Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

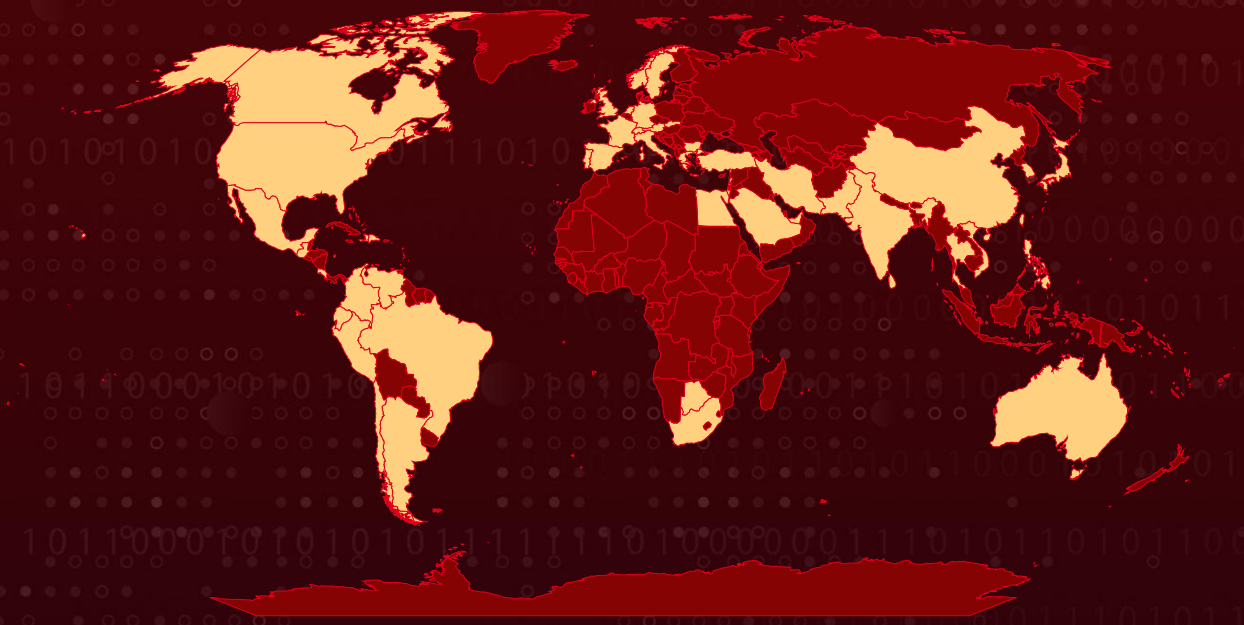
DragonForce Evolves: Teams-Relayed C2 and BYOVD Kernel Evasion

Date of Publication	Admiralty Code	TA Number
September 25, 2026	A1	TA2026284

Summary

First Seen: December 2023
Targeted Regions: Taiwan, United States, France, United Kingdom, Dominican Republic, Portugal, Argentina, Brazil, Haiti, South Korea, China, Thailand, Germany, Colombia, Egypt, Canada, Botswana, Bahrain, South Africa, Switzerland, United Arab Emirates, India, Italy, Philippines, Ecuador, Saudi Arabia, Australia, Chile, Pakistan, Japan, Turkey, Sweden, Lebanon, Mexico, Sri Lanka, Peru, Netherlands, Israel, Spain, Austria, Singapore, Isle of Man, Greece, Norway, Vietnam, Guatemala, Slovakia, Iran, Costa Rica, Bulgaria, Venezuela
Targeted Platform: Windows
Targeted Industries: Aerospace, Defense, Agriculture, Associations, Aviation, Business Services & Consulting, Casino & Gambling, Charitable Organizations, Education, Energy, Financial Services, Food Service, Government, Healthcare, Hospitality, Insurance, Legal, Manufacturing, Media, Pharmaceutical, Real Estate, Religion, Retail, Technology, Telecommunications, Transportation
Malware: DragonForce Ransomware
Attack: DragonForce has evolved into a mature ransomware cartel, rebranding in March 2025 to let affiliates operate under their own brands on its LockBit/Conti-based infrastructure. In a late-2025 intrusion it debuted Backdoor.Turn, a Go-based backdoor that hides C2 inside legitimate Microsoft Teams TURN-relay traffic, the first known in-the-wild abuse of its kind, alongside multi-vector BYOVD driver exploitation for kernel-level defense evasion. Its Windows locker uses ChaCha8 encryption with RSA-4096 key wrapping and network-aware SMB-share encryption, marking a clear shift toward stealthy, high-impact targeted campaigns.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-52271	Topaz Antifraud Improper Access Control Vulnerability	Topaz Antifraud (wsftprm.sys driver)	✗	✗	✓
CVE-2025-61155	Hotta Studio GameDriver X64 Improper Access Control Vulnerability	Tower of Fantasy (Gamedriver x64.sys driver)	✗	✗	✗
CVE-2025-1055	K7 Computing K7 Security Anti-Malware Missing Authorization Vulnerability	K7 Security (K7RKScan.sys driver)	✗	✗	✓

Attack Details

#1

DragonForce has matured from a conventional ransomware brand into one of the most capable and organizationally mature operations active today. Its payloads are built on leaked LockBit 3.0 and Conti code, and a RaaS program formalized in mid-2024 offered affiliates up to 80% of ransom proceeds. On March 19, 2025, it rebranded as the "DragonForce Ransomware Cartel," letting affiliates operate under their own brands using its infrastructure and tools. Within 24 hours it defaced the BlackLock and Mamona leak sites, and it subsequently absorbed RansomHub's orphaned affiliates.

#2 The most significant technical upgrade appeared in an intrusion against a major U.S. services firm, where operators gained access in December 2025 and remained for one to two months. They deployed Backdoor.Turn, a custom Go-based backdoor that obtains an anonymous Teams visitor token through Skype-backed identity services, sets up its connection via a legitimate Microsoft TURN relay, then runs a QUIC session to the real C2, so defenders see only outbound traffic to genuine Teams servers. This is the first known in-the-wild abuse of TURN relays for this purpose.

#3 Defense evasion advanced through multi-vector BYOVD abuse combining three signed vulnerable drivers (CVE-2023-52271, CVE-2025-61155, CVE-2025-1055) with a novel "Havoc Process Terminator" technique exploiting Huawei's HWAuidoOs2Ec.sys, a driver not previously known to be exploited in the wild. Separately, they used a custom malicious driver masquerading as a Palo Alto component. The goal throughout was kernel access to terminate security processes.

#4 The Windows locker pairs per-file ChaCha8 encryption with RSA-4096 key wrapping and appends a fixed 537-byte metadata footer. It scans private IP ranges and TCP/445, then encrypts reachable SMB shares under the current token, skipping only the ADMIN$ share. Together, these upgrades, stealthy C2, novel driver abuse, and a cartel-style affiliate model, mark a deliberate move toward high-impact, resource-heavy, targeted campaigns.

Recommendations

Restrict and Monitor SMB Reach: Immediately segment storage networks, minimize writable share access, and monitor for TCP/445 fan-out, NetShareEnum enumeration, and bulk remote writes, since a single privileged token can encrypt many reachable shares even without worm-like propagation.

Hunt for `.df_win` and the Fixed Footer: Deploy detection for files renamed with the `.df_win` extension and for the deterministic 537-byte recovery footer appended to encrypted files, both of which are durable artifacts independent of builder-configured indicators.

Block Known Command-and-Control Infrastructure: Block the identified downloader command-and-control domains, the Backdoor.Turn C&C IP, and the malicious archive download URL at the network perimeter, and hunt historical logs for connections to them.

Enforce Vulnerable Driver Blocklisting: Enable Microsoft's vulnerable-driver blocklist and application-control policies to prevent loading of the abused signed drivers (wsftprm.sys, Gamedriverx64.sys, K7RKScan.sys, HWAuidoOs2Ec.sys) and the impersonating Palo Alto driver used for kernel-level defense evasion.

Protect Shadow Copies and Recovery Paths: Monitor WMI and WMIC calls that enumerate and delete Win32_ShadowCopy objects, restrict the accounts able to remove volume shadow copies, and maintain offline, immutable backups outside the reach of the current security token.

Harden Internet-Facing Database Servers: Prioritize patching, credential hygiene, and exposure reduction for SQL and MSSQL servers, the assessed initial-access surface, and place them behind restrictive network controls.

Inspect Anomalous Microsoft Teams Traffic: Because the backdoor hides command-and-control inside legitimate Teams TURN-relay traffic, baseline expected Teams connectivity and investigate anonymous Teams visitor-token requests or QUIC sessions that do not correspond to genuine user conferencing activity.

Maintain Offline, Tested Backups: Keep immutable or offline backups and rehearse restoration, since the operation still threatens encryption under its double-extortion model.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	
Execution	T1047: Windows Management Instrumentation	
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
Persistence	T1136: Create Account	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
	T1027: Obfuscated Files or Information	
	T1112: Modify Registry	
Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers

Tactic	Technique	Sub-technique
Credential Access	T1003: OS Credential Dumping	
Discovery	T1046: Network Service Discovery	
	T1135: Network Share Discovery	
	T1018: Remote System Discovery	
	T1087: Account Discovery	T1087.002: Domain Account
Lateral Movement	T1021: Remote Services	
Command and Control	T1090: Proxy	
	T1102: Web Service	
	T1071: Application Layer Protocol	
Exfiltration	T1048: Exfiltration Over Alternative Protocol	
Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1489: Service Stop	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	82b37a92589dfd4d67ca87eb9e52ac8e682e8e60d2211f59074cd5ccc693013b, 821da79d727351dd67ce5df7950e9a3de6647a3cf474bb3a093f67507fed92a6, b6628d201c2a68d2a3de2a87de7a5acfe21b101a97928e1c8d5c82102d967383, ce66b8221446c9b6d83f0ce6382f430e519601641e5daaaf1ca7a8a8806cb0b0, f174c19902523dcf005fa044b6598403a5e5c0a5982398d1bc0dcc5ec1cd351b, 142bac0e2148e0d47891b6cd7311195c4acbe33b700fad54a201c52a2bc46219, 8395b621bb4415090f232c59fc41d24ea41a519b58eabe512f3ae7d2fdf049a3, 9335f61f8ad276d94455c5b6876fea48152c3cea759f2598c8108ee461fa5759, cd078957167e1af4de39aecdb981cd14156fa81d5a9c6ac51e74ae5b6199a12a, b16e217cdca19e00c1b68bdfb28ead53b20adeabd6edcd91542f9fbf48942877, d20a3c928761fe00ac522eeb474612b5804cd9108453ea8591106d5d4428428e, 8284c8676cc22c4b2e66826ac16986da7ddecba1f2776b16771be17bfdc45dc2, 65ab49119c845801f29a57e8aa177146b2ffbd289d4278109b146f933380f951, 6bbf10bcbef7ac5102b54c81137859891a3802dbacd888be90f990d50e18b0b4, 252a8bb2eb9c96c5e6cc7cab822e2ed0d508032f9350351221781684e86c03ab, 8a4033425d36cd99fe23e6faef9764fbf555f362ebdb5b72379342fbbe4c5531, e45b18c93d187aac5c4486f57483bc87580e15def82a312bfb377ff16eb96b22

TYPE	VALUE
SHA256	087f002df0a02c8c74f3ba5cd99cf29fb9efff38bf57b3d808e34a5dd4200dd2, 048e18416177de2ead251abdf4d89837f6807c6aba4d5b1debe49adfdecbf05c, 6f9fbe29f8cc2788e2bc9d631e0eea2a8e9837076837b55838005a0e654f0a9e, d0da2832ae1e13a98f7ce7e33a66c1b0d9797b81f69ece134e4462ea55ac923e, aea26980059ef2ad11e99556a4edfa1f8ec769fa9f06aa573b81bedf319954b5, a4eb9be98d00c961ad8c3329ee80690c1eec98d4c8fa8dd91c371d9ecc451581
SHA1	55acb53f348c9f6b89343dc8d96522aa75e4cfdb
MD5	bd47ae24b03e5ba0f1ab2e95e7acb989
Domains	projetosmecanicos[.]com[.]br, socialbizsolutions[.]com, professionalhomebasedbusiness[.]com, safefire[.]jo, glanz-gmbh[.]de, turnkeyaiagents[.]com, comunidadesparentais[.]com[.]br, mysimerp[.]net
IPv4	62[.]164[.]177[.]25
URL	hxxp[:]//192[.]36[.]27[.]51/TechSupV18Fix3[.]zip

TYPE	VALUE
Filename	vboxrt.dll, DbgView64.exe, readme.txt, HWAuidoOs2Ec.sys, wsftprm.sys, Gamedriverx64.sys, K7RKScan.sys, truesight.sys, rentdrv2.sys, TechSupV18Fix3.zip
File Path	C:\Users\Public\log.log
Mutex	hsfjuukjzloqu28oajh727190
Tox ID	1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20
TOR Address	3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd[.]onion, z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion

Patch Details

CVE-2023-52271: Topaz Antifraud (wsftprm.sys) - Fixed in version above 2.0.0.0.

CVE-2025-1055: K7 Security Anti-Malware (K7RKScan.sys) - Fixed in version 23.0.0.10 or later.

Recent Breaches

https://www.hec-group.com.tw
https://www.arizonavascular.com
https://www.pjemetal.com
https://www.polyresine.com
https://www.communitypropertymanagement.com
https://www.owenleighoptometry.co.uk
https://www.medicaldepartmentstore.com
https://www.norwoodlegal.com
https://www.homewoodsales.com
https://www.arsrenacer.com
https://www.frato.com
https://www.winfashion.com
https://www.brookviewfinancial.com
https://www.wozair.com
https://www.criba.com.ar
https://www.hoganomidi.com
https://www.rdmachine.com
https://www.vermont.com.br
https://www.rubbermill.com
https://www.gbgroup.com

References

https://www.security.com/threat-intelligence/dragonforce-msteams-backdoor

https://blog.barracuda.com/2025/06/09/dragonforce-ransomware-cartel-vs--everybody

https://darkatlas.io/blog/dragonforce-ransomware-analysis-windows-locker

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 • 08:30 AM

More at www.hivepro.com