GROUP-IB

← Blog

Nikolay Kichatov

Cyber Intelligence Analyst, Group-IB (APAC)

Inside the Dragon: DragonForce Ransomware Group

In this blog, we look at the DragonForce ransomware group, which poses a severe threat with two variants—a LockBit fork and a customized Conti fork with advanced features and SystemBC malware.

September 25, 2024 · min to read · Ransomware

Conti DragonForce LockBit Ransomware

Introduction

In light of the escalating frequency and complexity of ransomware attacks, are security leaders confident in their organization's defenses? According to Group-IB's Hi-Tech Crime Trends 2023/2024 Report, ransomware will have an increasingly significant impact in 2024 and beyond. Key trends driving this include the expansion of the Ransomware-as-a-Service (RaaS) market, the proliferation of stolen data on Dedicated Leak Sites (DLS), and a rise in affiliate programs.

Furthermore, the evolution of ransomware variants is outpacing the advancements in cyber defence, leaving organizations unprepared for the threats on the horizon. To stay ahead, businesses must stay updated on the most pressing cybersecurity threats, and prominent threat actors that have recently emerged and continue to pose significant risks this year and in the future.

In this blog, we delve into the inner workings of the **DragonForce ransomware group**. Discovered in August 2023, DragonForce has been targeting companies in critical sectors using a variant of a leaked LockBit3.0 builder, and more recently in July 2024 with their own variant of ransomware.

Key discoveries in this blog

DragonForce Ransomware Overview and Tactics: DragonForce operates a Ransomware-as-a-Service (RaaS) affiliate program utilizing a variant of LockBit3.0, and the other, though initially claimed as original, is based on ContiV3. The group employs double extortion tactics, encrypting data, and threatening leaks unless a ransom is paid.

Affiliate Program and Customizable Ransomware: The affiliate program, launched on 26 June 2024, offers 80% of the ransom to affiliates, along with tools for attack management and automation. Affiliates can create customized ransomware samples, including disabling security features, setting encryption parameters, and personalizing ransom notes.

Security Bypass Techniques and Defense Evasion: DragonForce uses the “Bring Your Own Vulnerable Driver” (BYOVD) technique, included in their Conti variant of ransomware, to disable security processes and evade detection. Additionally, they clear Windows Event Logs post-encryption to hinder forensic investigations and obscure their tracks.

Targeted Industries and Ransomware Payload Analysis: Between August 2023 and August 2024, DragonForce targeted 82 victims across various industries, focusing on Manufacturing, Real Estate, and Transportation industries. The ransomware payload features advanced encryption techniques and anti-analysis countermeasures.

SystemBC, Cobalt Strike, and Network Reconnaissance: The DragonForce ransomware group utilizes the SystemBC backdoor for persistence, Mimikatz and Cobalt Strike for credential harvesting, and Cobalt Strike for lateral movement. The group also uses network scanning tools like SoftPerfect Network Scanner to map networks and facilitate the spread of ransomware.

What is DragonForce Ransomware?

DragonForce is a Ransomware-as-a-Service (RaaS) affiliate program that now uses 2 versions of ransomware to target its victims. Many DragonForce ransomware attacks are customized to each victim to maximize its impact. To do this, the threat actors can leverage tactics such as changing the filename extensions of encrypted files, and terminating specific processes and services. Its ransomware builder allows affiliates the capability to specify exactly which processes the ransomware should terminate, to ensure the successful encryption of all important data on the victim's devices.

Based on the observations by Group-IB's Threat Intelligence analysts, DragonForce advertises their ransomware on the dark web. It has a proprietary DLS that contains unique company IDs and leaked account details.

The operators of DragonForce utilize a double extortion technique, where they exfiltrate a victim's sensitive data in addition to encrypting it. They then demand ransom payment from their victims in return for a decryptor, and the "promise" that their stolen data will not be released.. This dual-pronged approach of losing both access to their data as well as having their confidential information exposed adds significant pressure on the victim to comply with the attackers' demands as there might be potential damage to their reputation, privacy, or business continuity if their data is made public.

From August 2023 to August 2024, DragonForce ransomware listed a total of 82 victims on their Dark Web site. Of these, 43 attacks occurred in the United States, making up 52.4% of the incidents. Other significant targets included the United Kingdom with 10 attacks (12.2%) and Australia with 5 attacks (6%).

Figure 1. Heatmap of targeted countries by DragonForce ransomware and its affiliates.

The manufacturing industry was the most targeted, with 12 attacks accounting for 14.6% of the total incidents. The Real Estate sector followed as the second most attacked, experiencing 11 incidents, which represents 13.4% of the total. The third most affected industry was Transportation, with 10 attacks, making up 12.2% of the total.

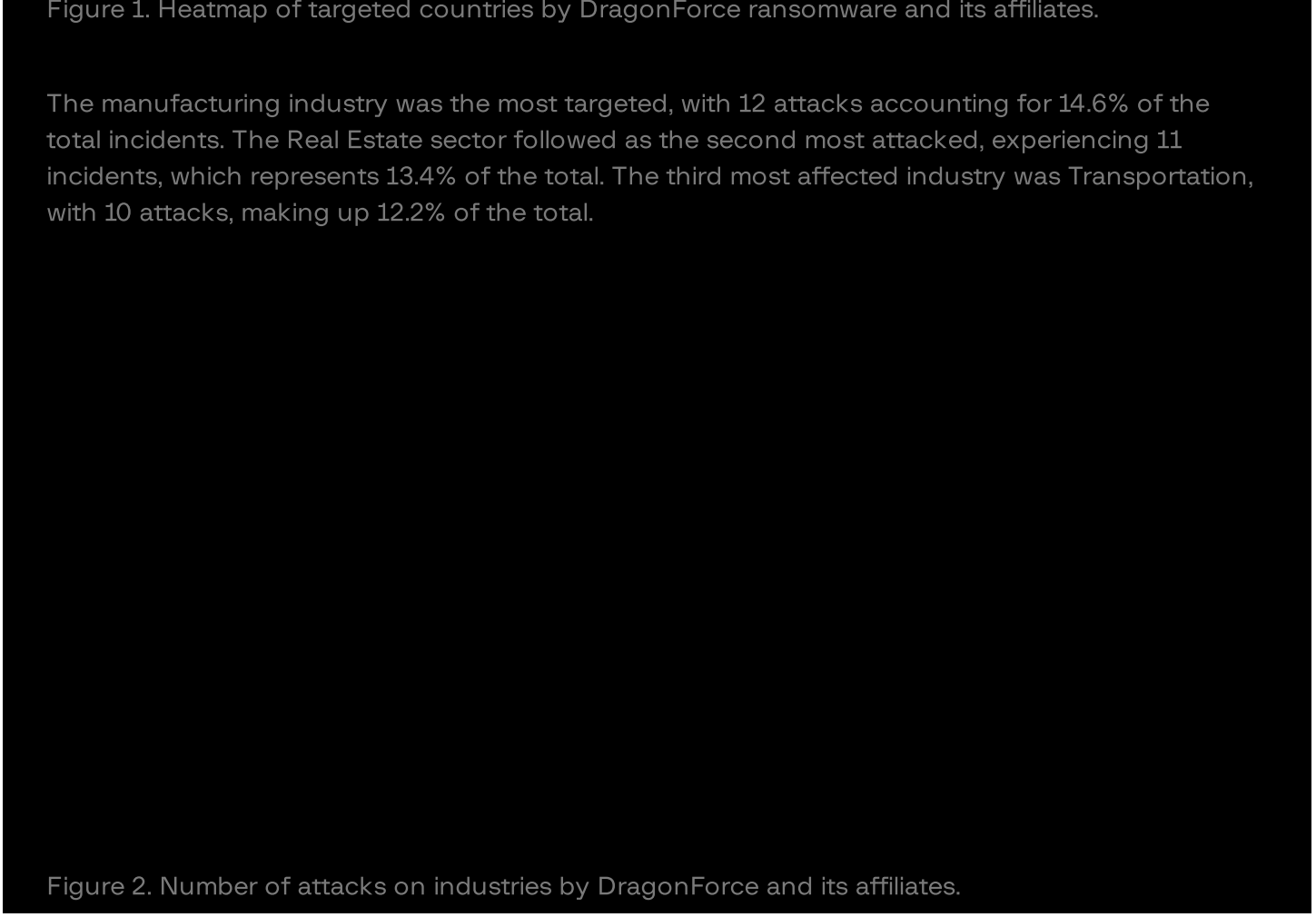


Figure 2. Number of attacks on industries by DragonForce and its affiliates.

Inside the belly of the beast

On 26 June 2024, a user with the handle “dragonforce” started promoting an affiliate program of the DragonForce Ransomware on the underground forum “RAMP”, which contained information on how its affiliates can earn 80% of the total ransom amount, as well as key features of its ransomware including client tracking, automated file delivery, secure access control, and support for extended detection and response (XDR) / endpoint detection and response (EDR) bypass, encryption, and SYSTEM impersonation, adding that comprehensive support services are also available to their affiliates.

Figure 3: Screenshot of a post by DragonForce promoting its ransomware-as-a-service on the RAMP forum.

The following is a translation of the post made by DragonForce on 26 June, 2024:

Figure 4. Screenshot of the user profile 'dragonforce' on the RAMP forum.

On July 4, DragonForce announced on the RAMP forum that they now only accept affiliates who have pre-acquired access, complete proof of their access, and have already exfiltrated victim data.

Figure 5. Screenshot of DragonForce's post dated 4 July 2024.

The following is a translation of the post made by DragonForce on 4 July, 2024:

The DragonForce affiliate program officially began on June 26, 2024. Before launching this program, the group operated with their own team, conducting attacks independently. The introduction of the affiliate program allows other cybercriminals to join forces, significantly expanding the group's reach and potentially leading to a surge in ransomware infections.

In a private conversation on Tox, **Group-IB's Threat Intelligence** specialists obtained the following information from the attacker:

> Each affiliate has a unique .onion address, and a new profile needs to be created for each team member to grant them their own access.
>
> The affiliates have two ransomware variants for Windows: one of their own creation, and a variant of LockBit that allows individuals coming from LockBit to adapt quickly. According to DragonForce, their ransomware can bypass XDR and EDR.

During the course of our research, Group-IB's Threat Intelligence specialists were able to obtain access to DragonForce' panel.

Figure 6.1. A screenshot of the DragonForce login panel

The Affiliates' panel of DragonForce ransomware group has the following sections:

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

Clients

The "Clients" section contains information about the companies attacked (victims), and includes details such as the amount of the ransom, status of ransom, creator of the builder, ID of the client, DLS, size of the leak, clients' status step (paid, or negotiation in the process), last seen, and if the leak has been published.

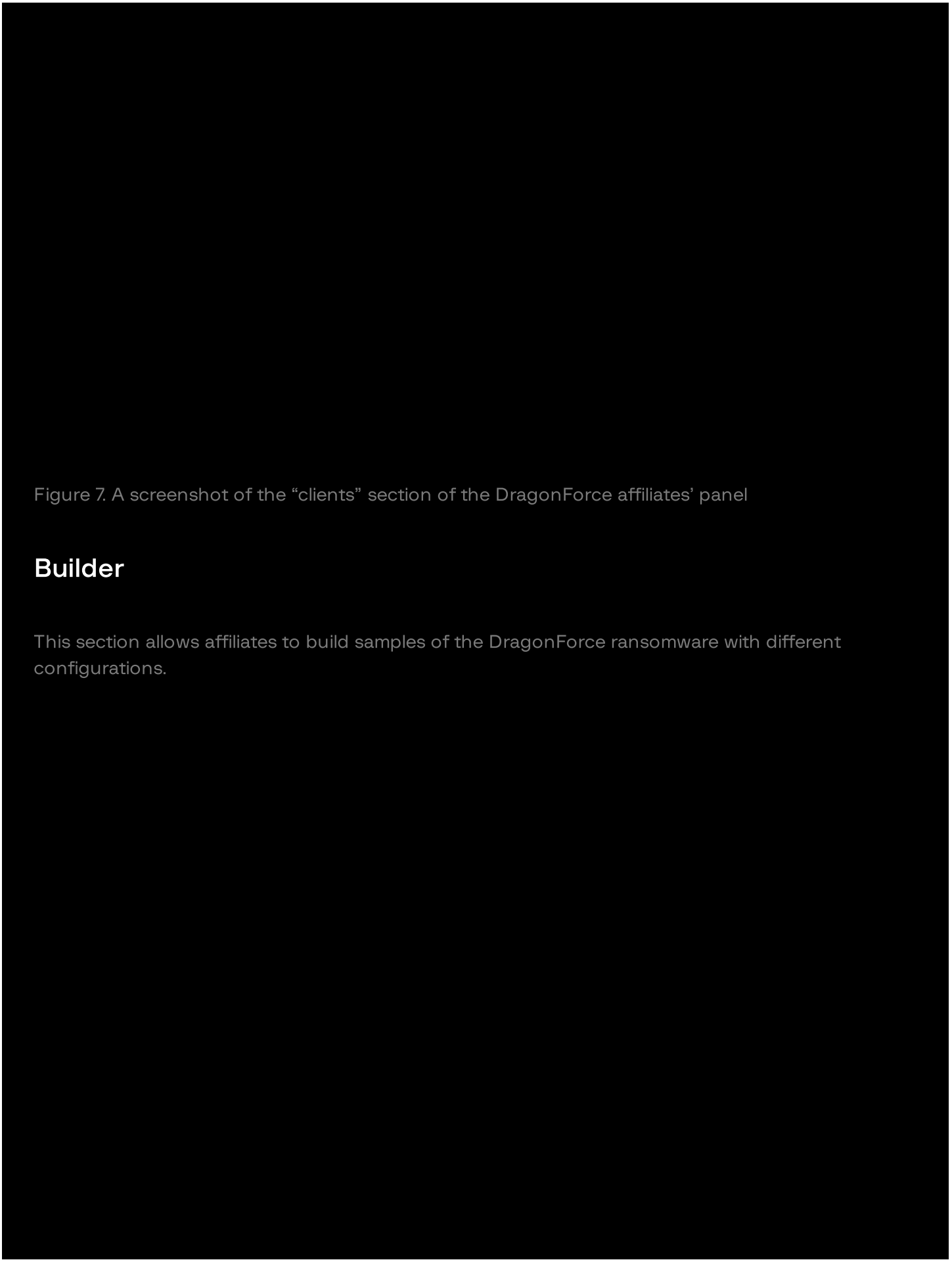


Figure 7. A screenshot of the “clients” section of the DragonForce affiliates’ panel

Builder

This section allows affiliates to build samples of the DragonForce ransomware with different configurations.

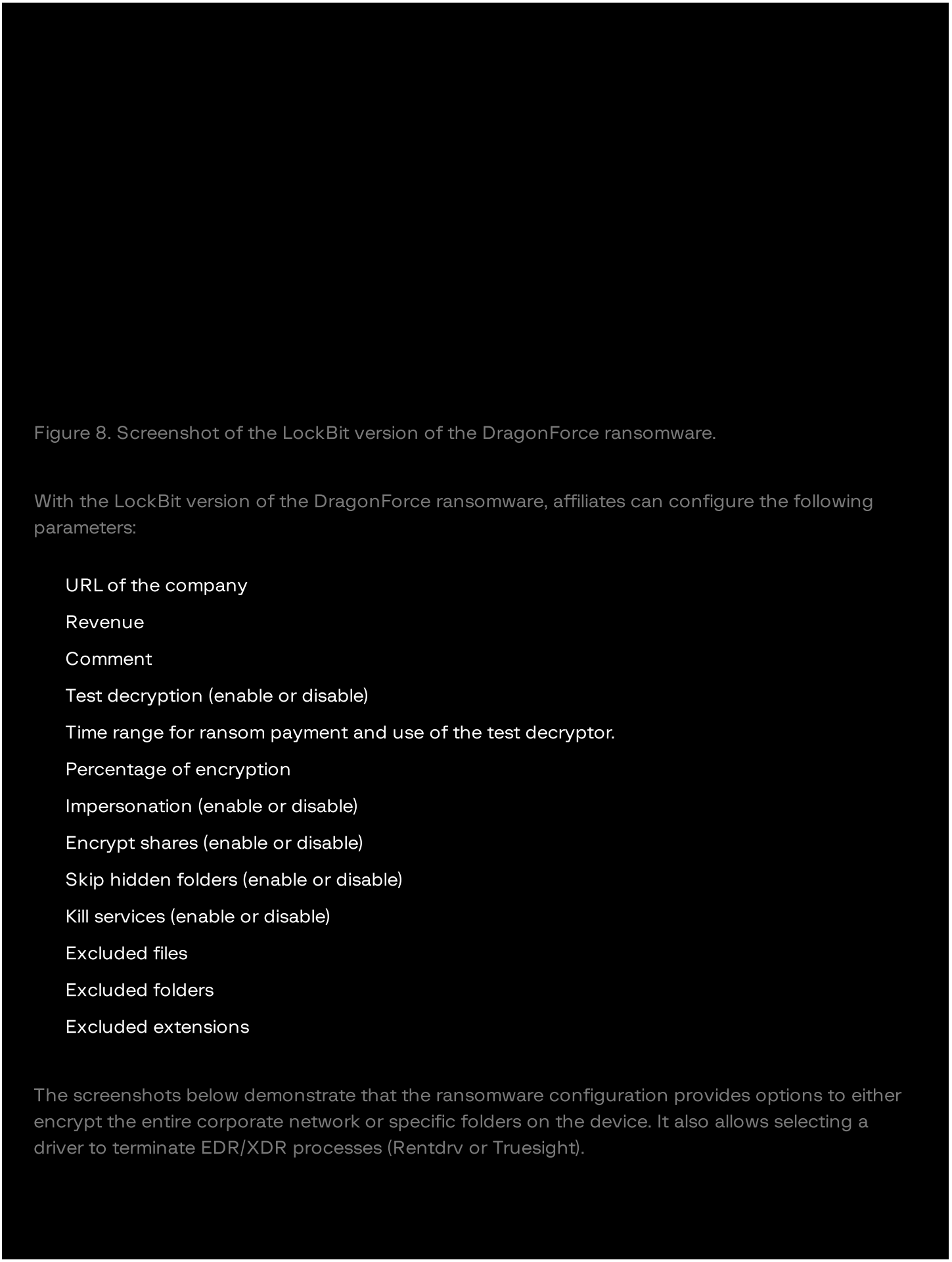


Figure 8. Screenshot of the LockBit version of the DragonForce ransomware.

With the LockBit version of the DragonForce ransomware, affiliates can configure the following parameters:

- URL of the company
- Revenue
- Comment
- Test decryption (enable or disable)
- Time range for ransom payment and use of the test decryptor.
- Percentage of encryption
- Impersonation (enable or disable)
- Encrypt shares (enable or disable)
- Skip hidden folders (enable or disable)
- Kill services (enable or disable)
- Excluded files
- Excluded folders
- Excluded extensions

The screenshots below demonstrate that the ransomware configuration provides options to either encrypt the entire corporate network or specific folders on the device. It also allows selecting a driver to terminate EDR/XDR processes (Rentdrv or Truesight).

Figure 9. The “original” (based on ContiV3) version of the DragonForce ransomware.

As for the “original” version of the DragonForce ransomware, when an affiliate creates a builder, they set up a “client” page for the victim and can configure a DragonForce ransomware sample. They have the option to choose between the LockBit version or the original DragonForce sample, which is capable of terminating EDR/XDR processes.

With this version, affiliates can configure the following parameters:

- URL of the company
- Revenue
- Comment
- Test decryption (enable or disable)
- Time range for ransom payment and use of the test decryptor.
- Encrypt whole system + Network or only Local Path
- Percentage of encryption
- Extension for encrypted files
- Choice of driver to terminate EDR/XDR processes
- Name of ransom note
- Excluded files
- Excluded folders
- Excluded extensions
- Excluded shares

After creating a new client, the affiliate can download samples related to the specific client. If a sample of the “original” DragonForce ransomware is selected, a set of samples for both Windows and ESXi will be downloaded.

The “original” version of the DragonForce ransomware offers greater customization options. It allows affiliates to encrypt either the entire system and corporate network or just specific local paths. Affiliates can also choose the file extension for encrypted files, select a driver to terminate EDR/XDR processes, and configure the name of the ransom note.

My Team

Within the “My Team” section contains an interface viewing advertisers (partners) related to the affiliate.

Figure 10. A screenshot of the “My Team” section.

Add Adver

The “Add Adver” section contains an interface for creating advertisers for the affiliate (adding partners), and editing access rights.

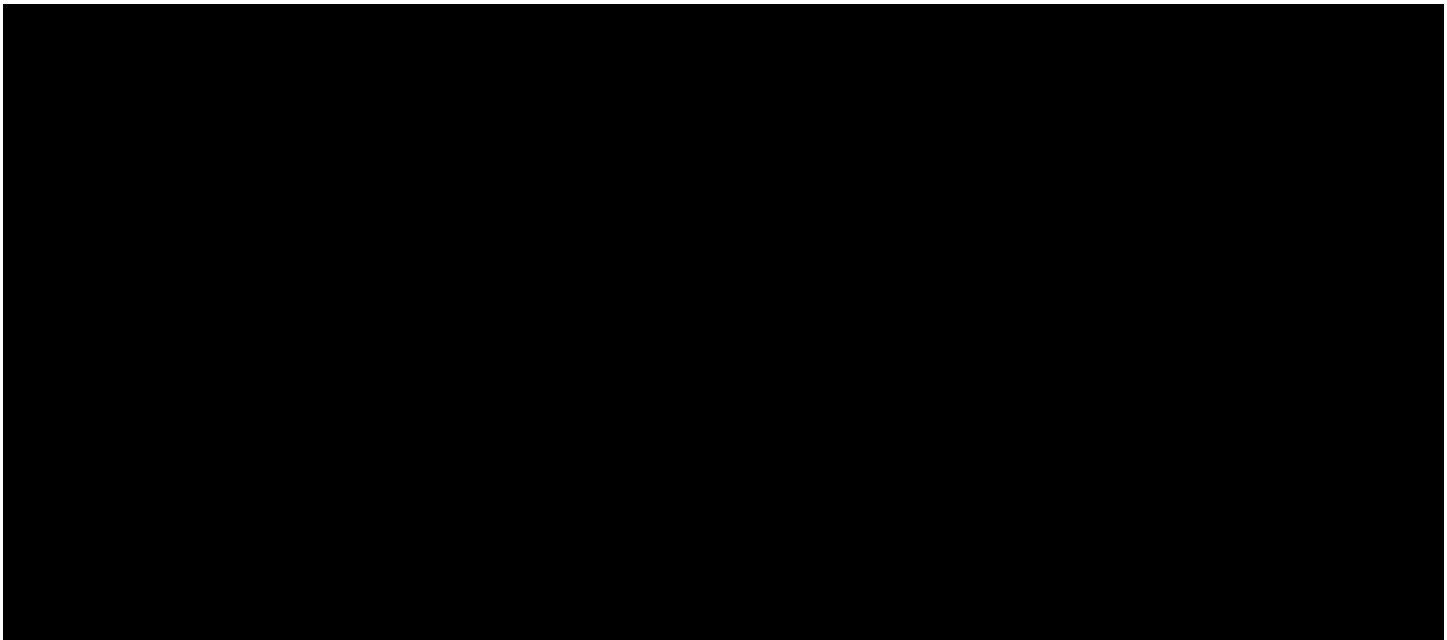


Figure 11. A screenshot of the “Add Adver” section.

Publications

The “Publications” section contains information about data of victims that have been published on the dedicated leaks site by an affiliate of DragonForce.

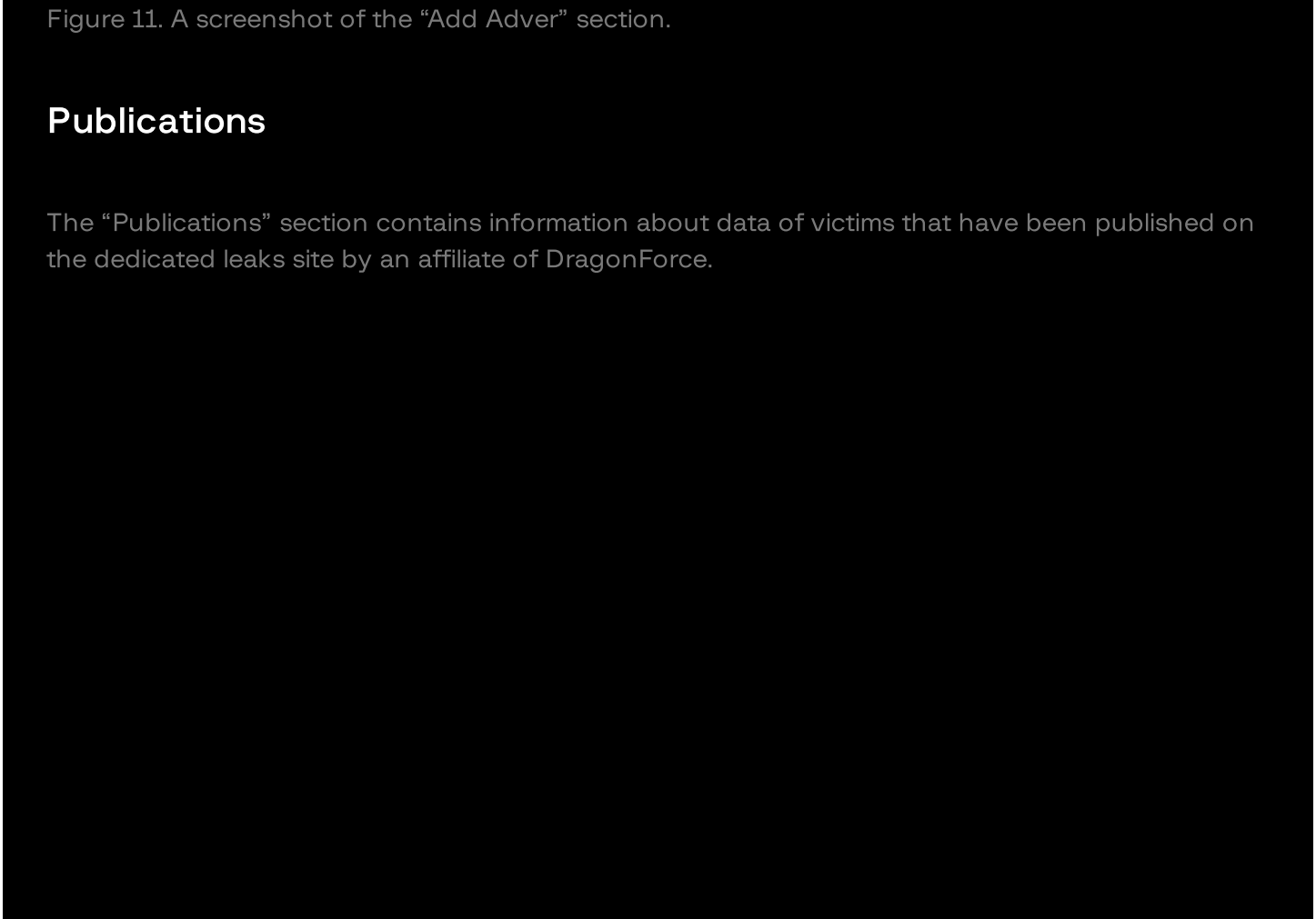


Figure 12. A screenshot of the “Publications” section.

Constructor

Within the “Constructor” section, affiliates can schedule a date for publishing victims’ data, in the event that the victims choose not to pay the ransom.

Figure 13. A screenshot of the “Constructor” section.

Rules

In the “Rules” section, the administrators of the DragonForce ransomware group publish their rules, guides, and contacts relating to the use of the DragonForce ransomware in Russian.

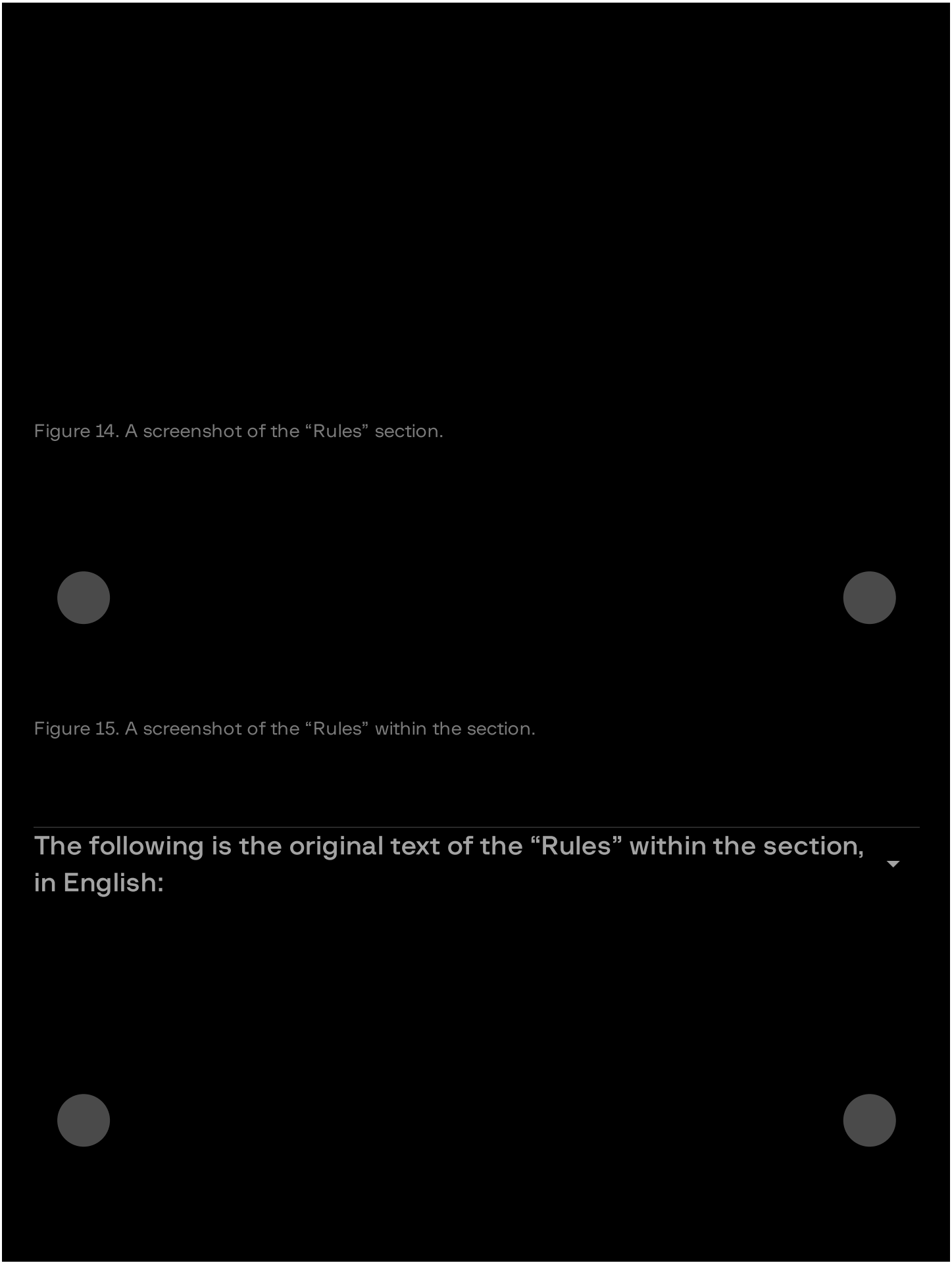


Figure 14. A screenshot of the “Rules” section.

Figure 15. A screenshot of the “Rules” within the section.

The following is the original text of the “Rules” within the section, in English:

Figure 16. A screenshot of the “Guides” within the section.

The following is the original text of the “Guides” within the section, in English:

Figure 17. A screenshot of the “Contacts”.

The following is the original text of the “Contacts” within the section, in English

Blog

Within the “Blog” section contain links to the Dedicated Leaks Site (DLS) of DragonForce ransomware:

hxxp://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion

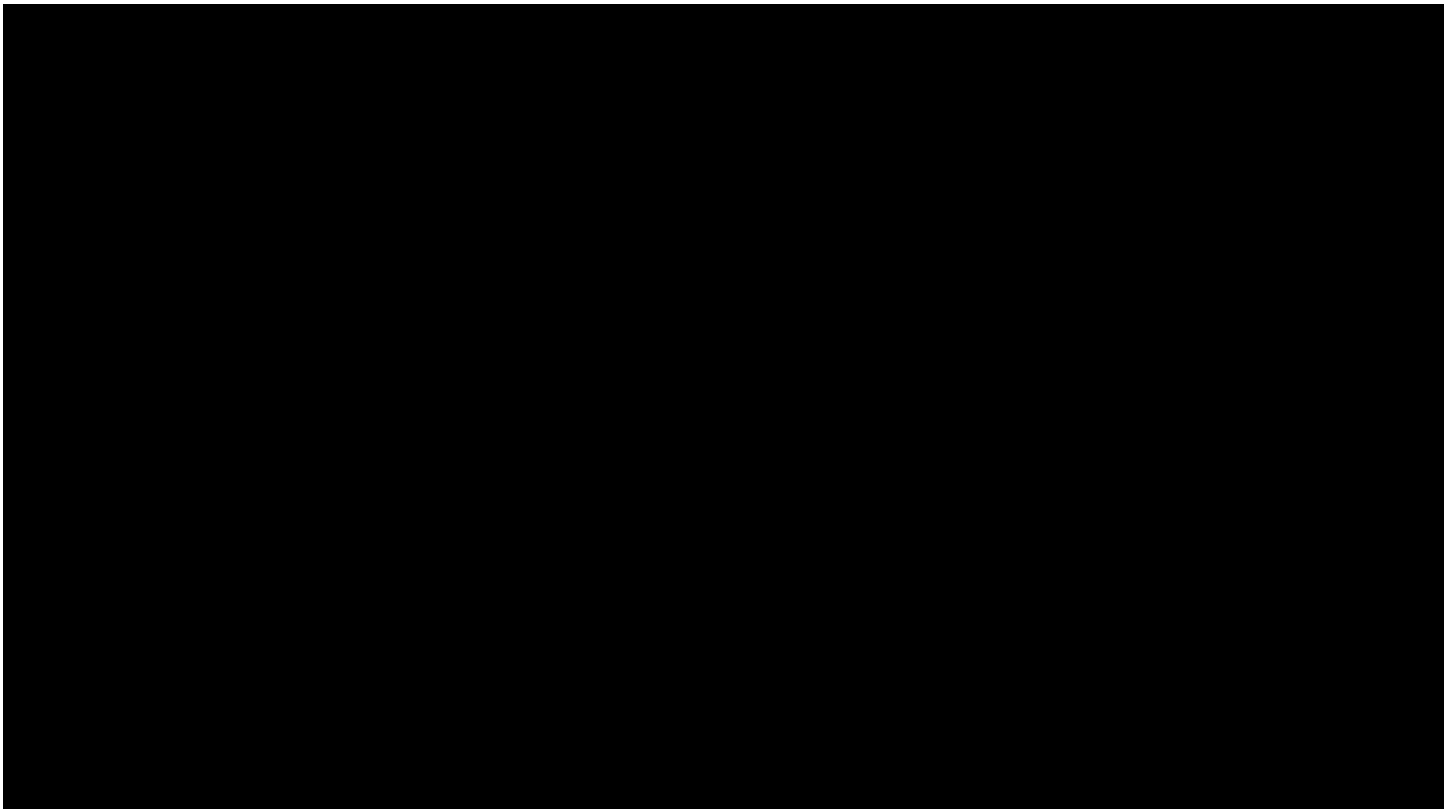


Figure 18. A screenshot of the “DLS” of the DragonForce ransomware.

Profile

The “Profile” section contains information about the affiliate, their authentication history, as well as functions to change passwords, log out, and to check their unique onion page.

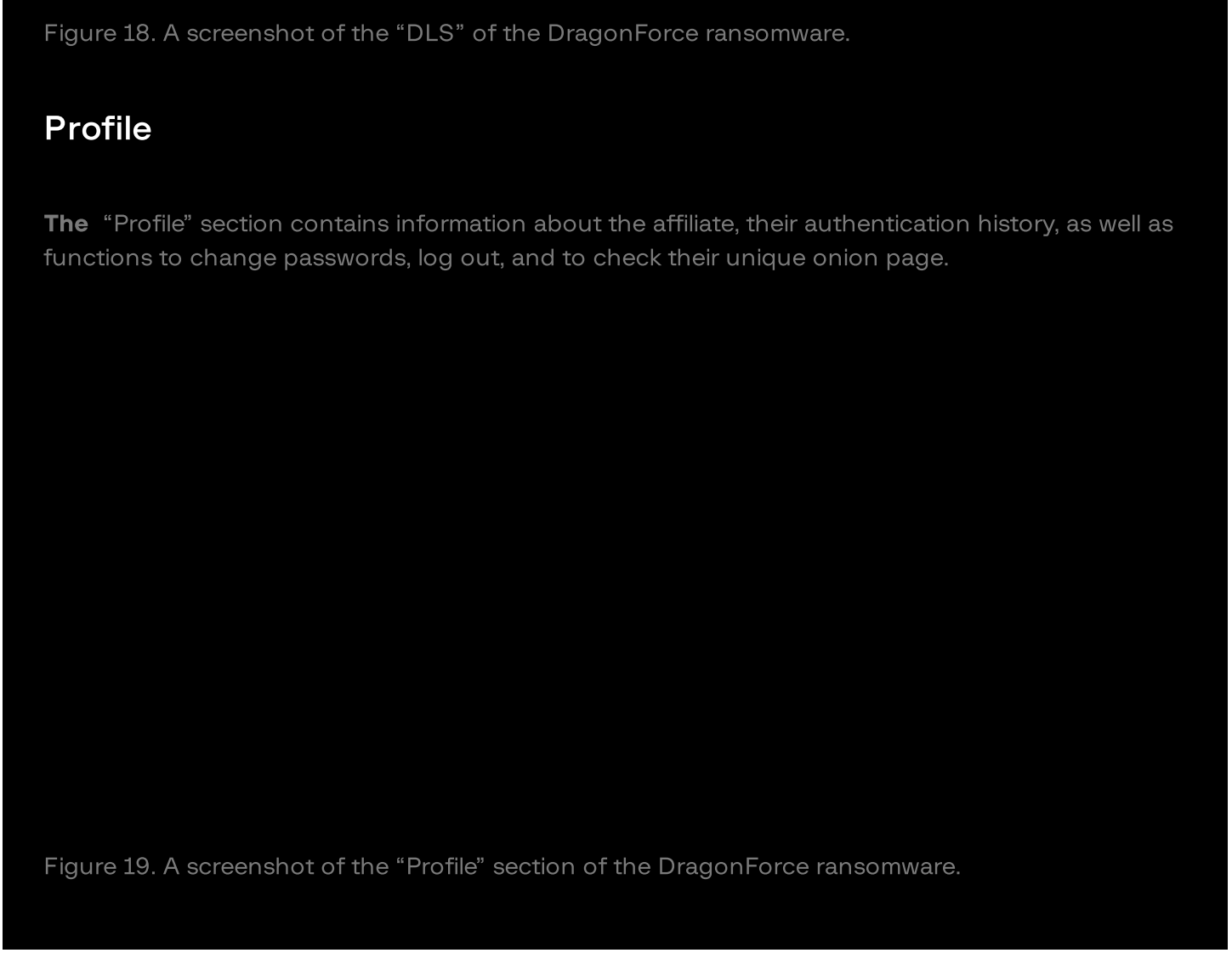


Figure 19. A screenshot of the “Profile” section of the DragonForce ransomware.

Tactics, Techniques, and Procedures (TTPs)

In 2023, Group-IB's Digital Forensics and Incident Response (DFIR) team responded to an incident, and can now reveal the impact of the DragonForce ransomware by analyzing the attacker's tactics, techniques, and procedures (TTPs) from initial access via a public facing web application server.

Incident Response Case: September DragonForce Attack

Initial Access

T1078 Valid Accounts

During the course of the investigation, Group-IB's DFIR analysts identified the initial access to the target network through a public-facing remote desktop server. Suspicious login activity was observed involving three different IP addresses using valid domain accounts. These accounts were used to gain unauthorized access in September 2023.

Date and time of first sighting:

Timestamp	Source IP Address
2023-09-21 20:11:08	2[.]147[.]68[.]96
2023-09-21 20:40:24	185[.]59[.]221[.]75
2023-09-21 22:34:47	69[.]4[.]234[.]20
2023-09-22 16:22:56	69[.]4[.]234[.]20

Execution

T1059.001 Command and Scripting Interpreter: PowerShell

Based on the data collected, Group-IB's DFIR analysts found that PowerShell commands were executed on several hosts within the network. The purpose of these commands was to remotely download and execute a malicious payload, which was later identified as a Cobalt Strike beacon.

Figure 20: Snippet of the Remote Download of Cobalt Strike Beacon.

Persistence

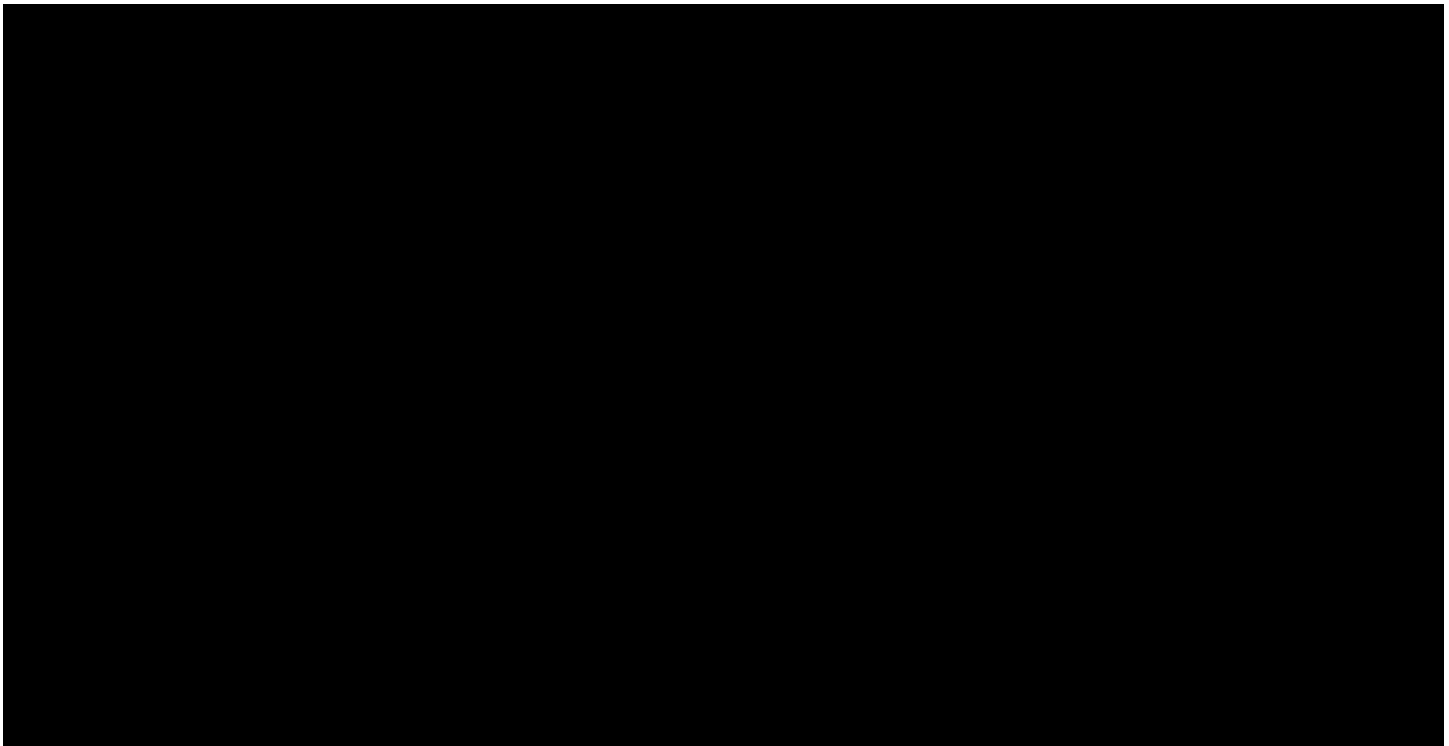
T1078.002 Valid Accounts: Domain Accounts

T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

T1543.003 Create or Modify System Process: Windows Service

They also identified compromised accounts that were used by the threat actor to maintain persistence, and move laterally within the organization. The SystemBC malware was found to create a registry key under “Software\Microsoft\Windows\CurrentVersion\Run” with the name “socks5” to ensure persistence. Two additional hosts were also found to be infected with SystemBC, although further data was unavailable for analysis.

Figure 21: Windows Defender event log quarantine of Cobalt Strike.



Figures 22 & 23: Attempted service installation on the system.

Defense Evasion

T1070.001 Indicator Removal: Clear Windows Event Logs

The ransomware executable “df.exe” was found to have the capability to clear Windows Event Logs after completing its encryption tasks. This action is likely intended to hinder forensic investigation post-attack.

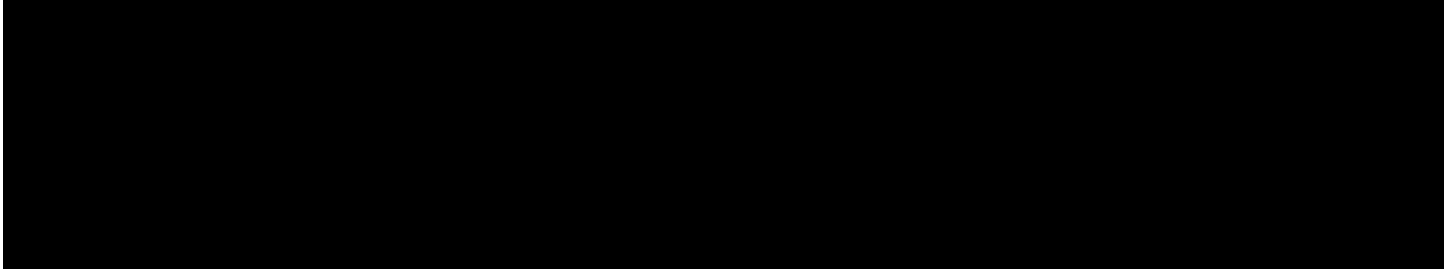


Figure 24: Sample of logs cleared identified in the target network.

Credential Access

T1003.001 OS Credential Dumping: LSASS Memory

Group-IB’s DFIR analysts identified that the threat actor executed Mimikatz, a credential dumping tool, on four different hosts. The execution of Mimikatz resulted in the creation of a file named “123.txt,” which contained clear text credentials of the compromised users.

Discovery

T1482 Domain Trust Discovery

T1018 Remote System Discovery

T1016 System Network Configuration Discovery

T1082 System Information Discovery

T1083 File and Directory Discovery

On one host, a compromised user executed the ADFind tool, saving the results in a file named "AD_subnet.txt." This execution indicates that the attacker was gathering information about the network's Active Directory. Additionally, on two other hosts, the network scanner tool "netscanold.exe" was found to have been executed, further supporting the attacker's efforts to map out the network.

Execution Time	File Location
23/09/2023 4:04:46	C:\Users\[Redacted]\AppData\Local\Temp\2\netscanold.exe
23/09/2023 4:11:47	C:\Users\[Redacted]\Music\netscanold.exe

Lateral Movement

T1021.001 Remote Services: Remote Desktop Protocol

Group-IB's DFIR analysts determined that the attacker used Remote Desktop Protocol (RDP) to move laterally within the network. After gaining initial access through the public-facing web application server, the attacker used RDP to access internal servers and continued moving across the network.

Here's a detailed list of the unique malicious activities observed during the RDP sessions:

- **Multiple RDP Connections** – Used for lateral movement within the network.
- **Mimikatz Execution** – Used to dump credentials from LSASS memory.

ADFind Execution – Used for Active Directory enumeration.

SystemBC, CobaltStrike, and Network Scanner Execution – Used to establish persistence, command-and-control communication, and perform network reconnaissance.

Disabling Antivirus – Antivirus features were disabled, exceptions added, and antivirus uninstalled to avoid detection.

Ransomware Execution – Deployed ransomware to encrypt files across multiple systems.

Clearing Event Logs – Event logs were cleared after ransomware execution to cover tracks.

Command and Control

T1071.001 Application Layer Protocol: Web Protocols

Analysis of the Cobalt Strike beacons revealed the command-and-control (C2) address 185[.]73[.]125[.]8 utilizing the HTTP protocol. An additional C2 address associated with SystemBC malware was identified as 94[.]232[.]46[.]202. Firewall logs indicated connections to these C2 addresses.

Impact

T1486 Data Encrypted for Impact

Ransomware was deployed across the network, with the malicious executable responsible for the encryption identified as "***df.exe***".

Figure 25: Screenshot of the ransom note.

Malware Analysis

SystemBC

File path	MD5 Hash
C:\Users\username\AppData\Local\Temp\2\ socks aug\socks.exe	97B70E89B5313612A9E7A339EE82AB67

The file ***socks.exe*** with corresponding MD5-hash checksum 97B70E89B5313612A9E7A339EE82AB67 is a backdoor which allows a remote attacker to upload additional executable files and execute them on a controlled host, which is related to a malware family “SystemBC”.

The file ***socks.exe*** is configured to connect to a C2 server with the IP-address 94[.]232.46.202 every 180 seconds. Upon the attacker’s command, the sample can download the file, save it in a specified directory on the infected host and execute it.

The file ***socks.exe*** can also achieve persistence by creating a value with a name “*socks5*” within the registry key *HKLM|Software|Microsoft|Windows|CurrentVersion|Run*, which is responsible for automatic execution upon user logon or system boot. When the user logs on or initiates a system boot, the created value will contain the command ‘powershell.exe -windowstyle hidden -Command & ‘path_to_executable_file’, which will be executed, where ‘path_to_executable_file’ is a file path where a SystemBC sample is located in a filesystem.

Cobalt Strike Beacon

File path	MD5 Hash
C:\Users\username\AppData\Local\Temp\ 2\a65.exe	A50637F5F7A3E462135C0AE7C7AF0D91

The file ***a65.exe*** with corresponding MD5-hash checksum A50637F5F7A3E462135C0AE7C7AF0D91 is a payload of the post-exploitation framework Cobalt Strike which allows remote attacker to perform various actions on an infected system, including but not limited to, uploading/downloading files, executing files and commands in command interpreter, gather credentials of users, move laterally across network. The file is configured to connect to a URL http[:]//185[.]73.125.8/ broadcast and receive commands from this URL.

SoftPerfect Network Scanner

File path	MD5 Hash
C:\Users\username\AppData\Local\Temp\2\netscanold.exe	BB7C575E798FF5243B501477725363

The file ***netscanold.exe*** with corresponding MD5-hash checksum BB7C575E798FF5243B5014777253635D is a network scanning tool known as SoftPerfect Network Scanner. It is a system administration tool which allows its user to get the list of reachable hosts and network shares, as well as perform connection to discovered hosts via RDP, WMI, SMB.

Ransomware Payload

File path	MD5 Hash
df.exe (dropped in multiple paths)	C111476F7B394776B515249ECB6B20E6

The file ***df.exe*** with corresponding MD5-hash checksum C111476F7B394776B515249ECB6B20E6 is a malicious file which is intended to encrypt contents of files within the filesystem. It utilizes a combination of RSA-1024 and Salsa20 encryption algorithms, so it is impossible to decrypt files without the knowledge of a private key. After the encryption of files is completed, ***df.exe*** clears the Windows event logs.

In the next section, we turn our attention to the different versions of the DragonForce ransomware.

Technical information about ransomware builds

DragonForce offers two different builds. Based on the information they provided, one is a variant of LockBit 3.0, while the other was claimed by DragonForce to be their own original Dragonforce ransomware variant. However, after analysis of the latter, we found that it is actually a variant of ContiV3, enhanced with new features such as the “Bring Your Own Vulnerable Driver” (BYOVD).

This is unsurprising as modern ransomware operators are increasingly reusing and modifying builders from well known ransomware families that were leaked, to tailor to their needs. Conti, Babuk, LockBit are among the common families that have been modified.

ContiV3 fork

A sample of this has been seen in the wild since July 2024. It creates a mutex “dragonforce_encrypted_system” and usually renames files with a “.dragonforce_encrypted” extension, which can be changed by its affiliates. As ContiV3 codes have been leaked and analyzed, we will mainly focus on features that have been added by DragonForce.

New features! Buy me instead! (Differences from Conti)

- Embedded Configuration
- Bring Your Own Vulnerable Driver (BYOVD) for process termination
- Encrypt filenames
- Persistence via Scheduled tasks
- Verbose logging
- DragonForce wallpaper and icon

Obfuscation / Anti-analysis

Its anti-analysis techniques are inherited from Conti.

- String obfuscation using ADVobfuscator
- Resolving APIs by Hash – Names are hashed with `MurmurHash2A` algorithm with the seed value of `0xB801FCDA`
- Anti-hooking – compares the currently loaded functions with the original files. If the bytes have been modified, it replaces them with the original bytes
- Deleting Shadow Copy with COM Objects – enumerates shadow copies and deletes them.

```
SELECT * FROM Win32_ShadowCopy

cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy where "ID='%s'" delete
```

Command-line Arguments

These are mostly inherited from Conti as well.

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

Configuration

In contrast to Conti, DragonForce embeds a configuration inside the binary so that no command line options are needed. However, when command line options are used, it will override those specified in the configuration.

Figure 26: Screenshot of a snippet of decrypted configuration.

These configuration values correspond to the aforementioned guides. Here's a concise summary, to spare one from reading the nitty-gritty byte-by-byte details:

```
start_marker: 0xDEAD
build_key
offset_embedded_resource
encrypt_mode: 10/11/12/14 - all/local/network/path
time_sync
logging option and filepath
filesize_for_fullencrypt
filesize_for_headerencrypt
header_encrypt_size
other_encrypt_chunk_percent
encrypt_file_names
custom_icon option, size and filepath
schedule_job details
kill
use_sys: 0/1/2 - None, Truesight, RentDrv
driver offset and sizes
driver encryption key
driver encryption nonce
list of processes to kill (priority)
list of processes to kill
custom_extension
whitelisted paths
whitelisted extensions
whitelisted filenames
whitelisted shares
custom_ransomnote_name
custom_wallpaper option, size and filepath
end_marker: 0xBEEF
```

BYOVD for terminating processes

Conti uses Windows Restart Manager to kill processes that are currently using the resources. DragonForce has implemented additional ways to kill processes, especially for protected processes.

The "Bring Your Own Vulnerable Driver" (BYOVD) technique has become a favored technique within ransomware groups to disable EDR products. This tactic involves bringing vulnerable drivers onto compromised systems and leveraging them to execute malicious code at the kernel level. By default, 64-bit versions of Windows Vista and later will load a kernel-mode driver only if the kernel can verify

the driver signature. DragonForce abuses digitally signed but vulnerable drivers by bringing them onto the systems and using it to terminate critical AV or EDR processes, enabling them to operate undetected in the compromised environment.

During the build phase, two different vulnerable driver options are provided to the user. These drivers expose IOCTL commands with privileged functionality, but lack adequate access controls. The selected driver is then compressed, encrypted, and then embedded into the binary. Both drivers perform the same method of process termination by calling `ZwOpenProcess()` and `ZwTerminateProcess()`. Both drivers have been published on the Microsoft recommended driver block rules.

1. TrueSight.sys

TrueSight.sys is actually a RogueKiller Antirootkit Driver v3.3 developed by Adlice Software. The company, Adlice, has already published a fix in v3.4. The `0x22E044` control code terminates the target process provided by its PID.

Figure 27: Screenshot of the `0x22E044` control code in Truesight driver.

2. RentDrv.sys

A driver developed by Hangzhou Shunwang Technology. Not much information about the driver can be found online. The `0x220E010` control code terminates the target process provided by its PID.

Figure 28: Screenshot of the `0x220E010` control code in RentDrv driver.

In user-mode, the program retrieves a device handle to the driver and communicates with the driver via DeviceIoControl. Since the methods of loading and using these drivers are similar, codes are reused and supplement with a simple switch statement.

Figure 29: Screenshot of the program communicating with the driver via DeviceIoControl.

Hashes of Drivers

Name	SHA256
RentDrv.sys	1aed62a63b4802e599bbd33162319129501d603cceeb5e1eb22fd4733b3018a3
RentDrv.sys (64-bit)	9165d4f3036919a96b86d24b64d75d692802c7513f2b3054b20be40c212240a5
Truesight.sys	bfc2ef3b404294fe2fa05a8b71c7f786b58519175b7202a69fe30f45e607ff1c

Although DragonForce has advertised that one can configure two kill processes lists– one for a single termination and the other for continuous termination–we found that it starts two threads for killing processes. Both threads actually run in an infinite loop constantly checking for processes to be terminated. The ‘priority’ thread sleeps for 15 ms after checking, while the ‘normal’ thread sleeps for 250 ms per loop.

Privilege Escalation

In order to kill processes, the ransomware requires at least administrator privileges. Once it confirms that it has elevated privileges, it attempts to execute itself as SYSTEM using Access Token Manipulation.

It enumerates running processes to find one running with SYSTEM-level privileges, then duplicates its access token with `DuplicateTokenEx()`, and uses it with `CreateProcessWithTokenW()` to create a new process running under the security context of `NT AUTHORITY\SYSTEM`.

Figure 30: Screenshot of the program attempting to perform privilege escalation.

Encryption Schema

There are no major modifications to Conti's encryption schema, except that some values are now customizable during the build and filenames can be encrypted.

For those that are unfamiliar with Conti's encryption schema, for each file, the ChaCha8 key and IV is generated by the `CryptGenRandom()` function. They are then used to initialize the ChaCha8 initial state and subsequently to encrypt the file. The key and IV are then concatenated, encrypted with RSA and appended to the end of the file.

Other than the four encryption modes (all, net, local, path) mentioned in the above operator guide, there are three different encryption types, namely, FULL_ENCRYPT, PARTLY_ENCRYPT, HEADER_ENCRYPT and the type of encryption is chosen based on their file types and file sizes:

- Files with Database extensions are fully encrypted
- Files with Virtual machine extensions are 20% encrypted
- For other files:

File size < full_encrypt_threshold: Full encryption

File size < header_encrypt_threshold: Only the first [header_encrypt_size] bytes are encrypted

Other: Encrypted by [other_encrypt_chunk_percent]

The following is a list of database file extensions:

.4dd, .4dl, .accdb, .accdc, .accde, .accdr, .accdt, .accft, .adb, .ade, .adf, .adp, .arc, .ora, .alf, .ask, .btr, .bdf, .cat, .cdb, .ckp, .cma, .cpd, .dacpac, .dad, .dadiagrams, .daschema, .db, .db-shm, .db-wal, .db3, .dbc, .dbf, .dbs, .dbt, .dbv, .dbx, .dcb, .dct, .dcx, .ddl, .dlis, .dp1, .dqy, .dsk, .dsn, .dtsx, .dxl, .eco, .ecx, .edb, .epim, .exb, .fcd, .fdb, .fic, .fmp, .fmp12, .fmpsl, .fol, .fp3, .fp4, .fp5, .fp7, .fpt, .frm, .gdb, .grdb, .gwi, .hdb, .his, .ib, .idb, .ihx, .itdb, .itw, .jet, .jtx, .kdb, .kexi, .kexic, .kexis, .lgc, .lwx, .maf, .maq, .mar, .mas, .mav, .mdb, .mdf, .mpd, .mrg, .mud, .mwb, .myd, .ndf, .nnt, .nrmlib, .ns2, .ns3, .ns4, .nsf, .nv, .nv2, .nwdb, .nyf, .odb, .oqy, .orx, .owc, .p96, .p97, .pan, .pdb, .pdm, .pnz, .qry, .qvd, .rbf, .rctd, .rod, .rodx, .rpd, .rsd, .sas7bdat, .sbf, .scx, .sdb, .sdc, .sdf, .sis, .spq, .sql, .sqlite, .sqlite3, .sqlitedb, .te, .temx, .tmd, .tps, .trc, .trm, .udb, .udl, .usr, .v12, .vis, .vpd, .vvv, .wdb, .wmdb, .wrk, .xdb, .xld, .xmlff, .abcddb, .abs, .abx, .accdw, .adn, .db2, .fm5, .hjt, .icg, .icr, .kdb, .lut, .maw, .mdn, .mdt

The following is a list of virtual machine file extensions:

.vdi, .vhd, .vmdk, .pvm, .vmem, .vmsn, .vmsd, .nvram, .vmx, .raw, .qcow2, .subvol, .bin, .vsv, .avhd, .vmrs, .vhdx, .avdx, .vmcx, .iso

For Network Encryption, it enumerates network shares and encrypts shares that are not named “ADMIN$”.

When the encrypt_filename option is checked, filenames are encoded with Base32 with the following custom set of alphabet `gwfn6l3bk45o2zecvi7xtyqrpsudmahj`

Persistence via Scheduled tasks

This DragonForce variant of Conti ransomware has the option to create scheduled tasks. It uses the COM TaskScheduler class to schedule a task daily to run the current binary, specifying a time and task name. They can also choose to move the binary to a different location and run the scheduled

task from there instead. COM objects allow privileged users to schedule a task without using the `schtasks` or the `at` command.

Logging

Dragonforce has more verbose logging, of course only if the logging option is turned on. It logs the selected configuration values and also the encryption type (i.e. if it is excluded, full, header, or percentage) used per file. Each line of log is preceded with the execution time and thread ID. Logs are encrypted with ChaCha8 and written to C:\Users\Public\log.log

Here are some snippets of decrypted logs:

Figure 31: Screenshot of the configuration values in decrypted logs.

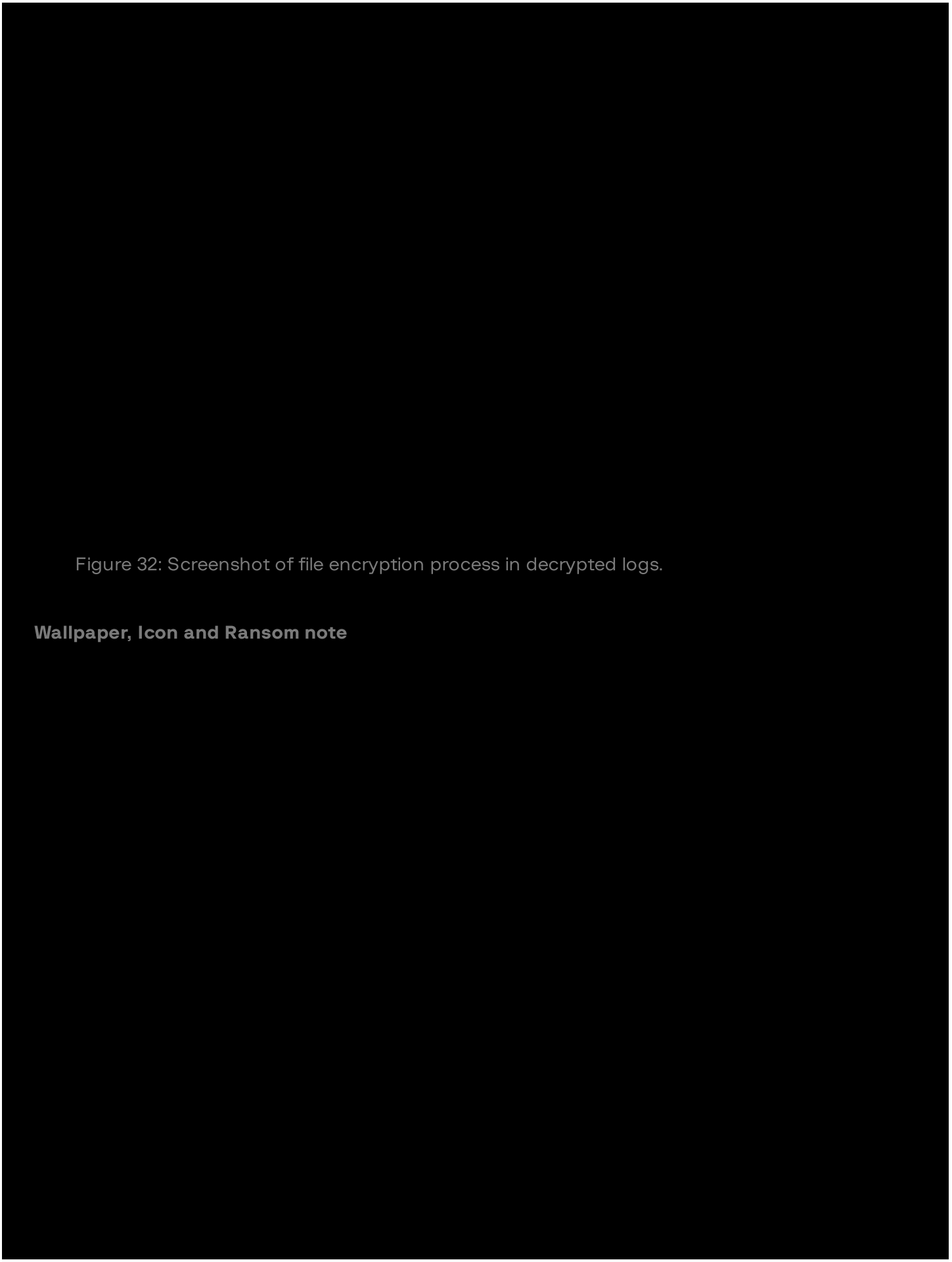


Figure 32: Screenshot of file encryption process in decrypted logs.

Wallpaper, Icon and Ransom note

Figure 33: Screenshot of the wallpaper and icon of DragonForce after a system has been encrypted.

Figure 34: Screenshot of the ransom note.

LockBit 3.0 fork

LockBit 3.0 is also known as LockBit Black ransomware. It gained this alias as LockBit 3.0 seems to reuse code from BlackMatter ransomware.

The sample that we have obtained does not require a custom password to execute, as most LockBit 3.0 samples are observed to have been generated using the password option. There were very little differences observed between this and other generic LockBit 3.0 variants, hence we will not go into details here.

Comparing the customisation options currently provided in the builder and the JSON configuration used in LockBit 3.0, it was only a subset of what LockBit 3.0 offered. As LockBit 3.0 uses a separate JSON file for build configuration, it is rather easy for DragonForce to expand the configuration options offered in their builder in the future as well.

The following is a sample of the JSON configuration for Lockbit:


```
"config": {
  "settings": {
    "encrypt_mode": "auto",
    "encrypt_filename": false,
    "impersonation": true,
    "skip_hidden_folders": false,
    "language_check": false,
    "local_disks": true,
    "network_shares": true,
    "kill_processes": true,
    "kill_services": true,
    "running_one": true,
    "print_note": true,
    "set_wallpaper": true,
    "set_icons": true,
    "send_report": false,
    "self_destruct": true,
    "kill_defender": true,
    "wipe_freespace": false,
    "psexec_netspread": false,
    "gpo_netspread": true,
    "gpo_ps_update": true,
    "shutdown_system": false,
    "delete_eventlogs": true,
    "delete_gpo_delay": 1
  },
  "white_folders": "",
  "white_files": "",
  "white_extens": "",
  "white_hosts": "",
  "kill_processes": "",
  "kill_services": "",
  "gate_urls": "",
  "impers_accounts": "",
  "note": ""
}
```

Conclusion

The DragonForce ransomware group has rapidly emerged as one of the most dangerous threats in the cybersecurity domain, largely due to their use of two distinct ransomware variants: a fork of LockBit, and a highly customized fork of Conti. The Conti variant offers significant advantages, including advanced encryption techniques, the ability to terminate EDR/XDR processes using the "Bring Your Own Vulnerable Driver" (BYOVD) method, and enhanced anti-analysis features. These enhancements make their attacks more sophisticated and difficult to detect and mitigate.

Additionally, the integration of SystemBC malware into their operations add another layer of complexity. SystemBC facilitates persistent access, enables network reconnaissance, and supports lateral movement within compromised networks, making it a critical component of their attack chain.

By targeting key industries such as manufacturing, real estate, and transportation, and employing these advanced tools and tactics, DragonForce has proven to be a formidable adversary. Organizations must prioritize strengthening their defenses, staying informed about the specific tactics, techniques, and procedures (TTPs) used by DragonForce, and adopting a comprehensive and adaptive security strategy to protect their critical assets and ensure resilience against the evolving threat of ransomware attacks.

Recommendations

How to prevent ransomware? Although ransomware groups have gained notoriety for targeting companies in critical sectors, they are a threat to organizations across all industries. In addition to having new members in its network, ransomware affiliate programs equip members with upgraded tools and techniques. That being said, it is essential that businesses take specific steps immediately to keep their mission-critical operations and data secure. We recommend the following:

Add more layers of security: Multi-factor authentication (MFA) and credential-based access solutions help businesses secure their critical assets and high-risk users, making it harder for attackers to be successful.

Stop ransomware with early detection: Leverage the behavioral detection capabilities of the Endpoint Detection and Response (EDR) solution to help identify ransomware indicators across your managed endpoints, promptly alerting your teams to any suspicious activity for further scrutiny. This proactive approach enables agile detection, investigation and remediation of both known and unknown threats on your endpoints.

Have a backup strategy: Data backup processes should be conducted regularly as they reduce damage and help organizations avoid data loss following ransomware attacks.

Leverage an advanced malware detonation solution: Organizations should leverage AI-infused, advanced analytics-based solutions to detect intrusions in real time. Learn how Group-IB's Managed XDR coupled with Threat Intelligence helps businesses to:

- gain insights into the unique Tactics, Techniques, and Procedures (TTPs) used by Advanced Persistent Threats (APTs) and other cybercriminal groups and pivot their security strategies accordingly; and
- enable multi-layered cybersecurity (endpoint, email, web, and network) through automated threat detection and response.

Patch it up: The longer a vulnerability remains unpatched, the greater the risk that it will be exploited by cybercriminals. Security patches should therefore be prioritized, and organizations should also set up a process to regularly review and apply patches as they become available.

Train employees: The human factor remains one of the greatest vulnerabilities in cybersecurity. Educate employees about the risks relating to the organization's network, assets, devices, and infrastructure. Organizations should conduct training programs and security drills to help employees identify and report the tell-tale signs of cybercrime (e.g. phishing emails).

Control vulnerabilities: Do not turn a blind eye to emerging vulnerabilities. Checking your infrastructure annually with a technical audit or security assessment is not only a good habit, it also adds a much-needed layer of protection. Infrastructural integrity and digital hygiene processes should be monitored continually.

Financially-motivated threat actors are driven to make you pay more. Even if one attacker returns your data, another will find out about your willingness to pay, which will lead to an increase in the number of attempted attacks on your company. The best you can do is to contact incident response experts as quickly as possible.

IOCs

IP Addresses

File Hashes

File path	MD5 Hash

C:\Users\[Redacted]\AppData\Local\Temp\2\socks aug\socks.exe	97B70E89B5313612A9E7A339EE82AB67
C:\Users\[Redacted]\AppData\Local\Temp\2\a65.exe	A50637F5F7A3E462135C0AE7C7AF0D91
C:\Users\[Redacted]\AppData\Local\Temp\2\netscanold.exe	BB7C575E798FF5243B5014777253635D
df.exe (dropped in multiple paths)	C111476F7B394776B515249ECB6B20E6

MITRE ATT&CK

Tactic	Technique with ID	Description
Initial Access	Valid Accounts (T1078)	DragonForce affiliates gain access using compromised valid domain accounts.
Execution	Command and Scripting Interpreter: PowerShell (T1059.001)	PowerShell is used to download and execute malicious payloads like Cobalt Strike.
Persistence	Valid Accounts: Domain Accounts (T1078.002)	Maintaining access by using compromised domain accounts.
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)	Registry keys are created to ensure malware execution at startup.
Persistence	Create or Modify System Process: Windows Service (T1543.003)	SystemBC creates services for persistence.

Found it interesting? Don't hesitate to share it to wow your friends or colleagues

GROUP-IB

Products

- Threat Intelligence
- Fraud Protection
- Managed XDR
- Attack Surface Management
- Digital Risk Protection
- Business Email Protection
- Cyber Fraud Intelligence Platform
- Unified Risk Platform
- Integrations

Resources

- Research Hub
- Success Stories
- Knowledge Hub
- Certificates
- Webinars
- Podcasts
- TOP Investigations
- Ransomware Notes
- AI Cybersecurity Hub

Partners

- Partner Program
- MSSP and MDR Partner Program
- Technology Partners
- Partner Locator

Company

- About Group-IB
- Team
- CERT-GIB
- Careers
- Internship
- Academic Aliance
- Sustainability
- Media Center

Contact

Subscription plans

Services

Resource Center

Contact

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends