ZEROFOX INTELLIGENCE

Flash

DragonForce Conceals C2 in Legitimate Relay Infrastructure

F-2026-06-19b

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Ransomware, Threat Actor, Malware

June 19, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 10:00 AM (EDT) on June 19, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | DragonForce Conceals C2 in Legitimate Relay Infrastructure

| Key Findings

- On June 16, 2026, cybersecurity researchers disclosed a December 2025 intrusion at a major U.S. services firm in which operators from the DragonForce ransomware collective deployed a custom backdoor called Backdoor.Turn into the firm's enterprise collaboration infrastructure.
- Backdoor.Turn is a previously unseen in the wild Go-based remote access trojan (RAT) that can be injected into legitimate trusted collaboration instances to avoid detection. DragonForce almost certainly used this RAT to establish a command-and-control (C2) node within the trusted U.S. services firm's network in order to maintain persistence.
- ZeroFox assesses that abusing trusted, widely deployed collaboration services for C2, exfiltration, and malware delivery is very likely a tradecraft trend that has evolved since at least mid-2025. This likely represents a further maturation of the ransomware-as-a-service (RaaS) ecosystem, which almost certainly increases detection difficulties for defenders relying primarily on network egress monitoring.
- This type of intrusion also likely represents a continuing shift from single-event extortion toward dual monetization: initial encryption and data theft followed by

durable access that can be exploited later or sold to other criminal operators on deep and dark web (DDW) forums.

Details

On June 16, 2026, cybersecurity researchers disclosed a December 2025 intrusion at a major U.S. services firm in which operators from the DragonForce ransomware collective deployed a previously unseen in the wild custom backdoor called RAT Backdoor.Turn into the firm's Microsoft Teams instance.[1] The threat actor almost certainly maintained access to the victim network for one to two months before detection.

- The specific entry method is unknown at this time, however, there is a roughly even chance the threat actor purchased access from an initial access broker (IAB).
- This breach is an abuse of the platform's trust model and does not represent a vulnerability in Microsoft Teams.[2]

Backdoor.Turn is a Go-based RAT that can be injected into legitimate trusted collaboration instances to avoid detection. Its capabilities include remote command execution and process creation, network scanning, TLS certificate collection, LDAP and Active Directory enumeration, browser credential theft, and credential-based lateral movement.[3][4] Once deployed, the RAT is almost certainly used to establish a C2 node, from which DragonForce can manage other attack activities.

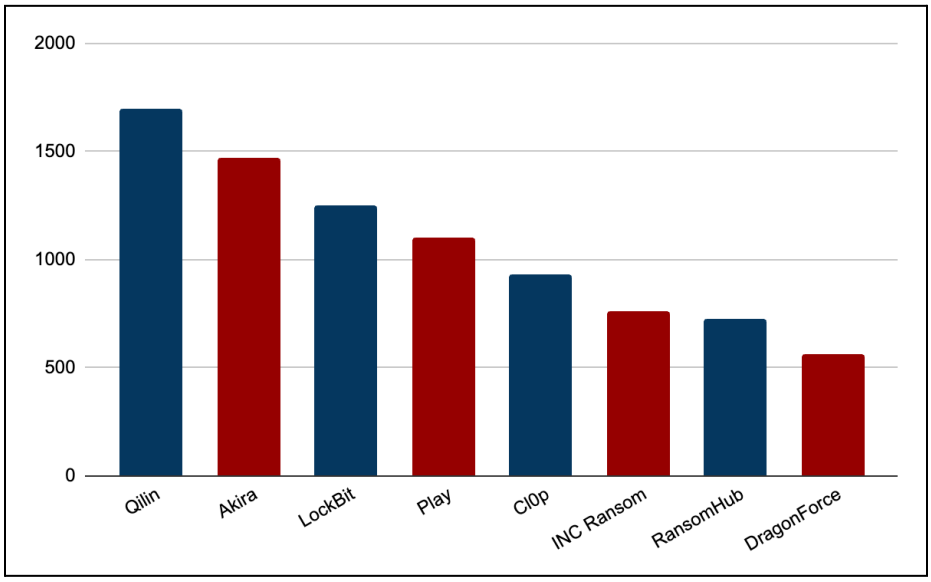
The malware first obtained an anonymous Microsoft Teams visitor token from Microsoft's Skype-backed identity service, then used a legitimate Microsoft relay server to establish a connection, and finally ran a transport session that linked the infected host to an attacker-controlled server. From a network defender's perspective, the resulting traffic

[1] hXXps://www.bleepingcomputer[.]com/news/security/ransomware-gang-abuses-microsoft-teams-relays-to-hide-malicious-traffic/
[2] hXXps://www.praetorian[.]com/blog/ghost-calls-abusing-web-conferencing-for-covert-command-control-part-1-of-2/
[3] hXXps://www.security[.]com/threat-intelligence/dragonforce-msteams-backdoor
[4] hXXps://www.bleepingcomputer[.]com/news/security/ransomware-gang-abuses-microsoft-teams-relays-to-hide-malicious-traffic/

would be largely indistinguishable from normal Microsoft Teams relay activity.[5][6][7] For persistence and continued access, the operators modified the Windows "Limit Blank Password" policy to permit blank-password access, created new user accounts, and altered firewall rules to keep C2 communication reachable.[8]

Since its first attack in June 2023, DragonForce has conducted at least 560 attacks across all business sectors. This is half as many as Qilin, the most active collective over that same period.

- In May 2025, DragonForce claimed responsibility for the attacks on UK retail outlets Marks & Spencer (M&S), Co-Op, and Harrods, although it is likely the attacks were carried out by Scattered Spider using DragonForce ransomware.[9]
- While DragonForce uses affiliates to conduct attacks utilizing its infrastructure, it is likely that that the Backdoor.Turn RAT originated with DragonForce itself rather than with one of its affiliates.



Attacks by RaaS collectives since June 2023
Source: ZeroFox Intelligence

[5] hXXps://www.security[.]com/threat-intelligence/dragonforce-msteams-backdoor
[6] hXXps://www.helpnetsecurity[.]com/2026/06/16/dragonforce-microsoft-teams-malware-backdoor-turn/
[7] hXXps://cybersecuritynews[.]com/microsoft-teams-relay-abused/
[8] hXXps://www.security[.]com/threat-intelligence/dragonforce-msteams-backdoor
[9] hXXps://www.bbc[.]co[.]uk/news/articles/crkx3vy54nzo

It is almost certain that DragonForce routed C2 through the major U.S. services firm's Microsoft Teams relay infrastructure to defeat outbound-traffic heuristics, as the malicious sessions blend with legitimate traffic. ZeroFox assesses that abusing trusted, widely deployed collaboration services for C2, exfiltration, and malware delivery is very likely a tradecraft trend that has evolved since at least mid-2025 and likely represents a further maturation of the RaaS ecosystem; this almost certainly increases detection difficulties for defenders that rely primarily on network egress monitoring.

- In March 2026, threat actors linked to Iran's Ministry of Intelligence and Security (MOIS) routed their C2 through a Telegram API call during an operation targeting dissidents after the start of the U.S.-Israeli airstrikes against the Islamic Republic.[10]
- In February 2025, Russia-aligned threat actor Storm-2372 abused Teams meeting-invite lures and Microsoft's own device-code authentication flow to steal tokens without cracking multi-factor authentication (MFA).[11]

This likely also represents a continuing shift beyond single-event extortion toward dual monetization: initial encryption and data theft followed by durable access that can be exploited later or sold to other criminal operators on DDW forums. Since at least mid-2025, threat actors have increasingly developed methodologies for creating multiple revenue streams from single breach events.

- The Gentlemen RaaS collective used pre-existing stockpiles of accesses to extort at least 184 victims in Q1 2026. This was done in part by recruiting IABs on BreachForums.[12]
- In March 2025, the threat actor Medusa advertised stolen victim data for sale to third parties while the ransomware countdown was still ongoing—an example of one exfiltration generating two revenue streams. Medusa also created domain accounts on victim networks, very likely for persistence and to conduct post-payment re-extortion.

[10] hXXps://www.ic3[.]gov/CSA/2026/260320.pdf
[11] hXXps://www.microsoft[.]com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
[12] hXXps://www.microsoft[.]com/en-us/security/blog/2026/05/28/the-gentlemen-ransomware-dissecting-a-self-propagating-go-encryptor/

Throughout the remainder of 2026, it is almost certain that threat actors will continue to embed themselves in trusted, mainstream software-as-a-service (SaaS) platforms to maintain persistence and avoid detection. It is vital that both SaaS platforms and their clients establish effective tactics, techniques, and procedures (TTPs) to detect digital squatters in their sessions rather than relying on egress detection to discover attackers.

Additionally, it is very likely that the RaaS ecosystem will continue to expand the dual-monetization model of operations. As roughly 49 percent of ransomware victims do not opt to pay the ransom,[13] threat actors very likely view multiple revenue streams as a necessity in order to remain profitable in a highly competitive landscape.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant MFA, and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

[13] hXXps://cybersecurityventures[.]com/most-ransomware-victims-who-pay-up-dont-get-their-data-back/

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%