Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

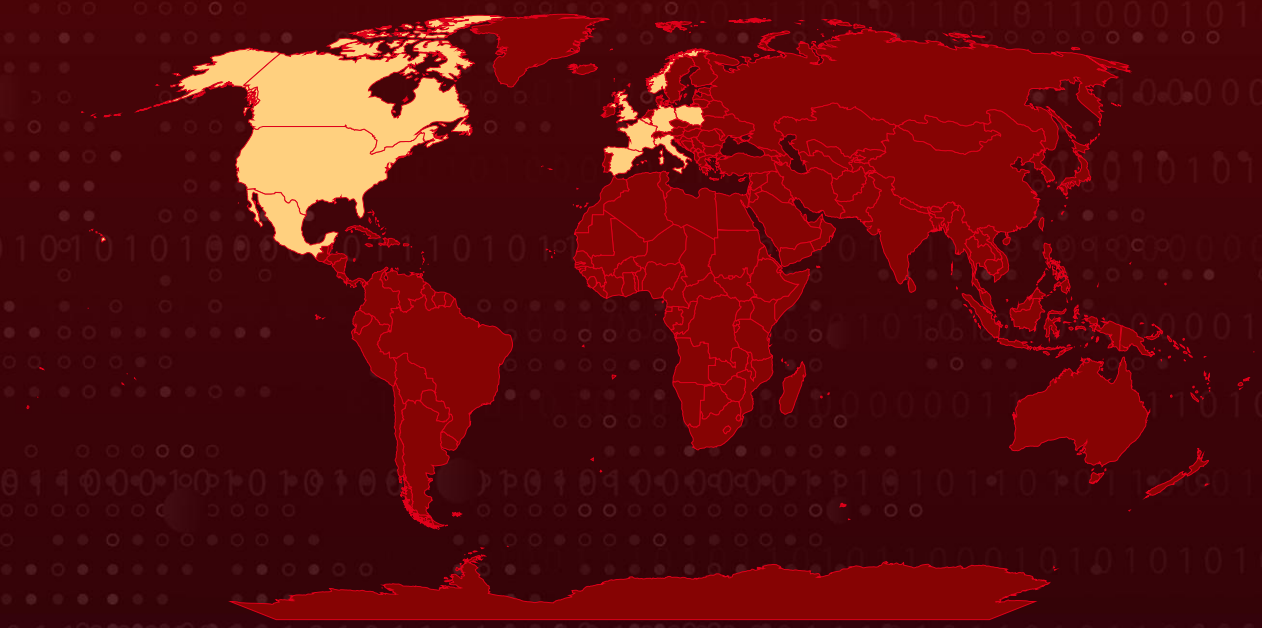
Payouts King Ransomware Blending In Before Breaking Through

Date of Publication	Admiralty Code	TA Number
April 17, 2026	A1	TA2026104

Summary

First Seen: April 2025
Targeted Regions: United States, Germany, Canada, France, Italy, Spain, United Kingdom, Norway, Mexico, Poland, Belgium
Targeted Platforms: Microsoft Windows
Targeted Products: Microsoft Teams, Quick Assist (legitimate tools abused for initial access)
Targeted Industries: Healthcare, Manufacturing, Construction, Mechanical, Education, Agriculture, Food and Beverage, Telecommunications, Energy, Maritime and Shipping, Hospitality and Restaurants, Logistics, Technology, Business Services & Consulting, Transportation, Retail, Financial Services, Real Estate, Government, Pharmaceutical
Malware: Payouts King Ransomware
Attack: Payouts King is a ransomware operation that emerged in April 2025 and has been linked with high confidence to former BlackBasta initial access brokers, with attack activity intensifying in early 2026. The operation gains initial access through spam-bombing combined with vishing, in which threat actors flood victims' inboxes with emails and then impersonate internal IT staff on Microsoft Teams to convince users to launch Quick Assist and grant remote control. After establishing a foothold, the ransomware leverages obfuscated command-line arguments, scheduled task persistence, SYSTEM-level privilege elevation, and direct system call invocation to terminate antivirus and EDR processes.

Attack Regions



Attack Details

#1

Payouts King is a little-known ransomware group first observed in April 2025. It combines data theft with targeted file encryption, using pressure and precision rather than wide, noisy attacks. Its operations begin with a calculated social engineering scheme designed to overwhelm and mislead. The attack starts with spam bombing flooding a victim's inbox to create urgency and confusion. Shortly after, the attacker poses as an internal IT staff member and urges the target to join a Microsoft Teams call. During the call, the victim is guided to open Quick Assist, a legitimate remote support tool. Once access is granted, the attacker takes control of the system and installs the ransomware, securing a foothold within the network.

#2

Before activating, the malware checks for specific conditions to avoid detection in testing environments. If these checks pass, it quietly prepares itself by decoding hidden instructions and linking to essential Windows functions. It then establishes persistence by creating a hidden scheduled task that runs with full system privileges at startup, ensuring continued access even after reboots.

#3

To expand its reach, the ransomware can focus on local files, network shares, or both. It uses elevated privileges to move across systems, especially when higher-level credentials are available. At the same time, it scans active processes and shuts down known security tools, allowing it to operate without interference.

#4

Data theft plays a central role in the attack. Files are encrypted using strong cryptographic methods, with smaller or high-value files fully locked and larger files partially encrypted to save time while still causing disruption. The malware also removes backup copies, clears logs, and deletes recovery options to prevent restoration. Finally, a ransom note is placed on the system, directing victims to contact the attackers through encrypted messaging and visit a hidden website for negotiation. The message is clear: pay, or risk losing both your data and its confidentiality.

Recommendations

Restrict and Monitor Quick Assist Usage: Disable Quick Assist on systems that do not require it, restrict outbound Teams external federation where business needs allow, and configure detection rules that alert when `quickassist.exe` is launched following inbound Teams calls from unverified external tenants.

Hunt for the Mozilla Scheduled Task Persistence Markers: Build SIEM and EDR detections for the creation of scheduled tasks under the `\Mozilla\` path, specifically `\Mozilla\UpdateTask` and `\Mozilla\ElevateTask`, executed via `schtasks.exe` with `ONSTART` and SYSTEM run-as parameters, since these are hardcoded in the Payouts King binary.

Detect Direct System Call Abuse and EDR Tampering: Deploy behavioral detection capable of flagging unhooked syscall invocation patterns, processes attempting to terminate security tooling such as `MsMpEng.exe`, `MsSense.exe`, `SentinelAgent.exe`, `CSFalconService.exe`, or `cb.exe`, and unusual enumeration of `ntdll` exports indicative of dynamic syscall resolution.

Maintain Immutable, Offline, and Tested Backups: Ensure critical systems are protected by 3-2-1 backup architecture with immutable or air-gapped copies that cannot be reached through SMB shares or domain credentials, since Payouts King supports a `-mode share` flag designed to encrypt network shares; verify restoration procedures regularly through tabletop exercises.

Segment the Network and Restrict SMB Lateral Pathways: Apply micro-segmentation between user subnets, file servers, and domain controllers; restrict SMB traffic between workstations using host firewalls and minimize the number of users with write access to shared file repositories.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1585: Establish Accounts	T1585.002: Email Accounts
Initial Access	T1566: Phishing	T1566.004: Spearphishing Voice
		T1566.003: Spearphishing via Service
	T1199: Trusted Relationship	
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
	T1106: Native API	
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Defense Evasion	T1027: Obfuscated Files or Information	T1027.007: Dynamic API Resolution
		T1027.013: Encrypted/Encoded File
	T1140: Deobfuscate/Decode Files or Information	
	T1622: Debugger Evasion	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
	T1564: Hide Artifacts	T1564.003: Hidden Window
	T1218: System Binary Proxy Execution	

Tactic	Technique	Sub-technique
Defense Evasion	T1036: Masquerading	
Discovery	T1057: Process Discovery	
	T1083: File and Directory Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
Lateral Movement	T1021: Remote Services	T1021.002: SMB/Windows Admin Shares
Command and Control	T1219: Remote Access Software	
Exfiltration	T1567: Exfiltration Over Web Service	
Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	335ad12a950f885073acdfebb250c93fb28ca3f374bbba5189986d9234dcbff4, d68ce82e82801cd487f9cd2d24f7b30e353cafd0704dcdf0bb8f12822d4227c2
TOR	payoutsgn7cy6uliwevdqspncjpfxpmzgirwl2au65la7rfs5x3qnbqd[.]onion, v2mw3spxqhggig5zjd6tjnfamwntrprreij3dq77jlq74dduyjafeead[.]onion, c6nrwsloenpiat7zilh243nvhe7a3edsfm3ct3kpxhu2fv7z36ksjcad[.]onion
Tox ID	535F403A2EA2DC71A392E18D7DB77FEF70845C0B7E5B9114CD30D301870304379C3547E324E2, E37F4D443B7FECE0E9775E82D6DC3B304890F80BA03F5101DFD43B2C249AD625CF00EC8B57D4
Encrypted File Extension	.ZWIAAW
Backup File Extension	.esVnyj
Ransom Note Filename	readme_locker.txt

Recent Breaches

https://www.tessco.com/
https://grace-design.com/
https://www.blanchard.com/
https://www.cng-inc.com/
https://www.powell.com/
https://www.grantpts.com/
https://www.sofinter.it/
https://www.kichler.com/
https://www.delmontefoods.com/
https://www.lcindustries.com/
https://eyemartexpress.com/
https://www.peachtreegroup.com/
https://ufpt.com/
https://esentiaenergy.com/
https://www.praterengineering.com/
https://www.bay-ship.com/
https://www.telia.no/
https://vortexcompanies.com/
https://www.bhid.co.uk/
https://vfraas.com/
https://www.ashandlacy.com/
https://caunton.co.uk/
https://www.rameder.de/
https://www.baer-cargolift.com/
https://chemirol.com.pl/
https://www.soapeople.com/
https://visionwheel.com/
https://www.jjwhiteinc.com/
https://www.vereinigte-stadtwerke.de/
https://www.lithographix.com/
https://www.klueber-elektro.de/
https://accordcarton.com/
https://www.irwincar.com/
https://timeequities.com/
https://linxxglobal.com/
https://www.montereymushrooms.com/
https://www.sofofoods.com/
https://www.creditinfo.com/

https://www.medialab3dsolutions.com/
https://thompsonhanson.com/
https://schlemmer.com/home
https://www.cr-architects.com/
https://www.beplastics.com/
https://kolbus.com/de/
https://bariatrix.com/
https://www.arch-con.com/
https://www.silentgliss.it/itit/
https://crenshawcommunityhospital.com/
https://gatewaycommunity.com/
https://www.ice.edu/
https://praterengineering.com
https://accordcarton.com
https://klueber-elektro.de
https://lithographix.com
https://irwincar.com
https://kolbus.de
https://bariatrix.com
https://medialab3dsolutions.com
https://timeequities.com
https://linxxglobal.com
https://montereymushrooms.com
https://sofofoods.com
https://creditinfo.com
https://thompsonhanson.com
https://schlemmer.com

References

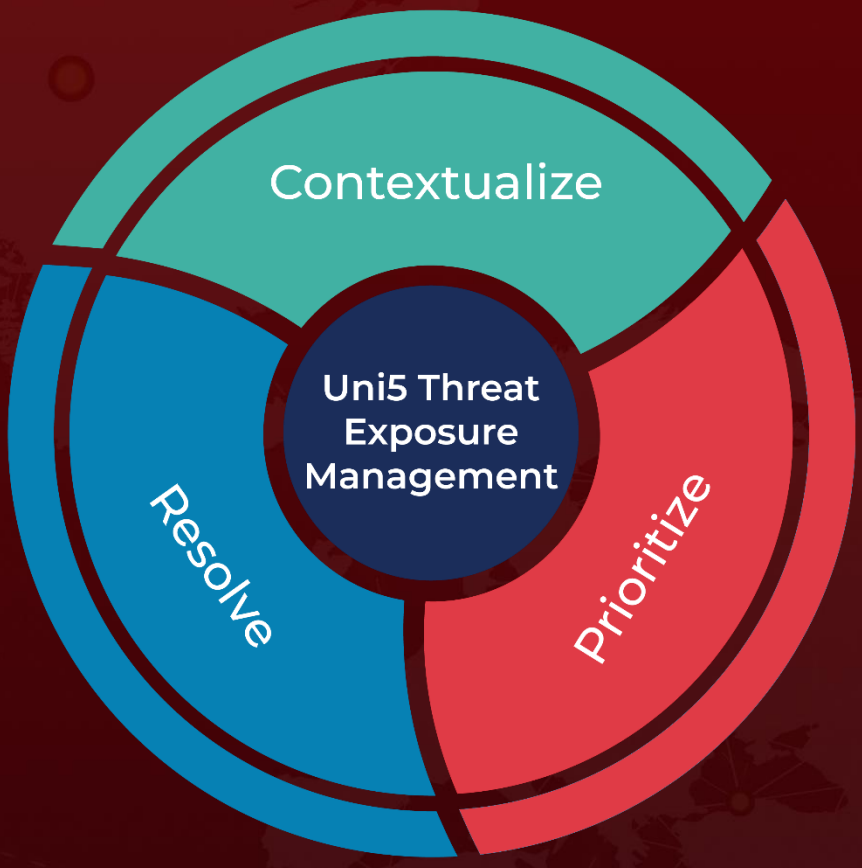
https://www.zscaler.com/blogs/security-research/payouts-king-takes-aim-ransomware-throne

https://hivepro.com/threat-advisory/black-bastas-evolution-sophisticated-social-engineering-meets-advanced-payloads/

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 17, 2026 • 07:00 AM

More at www.hivepro.com