


# How RMM abuse fuelled Medusa & DragonForce attacks

 [zensec.co.uk/blog/how-rmm-abuse-fuelled-medusa-dragonforce-attacks](https://zensec.co.uk/blog/how-rmm-abuse-fuelled-medusa-dragonforce-attacks)

Francesca Rondeau

October 30, 2025



If you are reading this because you have experienced a ransomware incident and are unsure how to deal with it, [contact Zensec](#) immediately.

## Summary

In early 2025, Zensec investigations uncovered a wave of ransomware incidents exploiting the SimpleHelp Remote Monitoring and Management (RMM) platform, a tool trusted by Managed Service Providers (MSPs) and software vendors worldwide. Threat actors, including the Medusa and DragonForce ransomware groups, weaponised a trio of vulnerabilities ([CVE-2024-57726](#), [CVE-2024-57727](#), and [CVE-2024-57728](#)) to gain downstream access into customer environments.

By compromising third-party RMM servers running as SYSTEM, attackers achieved full control over victim networks, deploying discovery tools, disabling defences, exfiltrating data via RClone and Restic, and finally encrypting systems.

These campaigns illustrate a growing reality: your security is only as strong as your supplier's patch hygiene. This report breaks down how two ransomware RaaS groups used exploited SimpleHelp instances, what tools and tactics they used, and what every organisation should do now to defend against similar supply-chain intrusions.

This report is split into two parts for both ransomware groups.

## Background on SimpleHelp

---

SimpleHelp is a remote monitoring and management (RMM) platform commonly used by MSPs and software suppliers to manage customer endpoints and servers. From January 2025 onward multiple intrusions traced back to compromised SimpleHelp servers running unpatched versions affected by [CVE-2024-57726](#) / [CVE-2024-57727](#) / [CVE-2024-57728](#).

Where the controlling RMM within environments ran as SYSTEM, attackers could act with a high level of privilege including that of key assets (e.g. domain controllers) and reach downstream customers with minimal friction. Patches for SimpleHelp have been available and exploits dubbed “Severe” by the RMM software vendor.

## Who abused SimpleHelp for ransomware deployment?

---

**Medusa** – In Q1 2025, multiple UK organisations fell victim to a coordinated ransomware campaign by the Medusa ransomware RaaS. The attackers leveraged vulnerabilities in the SimpleHelp Remote Monitoring and Management (RMM) tool to gain initial access via suppliers and MSPs using their own tools to manage customers. From there the threat actor pivoted into victim networks. In half of the cases data was exfiltrated using RClone before encryption, with large outbound data spikes being observed and file tree listings appearing on Medusa’s dark web leak site days later. Across all attacks, systems were encrypted with the “.MEDUSA” file extension, and ransom notes titled “!!!!READ\_ME\_MEDUSA!!!!.txt” were left on infected machines.

**Dragon Force** – In Q2 2025, multiple UK organisations fell victim to a coordinated ransomware campaign by the Dragon Force ransomware as a Service (RaaS) group. They’re a relatively new group starting up in 2023. The attackers leveraged vulnerabilities in the SimpleHelp Remote Monitoring and Management (RMM) tool to gain initial access to supplier controlled RMM tools. From there the threat actor pivoted into victim networks. In all cases observed by ZenSec data was exfiltrated using a tool called Restic before encryption, with large outbound data spikes being observed. Across all attacks, systems were encrypted with the “\*.dragonforce\_encrypted” file extension, and ransom notes titled “readme.txt” were left on infected machines. In these cases, file names were also obscured with the random characters equalling the same length of characters as the original file name.

## Medusa campaign analysis

---

### Initial access & abuse of SimpleHelp

In all observed incidents the initial access vector was an unpatched or misconfigured SimpleHelp RMM instance belonging to a third-party supplier or MSP. Because all observed instances of SimpleHelp installs run with SYSTEM-level privileges, attackers were able to use the compromised controlling RMM server of the third-party as a staging point to reach downstream customer environments with minimal friction once logged into the victims to perform the attack.

### Execution and lateral movement

Once into the network using SimpleHelp the threat actor Medusa deployed multiple service installations for PDQ Inventory and PDQ Deploy which were observed in half of the cases. These tools were then utilised to execute the ransomware payloads “Gaze.exe” or “REDACTED.exe” where the redacted name is that of the target organisation. Gaze is also referenced in multiple other MEDUSA public sources including CISA reports.

### PDQ Deploy Weaponisation

PDQ Deploy was leveraged to push and run base64-encoded PowerShell commands that disabled or altered Microsoft Defender and added Defender exclusions.

*Figure 1 – Encoded*

*Figure 2 – Decoded*

PDQ was also used to add exclusions and modify Windows Defender utilising the following PowerShell commands:

Figure 3

In the remaining cases, the ransomware payload was directly executed via the RMM tool SimpleHelp without PDQ being required.

## Discovery tooling

---

Early in some intrusions the actors ran network discovery tooling such as netscan.exe to enumerate hosts and services, enabling targeted lateral movement and prioritisation of high-value targets (file servers, backup servers, domain controllers).

## Persistence and C2 (Command and Control)

---

While the SimpleHelp compromise often provided sufficient access, in several cases attackers added additional remote management/C2 channels:

- AnyDesk was installed and used for interactive control in some incidents (binary observed as AnyDesk.exe).
- In at least one incident the attackers repointed SimpleHelp clients to a threat-actor-controlled SimpleHelp server (observed IP: 213[.]183.63.41) to maintain access independent of the initial vendor instance.

Because SimpleHelp runs as SYSTEM in many deployments, these actions provided robust, high-privilege persistence without the need for any further C2.

## Exfiltration

---

The threat actor group Medusa used RClone for file theft, renaming the binary to evade naive detections (observed as lsp.exe). In the cases we analysed RClone was used with filters to transfer files matching specific age/size criteria (e.g., “files over 1500 days old and under 1500MB”, a likely attempt to prioritise user data while avoiding very large unneeded data). Operators also removed RClone configuration files post-exfiltration to hinder forensic recovery.

Note: ZenSec observed exfiltration in approximately 50% of the Medusa incidents analysed; in other cases, the campaign relied on encryption-only disruption. The attackers deleted RClone configuration files after execution to hinder forensic recovery.

The following commands were used with Rclone (lsp.exe) after a successful RDP session to the file servers within the environment.

## Encryption and impact

---

Encryption occurred on the majority of online systems within the victims networks facilitated manually or via PDQdeploy. In addition, multiple defence evasion techniques using PowerShell to disable Defender and “2Gk8.exe” with related drivers also inhibited traditional AV products. One driver utilised that goes by multiple names “smuot.sys” and “CSAgent.sys” has been dubbed as Abyssworker by Elastic Security Labs.

Where encryption had taken place, the ransomware readme was dropped as “!!!READ\_ME\_MEDUSA!!!.txt” and files encrypted were appended with the following extension “.MEDUSA”.

Sorry to interrupt your busy business.

## WHAT HAPPEND?

1. We are the best Ransomware Group MEDUSA.

Please stay calm if you are not the manager of **IT service provider of your company. (Call group II members)**  
In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to several companies they manage!  
You're running a highly valued business and your data was very crucial. But it's in danger now.  
Please ask your IT service provider to solve this.

2. We have ENCRYPTED your files.

While you are reading this message, it means your files and data has been ENCRYPTED by world's strongest ransomware. Your files have encrypted with new military-grade encryption algorithm and you can not decrypt your files. But don't worry, we can decrypt your files.

There is only one possible way to get back your computers and servers, keep your privacy safe - CONTACT us via LIVE CHAT and pay for the special MEDUSA DECRYPTOR and DECRYPTION KEYS.  
This MEDUSA DECRYPTOR will restore yours and client's entire network within 24 hours.

## WHAT GUARANTEES?

We can post all of your critical data to the public and send emails to your competitors.

We have professional OSINTs and media team for leak data to telegram, facebook, twitter channels and top news websites. You can easily search about us. You can suffer significant problems due to disastrous consequences, leading to loss of valuable intellectual property and other sensitive information, costly incident response efforts, information misuse/abuse, loss of customer trust, brand and reputational damage, and legal and regulatory issues.

After paying for the data breach and decryption, we guarantee that your data will never be leaked and make everything silent, this is also for our reputation.

YOU should be AWARE!

We will speak only with an authorized person. It can be the CEO, top management etc.  
Inform your supervisors and stay calm!

If you do not contact us within 48 hours, We will start publish your case to our official blog and everybody will start notice your incident!

<https://t.me/+lyskiDn9KiYxZj1h>

```
-----[ Official blog tor address ]-----
Using TOR Browser(https://www.torproject.org/download/):
```

http://xfv4jzckytb4g3ckwemcny3ihv4i5p4lqzdp1624cxisu35my5fwi5qd.onion/  
http://s7lmmhlt3iwnwirxvgjidl6omcblvw2rg75txjfdy73kx5brlmiulad.onion/

## Post-encryption activity & leak site behaviour

Medusa operates as a Ransomware-as-a-Service (RaaS) and commonly enacts double extortion. Victim organisations were listed on the group's data leak site with "proof-of-life" packs: screenshots, document previews, and browsable file trees. The leak site and peripheral Telegram channels were used to pressure victims and sometimes to publish larger sets of stolen data.



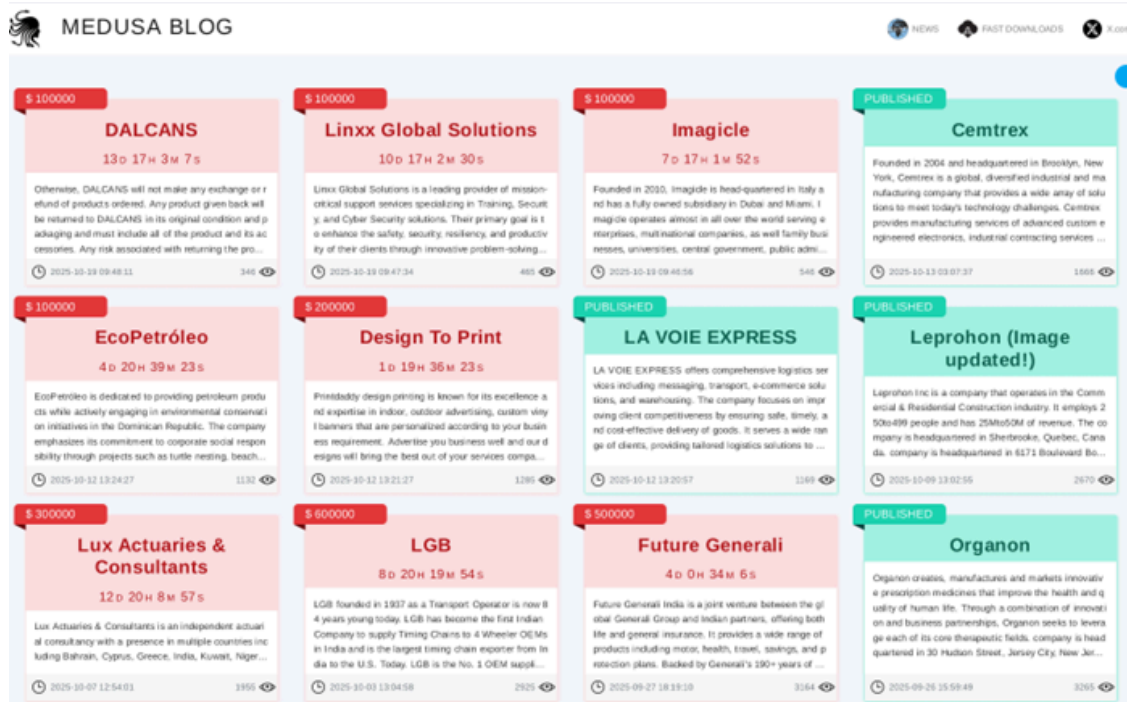


Figure 4 – [https://s7lmmhlt3iwnwirxvgjidl6omcblvw2rg75txjfdy73kx5brlmiulad\[.\]onion/](https://s7lmmhlt3iwnwirxvgjidl6omcblvw2rg75txjfdy73kx5brlmiulad[.]onion/)

Until recently the data wasn't directly published to the darknet leak site other than proof of life data however various telegram channels linked to the group listed the files such as the previously linked telegram channel named "information support aka OSINT without borders".

The Medusa leak site is functional at the time of writing with many victims published. The link is found at the top of the site hyperlinked. Alongside the DLS link is a link for osintcorp[.]net a site no longer available and last indexed by the Internet Archive (Wayback Machine) in April 2025. This site was an online presence for the group pretending to be a cyber security news site. The threat actors would public videos to this site documenting the leaks sometimes as long as 20 minutes long scrolling through documents of victims.

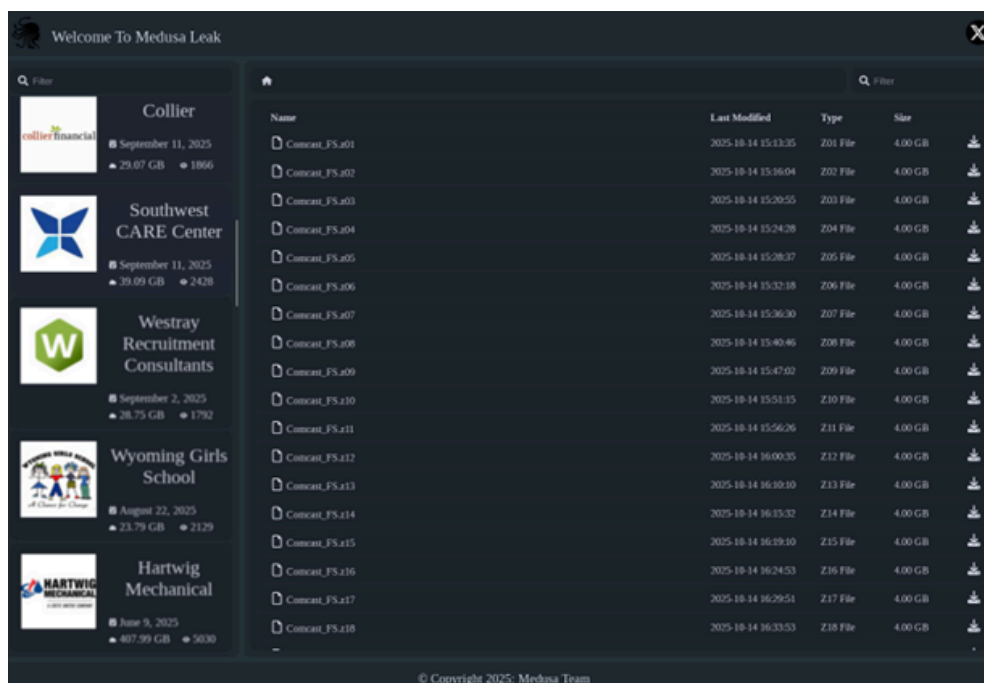
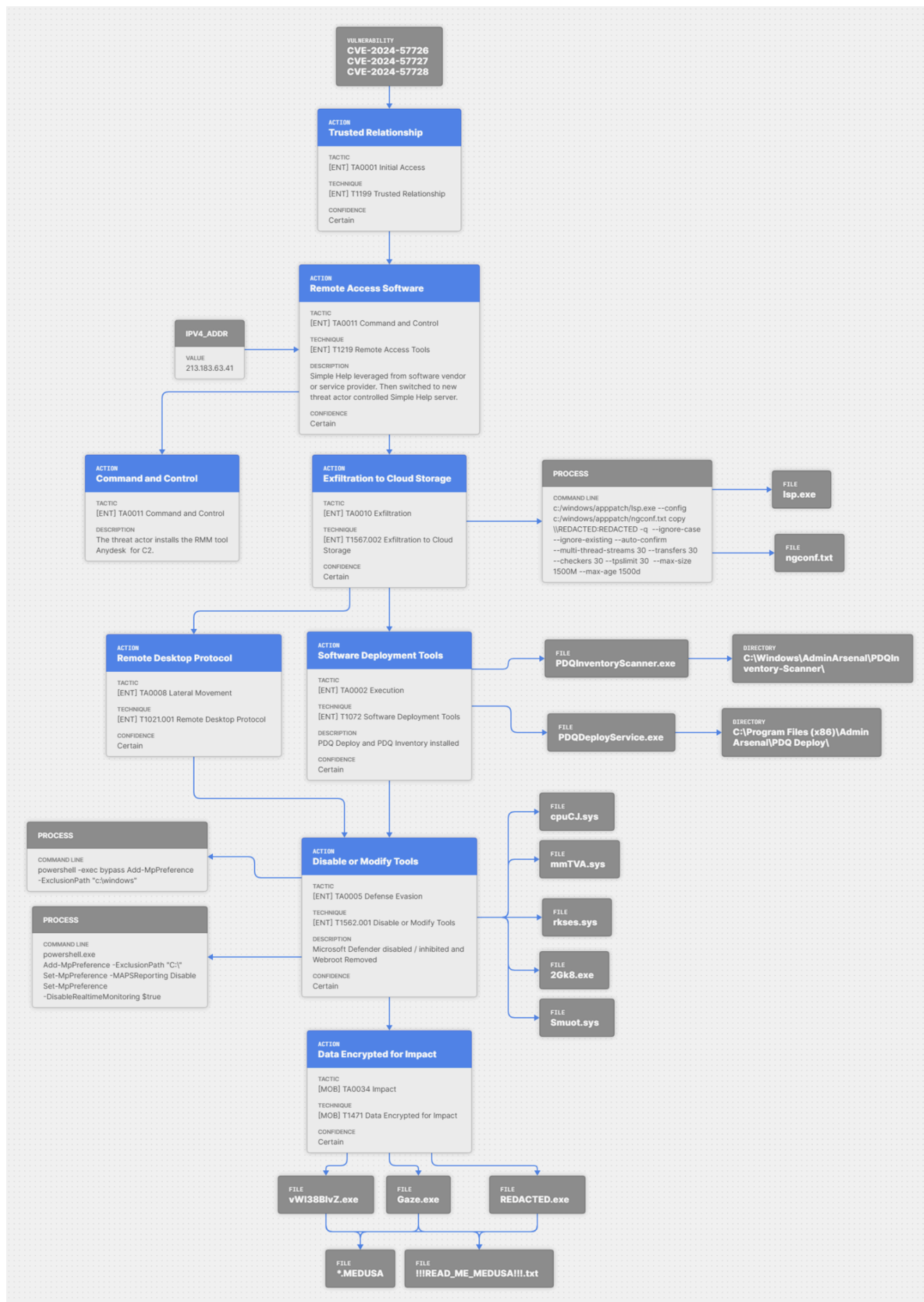


Figure 5 – [https://7aqabivkwmpvjkyefonf3gpy5gsubopqni7kcirsrq3pflckxq5zz4id\[.\]onion/](https://7aqabivkwmpvjkyefonf3gpy5gsubopqni7kcirsrq3pflckxq5zz4id[.]onion/)

## Medusa Mitre Attack Flow Map

---

The full map can be seen [here](#).



## DragonForce campaign analysis

---

### Initial access via abused RMM

In the observed incidents DragonForce similarly abused compromised SimpleHelp installs belonging to MSPs and third-party suppliers. Using the elevated access afforded by those RMM instances, operators installed additional remote access tools (notably AnyDesk) and created local administrator accounts “admin” to retain interactive control and simplify lateral movement.

Because compromised RMM instances often run with SYSTEM privileges, DragonForce’s operator-controlled agents could transfer files, run tooling, and stage payloads without needing additional command and control or additional persistence in most cases.

Additionally in order to run tooling and ingress malicious files into the environment DragonForce disabled security protections like Microsoft Defender on systems.

### Credential harvesting from Veeam

To escalate access and harvest backup credentials, DragonForce operators executed credential-harvesting scripts targeting Veeam backup servers. Variants of Get-Veeam-Creds.ps1 were used to extract plaintext credentials from Veeam SQL password stores and configuration artefacts.

### Exfiltration

Unlike the Medusa cases where RClone was common, DragonForce frequently used Restic, an open source backup tool to move data offsite. Restic supports multiple backends (S3-compatible endpoints, SFTP, Azure, Google Cloud), and in the incidents we reviewed the group targeted S3-compatible storage with references to wasabisys[.]com (a known S3-compatible cloud storage provider and backup provider). Essentially the victims were provided an unscheduled off-site backup. In jest this is the threat actor exfiltrating the data to their controlled storage.

The service URLs matched that of those on Wasabi products storage regions found here <https://docs.wasabi.com/docs/what-are-the-service-urls-for-wasabi-s-different-storage-regions>. Restic was launched with PowerShell by the threat actor.

### Encryption / Impact

The ransomware payload was launched using the threat actor created accounts, in cases examined ransomware payloads can be called “organisation name.exe” where the file name is specific to the company and “win.exe”. File ingress of the ransomware payload can be seen using the built in functionality of SimpleHelp file transfer.

Encryption occurred on the majority of online systems within the victim’s networks facilitated manually in the cases witnessed targeting Hyper-V VHDX files of servers.

As ordinarily encountered in ransomware attacks, the DragonForce ransomware payload places a ransom note on the affected system(s) with details of what has occurred, what not to do and how to contact them, as well as the consequences of failing to negotiate a settlement. During this attack, a ransom note named “readme.txt” was placed in numerous folders on the various systems upon which encryption had taken place. Files encrypted were appended with the following extension “\*.dragonforce\_encrypted” and file names obscured with random characters. It is a ransom note with no direct reference to the client and contains a link to follow on how to contact the ransomware group via a TOX ID chat.



```

Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are not associated with politics. All you need to do is contact us and pay.

--- Our communication process:

1. You contact us.
2. We send you a list of files that were stolen.
3. We decrypt 1 file to confirm that our decryptor works.
4. We agree on the amount, which must be paid using BTC.
5. We delete your files, we give you a decryptor.
6. We give you a detailed report on how we compromised your company, and recommendations on how to avoid such situations in the future.

--- Client area (use this site to contact us):

Link for Tor Browser: http://3pktcrbcmssvrme5skburdwe2h3v6ibdn5kbjgihsg6eu6s6b7ryqd.onion
>>> Use this ID: ██████████ to begin the recovery process.

* In order to access the site, you will need Tor Browser,
  you can download it from this link: https://www.torproject.org/

--- Additional contacts:

Support Tox: ██████████

--- Recommendations:

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.

--- Important:

If you refuse to pay or do not get in touch with us, we start publishing your files.
18/04/2025 00:00 UTC the decryptor will be destroyed and the files will be published on our blog.

Blog: http://z3wqggtxtft7id3ibr7srivv5gjof5fwg76slewnzwakjuf3nlhukdid.onion

```

Figure 6

## Post Encryption

DragonForce operates as a RaaS and carries out double extortion. Victims are first previewed or listed on a public-facing blog, then later published to a data leak site (DLS) where files are browsable and downloadable.

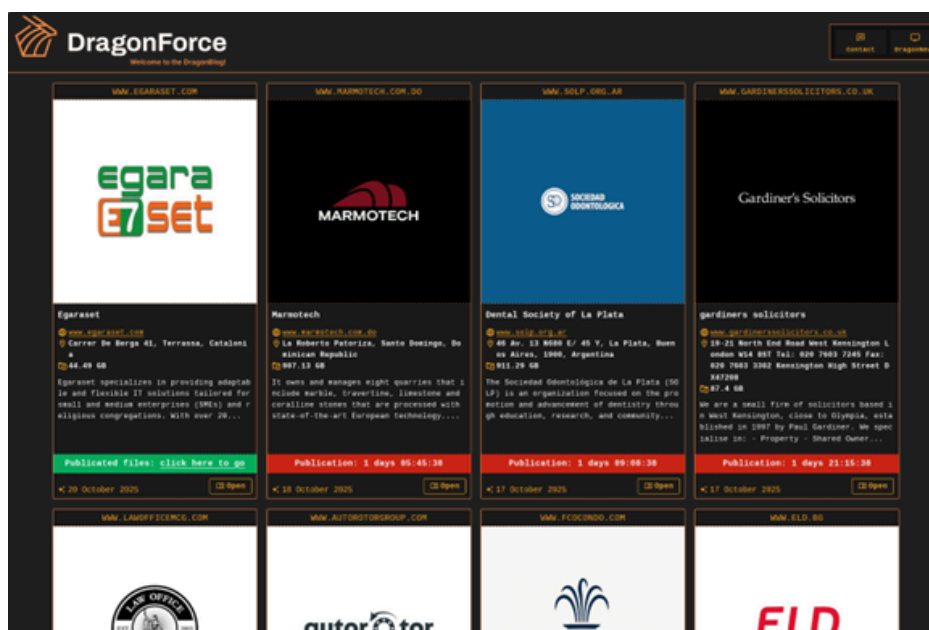


Figure 7 – Blog site – z3wqggtxtft7id3ibr7srivv5gjof5fwg76slewnzwakjuf3nlhukdid[.onion]


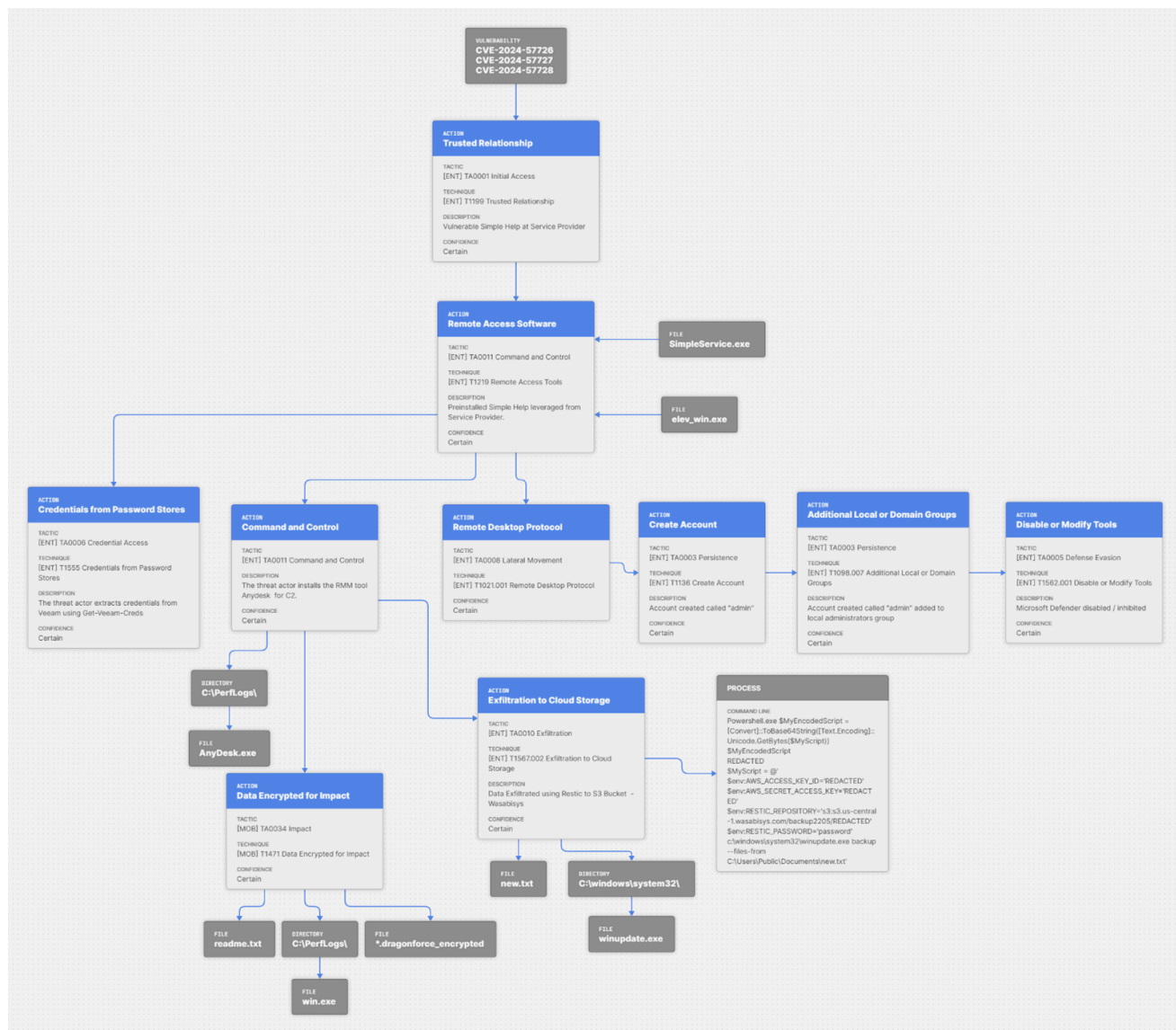
 <b>DragonForce</b> Welcome to the DragonFiles!		
<a href="#">gardeners solicitors (gardenerssolicitors.co.uk)</a>	2025-10-25 08:30:00 UTC	87G
<a href="#">Dental Society of La Plata (www.solp.org.ar)</a>	2025-10-24 20:23:00 UTC	911G
<a href="#">Marmotech (www.marmotech.com.do)</a>	2025-10-24 17:00:00 UTC	907G
<a href="#">Autorotor (www.autorotorgroup.com)</a>	PUBLISHED	125G
<a href="#">Fountains Condominium Operations (www.fcocondo.com)</a>	PUBLISHED	454G
<a href="#">The Law Offices of Michael C. George (www.lawofficemcg.com)</a>	PUBLISHED	443G
<a href="#">Express Logistics and Distribution Ltd (eld.bg)</a>	PUBLISHED	578G
<a href="#">Egaraset (egaraset.com)</a>	PUBLISHED	44G
<a href="#">Downes (downesbrokerage.com.au)</a>	PUBLISHED	99G
<a href="#">LC Informatique Sàrl (lc-informatique.ch)</a>	PUBLISHED	1G
<a href="#">Grupo Serex (gruposerex.com)</a>	PUBLISHED	111G
<a href="#">Asserson (asserson.co.uk)</a>	PUBLISHED	388G
<a href="#">FTCS Forage (ftcs-forage.com)</a>	PUBLISHED	193G
<a href="#">Greenville Legal (www.greenvillelegal.com)</a>	PUBLISHED	3075G
<a href="#">Allgäu Stern Hotel (allgaeustern.de)</a>	PUBLISHED	13G
<a href="#">Engineered Advantage (www.eapsc.net)</a>	PUBLISHED	249G
<a href="#">Cardinal Machinery (www.cardinalmachinery.com)</a>	PUBLISHED	104G
<a href="#">Caprez Ingenieure AG (www.caprez-ing.ch)</a>	PUBLISHED	747G
<a href="#">Memphis Millwork (memphismasterworks.com)</a>	PUBLISHED	109G
<a href="#">Rothmann Immobilien (engelvoelkers.de)</a>	PUBLISHED	103G
<a href="#">Engineered Components (engcomponents.com)</a>	PUBLISHED	111G
<a href="#">Concord New Energy Group (cn.cnegroup.com)</a>	PUBLISHED	109G
<a href="#">Grupo DIRIA (www.grupodiria.com)</a>	PUBLISHED	148G
<a href="#">The Smile Spa (www.drrussosmilesipa.com)</a>	PUBLISHED	65G
<a href="#">Provalve Armaturen GmbH &amp; Co. KG (provalve.de)</a>	PUBLISHED	12G
<a href="#">Toowoomba Friendly Society Dispensary (tfsd.com.au)</a>	PUBLISHED	36G
<a href="#">Hilco Metal Building &amp; Roofing Supply (hilcosupply.com)</a>	PUBLISHED	94G

Figure 8 – Data Leak Site – dragonforxxbp3awc7mzs5dkswrua3znqyx5roefmi4smjrdsi22xwqd[.]onion

## DragonForce Mitre Attack Flow Map

The full map can be seen [here](#).



## IOCs

### Medusa ASNs observed

ASN	Org
AS56630	Melbikomas UAB

### Medusa Network IOCs

IP Address	Description
213[.]183.63.41	Threat actor-controlled SimpleHelp server used for C2.

### Medusa File-based IOCs

Filename	SHA256	Note
----------	--------	------

gaze.exe		Ransomware Payload
2Gk8.exe	df6cb5199c272c491b3a7ac44df6c4c279d23f7c09daed758c831b26732a4851	Inhibit AV
COMPANY NAME.exe		Ransomware Payload
0ZI9.exe		Ransomware Payload
vWI38BlvZ.exe		Ransomware Payload
Smuot.sys	b7703a59c39a0d2f7ef6422945aaeaaf061431af0533557246397551b8eed505	Related to 2Gk8.exe. Driver to inhibit AV.
cpuCJ.sys	89d473ad486e144f3c71ad95ed6016248613fc33d76792e8632206cea86ecfdd	Driver to inhibit AV.
mmTVA.sys		Driver to inhibit AV
rkses.sys		Driver to inhibit AV
lsp.exe		Rclone
ngconf.txt		Rclone Config
PDQInventoryScanner.exe		PDQ Inventory
PDQInventory-Scanner-1.exe		PDQ Inventory
PDQDeployService.exe		PDQ Deploy
Netscan.exe		Netscan network discovery tool
!!!READ_ME_MEDUSA!!!.txt		Ransomware Readme

**DragonForce ASNs observed**

ASN	Org
AS209132	Alviva Holding
AS57509	L&L Investment

### DragonForce Network IOCs

IP Address	IoC
179[.]60.146.40	TA infrastructure used to conduct majority of attack via SimpleHelp Cobalt Strike C2 server.
91[.]191.209.110	Cobalt Strike C2 server.

### DragonForce File-based IOCs

Filename	SHA-256	Note
[REDACTED COMPANY NAME].exe		Ransomware Payload
AnyDesk.exe	aea8f85e569443a8c00b94fa19b5155b9122183f05bedfdcdccd1d18451760fd	RMM tool install
win.exe		Ransomware Payload
SimpleService.exe	e414f781c73f6984158f5d12af9f89c57d993e8db0322ebc0da346179a8b9e2d	SimpleHelp existing install prior to TA
elev_win.exe		SimpleHelp existing install prior to TA
winupdate.exe	98394683d8f30ce9fb313100f593dc16e97a52723b18d534cf586391a97cdc1d	Restic exfiltration tool

### Recommendations for all organisations

- Ensure your vendors and suppliers that use SimpleHelp are on the latest version of at least (5.5.13) which covers the latest known vulnerabilities
- Monitor for Anomalous RMM Behaviour E.g. Track unusual user creation, file transfers, process launches, and new service installs.
- Require vendors to maintain patch compliance and MFA.

- Audit all RMM tools in use across your organisation using network telemetry and software management tools to identify outliers.

Once you have a list of tools review their use and why it is there.

- Block unused or untrusted RMM tools with application whitelisting and firewall application filtering.
- There are many tools out there a good project to review or use for threat hunting is LOLRMM which tracks 276 total tools. <https://lolrmm.io>
- Consider implementing monitoring for security alerts 24/7
- Ensure on-site backups are not domain-joined.
- Ensure backup products are patched to the latest level.
- Ensure off-site immutable backups are in place.
- Monitor for new RMM tool use
- Where possible, block unknown RMM tools and monitor existing RMM tool use.
- Ensure EDR is implemented across the whole estate to monitor for unusual PowerShell commands, discovery tooling and exfiltration tooling.

## References:

---

- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a>
- <https://www.elastic.co/security-labs/abyssworker>
- <https://www.security.com/threat-intelligence/medusa-ransomware-attacks>
- <https://www.bleepingcomputer.com/news/security/hackers-exploiting-flaws-in-simplehelp-rmm-to-breach-networks/>
- <https://simple-help.com/kb—security-vulnerabilities-01-2025#send-us-your-questions>