Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

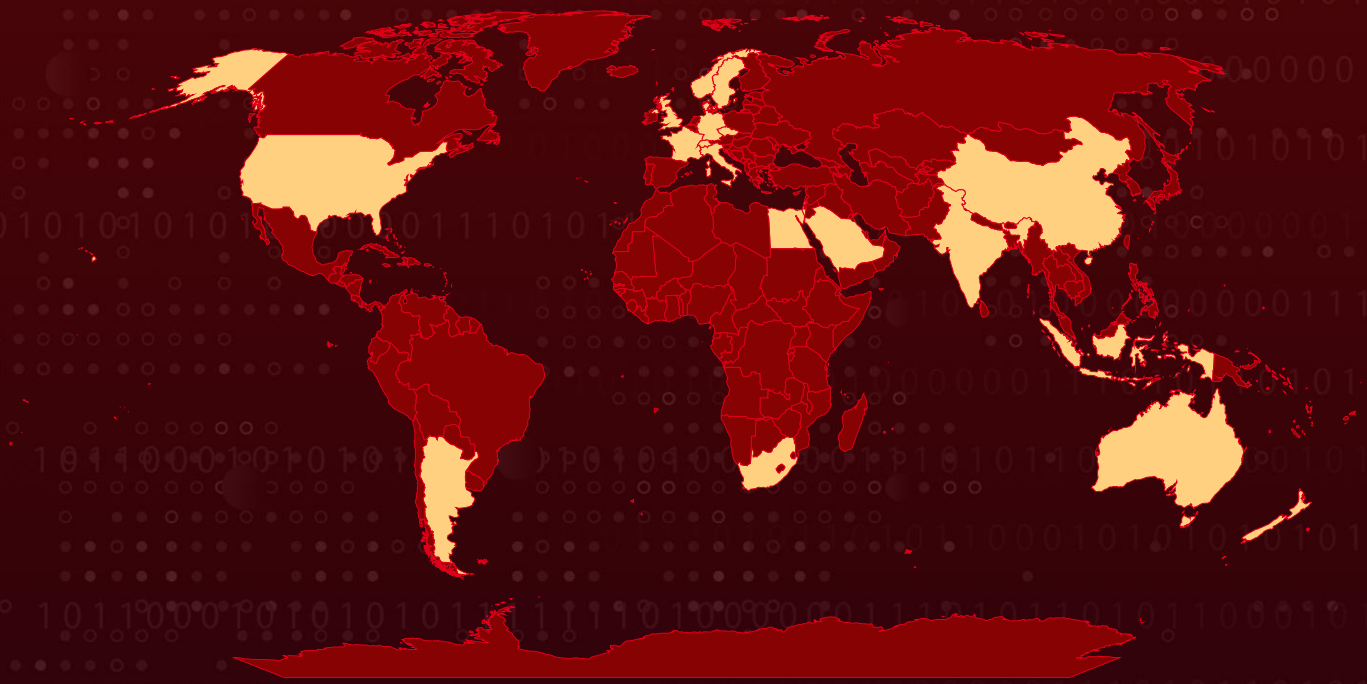
# DragonForce Is Selling DIY Ransomware Kits

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| May 9, 2025 | A1 | TA2025141 |

# Summary

**Active Since:** December 2023
**Malware:** DragonForce Ransomware
**Targeted Platforms:** Windows, Linux, ESXi, and NAS
**Targeted Industries:** Aerospace, Banking, Business Services & Consulting, Chemical, Construction, Defense, Education, Electronics, Energy, Financial Services, Food Service, Government, Healthcare, Insurance, Legal, Logistics, Manufacturing, Maritime, Media, Oil and Gas, Political, Professional Services, Real Estate, Retail, Technology, Telecommunications, Textiles, Transportation, Utilities
**Targeted Countries:** Argentina, Australia, China, Czech Republic, Denmark, Egypt, France, Germany, India, Indonesia, Israel, Italy, New Zealand, Norway, Saudi Arabia, Singapore, South Africa, Sweden, Switzerland, United Kingdom, United States
**Attack**: DragonForce burst onto the cybercrime scene in late 2023 and has rapidly evolved into a ruthless, hybrid ransomware group blending hacktivism with profit-driven extortion. Known for targeting retailers and government entities, the group lures affiliates with customizable ransomware kits, ready-made infrastructure, and a cutthroat business model. Leveraging phishing, credential stuffing, and high-profile exploits like Log4Shell, DragonForce operates a multi-extortion playbook - stealing data, threatening leaks, and crippling critical systems.

## Attack Regions



## CVEs

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2021-44228 | Log4shell (Apache Log4j2 Remote Code Execution Vulnerability) | Apache Log4j2 | ✓ | ✓ | ✓ |
| CVE-2023-46805 | Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability | Ivanti Connect Secure and Policy Secure | ✓ | ✓ | ✓ |
| CVE-2024-21412 | Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability | Microsoft Windows Internet Shortcut Files | ✓ | ✓ | ✓ |
| CVE-2024-21887 | Ivanti Connect Secure and Policy Secure Command Injection Vulnerability | Ivanti Connect Secure and Policy Secure | ✓ | ✓ | ✓ |
| CVE-2024-21893 | Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability | Pulse Connect Secure, ZTA gateways, Pulse Policy Secure | ✓ | ✓ | ✓ |
| CVE-2022-26134 | Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability | Atlassian Confluence Server and Data Center | ✓ | ✓ | ✓ |

# Attack Details

**#1**

Emerging in early December 2023, DragonForce quickly established itself within the cybercrime underworld. Originally known by their dark web data leak site DragonLeaks, the group has since rebranded and evolved into a formidable ransomware operation. By 2025, DragonForce had matured into a fully-fledged ransomware-as-a-service (RaaS) collective, with a business model specifically designed to attract displaced cybercriminals and freelance affiliates.

**#2** Offering a 20% revenue share lower than most RaaS offerings DragonForce compensates for this with enticing features. Affiliates receive white-label ransomware kits, allowing them to create distinct variants, compile their payloads, and customize ransom notes and file extensions. Additionally, they gain access to a ready-made infrastructure that includes negotiation tools, encrypted storage, and templated leak sites marketed under the brand RansomBay.

**#3** Their campaigns employ a multi-extortion strategy, combining data theft with the threat of public data leaks and reputational damage via their leak sites. The group typically achieves initial access through phishing campaigns, exploitation of known vulnerabilities, or by leveraging leaked and stolen credentials to breach internet-facing systems.

**#4** Over the years, they've actively exploited critical vulnerabilities such as Log4Shell in Apache Log4j2, as well as multiple flaws in Ivanti Connect Secure. Credential stuffing attacks targeting Remote Desktop Protocol (RDP) services and VPN portals using compromised username-password pairs remain a favored tactic.

**#5** Once inside a network, DragonForce operators deploy a suite of post-exploitation tools including Mimikatz, Advanced IP Scanner, PingCastle, and various remote management utilities to escalate privileges, conduct reconnaissance, and establish persistence within compromised environments.

**#6** Affiliates have the capability to tailor the ransomware for different platforms, producing variants designed for Windows, Linux, VMware ESXi, and NAS systems, enabling them to strike a broad range of infrastructure. In one notable incident from February 2025, DragonForce exfiltrated and publicly leaked over 6 terabytes of sensitive data from a Middle Eastern organization after ransom negotiations failed. This event highlighted not only the group's aggressive extortion tactics but also the vast scale of data theft they are capable of executing.

# Recommendations

**Patch Management:** Prioritize patching of high-risk vulnerabilities frequently exploited by DragonForce, including Log4Shell and Ivanti Connect Secure bugs. Implement a formal, rapid patching protocol for all critical infrastructure and public-facing systems.

**Credential Hygiene:** Enforce the use of strong, unique passwords across all systems. Regularly scan for exposed credentials in data breaches and dark web dumps. Apply rate-limiting and account lockout mechanisms to prevent credential stuffing attacks.

**Implement the 3-2-1 Backup Rule:** Maintain three total copies of your data, with two backups stored on different devices and one backup kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

**Network Segmentation & Zero Trust Implementation:** Segment critical infrastructure to isolate sensitive data and limit lateral movement. Implement Zero Trust Network Access (ZTNA) by enforcing identity-based policies rather than traditional perimeter security.

**Backup & Recovery Preparedness:** Maintain offline, immutable, and regularly tested backups. Ensure recovery time objectives (RTOs) and recovery point objectives (RPOs) meet business continuity requirements in the event of ransomware deployment.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001 Initial Access | TA0002 Execution | TA0003 Persistence | TA0005 Defense Evasion |
| TA0006 Credential Access | TA0007 Discovery | TA0008 Lateral Movement | TA0009 Collection |
| TA0011 Command and Control | TA0010 Exfiltration | TA0040 Impact | TA0042 Resource Development |
| T1566 Phishing | T1190 Exploit Public-Facing Application | T1078 Valid Accounts | T1059 Command and Scripting Interpreter |

| | | | |
|---|---|---|---|
| **T1203** Exploitation for Client Execution | **T1027** Obfuscated Files or Information | **T1070.004** File Deletion | **T1562.001** Disable or Modify Tools |
| **T1562** Impair Defenses | **T1003** OS Credential Dumping | **T1046** Network Service Discovery | **T1087** Account Discovery |
| **T1018** Remote System Discovery | **T1482** Domain Trust Discovery | **T1560** Archive Collected Data | **T1005** Data from Local System |
| **T1041** Exfiltration Over C2 Channel | **T1486** Data Encrypted for Impact | **T1490** Inhibit System Recovery | **T1531** Account Access Removal |
| **T1491** Defacement | **T1588** Obtain Capabilities | **T1588.006** Vulnerabilities | **T1204** User Execution |
| **T1204.002** Malicious File | **T1070** Indicator Removal | **T1083** File and Directory Discovery | **T1082** System Information Discovery |
| **T1133** External Remote Services | **T1059.001** PowerShell | **T1547** Boot or Logon Autostart Execution | **T1547.001** Registry Run Keys / Startup Folder |
| **T1053** Scheduled Task/Job | **T1053.005** Scheduled Task | **T1543** Create or Modify System Process | **T1543.003** Windows Service |
| **T1078.002** Domain Accounts | **T1070.001** Clear Windows Event Logs | **T1003.001** LSASS Memory | **T1016** System Network Configuration Discovery |
| **T1021.001** Remote Desktop Protocol | **T1021** Remote Services | **T1021.002** SMB/Windows Admin Shares | **T1071.001** Web Protocols |
| **T1071** Application Layer Protocol | **T1569.002** Service Execution | **T1569** System Services | **T1499** Endpoint Denial of Service |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA1 | 343220b0e37841dc002407860057eb10dbeea94d, ae2967d021890a6a2a8c403a569b9e6d56e03abd, c98e394a3e33c616d251d426fc986229ede57b0f, f710573c1d18355ecdf3131aa69a6dfe8e674758, 011894f40bab6963133d46a1976fa587a4b66378, 0b22b6e5269ec241b82450a7e65009685a3010fb, 196c08fbab4119d75afb209a05999ce269ffe3cf, 1f5ae3b51b2dbf9419f4b7d51725a49023abc81c, 229e073dbcbb72bdfee2c244e5d066ad949d2582, 29baab2551064fa30fb18955ccc8f332bd68ddd4, 577b110a8bfa6526b21bb728e14bd6494dc67f71, 7db52047c72529d27a39f2e1a9ffb8f1f0ddc774, 81185dd73f2e042a947a1bf77f429de08778b6e9, a4bdd6cef0ed43a4d08f373edc8e146bb15ca0f9, b3e0785dbe60369634ac6a6b5d241849c1f929de, b571e60a6d2d9ab78da1c14327c0d26f34117daa, bcfac98117d9a52a3196a7bd041b49d5ff0cfb8c, e164bbaf848fa5d46fa42f62402a1c55330ef562, e1c0482b43fe57c93535119d085596cd2d90560a, eada05f4bfd4876c57c24cd4b41f7a40ea97274c, fc75a3800d8c2fa49b27b632dc9d7fb611b65201 |
| TOR Address | 3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd[.]onion, Ijbw7iiyodqzpg6ooewbgn6mv2pinoer3k5pzdecoejsw5nyoe73zvad[.]onion, Kfgjwkho24xiwckcf53x7qyruobbkhx4eqn2c6oe4hprbn23rcp6qcqd[.]onion, Rnc6scfbqslz5aqxfg5hrjel5qomxscllc6jvhahi6qwt7op5qc7iad[.]onion, rrrbay3nf4c2wxmhprc6eotjlpqkeowfuobodic4x4nzqtosx3ebirid[.]onion, rrrbayguhgtgxrdg5myxkdc2cxei25u6brknfqkl3a35nse7f2arblyd[.]onion, rrrbaygxp3f2qtgvfqk6ffhdrm24ucxvbr6mhxsga4faefqyd77w7tqd[.]onion, Z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion |
| Tox ID | 1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20, 258C79F73CCC1E56863030CD02C2C7C4347F80CAD43DD6A5B219A618FD17853C7BB1029DAE31 |

## Patch Links

https://logging.apache.org/security.html

https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412

https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure

https://jira.atlassian.com/browse/CONFSERVER-79016

## Recent Breaches

https://citrusmagic.com
https://rrsfoodservice.com
https://www.irisid.com
https://www.cityofgroveok.gov
https://www.setpointsystems.com
https://pratthomes.com
https://pryor-morrow.com
https://kraftkisarna.se
https://ossman.co.uk
https://www.harrissteelco.com
https://stitaly.it
https://millercaggiano.com
https://dac-law.com
https://www.precisiontextiles-usa.com
https://www.texlaenergy.com
https://iacc.holdings
https://www.condista.com
https://altara.com
https://net-move.com
https://industrialdynamics.com
https://www.dermatologysolutions.com
https://southernavionics.com
https://atlplasticsurgeon.com
https://jtalleycorp.com
https://www.philsmithauto.com
https://thaonlesvosges.fr
https://architekturbuero-heller.de
https://www.colemanmaterials.com
https://yadea.com

https://dtsservices.uk
https://moncaro.com
https://kleen-pak.com
https://vercoes.co.nz
https://steel-dynamics.co.uk
https://cotswold-fayre.co.uk
https://eleetwoodworking.com
https://www.gsfloor.com
https://tristrameuropean.co.nz
https://www.albawani.net
https://accelerator.no
https://oandsassociates.com
https://nasltd.com
https://heartcentre.net.au
https://cogitis.fr

## References


https://www.sentinelone.com/blog/dragonforce-ransomware-gang-from-hacktivists-to-high-street-extortionists/

https://hivepro.com/threat-advisory/dragonforce-unleashes-chaos-with-leaked-lockbit-builder/

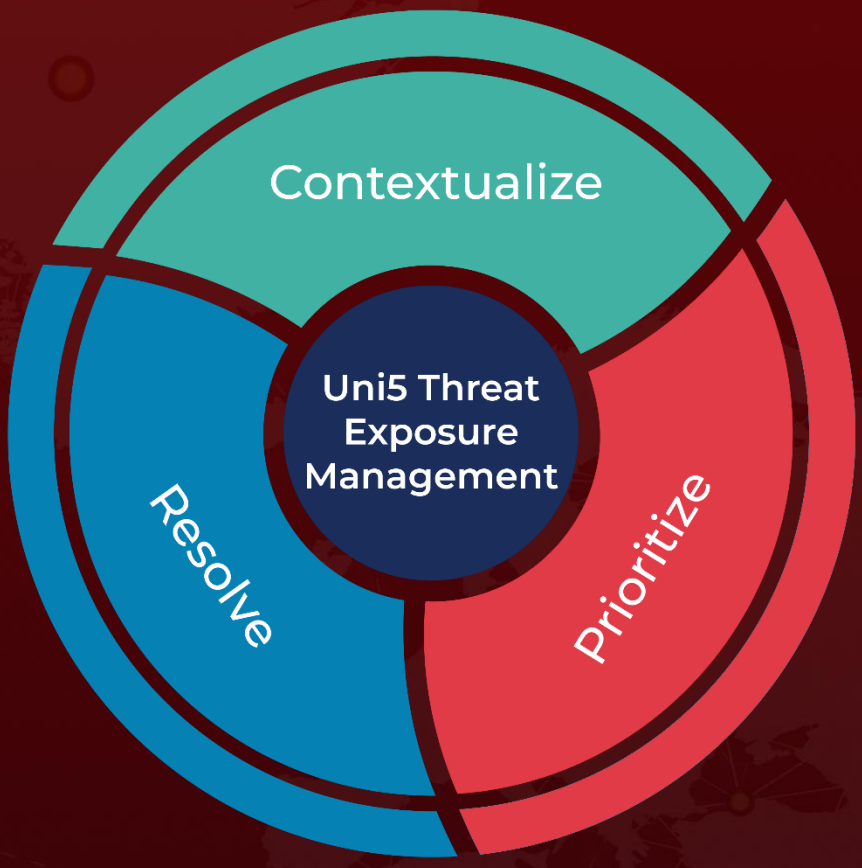
https://blog.checkpoint.com/security/dragonforce-ransomware-redefining-hybrid-extortion-in-2025/

https://www.cloudsek.com/threatintelligence/hacktivist-group-dragonforce-malaysia-releases-windows-lpe-exploit-discloses-plans-to-evolve-into-a-ransomware-group

# 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

**May 9, 2025 • 3:30 AM**



More at www.hivepro.com