CYBER THREAT INTELLIGENCE

CRITICAL**START**® Security Advisory

TLP CLEAR // [CS-SA-26-0303] The Threat – Handala Hack Team

Executive Summary

Handala Hack Team is a pro-Palestinian, anti-Israel hacktivist persona associated with destructive cyber operations that combine wiper malware, hands-on-keyboard intrusion, and hack-and-leak messaging. The group frequently frames attacks as retaliation against Israel and its allies, including the United States. In March 2026, the group claimed responsibility for a disruptive incident affecting Stryker. The company reported widespread operational disruption and stated it had no indication of ransomware and believed the incident was contained, while reporting indicated some devices appeared to have been wiped. Security researchers have linked Handala activity to destructive campaigns since late 2023, including phishing-delivered wipers and the use of Telegram infrastructure. Check Point Research assesses the persona as connected to Void Manticore, which it associates with Iran's Ministry of Intelligence and Security (MOIS). Reported activity emphasizes credential compromise, RDP-based lateral movement, and domain-wide distribution of destructive payloads. Handala's operations appear to support Iranian strategic objectives while maintaining plausible deniability through a hacktivist front. Several operations have occurred during periods of geopolitical tension involving Iran, Israel, and the United States, suggesting potential retaliatory signaling or opportunistic timing.

Key Findings for Defenders

- Handala conducts manual, hands-on intrusions using custom and publicly available tools, with a deliberate focus on maximum destructive impact rather than long-term espionage.
- Initial access relies primarily on VPN credential abuse, phishing (including SMS phishing), and supply-chain compromise of IT/MSP providers.
- Wiping operations employ at least four simultaneous destruction techniques distributed via Group Policy, designed to overwhelm partial defenses and prevent recovery.
- A new, high-impact TTP confirmed in the Stryker attack involves abuse of Microsoft Intune MDM to issue authenticated mass remote device wipes, bypassing endpoint security software entirely.
- The group's targeting has expanded from exclusively Israeli organizations to U.S. entities with Israeli business ties or U.S. Department of Defense contracts.
- Handala's operational security has degraded since early 2026; the group has been observed connecting directly from Iranian IP addresses and Starlink IP ranges.

Threat Actor Operational Characteristics

Handala is distinguished from many nation-state actors by its preference for manual, hands-on intrusions rather than fully automated attack chains. The group typically establishes access and conducts reconnaissance weeks or months before executing the destructive phase. When the destructive phase begins, it is rapid and multi-vector, designed to inflict maximum damage before defenders can respond. The group publicizes attacks on Telegram and at handala-hack[.]to, typically with manifestos framing operations in terms of political retaliation. Defenders should note that Handala has a documented history of exaggerating the scale of attacks. At least one organization previously denied Handala's claimed compromise. Claimed metrics (e.g., number of systems wiped, data exfiltrated) should be treated as potentially inflated, while confirmed TTPs and IOCs must be taken seriously.

© 2026 Critical Start. All rights reserved.

Tactics, Techniques, and Procedures (TTPs)

Handala's intrusions begin with credential-based initial access, primarily through brute-force and credential abuse against organizational VPN infrastructure, originating from commercial VPN nodes. The group also uses Spearphishing via email and SMS, with at least one member assessed as fluent in Hebrew based on the quality of lures. IT and service providers are deliberately targeted as supply-chain footholds to reach downstream victims.

Once inside, lateral movement is conducted manually via RDP. In recent intrusions, the group deployed NetBird, a legitimate open-source zero-trust mesh VPN tool, by connecting to compromised hosts via RDP and downloading it directly from the official NetBird website using the local browser. At least five attacker-controlled machines were observed operating simultaneously within one victim environment using this method. Credential theft runs in parallel: LSASS is dumped via comsvcs.dll through rundll32.exe, sensitive registry hives are exported via wmic.exe, and ADRecon (renamed dra.ps1) is used for Active Directory enumeration. Initial access in at least one confirmed intrusion was established months before the destructive phase.

During the destructive phase, Handala deploys four wiping techniques in parallel: a custom executable wiper (handala.exe) with MBR overwrite capability, a PowerShell-based wiper, Group Policy logon scripts distributing both components domain-wide, and confirmed in the Stryker attack, abuse of Microsoft Intune MDM to issue remote wipe commands across enrolled devices. In the Stryker incident, employees with Microsoft Outlook configured on personal devices had those devices wiped as well. Earlier campaigns used an NSIS installer disguised as a legitimate update, with batch script obfuscation and time-based delays to evade sandbox analysis and bypass antivirus process checks. Post-destruction, login pages are defaced with the Handala logo and stolen data is published to the group's Telegram channel and leak site. Appendix B contains a table that maps observed Handala behaviors to the MITRE ATT&CK framework. Entries are derived from published research. Behaviors from prior operations that remain likely to recur are included.

Consolidated Industry Overview of Handala Targets

Based on Handala Hack Team’s claimed victims in H2 2025, targeted entities fall across several broad sectors not limited to:

Sector	Description
Israeli Organizations (All Sectors)	Israeli entities remain the primary focus. Targets span government, telecommunications, healthcare, energy, defense contractors, and private sector organizations. Nearly any Israeli-affiliated organization may be considered a viable target.
Media and Information	Journalists, media figures, and broadcasting organizations targeted for access to communications, editorial networks, and influence opportunities.
Government	Political leaders and senior government staff targeted for potential insight into policymaking and internal communications.
Defense, Aerospace, and Security	Engineers, researchers, and specialists connected to missile defense systems, drone programs, and cyber units.
Technology and Telecoms	Software companies, technology platforms, cybersecurity professionals, and telecommunications infrastructure.
Critical Infrastructure and Energy	Organizations operating essential systems such as fuel distribution and other infrastructure supporting national operations.

© 2026 Critical Start. All rights reserved.

Industrial and Commercial Services	Manufacturing, construction, catering, logistics, legal services, and technology retail organizations that may provide indirect access to supply chains or operational data.
Healthcare	Hospitals, medical providers, and healthcare systems that manage sensitive patient data and essential operational services.

Implications for Organization

Handala's expanding targeting scope makes this threat relevant well beyond Israeli organizations. Any organization that is publicly affiliated with Israel, conducts business with Israeli companies, has acquired Israeli subsidiaries, holds U.S. Department of Defense contracts, or is perceived as opposing Iranian or Palestinian interests should consider itself a potential target. Handala has explicitly cited Stryker's 2019 acquisition of Israeli medical technology company OrthoSpace and Stryker's U.S. military contracts as justification for the attack. Organizations in healthcare, defense supply chain, critical infrastructure, financial technology, and IT services with any of these affiliations should move to a heightened alert posture immediately.

The group's recent expansion to U.S.-based enterprises, combined with a documented decline in operational security including direct connections from Iranian IP addresses, suggests an acceleration in operational tempo rather than restraint. The Stryker attack occurred just two days after the White House released its Cyber Strategy for America framework and follows a pattern of Iranian cyber activity timed to kinetic military escalation. Organizations should treat the current geopolitical environment as an active threat condition, not a watch-and-wait situation.

The Intune MDM abuse confirmed in the Stryker attack represents a category shift in destructive capability. A single compromised cloud administrator credential can now result in the simultaneous, irreversible destruction of an organization's entire global device fleet with no malware required on endpoints. Traditional endpoint detection will not catch this. Defenders must prioritize identity and cloud management plane security with the same urgency previously reserved for perimeter defenses.

Organizational Mitigation Strategies

In light of the elevated threat environment following Operation Epic Fury and Handala's confirmed expansion to U.S. targets, organizations should implement or validate the following controls, prioritized by recommended timeframe.

24 to 48 Hours

- Audit Azure AD and Intune administrator role assignments. Remove any accounts with Global Administrator or Intune Device Administrator privileges that are not actively required. Enable Privileged Identity Management (PIM) for just-in-time elevation on all remaining admin accounts.
- Review Microsoft Intune audit logs for any bulk device wipe commands or anomalous admin activity. Correlate against Azure AD sign-in logs for the same accounts.
- Send employee awareness communications specifically addressing conflict-themed phishing lures, including SMS-based phishing impersonating IT vendors, security firms, and device manufacturers.
- Validate that MFA is enforced on all VPN, remote access, and Microsoft 365 admin accounts. Disable legacy authentication protocols that bypass MFA enforcement.
- Block or alert on authentication attempts to enterprise VPN gateways originating from commercial VPN provider IP ranges, including the 169.150.227.x and 149.88.26.x segments, and from Starlink IP ranges (188.92.255.x, 209.198.131.x), which have been confirmed in Handala egress activity.

1 Week

- Audit and restrict Group Policy Object modification rights. Alert on any new GPO logon scripts or scheduled task additions created outside of your change management process, as these are Handala's primary domain-wide wiper distribution mechanism.

© 2026 Critical Start. All rights reserved.

- Hunt across EDR telemetry for the IOCs listed in this advisory: handala.exe, handala.bat, dra.ps1, NetBird installation artifacts, and LSASS dump activity via comsvcs.dll through rundll32.exe.
- Audit all RMM tools and remote access utilities (AnyDesk, Atera, ScreenConnect) for unauthorized instances. Validate that only approved tools are present and that access logs are being collected.
- Block or alert on installation of peer-to-peer mesh VPN tools (NetBird, Tailscale, ZeroTier) on endpoints not in an approved software inventory. Outbound connections to netbird.io from internal hosts should be flagged immediately.
- Validate email security controls (DMARC, DKIM, SPF) and confirm that macro-enabled attachments and NSIS installer packages arriving via email are sandboxed or blocked.

30 Days

- Test offline backup recoverability end-to-end. Handala deploys at least four simultaneous wiping mechanisms specifically designed to defeat partial backup strategies. Confirm that at least one backup copy is fully air-gapped and that recovery time has been validated under a simulated total-wipe scenario.
- Review and enforce network segmentation to ensure domain controllers are not reachable via RDP from general user network segments. Implement RDP gateway controls with session logging.
- Develop or update incident response playbooks for a simultaneous enterprise-wide device wipe, including out-of-band communication procedures that do not depend on the Microsoft tenant.
- Conduct a tabletop exercise simulating full Microsoft environment compromise. Key questions: can the organization operate for 72 hours with no corporate email, no Teams, no Intune-managed devices, and no Azure AD authentication.
- Review third-party vendor and MSP access, specifically any delegated Azure AD or Intune administrator permissions. Require hardware MFA for all vendor accounts and validate that access is scoped to the minimum necessary.

What Critical Start is Doing

The Critical Start Cyber Research Unit is actively monitoring Handala and the broader Iranian threat actor ecosystem. If you are a Critical Start MDR customer, our SOC is positioned to hunt for Handala IOCs across your environment, validate your Intune and Azure AD administrator controls, identify exposure to confirmed Handala network indicators, and provide tailored briefings for your security leadership or board.

For an overview of the Cyberattack on Stryker by Handala Hack Team as reported, visit Critical Start's Intel Hub. If you are not yet a Critical Start customer and want to understand your exposure, reach us at criticalstart.com.

Conclusion

Handala Hack Team has been an active and persistent threat since late 2023, conducting sustained wiper attacks and hack-and-leak operations across Israeli government, healthcare, critical infrastructure, and private sector targets throughout 2024 and into 2026. The March 2026 Stryker attack was not an emergence but an escalation, marking the group's most consequential operation to date and confirming its expansion to large U.S. enterprises.

There is no indication the group is slowing down. The current geopolitical environment, marked by active military conflict between Israel, the U.S., and Iran, continues to provide both the motivation and the political cover for further operations. Handala has shown a consistent pattern of timing attacks to kinetic escalation events, and with that conflict ongoing, additional retaliatory operations should be expected. The group's TTPs are well-documented and largely consistent, which means defenders have clear, actionable detection and hardening opportunities. Organizations with any visible affiliation to Israel, U.S. defense interests, or industries perceived as opposing Iranian or Palestinian interests should treat Handala as an active and credible threat, not a regional concern to monitor from a distance.

© 2026 Critical Start. All rights reserved.

Further Reading

1. Check Point Research: Handala Hack -- Unveiling Group's Modus Operandi
2. Splunk Threat Research Team / Cisco Talos, "Handala's Wiper: Threat Analysis and Detections
3. Intezer - Operation HamsaUpdate: Wipers Put Israeli Infrastructure at Risk
4. Trellix Advanced Research Center - Handala's Wiper Targets Israel
5. KrebsOnSecurity - Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker
6. The Record (Recorded Future News) Medical Device Giant Stryker Confirms Cyberattack
7. Help Net Security - War Spreads into Cyberspace after Iran-Linked Hackers Hit Stryker
8. Nextgov/FCW - CISA Launches Investigation into Stryker Cyberattack
9. HackRead - Iran-Linked Handala Hackers Claim Major Hacks on Stryker and Verifone
10. DataBreaches.net - Clalit Probes Suspected Cyberattack after Iranian-Linked Hackers Leak Patient Files
11. Tenable - Cyber Retaliation: Analyzing Iranian Cyber Activity Following Operation Epic Fury
12. Security Boulevard - Operation Epic Fury: Potential Iranian Cyber Counteroffensive
13. CISA Advisory AA22-264A - Iranian Government-Sponsored APT Actors Compromise Albanian Government

© 2026 Critical Start. All rights reserved.

Appendix A: Named CVEs Referenced

The following CVEs are referenced in reporting on Handala / Void Manticore operations or the broader MOIS threat actor ecosystem. CVEs exploited by related MOIS actors (Scarred Manticore, MuddyWater) are included given documented collaboration within the MOIS offensive cyber apparatus.

CVE ID	Affected Product	CVSS	Relevance to MOIS Operations	Recommended Action
CVE-2023-27350	PaperCut NG/MF	9.8 Critical	Pre-auth RCE in print management software. Exploited by multiple Iranian-affiliated actors for initial access to enterprise environments.	Patch to v22.0.10+
CVE-2021-26084	Atlassian Confluence	9.8 Critical	OGNL injection enabling pre-auth RCE. Exploited by MOIS-linked clusters including Void Manticore for initial access.	Patch to v7.13.7+ / v7.14.3+
CVE-2022-47966	Zoho ManageEngine	9.8 Critical	Pre-auth RCE via SAML. Used by Iranian threat actors in 2022 to 2023 campaigns to gain access to IT management infrastructure.	Patch immediately
CVE-2024-3400	Palo Alto PAN-OS	10.0 Critical	Command injection in GlobalProtect VPN. Observed in Iranian-affiliated campaigns to obtain VPN/network gateway access.	Patch to v11.1.2-h3+

Appendix B: Tactics, Techniques, and Procedure

The following tactics, techniques, and procedures (TTPs) are referenced in reporting on Handala / Void Manticore operations and associated activity across the broader Iranian Ministry of Intelligence and Security (MOIS) cyber ecosystem.

Tactic	MITRE ATT&CK Technique	Observed Behavior
Initial Access	T1078 -- Valid Accounts	VPN credential abuse via brute-force; hundreds of logon attempts against organizational VPN infrastructure from commercial VPN nodes (e.g., 169.150.227.x range). Post-Jan 2026 shift to Starlink IP ranges.
Initial Access	T1566.001 -- Spearphishing Attachment	Phishing campaigns using PDF lures (e.g., fake CrowdStrike fix tool); well-crafted Hebrew-language emails targeting Israeli organizations.
Initial Access	T1566.002 -- Spearphishing Link	SMS phishing (smishing) with malicious links leading to wiper payloads; at least one member assessed fluent in Hebrew based on email quality.
Initial Access	T1195 -- Supply Chain Compromise	Deliberate targeting of IT and service providers to harvest credentials for downstream victim access; a documented primary ingress strategy.
Execution	T1059.001 -- PowerShell	AI-assisted PowerShell wiper script; distributed via Group Policy logon scripts across victim network.
Execution	T1059.003 -- Windows Command Shell	Batch launcher scripts (handala.bat) with garbage-code obfuscation to trigger wiper components and hinder static analysis.

© 2026 Critical Start. All rights reserved.

Tactic	MITRE ATT&CK Technique	Observed Behavior
Execution	T1204.002 -- Malicious File	NSIS installer package disguised as a legitimate software update (e.g., update.zip) delivers wiper payload.
Execution	T1072 -- Software Deployment Tools	Abuse of Microsoft Intune MDM platform to issue authenticated remote wipe commands across all enrolled enterprise devices. Confirmed vector in Stryker (Mar 2026).
Lateral Movement	T1021.001 -- Remote Desktop Protocol	Primary lateral movement method. Manual RDP-based traversal between hosts; intensive hands-on approach within victim networks.
Lateral Movement	T1090 -- Proxy / Tunnel	Deployment of NetBird (legitimate open-source zero-trust mesh VPN) on compromised hosts to establish internal tunnels and pivot between network segments.
Discovery	T1087 / T1069 -- Account / Group Discovery	ADRecon (renamed dra.ps1) PowerShell framework used for Active Directory enumeration to identify pathways to Domain Administrator credentials.
Credential Access	T1003.001 -- LSASS Memory	LSASS process dump via comsvcs.dll / rundll32.exe to extract plaintext and hashed credentials from memory.
Credential Access	T1552.002 -- Registry Credentials	Export of sensitive registry hives (HKLM\SAM, SYSTEM, SECURITY) via wmic.exe and copy from Volume Shadow Copy.
Defense Evasion	T1562.001 -- Impair Defenses	Disabling Windows Defender prior to destructive phase. Antivirus process checks (avastui.exe, avgui.exe, bdservicehost.exe, sophoshealth.exe) to fingerprint the environment.
Defense Evasion	T1027 -- Obfuscated Files	Batch script obfuscation using invalid/garbage Windows commands interspersed with valid instructions to defeat static analysis.
Defense Evasion	T1497.003 -- Time-Based Evasion	90 to 180 second sleep delays injected if specific AV processes are absent, designed to evade automated sandbox execution analysis.
Defense Evasion	T1036 -- Masquerading	Wiper delivered as a fake CrowdStrike fix tool. Group impersonates legitimate IT brands in phishing campaigns.
Collection / Exfil	T1041 -- Exfiltration Over C2 Channel	Claimed exfiltration of 50 TB of data from Stryker. Stolen data published to Handala Telegram channel and the handala-hack[.]to leak site.
Command & Control	T1102 -- Web Service	Telegram channel (t.me/handala_hack8) used as a C2 communication channel, leak announcement platform, and propaganda outlet.
Impact	T1485 -- Data Destruction	Custom Handala Wiper (handala.exe) overwrites file contents across the file system; distributed as a scheduled task via Group Policy. PowerShell wiper deployed in final stage.
Impact	T1561.002 -- Disk Structure Wipe	MBR overwrite deployed alongside file-based wiping to prevent system recovery and re-imaging.
Impact	T1490 -- Inhibit System Recovery	Volume Shadow Copy deletion via vssadmin / wmic to prevent data restoration from local backups.
Impact	T1491.002 -- External Defacement	Entra ID / Azure AD login pages defaced with Handala logo post-compromise. Device login pages replaced across wiped systems to signal the attack publicly.

© 2026 Critical Start. All rights reserved.

Appendix C: Indicators of Compromise (IOCs)

These indicators may be ingested into SIEM, EDR, and threat hunting platforms. Network-layer IOCs (IP addresses) associated with Handala are short-lived due to the group's use of commercial VPN infrastructure. Behavioral indicators and file-based IOCs are more durable. All IP addresses should be defanged before ingestion into production blocking systems.

Indicator Type	Value	Context / Source
IP Address	107.189.19[.]52	Handala C2 server; payload retrieval during pre-destructive phase. (Check Point Research, 2026)
IP Address	146.185.219[.]235	VPN exit node assessed as linked to Handala operational infrastructure. (Check Point Research, 2026)
IP Address	31.192.237[.]207:2515	C2 endpoint identified in wiper sample analysis. (Intezer, 2023)
IP Range	169.150.227[.]x	Commercial VPN egress segment used by Handala during Israel operations. (Check Point Research, 2026)
IP Range	149.88.26[.]x	Additional commercial VPN range cited in Handala infrastructure. (Check Point Research, 2026)
IP Range	188.92.255[.]x	Starlink egress range observed post-Iran internet shutdown, Jan 2026. (Check Point Research, 2026)
IP Range	209.198.131[.]x	Starlink egress range observed post-Iran internet shutdown, Jan 2026. (Check Point Research, 2026)
Domain	handala-hack[.]to	Official Handala data leak and announcement website.
URL	sjc1.vultrobjects[.]com/f5update/update[.]sh	Payload delivery URL in Operation HamsaUpdate (F5 device impersonation). (Intezer, 2023)
MD5	5986ab04dd6b3d259935249741d3eff2	Handala Wiper executable. (Check Point Research, 2026)
MD5	3cb9dea916432ffb8784ac36d1f2d3cd	Handala PowerShell Wiper script. (Check Point Research, 2026)
MD5	3236facc7a30df4ba4e57fddfba41ec5	VeraCrypt installer used in wiping operations. (Check Point Research, 2026)
MD5	3dfb151d082df7937b01e2bb6030fe4a	NetBird installer deployed for lateral movement tunneling. (Check Point Research, 2026)
MD5	e035c858c1969cffc1a4978b86e90a30	NetBird binary. (Check Point Research, 2026)
SHA256	96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8	Wiper payload. (Splunk/Talos, 2024)
SHA256	19001dd441e50233d7f0addb4fcd405a70ac3d5e310ff20b331d6f1a29c634f0	Phishing attachment PDF lure. (Splunk/Talos, 2024)

© 2026 Critical Start. All rights reserved.

Indicator Type	Value	Context / Source
SHA256	8316065c4536384611cbe7b6ba6a5f12f10db09949e66cb608c92ae8b69e4d67	OpenFileFinder.dll component. (Splunk/Talos, 2024)
SHA256	fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2	F5UPDATER.exe loader, Operation HamsaUpdate. (Intezer, 2023)
SHA256	ca9bf13897af109cb354f2629c10803966eb757ee4b2e468abc04e7681d0d74a	F5UPDATER.exe loader variant, Operation HamsaUpdate. (Intezer, 2023)
SHA256	454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567	Handala.exe Delphi wiper component. (Intezer, 2023)
SHA256	e28085e8d64bb737721b1a1d494f177e571c47aab7c9507dba38253f6183af35	Hatef.exe wiper component. (Intezer, 2023)
File Name	handala.exe	Primary Handala Wiper; deployed via Group Policy scheduled task. MBR-wiping capability confirmed.
File Name	handala.bat	Batch launcher script triggering handala.exe and PowerShell wiper; distributed via Group Policy logon scripts.
File Name	dra.ps1	ADRecon PowerShell AD enumeration framework renamed for Handala intrusions.
File Name	handala.gif	Propaganda image placed on logical drives as a defacement artifact during the wiping stage. (Check Point Research, 2026)
Tool / Binary	NetBird	Legitimate zero-trust mesh VPN abused for lateral movement tunneling. Installed manually by attackers via browser from netbird.io.
Tool / Binary	comsvcs.dll via rundll32.exe	Used for LSASS memory dump during credential theft phase.
Behavioral Pattern	DESKTOP-XXXXXX / WIN-XXXXXX hostnames	Default Windows hostname pattern tied to Handala VPN brute-force infrastructure. Use as heuristic, not definitive attribution. (Check Point Research, 2026)
Behavioral Pattern	Bulk Intune remote wipe via MDM	Abuse of Microsoft Intune to issue enterprise-wide authenticated device wipe commands. Confirmed vector in Stryker attack (Mar 2026).
Behavioral Pattern	Azure AD / Entra login page defacement	Handala logo placed on Entra ID login pages post-compromise as a public-facing impact indicator.
Behavioral Pattern	"Gaza Hackers Team Handala Machine" string	Do-not-run hostname string in wiper code path; useful for hunting sandbox/analyst evasion logic in samples. (Trellix, 2024)
C2 Channel	t.me/handala_hack8	Primary Handala Telegram channel for C2, data leak announcements, and propaganda.
Telegram Bot Token	6428401585:AAGE6SbwtVJxOpLjdMcrL45gb18H9UV7tQA	Bot token used in C2 for Operation HamsaUpdate. (Intezer, 2023)
Telegram Chat ID	6932028002	Chat ID associated with Operation HamsaUpdate C2. (Intezer, 2023)

© 2026 Critical Start. All rights reserved.

Indicator Type	Value	Context / Source
Telegram Bot Token	7277950797:AAF99Nw5rAT1BHnMmwY_tQNYJFU3dYJ5RHc	Bot token identified in 2024 wiper campaign. (Trellix, 2024)
Telegram Chat ID	7436061126	Chat ID associated with 2024 wiper campaign. (Trellix, 2024)

© 2026 Critical Start. All rights reserved.