

Millenium: A RAT Rewritten, A Threat Multiplied

 group-ib.com/blog/millenium-rat-maas

June 25, 2026

Threat Actor Profile

GROUP-IB



ShinyEnigma

ShinyEnigma is the developer of Millenium RAT and DotStealer.

Modus operandi

Threat actor utilizes various channels to advertise malware, such as underground forums, dedicated website, and platforms like GitHub, offering it as Malware-as-a-Service (MaaS) under a subscription model.

First seen
September 2023

Skillset
.NET, C++

Toolset
Millenium RAT, DotStealer

Targeted Countries
Global

Motivation
Financial gain, Stealing sensitive data

Group-IB, 2026

Introduction

The Millenium RAT first surfaced in a threat report by [CYFIRMA](#) on November 3, 2023, initially tracked with malware version 2.4. Group-IB's current intelligence suggests a significant evolution in the threat landscape, evidenced by the predominant use of version 4.* of the malware. This newer version continues to leverage a C2 architecture via Telegram bot API. As a full-featured remote access trojan, Millenium RAT 4.* is designed to compromise Windows machines. It enables threat actors to exfiltrate sensitive browser and system data, capture screenshots and audio, perform keylogging, and download and run arbitrary executables.

The malware continues to be promoted across underground forums and even legitimate platforms like GitHub, by the developer operating under the moniker "shinyenigma". The malware is offered as Malware-as-a-Service (MaaS) with a pricing model of \$50 USD for the first month, \$10 USD for subsequent months, or a one-time \$90 USD lifetime purchase.

The active exploitation campaigns detailed within this blog are carried out by the threat actor cluster Group-IB tracks as the Y2K Operators, and a critical architectural shift is observed in the 4.* versions. The malware is no longer being developed using the .NET framework but is

written in C++ and compiled as a native application. Analyzing our telemetry, Group-IB's Threat Intelligence has documented a substantial number of compromised endpoints, specifically identifying 62,289 infected devices with the Millenium RAT 4.* versions. The velocity of these infections appears to have accelerated recently, with 39,730 of the total compromised devices having been infected within the first quarter of 2026 alone.

Group-IB analysts will provide a comprehensive look at the threat actor cluster, Y2K Operators, examining their methods, including the social engineering tactics they utilize to lure victims globally, and detailing the extensive victimology across affected geographies. The following sections will then break down the technical specifics of the Millenium RAT version 4.*, diving deep into its configuration loading and decryption process.

Key discoveries

- Millenium RAT version 4.* is written in C++, shifting from earlier .NET versions and removing the dependency on the .NET framework.
- The malware uses Telegram bots as C2.
- The RAT's functionality relies entirely on standard Windows API calls.
- Group-IB telemetry reveals over 62,000 compromised endpoints across 160+ countries, with Q1 2026 alone accounting for over 39,000 infections.
- Millenium developer distributes the RAT via a subscription-based MaaS model.

Who may find this blog interesting:

- Cybersecurity analysts
- Malware researchers
- Threat intelligence analysts and specialists
- Law enforcement investigators

Group-IB Threat Intelligence Portal

Group-IB customers can access our Threat Intelligence portal for more information about this threat actor / malware.

Threat Actors:

- [ShinyEnigma](#)
- [Y2K Operators](#)

Malware:

Public Malware Detonations:

Access free detonation reports linked to Millenium RAT and watch malware operate in real time through detailed insights from the [Group-IB Malware Detonation Platform](#):

- [Millenium RAT Sample #1](#)
- [Millenium RAT Sample #2](#)
- [Millenium RAT Sample #3](#)

Threat Actor Profile





ShinyEnigma

ShinyEnigma is the developer of Millenium RAT and DotStealer.

Modus operandi

Threat actor utilizes various channels to advertise malware, such as underground forums, dedicated website, and platforms like GitHub, offering it as Malware-as-a-Service (MaaS) under a subscription model.



First seen
September 2023

Skillset
.NET, C++

Toolset
Millenium RAT,
DotStealer

Targeted Countries
Global

Motivation
Financial gain,
Stealing sensitive data

Group-IB, 2026



Millenium RAT

Platforms

Windows

First seen

September 2023

Millenium RAT is a malware targeting Windows machines. It enables its operators to exfiltrate browser data and data from local systems, download and run arbitrary executables, capture screenshots, audio, and perform keylogging. Notably, versions 4.* are written in C++ and compiled as a native application, which removes the dependency on the .NET framework. It also utilizes a C2 architecture based on the Telegram Bot API.

Used by

ShinyEnigma

Y2K Operators



Techniques

T1106 - Native API

T1204.002 - User Execution. Malicious File

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

T1548.002 - Abuse Elevation Control Mechanism. Bypass User Account Control

T1036.005 - Masquerading. Match Legitimate Resource Name or Location

T1539 - Steal Web Session Cookie

T1217 - Browser Information Discovery

T1560 - Archive Collected Data

T1041 - Exfiltration Over C2 Channel

T1102.002 - Web Service. Bidirectional Communication

Group-IB, 2026

Millenium RAT-vertising

The developer of Millenium RAT operates under the moniker “shinyenigma” and advertises in underground forums, legitimate developer platforms like GitHub and its own website [hxxps://milleniumrat\[.\]online](https://milleniumrat[.]online).

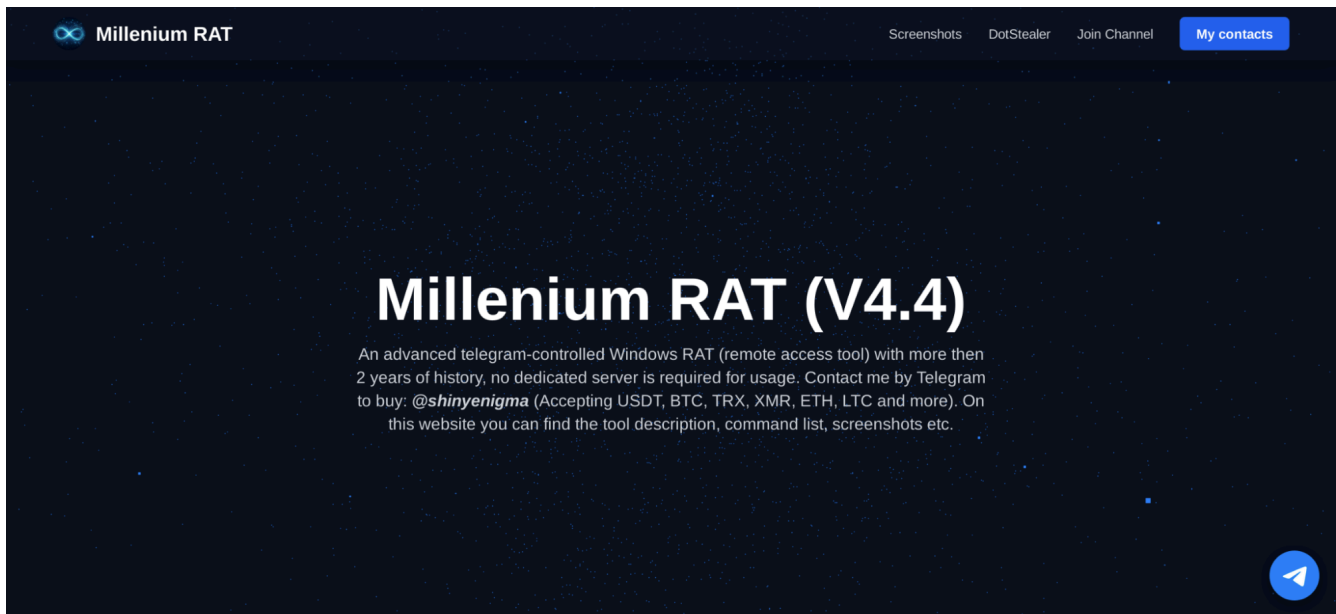


Figure 1. [hxxps://milleniumrat\[.\]online](https://milleniumrat[.]online)

Through the course of this research, the following repositories were observed to be used by ShinyEnigma to advertise Millenium RAT v4.*. However, at the time of writing, the GitHub and Gitea repositories have already been removed. It is important to note that the original commit messages in the Gitea repository were in Russian.

- [hxxps://gitlab\[.\]com/shinyspace/millenium-rat](https://gitlab[.]com/shinyspace/millenium-rat)
- [hxxps://github\[.\]com/shienigma/Millenium-RAT](https://github[.]com/shienigma/Millenium-RAT)
- [hxxps://gitea\[.\]com/shinyenigma/Millenium-RAT](https://gitea[.]com/shinyenigma/Millenium-RAT)

shinyenigma / Millenium-RAT

📶

👁 Watch

2

☆ Star

2

🍴 Fork

1

<> Code

🔍 Issues

🔗 Pull Requests

🎮 Actions

📁 Projects

📦 Releases

📖 Wiki

🔥 Activity

🕒 19 Commits

🌿 1 Branch

🏷 0 Tags

🌿 main

🌿 Commit Graph

19 Commits

Search commits...

This Branch

🔍

Author	SHA1	Message	Date		
shinyenigma	e69715be37	Обновить README.md	last month		
shinyenigma	b767419713	Обновить README.md	4 months ago		
shinyenigma	1ab8ec66fe	Загрузить файлы в «files»	4 months ago		
shinyenigma	0bd0ab16cb	Загрузить файлы в «files»	4 months ago		
shinyenigma	621d38b984	Удалить 6.png	4 months ago		
shinyenigma	e4205c00ed	Удалить 5.png	4 months ago		
shinyenigma	21494ea789	Удалить 4.png	4 months ago		
shinyenigma	61bdf9281d	Удалить 3.png	4 months ago		
shinyenigma	53159ff787	Удалить 3.1.png	4 months ago		
shinyenigma	769ec3d806	Удалить 2.png	4 months ago		
shinyenigma	0fc2bdf556	Удалить 1.png	4 months ago		
shinyenigma	86845a6e1c	Удалить 0.png	4 months ago		
shinyenigma	2328043f43	Обновить README.md	4 months ago		
shinyenigma	9ce3274ba7	Обновить README.md	8 months ago		
shinyenigma	dc4f928812	Загрузить файлы в «/»	8 months ago		
shinyenigma	de714bef2d	Обновить README.md	8 months ago		
shinyenigma	60916bb5c8	Загрузить файлы в «/»	8 months ago		
shinyenigma	12bbcb9649	Обновить README.md	8 months ago		
shinyenigma	8c5607e23b	Initial commit	8 months ago		

Figure 2. Commit messages in Gitea repository.

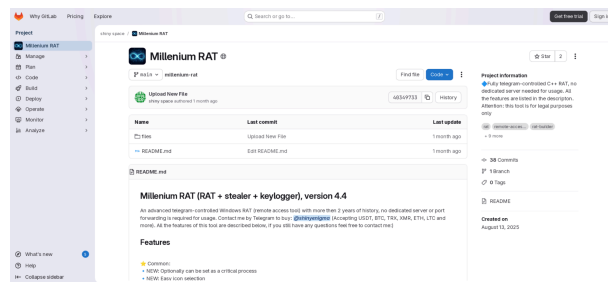


Figure 3. Examples of ShinyEnigma posting RAT advertisements in various git repository platforms.

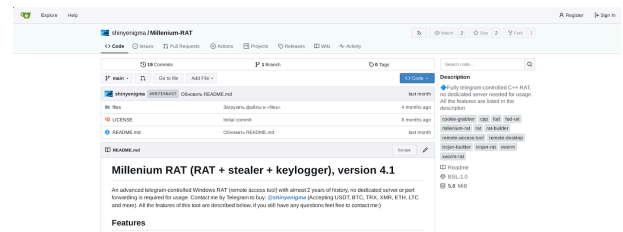


Figure 3. Examples of ShinyEnigma posting RAT advertisements in various git repository platforms.

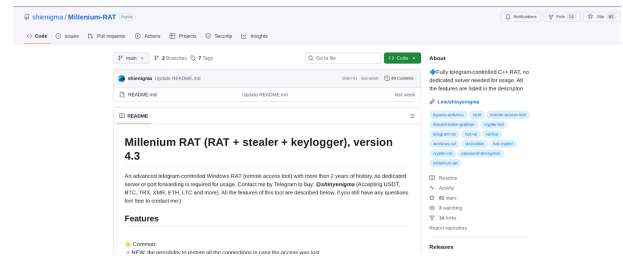


Figure 3. Examples of ShinyEnigma posting RAT advertisements in various git repository platforms.

1

shinyenigma

4 days ago

[SELL] Millenium RAT (Telegram-controlled Remote Access Tool + Stealer + Keylogger)

Sell

Selling an affordable C++ telegram-controlled RAT, only for Windows machines. The tool is already 2 years old and will be receiving more updates

General information:

- x86 native executable. No .NET, Microsoft Visual C++ is required
- Works on Windows 7-11 and (both x86 and x64 systems)
- No dedicated server needed - everything is controlled inside Telegram chat (private or group)
- Includes keylogger and stealing features
- The tool has installation module, anti-VM, anti-debug etc
- Fast Access Buttons (added in 4.1, can be enabled from the Advanced settings menu)

Available Features:

- NEW: Microphone capture
- Remote Powershell/CMD command execution
- Computer info grabbing (CPU, GPU, RAM, Country, city, IP, Mac Address etc)
- Discord token grabbing (from discord client and all the main browsers)
- Telegram data grabbing
- Browsers data grabbing: downloads, cookies, passwords, credit cards, history (with cookie app-bound key decryption)
- Wallet Recovery
- Webcam Capture
- Privilege elevation
- Messageboxes, setting wallpaper, display rotation
- Keylogger
- One-command desktop files grabbing
- User file encryption/decryption
- Minimize/maximize windows
- Get active window title/battery info/installed software list
- User log off/PC hibernating
- SendKeyPress feature
- Blue Screen of Death

Figure 4. Example of Millenium RAT advertisement in the Dread forum.

Malware Analysis

Millenium RAT version 4.* is built differently from the earlier versions which were written in .NET. Version 4 is written in C++ and compiled as a native application, which removes the dependency on the .NET framework. For communication, it uses libcurl to send and receive requests to the Telegram API.

Immediately after execution, the RAT loads its configuration from an embedded PE resource of type RCDATA. The resource contains Base64 encoded configuration data that is decoded at runtime. In addition to the actual configuration, the resource includes extra random Base64 data separated from the configuration by the “|” character. This additional data increases the overall size of the resource and is likely intended to alter the resulting file hash even when the core configuration remains unchanged.

In addition to Base64 encoding, the configuration is protected with a custom XOR-based algorithm. After decoding from Base64, the data is decrypted using a password embedded directly in the PE file.

```
[REDACTED] | [REDACTED] | 8Ze6Tf37GZVa | MsEdgeUpdate | 0 | 1 | [init_cmd_base64_encode  
d] | NONE | NONE | NONE | [endpoint_base64_encoded | Liu5GgJiKiKqe2Qs | svchost.exe | GTR  
1YB4A7s | Wjqs4e962HK.g0 | TRUE | TRUE | TRUE | TRUE | FALSE | TRUE | TRUE | FALSE
```

Figure 5. Decrypted configuration example.

The configuration itself is stored as a plain text string, with individual fields separated by the “|” character.

```
{
  "token": "telegrambot:token",
  "Id": chat_id_number,
  "name": "8Ze6Tf37GZVa",
  "startup_name": "MsEdgeUpdate",
  "start_delay": "0",
  "query_delay": "1",|
  "init_cmd": "/powershell*Add-MpPreference -ExclusionPath 'C:\\\\'",
  "content_type": "NONE",
  "caption": "NONE",
  "post_field": "NONE",
  "api": "https://api.telegram.org/",
  "install_foldername": "Liu5GgJiKiKqe2Qs",
  "install_filename": "svchost.exe",
  "keylog_foldername": "GTR1YB4A7s",
  "keylog_filename": "Wjqs4e962HK.g0",
  "persist": "TRUE",
  "keylogger": "TRUE",in
  "start_sysinfo": "TRUE",
  "procmon": "TRUE",
  "detect_sandbox": "FALSE",
  "elevate": "TRUE",
  "auto_steal": "TRUE",
  "decode_name": "FALSE"
}
```

Figure 6. JSON config representation.

The configuration format is a structured text string containing multiple fields:

Field Name	Description
token	Telegram bot token used for API communication
id	Telegram chat or group identifier used for command and control
name	Mutex name and registry value under HKCU\Software
start_delay	Fixed delay in seconds added to a random startup delay
query_delay	Fixed delay in seconds between requests to the Telegram API
init_cmd	Bot commands executed during the first launch
content_type	Likely used in HTTP requests, possibly for proxy handling

caption	Used when uploading files to Telegram and possibly in proxy related requests
post_field	Appears to define the HTTP POST parameter, possibly for proxy handling
end_point	Telegram API endpoint address
install_foldername	Name of the persistence directory in %APPDATA%
install_filename	Filename used when copying the bot into install_foldername
keylog_foldername	Directory name for keylogger logs in %APPDATA%
keylog_filename	Filename storing captured keystroke data
persist	Boolean flag indicating whether persistence logic should be executed
keylogger	Enables or disables keylogging functionality
start_sysinfo	Sends system information on startup if enabled
procmon	Enables detection of AV or EDR related processes
detect_sandbox	Enables sandbox environment detection
elevate	Attempts privilege escalation via UAC
auto_steal	Collects and sends system data immediately after startup
decode_name	Indicates that install_foldername is Base64 encoded

After execution, the RAT follows the logic defined in the configuration. It either immediately sends a startup notification to Telegram or first installs itself for persistence. In the persistence scenario, it creates a directory at %APPDATA%\%[install_foldername], copies itself as [install_filename], and adds an autorun entry under HKCU\Software\Microsoft\Windows\CurrentVersion\Run using the value name defined in the configuration as [start_name].

The registry key HKCU\Software\[name] is used both for storing internal data and as a semaphore. Its presence or stored values influence execution flow, allowing the malware to alter behavior depending on whether it is the first launch or a subsequent run.

The bot retrieves commands by polling the Telegram Bot API using the `getUpdates` method. It periodically sends HTTPS requests to the configured endpoint and parses the response to extract new messages. These messages are interpreted as commands and executed according to the implemented functionality.

Commands follow a structured text format:

```
/[botid]*command*parameter1*parameter2*parameterN
```

The **[botid]** is a randomly generated four digit number created during the first execution and used as an identifier. The asterisk character is used as the field separator. The RAT parses incoming messages, verifies the **[botid]** value, then splits the string by the separator to extract the command name and its parameters before execution.

List of commands

```
/online - See all your bots
/[ID]*help - help
/[ID]*desktop* - grab a screenshot
/[ID]*screens - check the amount of screens
/[ID]*telegram - grab telegram data
/[ID]*discord - grab discord data
/[ID]*whois - get user location
/[ID]*webcam - take a photo using Webcamera
/[ID]*micro - record a 15 second audio
/[ID]*history - grab browser history
/[ID]*historyForce - grab more browser history by killing browser processes, use carefully
/[ID]*browsers - grab browser data
/[ID]*browsersForce - grab more browser data by killing browser processes, use carefully
/[ID]*noAppBound - disable Chromium App-Bound protection
/[ID]*askElevation - request admin privileges (the tool will be restarted)
/[ID]*getDesktop - grab useful desktop files (.pdf, .txt etc)
/[ID]*systeminfo - grab system information
/[ID]*walletRecovery - get browser extension wallets
/[ID]*activewindow - get active window title
/[ID]*batteryinfo - get battery status
/[ID]*programlist - get the list of installed software
/[ID]*uninstall - uninstall RAT from victim's PC
/[ID]*message** - show messagebox to user,
    leave second argument empty for the default messagebox type
/[ID]*minimize - minimize all opened windows
/[ID]*maximize - maximize all the windows back
/[ID]*openurl* - open given url in the default user browser
/[ID]*shutdown - turn Off the PC
/[ID]*restart - restart the PC
/[ID]*hibernate - enter the hibernating mode
/[ID]*logoff - user log off
```

```

/[ID]*bsod - invoke the Blue Screen of Death
/[ID]*sendkeypress - the victim will "press" given keyboard keys
/[ID]*displayrotation<0/90/180/270> - Set the angle of display rotation, 0 - normal mode
/[ID]*encrypt** - encrypt a folder/all user
    files with the given password, must be remembered for decryption
/[ID]*decrypt** - decrypt user files, all the files will
    be destroyed if the password is wrong
/[ID]*copy** - copy a file or directory, e.g.
    /[ID]*copy*C:\Users\User\Downloads\1.txt*C:\Users\User\1.txt
/[ID]*list*
    - shows files and folders in a directory, e.g. /[ID]*list*C:\Users
/[ID]*size* - get the file/directory size
/[ID]*delete* - deletes a file or folder
/[ID]*run* - runs a file (e.g. exe, png, txt etc)
/[ID]*upload* - Grabs a file from victim's PC, won't work if the file is too big
/[ID]*gofile* - Uploads a file/folder from victim's PC via gofile
/[ID]*download - victim's PC downloads the file attached to this message,
    if it is a picture it should also be attached as a file
/[ID]*download* - victim's PC downloads the file from the provided URL
/[ID]*droprun - victim's PC downloads and starts the file attached to this message
/[ID]*droprun* - victim's PC downloads the file from the provided URL and starts it
/[ID]*processlist - shows the list of current processes running
/[ID]*processkill* - kill a process by name, must not add .exe
/[ID]*processpath* - Show the path to process, must not add .exe
/[ID]*desktopPath - show the path to desktop
/[ID]*startuplist - see the list of startup programs
/[ID]*startupadd* - add the RAT to startup
/[ID]*cmd* - run a cmd command on victim's PC
/[ID]*powershell* - run a Powershell command on victim's PC
/[ID]*gift*** - gift this bot to another user, his telegram bot has to be started
/[ID]*keylogger - get user keylogs
/[ID]*keyloggerClear - clear user keylogs
/[ID]*about - about

```

Although the RAT provides a wide range of features, it does not include exploits or advanced privilege bypass techniques. All functionality is implemented using standard Windows API calls. Even the attempt to obtain administrative privileges relies on the legitimate UAC prompt mechanism, assuming the user will approve the elevation request.

```

sei.cbSize = sizeof(sei);
sei.fMask = SEE_MASK_NOCLOSEPROCESS;
sei.lpVerb = L"runas";           // request elevation
sei.lpFile = L"cmd.exe";         // target executable
sei.lpParameters = L"/c whoami"; // command line parameters
sei.nShow = SW_HIDE;             // window state

if (!ShellExecuteExW(&sei))
{
    DWORD err = GetLastError();
    wprintf(L"ShellExecuteExW failed: %lu\n", err);
    return 1;
}

```

Figure 7: All functionality is implemented using standard Windows API calls.

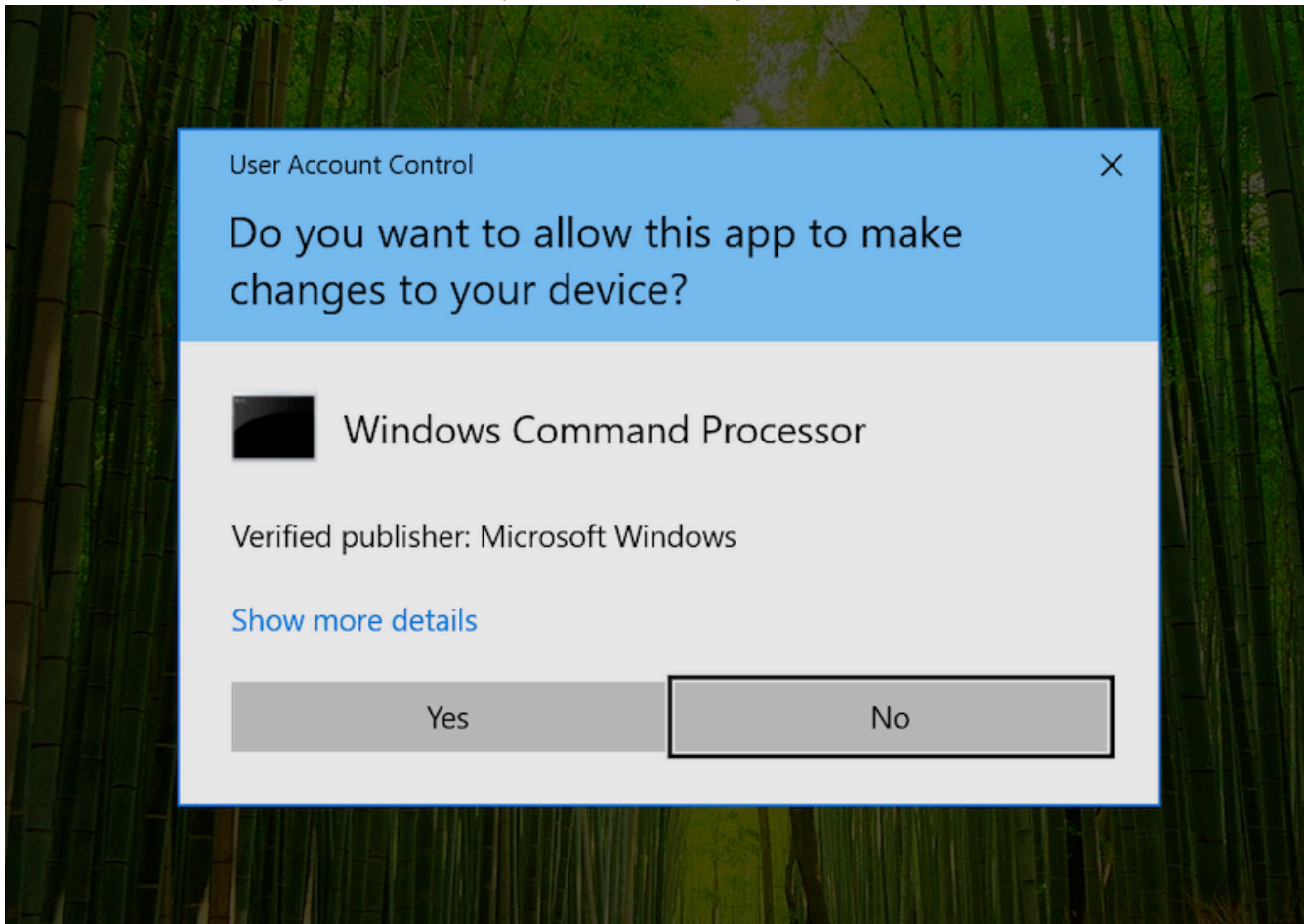


Figure 8. UAC elevation example, as implemented in Millenium RAT.

Threat Actor Profile

GROUP-IB



Y2K Operators

Y2K Operators is a threat actor cluster using Millenium RAT version 4.* in their operations.

Modus operandi

Y2K Operators rely on social engineering as the primary vector for delivery, employing various lures designed to trick victims into executing malicious payloads. These typically masquerade as legitimate software, cracked applications, or other files of perceived value to the target, encouraging the victim to run the file voluntarily. Once executed, the payload deploys Millenium RAT 4.*, granting the operators remote access and control over the compromised host.



First seen
22 May 2025

Skillset
Social Engineering

Toolset
Millenium RAT

Targeted Countries
Refer to victimology map

Motivation
Financial gain,
Stealing sensitive data

Group-IB, 2026

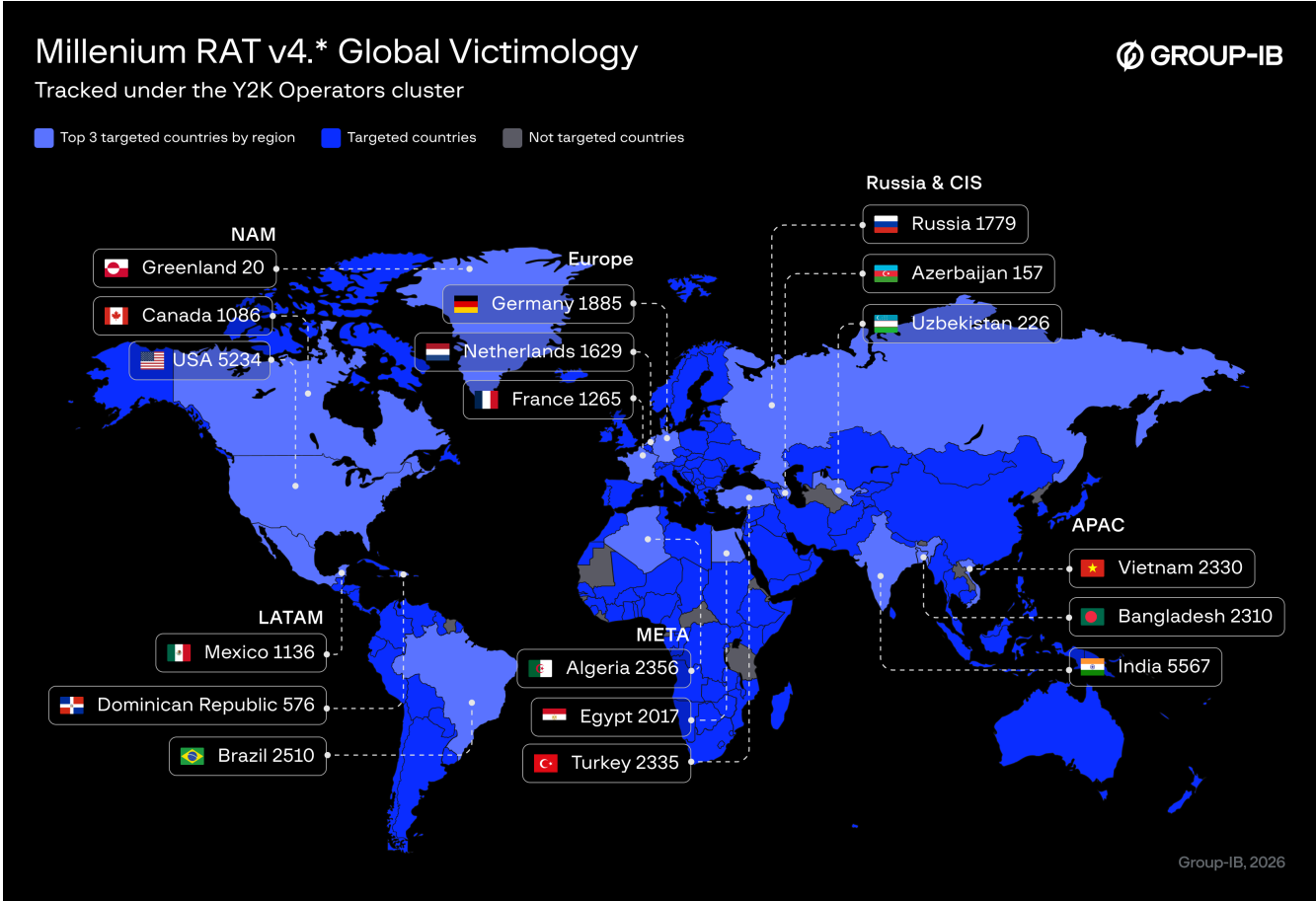


Figure 9. Global victimology of Millenium RAT v4.

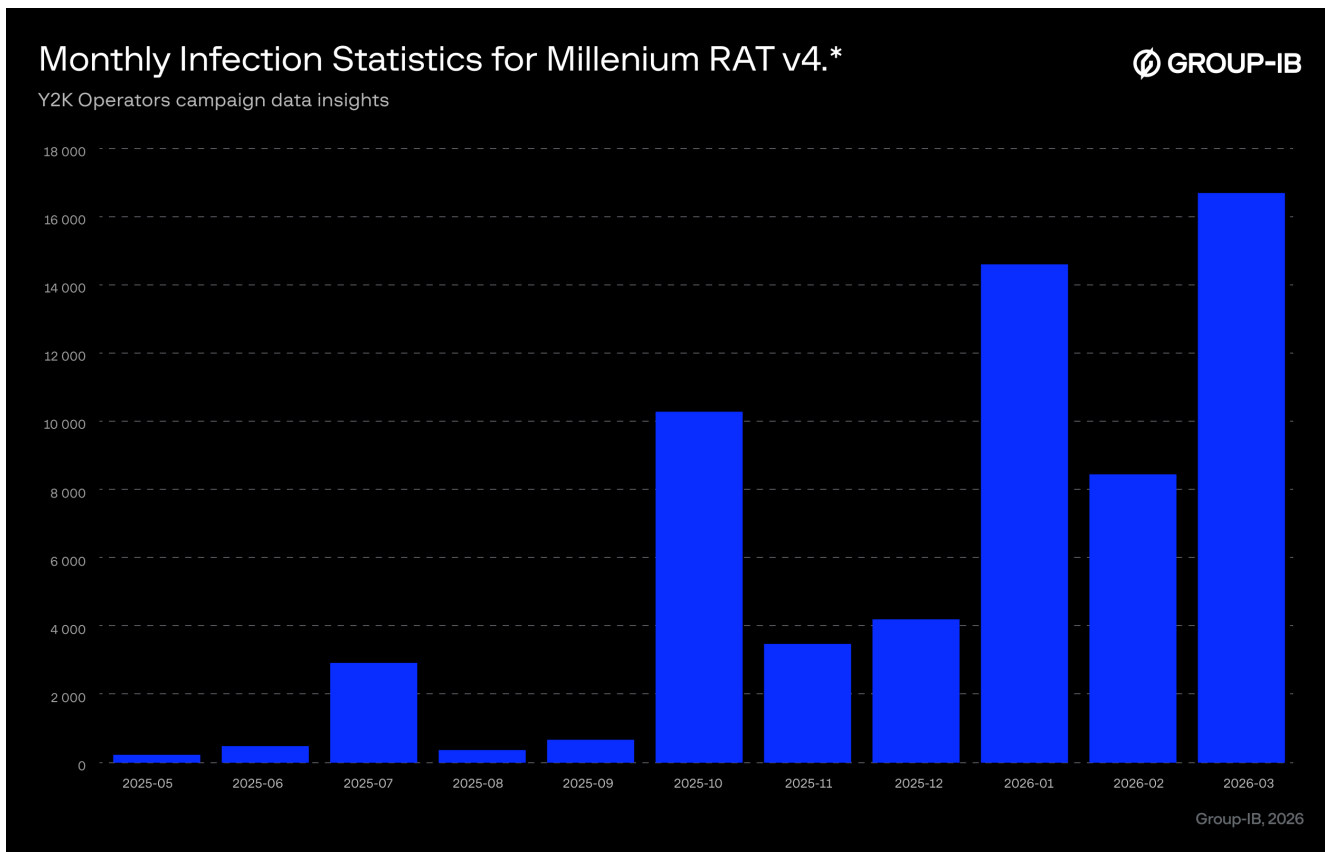


Figure 10. Monthly infection statistics.

Social engineering delivery tactics

Based on observed Y2K Operators campaign involving Millenium RAT v4, initial delivery relies on compressed archives or disguised executables, with filenames chosen to entice targets into running them. The lures fall into a few recurring themes, highlighting the wide net cast by the threat actors to maximise distribution of the trojan across all industries and victim groups.

- 1. Fraud and cybercrime utilities.** These target users looking for easy illicit income, posing as generators and balance checkers:
 - [HOT] Steam Wallet Gift Card Generator {With Internal Gift Checker}.exe
 - Valid Credit Card Generator [Effortlessly Buy Crypto, Access Free Trials, & Generate & Verify Cards].zip
 - Crypto Balance Checker [Seed Phrases, Keys, Logs] V4.5 Updated + Screenshot.zip
- 2. Hacking and OSINT toolkits.** A large share of the samples is aimed at aspiring hackers and security enthusiasts, packaged as ready-to-use bundles:
 - Hack Pack 2026 Contains Tools and Tutorials For Hacking.zip
 - WiFi Hacking for Beginners.exe
 - INSTAGRAM OSINT TOOL EXTRACT EMAIL PHONE NUMBER, AND MORE.zip

3. **Software cracks and bypasses.** Users trying to defeat licensing or identity-verification systems are a frequent target:

- Advance Bulk Mailer 4.5 Cracked (Advance Bulk Mailer 4.5.7.55).zip
- [AI KYC Bypass Tools] PhantomKYC Pro + Volcam + ID Editor Bypass SumSubOnfidoJumioVeriff 92% Success.zip

4. **Gaming community lures.** Roblox appears repeatedly, reflecting both the platform's young user base and its active cheating and modding scene:

- roblox-username-checker-main.exe
- ROBLOX Cracking Tools Pack.zip
- ROBLOX SILVERBULLET CONFIG WITH FULL CAPTURE (1).zip

One subset of the samples observed by Group-IB in this research was especially revealing: the operators even target *other cybercriminals*. They take popular RATs, builders, and exploit kits, add a backdoor, and redistribute them — so the would-be attacker downloads a working tool and gets infected at the same time. [CloudSEK](#) documented the same pattern with a trojanised XWorm builder, and it remains an active distribution trend here.

1. **RATs and builders observed in the lure set:**

- Token-Grabber-Builder.7z
- AsyncRAT_v0.5.6.exe
- XWorm V7.2.rar
- njRAT v0.11.exe

2. **Exploitation kits:**

- Multi Exploit Builder.rar
- PDF and Doc exploit 2025.7z
- Razor Batch Virus Builder 2025.exe

In another one of the analyzed samples, the threat actors used 75877[.]mcdir[.]me domain to proxy Telegram Bot API requests. In this case, PDF lures in Russian language were observed to be dropped along with the RAT:

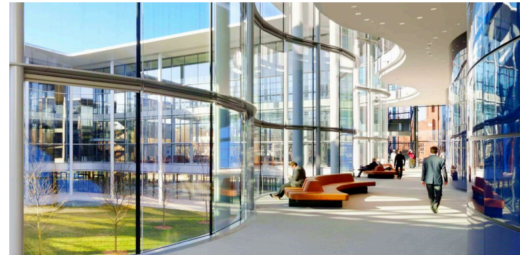
- Victim receives and executes a shortcut disguised as a PDF document.
- The LNK silently launches powershell.exe (hidden window, working directory %TEMP%).
- PowerShell downloads 2.vbs from hxxps://75877[.]mcdir[.]me/files/2.vbs and executes it via Shell.Application → ShellExecute.
- 2.vbs downloads two files from the same host: a decoy PDF (glass_example.pdf) and the Millenium RAT payload (doc1.exe).
- doc1.exe is written to %TEMP%\doc1.exe and run silently in the background, executing the RAT.

- The decoy PDF is written to %USERPROFILE%\Downloads\document_kp_glass.pdf and opened in the foreground.
- 2.vbs deletes itself to remove evidence.

Once the archive is opened and execution begins, the payload itself uses a very different naming style. The goal shifts from attracting clicks to staying unnoticed on the host. Four patterns recur:

1. **Impersonating Windows system processes.** Payloads adopt the names of real system binaries to blend into Task Manager and casual process listings:
 - svchost.exe
 - rcsdriver.exe
 - MsEdgeUpdate.exe
2. **Posing as security software.** Some samples imitate antivirus components so users are less inclined to terminate them:
 - Microsoft Antivirus.exe
 - MSAV.exe
3. **Generic installer and update names.** Bland filenames slip past manual file-system review without raising suspicion:
 - update1.exe
 - setup.exe
 - Udate.exe
 - Built.exe

Выдающийся 2750 мм X 6200 мм гигантский размер изогнутых стеклопакетов производителей

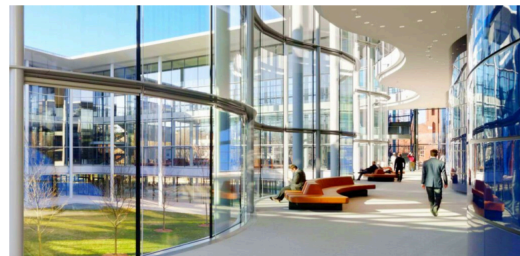


Подобно плоским стеклопакетам, также могут быть изготовлены изогнутые стеклопакеты большого размера. Изоляционная функция достигается тем, что две изогнутые панели с впадиной, заполненной воздухом, собираются с помощью рамы.

Изогнутое стекло связывает свободу в архитектурном дизайне с преимуществами и качествами стеклянных изделий.

Figure 11. PDF lures will launch decoy PDFs to mask RAT payload in the background.

Outstanding 2750mm x 6200mm giant size curved glass units from manufacturers



Like flat glass units, large curved glass units can also be manufactured. The insulating function is achieved by joining two curved panels with an air-filled cavity within a frame.

Curved glass combines freedom in architectural design with the benefits and qualities of glass products.

Figure 11. PDF lures will launch decoy PDFs to mask RAT payload in the background.

Запрос коммерческого предложения

Фасадное остекление «под ключ» | Производственный корпус, г. Санкт-Петербург

№ 3П-2026-ФС / СМР: сентябрь 2026

Уважаемые партнёры!

В рамках реализации проекта по строительству производственного корпуса в г. Санкт-Петербург, Приморский район, ОЭЗ «Новоорловская» мы ищем подрядчика, который может выполнить работы по монтажу фасадного остекления «под ключ».

ОБЩАЯ ПЛОЩАДЬ
ОСТЕКЛЕНИЯ

3 523,21 м²

В Т.Ч. МОЛЛИРОВАННОЕ
СТЕКЛО + ГНУТЫЙ ПРОФИЛЬ
(Ф2, М/О Е-Ж 1-2)

163,97 м²

СРОК СТРОИТЕЛЬНО-
МОНТАЖНЫХ РАБОТ

Сентябрь 2026
г.

Состав работ: проектирование разделов КМ и КМД, изготовление, доставка и монтаж фасадного остекления. Часть фасадного остекления Ф2 (м/о Е-Ж 1-2) необходимо выполнить из моллированного стекла и гнутого алюминиевого профиля (S=163,97 м²).

Figure 11. PDF lures will launch decoy PDFs to mask RAT payload in the background.

Request for quotation

Turnkey facade glazing | Production facility, St. Petersburg

No. 3П-2026-ФС / СМР: September 2026

Dear partners!

As part of a project to build an industrial building in St. Petersburg, Primorsky District, Novoorlovskaya SEZ, we are seeking a contractor who can perform turnkey façade glazing installation.

TOTAL GLAZING AREA

3,523.21 m²

INCLUDING BENT GLASS + BENT
PROFILE (F2, M/O E-F 1-2)

163.97 m²

PERIOD OF CONSTRUCTION AND
INSTALLATION WORKS

September 2026
G.

Scope of work: design of the KM and KMD sections, fabrication, delivery, and installation of façade glazing. Part of the façade glazing, F2 (m/o E-G 1-2), must be made of curved glass and bent aluminum profile (S=163.97 m²).

Figure 11. PDF lures will launch decoy PDFs to mask RAT payload in the background.

Conclusion

Group-IB investigation into the current iteration of Millenium RAT reveals a significant paradigm shift in its development, with the malware migrating from the .NET framework to a native C++ application. This architectural choice, combined with the continued utilization of the Telegram bot API for command and control, positions the malware as a highly resilient and formidable threat, capable of circumventing less advanced detection mechanisms.

Furthermore, the availability of the Millenium RAT as Malware-as-a-Service with low entry price drastically expands the pool of potential threat actors, allowing even less-skilled or financially constrained individuals to rapidly escalate their operations.

19/30

Given the malware developer is actively releasing new versions, we anticipate a continued commitment. Future iterations will likely prioritize the further enhancement of additional functionality and anti-forensic capabilities.

Recommendations

- **Treat unexpected elevation prompts as suspicious.** Millenium RAT obtains administrative rights simply by displaying a standard User Account Control prompt and relying on the user to approve it. As in the example, this appears as a request from “Windows Command Processor” with a Microsoft-signed publisher. If a UAC prompt appears that you did not initiate — in particular a command-processor request you did not trigger – choose **No**, and use “Show more details” to confirm what is asking for access.
- **Do not run files from untrusted sources.** Avoid executables from unsolicited email attachments, links shared in messaging apps, cracked software, and unofficial download sites. Verify the sender or source before opening anything.
- **Use a standard (non-administrator) account for day-to-day work.** Operating without admin rights limits what an infection can do and makes an unexpected elevation request far more conspicuous.
- **Keep built-in protections enabled and the system patched.** Leave Microsoft Defender and SmartScreen on and apply updates promptly. Be aware that legitimate software does not exclude an entire drive from antivirus scanning – the RAT attempts exactly this (an exclusion for C:\) to neutralise protection.
- **Enable multi-factor authentication.** MFA reduces the value of any credentials captured by the keylogger or collected automatically, limiting account takeover even if a device is compromised.
- **Report a suspected infection rather than cleaning it yourself.** A RAT’s persistence and command channel can allow it to restore itself. Disconnect the device from the network and escalate to your security team.
- **For IT and power users: watch for persistence artefacts** – autorun entries under HKCU\...\Run, unfamiliar folders in %APPDATA%, and system-named processes such as svchost.exe running from user-writable locations rather than System32.

Frequently Asked Questions (FAQ)

What is the most significant change in Millenium RAT version 4.*?

arrow_drop_down

The most critical change is the architectural shift from the .NET framework to a native C++ application. This transition eliminates dependencies on the .NET framework.

How does Millenium RAT 4.* communicate with its operators?

arrow_drop_down

Millenium RAT 4.* uses the Telegram bot API for its C2 communication. By leveraging this legitimate, cloud-based messaging platform, the malware is able to effectively mask its malicious traffic, making C2 communication blend in with normal network activity and bypass traditional filtering mechanisms.

What sensitive data does Millenium RAT 4.* target?

arrow_drop_down

As a full-featured Remote Access Trojan, Millenium RAT 4.* is designed to compromise Windows machines to exfiltrate sensitive browser and system data, in addition to capturing screenshots and performing persistent keylogging.

What is the scope of the Y2K Operators' campaign?

arrow_drop_down

The campaign is both high-volume and global. Our telemetry has identified 62,289 unique compromised devices, with a significant acceleration observed in the first quarter of 2026 alone.

Who is the developer of the Millenium RAT?

arrow_drop_down

The malware is promoted and developed by an individual operating under the moniker “shinyenigma” across underground forums and platforms like GitHub.

MITRE ATT&CK

Tactic	Technique	Procedure
Execution (TA0002)	Command and Scripting Interpreter. PowerShell (T1059.001)	Uses PowerShell to run commands.
	Command and Scripting Interpreter. Windows Command Shell (T1059.003)	Executes commands using cmd.
	Input Injection (T1674)	Can simulate keyboard input.
	Native API (T1106)	RAT functionality is implemented using standard Windows API calls.
	User Execution. Malicious File (T1204.002)	The malicious file is executed by the user.
Persistence (TA0003)	Boot or Logon Autostart Execution. Registry Run Keys / Startup Folder (T1547.001)	Adds an autorun entry under HKCU\Software\Microsoft\Windows\CurrentVersion\Run.
Privilege Escalation (TA0004)	Abuse Elevation Control Mechanism. Bypass User Account Control (T1548.002)	Attempts to obtain administrative privileges using UAC.

Defense Evasion (TA0005)	Deobfuscate/Decode Files or Information (T1140)	Deobfuscates configuration file using Base64 and XOR.
	Impair Defenses. Disable or Modify Tools (T1562.001)	Modifies Windows defender preferences.
	Indicator Removal. File Deletion (T1070.004)	Has the ability to uninstall itself.
	Masquerading. Match Legitimate Resource Name or Location (T1036.005)	Uses a legitimate system filename "svchost.exe".
	Obfuscated Files or Information. Encrypted/Encoded File (T1027.013)	Configuration obfuscated using Base64 and XOR.
	Virtualization/Sandbox Evasion (T1497)	Has sandbox environment detection.

Credential Access (TA0006)	Credentials from Password Stores. Credentials from Web Browsers (T1555.003)	Can extract passwords from browsers.
	Steal Web Session Cookie (T1539)	Can steal cookies from browsers.

Discovery (TA0007)	Browser Information Discovery (T1217)	Can retrieve browser history and search for cryptocurrency wallet extensions.
	File and Directory Discovery (T1083)	Has the ability to enumerate files and folders.
	Process Discovery (T1057)	Enumerates running processes.
	Query Registry (T1012)	Queries registry to enumerate startup programs.
	Software Discovery (T1518)	Enumerates installed software.
	Software Discovery. Security Software Discovery (T1518.001)	Checks for AV or EDR related processes.
	System Information Discovery (T1082)	Collects system information such as battery status.
	System Location Discovery (T1614)	Determines IP geolocation of a victim.
	System Owner/User Discovery (T1033)	Collects victim username.

Collection (TA0009)	Archive Collected Data (T1560)	Collected browser data is archived in .zip prior exfiltration.
	Audio Capture (T1123)	Has the ability to record audio.
	Data Staged. Local Data Staging (T1074.001)	Stages keylogger data into file prior exfiltration.
	Data from Local System (T1005)	Collects session files related to Discord, Telegram.
	Input Capture. Keylogging (T1056.001)	Can perform keylogging.
	Screen Capture (T1113)	Can capture screenshots.
	Video Capture (T1125)	Can access the victim's webcam.

Command and Control (TA0011)	Application Layer Protocol. Web Protocols (T1071.001)	Uses Telegram Bot API over HTTPS.
	Ingress Tool Transfer (T1105)	Has the ability to download additional files from a given URL.
	Web Service. Bidirectional Communication (T1102.002)	Uses Telegram Bot API.
Exfiltration (TA0010)	Exfiltration Over C2 Channel (T1041)	Exfiltrates data using Telegram Bot API.
	Exfiltration Over Web Service. Exfiltration to Cloud Storage (T1567.002)	Can exfiltrate data from the victim using Gofile.
Impact (TA0040)	Data Destruction (T1485)	Wrong password destroys encrypted files.
	Data Encrypted for Impact (T1486)	Encrypts user files requiring password.
	System Shutdown/Reboot (T1529)	RAT supports remote system disruption via shutdown, restart, hibernate, logoff or trigger BSOD.

Indicators of Compromise (IOCs)

Network IOCs

- hxxp://158[.]94[.]208[.]168/files/8514679081/DRTjyu7[.]exe
- hxxps://www[.]thesnapchatmodapk[.]com/update1[.]exe
- hxxps://modedapk[.]net/update1[.]exe
- hxxps://75877[.]mcdi[.]me/files/doc1.exe
- hxxp://kuttabilla[.]top/mr[.]exe
- hxxp://62[.]60[.]226[.]97:5553/voshod[.]exe
- hxxp://130[.]12[.]180[.]43/files/7924412375/upOSLDn[.]exe
- hxxps://blackhatusa[.]com/setup[.]exe
- hxxps://blackhatusa[.]com/clip[.]exe
- hxxp://blackhatusa[.]com/mr[.]exe
- hxxps://blackhatusa[.]com/update[.]exe

File Hashes

1d699a46339626db299548e32ed3a77eec267840c3de39b49caf38b88aeb150d
2267d05dbd5e30c6dfcdde25731280dd755e689faa684bd21cfbef5281fd3e86
12b41c07299d2535f7cdc194d97496acd944a9eb5d94b8d24b19291ed9d0830c
1d52ded1f3838a1eee849ae20b2fee6c84b183cc98abe7244365b9f34b925eea
4e035575be8fe350a9e36cf29dbbc8826af2f772672bd08c9e489a243cb90e31
1c01ab1b59245f24ebdc5d9c414fc4e2ce31f71f181522efc5a3d27476c8e21
e4496565d9fd2f9425c10a98d3a8632c12af5fe4259484cb202d7f65532b7df2
ad0f892b7b99b68491ade4949ef6b575e64d9df5f84a53019b5c1e4eeb4c46a9
ad74f502cc37e815482df49f118b2f678daf1a3f522daf07a2abeb32c2ed3831
2d8e5a2763f9a899fda44390d5b8495836c11fb266a61868d52d1f397c5243ee
cc47209d2e4d5a9b2b1d71622b0ad7f73e9c4aa56edd9aaf1e29265650c30f16
85816d89dac648645a9026973772815e956c267232b3d2577a06a43418f19ed3
92710bdb44279dbe8ccff34ba698d1558fa6d271c99ed4960ccbfb6d518d9418
a8acc24bb3e6a1a3b66a31ceaefda07d4a0e17415468683458b499f2ba240450
d55ce447e249ef9045750865fa196c8ca8434c8c484f861b7bdecbbceeab7c16e
a97f15d7bfad02a600eba426c3ef72be34e944a7c8364a975c53866735f7aa4e
fc41c336b79cbc6559a17d716b84101dbef1adc5357b643a75111af442719611
5a23ca644cb1f310be1abd5f6c6a3b3e15681ced99b0947a7f3465a79aae5089
3e17ce0b30b9fd6863b341ae58ee118dc13f2ee7f1c92ac4b81c04d54480d0e0
7d8b6a64f7b65b281e7b5568929c6f96c62bbae9628162aabe7d8140a86d3de8
307964ed02f34bff4e40c5402cc936be07fd9957ef400596a4b3e2cd98c50ec1
8bef879c6920cdce7c01b8dbb7da24dca23b8822a7aa00dfc72cb32f55879a24

19e0070e5009bd5b376b9be997361d0773dcb004200ee8fafe6c14b96cbd93e4
88f9e169a85dcf6a1c03bf3ca1b1a262ed32baeca46cb87f0324adfdc098d4a2
5562246e38f8935ba8b07350e6aaa44bc22abf37b77f49836fde5999f4b61cf1
de3842bbb6626912d5b9b01fb775e1843004edb5855d4e627fd74b88bc7fe33b
ccca11a6d5835999c40a0a5264084b3740633600c157754fad2ef59559e31736
8f8a71352d2f18162f2f74090dc6f0cae6b37029e3244e6522825ade75163055
57edeb575862ce8d3bff2eb4d32d9e3fa1ffb7cb8f818e2e7fc6d25a506faea6
2d5615acd1b0666995fd124fb72f2713c6609b5368350340288b52fecbdd016d
848036661c71b80ee41566918faa5eae3bf4f03ae807bb4af42cb483b6c141e2
aa2ccd18a7a09f66ca5c1bbd927f7fe411bd3874df77b0eaf40738dab7566606
a4b34b94a905fe330b0a3e4502aa45356e383a8f45ff1d008b785ea0ec14acaf
a911fe0259772906447d7e80a902ea954f3530edd9ea7d0427b6380707a8e681
7a370a9262d37de6a24706f92ff0cdded7202281a6ff3bf313721756226ebff9
66bf111030a2e22db575c0b7b7b677208745eef8b44265bb4259f41f126f1bf8
512adab2c69feaf026adfb12cbd7d2eb4fee746120491e44f476eebddcbb19f2
8419b1f0acca46d45f4c54c315c8cc4784946e07d547fe55187b928fa6c6b8f5
4991873515d6dea70d7769cf67ccd8ea69184e5e454a6e6d1e093b6a3c48eb47

DISCLAIMER: All technical information, including malware analysis, indicators of compromise and infrastructure details provided in this publication, is shared solely for defensive cybersecurity and research purposes. Group-IB does not endorse or permit any unauthorized or offensive use of the information contained herein. The data and conclusions represent Group-IB's analytical assessment based on available evidence and are intended to help organizations detect, prevent, and respond to cyber threats.

Group-IB expressly disclaims liability for any misuse of the information provided. Organizations and readers are encouraged to apply this intelligence responsibly and in compliance with all applicable laws and regulations.

This blog may reference legitimate third-party services such as Telegram and others, solely to illustrate cases where threat actors have abused or misused these platforms.

This material is provided for informational purposes, prepared by Group-IB as part of its own analytical investigation, and reflects recently identified threat activity.

All trademarks referenced herein are the property of their respective owners and are used solely for informational purposes, without any implication of affiliation or sponsorship.

© 2003 – 2026 Group-IB is a global leader in the fight against cybercrime, protecting customers around the world by preventing breaches, eliminating fraud and protecting brands.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. Learn more about Group-IB Cookies from [Cookie Policy](#).