blackpoint

THREAT PROFILE:

# DragonForce Ransomware

# TABLE OF CONTENTS


| | |
|---|---|
| Executive Summary | 2 |
| Diamond Model | 3 |
| Description | 4 |
| Previous Targets: Industries & Regions | 6 |
| Data Leak Site | 8 |
| Known Exploited Vulnerabilities | 9 |
| Associations | 10 |
| Known Tools | 12 |
| Observed Behaviors: Windows & Linux | 15 |
| Kill Chain | 21 |
| MITRE ATT&CK® Mappings | 22 |
| References | 27 |

# Executive Summary

### First Identified:
2023

### Operation style:
Ransomware-as-a-Service (RaaS); as of 2025 the group has been reported to operate a white-label cartel operation.

### Extortion method:
Double extortion – combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

### Most frequently targeted industry:
- Industrials (Manufacturing)

### Most frequently targeted victim HQ region:
- North America

### Known Associations:
- Conti Ransomware
- DragonForce Malaysia
- LockBit 3.0 Ransomware
- Ransombay Service
- Ransomhub Ransomware
- Scattered Spider

**INITIAL ACCESS** → **PERSISTENCE** → **LATERAL MOVEMENT**

Valid accounts, exploitation of external remote services, drive-by compromise, vulnerability exploitation, social engineering (MITRE ATT&CK: T1078, T1133, T1189, T1190, T1566)

Scheduled tasks, valid Accounts, abuse of system processes, Registry Keys, Startup Folder (MITRE ATT&CK: T1053, T1078, T1543, T1547)

Abuse of remote systems, lateral tool transfer (MITRE ATT&CK: T1021, T1210, T1570)

# Diamond Model

# Description

DragonForce ransomware was first identified in August 2023. DragonForce ransomware operated as a private group until June 2024 when the group advertized their affiliate program on the Russian-language cybercriminal forum, RAMP. The group reportedly offers 80% of a ransom payment to the affiliates.

Security researchers with Group-IB reported that each affiliate in the DragonForce operation receives a unique .onion address and a new profile created to grant the user access. The affiliate panel contains multiple sections for the affiliates, including:

- Clients
- Builder
- My Team
- Add Adver
- Publications
- Constructor
- Rules
- Blog
- Profile

There is an even chance that the ransomware is related to the hacktivist group, “DragonForce Malaysia”, based on the groups’ 2023 claims that they were going to start a ransomware operation. The group reportedly made the announcement via their Telegram channel. However, this has yet to be confirmed. There is an even chance that another operation has adopted the name in an effort to evade detection and attribution.

DragonForce has two ransomware variants - one based on LockBit Ransomware and another based on the Conti Ransomware variant. The Conti fork of DragonForce renames files with a “.dragonforce_encrypted” extension; however, affiliates reportedly have the option to customize the extension.

**DragonForce started a RaaS program in June 2024; previously operated as a private group.**

The Conti version utilizes nearly the same encryption method, but DragonForce has some customizable values. For each file, the ChaCha8 key and IV is generated by the `CryptGenRandom()` function.

The ransomware includes the following command-line arguments:

- -p: EncryptMode - path
- -m: EncryptMode - all, local, net
- -log: Specify log file
- -size: Specify file encryption percentage
- -nomutex: Do not create mutex

Additionally, there are three encryption types:

- FULL_ENCRYPT: files with database extensions are fully encrypted
- PARTLY_ENCRYPT: files with VM extensions are 20% encrypted.
- HEADER_ENCRYPT: only the first [header_encrypt_size] bytes are encrypted.

There is reportedly little difference between the DragonForce variant based on the leaked builder of LockBit 3.0 and many other variants based on the same builder.

Similar to other operations, DragonForce deletes Shadow Copies, kills running processes, and abuses digitally signed but vulnerable drivers during reported incidents.

# Description

DragonForce operators and affiliates have been reported to have gained initial access via public-facing remote desktop servers and social engineering attacks. The group has been reported to utilize the “Bring Your Own Vulnerable Driver” (BYOVD) technique.

DragonForce has been reported to gain persistence in targeted networks by abusing valid accounts, manipulating Registry Run Keys, and creating new system processes and scheduled tasks.

DragonForce has been reported to conduct lateral movement via abusing RDP to access internal servers and move through the network and utilizing post-exploitation malware, such as Cobalt Strike.

DragonForce drops a ransom note for each victim and signs the note with “01000100 01110010 01100001 01100111 01101111 01101110 01000110 01101111 01110010 01100011 01100101”, which means DragonForce in its binary representation.

In June 2024, DragonForce reportedly released a recording of an intimidation call made to a purported victim. This indicates that the group likely calls victims after an attack in attempt to apply additional pressure to pay the ransom demand.

In March 2025, the group announced their shift to a “ransomware cartel”. In the announcement, affiliates were encouraged to continue using DragonForce tools but to branch out and create their own brand.

**DragonForce ransomware maintains a Conti fork and LockBit 3.0 for variant of encryptors.**

Around the same time, the group was linked to attacks from the BlackLock (AKA Mamona) operation and appeared to be in conflict with the Ransomhub operation.

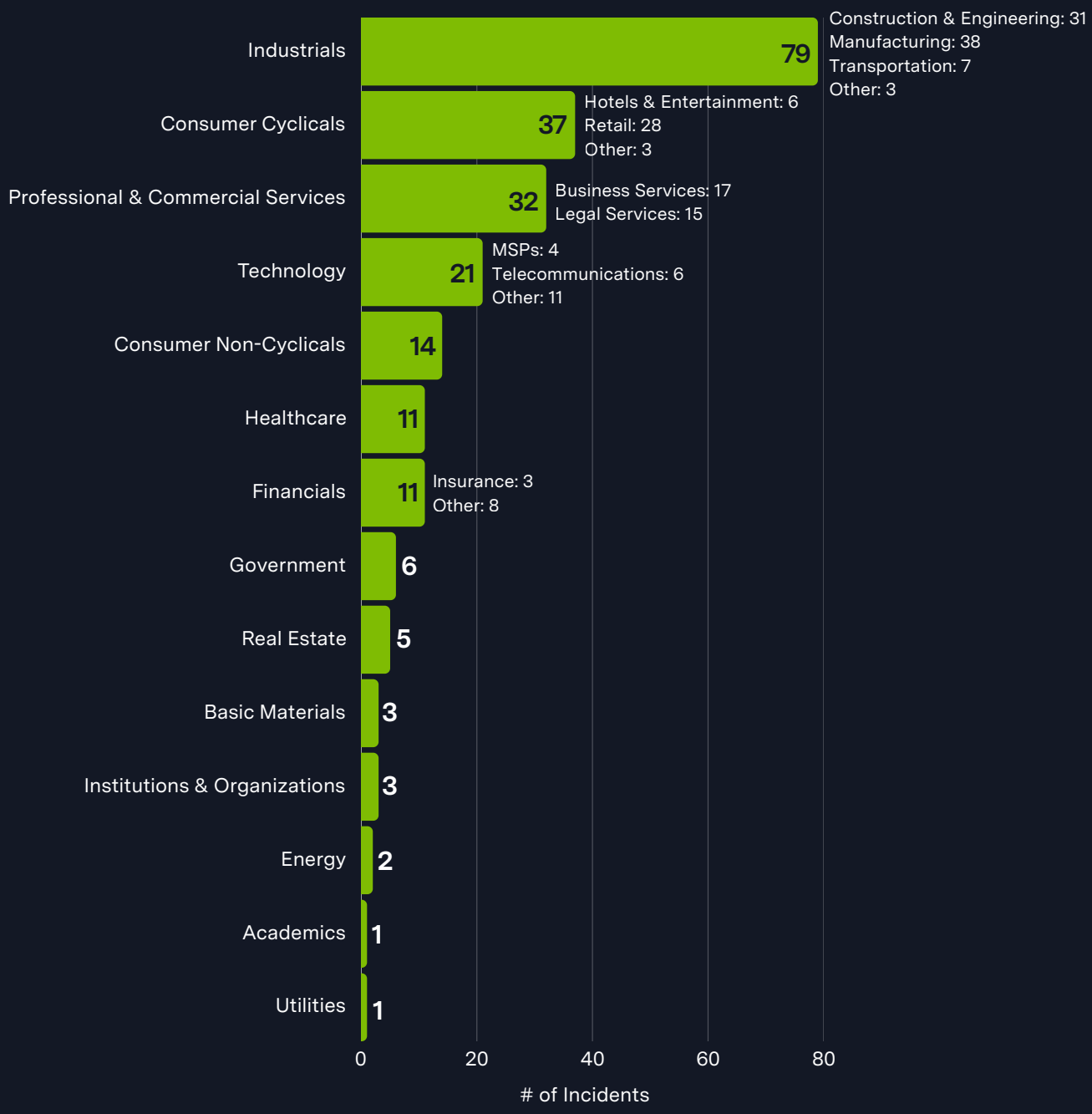
In August 2025, the group reportedly launched a “data analysis service” for creating tailored extortion materials, which was offered to affiliates targeting organizations with an annual revenue of $15 million or more.

This function reportedly serves as a risk audit of both the targeted organization and the stolen data, generating things like call scripts, drafts of letters to management, and pseudo legal analysis and advice reports. The fee for this service reportedly ranges from 0-23% of ransom payments.

This type of business model will likely allow lower skill level threat actors to participate in ransomware campaigns without requiring the skill and resources to maintain their own infrastructure and malware.

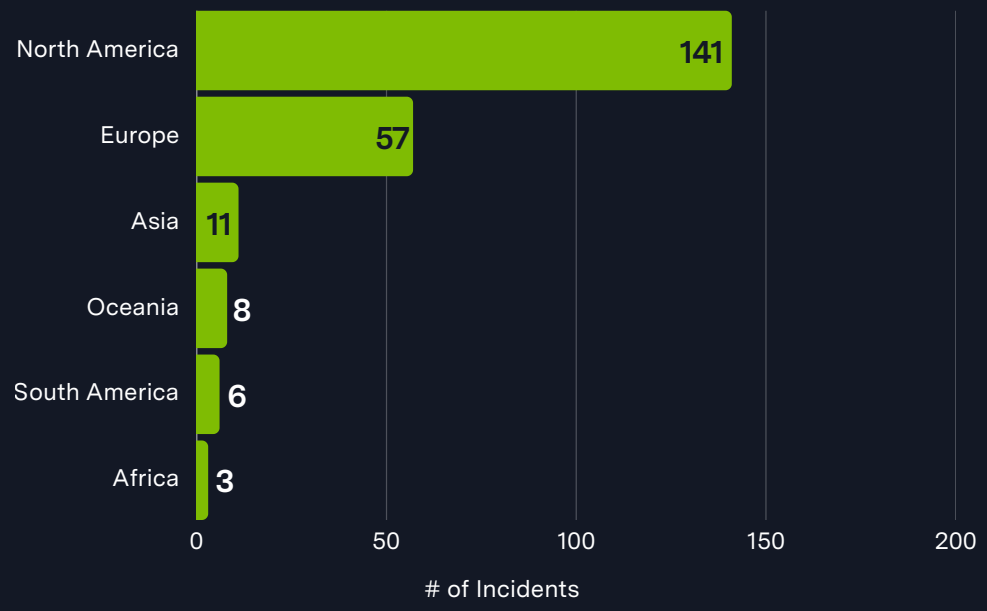
# Previous Targets

## Previous Industry Targets from 01 Jan 2025 to 31 Dec 2025

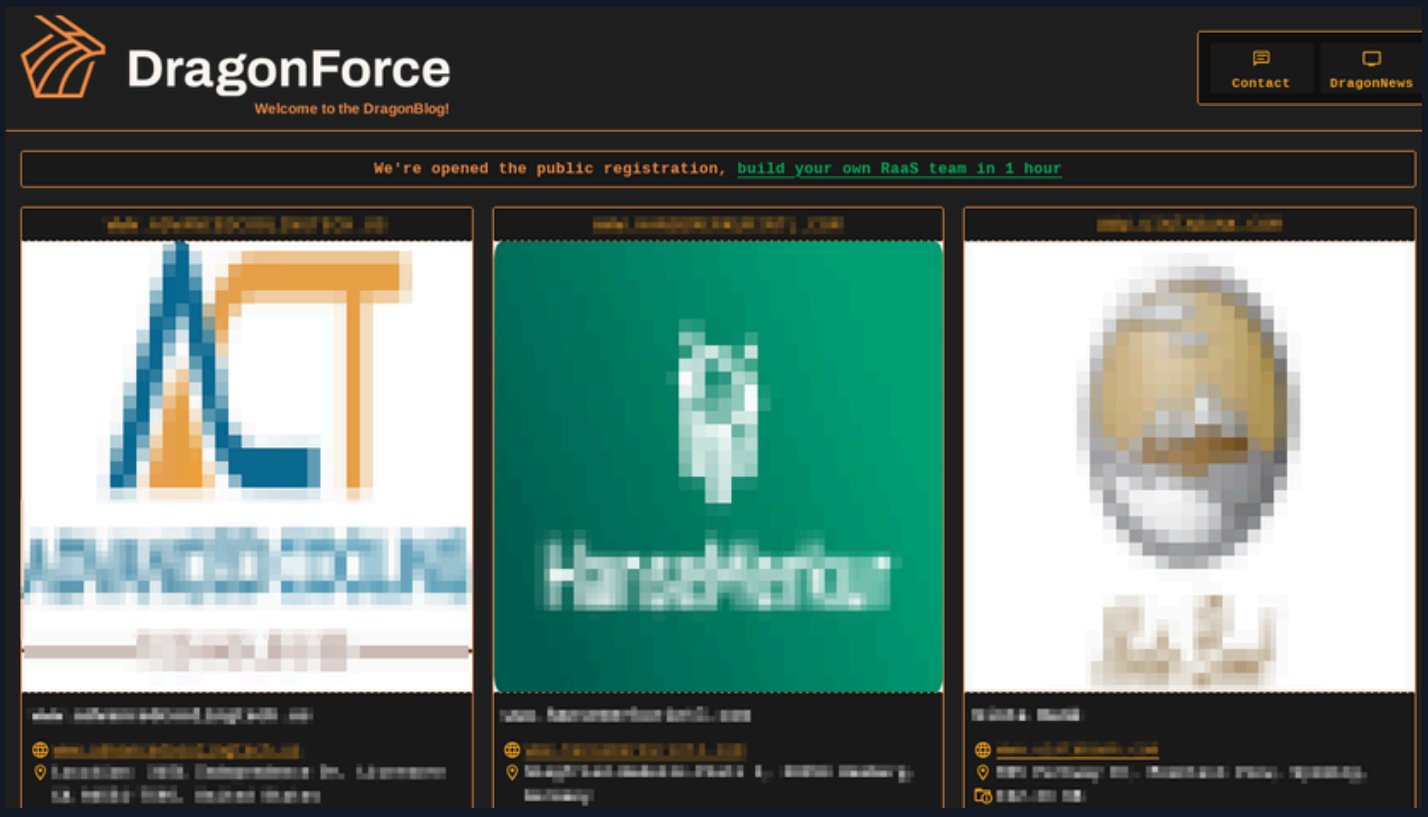


# Previous Targets

## Previous Victim HQ Regions from 01 Jan 2025 to 31 Dec 2025



# Data Leak Site




*hxxp://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion/*
*hxxp://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd[.]onion*

# Known Exploited Vulnerabilities

| Vulnerability | Description | Product Affected | CVSS |
|---|---|---|---|
| CVE-2021-44228 | RCE Vulnerability | Apache Log4j Java Library | 10 |
| CVE-2023-46805 | Authentication Bypass Vulnerability | Ivanti Connect Secure and Policy Secure | 8.5 |
| CVE-2024-21412 | Security Feature Bypass Vulnerability | Microsoft Windows Internet Shortcut Files | 8.1 |
| CVE-2024-21762 | Out-of-bound Write in sslvpnd | FortiOS | 9.8 |
| CVE-2024-21887 | Command Injection Vulnerability | Ivanti Connect Secure and Policy Secure | 9.1 |
| CVE-2024-21893 | Server-Side Request Forgery (SSRF) Vulnerability | Ivanti Connect Secure, Policy Secure, and Neurons | 9.1 |
| CVE-2024-40766 | SonicOS Improper Access Control Vulnerability | SonicOS | 9.8 |
| CVE-2024-57726 | Privilege Escalation Vulnerability | SimpleHelp | 9.9 |
| CVE-2024-57727 | Path Traversal Vulnerability | SimpleHelp | 7.5 |
| CVE-2024-57728 | Arbitrary File Upload Vulnerability | SimpleHelp | 7.2 |
| CVE-2024-55591 | Authentication Bypass Vulnerability in Fortinet FortiOS and FortiProxy | FortiOS | 9.8 |

# Associations

## BlackLock Ransomware

DragonForce has been linked to attacks from BlackLock (which rebranded to Mamona); there is an even chance this is part of the “ransomware cartel” operation DragonForce annouced.

## Bjorka

A user identified on multiple cybercriminal forums (BreachForums, RaidForums) and linked to the Babuk2 operation in 2025 - a data leak site that appeared to publish mostly recycled data already leaked by other groups. Bjorka has been linked to the DragonForce operation via a database leaked from BreachForums that had Bjorka email (bjorkaact) listed as the username for the DragonForce profile.

## Conti Ransomware

Security researchers with Group-IB reported that DragonForce maintains a variant based off the Conti ransomware. The DragonForce version reportedly gives affiliates the opportunity to customize various parts of the encryptor.

## Devman

Security researchers have reportedly identified Devman ransomware payloads that are build on DragonForce infrastructure. As Devman has also been linked to Qilin, it is likely Devman is a part of the previously reported “ransomware cartel”.

## DragonForce Malaysia

A hacktivist group from Malaysia that announced via their Telegram in 2023 that they were planning on developing a ransomware operation. Any connection between the two groups has not been confirmed.

## LockBit Ransomware

Security researchers with Cyble reported that DragonForce and LockBit 3.0's leaked builder have nearly identical source code. The extent of the relationship is unverified but it is likely that DragonForce created their ransomware encryptor using the LockBit 3.0 builder. In August 2025, DragonForce announced a partnership with the LockBit operation to create a “ransomware cartel.”

## Qilin Ransomware

DragonForce operators posted on a dark web forum that they were launching a partnership between themselves, LockBit, and Qilin operations.

# Associations

## Ransombay Service

Security researchers have reported the announcement of the Ransombay service and portals in connection with the DragonForce white-label cartel offering. Under this offering, DragonForce reportedly charges 20% of the ransom payment and, in exchange, provides the infrastructure, malware, and ongoing support services.

## Ransomhub Ransomware

There are mixed reports of the relationship between Ransomhub and DragonForce. DragonForce first reported that Ransomhub was joining their cartel, then listed Ransomhub as a victim on their data leak site. Theories range from a cooperative merge of the groups to Ransomhub pulling an exit scam.

## Scattered Spider

AKA oktapus, Starfraud, UNC3944, Scatter Swine, Octo Tempest, and Muddled Libra. Security researchers have reported that Scattered Spider has been observed deploying the DragonForce ransomware variant against targets in the Consumer Cyclicals (Retail) vertical.

## Water Tambanakua

Threat group behind the DragonForce Ransomware operation as tracked by Trend Micro.

# Known Tools

| Function | Tool | Description |
|---|---|---|
| **Execution** | PowerShell | Command line shell, scripting language, and automation framework utilized to execute scripts and payloads. |
| | WMI | Microsoft's framework for managing data and operations used to execute commands and queries remotely. |
| **Persistence** | at | Command line utility used to schedule commands, scripts, or programs to run at a specific date/time. |
| | schtasks | Command line tool used to create, delete, run, manipulate, and query scheduled tasks. |
| | SimpleHelp | Legitimate RMM tool used to maintain persistence access to environment. |
| **Privilege Escalation** | BadRentdvr2 | Vulnerable driver that uses ThrottleStop.sys to execute kernel-mode routines. |
| **Defense Evasion** | ADV obfuscator | Open-source C++ library used to obfuscate code and data. |
| | bcdedit | Command line tool used to modify boot configuration data for system level changes. |
| | Rogue Killer Antirootkit Driver | Kernel-level driver module used to terminate security processes. |
| | TrueSigntKiller | Tool used to terminate antivirus (AV) and endpoint detection and response (EDR) software on Windows systems. |
| | Windows Restart Manager | Legitimate API abused to disable security tools, terminate process, and manipulate system processes. |
| **Credential Access** | LaZagne | Open-source exploitation tool used to retrieve credentials stored on a local device. |
| | Mimikatz | Hacktool used to extract Windows passwords in plain-text from memory. |
| | PassView | Part of the NirSoft suite used to reveal passwords stored on a Windows device. |
| **Discovery** | AdFind | Command line query tool used to gather information from Active Directory (AD) environments. |
| | Advanced IP Scanner | Network scanner for Windows used to identify connected devices within a compromised environment. |

# Known Tools

| Function | Tool | Description |
|---|---|---|
| **Discovery** | PingCastle | Tool designed to identify and report the health and security posture of AD environments, often abused to identify weaknesses in AD networks. |
| | Process Hacker | Tool used to view and manipulate processes, kernel options, and more. |
| | SoftPerfect Network Scanner | Tool that scans networks for connected devices, shared folders, and open ports. |
| **Lateral Movement** | Cobalt Strike | Red Teaming platform abused for post-exploitation activities, including moving laterally. |
| | PsExec | Command line tool abused to execute a program on another computer. |
| | RDP | Microsoft protocol used to remotely connect to a Windows computer. |
| **Command and Control** | SystemBC | Malware variant that provides both remote access and functions as a SOCKS5 proxy. |
| | Wget | Command line utility for retrieving content and files from web servers. |
| **Exfiltration** | Amazon S3 Buckets | Cloud storage containers used to store and manage data as objects. |
| | MEGA | User-controlled cloud storage and communication service often abused to host stolen data. |
| | MEGASync | Application used to synchronize files between a user's computer and a MEGA cloud storage instance. |
| | Rclone | Command line program used to manage, sync, and transfer files. |
| **Impact** | 7-zip | Open-source file archiver used to compress, decompress, and encrypt files. |
| | PC Hunter | Legitimate toolkit used to disable security software and facilitate encryption. |
| | vim-cmd | Command Line Interface (CLI) tool used to manage VMware ESXi hosts and virtual machines (VMs). |
| | VssAdmin | Command line tool abused to delete Volume Shadow Copy Service (VSS). |
| | wbadmin | Command line utility abused to delete backup data. |
| | Windows Restart Manager | A Windows service that is often abused to manipulate running processes and is abused to facilitate the encryption of locked files, maximizing impact. |

# Known Tools

| Function | Tool | Description |
|---|---|---|
| **Infrastructure** | TOR | Open-source software enabling anonymous malicious activities, such as command and control, operating data leak sites, and more. |
| | TOX | Open-source instant messaging protocol used for ransom negotiations. |

# Observed Behaviors: Windows

| Tactic | Evidence Type | Observed Behavior |
|---|---|---|
| **Execution** | Command Execution | Process creation via CreateProcess() |
| | | System information querying via NtQuerySystemInformation() |
| | | File creation and access via CreateFileW() |
| **Persistence** | Command Execution | powershell.exe -windowstyle hidden -Command <executable> |
| | Configuration Change | HKLM\Software\Microsoft\Windows\CurrentVersion\Run\socks5 |
| | | bcdedit /set {default} bootstatuspolicy ignoreallfailures |
| **Privilege Escalation** | Command Execution | Token duplication via DuplicateTokenEx() |
| | | Process creation under alternate token via CreateProcessWithTokenW() |
| **Defense Evasion** | Command Execution | Process handle access via ZwOpenProcess() |
| | | Process termination via ZwTerminateProcess() / TerminateProcess() |
| | | Shadow copy enumeration via SELECT * FROM Win32_ShadowCopy |
| | | Shadow copy deletion via WMIC shadowcopy delete / vssadmin delete shadows /all /quiet |
| | | Backup catalog deletion via wbadmin delete catalog -quiet |
| | | System state backup deletion via wbadmin delete systemstatebackup |
| **Impact** | Command Execution | Cryptographic operations supporting encryption via CryptGenRandom() |
| | | Cryptographic key handling via CryptImportKey() |
| | Configuration Change | Disable recovery via bcdedit /set {default} recoveryenabled No |
| | | File association and icon modification for encrypted files (.dragonforce_encrypted) |
| | | Desktop wallpaper modification via registry (Wallpaper, WallpaperStyle) |

# Observed Behaviors: Windows

| Tactic | Evidence Type | Observed Behavior |
|---|---|---|
| **Impact** | Output/Artifact | Deletion of user-facing file (Contact Us.txt) from system drive |
| | | Ransomware wallpaper C:\Users\Public\wallpaper_white.png |

# Arguments: Windows

| Argument | Description |
|---|---|
| -safe | Reboots in safe mode, then encrypts the user's machine. |
| -wall | Changes system Wallpaper and Print ransom note on printers then deletes itself after renaming for 26 times. |
| -path | Specifically encrypt the target, can be file or folder. |
| -gspd | Perform Group Policy Modification for Lateral Movement. |
| -psex | Lateral Movement via Admin Shares. |
| -gdel | Delete group policy updates. |
| -del | Deletes itself after renaming for 26 times.. |

# Observed Behaviors: Linux

| Tactic | Evidence Type | Observed Behavior |
|---|---|---|
| **Execution** | Command Execution | Force filesystem-based execution and discovery using -paths |
| | | Force ESXi discovery and execution mode using -vmsvc |
| | | Disable encryption to run in discovery-only mode using -n |
| | | Delayed execution using -h <hours> -m <minutes> -s <seconds> |
| | | Select encryption mode and parameters using -e <mode> <X> <Y> |
| | | Override filesystem discovery paths using -p <path> |
| | | Override log file location using -l <logfile> |
| | | Override execution thread count using -i <threads> |
| | | Suppress standard output using -q |
| | | Enable verbose runtime logging using -v |
| | | Exclude specific VMs from execution by ID using -vwi <ID> |
| | | Exclude specific VMs from execution by name using -vwn <name> |

# Arguments: Linux

| Argument | Description |
|---|---|
| -paths | Sets a variable either 1 or 0 but no purpose. |
| -vmsvc | Forces search in the ESXi detection mode using vim-cmd. |
| -n | Do not perform encryption/decryption (only file detection). |
| -h H -m M -s S | Wait H hours, M minutes, and S seconds before starting. |
| -e M X Y | Encryption mode with parameters M, X, and Y. |
| -p PATH | Redefines the file system paths for detection. |
| -l LOGFILE | Redefines the log file location. |
| -j X | Redefines the number of threads to use. |
| -q | Disables output to STDOUT. |
| -v | Enables detailed logging. |
| -wvi ID | Redefines the list of ignored BMs by ID. |
| -wv NAME | Redefines the list of ignored BMs by name. |

# Configuration File Options

| Option | Description |
|---|---|
| dry_run | Mode without actual encryption/decryption (for testing purposes). |
| encryption.expansion | Defines the file extension for encrypted files. |
| encryption.rename | Renames encrypted files. |
| encryption.mode | Specifies the encryption mode (options: striped, percent, header, normal). |
| encryption.p1<br>encryption.p2 | Parameters for encryption mode. |
| work_mode | Specifies the working mode (options: vmsvc, paths). |
| paths | Paths for encrypting files. |
| note_file | Name of the file that stores the ransom note. |
| log.file | Path to the log file. |
| log.encrypted | Enables encryption logging. |
| delay | Delay before starting the encryption process (in seconds). |
| whitelist.paths | Directories to be excluded from encryption. |
| whitelist.extensions | File extensions to be excluded from encryption. |
| whitelist.filesnames | Specific file names to be excluded from encryption. |
| whitelist.vm_ids | Virtual machine IDs to be excluded from encryption. |
| whiteliste.vm_names | Virtual machine names to be excluded from encryption. |

# Kill Chain

## Initial Access

- Compromised RDP Servers
- Drive-by Compromise
- Social Engineering

## Persistence

- Valid Accounts
- Scheduled Tasks
- Registry Run Keys
- Windows Service

## Defense Evasion

- Delete Files
- Disable/Modify Tools
- Modify Registry
- Hide Artifacts

## Lateral Movement

- RDP
- Cobalt Strike Beacons
- Exposed Services

## Exfiltration

- Cloud Services - MEGA, AWS S3
- TOR-hosted leak sites

## Impact

- Data Encryption
- Data Exfiltration
- Operational Disruption

# MITRE ATT&CK® Mappings

| | |
|---|---|
| **Reconnaissance** | |
| T1595: Active Scanning | .002: Vulnerability Scanning |
| **Resource Development** | |
| T1585: Establish Accounts | .002: Email Accounts |
| T1587: Develop Capabilities | .001: Malware |
| T1588: Obtain Capabilities | .001: Malware<br>.002: Tools |
| **Initial Access** | |
| T1078: Valid Accounts | .002: Domain Accounts |
| T1133: External Remote Services | |
| T1189: Drive-by Compromise | |
| T1190: Exploit Public-Facing Application | |
| T1566: Phishing | .001: Spearphishing Attachment<br>.004: Spearphishing Voice |
| **Execution** | |
| T1047: Windows Management Instrumentation | |
| T1059: Command and Scripting Interpreter | .001: PowerShell<br>.003: Windows Command Shell<br>.012: |
| T1204: User Execution | .002: Malicious File |
| T1559: Inter-Process Communication | .001: Component Object Model |
| T1569: System Services | .002: Service Execution |

# MITRE ATT&CK® Mappings

| | |
|---|---|
| **Persistence** | |
| T1053: Scheduled Task/Job | .005: Scheduled Task |
| T1078: Valid Accounts | .002: Domain Accounts |
| T1543: Create or Modify System Process | .003: Windows Service |
| T1547: Boot or Logon Autostart Execution | .001: Registry Run Keys/Startup Folder |
| **Privilege Escalation** | |
| T1068: Exploitation for Privilege Escalation | |
| T1078: Valid Accounts | .002: Domain Accounts |
| T1134: Access Token Manipulation | .001: Token Impersonation/Theft |
| **Defense Evasion** | |
| T1027: Obfuscated Files or Information | .002: Software Packing |
| T1070: Indicator Removal | .001: Clear Windows Event Logs<br>.004: File Deletion |
| T1112: Modify Registry | |
| T1140: Deobfuscate/Decode Files or Information | |
| T1211: Exploitation for Defense Evasion | |
| T1218: System Binary Proxy Execution | |
| T1222: File and Directory Permissions Modification | |
| T1553: Subvert Trust Controls | .002: Code Signing |
| T1562: Impair Defenses | .001: Disable or Modify Tools |
| T1564: Hide Artifacts | .003: Hidden Window |

# MITRE ATT&CK® Mappings

| | |
|---|---|
| **Defense Evasion** | |
| T1679: Selective Exclusion | |
| **Credential Access** | |
| T1003: OS Credential Access | .001: LSASS Memory<br>.002: Security Account Manager |
| **Discovery** | |
| T1012: Query Registry | |
| T1016: System Network Configuration Discovery | |
| T1018: Remote Services Discovery | |
| T1057: Process Discovery | |
| T1069: Permission Groups Discovery | .002: Domain Groups |
| T1082: System Information Discovery | |
| T1083: File and Directory Discovery | |
| T1087: Account Discovery | .002: Domain Account |
| T1135: Network Share Discovery | |
| T1482: Domain Trust Discovery | |
| T1673: Virtual Machine Discovery | |
| **Lateral Movement** | |
| T1021: Remote Services | .001: Remote Desktop Protocol<br>.002: SMB/Windows Admin Shares |
| T1210: Exploitation of Remote Services | |

# MITRE ATT&CK® Mappings

| | |
|---|---|
| **Lateral Movement** | |
| T1570: Lateral Tool Transfer | |
| **Collection** | |
| T1005: Data from Local System | |
| T1560: Archive Collected Data | .001: Archive via Utility |
| **Command and Control** | |
| T1071: Application Layer Protocol | .001: Web Protocols |
| T1090: Proxy | |
| T1105: Ingress Tool Transfer | |
| T1219: Remote Access Tools | .002: Remote Desktop Software |
| T1571: Non-Standard Port | |
| **Exfiltration** | |
| T1041: Exfiltration Over C2 Channel | |
| T1048: Exfiltration Over Alternative Protocol | .003: Exfiltration Over Unencrypted Non-C2 Protocol |
| T1567: Exfiltration Over Web Service | .002: Exfiltration to Cloud Storage |
| **Impact** | |
| T1486: Data Encrypted for Impact | |
| T1489: Service Stop | |
| T1490: Inhibit System Recovery | |

# MITRE ATT&CK® Mappings

| Impact | |
|---|---|
| T1491: Defacement | .001: Internal Defacement |
| T1529: System Shutdown/Reboot | |
| T1657: Financial Theft | |

# References


- Acronis Threat Research Unit (2025, November 04) “The DragonForce Cartel: Scattered Spider at the gate.” https://www.acronis.com/en/tru/posts/the-dragonforce-cartel-scattered-spider-at-the-gate/
- Bradshaw, Anthony; Neal, Hunter; Demboski, Morgan; et. al. (2025, May 27) Sophos: “DragonForce actors target SimpleHelp vulnerabilities to attack MSP, customers.” https://news.sophos.com/en-us/2025/05/27/dragonforce-actors-target-simplehelp-vulnerabilities-to-attack-msp-customers/
- Broadcom (2025, April 16) “DragonForce Ransomware's Campaign Intensifies in 2025.” https://www.broadcom.com/support/security-center/protection-bulletin/dragonforce-ransomware-s-campaign-intensifies-in-2025
- Cyble (2024, April 24) “LOCKBIT Black’s Legacy: Unraveling the DragonForce Ransomware Connection.” https://cyble.com/blog/lockbit-blacks-legacy-unraveling-the-dragonforce-ransomware-connection/
- Cyble (2025, February 20) “Threat Actor Profile: DragonForce Ransomware Group.” https://cyble.com/threat-actor-profiles/dragonforce-ransomware-group/
- DarkTrace (2025, November 5) “Tracking a Dragon: Investigating a DragonForce-affiliated ransomware attack with DarkTrace.” https://www.darktrace.com/blog/tracking-a-dragon-investigating-a-dragonforce-affiliated-ransomware-attack-with-darktrace
- Kichatov, Nikolay; Low, Sharmine; Kashtanov, Alexey (2024, September 25) Group-IB: “Inside the Dragon: DragonForce Ransomware Group. https://www.group-ib.com/blog/dragonforce-ransomware/
- Resecurity (2025, March 03) “DragonForce Ransomware - Reverse Engineering Report.” https://www.resecurity.com/blog/article/dragonforce-ransomware-reverse-engineering-report
- S2W TALON (2025, December 23) “DragonForce Ransomware Analysis Report.” https://s2w.inc/en/resource/detail/985
- Secureworks CTU (2025, April 16) “Ransomware Groups Evolve Affiliate Models.” https://www.secureworks.com/blog/ransomware-groups-evolve-affiliate-models
- Sharma, Ax (2023, December 27) Bleeping Computer: “Yakult Australia confirms 'cyber incident' after 95 GB data leak.” https://www.bleepingcomputer.com/news/security/yakult-australia-confirms-cyber-incident-after-95-gb-data-leak/
- SOCRadar (2024, June 20) “Dark Web Profile: DragonForce.” https://socradar.io/dark-web-profile-dragonforce-ransomware/
- Threat Intelligence Team (2024, January 11) Malwarebytes: “Ransomware review: January 2024.” https://www.malwarebytes.com/blog/threat-intelligence/2024/01/ransomware-review-january-2024
- Trend Research (2025, October 29) “Ransomware Spotlight: DragonForce.” https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-dragonforce

# References


- Tsipershtein, Mark; Ananin, Evgeny (2026, February 03) LevelBlue: “The Godfather of Ransomware? Inside DragonForce’s Cartel Ambitions.” https://www.levelblue.com/blogs/spiderlabs-blog/the-godfather-of-ransomware-inside-dragonforces-cartel-ambitions
- Walter, Jim (2025, May 02) Secureworks: “DragonForce Ransomware Gang | From Hacktivists to High Street Extortionists.” https://www.sentinelone.com/blog/dragonforce-ransomware-gang-from-hacktivists-to-high-street-extortionists/
- WatchGuard (n.d.) “DragonForce.” (Active). https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/dragonforce
- White, Marcus (2025, November 11) Specops: “DragonForce: Inside the Ransomware-as-a-Service Group.” https://specopssoft.com/blog/dragonforce-ransomware-as-a-service/


# Adversary Pursuit Group

blackpoint