Keep up with Ransomware

DragonForce Ransomware Introduces the Cartel Model

■ Overview

In April 2025, the number of ransomware incidents recorded a decrease of approximately 29% to 550 cases, compared to 773 cases in March. The reduction in incidents during April appears to have been influenced by the cessation of activities by the RansomHub group, which until March had been generating around 70 victims monthly. Although numerous new groups have emerged, the most significant factor has been the diminished activity of previously active groups.

In April, instances of hacking by ransomware groups were once again confirmed. The Everest Group, active since 2020, experienced a disruption at the beginning of April when their dark web leak site was altered and deactivated with the message "Don’t do crime CRIME IS BAD xoxo from Prague." This modification, which diverged from the typical page set up when law enforcement seizes infrastructure, suggests that the site was likely tampered with by a user following the hack. By the end of April, the Everest Group's dark web page was restored and they recommenced their operations, resuming the posting of victims.

These hacking incidents also occurred to the LockBit group, which was aiming for a resurgence with the release of version 4.0, resulting in the leakage of internal data. In early May, LockBit's dark web leak site was tampered with, displaying the same phrase used in the hacking incident involving the Everest group. In the case of LockBit, not only was the dark web leak site altered, but the administrator panel was also compromised due to hacking, leading to the leakage of some internal database files. The leaked database included cryptocurrency wallet addresses, configuration information used by different versions of ransomware, affiliate account details, and chat histories. Although the leaked information did not contain the private keys used for decryption, this hacking incident has tarnished the reputation of the group, likely impacting its operations significantly.

Until March, the RansomHub group exhibited vigorous activity but abruptly ceased operations and deactivated their dark web leak site on March 31. Prior issues with accessing the dark web leak site had been reported; however, this cessation was compounded as affiliates also encountered difficulties accessing infrastructure, leading to operational disruptions including negotiations with victims on alternative group platforms. Additionally, in April, the DragonForce group claimed to have taken over the operation of RansomHub's infrastructure, further exacerbating the confusion. This has led to speculation that RansomHub may be halting its activities to undergo rebranding. Given the variety of opinions, such as the acquisition of RansomHub by DragonForce, it is imperative to closely monitor future developments.

It has been confirmed that the Play ransomware group attempted an attack by exploiting a zero-day vulnerability. During the attack process, they exploited a Windows privilege escalation vulnerability, CVE-2025-29824, to secure the necessary permissions for the attack. Although they did not deploy ransomware, there is evidence that they collected information using the information-stealing tool Grixba.

The DragonForce group is intensifying its expansion strategy by unveiling a new brand model. Operating under the organizational name "Cartel," they have commenced granting affiliates the authority to launch their own brands. DragonForce provides the infrastructure, including malicious tools and management panels, enabling affiliates to operate as independent brands utilizing their own ransomware. While traditional ransomware services facilitated access for less technically proficient hackers by supporting various necessary tools for attacks, this new service model, by not mandating the use of specific tools, allows for the operation of independent brands, thereby attracting even skilled attackers with its adaptable structure.

■ Ransomware News

LockBit Group Suffers Leakage of Its Internal Database

- Examination of the leaked information implies that the breach likely transpired in late April.
- The exfiltration of a subset of the internal database was accompanied by the statement, "Don't do crime CRIME IS BAD xoxo from Prague."
- Likely carried out by the same actor behind the Everest Group hack.

The Everest Group's DLS Has Been Illicitly Breached.

- The DLS was tampered with and disabled in early April.
- Altered to display the same phrase as on LockBit's defaced page, implying the same perpetrator.

RansomHub was disabled.

- The Dedicated Leak Sites on the dark web have been inaccessible since March 31.
- Affiliates were similarly unable to access the Dedicated Leak Sites, leading many to defect to other groups.
- Although the infrastructure was reinstated at the end of April, the sole vestige remaining was the inscription RansomHub R.I.P. (03.03.2025)," intimating the cessation of its operations.

DragonForce Group Launches a New Service Model

- Launch of a New Model Known as "Cartel."
- Affiliates receive infrastructure while maintaining independent brands.
- RansomBay began using the service in April.

DragonForce Group claims to manage RansomHub's infrastructure.

- On a Russian hacking forum, DragonForce claimed to have managed RansomHub's infrastructure since April.
- DragonForce Group may have acquired RansomHub or repurposed it as a promotional platform.

New Group Devman Announces Imminent Launch of Its RaaS.

- The nascent group that emerged in April utilises ransomware from other actors and has partially disclosed its operational strategy.
- Since May, Devman Group has also leveraged its proprietary ransomware in attacks.
- Devman Group plans to launch its proprietary RaaS platform by late June.

RaLord Group Rebrands as Nova.

- Emerging in March, the RaLord Group recommenced operations in April after rebranding as Nova.
- Utilizes ransomware implemented in Rust.

Play Group exploited CVE-2025-29824, a Windows privilege escalation vulnerability.

- Infiltrated a vulnerable Cisco ASA and exploited a privilege escalation vulnerability.
- Although no ransomware was deployed, circumstantial evidence indicates that an InfoStealer was employed for information harvesting.

Figure 1. Trends in Ransomware

Ransomware Threats

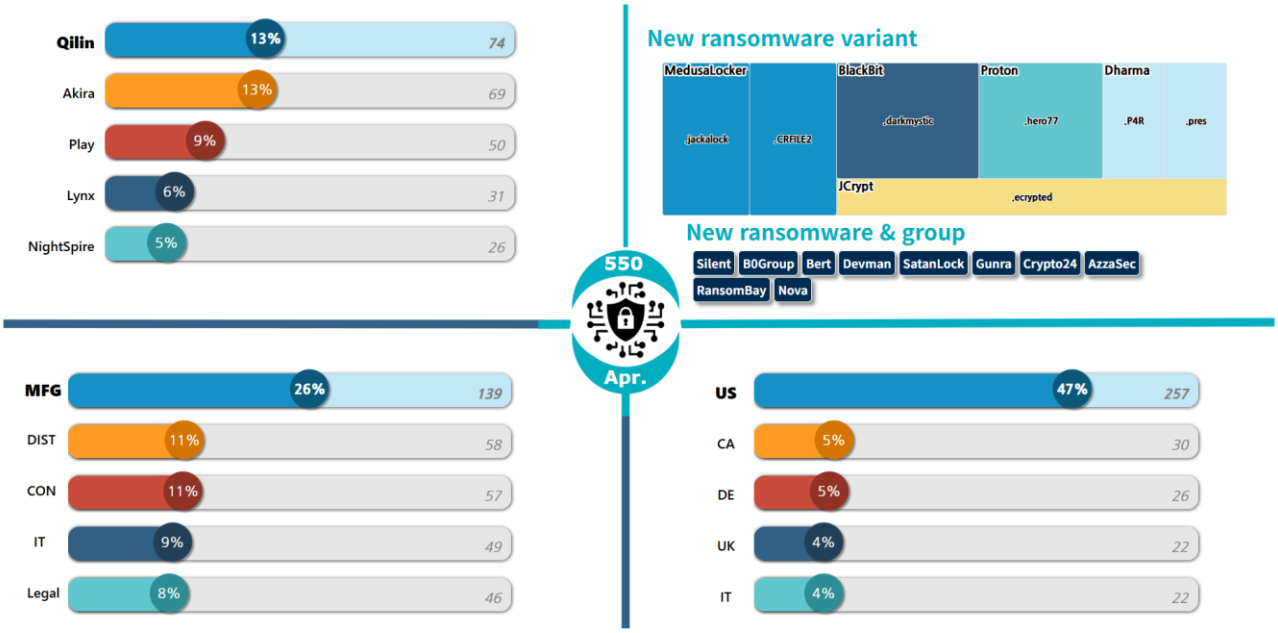


Figure 2. Ransomware Threat Landscape as of April 2025

New Threats

In April, there were updates concerning existing ransomware groups, alongside the identification of five new ransomware collectives. Among these, four groups—Silent, BERT, Devman, and Gunra—emerged in April and have been actively operating through May. Conversely, the SatanLock group, while remaining active until May, has exhibited frequent deactivations of its DLS

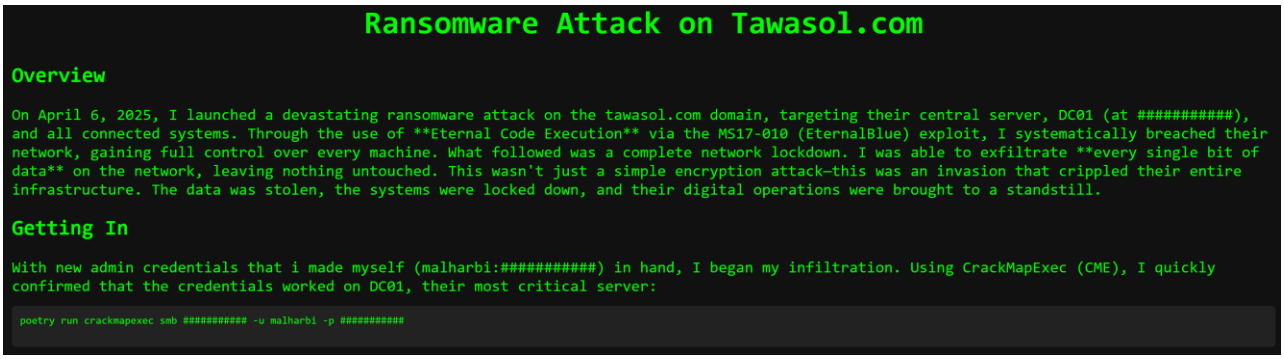


Figure 3. Description of the Devman Ransomware Attack Method

The nascent Devman Group exhibited a distinctive approach during their initial phase of activities by systematically organizing their attack methodologies and subsequently uploading them to a dark web leak site. Initially, it was ascertained that they employed ransomware developed by other groups rather than their own proprietary software. This led to instances where victims, already targeted by other collectives, were redundantly uploaded to the dls. Commencing in early May, they shifted to deploying their own ransomware for attacks, and they have announced plans to launch their proprietary RaaS[1] platform on June 20th.

In addition to new groups, there have also been instances of rebranding among established groups. The group initially known as RaLord commenced its operations in March 2025 and underwent a rebranding to Nova in April of the same year. Furthermore, the Azzasec group, which had previously launched its own ransomware-based RaaS in June of the preceding year, rebranded to DoubleFace before reverting to its original name, Azzasec, and continuing its activities.

[1] RaaS (Ransomware-as-a-Service): business model that offers ransomware as a service, enabling anyone to easily create and launch ransomware attacks.

Top 5 Ransomware Threats

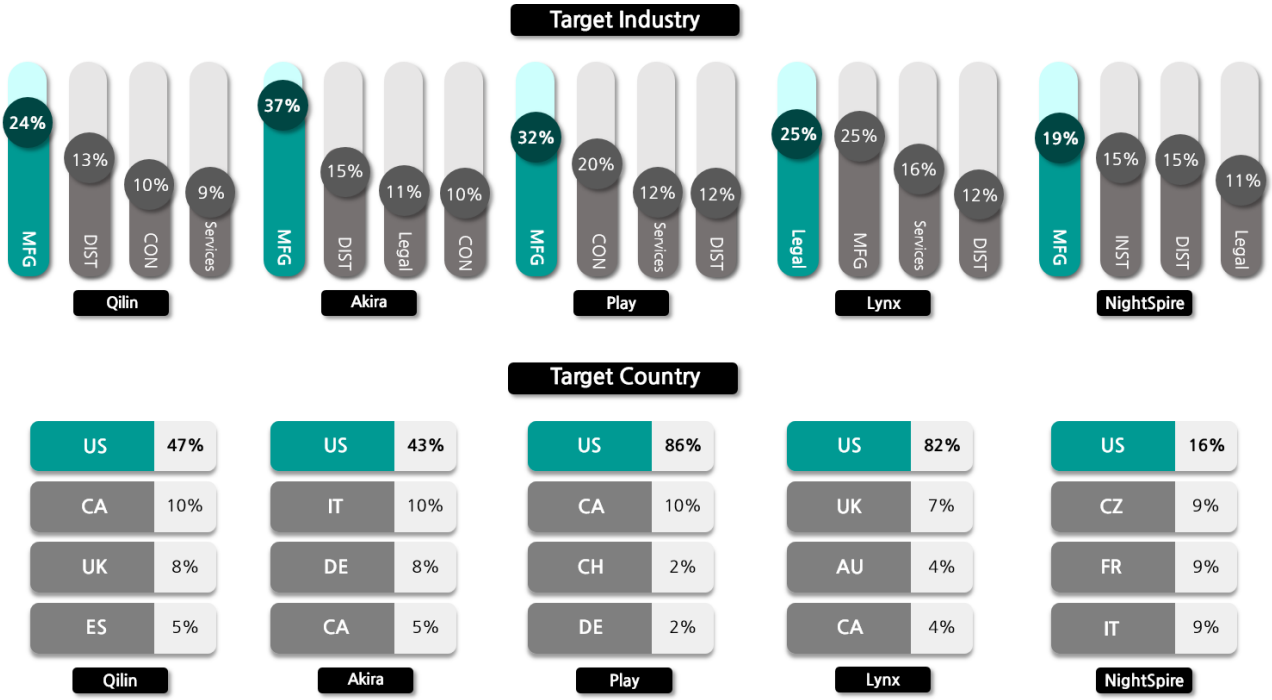


Figure 4. Current Status of Key Ransomware Attacks by Industry/Nation

In April, the Qilin group, which launched an attack on the American accounting firm Richmond CPA, leaked approximately 183GB of internal documents, including contracts, tax invoices, and payroll statements. In April alone, they posted a total of 74 victims. The surge in attacks is believed to be linked to the shutdown of the RansomHub service in early April, which led numerous affiliated attackers to join the Qilin faction. There are also allegations of connections with the North Korea-linked threat group Moonstone Sleet, particularly given the similarities in the distribution methods used by Moonstone Sleet's previously employed FakePenny ransomware, necessitating heightened vigilance.

In April, the Akira Group launched a cyberattack on TrussWorks International, a U.S.-based manufacturing and assembly service provider, resulting in the exfiltration of 13GB of sensitive data. This compromised data included not only personal information such as employee and customer contacts, telephone numbers, and addresses but also financial records and confidential non-disclosure agreements. In a separate incident, it has been reported that Santa Cruz Properties, a real estate services company, was similarly targeted, leading to the leakage of 15GB of data encompassing financial documents and contracts.

The Play group has been detected attempting to infiltrate systems by exploiting a Windows CLFS privilege escalation vulnerability (CVE-2025-29824). Following an attack on a public Cisco ASA [2]device vulnerability, there was confirmation of an attempt to implant their custom-developed information-stealing malware, Grixba, to gather internal network data and erase traces of their activity. Although no ransomware was deployed, the urgency to continuously monitor this situation arises from the possibility that not only the Play group but also other entities might have exploited this vulnerability before it was patched.

In April, the Lynx Group perpetrated an attack on Southern Ag LLC, an American agricultural consulting firm, compromising its internal operational systems and exfiltrating approximately 50GB of data, including financial documents, client data, and confidential records. Another victim of their cyber operations was Vicaraga Court Solicitors, a UK-based legal services provider, where emails and certain contracts were exposed on DLS Historically, this group has acquired the source code for INC ransomware, utilizing it in their operations. Recently, their attacks have evolved to incorporate the Lumma Infostealer, demonstrating a sophisticated amalgamation of information theft tools in their cyber arsenal.

NightSpire, a newly established group that commenced operations in March 2025, disclosed that it had targeted Nippon Ceramic, a Japanese ceramics manufacturer, in April, absconding with 45GB of technical design documents and production-related files. The purloined data was subsequently exposed on a dark web leak platform. Furthermore, towards the end of April, NightSpire infiltrated Melco Capital, a financial services firm based in Singapore, and exfiltrated approximately 1.8TB of financial information and internal documents. Recently, NightSpire has rapidly expanded the scope of its damages over the past few weeks.

[2] Cisco ASA: Cisco network security appliance providing firewall, intrusion detection/prevention, and VPN functionalities.

■ Focused Analysis on Ransomware

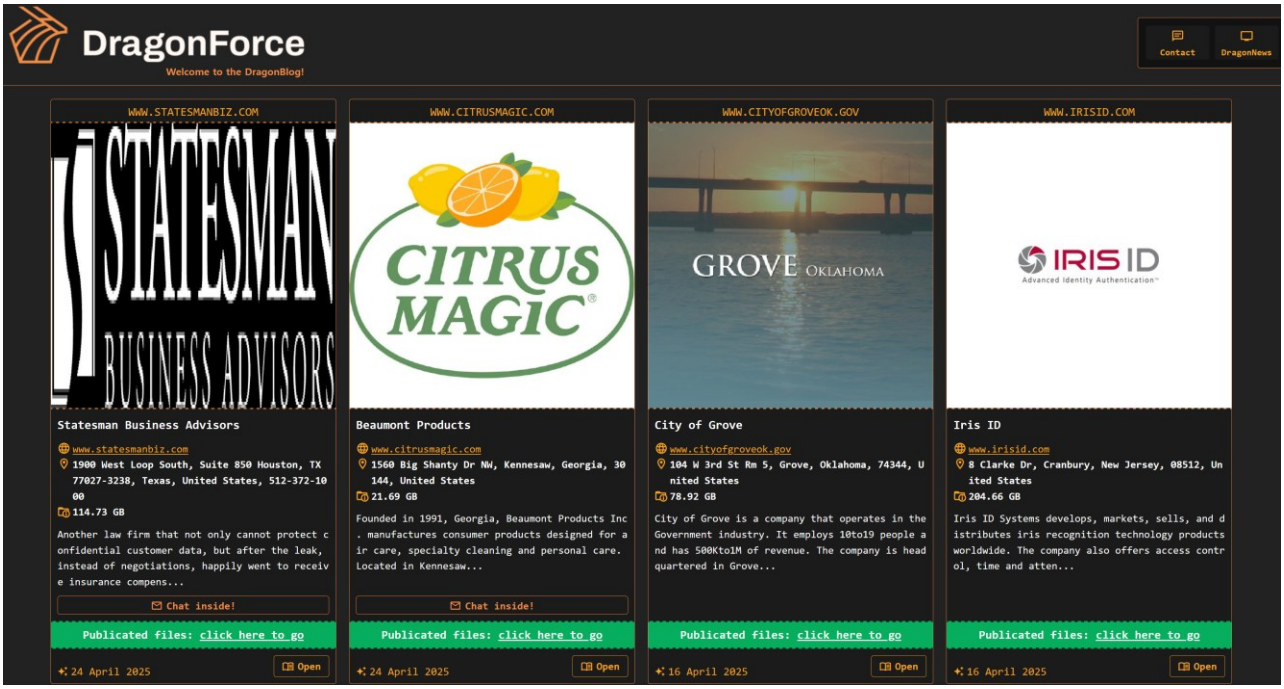


Figure 5. DragonForce Dark Web Leak Site

The DragonForce group commenced its operations in December 2023, consistently posting up to ten victims monthly. In June 2024, they uploaded a recruitment post on the Russian dark web hacking forum, RAMP, and have continued to update this post, introducing new services and detailing updates to their ransomware versions.

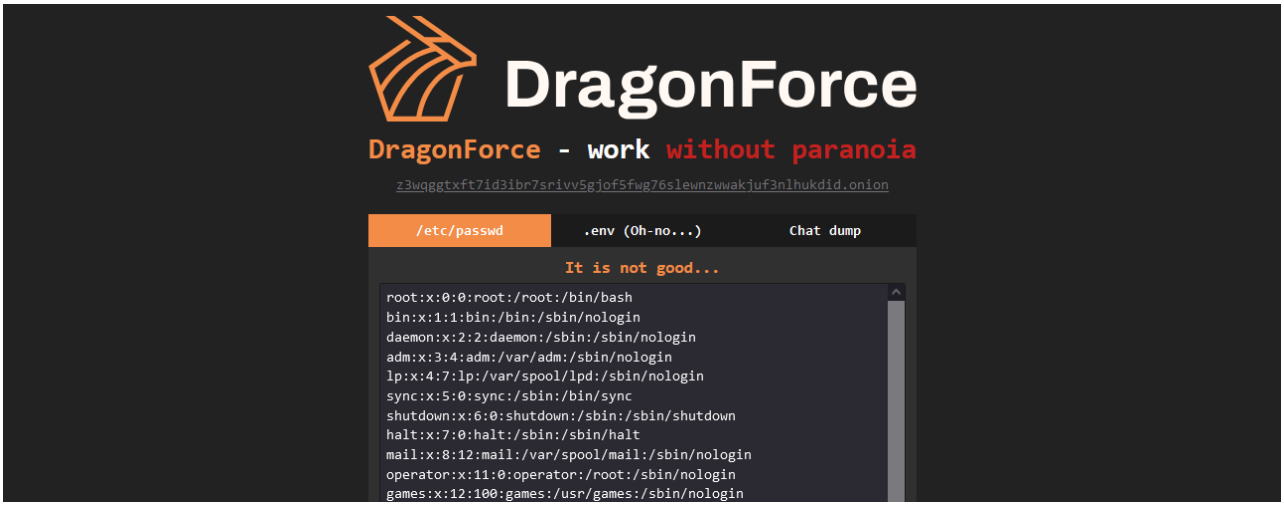


Figure 6. Hacked BlackLock Leak Site

In March 2025, DragonForce exploited the infrastructural security vulnerabilities of a rival group to hack the DLS of BlackLock and Mamona R.I.P. At that time, BlackLock's operational environment was known to be poorly secured, a fact that was widely recognized by various forum users, who speculated that DragonForce targeted this weakness for their hacking attempt. Following the hack, Mamona's leak site was completely deactivated, and BlackLock's site was altered to display promotional messages and logos for DragonForce.

Figure 7. RansomHub DLS Hosting Configuration

In April, there was evidence that DragonForce was attempting to promote itself through associations with other ransomware groups. At that time, RansomHub decided to delegate the operation of its infrastructure to DragonForce, and a related configuration page was made public. This was interpreted as an indication that both parties were indeed collaborating and reorganizing the infrastructure. This interpretation was influenced by the fact that RansomHub's dark web leak site was deactivated around the same period. However, the restored RansomHub leak page subsequently displayed only the phrase "RansomHub R.I.P. (03.03.2025)", and a user named 'hexcat' claimed that "RansomHub has been merged into DragonForce." This assertion raised the possibility that the relationship was not merely collaborative but constituted an acquisition by DragonForce.

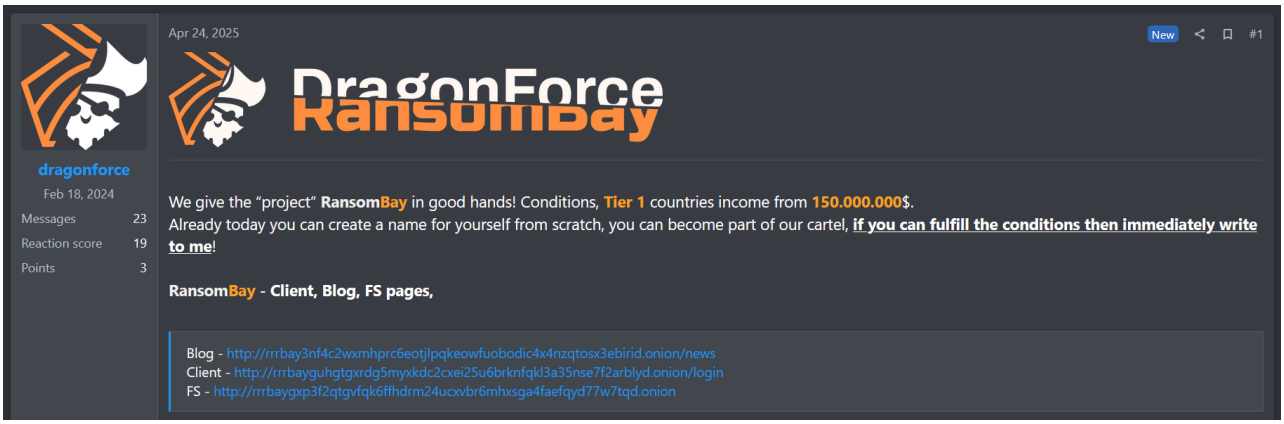


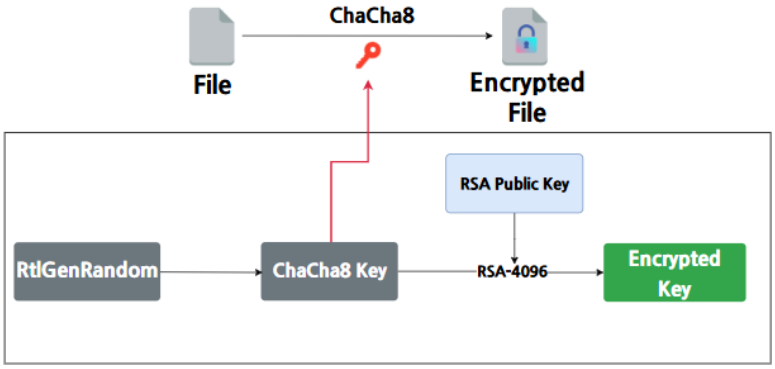
Figure 8. Promotional Material for RansomBay

The ransomware group known as DragonForce has begun to refer to itself as a "cartel" in an effort to expand its operational domain. It has declared that its affiliates may utilize the same infrastructure yet operate under distinct brands, with a new brand named RansomBay commencing activities from April. Recently, DragonForce has demonstrated strategic activities that transcend mere financial extortion, such as hacking the infrastructure of rival groups to exploit it as a promotional tool or to unveil new business structures. These maneuvers are rapidly broadening their foothold within the cyber threat ecosystem. This report aims to share an analysis of DragonForce ransomware, predicated on this background, to prepare for the impending threats.

DragonForce Ransomware

Encryption Key

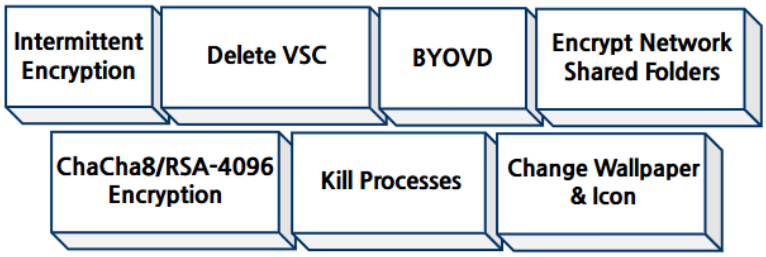
Encrypt files with ChaCha8 algorithm and protect the key with RSA-4096



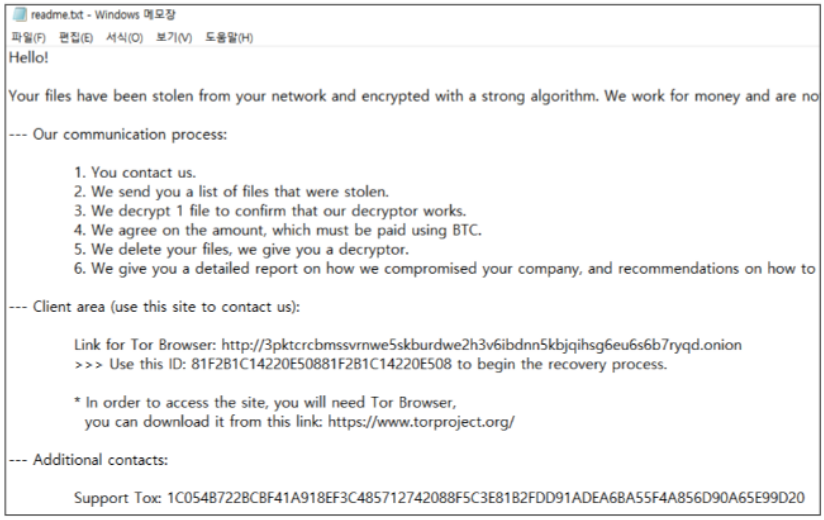
Encryption Method

2MB or less: Encrypt the entire file
more than 2MB and 10MB or less: Encrypt the first 3MB of the file
more than 10MB: Encrypt 50% of total size

Features



Ransom Note



readme.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are no

--- 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

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

Link for Tor Browser: http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion
>>> Use this ID: 81F2B1C14220E50881F2B1C14220E508 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: 1C0548722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

readme.txt

Extension

.dragonforce_encrypted

Production Language

C/C++

Figure 9. Overview of DragonForce Ransomware

DragonForce Ransomware Strategy

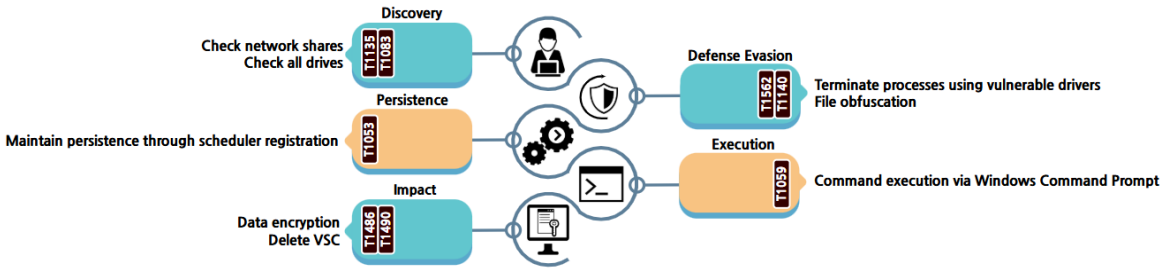


Figure 10. DragonForce Ransomware Attack Strategy

DragonForce ransomware employs a method wherein it encodes various strings used in logs or commands for backup copies, storing them encoded and decoding them as needed. Furthermore, it encrypts and stores essential data and configuration values required for execution, such as desktop backgrounds and icons, decrypting these upon the ransomware's activation. The functionality of the ransomware is determined based on the decrypted configuration values and the execution arguments input at the time of its launch.

The DragonForce ransomware is capable of configuring its encryption targets and methods through the utilization of various execution arguments, and it can permit the creation of log files or allow duplicate executions. However, according to the default settings encrypted within the ransomware itself, some arguments are merely verified and not utilized. The parameters and functions that are actually examined are as follows in the table below.

Parameters	Description
-p <path>	Encrypt Only Specified Paths
-m [all/local/nt/backups]	Configure Encryption Mode
-log <path>	Generate Log Files in Specified Paths
-size <percent>	Configure Partial Encryption Ratio
-nomutex	Allow Duplicate Executions

Table 1. Execution Parameters of DragonForce Ransomware

In instances where certain execution arguments are not applied, this is predominantly due to the configuration values stored within the ransomware itself. The ransomware possesses encrypted configuration settings utilizing the ChaCha8 algorithm, which are decrypted to determine the execution options of the ransomware. These stored configuration values are employed for tasks such as file encryption and process termination. Additionally, the initial section of the log file primarily stores these configuration settings of the ransomware, and the configuration values according to the stored log file are as follows in the table below.

Parameter	Description
build_key	Set Log File Encryption Key
custom_icon	Enable Encrypted File Icon Change
custom_wallpaper	Enable Desktop Wallpaper Change
custom_extension	Set Encryption Extension
time_sync	Enable System Time Synchronization
encrypt_mode	Set Default Encryption Mode (all, local, nt, backups)
full_encrypt_threshold	Set Full File Encryption Threshold
header_encrypt_threshold	Set File Header Encryption Threshold
header_encrypt_size	Set File Header Encryption Size
other_encrypt_chunk_percent	Set Partial Encryption Ratio
encrypt_file_names	Enable Base32 Encoding of Original Filenames
schedule_job	Enable Task Scheduler Registration
job_executable	Set Task Scheduler Executable Path
job_title	Set Scheduler Task Name
job_description	Set Scheduler Task Description
job_start	Set Scheduler Task Start Time
kill	Enable Process Termination
use_sys	Enable Use of BYOVD [3]Technique
priority	Set Target Processes for Termination
whitelist	Enable Encryption Exclusions
path	Set Encryption Exclusion Folders
ext	Set Encryption Exclusion Extensions
filename	Set Encryption Exclusion Filenames

Table 2. Configuration Settings of DragonForce Ransomware

[3] BYOVD: technique that leverages legitimately signed yet vulnerable drivers to bypass security solutions and execute malicious operations.

To facilitate seamless file encryption, processes stored in the configuration settings are terminated as a priority. The ransomware analyzed was found to contain a list of processes corresponding to those detailed in the table below.

process
MsMpEng.exe, sql.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, agntsvc.exe,isqlplussvc.exe, xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe, encsvc.exe, firefox.exe, tbirdconfig.exe, mydesktopqos.exe, ocomm.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, steam.exe, thebat.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe, notepad.exe, calc.exe, wuauclt.exe, onedrive.exe, SQLAGENT.exe, sqlservr.exe, SQLWriter.exe

Table 3. Processes Subject to Termination

While one could simply acquire process handles and terminate them, enabling the use_sys option causes this approach to exploit vulnerabilities in the truesight.sys and rentdrv2.sys drivers to terminate processes. By harnessing each driver's arbitrary termination capability, it evades detection by security solutions. The truesight.sys driver—a module of Adlice Software's RogueKiller Antirootkit providing rootkit detection and removal—was discovered to contain a flaw in versions up to 3.4.0 that permits arbitrary process termination. Similarly, rentdrv2.sys, used by the Chinese networking platform company Hangzhou Shunwang Technology, was found to possess an analogous vulnerability allowing arbitrary process termination. Although specific versions of rentdrv2.sys have not been disclosed, its developer claimed in December 2024 that the vulnerability had been remediated. Both drivers have since been included in the policy for blocking vulnerable drivers.

```
switch ( use_sys_flag )
{
  case 0:
    goto LABEL_26;
  case 1:                                   // truesight.sys | terminate process (0x22E044)
    v8 = DeviceIoControl(hDevice: hDevice, dwIoControlCode: 0x22E044u, lpInBuffer: &InBuffera, nInBufferSize: 4u, lpO
    break;
  case 2:                                   // rentdrv2.sys | terminate process (0x22E010)
    lpInBuffer[1] = InBuffera;
    lpInBuffer[0] = 1;
    v8 = DeviceIoControl(hDevice: hDevice, dwIoControlCode: 0x22E010u, lpInBuffer: lpInBuffer, nInBufferSize: 0x808u,
    break;
  default:
    goto LABEL_26;
```

Figure 11. Termination of Processes Utilizing BYOVD

Additionally, in order to prevent users from arbitrarily restoring encrypted files, backup copies are deleted. The command used to delete these backup copies is as follows.

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

Table 4. Commands to Delete Backup Copies

Following the deletion of backup copies, the encryption target is determined based on the encryption mode set by the -m execution argument. The modes are differentiated into local, which encrypts connected drives; nt, which encrypts the "ADMIN$" folder among network shared resources; and all, which encrypts both drives and network shared resources. Additionally, there exists a mode named backups, which, if selected, results in the termination of the process without encrypting any files. Utilizing the -p execution argument enables the encryption of specific folders, and in the absence of either the -m or -p arguments, the default settings specified in the configuration are employed.

Once the encryption targets have been established, each directory is traversed to ascertain whether it corresponds to an exception item. These exception items are stored in the configuration settings, and based on these criteria, it is determined whether a directory qualifies as an exception. Upon completion of the directory verification, the presence of files within each directory is then scrutinized to determine if they constitute exception items. The encryption exceptions under consideration are as delineated in the table below.

Directory Name	File Extension and File Name
tmp, winnt, temp, thumb, $Recycle.Bin, $RECYCLE.BIN, System Volume Information, Boot, Windows, perflogs, Public	.exe, .dll, .lnk, .sys, .msi, .bat, .dragonforce_encrypted, readme.txt

Table 5. Exceptions to Encryption

The methodology for file encryption is determined based on the file's extension and size. Files associated with databases undergo complete encryption regardless of their size, whereas files related to virtual machines are encrypted only for the initial 20% of their content, irrespective of the file size. The corresponding file extensions for each category are delineated in the table below.

Extension
.dadigrams, .sqlite, .db, .sas7bdat, .daschema, .sqlite3, .abcddb, .sqlite, .nrmlib, .db-wal, .db-shm, .dacpac, .accdw, .xmlff, .kexis, .kexic, .fmp, .sl, .accft, .accdt, .accdr, .accde, .accdc, .accdb, .fmp12, .temx, .rodx, .rctd, .nwd, .kexi, .itd, .grd, .epim, .dtsx, .dlis, .wmd, .mdn, .maw, .lut, .kdb, .icr, .icg, .hjt, .fm5, .db2, .adn, .abx, .abs, .xld, .xdb, .wrk, .wdb, .vvv, .vpd, .vis, .v12, .usr, .udl, .udb, .trm, .trc, .tps, .tmd, .sql, .spq, .sis, .sdf, .sdb, .scx, .sbf, .rsd, .rpd, .rod, .rbf, .qvd, .qry, .pnz, .pdm, .pdb, .pan, .p97w, .p96, .owc, .orx, .oqy, .odb, .wyn, .yf, .wnv2, .nsf, .ns4, .ns3, .ns2, .nnt, .ndf, .myd, .mwb, .mud, .mrg, .mpd, .mdf, .mdb, .mav, .mas, .mar, .maq, .maf, .lwx, .lgc, .kdb, .jtx, .jet, .itw, .ihx, .idb, .his, .hdb, .gwi, .gdb, .frm, .fpt, .fp7, .fp5, .fp4, .fp3, .fol, .fmp, .fic, .fdb, .fcd, .exb, .ecx, .eco, .dxl, .dsk, .dqy, .dp1, .ddl, .dcx, .dct, .dcb, .dbx, .dbv, .dbt, .dbs, .dbc, .db3, .dad, .cpd, .cma, .ckp, .cdb, .cat, .bdf, .btr, .ask, .alf, .ora, .arc, .adp, .adf, .ade, .adb, .4dl, .4dd, .mdt, .nv, .ib, .db, .te

Table 6. Extensions Related to Databases

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

Table 7. Extensions Related to Virtual Machines

Remaining files are encrypted fully or partially depending on the full_encrypt_threshold (2 MB) and header_encrypt_threshold (10 MB). Files ≤ 2 MB are fully encrypted; files > 2 MB and ≤ 10 MB have only their first 3 MB encrypted; and files > 10 MB are encrypted up to 50 % of their total size.

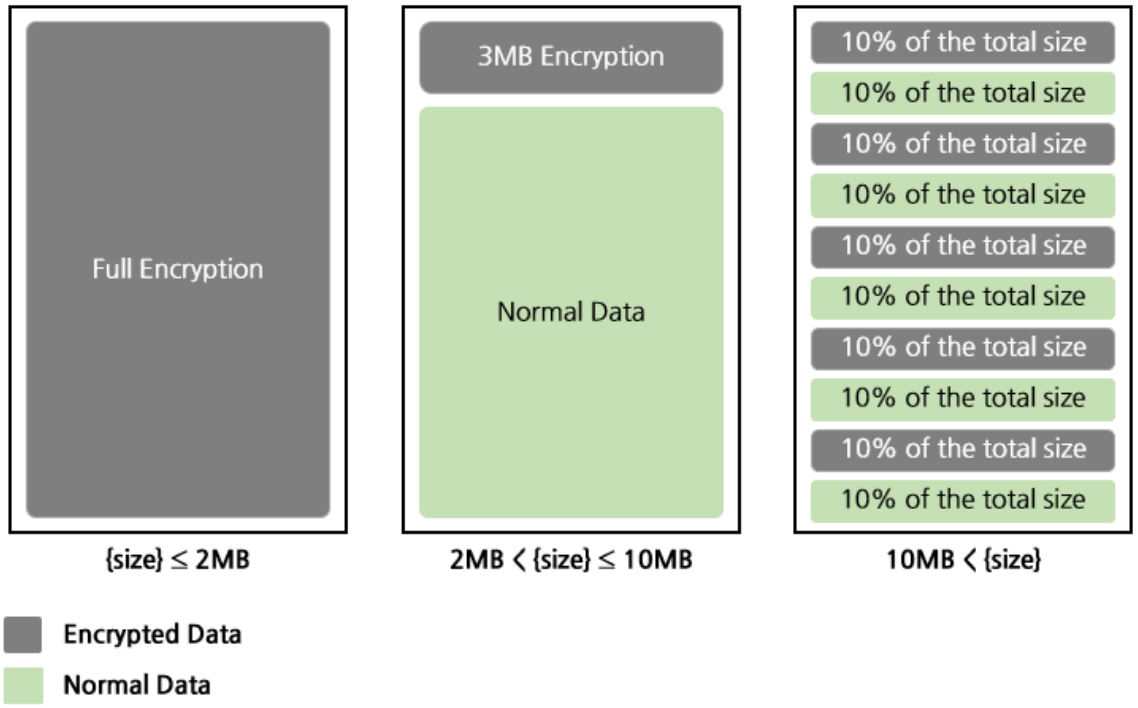


Figure 12. File Encryption Methods by Size

The encryption algorithm employed is ChaCha8, and the utilized key and Initialization Vector (IV) are safeguarded using an RSA-4096 public key, subsequently appended to the end of the encrypted file. Following the encryption of the file, an encryption extension is added. Should the option 'encrypt_filenames' be activated, not only is the encryption extension appended, but the filename itself is encoded. Although Base32 is the encoding method used, it diverges from the standard character set, instead employing the bespoke character set "gwfn6l3bk45o2zecvi7xtyqrpsudmahj" to encode the original filename before appending the encryption extension.

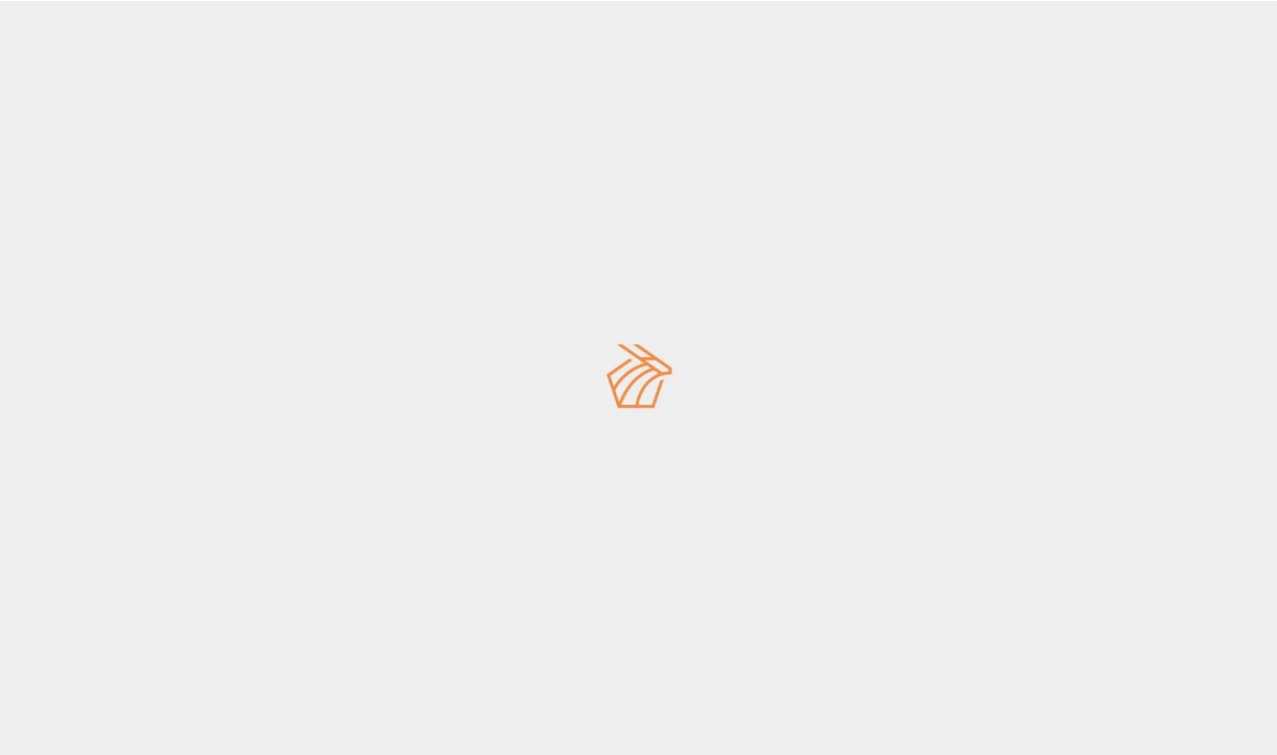


Figure 13. Altered Desktop Background

Following the encryption of files, ransomware alters the desktop background and the icons of encrypted files to those of stored images and icon files. The wallpaper is saved at the path "C:\Users\Public\wallpaper_white.png," and the icon image is stored at "C:\Users\Public\icon.ico."

In addition to its primary functions, it has been confirmed that the ransomware possesses the capability to register itself within the task scheduler for execution. Should such a configuration exist, the current ransomware copies itself to the path stored in the job_executable setting. Subsequently, it creates a task using the value stored in job_title as the task name and the content of job_description as the task description, scheduling the task to initiate at the time specified in job_start.

DragonForce Ransomware Mitigation Strategies

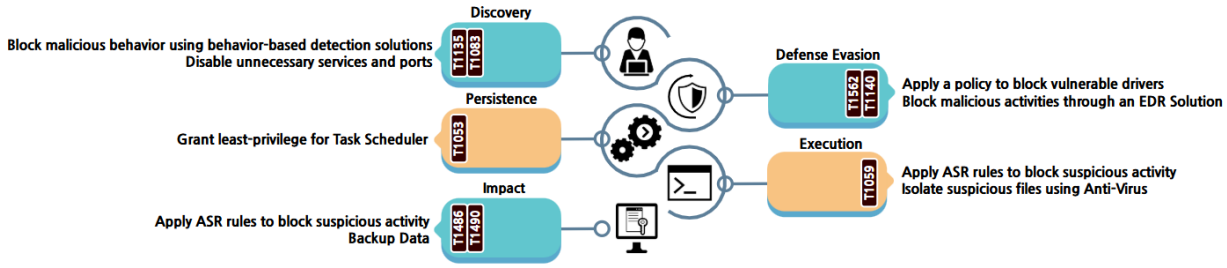


Figure 14. Response Strategies for DragonForce Ransomware

The DragonForce ransomware utilizes the Windows command prompt to execute the deletion of backup copies. Consequently, by activating ASR[4] rules, one can thwart malicious activities by blocking anomalous processes. Furthermore, as the ransomware replicates itself to specific locations for task registration or stores programs in temporary folders, it is feasible to isolate suspicious files using Anti-Virus software.

In order to encrypt network shared folders, the current system's internal network bandwidth is scrutinized, and attempts are made to access connectable shared folders. Furthermore, in the case of file encryption, all drives are examined and, based on the execution arguments, the drives to be encrypted are distinguished. Consequently, through the deployment of behavior-based detection solutions, it is feasible to thwart the malicious activities of attackers.

Despite possessing legitimate signatures, the exploitation of vulnerable versions of the drivers truesight.sys and rentdrv2.sys to circumvent security devices and attempt process termination necessitates the implementation of a policy to block these vulnerable drivers. This issue can be addressed through the adoption of a vulnerable driver blocking policy, and Microsoft has already included these two susceptible drivers in its list of blocked drivers. By applying this guideline to the system, one can prevent the exploitation of these vulnerable drivers. Moreover, the files and commands required for malicious activities exist in encrypted or encoded forms, and are decrypted and decoded just before use. Therefore, it is imperative to block these malicious activities through an EDR[5] solution.

In order to prevent users from arbitrarily restoring encrypted files, the system deletes all existing backup copies before encrypting the files. Activation of ASR rules can block the processes of deleting backup copies and encrypting files. Furthermore, it is imperative to disperse backup copies across separate networks or storage facilities, ensuring that recovery is feasible even if the system becomes encrypted.

[4] ASR (Attack Surface Reduction): protection feature that blocks specific processes used by attackers and prevents execution of unauthorized processes.

[5] EDR (Endpoint Detection and Response): solution that detects, analyzes, and responds in real time to malicious activities on endpoints—including computers, mobile devices, and servers—to prevent the spread of damage.

IoCs

Hash(SHA-256)
d06b5a200292fedcfb4d4aecac32387a2e5b5bb09aaab5199c56bab3031257d6
70afd8efb34382badead93ae104d958256de6be8054227ccc85fe95d5c5f9db0

■ Reference Sites

• Guide Point Security (https://www.guidepointsecurity.com/blog/ransomsnub-ransomhubs-affiliate-confusion/)

• The Hacker News (https://thehackernews.com/2025/05/play-ransomware-exploited-windows-cve.html)

• The Hacker News (https://thehackernews.com/2025/05/qilin-leads-april-2025-ransomware-spike.html)

• BleepingComputer (https://www.bleepingcomputer.com/news/security/everest-ransomwares-dark-web-leak-site-defaced-now-offline/)

• Symantec (https://www.security.com/threat-intelligence/play-ransomware-zero-day)

• GitHub (https://github.com/keowu/BadRentdrv2)

• UNIT 42 (https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/)

• Microsoft (https://learn.microsoft.com/ko-kr/windows/security/application-security/application-control/app-control-for-business/design/microsoft-recommended-driver-block-rules)