THREAT PROFILE:

DragonForce Ransomware

TABLE OF CONTENTS

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:

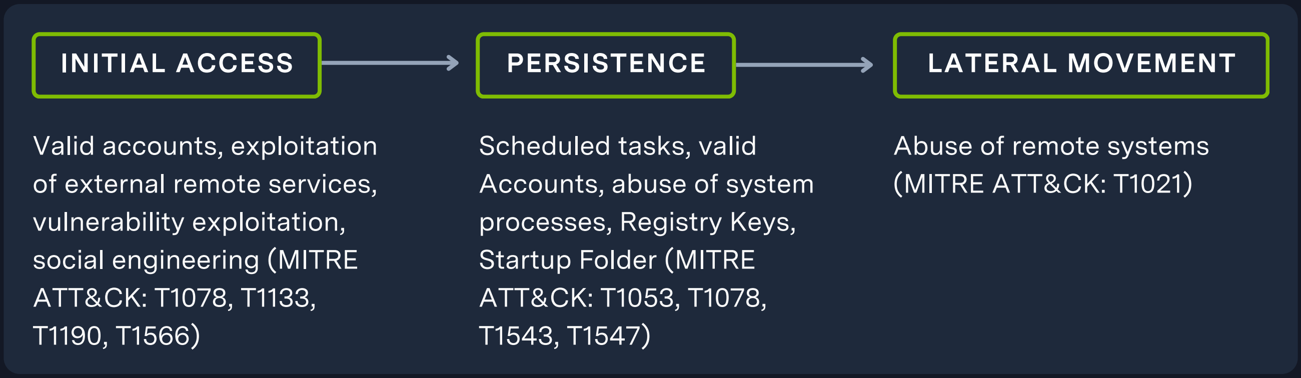
- Industrials (Manufacturing)

Most frequently targeted victim HQ region:

- North America

Known Associations:

- Conti Ransomware
- DragonForce Malaysia
- LockBit 3.0 Ransomware
- Ransombay Ransomware
- Ransomhub Ransomware
- Scattered Spider



INITIAL ACCESS

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

PERSISTENCE

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

LATERAL MOVEMENT

Abuse of remote systems (MITRE ATT&CK: T1021)

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.

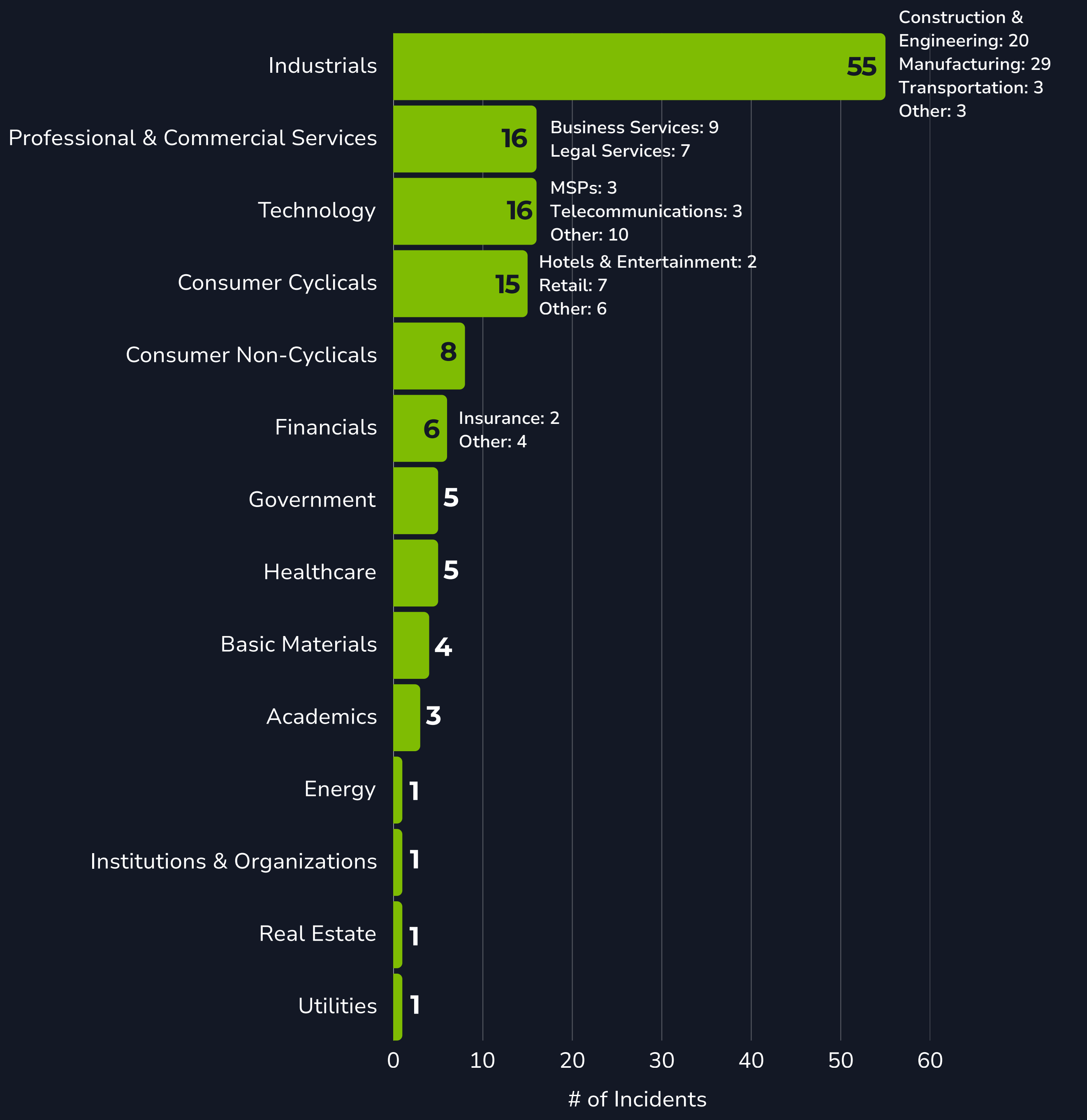
DragonForce ransomware maintains a Conti fork and LockBit 3.0 for variant of encryptors.

In 2025, DragonForce was reported to have launched a white-label ransomware cartel operation. The group reportedly offers infrastructure, malware, and support services for affiliates to launch campaigns under their own brand in exchange for 20% of the ransom payment.

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.

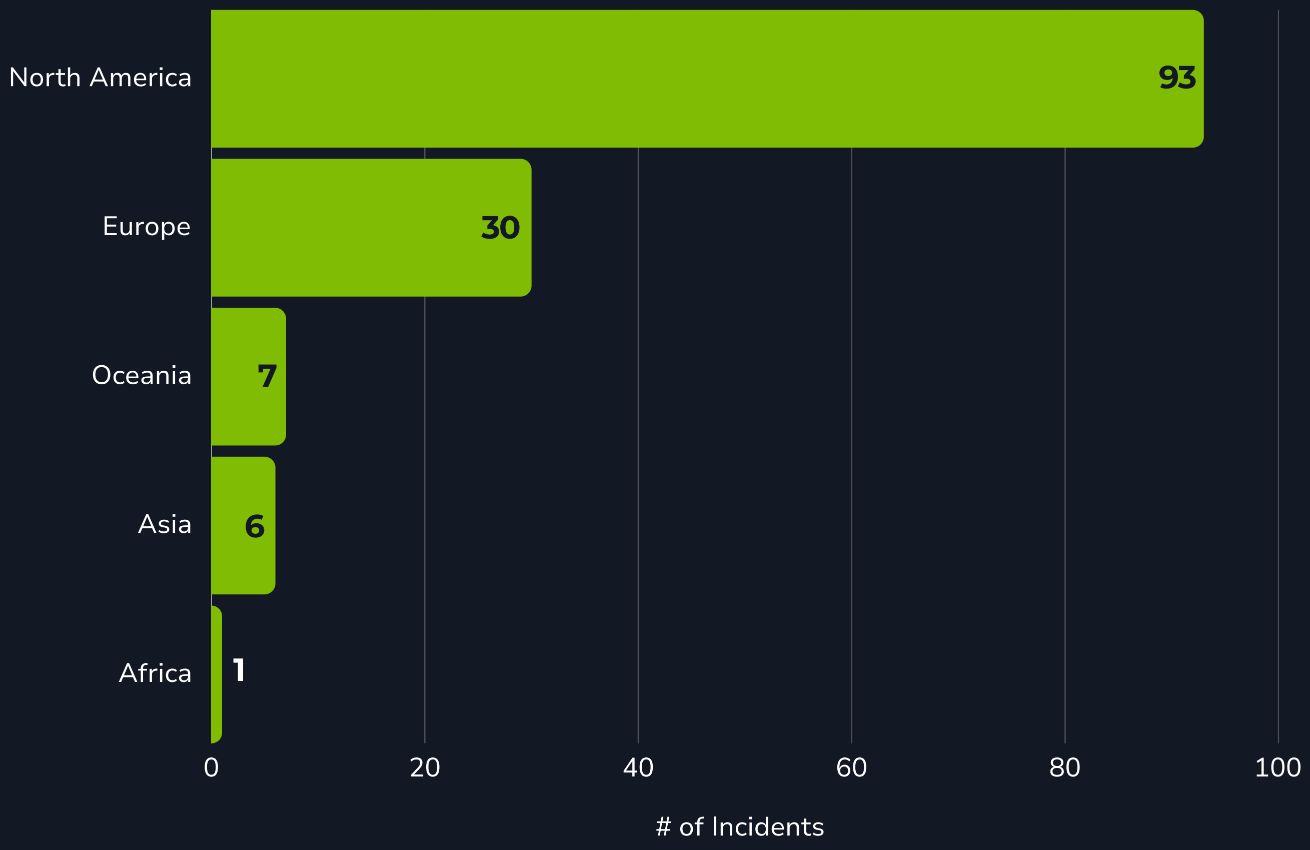
Previous Targets

Previous Industry Targets from 01 Jul 2024 to 30 Jun 2025

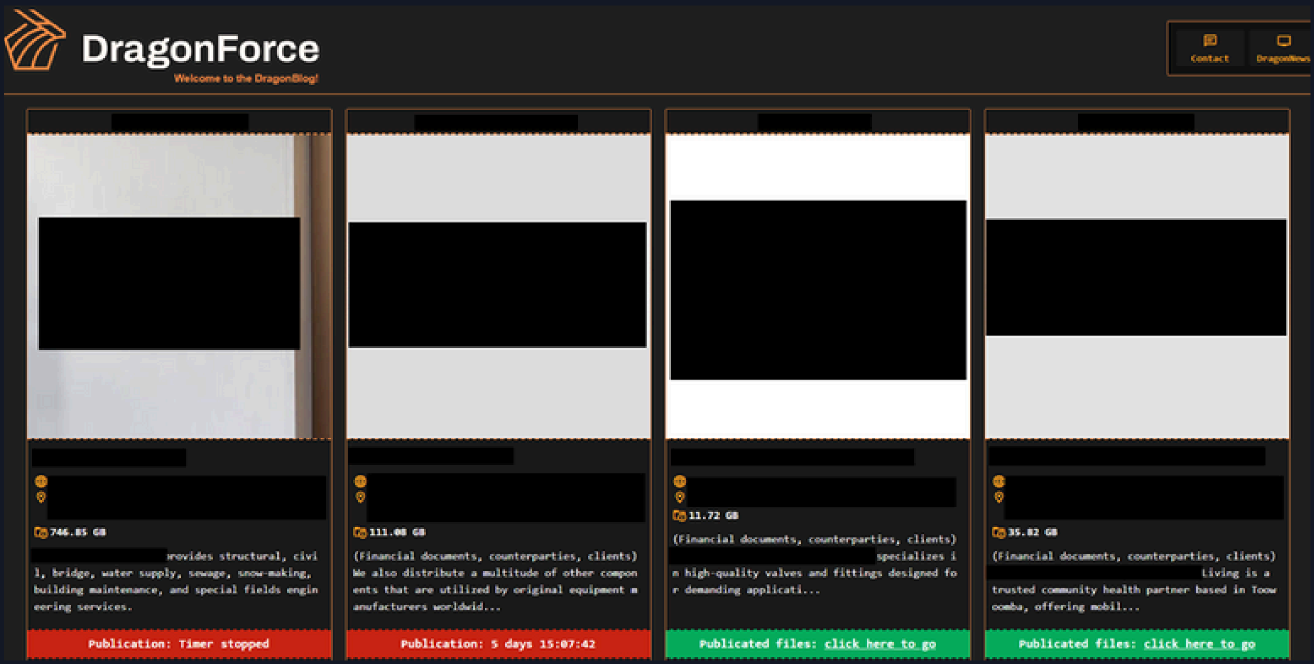


Previous Targets

Previous Victim HQ Regions from 01 Jul 2024 to 30 Jun 2025



Data Leak Site



[redacted]

[redacted]

[redacted]

[redacted]

746.85 GB

[redacted] provides structural, civil, bridge, water supply, sewage, snow-making, building maintenance, and special fields engineering services.

Publication: Timer stopped

[redacted]

[redacted]

[redacted]

[redacted]

111.08 GB

(Financial documents, counterparties, clients) We also distribute a multitude of other components that are utilized by original equipment manufacturers worldwid...

Publication: 5 days 15:07:42

[redacted]

[redacted]

[redacted]

[redacted]

11.72 GB

(Financial documents, counterparties, clients) [redacted] specializes in high-quality valves and fittings designed for demanding applicati...

Publicated files: click here to go

[redacted]

[redacted]

[redacted]

[redacted]

35.82 GB

(Financial documents, counterparties, clients) [redacted] Living is a trusted community health partner based in Toowoomba, offering mobil...

Publicated files: click here to go

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

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2021-44228	Hardcoded Cryptographic Key Vulnerability	Fortinet FortiOS	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-2024-21887	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-2024-57726	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

Associations

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.

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 3.0 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.

Ransombay Ransomware

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.

Known Tools

AdFind	A free command-line query tool that can be used for gathering information from Active Directory.
Advanced IP Scanner	A fast and powerful network scanner with a user-friendly interface. It can locate all computers on your wired or wireless local network and scan their ports.
At	A Windows command that can be used to schedule a command, a script, or a program to run at a specified date and time.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
MEGA	A cloud storage and file hosting service. The service is frequently used to host exfiltrated data from victims.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
PingCastle	A tool used to enumerate AD and provides an AD map to visualize the hierarchy of trust relationships.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
Rogue Killer Antirootkit Driver	A security tool that can be used to terminate and remove malicious processes and programs from a computer. Threat actors can abuse the tool to remove or terminate processes during an intrusion.
schtasks	A utility used to schedule execution of programs or scripts on a Windows system to run at a specific date and time.
SoftPerfect	A network scanner that can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices.

Known Tools

SystemBC	AKA Coroxy. A malware written in C that turns infected computers into SOCKS5 proxies.
Windows Restart Manager	A library for reducing required reboots during software updates. The tool is often used by threat actors to support the encryption process and retrieve processes running on the system.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.

Observed Behaviors: Windows

Tactic	Commands Observed
Persistence	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\socks5 ‘powershell.exe -windowstyle hidden -Command & ‘path_to_executable_file’

Privilege Escalation	DuplicateTokenEx()
	CreateProcessWithTokenW()

Defense Evasion	**ZwOpenProcess()**
	ZwTerminateProcess()
	SELECT * FROM Win32_ShadowCopy
	cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy where "ID='%s'" delete

Impact	CryptGenRandom()

Observed Behaviors: Linux

Tactic	Commands Observed
Execution	-paths: force run in file-system search mode -vmsvc: force run in ESXi vim-cmd discovery mode -n: do not perform encryption/description (file discovery only) -h H -m M -s S: wait H hours, M minutes, S seconds before starting -e M X Y: encryption mode M with parameters X and Y -p PATH: override file-system paths for discovery -l LOGFILE: override the log-file location -i X: override the number of threads -q: disable output to STDOUT -v: verbose logging -vwi ID: override list of ignored VMs by ID -vwn NAME: override list of ignored VMs by name

MITRE ATT&CK® Mappings

Resource Development	
T1588: Obtain Capabilities	
Initial Access	
T1078: Valid Accounts	
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .004: Spearphishing Voice
Execution	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1204: User Execution	.002: Malicious File
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	
T1134: Access Token Manipulation	

MITRE ATT&CK® Mappings

Defense Evasion	
T1027: Obfuscated Files or Information	
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion
T1562: Impair Defenses	.001: Disable or Modify Tools
Credential Access	
T1003: OS Credential Access	.001: LSASS Memory
Discovery	
T1016: System Network Configuration Discovery	
T1018: Remote Services Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1482: Domain Trust Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol
Collection	
T1560: Archive Collected Data	

MITRE ATT&CK® Mappings

Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1090: Proxy	
T1105: Ingress Tool Transfer	
Impact	
T1486: Data Encrypted for Impact	
T1657: Financial Theft	

References

- 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/
- 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
- 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
- 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

Adversary Pursuit Group

blackpoint