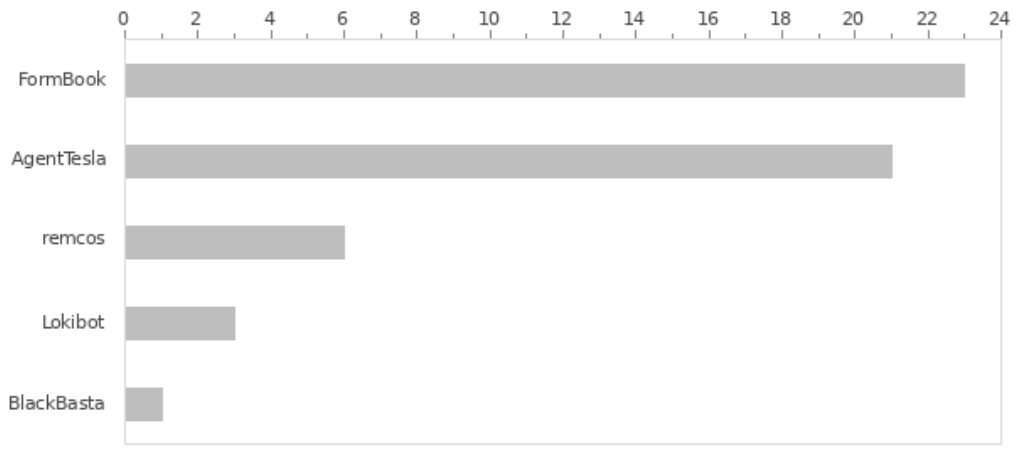
©2023. GLESEC. All Rights Reserved.

TLP:AMBER

MSS-INT REPORT

TROPIGAS 11/17/2026

Relevant Top Malware Families



Relevant Top Threat Actors

ThreatActor	client	count
teampcp	TROPIGAS	3
agent tesla	TROPIGAS	1
aurora	TROPIGAS	1
blitz brigantine	TROPIGAS	1
cl-unk-1068	TROPIGAS	1

Persistence of Blocked Attacks to Organization's Perimeter

	181.197.127.222	181.197.52.116	198.57.41.238	195.178.110.102	20.225.18.9	34.62.234.122	54.85.110.29	9.141.30.218
198.18.13.8	628 (3%)	1040 (4%)	1064 (5%)	1656 (7%)	16598 (70%)	1040 (4%)	854 (4%)	714 (3%)
portal.bambitospringwat	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	2088 (99%)	28 (1%)	0 (0%)
portal.tropigas.com.pa	0 (0%)	0 (0%)	0 (0%)	0 (0%)	8 (0%)	0 (0%)	1660 (63%)	952 (36%)
pulse.ppacservices.com	0 (0%)	0 (0%)	0 (0%)	0 (0%)	8 (100%)	0 (0%)	0 (0%)	0 (0%)
spc.tropigas.com.pa	0 (0%)	2080 (34%)	2128 (35%)	1404 (23%)	0 (0%)	0 (0%)	0 (0%)	476 (8%)
trencoapp.tropigas.com.	256 (3%)	0 (0%)	0 (0%)	1908 (5%)	33180 (91%)	0 (0%)	0 (0%)	0 (0%)

Ongoing cases

Case #	Service	Priority	Hours	Status
44109 Tropigas TEAR 060826	MSS-INT	High	0	Answered
48178 Notable Event Alert: Analysis of Gamaredon campaign targeting Ukraine weaponizing CVE-2025-8088	MSS-INT	High	0	Answered

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL

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

TLP:AMBER

GLESEC
COMPLETELY PERCEPTI

MSS-INT REPORT

TROPIGAS 11/17/2026

Case #	Service	Priority	Hours	Status
49042 Notable Event Alert: Mustang Panda Targets India With ZOHOMURK And MINIRECON Implants	MSS-INT	Medium	0	Answered
49421 Notable Event Alert: LokiBot After a Decade An Analysis of a Recent LokiBot Campaign	MSS-INT	High	0	Answered
49819 Notable Event Alert: StrikeShark Campaign Delivers Cobalt Strike Via Custom SharkLoader Malware	MSS-INT	Medium	0	Answered
49913 Notable Event Alert: Armored Likhos New Weapon BusySnake Stealer	MSS-INT	High	0	Answered
50025 Notable Event Alert: From Phishing to Persistence A CrySome RAT Infection Chain Analysis	MSS-INT	High	0	Answered
50329 Notable Event Alert: Cavern Manticore Exposing Iran Linked Modular C2 Framework	MSS-INT	High	0	Answered
50573 Notable Event Alert: APT-C-20 Uses Explorer Hijacking And LSB Steganography Techniques	MSS-INT	High	0	Answered
50662 Notable Event Alert: Vidar Infostealer Distributed Through Phishing Email Campaigns	MSS-INT	Medium	0	Answered

Cybersecurity News

Title	Categories	Industries
QUIC and Covert: Novel HTTP/3-Powered RATs Target Southeast Asian Governments	Cyber Attacks, Data Breaches, Malware	Government, Utilities, Education, Legal Services, Cryptography
⚡ Weekly Recap: N-able 0-Days, Windows 0-Days, Chrome 0-Days, Fridge 0-Days, and More Bad Days	Cyber Attacks, Vulnerabilities, Malware	Utilities, Legal Services, Blockchain
BO Team Exploits Log4Shell in VMware vCenter, Compromises Russian Firm's Code-Signing Server	Cyber Attacks, Vulnerabilities, Malware	Utilities, Military
The XG Files: Falcon C2 Flying Under The (Browser) Radar	Cyber Attacks, Malware	Government, Utilities, Education, Legal Services, Military, Blockchain
Three China-Nexus Espionage Campaigns Linked Through Sparrow Malware Ecosystem	Cyber Attacks, Malware	Government, Utilities, Telecommunication, Military
Not All That Glitters Is Gold: Tracking CopperDragon’s Sparrow Framework Around the Globe	Cyber Attacks, Malware	Government, Utilities, Telecommunication, Military

MSS-INT-V

Immediate Threat Intelligence Assessment

©2023. GLESEC. All Rights Reserved.

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

MSS-INT REPORT

TROPIGAS 11/17/2026

Threat	Status	Weakness	Tactic	Technique	APT	Rules of Engagement	related_countries	related_industries
3AM Ransomware Affiliate Hits European Schools With Hybrid AI Attack	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		
Analysis of Wpcdoor Attack Case Distributed Through Domestic DVR Management Software	Blocked | Not Blocked	Antivirus Not Prevented 4/4 | Email Gateway Prevented 2/2 | Web Gateway Not Prevented 6/6	Execution, Initial Access	Drive-by Compromise, Malicious File, Spearphishing Link	N/A	Countries: N/A | Industries: N/A		
Beyond testmetest Native Addon Camouflage and 42 Armed GitHub Repositories Reveal a Hidden npm Publisher	Blocked | Not Blocked | Partial Blocked	Antivirus Not Prevented 2/2 | Email Gateway Prevented 4/4 | Web Gateway Not Prevented 2/4	Execution, Initial Access	Drive-by Compromise, Malicious File, Spearphishing Attachment, Spearphishing Link	N/A	Countries: N/A | Industries: N/A		
Citrus Ransomware tactics techniques procedures and links to Toy Ghouls	Not Blocked	Antivirus Not Prevented 2/2 | Web Gateway Not Prevented 2/2	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
DarkCore A Data-Theft RAT With a Session-Hijacking Browser	Blocked | Not Blocked | Partial Blocked	Antivirus Not Prevented 6/6 | Email Gateway Prevented 2/2 | Web Gateway Not Prevented 6/8	Execution, Initial Access	Drive-by Compromise, Malicious File, Spearphishing Link	N/A	Countries: N/A | Industries: N/A		
Deletion attacks against organizational networks in Israel using Checkpoint equipment	Blocked	Web Gateway Prevented 8/8	Initial Access	Drive-by Compromise	N/A	Countries: N/A | Industries: N/A		

©2023. GLESEC. All Rights Reserved.

MSS-INT REPORT

TROPIGAS 11/17/2026

Threat	Status	Weakness	Tactic	Technique	APT	Rules of Engagement	related_countries	related_industries
Download 648efc19_11_Exe.exe - Inside Qilin ransomware ESXi attacks affiliate networks and double ex	Not Blocked	Web Gateway Not Prevented 2/2	Initial Access	Drive-by Compromise	N/A	Countries: N/A | Industries: N/A		
Drop file 648efc19_11_Exe.exe - Inside Qilin ransomware ESXi attacks affiliate networks and double e	Not Blocked	Antivirus Not Prevented 2/2	Execution	Malicious File	N/A	Countries: N/A | Industries: N/A		
Fake-Download Campaign Uses Trojanized Installers For Monetization Payloads	Blocked | Not Blocked | Partial Blocked	Antivirus Not Prevented 14/14 | Email Gateway Prevented 28/28 | Web Gateway Not Prevented 14/42	Execution, Initial Access	Drive-by Compromise, Malicious File, Spearphishing Link	N/A	Countries: N/A | Industries: N/A		
From Business Emails to XLoader An Order Lure That Led to In-Memory Injection	Not Blocked | Partial Blocked	Antivirus Not Prevented 12/26 | Web Gateway Not Prevented 32/32	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
GhostFrame ESXi Implant Linked To Settra Ransomware Group	Blocked | Not Blocked	Email Gateway Prevented 2/2 | Web Gateway Not Prevented 2/2	Initial Access	Drive-by Compromise, Spearphishing Link	N/A	Countries: N/A | Industries: N/A		
Microsoft Lookalike Domain Delivers ClickFix RAT Targeting Czech Company	Not Blocked	Antivirus Not 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		

©2023. GLESEC. All Rights Reserved.

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

Threat	Status	Weakness	Tactic	Technique	APT	Rules of Engagement	related_countries	related_industries
Volta Infostealer Uses LLMs To Rank Victim Assets	Not Blocked	Antivirus Not Prevented 2/2 | Web Gateway Not Prevented 2/2	Execution, Initial Access	Drive-by Compromise, Malicious File	N/A	Countries: N/A | Industries: N/A		
n0n Ransomware Exposed Workspace Reveals AI-Assisted Extortion Operation	Not Blocked | Partial Blocked	Antivirus Not Prevented 6/6 | Web Gateway Not Prevented 6/20	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.**

©2023. GLESEC. All Rights Reserved.

PROPRIETARY & CONFIDENTIAL

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.

©2023. GLESEC. All Rights Reserved.

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