Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

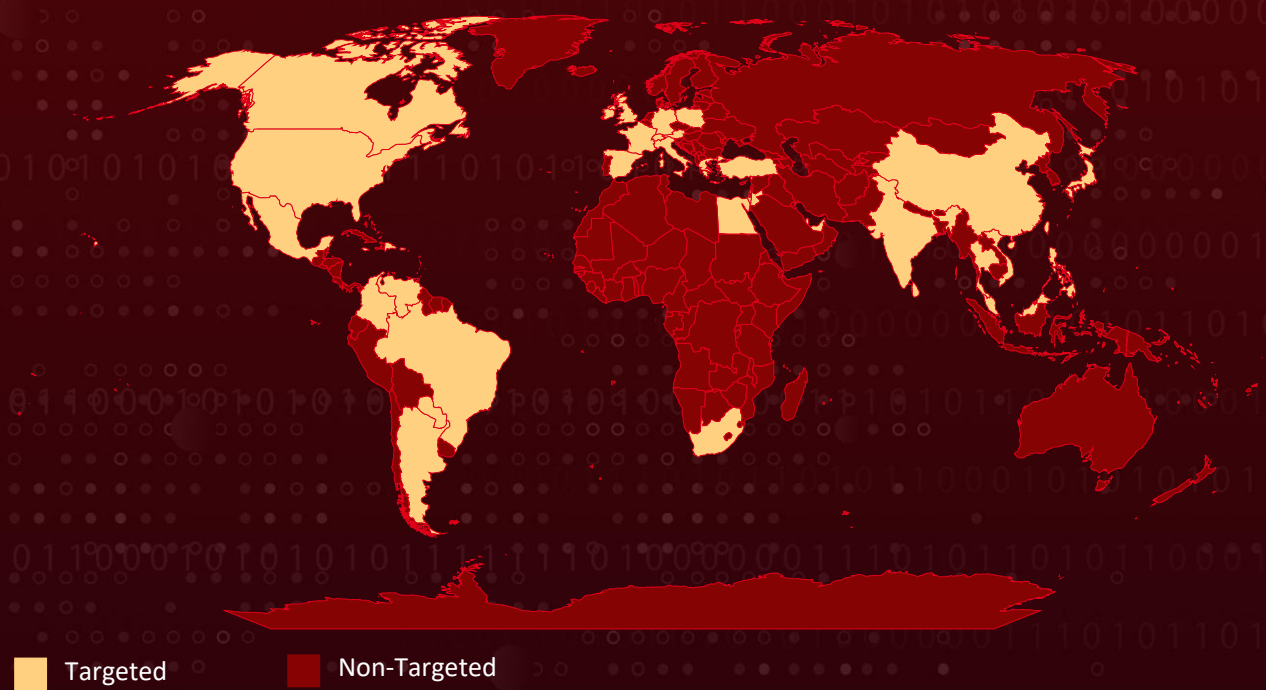
PAYLOAD Ransomware Emerges as a Fast-Growing Extortion Threat

Date of Publication	Admiralty Code	TA Number
September 25, 2026	A1	TA2026282

Summary

First Seen: February 15, 2026
Targeted Regions: Argentina, Austria, Bahrain, Brazil, Canada, China, Colombia, Dominican Republic, Egypt, France, Germany, Greece, India, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Malaysia, Mexico, Paraguay, Philippines, Poland, Puerto Rico, Qatar, Singapore, South Africa, Spain, Sri Lanka, Switzerland, Taiwan, Thailand, Turkey, United Arab Emirates, United Kingdom, United States, Venezuela, Vietnam
Targeted Products: Microsoft Active Directory (Group Policy), Fortinet FortiGate SSL VPN, VMware ESXi
Targeted Industries: Agriculture, Aviation, Business Services & Consulting, Construction, E-Commerce, Education, Energy, Engineering, Financial Services, Food & Beverage, Government, Healthcare, Hospitality, Insurance, Legal, Logistics, Manufacturing, Media, Professional Services, Real Estate, Retail, Technology, Telecommunications, Transportation, Utilities
Malware: PAYLOAD ransomware
Attack: PAYLOAD is a ransomware and data extortion operation that surfaced in February 2026 and quickly listed around 50 victims on its Tor leak site. In an intrusion against a Middle Eastern manufacturer, operators holding domain admin rights skipped the encryptor altogether, abused a FortiGate SSL VPN login with stolen credentials, and pushed malicious Group Policy Objects domain-wide to drop ransom notes, deface screens, disable the firewall, and lock out local administrators, while stealing data from file servers for publication.

Attack Regions



Attack Details

#1

PAYLOAD is a ransomware and data extortion group that first appeared on February 15, 2026. By late March 2026, it had posted about 50 victims on its leak site. Most were in Egypt and the wider Middle East and North Africa region, with others in Mexico, Poland, and elsewhere. Victims span the logistics, transportation, real estate, construction, manufacturing, professional services, and technology sectors.

#2

In April 2026, the group breached a manufacturing company in the Middle East by logging into its FortiGate SSL VPN with a stolen employee account. It is unclear how the attackers obtained the password; it may have come from password guessing, phishing, or a purchase on criminal markets.

#3

With administrator rights over the whole domain, the attackers used Group Policy, the built-in Windows tool for managing settings across a company's computers, to push malicious changes to every connected system at once. These changes dropped ransom notes, displayed a ransom message at login, replaced desktop and lock screen images, turned off the Windows Firewall, and disabled the local administrator account. The changes took effect the next day, when most computers restarted. Because the settings reapplied on every restart, they stayed in place without any malware on the machines. No files were encrypted in this attack. Instead, the attackers stole data from file servers and other systems and later published it online.

#4

When the group deploys its Windows ransomware, the program first stops dozens of applications and services, including databases, Office programs, email clients, backup tools, and security software, so that files are unlocked for encryption and are harder to recover. It deletes Windows backup snapshots, hides its activity from security monitoring, and can spread to shared network drives, allowing a single infected machine to affect files across the network.

#5

The ransomware locks each file with a unique encryption key, so files cannot be recovered without the attackers' key, and adds the .payload extension to each file name. It then leaves a ransom note, wipes Windows event logs to hide its tracks, and can delete itself. The note gives victims 72 hours to make contact and threatens to publish stolen data after 10 days. Whether or not files are encrypted, stealing data and threatening to leak it is how the group pressures victims to pay.

Recommendations

Remove Malicious PAYLOAD and Firewall GPOs: Search Group Policy for objects named "PAYLOAD" or "win Firewall Off", or matching the GUIDs listed in this advisory, delete them from domain controllers, and remove their links from the domain root and any OUs.

Clean SYSVOL of Staged Artifacts: Inspect SYSVOL for unexpected files such as payload.jpg and hello.txt, remove them, and confirm that replication has cleared them from every domain controller.

Restore Endpoint Security Settings: Force a Group Policy refresh after removing the malicious GPOs, re-enable Windows Firewall on all profiles, restore the legitimate state of the local Administrator account, and reset legal notice, wallpaper, and lock screen settings.

Reset Compromised and Privileged Credentials: Reset the credential used for VPN access along with all domain admin and GPO-capable accounts, and reset the KRBTGT password twice if broader domain compromise is suspected.

Audit Directory Service Changes: Enable auditing for Event IDs 5136, 5137, and 5141, and alert on new GPO creation and gPLink changes, especially links at the domain root outside approved change windows.

Separate GPO Creation from Linking Rights: Restrict who can create GPOs and who can link them, and require change approval for any policy linked at the domain level.

Harden ESXi Hosts: Restrict ESXi management access to dedicated admin networks, monitor for changes to hypervisor security policies, and keep hosts at supported, patched versions.

Protect Backups from Tampering: Keep offline or immutable backups isolated from domain credentials, and regularly test restores so recovery does not depend on shadow copies or reachable backup services.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	
	T1133: External Remote Services	
Privilege Escalation	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
Defense Evasion	T1686: Disable or Modify System Firewall	
	T1562: Impair Defenses	T1562.006: Indicator Blocking
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1480: Execution Guardrails	T1480.002: Mutual Exclusion
Execution	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
	T1106: Native API	
Discovery	T1083: File and Directory Discovery	
	T1135: Network Share Discovery	
Collection	T1005: Data from Local System	
Command and Control	T1071: Application Layer Protocol	

Tactic	Technique	Sub-technique
Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1489: Service Stop	
	T1491: Defacement	T1491.001: Internal Defacement
	T1531: Account Access Removal	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1CA67AF90400EE6CBBD42175293274A0F5DC05315096CB2E214E4BFE12FFB71F
SHA1	DDE1B933AAD33C5D96C2E45AD46434A200DC46A6
MD5	E0FD8FF6D39E4C11BDAF860C35FD8DC0, 0108656A3E1ADE6CA4F21B084F5E1208, BEA5E267F24D7DA59F6821BFFDBFF293
IPv4	37[.]19[.]210[.]12, 146[.]70[.]117[.]239, 149[.]102[.]229[.]154, 104[.]164[.]55[.]46, 104[.]28[.]162[.]228, 104[.]28[.]163[.]162, 64[.]190[.]76[.]14, 192[.]42[.]116[.]50, 192[.]42[.]116[.]12, 192[.]42[.]116[.]56, 192[.]42[.]116[.]97, 192[.]42[.]116[.]52
Filename	killer.exe, kill.exe, payload.jpg, hello.txt, README-payload.txt, RECOVER_payload.txt
Mutex	MakeAmericaGreatAgain

TYPE	VALUE
TOR Address	payloadrz5yw227brtbvdqpnlhq3rdcdekdnn3rgucbcdeawq2v6vuyd[.]onion, payload6eualw6kni6v2lqn7ovjcl76ojx25z5unsyvqo3lbqy3bo5qd[.]onion, payloadynyvabjacbun4uwhmxc7yvdzorycslzmnleguxjn7glahsvqd[.]onion
Registry Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\legalnoticecaption, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\legalnoticetext
GPO GUID	{C897F2C7-C2AC-4E6F-BF48-58036FF29E79}, {22099AD2-E062-4F56-B574-5099BBA4E7A6}
File Extension	.payload

Recent Breaches

https://qualiflex-solutions.ch
https://zaraholding.com
https://stuecheli.ch
https://baya-tech.com
https://bb-hydraulik.de
https://kronenberg-gmbh.de
https://ckr.co.za
https://roofinox.com
https://castries.fr
https://velafilmsrl.com
https://tofutown.com
https://www.mosaic-partners.com
https://clinicalasabana.com
https://softwarearge.com
https://qualiflex.ch
https://vitale.com.br
https://preferred-properties.org
https://www.myenb.ch
https://sporton.com.tw
https://myipo.gov.my
https://plazalama.com.do
https://vpd.attanahotels.com
https://hansoll.com
https://asonic-logistics.com
https://www.gtf-freese.de
https://robinsons.com.sg
https://impcullman.com
https://hs1992.jp
https://www.elohimlaw.com
https://tangsengservices.com
https://goreycs.ie

https://amemanufacturing.com.my
https://ros-management.com
https://rmgimli.com
https://b3-bruck.at
https://meditron.com.ve
https://pstbn.com.py
https://caravaningcity.com
https://betterhouse-eg.com
https://johinvestments.com
https://alsulaitilawfirm.com
https://www.marino.co.in
https://sunlightair.ph
https://www.orientalweavers.com
https://www.tfegroup.com.hk
https://franziskusschule-wilhelmshaven.de
https://wastani.com.eg
https://tscherne.at
https://uf-eg.com
https://www.sayegh1944.com
https://www.nkartravelhouse.com
https://q2als.com
https://aaagroup.com
https://www.carlysle.net
https://vancompare.com
https://www.igls.net
https://www.hoppecke.com
https://tslines.com
https://notaria89nl.com
https://lucky-mfg.com
https://www.royalbahrainhospital.com
https://tylermedia.com
https://riograndepr.net
https://www.thaisolarenergy.com
https://www.unitedlimsun.com
https://www.easyservizi.com
https://www.prizmpain.com
https://insacor.com.ar
https://jtpackoffoods.com
https://afdrd.com
https://sodic.com
https://gridff.com
https://adfsa.com.mx

References

https://securelist.com/tr/payload-ransomware-via-group-policy/121335/

https://darkatlas.io/blog/behind-payload-in-depth-technical-analysis-of-payload-ransomware

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 25, 2026 • 2:00 AM

More at www.hivepro.com