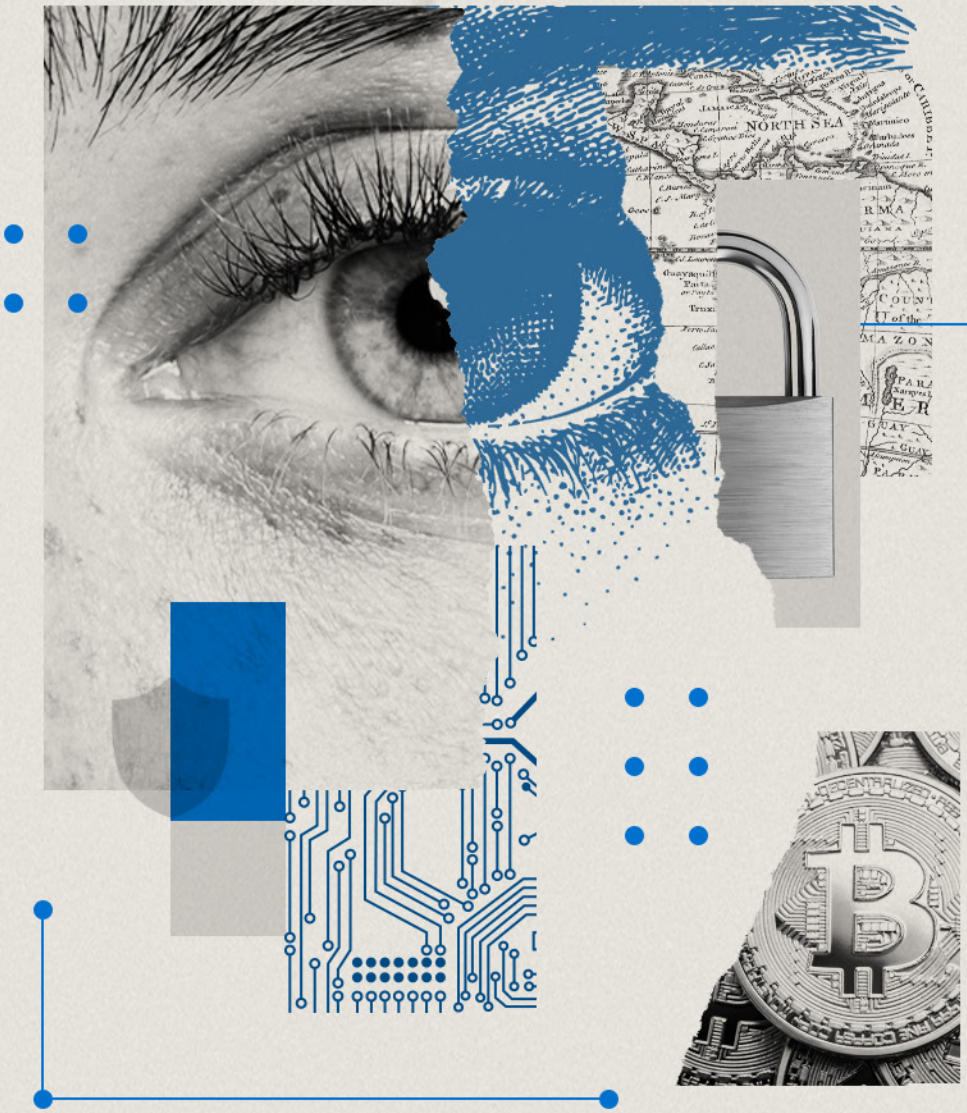
MALWARE/
TOOL
PROFILE

Recorded Future®

By Insikt Group®

September 26, 2024



Rhadamanthys Stealer Adds Innovative AI Feature in Version 0.7.0

Rhadamanthys Stealer v0.7.0 introduces AI-powered OCR capability, enabling the extraction of cryptocurrency seed phrases from images and demonstrating how AI is weaponized to enhance data theft.

Detections and preventative measures unveiled for Rhadamanthys Stealer v0.7.0 provide an effective defense against this evolving threat, offering organizations strategies to prevent data theft and strengthen security.

Rhadamanthys Stealer v0.7.0 is a global cyber threat with AI-driven features and advanced evasion tactics, mainly targeting organizations across North and South America.

Executive Summary

Rhadamanthys is an advanced information stealer that first appeared in 2022. It is known for its rapid releases and has seen at least ten different releases since its inception. The malware is advertised and sold on underground forums, and despite being banned for allowing the targeting of Russian and/or former USSR entities, it is still being actively sold. The fee structure starts at $250 for 30 days of access, making it an affordable and attractive option for cybercriminals.

Rhadamanthys is a full-featured information stealer that supports collecting system information, credentials, cryptocurrency wallets, browser passwords, cookies, and a wide range of other applications. It includes numerous anti-analysis techniques that complicate analysis efforts and make it difficult for the malware to run successfully in a sandbox environment.

Insikt Group obtained and analyzed the most recent version of Rhadamanthys, 0.7.0, and noted many new features that have been added. The most innovative new feature is its ability to use AI (via optical character recognition [OCR]) to extract cryptocurrency wallet seed phrases from images automatically. This feature has client- and server-side components that allow Rhadamanthys to identify seed phrase image candidates on the client and fully extract the seed phrase after the image has been exfiltrated back to the malware's command-and-control server. Additionally, a new feature was added to allow threat actors to run and install Microsoft Software Installer (MSI) files, which may not be flagged as malicious by conventional detection systems.

Rhadamanthys is a popular choice for cybercriminals. Coupled with its rapid development and innovative new features, it is a formidable threat all organizations should be aware of. Organizations are encouraged to implement the mitigation strategies outlined in this report. In addition to the mitigations, various detections are available to identify Rhadamanthys and a mutex kill switch is described in the report that can be used as a vaccine against current infections.

Information stealers represent a significant threat to organizational security. The widespread practice of password reuse exacerbates this issue, as credentials stolen from personal accounts can often be leveraged to gain unauthorized access to corporate systems. For example, an attacker could retrieve an individual's personal email and password from a compromised social media account and then use that same password to infiltrate their professional email account, especially if the email address can be easily guessed or found on professional networking sites like LinkedIn.

Additionally, the increasing overlap between personal and professional use of devices further complicates the security landscape. Employees frequently use work laptops for personal activities, inadvertently downloading infostealers through malicious advertisements or compromised websites. Similarly, when individuals log in to work accounts from personal devices, those credentials may become compromised if an employee or their family member unknowingly becomes infected with an infostealer. These scenarios underscore the critical need for robust cybersecurity measures, including

stringent password policies, regular employee training on safe browsing practices, and rigorous access controls to mitigate the risks posed by infostealers and compromised credentials.

Key Findings

- Rhadamanthys, now in its latest version, 0.7.0, is a rapidly evolving malware family that continuously updates with new features, making it a formidable weapon for cybercriminals. It is global, affecting various sectors and regions, with most targets in North and South America.
- Insikt Group identified a killswitch to prevent Rhadamanthys from executing its stealers and extensions by setting known Rhadamanthys mutexes on a non-infected machine.
- Rhadamanthys, leading the trend of incorporating AI into malware with client-side features like OCR for extracting seed phrases from images, demonstrates how AI is weaponized to enhance data theft and is expected to remain at the forefront of this evolving trend.
- The threat actor “kingcrete2022", the developer of Rhadamanthys, is banned on both XSS and Exploit Forums. The ban was imposed because the threat actor had been accused of targeting Russian and/or former USSR entities. Currently, the threat actor relies on private messaging via TOX, Telegram, and Jabber to continue advertising new versions of the Rhadamanthys stealer.
- Insikt Group has identified a new feature of Rhadamanthys involving the use of MSI packages, representing an additional defense evasion technique. MSI files, typically associated with legitimate software installations, often bypass security scrutiny because they are perceived as trustworthy and may not be detected by conventional systems.
- Rhadamanthys has a built-in way to prevent re-execution within a configurable time frame. In version 0.7.0, the author updated this feature to make it tamper-proof through encryption and hashing.

Background

Rhadamanthys is an advanced information stealer that first appeared in the cybercrime ecosystem in September 2022. The malware is attributed to an individual or group known under the alias "kingcrete2022". kingcrete2022 started advertising the malware on various special-access forums, including XSS, Exploit, Best Dark, Opencard, and Center-Club, with the following fee structure.

License Type	30 Days	90 Day
Normal	$250	$550
VIP	$300	$750

***Table 1**: Rhadmanthys fee structure (Source: Recorded Future)*

The threat actor used different handles on different forums, including "kingcrete2022" on Exploit (currently banned for unknown reasons), "freeide" on XSS (currently banned for targeting Russian and/or former USSR entities, as shown in **Figure 1** below), "kingcrete" on Opencard and Best Dark, and "rhadamanthys" on Center-Club.

The threat actor uses TOX (5BCB80569AC334FDA5B7806ABC05DDFE3AF8F126E08D0EA6D21DA3C13B43F164188C3EEE89E9), an open-source, free, and encrypted communication protocol favored by many Russian- and English-speaking threat actors as a contact method. The threat actor also uses Telegram (@kingcrete), Jabber (*rhadamanthys@exploit[.]im*), and *kingcrete2022@thesecure[.]biz* for communication. Based on a search for the threat actor's TOX ID in the Recorded Future® Intelligence Cloud, additional advertisements for the Rhadamanthys under different handles, possibly operated by the same threat actor, are listed in the table below. The Telegram handles listed below advertised malware logs for sale, which indicated that the sale of the logs for Rhadamanthys was part of the threat actor's business model.

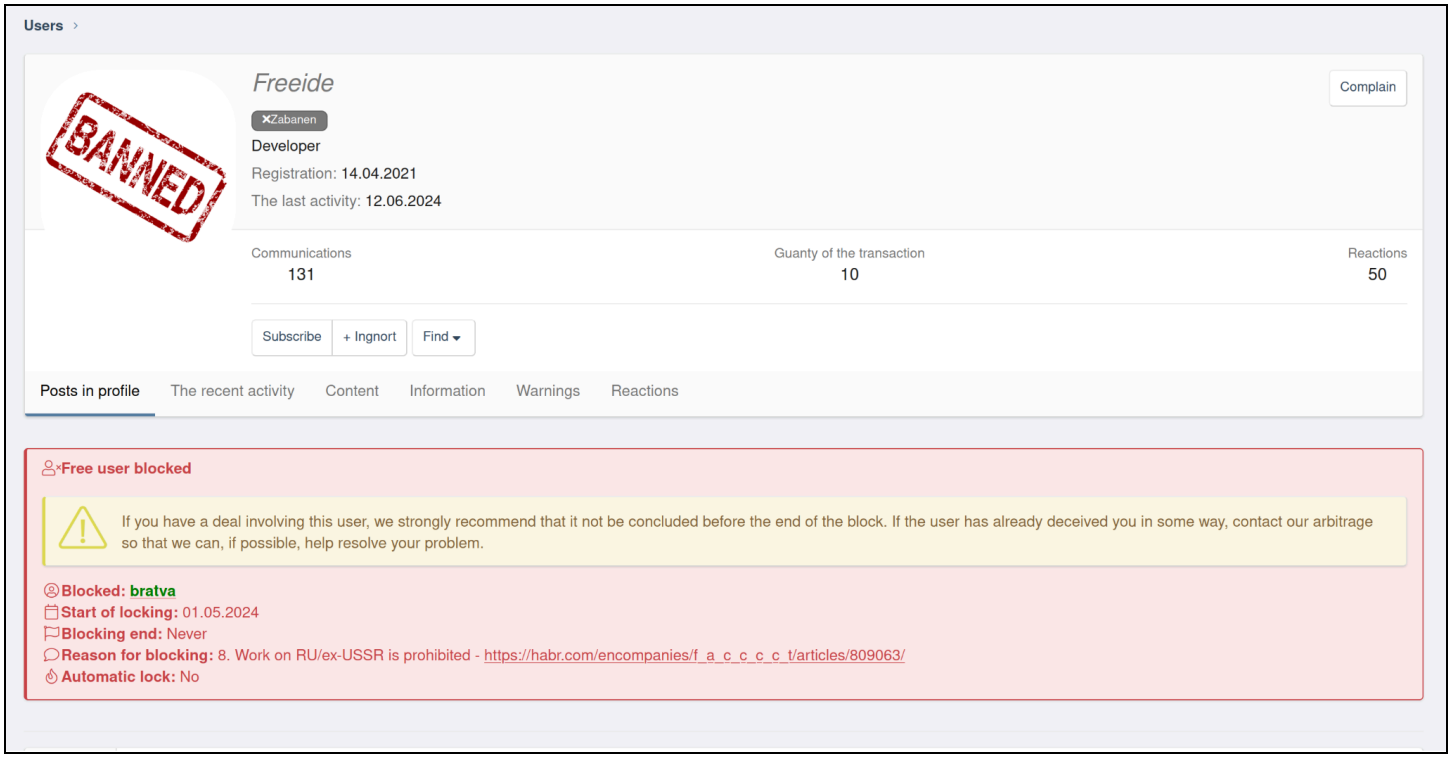


***Figure 1**: The handle "Freeide" used by the threat actor kingcrete2022 on XSS is banned for targeting Russian and/or former USSR entities (Source: XSS)*

Source	Handles
XSS	freeide, "DaF0x", "Free IDE"
Exploit	kingcrete2022
Best Dark	kingcrete
Opencard	kingcrete
SkyNetZone	kingcretekingcrete
Center-club	rhadamanthys
Best Hack	Rhadamanthys
Telegram	"dailyfreshlogs", "freshtrafficandlogs", "TrafficLogsMalwaresinfo"

***Table 2**: Rhadmanthys developer handles (Source: Recorded Future)*

The handle "superman8848" has also been associated with the advertisement of the Rhadamanthys as early as August 2022 on both XSS and Exploit. The accounts were banned on both forums. It is possible that "superman8848" and "kingcrete2022" are operated by the same threat actor. A search of "superman8848" on Google yielded a GitHub account, a Reddit account, and a Chinese-language

forum, *right.com[.]cn* (Intelligence Card). The GitHub account under "superman8848" also commented on a Chinese-language post, pointing to the possibility that the threat actor behind the handle might be a Chinese speaker.

kingcrete2022 uses the blog service *telegra[.]ph* (Intelligence Card) to document Rhadamanthys stealer updates.

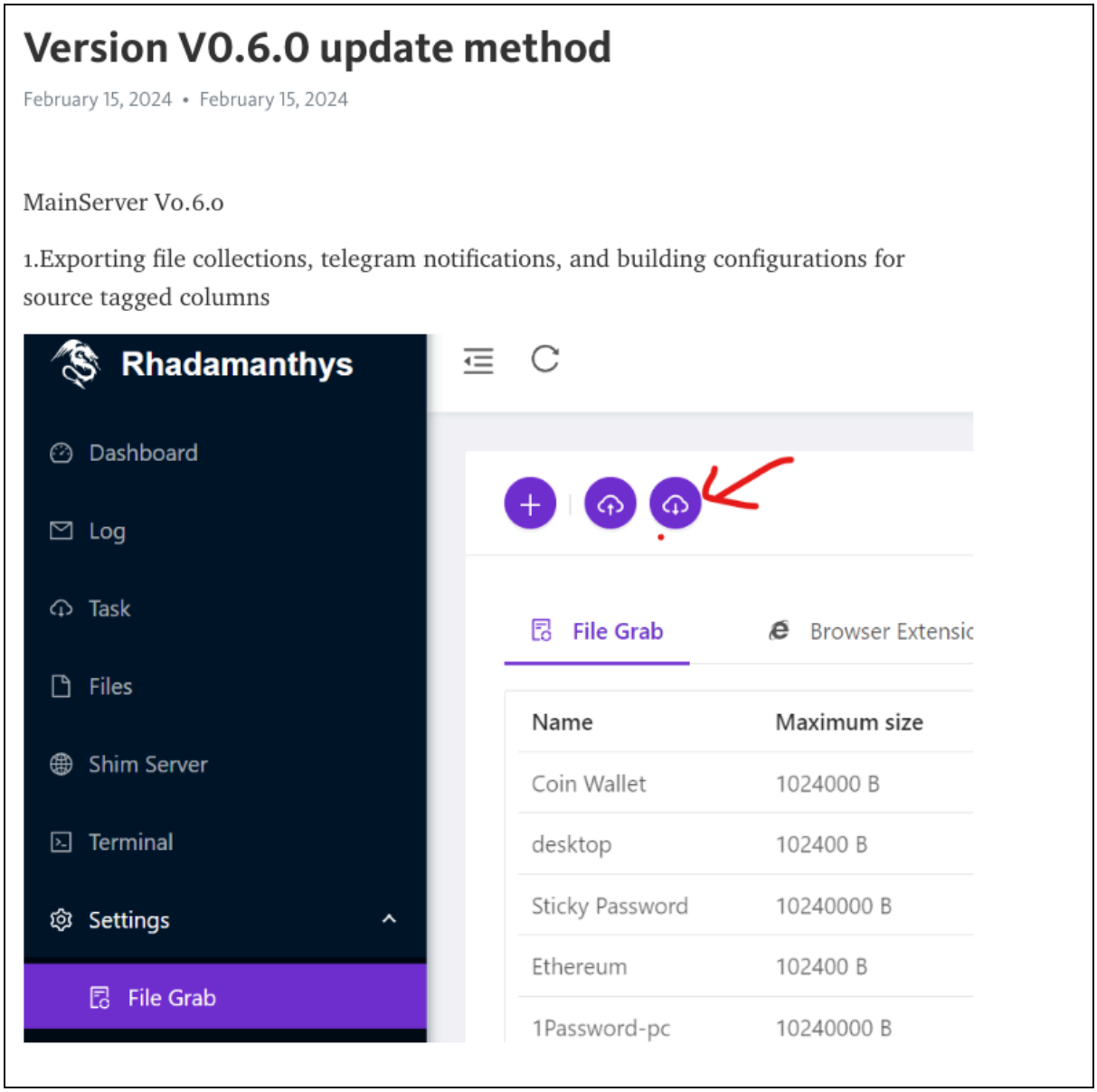


***Figure 2**: Example Rhadamanthys blog post from telegra[.]ph (Source: Recorded Future)*

The threat actor has also posted two instructional videos on Vimeo. One video was an overview of the "v0.3.2 updates". The second video was named "Wallter crack & Customized dictionaries", which showed how the infostealer targets cryptocurrency wallets.

Version 0.7.0 is the most recent version of the Rhadamanthys stealer, released in late June 2024. According to the banner message on TOX, the threat actor is working on Version 0.8.

Malware Capabilities and Versions

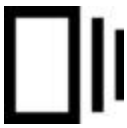
Rhadamanthys targets Windows operating systems and is designed to collect system information, credentials, cryptocurrency wallets, browser passwords, and cookies, among others. The stealers' collection targets are comprehensive, covering many targets, from major web browsers like Google Chrome to less common software such as the Pale Moon browser and Auvitas Wallet. The stealer not only exfiltrates data automatically upon infection but also allows operators the flexibility to deploy extensions and execute additional commands on compromised machines. The extensibility, constant updates, and feature expansions make Rhadamanthys a formidable tool for cybercriminals.

Anti-Behavioral Analysis: Rhadamanthys employs techniques to avoid behavioral analysis by analysis tools. These methods include timing and delay checks and monitoring for memory-write actions, making it harder for security researchers to trace its actions.

Anti-static Analysis: Rhadamanthys uses static analysis evasion techniques, including obfuscating its executable code, which makes it challenging for analysts to dissect and comprehend the malware's underlying structure.

Defense Evasion: Rhadamanthys uses sophisticated evasion tactics to bypass detection, including encrypting and encoding its files to obscure its contents, hijacking execution flow by exploiting legitimate Windows function calls, and altering file and directory permissions to avoid being flagged by security tools.

Execution: Rhadamanthys can leverage shared modules and command or scripting interpreters, such as PowerShell, to execute malicious payloads, enhancing its versatility in different environments.



Collection: Rhadamanthys collects data from infected systems, including credentials, browser data, system information, and cryptocurrency wallets.

Command-and-Control: Rhadamanthys communicates with a command-and-control server to receive instructions and exfiltrate stolen data. It typically uses HTTP/HTTPS protocols.

Malware Versions

Multiple versions of Rhadamanthys have been developed, with each iteration adding more features and refining existing ones. The malware's core capabilities have remained unchanged, focusing on

information stealing, but its deployment and execution have evolved. Reviewing the change logs on the developer's Telegram account, we identified the versions below and summarized their change logs. The change logs can be found in **Appendix B**.

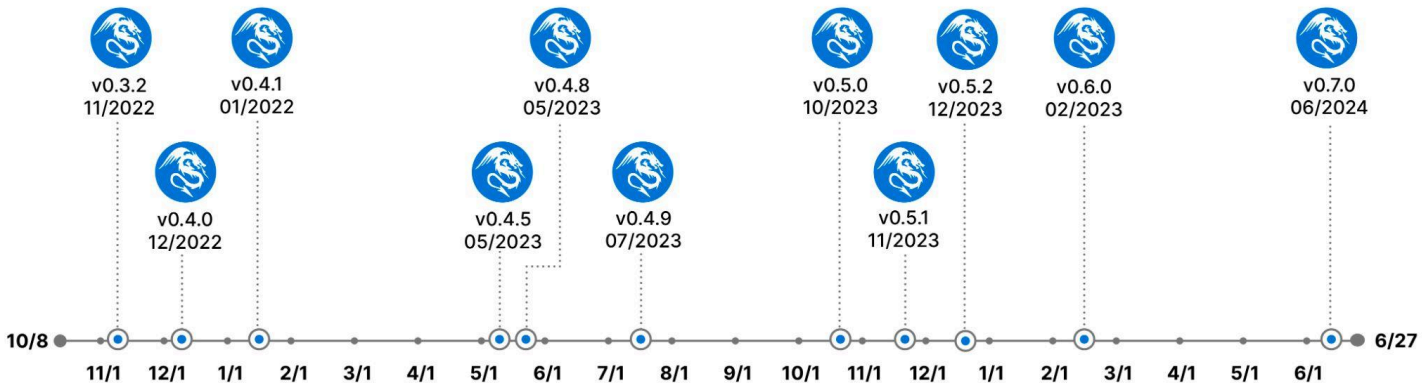


Figure 3: *Rhadamanthys version timeline (Source: Recorded Future)*

- **Version 0.4.0** provided major changes that were incompatible with prior versions. This version also required users to back up their configurations before updating and included new installation instructions and server panel access details.
- **Version 0.4.1** implemented critical fixes, such as preventing global download tasks from triggering when certain records were empty and addressing a significant security vulnerability related to panel session management. New features like customizable Telegram notification templates and enhanced support for third-party encryption services were also introduced.
- **Version 0.4.5** improved the client and panel by including a dedicated shim server and full transport layer security (TLS) support. It also added the capability to perform terminal operations directly from the panel. This update also focused on enhancing log export capabilities and implementing a download loader task system.
- With **version 0.4.8**, the client was completely rewritten to include independent encryption keys for each build, with extensive testing across various Windows versions. Server-side enhancements included password cracking algorithms, URL validity detection, and the ability to handle multiple crypt services.
- **Version 0.4.9** focused on refining existing features, such as resolving issues with log export records and enhancing panel search functionality. Improvements were also made to the Telegram notification system and stub cleanup processes.
- **Version 0.5.0** introduced observer mode and stub construction options and significantly improved the client execution process. It also expanded wallet cracking capabilities, improved Discord token acquisition, and upgraded panel search settings. This version added a plug-in module for task execution and introduced keylogger and data spy plug-ins, supporting secondary development.

- **Version 0.5.1** included a new Clippers plug-in, enhanced Telegram notification options, Google Account Cookie Recovery, and default build stub cleaning to bypass Windows Defender.
- **Version 0.5.2** enhanced the Shim Server disconnection detection with backend servers to better identify and repair connection issues. Clippers plug-in version 0.2 fixed bugs related to repeated uploads and log paging, introduced a full-text replacement feature for various copy operations and added a switch to ensure addresses were replaced only once. The reverse proxy plug-in now requires a separate virtual private server (VPS) for installation, with updates affecting only server-side files, ensuring no disruption to the running client system.
- **Version 0.6.0** enhanced server and panel functionalities, including geo- and IP- blocking, optimized log writing processes, and added support for new extended wallets. This version also improved the protection of the index database, simplified directory compositions for better compatibility with automatic processing tools, and enhanced stub cleaning and Windows Defender bypass features.
- **Version 0.7.0**, the most recent version, includes a complete rewrite of both client-side and server-side frameworks, improving the program's execution stability. Additionally, 30 wallet-cracking algorithms, AI-powered graphics, and PDF recognition for phrase extraction were added. The text extraction capability was enhanced to identify multiple saved phrases. Bugs and issues from the previous version were resolved. The Telegram module was rewritten to support HTML formatting and multi-token polling, while the synchronization module now includes file transfer protocol (FTP) support for remote log transfers. The search filter module has been rewritten, and an application programming interface (API) interface with an open platform has been introduced.

Rhadamanthys Identity Intelligence and Incidents

Recorded Future collects and analyzes malware log files from various information stealers advertised on underground markets. This data provides unique insight into information stealers' victimology and the markets in which they are advertised. The data analyzed from Rhadamanthys malware logs, as per Recorded Future Identity Intelligence, shows that Rhadamanthys is used globally, with most targets in North America and Brazil (see **Figure 4**).

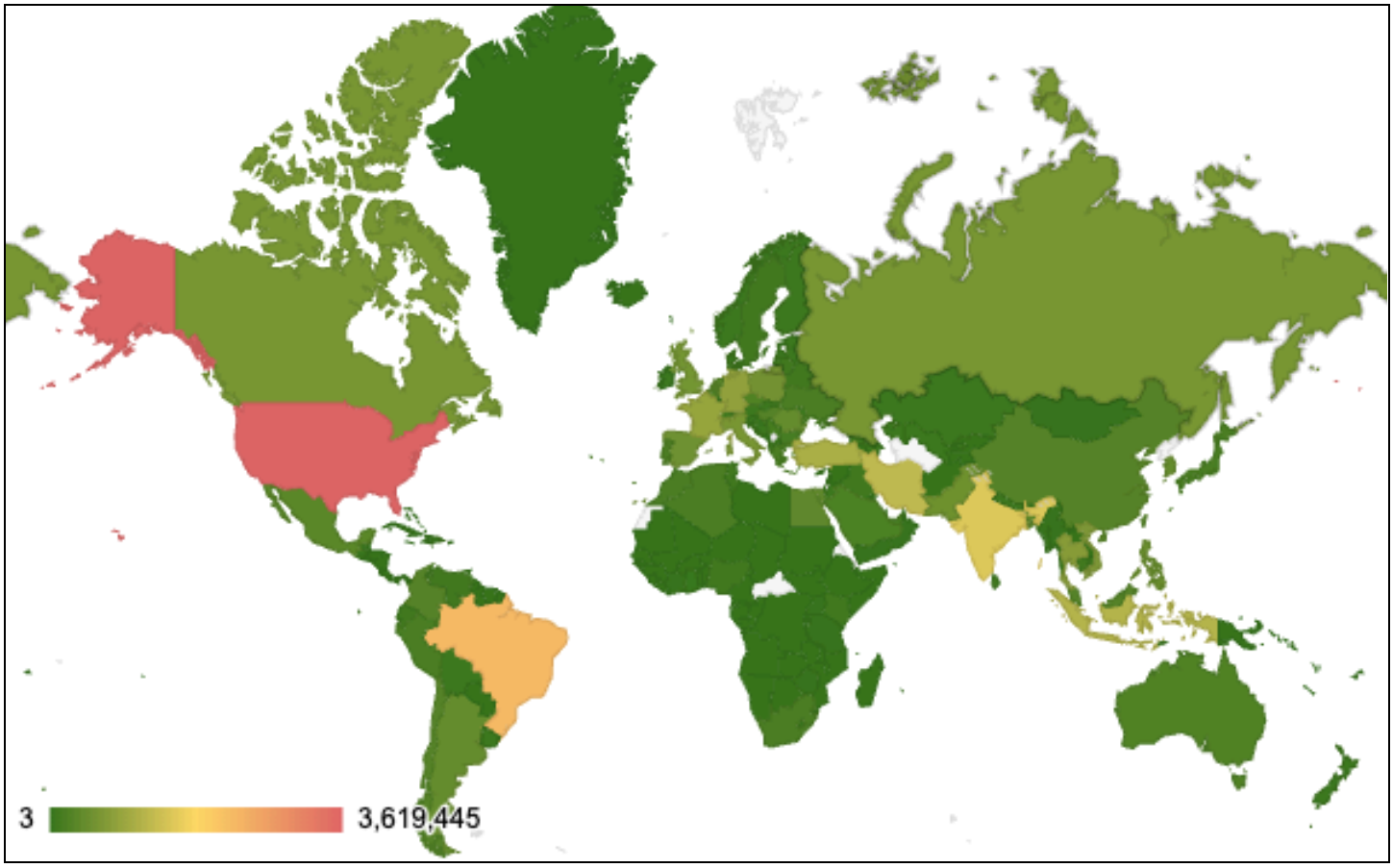


Figure 4: *Rhadamanthys victimology geographic locations (Source: Recorded Future)*

Although only a few uses of Rhadamanthys have been reported publicly, several notable events from the last twelve months are listed below.

- In October 2023, Rhadamanthys was dropped in an attack using the GHOSTPULSE loader. Rhadamanthys is delivered via MSIX installers masquerading as legitimate software like Google Chrome or Webex. GHOSTPULSE uses advanced techniques, including side-loading malicious dynamic-link libraries (DLLs) and encrypting payloads, to evade detection by security tools.
- In February 2024, Rhadamanthys was distributed through a phishing campaign targeting the oil and gas sector. The emails spoofed the Federal Bureau of Transportation and referenced a vehicle incident urging the recipient to download a malicious ZIP file containing an executable.
- In March 2024, TA547 targeted German organizations with a phishing campaign impersonating the German retail company Metro. The emails contained password-protected ZIP files containing malicious LNK files. Executing the LNK files runs a PowerShell script that decodes and executes Rhadamanthys in memory without writing it to disk. This attack chain likely uses a large language model (LLM)-generated PowerShell script that introduces a novel tactic that leverages machine-generated code for delivery while the payload remains the same.

- In August 2024, Rhadamanthys was delivered via phishing emails targeting Israeli users. The emails contained a password-protected RAR archive that, once extracted, revealed an `exe`, `dll`, and `image` file. When executed, Rhadamanthys was dropped and run.

Threat/Technical Analysis

Insikt Group analyzed a sample of Rhadamanthys v0.7.0 and found that its core functionalities have not changed significantly from v0.5.0. The Rhadamanthys modules and XS custom binary format remain the same, as does its overall infection chain, which relies on the below three stages and multiple modules loaded at runtime **(Figure 5)**.

- **Stage 1 (Unpacking and Loading of Stage 2)**: Stage 2 shellcode is copied to the '`.textbss`' section of the portable executable (PE) file, which is then executed. This marks the beginning of the unpacking and loading process for Stage 2.
- **Stage 2 (Prepare System and Download Stealers from C2)**: The system is prepared for further exploitation by performing process injection, unhooking, and various process and evasion checks. It then loads the `proto.x86` and `netclient.x86` modules to communicate with the C2 server and subsequently loads the CoreDLL (Stage 3).
- **Stage 3 (Run Stealers)**: Various modules are loaded, and default stealers are executed. Image/OCR processing and additional extensions are also run. The system then reports the collected data back to the C2 server.

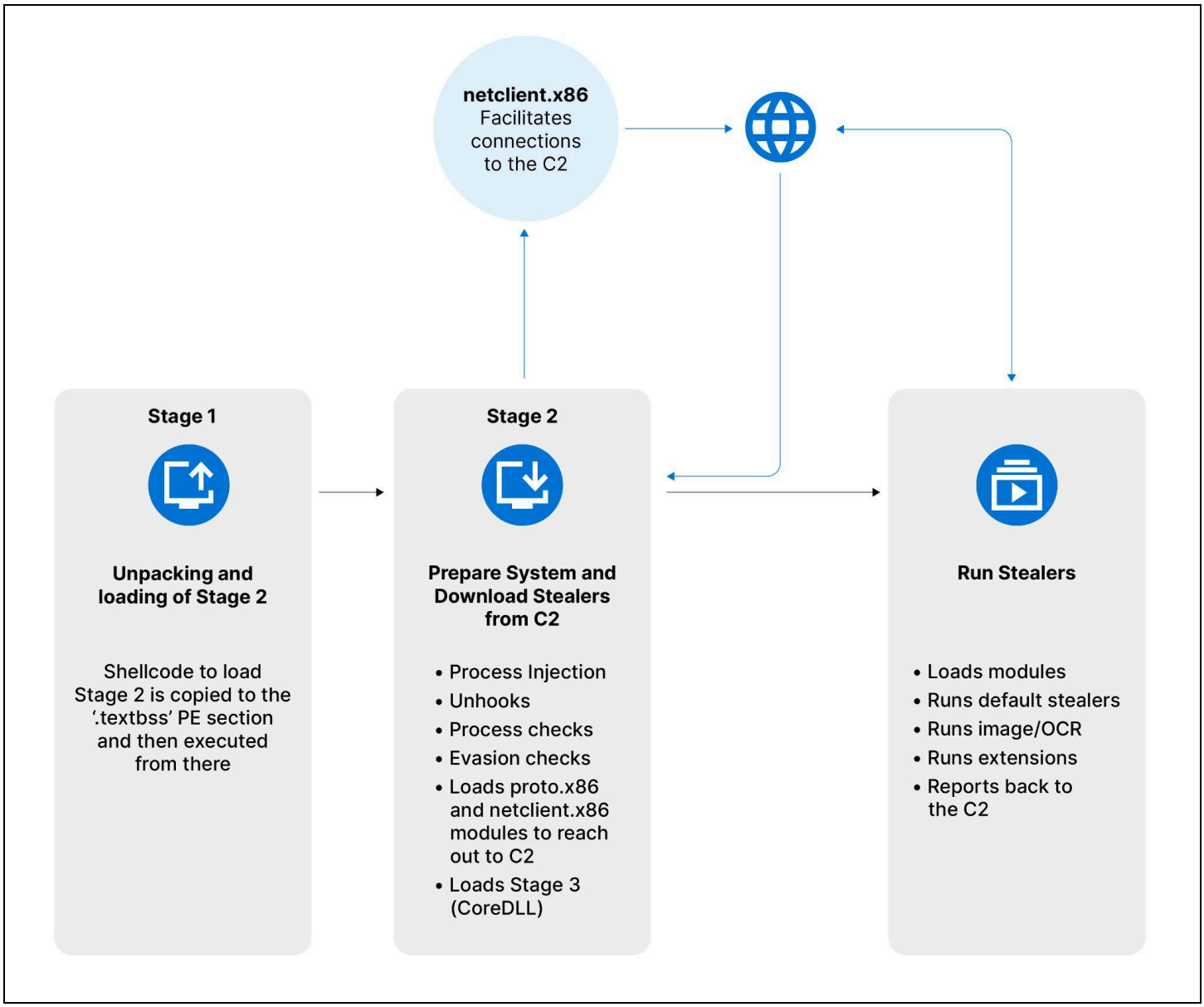


Figure 5: *Rhadamanthys's high-level infection chain (Source: Recorded Future)*

To avoid duplicating the in-depth analyses conducted by Checkpoint and others, Insikt Group has concentrated its analysis on the new features introduced in v0.7.0 and previously undocumented aspects of Rhadamanthys, including:

- The added ability for threat actors to install the payload disguised as an MSI file
- A Rhadamanthys mutex creation that can be used as a kill switch
- preventing re-execution by using a configurable timeframe specified in the Windows Registry
- Rhadamanthys's "Seed Phrase Image Recognition" feature enables users to search for crypto wallet seed phrases within image files
- Rhadamanthys's new extension delivery and extension analysis

New MSI Task Type

After establishing a connection to the C2 server, Rhadamanthys supports twelve different methods for running executables, modules, or scripts. A newly added option allows threat actors to execute an MSI file (a Microsoft Windows installer package commonly used by legitimate software) on the victim's machine. This option allows a threat actor to write data to a randomly named MSI file in the `%LOCALAPPDATA%\Microsoft\` directory and execute it via a call to ShellExecuteExW. Using an MSI file can be advantageous for threat actors because it can be perceived as legitimate by security tools, making it easier for attackers to bypass certain detection mechanisms. Furthermore, malicious payloads can be embedded and compressed within the MSI package, which can be difficult for analysis engines to detect.

```
DWORD __cdecl run_msi(int a1, LPCVOID msiBuffer, DWORD msiBufferSize, const WCHAR *arguments)
{
  DWORD executionResult; // esi
  int *localAppDataPath; // eax
  int localAppDataPathLength; // esi
  int *msiPath; // eax
  __int16 filePath[260]; // [esp+4h] [ebp-244h] BYREF
  SHELLEXECUTEINFOW execInfo; // [esp+20Ch] [ebp-3Ch] BYREF

  executionResult = 2;
  localAppDataPath = dec_wstring(enc__LOCALAPPDATA__Mi);// %LOCALAPPDATA%\Microsoft\
  if ( ExpandEnvironmentStringsW(localAppDataPath, filePath, 0x104u) )
  {
    localAppDataPathLength = lstrlenW(filePath);
    msiPath = dec_wstring(enc_msi);
    generate_random_filename_0(&filePath[localAppDataPathLength], msiPath);
    executionResult = write_data_to_file(filePath, msiBuffer, msiBufferSize);
    if ( !executionResult )
    {
      memset(&execInfo, 0, sizeof(execInfo));
      execInfo.lpDirectory = 0;
      execInfo.lpFile = filePath;
      execInfo.cbSize = 60;
      execInfo.fMask = 64;
      execInfo.lpParameters = arguments;
      execInfo.nShow = 1;
      execInfo.lpVerb = dec_wstring(enc_open);  // open
      if ( ShellExecuteExW(&execInfo) )
      {
        executionResult = 0;
        CloseHandle(execInfo.hProcess);
      }
      else
      {
        executionResult = GetLastError();
      }
    }
  }
  reset_tls_storage();
  return executionResult;
}
```

Figure 6: *Rhadamanthys's new MSI execution option (Source: Recorded Future)*

This new option is configurable in Rhadamanthys's C2 panel and can be seen when creating a new task, as shown in **Figure 7**.

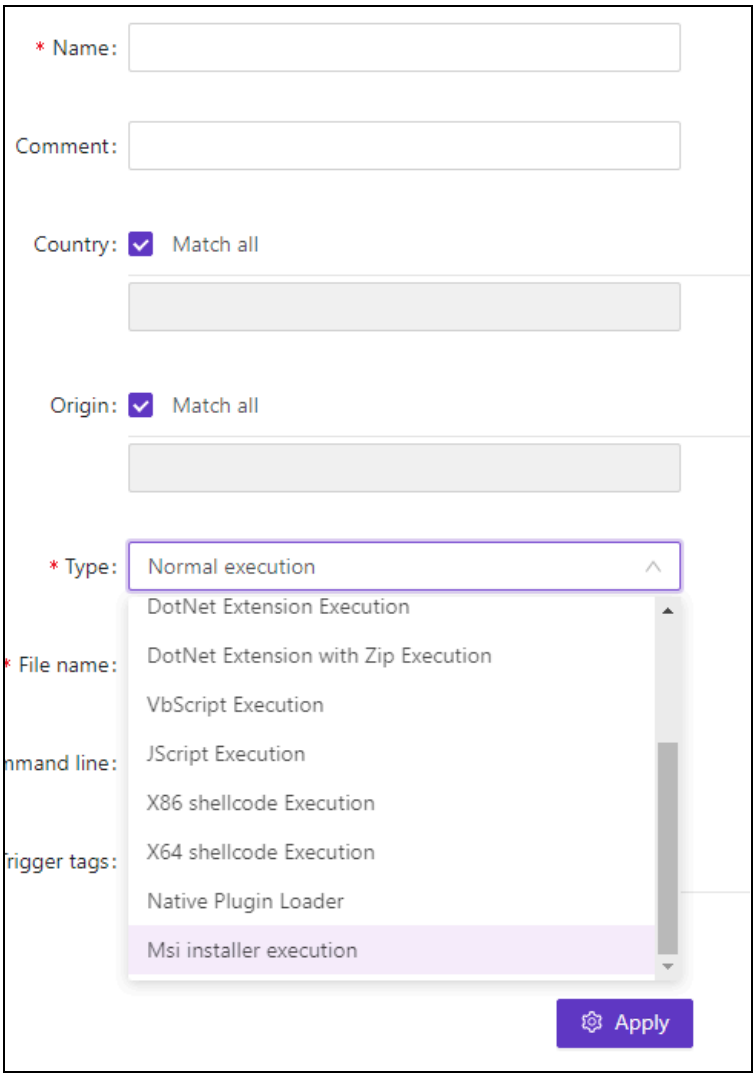


Figure 7: *Rhadamanthys's C2 new task dialog box supporting MSI installer execution (Source: Recorded Future)*

The Mutex Kill Switch

Rhadamanthys uses mutex objects to ensure that only one instance of itself runs on an infected host at any given time. A subset of the following bytes are used for mutex creation: `26 3f fb 04 18 9d b5 66 68 62 7b 8a 85 e4 b6 20 f9 da 5b 8e`. These bytes are the SHA1 hash value of the following eight hex bytes that are hard-coded in Rhadamanthys: `03 00 00 00 4E 4A 49 40`. The following C language format string is used to construct the Mutex strings:

```
"MSCTF.Asm.{%08lx-%04x-%04x-%02x%02x-%02x%02x%02x%02x%02x%02x}"
```

The function shown in **Figure 8** takes the bytes `03 00 00 00 4E 4A 49 40` and hashes them using the SHA1 algorithm, which then feeds the format string to create the mutex.

```
char sha1_hash[20]; // [esp+21Ch] [ebp-14h] BYREF

v60[2] = 0;
v60[1] = v58;
sha1_these_8_bytes[1] = 0x40494A4E;
sha1_these_8_bytes[0] = 3;
v60[0] = 0xC;
sha1_init_sub_80F0(sha1_context);
sha1_update_sub_9B2B(sha1_context, sha1_these_8_bytes, 8u);
sha1_final_sub_9BC4(sha1_hash, sha1_context);
v52 = sha1_hash[15];
v48 = sha1_hash[14];
v44 = sha1_hash[13];
v40 = sha1_hash[12];
v36 = sha1_hash[11];
v32 = sha1_hash[10];
v28 = sha1_hash[9];
v24 = sha1_hash[8];
v20 = *&sha1_hash[6];
v16 = *&sha1_hash[4];
v12 = *sha1_hash;
fmt_str = dec_wstring(51996);                   // get mutex format string
(snw_printf_loc_B81C)(v57, 128, fmt_str, v12, v16, v20, v24, v28, v32, v36, v40, v44, v48, v52);
```

Figure 8: *Mutex creation function (Source: Recorded Future)*

Nine mutexes are opened by Rhadamanthys using the Windows API function `OpenMutexW()`. If any of the mutexes listed below are found, Rhadamanthys will terminate.

```
Global\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\1\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\2\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\3\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\4\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\5\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\6\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\7\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\8\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
```

Table 3: *Rhadamanthys mutexes (Source: Recorded Future)*

Finally, Rhadamanthys uses the Windows API function CreateMutexW to create a slightly different value than the previous nine mutexes. The integer for the first format string parameter, `%08lx`, is the value of the variable used to count the mutex session count, which equals nine at this stage of execution to create the following mutex:

```
MSCTF.Asm.{00000009-4fb3f26-9d18-66b568-627b8a85e4b6}
```

Knowing the mutex values and that Rhadamanthys will terminate if they are present enables the creation of a killswitch/vaccine. If any of these mutexes are found on a non-infected system, Rhadamanthys will not execute.

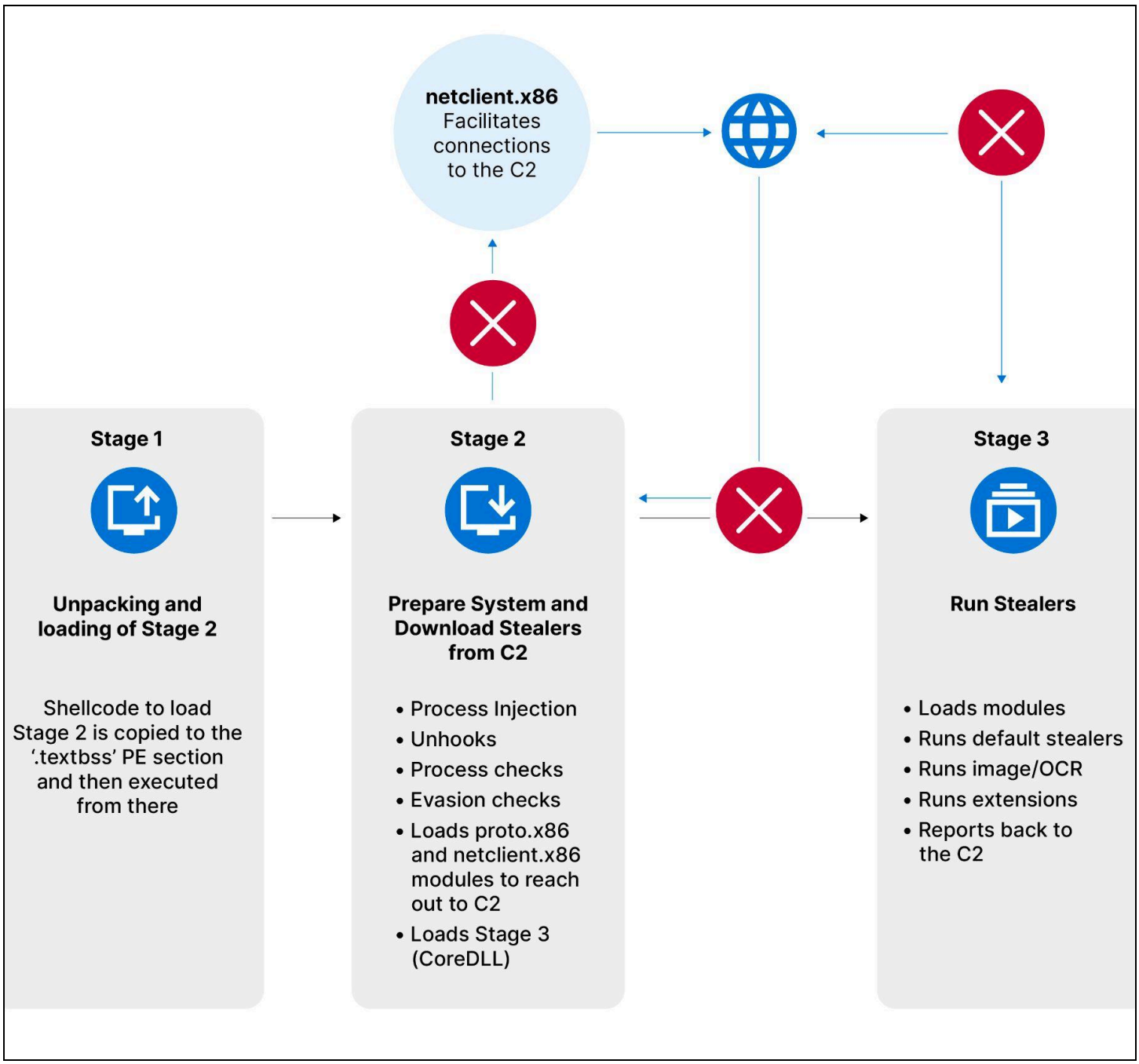


Figure 9: *Rhadamanthys's mutex kill switch (Source: Recorded Future)*

Note that the Microsoft DLL `msctf.dll` has been observed to create mutexes with a similar beginning string. However, the globally unique identifier (GUID) format in Rhadmanthys's mutex does not resemble

that. In terms of false positives, even if the formats matched precisely, the odds of using the same bytes as Rhadamanthys would make the occurrence of a false positive highly unlikely.

Re-Execution Delay Feature

Rhadamanthys contains a feature to prevent re-execution within a configurable time frame. The unique registry values used by this feature can be used to detect live and historical Rhadamanthys infections.

The configurable time frame for the re-execution delay is specified in minutes. It is contained in offsets five and six in the Rhadamanthys configuration (see **Figure 10**) and is calculated by taking the integer value of the two bytes. For Rhadamanthys v0.7.0, the twelve bytes in the configuration at offset `12 (hex 0x0c)` are used as a nonce during ChaCha20 encryption of the timestamp information.

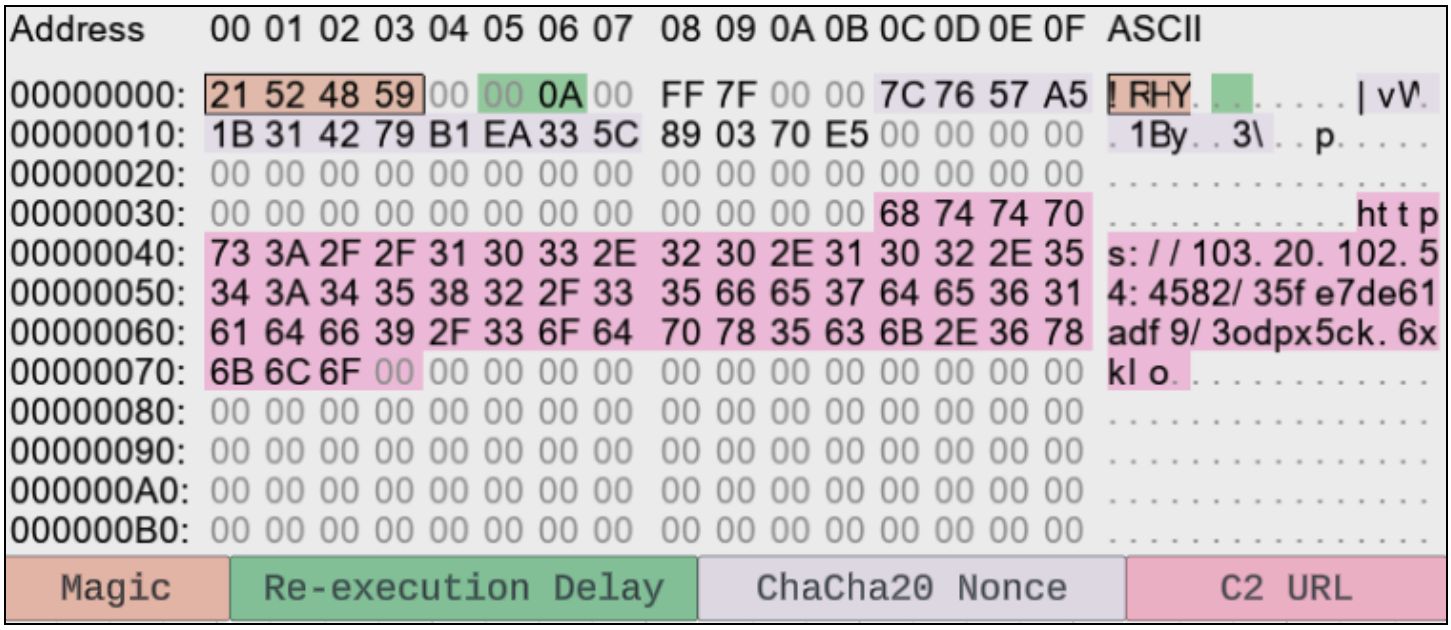


Figure 10: *Rhadamanthys's configuration and re-execution value (Source: Recorded Future)*

At startup, Rhadamanthys retrieves the number of seconds elapsed since midnight on January 1, 1970, via the `time()` function.

The re-execution delay feature implementation steps are:

1. SHA1 of the timestamp obtained at startup is calculated.
2. SHA1 of the timestamp is added to the front of a 128-byte buffer.
3. A null byte and then the timestamp itself is added to the above 128-byte buffer.
4. The above 128-byte buffer is encrypted using ChaCha20 with the following crypto parameters:
    - 64-byte key: SHA256 hash of the C2 URL against a zero-filled 128-byte buffer
    - 12-byte nonce: Taken from the configuration at offset 12 (hex 0x0c)
    - Counter: 64
5. Encrypted result of 64 bytes written to registry value `HKCU\SOFTWARE\SibCode\sn2`.

```
sha1_init_sub_80F0(sha1_context);
sha1_update_sub_9B2B(sha1_context, timestamp, 4u);
sha1_final_sub_9BC4(sha1_of_timestamp, sha1_context);
data_xfer_sub_10A0(timestamp_1, timestamp, 4u);
sha256_init_sub_7C43(sha256_context);
sha_256_update_sub_7C99(sha256_context, (config + 60), 128);// c2 url at offset 60
sha256_final_sub_7CFC(chacha20_key, sha256_context);
data_xfer_sub_10A0(nonce, (config + 12), 0xCu);// nonce at offset 12
chacha20_encrypt_sub_3787(chacha20_key, 64, nonce, sha1_of_timestamp, sibcode, timestamp_2)
```

Figure 11: *Rhadamanthys's re-execution function (Source: Recorded Future)*

On startup, Rhadamanthys will attempt to decrypt the value of `sn2`, verify the SHA1 hash of the saved timestamp, and finally subtract this saved timestamp from the current timestamp to check whether it is greater than the configured re-execution delay. The malware will exit if the time difference is within the configured time delay.

In v0.7.0, the author has made the re-execution delay feature tamper-proof through encryption and hashing. In versions before 0.7.0, the registry value `HKCU\SOFTWARE\SibCode\sn` is set instead of `HKCU\SOFTWARE\SibCode\sn2`. The registry key `HKCU\SOFTWARE\SibCode\sn` contains the time value alone. On startup, these earlier versions of Rhadamanthys simply subtract this value from the current time and ensure it is greater than the configured re-execution delay from the configuration.

Note that a Russian-based icon editor software also uses the registry key `HKCU\SOFTWARE\SibCode`. Due to this software likely not being used in an enterprise environment and the fact that the `sn` or `sn2` values created by the legitimate application were not observed while testing it, the risk of false positives is low.

Seed Phrase Image Recognition

A new feature added to Rhadamanthys in v0.7.0 is "Seed Phrase Image Recognition". This feature is part of the C2's configurable File Grab settings. It allows threat actors to specify maximum file size, minimum and maximum image resolutions, and which directories to look in for potential seed phrase images associated with cryptocurrency wallets.

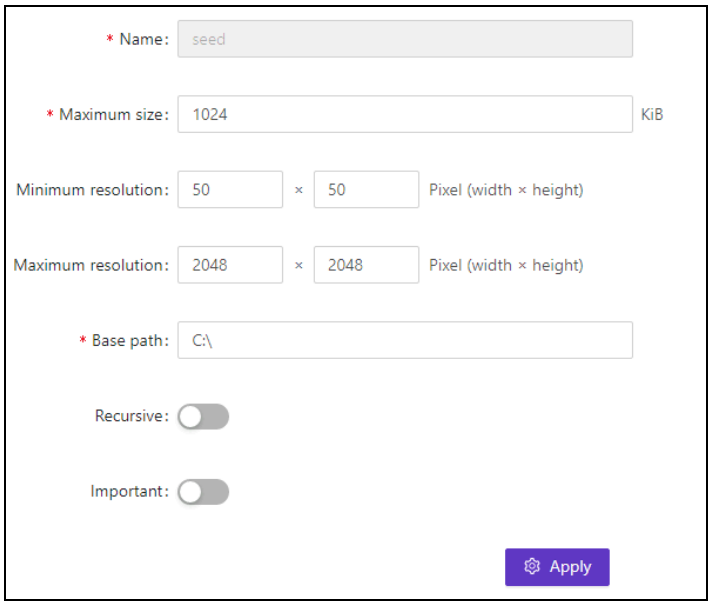


Figure 12: *Seed phrase image detection configuration settings (Source: Recorded Future)*

Figure 13 provides an overview of how the seed phrase image detection works. The `imgdt.bin` XS2 module and a `bip39.txt` file are saved as resources within Rhadamanthys's CoreDLL payload. When the `imgdt.bin` module is loaded, the `bip39.txt` file initializes OCR data for detection.

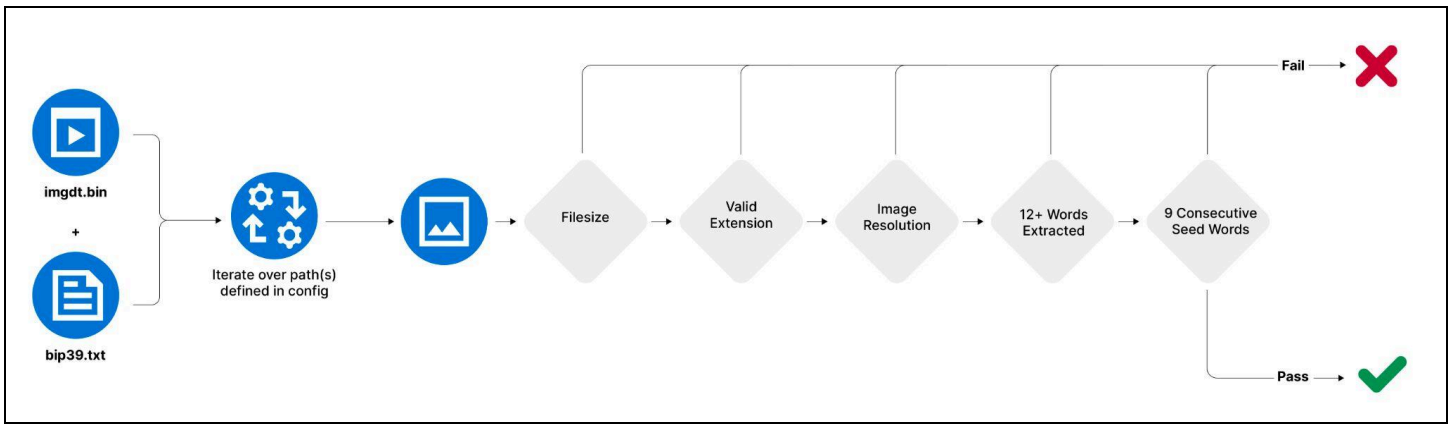


Figure 13: *Seed Phrase Image Detection workflow (Source: Recorded Future)*

Next, the base path for the seed phrase image detection configuration is inspected. If environment variables are present, they are expanded, and then the files and directories in the base path are enumerated. Each path is checked to see if it is a directory or a file. If it is a directory (and not a symlink), it will recursively search the directory depending on the seed phrase image detection configuration. If the path is a file, a check is done to ensure the file's size is within the bounds specified in the seed phrase image detection configuration before processing the file further.

Next, the provided file path is checked to see if it contains a valid extension (`*.bmp`, `*.tiff`, `*.png`, `*.jpeg`, `*.jpg`, or `*.bmp`). If so, the file is read into a buffer, and the minimum and maximum image

resolution defined in the seed phrase image detection configuration are passed to the `processImage` function in the `imgdt` module.

```
while ( !check_if_filenames_match(currentExtension, a3_fileName) )// check extensions
{
  currentExtension = currentExtensionPtr[1];
  ++currentExtensionPtr;
  if ( !currentExtension )
    return;
}
imgdt = a1->imgdt;
if ( imgdt )
{
  if ( imgdt->processImage )
  {
    fileContent = ret_a1(0LL);
    if ( readFile_0(a2_filePath, &fileContent, 0) )
    {
      imageDimensions[0] = seedConfig->minPixelWidth;
      imageDimensions[1] = seedConfig->minPixelHeight;
      maxPixelHeight = seedConfig->maxPixelHeight;
      imageDimensions[3] = seedConfig->maxPixelWidth;
      imageDimensions[2] = maxPixelHeight;
      if ( (imgdt->processImage)(imgdt->dword0, fileContent, HIDWORD(fileContent), imageDimensions) )
      {
        filePathLength = lstrlenW(a2_filePath);
        fileData = calloc(1u, 2 * filePathLength + 22);
        if ( fileData )
        {
          lstrcpyW(&fileData->filepath, a2_filePath);
          nextFilePointer = a1->nextFile;
          fileData->nextFile = nextFilePointer;
          *(nextFilePointer + 4) = fileData;
          fileData->prevFile = &a1->nextFile;
          a1->nextFile = fileData;
        }
      }
      free(fileContent);
    }
  }
```

Figure 14: *Seed Phrase Image Detection extension check (Source: Recorded Future)*

The `processImage` function of the `imgdt` module determines whether a seed phrase is detected by relying on the previously provided `bip39.txt` file contents OCR dictionary when attempting to identify whether a seed phrase is present. The `checkImageFeatures` function is responsible for determining whether a seed phrase is present.

The `checkImageFeatures` function ensures that at least nine Bitcoin Improvement Proposal 39 (BIP39) seed phrase words are detected and at least twelve total words are analyzed. It then analyzes the matches to check that nine BIP39 seed phrase words appear consecutively. Files with a suspected seed phrase are then returned to the threat actor via the C2.

```
if ( matches->ocr_words_detected >= 9u && matches->total_words_processed >= 12u )
{
  initializeBitStream(image_bitstream, bitstream_start);
  block_position = 0;
  while ( 1 )
  {
    one_count = 0;
    setBitStreamPosition((int)image_bitstream, block_position);
    for ( i = 0; i < 12; ++i )
    {
      bit_value = readBitFromStream(image_bitstream);
      *((_BYTE *)&bitstream_buffer[3] + i) = bit_value;
      if ( bit_value )
        ++one_count;
    }
    if ( one_count >= 9 )
    {
      max_zero_run = 0;
      for ( bit_index = 0; bit_index < 12; ++bit_index )
      {
        if ( !*((_BYTE *)&bitstream_buffer[3] + bit_index) )
        {
          zero_run_length = 0;
          for ( j = bit_index; j < 12; ++j )
          {
            if ( *((_BYTE *)&bitstream_buffer[3] + j) == 1 )
              break;
            ++zero_run_length;
          }
          if ( max_zero_run < zero_run_length )
            max_zero_run = zero_run_length;
        }
      }
      if ( max_zero_run < 2 )
        break;
    }
    if ( ++block_position > (unsigned int)(matches->total_words_processed - 12) )
      goto exit_func;
  }
  ret_val = 1;
```

Figure 15: *Seed Phrase Image Detection final validation (Source: Recorded Future)*

Upon receiving the suspected seed phrase images, the C2 server processes them using Tesseract, a robust open-source OCR engine, to extract the seed phrases accurately. For example, the image shown in **Figure 16** was identified as a suspected seed phrase image. Then, the resulting mnemonic phrase was extracted and presented to the threat actor within the C2 panel.

***Figure 16**: An example seed phrase image (Source: Wikimedia)*

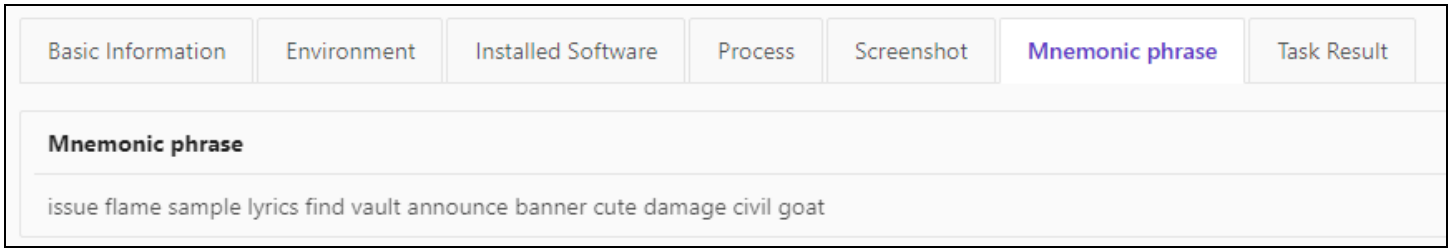


***Figure 17**: The extracted mnemonic phrase from the example image (Source: Recorded Future)*

New Extension Delivery

Rhadamanthys has extended its capabilities by offering additional plugins, starting in version 0.5.0 and continuing with new additions in later versions. Four key plugins have been identified:

- Keylogger
- Data Spyer
- Clipper
- Reversed Proxy

In version 0.5.0, these plug-ins were implemented as .NET assemblies and loaded via the `loader.dll` file, which is responsible for loading .NET assemblies. However, in v0.7.0, the plug-in system was updated. The plug-ins are now packaged as ZIP files containing two components, `classes.dex` and `manifest.json`, resembling an Android Package Kit (APK) file structure, though they are not actual APKs. The `classes.dex` file serves as the extension and contains several key elements:

- License check
- Loader code

- LZMA-compressed extension in XS2 format

This new structure allows Rhadamanthys to enhance its functionality further and maintain its adaptability in malware operations.

Extensions in Rhadamanthys are loaded and executed in a six-step process involving the CoreDLL and TaskCore modules:

1. TaskCore is injected into a process on the injected host.
2. CoreDLL sends the extension to TaskCore via a Named Pipe.
3. TaskCore verifies the extension's license to ensure it is valid for execution.
4. The extension is decompressed.
5. TaskCore executes the decompressed extension.
6. The compressed extension package is sent to TaskCore for further operations.

This process ensures that only licensed extensions are run and allows for efficient transmission and execution of malicious components.

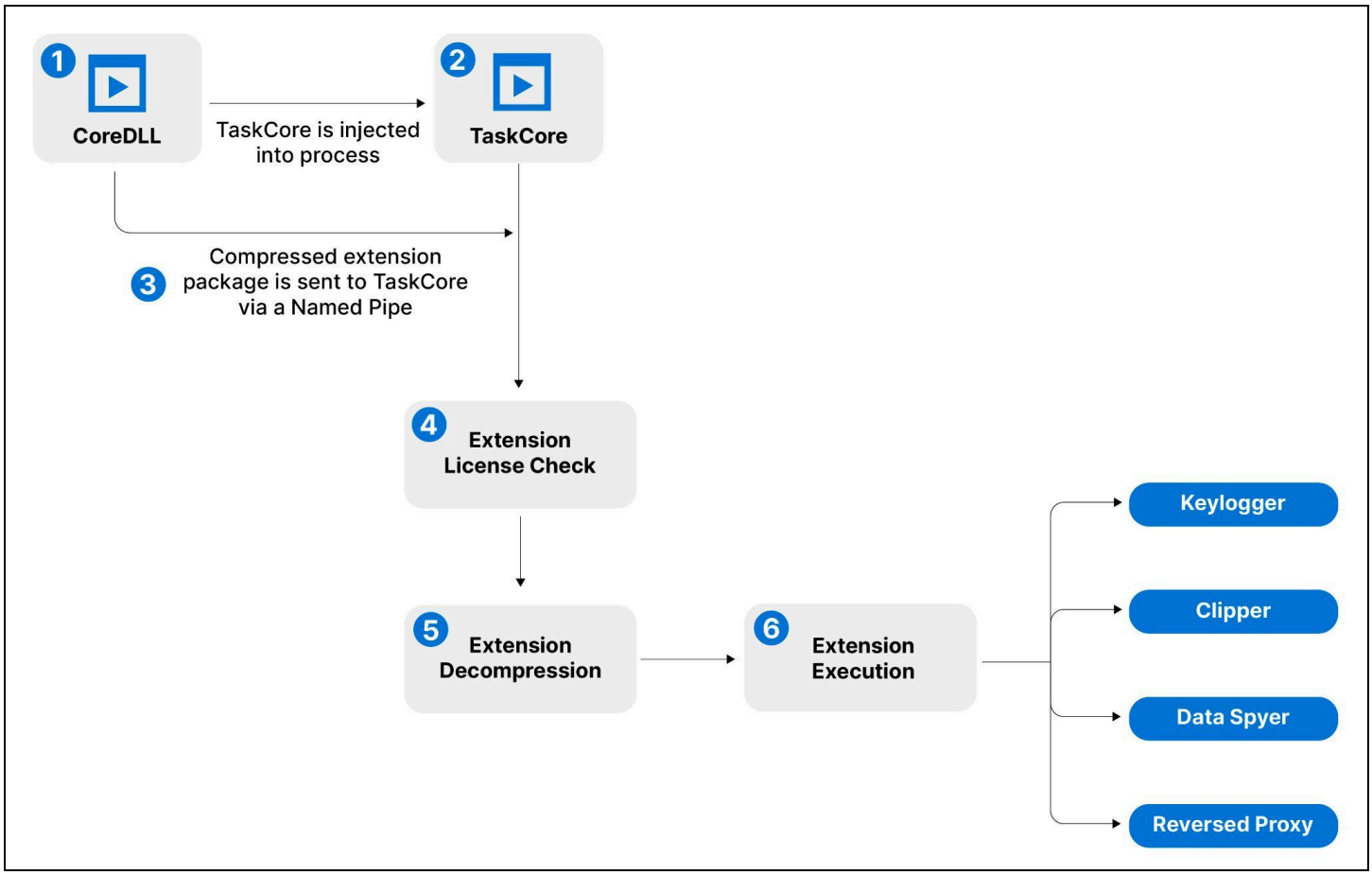


***Figure 18**: Rhadamanthys extension loading (Source: Recorded Future)*

Keylogger

The keylogger extension provides standard keylogging functionality. The core functionality revolves around hooking keystrokes, recording key presses and releases, and logging active window details to contextualize the stolen data. It achieves this by leveraging the `GetKeyboardLayout` API to understand keyboard layouts and correctly interpret keystrokes, regardless of language settings. The `GetKeyState` API helps track the state of special keys like `Shift`, `Ctrl`, and `Alt`, ensuring the accurate capture of uppercase characters and key combinations. The malware monitors active windows by polling the `GetForegroundWindow` API and recording titles and process IDs through `GetWindowTextW` and `GetWindowThreadProcessId`.

The keylogger also monitors the clipboard, exhibiting an intent to capture sensitive data often copied by users. The code explicitly uses a combination of `` `IsClipboardFormatAvailable` ``, `` `OpenClipboard` ``, `` `GetClipboardData` ``, and `` `GlobalLock` `` to detect when text content is copied, access the clipboard data, and read it.

The keylogger parses the `config.dat`, which is loaded in memory and passed from the CoreDLL,for the configuration items in **Table 4**:

Configuration Item	Description
`bufsize`	Record keyboard content buffer size.
`interval`	The maximum interval time to wait for sending. If the interval exceeds the last sending time and the keyboard buffer is not full, the data must be sent to the server.
`max clip`	Records the maximum number of bytes copied to the clipboard simultaneously. If the text data in the clipboard exceeds this setting, it will be discarded.
`filters`	A base64 string, which only performs keylogging of the process name set in the filter. The process names are not case-sensitive and are separated by a comma.

Table 4: *Keylogger configuration items (Source: Recorded Future)*

Data Spy

The purpose of the data spy plug-in is to steal login information. As of now, it targets remote desktop protocol (RDP) credentials. Given the focus on remote access tools, future extension developments would likely include stealing credentials for Citrix Virtual Apps and Desktops or virtual private network (VPN) solutions.

Clipper

Clipper is a cryptocurrency clipper malware designed to hijack clipboard operations and steal funds by replacing copied wallet addresses with those controlled by the attacker. The clipper demonstrates capabilities in identifying cryptocurrency addresses using a multi-faceted approach.

- First, the clipper uses pattern-matching techniques, using the built-in list of wallets and the replacement values found in the —`wallet-dict=` parameter passed in the configuration file `config.dat`, which is in memory.
- The clipper then implements checksum algorithms for each recognized cryptocurrency, ensuring only valid target addresses and maintaining high accuracy in targeting a wide range of cryptocurrencies.

Apart from the dictionary mentioned above parameter, the configuration also contains the keys in the table below.

Configuration Item	Description
`fulltext`	Enables address replacement over a full-text search and replace
`once`	Restricts replacing the same address to only one time
`wallet-dict`	Contains the list of target addresses to replace

Table 5: *Clipper configuration items (Source: Recorded Future)*

Reverse Proxy

The reverse proxy looks for the `-server` value in the `config.dat` containing the reverse proxy server to connect to and routes traffic to that address.

Configuration Item	Description
`server`	Provides the reverse proxy connection details

Table 6: *Reverse proxy configuration items (Source: Recorded Future)*

Mitigations

Mutex Kill Switch

By setting the known Rhadamanthys mutexes in the table below on a non-infected machine, a killswitch/vaccine to prevent Rhadamanthys from running its stealers and extensions can be created.

```
Global\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\1\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\2\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\3\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\4\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\5\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\6\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\7\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}
Session\8\MSCTF.Asm.{04fb3f26-9d18-66b5-6862-7b8a85e4b620}

MSCTF.Asm.{00000009-4fb3f26-9d18-66b568-627b8a85e4b6}
```

Table 7: *Rhadamanthys mutexes (Source: Recorded Future)*

Rhadamanthys Information Stealer Mitigations

Additionally, general hardening and logging techniques should be implemented to detect and mitigate attack methods commonly associated with stealer activity. Examples of these mitigations are listed below:

- **User Training:** Train employees on how to spot phishing emails and other common initial access methods used by threat actors to deliver stealer malware.
- **Multi-Factor Authentication (MFA)**: Use MFA for credentials to make using them more difficult for threat actors. However, please note that MFA can still be bypassed with session cookies.
- **Least Privilege Access:** Follow the principle of least privilege by granting users and devices only the minimum level of access needed for their job functions. If remote access solutions are crucial to daily operations, all remote access services and protocols (for example, Citrix and RDP) should be implemented with multi-factor authentication (MFA).
- **Security Information and Event Management (SIEM):** Implement SIEM solutions to centralized log security incidents across the network.
- **Endpoint Detection and Response (EDR):** Deploy EDR solutions on endpoints to monitor suspicious behavior commonly associated with stealer malware.
- **Recorded Future Hunting Packages:** Implement YARA, Sigma, and SNORT rules like the ones in Recorded Future Hunting Packages.
- **Credential Leaks:** Look for or create Recorded Future alerts for your credentials in dumps and criminal sale sources. A reset is recommended for every access method to any discovered credentials (cookies, sessions, passwords, and so on).

Outlook

Rhadamanthys has a rapid development cycle and is consistently evolving, with new versions being worked on even as the previous ones are released. This dynamic nature is evident when work on version 0.8.0 began after version 0.7.0 was released. Each version introduces significant enhancements in functionality, security, and evasion techniques. With the addition of AI features in 0.7.0 enhancing image detection capabilities, more advanced AI functionalities will probably be present in future

releases. While the detections and kill switch discussed in this report will prove valuable overall, the malware's consistent introduction of new features and evasion techniques will soon render the detections useless, continuing the difficult nature of detection engineering.

Rhadamanthys's global reach includes multiple campaigns targeting regions from North America to Europe and beyond. It is a popular tool in cybercriminal circles, supported by its versatile attack vectors and flexible plug-in system, making it a significant player in the underground malware market. Given this widespread adoption and continuous development, its influence will likely persist globally.

Appendix A: Tactics, Techniques, and Procedures (TTPs)

Tactic: Technique	Description	ATT&CK Code
Initial Access: Phishing	Rhadamanthys is distributed via phishing campaigns, often using email attachments like LNK files to deliver the malware.	T1566
Execution: Command and Scripting Interpreter	Rhadamanthys uses PowerShell scripts as part of its infection process, leveraging encoded commands to execute its payload.	T1059
Execution: User Execution	The infection often starts with user interaction, such as executing an LNK file from a phishing email.	T1204
Defense Evasion: Obfuscated Files or Information	Rhadamanthys uses multiple stages of obfuscation, including PowerShell scripts and encoded payloads, to evade detection.	T1027
Defense Evasion: Signed Binary Proxy Execution	The malware uses signed binaries, such as `AppLaunch.exe`, to execute its code and evade detection.	T1218
Defense Evasion: Process Injection	Rhadamanthys injects code into legitimate processes to avoid detection and ensure its malicious payload runs under the radar.	T1055
Defense Evasion: Virtualization/Sandbox Evasion	Rhadamanthys includes anti-virtual machine.	T1497
Credential Access: Unsecured Credentials	Rhadamanthys can steal credentials stored in FTP clients, email clients, and two-factor authentication.	T1552
Credential Access: Credentials in Files	The malware targets files containing saved credentials, such as browser password stores.	T1552.002
Discovery: System Information Discovery	Rhadamanthys gathers system information such as computer name, username, RAM capacity, and CPU cores.	T1082
Discovery: File and Directory Discovery	Rhadamanthys steals sensitive information by searching for specific files and directories on the system, such as Chrome user data.	T1083
Collection: Data from Local System	Rhadamanthys collects a wide range of data from the infected system, including system information, credentials, and cryptocurrency wallets.	T1005
Collection: Email Collection	Rhadamanthys can collect credentials from email clients using Outlook and Thunderbird.	T1114
Collection: Credential Dumping	Rhadamanthys can dump credentials from various sources on the infected system.	T1003

Command and Control: Application Layer Protocol	Rhadamanthys communicates with its C2 servers using HTTP and HTTPS, which allows it to blend in with normal network traffic.	T1071

Table 8: *Rhadamanthys TTPs (Source: Recorded Future)*

Appendix B: Rhadamanthys Change Logs

V0.4.0

```
v0.4.0 update completed!
Big update, server side and build and prior versions are not compatible,
if you need to update, please export the configuration backup on the old
version first,
and download the log data back to avoid unnecessary losses.

1.rpm -e rhadamanthys
2.rpm -ivh rhadamanthys-0.4.0-1.el8.x86_64.rpm
3.License renewal
4.systemctl restart rhadamanthys
Server panel
http://ip:443/admin/console/index.html
pass: 12345
```

V0.4.1

```
V0.4.1 update content
1. When the ALL TAG record is empty, the global download task push is not
triggered
2. Repair the major security vulnerability that the panel session is not
affected by password modification
3. Add telegram notification message template customization
4. Re-modify the client's construction form to fully support third-party
encryption services. It has been verified that all services available on the
market have been tested. You are also welcome to tell me about service
providers that I don't know yet.
5. Increase the one-click summary export of CC ftp phrase mnemonic words
6. Enhance the anti-ETW function of the client
```

V0.4.5

```
V0.4.5 update record
1. Add a dedicated shim server, the main server actively establishes the
connection, which can be switched on and off at any time. There is no
configuration reservation of the backend server IP on the shim server
2. The client and panel fully support ssl, support the use of self-signed
certificates, and enhance network breakthrough capabilities
3. The client is rebuilt, and all syscalls are implemented
4. The telegram module robot adds sending screenshots
id: <%id%>
tags: <%tags%>
```

```
id is the number of LOGS, tags is the URL tag set by the user
5. The terminal operation function is added to the panel, and the server can
be operated online. No need to log in remotely using SSH tools anymore.
6. Increase batch export of cookies by domain name
7. Increase the log download sign and the number of downloads
8. Export log format changes, and export compatible with redline format
9. The client adds the function of self-deletion after running
10. You can set the specified time to suppress repeated execution
11. Split all client information collection functions and choose to enable
them as needed
12. The download loader task system has been rebuilt, and the settings are
more convenient and intuitive

idaq.exe
idaq64.exe
autoruns.exe
dumpcap.exe
de4dot.exe
hookexplorer.exe
ilspy.exe
lordpe.exe
dnspy.exe
petools.exe
autorunsc.exe
resourcehacker.exe
filemon.exe
regmon.exe
procexp.exe
procexp64.exe
tcpview.exe
tcpview64.exe
Procmon.exe
Procmon64.exe
vmmap.exe
vmmap64.exe
portmon.exe
processlasso.exe
Wireshark.exe
Fiddler Everywhere.exe
Fiddler.exe
ida.exe
ida64.exe
ImmunityDebugger.exe
WinDump.exe
x64dbg.exe
x32dbg.exe
OllyDbg.exe
```

```
ProcessHacker.exe

If there are these processes, the program will exit automatically

v0.4.8

v0.4.8 update content
client:
completely rewrite the client
For each build, there will be an independent encryption key, reducing the
impact of correlation between users and each build.
Strictly tested hundreds of system versions locally, and fully supports all
versions of xp-win11
Actually test the following crypt services
@FoxCrypt_BOT
@PackLab_bot
https://cryptor.biz/crypt
@milianlzt
@zzipfile
@hAp_Crypt_Channel
@EasyCrypter_Bot
@AliceCrypt_help
@ferdenuk The encryption test only verifies that after the encryption process,
the RHAD program can start normally and complete the work. If the system not
supported by the crypt service itself or the stub is killed, you need to
contact the author of the crypt service to solve it.


Server:
Repair Trust walle deformation algorithm password cracking
Added multiple extension wallet interception
Includes UniSat Wallet KardiaChain real-time password cracking
Build pages and increase url validity detection. Avoid Misconfigured URLs
Traffic tags can be created directly during construction.
-----------------------------
V0.4.9 update content:
1. When repairing the export of all logs, the log download record does not add
1
2. Add country and build source tags as conditional items in the task module
3. The source label is added to the panel search, and the results can be used
in the export log operation
4. Added id number interval selection for panel search search criteria
5. Repair telegram configuration, when re-opening the settings page, the
selection status is displayed incorrectly.
6. Telegram notification adds machine name variable <%computername%>
7. Stub cleanup
```

V0.5.0

V0.5.0 Change List

01. Added observer mode
02. Diversify the construction of stubs and provide x86 x32 native Exe Shellcode Dotnet4 Dotnet2 to better adapt to various usage scenarios and crypt service needs.
03. The client execution process is completely rewritten, and the BUG in the syscall unhook code that caused the crash in the old version is fixed. The execution success rate is very high, and the runtime status is better.
04. Fixed the wallet upgrade support for several wallets where the cracking algorithm fails. Currently supported
(UniSat Wallet
Tronlink
Trust
Terra Station
TokenPocket
Phantom
Metamask
KardiaChain
Exodus Desktop
Exodus Web3
Binance
) Online real-time brute force cracking
05. Fixed Discord token acquisition, the correct encrypted token can now be decoded.
06. Break through the browser data acquisition when the browser is protected by third-party programs, and add the login data decryption algorithm of 360 Secure Browser
07. The panel search condition settings have been upgraded. You can now select conditions in batches and select categories with one click.
08. Add a quick setting search filter menu to directly menu the search conditions you need to check frequently.
09. Modify some changes required by users in the Telegram notification module and add new templates for use
10. When building a page, the traffic source tag can directly set the previously used tag, and the URL address will be updated simultaneously.
11. If permissions permit, data collection under other user accounts used on the same machine is supported.
12. The file collection module adds browser extension collection settings. For the Chrome kernel browser, you only need to provide the extension directory name and whether to collect Local Storage data at the same time. Firefox kernel browser can provide extension ID
13. Fix the issue of using the browser to use the online password library after logging in to a Google account in Chrome, and obtaining the login password.

14. The task module has been greatly upgraded, and a new plug-in module has been introduced to support users in secondary development of their own plug-ins.
Supports multiple task execution modes:
Normal execution
In Memory LoadPE Execution
Powershell Execution
DotNet Reflection Execution
DotNet Extension Execution
DotNet Extension with Zip Execution
VbScript Execution
JScript Execution
X86 shellcode execution
X64 shellcode execution
Native Plugin Loader
15. Keylogger: supports recording all keyboard input, process details, file name, window title, supports setting process filtering, sending time, buffer size
16. Data spy plug-in: currently supports correct login access and IP username and password for remote RDP access. The correct certificate file and password imported by the user.
17. Plug-ins and loader modules support secondary development and provide SDK support.

V0.5.1

V0.5.1 Change List

Added Clippers plug-in

2.Telegram notification, you can now choose whether to send wallet crack and seed records in the log ZIP

3.Google Account Cookie Recovery

4.Default build stub cleaning for Windows Defender, including cloud protection

V0.5.2

1. Shim Server V0.4.0
Enhanced disconnection detection with the backend server, allowing you to accurately learn about abnormal connection status and make repairs.
2. Clippers plug-in V.0.2
Fixed the bug of repeatedly uploading the same replacement result. Fixed log viewing paging function.
The biggest function is to add full text replacement function! Adapt replacement for various copy operations.

Added a new function switch that enables the same address to be replaced only once.
3. Reverse proxy plug-in
Reverse proxy requires another server to install the access server
The update will not affect the currently running client, but only involves file updates on the server.
09:35
(need another VPS to install the reverse proxy platform server. Build your own 911 reverse proxy network)

V0.6.0

v0.6.0 Update:

1. Both main server and temporary server support Block geo &ip . Function. Blocking or cancellation of IP or country/region blocking can be disabled or cancelled by simple operation on the panel.
2. Modify the process of writing library when the server receives client data, now you can save it while receiving. Optimised for clients with large log volume and slow network speed, there will not be a situation where log details cannot be listed.
3. Add new extended wallets (Leap Cosmos, compass-wallet-for-sei, Venom Wallet, Rise - Aptos Wallet, Rainbow) in the built-in collection, and fix the problem of incomplete data collection of COINBASE wallet.
4. a special icon has been added to the panel to indicate whether the collected files are seeded or not.
5. Restore factory mode added index library cleanup function, which can release the space occupied by index library and synchronously clean up the useless or obsolete space occupied by other directories.
6. export browser password and cookie operation, add refresh cache operation, reduce log deletion.
7. Enhance the protection of the index database.
8. Modify the composition of the extended wallet directory in the log, remove the use of [ ] symbols, to avoid the problem that the user's later automatic processing tools can not identify the processing.
9. build stub clean, bypass windows defender.
The next version is planned to be updated:
Open API interface
Add log file FTP or cloud storage distribution function.

V0.7.0

The main change in V0.7 is that the client-side and server-side frameworks have been rewritten, and now there is no problem with the execution stability of the program.
Added 30 wallet cracking algorithms.
Added AI graphics and PDF recognition to extract phrases.

```
Enhanced the extraction of multiple phrases saved inside the text.
Fixed all the bugs and problems in the previous version.
Rewritten Telegram module to support HTML format and multi-token polling.
Rewrote the synchronization module to support remote FTP synchronization for
transferring received logs.
Rewritten the search filter module.
Add API interface, open platform
```

Table 9: *Rhadamanthys Change Logs (Source: Recorded Future)*

Appendix C: Sigma Rule — Setting Registry Value `sn`

```
title: Rhadamanthys Stealer Malware Setting Registry Value sn
id: 3c7b2689-89d2-490f-a48e-c8579134c865
description: Detects the Rhadamanthys stealer malware setting HKCU\Software\SibCode\sn
with the current timestamp for the re-execution delay feature.
references:
 - ARMOR Internal Research
status: stable
Author: Insikt Group, Recorded Future
date: 2024/08/08
level: high
tags:
 - attack.t1112 # Modify Registry
logsource:
 category: registry_set
 product: windows
detection:
 target:
   TargetObject|endswith: '\Software\SibCode\sn'
 details:
   Details|startswith: 'DWORD'
 condition: target and details
falsepositives:
 - unlikely
```

Appendix D: Sigma Rule — Setting Registry Value `sn2`

```
title: Rhadamanthys Stealer Malware Setting Registry Value sn2
id: f3c78795-ad90-42e1-9dca-d84066bf35a4
description: Detects the Rhadamanthys stealer malware setting HKCU\Software\SibCode\sn2
with an encrypted timestamp and checksum for the re-execution delay feature.
references:
 - ARMOR Internal Research
status: stable
Author: Insikt Group, Recorded Future
date: 2024/08/08
level: high
tags:
 - attack.t1112 # Modify Registry
logsource:
 category: registry_set
 product: windows
detection:
 target:
   TargetObject|endswith: '\Software\SibCode\sn2'
 details:
   Details|startswith: 'Binary Data'
 condition: target and details
falsepositives:
 - unlikely
```

Appendix E: YARA Rule — Rhadamanthys Initial Stage

```
rule Rhadamanthys {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2024-08-07"
        description = "Detects the 1st stage of the Rhadamanthys Stealer Malware"
        version = "1.0"
        hash = "643d2764447b953c2203f53263ea1d66a361ceda7b72c3cdac7d633413596647"
        hash = "1b0215062992174a807e9203688e5727a27c8aaf8a1b5dbdcd10d0d0ea89f7aa"

    strings:
        $textbss = { 2E 74 65 78 74 62 73 73 [8] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 80 00 00 E0 }
        $masq = "Roland GS Sound"
        $xor1 = { F6 35 8D FA 4F A7 98 E6 }
        $xor2 = "xxxxxxxxxxxxxxxx"

    condition:
        uint16be(0) == 0x4d5a and filesize < 600KB and filesize > 350KB and $textbss and
(($xor1 or $xor2) or $masq)
}
```

Appendix F: Indicators of Compromise (IoCs)

IP Addresses:

5.230.67.168:5140
38.180.100.139:443
38.180.188.69:443
45.61.166.131:443
45.152.84.68:443
45.159.188.37:443
45.202.35.41:2085
57.128.169.122:443
74.81.56.118:8039
77.91.78.112:443
77.221.148.235:443
77.238.245.97:2017
77.238.248.142:443
80.66.75.110:9176
80.66.79.88:7691
81.19.131.103:2013
83.217.209.45:5902
83.217.209.52:443
85.209.90.135:443
88.99.62.143:3674
89.23.103.235:443
89.117.152.61:443
89.117.152.231:443
89.208.103.86:8537
92.246.139.134:443
94.232.249.76:443
94.232.249.92:443
95.216.91.91:1614
95.217.44.124:7584
103.148.58.146:5199
103.148.58.151:5199
103.148.58.152:5199
103.173.179.189:443
104.234.167.212:443
107.189.28.160:7705
135.181.4.162:2423
139.99.17.158:443
142.132.161.168:443
144.76.133.166:8034
147.45.44.107:443
147.45.44.126:443
147.45.44.143:443
147.45.44.187:443
147.45.44.195:443
147.45.70.184:1525
147.124.220.233:7843
149.102.143.198:9586
154.216.17.85:443

154.216.17.126:4501
154.216.17.181:443
154.216.18.122:2013
154.216.19.149:2047
162.254.34.46:443
167.88.170.44:443
170.205.38.149:443
172.236.107.96:443
178.22.31.64:443
185.161.251.6:5545
185.161.251.67:6777
185.184.26.10:4928
185.196.10.175:6491
185.196.11.237:9697
185.209.161.207:2421
185.234.216.132:2018
192.30.242.19:9480
192.30.242.44:6581
193.124.205.63:7404
193.143.1.77:1640
193.143.1.77:1641
193.188.20.191:443
193.200.134.94:9880
198.135.48.191:3090

Hashes:

31db744883c163774f75f9ed915f991a460517f793ccdd8e5fb05964b7b0789c
cc8b0af0cd9c2a09c33e266729d526f64e14790171014059694272 6c68ca820f
0bdaf3ea7f4b9a47d5d2a8d2309cc251eacce1abe2ab47e873a4bda82c8c3ace
b2a9ce1b9474564ed479861222f41161bca44bf584953f5c13348b0d5d3ab8ab
03c72cfabace07b6787d2d1fd66d6d6d9a2fbcb74a827ca4ab7e59aba40cb306
3290e7b795b9e84bd9c7233290b3df4bd404945451fa845ff613b9a394be63de
c339bc88c7ecc7c7d099e8457e16a7094fc2243e68ec30041d048b4f97b224c1
5abee9b851bc50e1399c5604376e2c8599b721eea0a24d231204726a8b1e5b6b
95897f8814e4c651671799af51c40fbe0a2334827683c82640627e270c57d9d7
0d3a0b5c502bdeeeda6930a71896e5adf70a0338f290be3b8edc9f8fe03b312f
d75a5e432832ffd4deaa2bccd75e01fa0a511e0874c2ac8a8c0bb199b01b439f
aeb4171ec2a9f0400f54d5dd7a89041bc89ffa61627d26c20297fa849a37ffe9
07c39df94416dfb58f22a0a1e46c8a9e2a2db3e273282574fbf13f574ec62b55
528f6c8f0c5d2399ea77e134bb4b4ab72883b4a8abe45e51dcef0e4abce0ce7e
80cebeda935ad7e193a97b4053d667caf31938b6500cc700df1e77a2f8bd208c
29d05396755f6102a42f199698b499b8d088324e8c79cc4cbb392d7ce1a5f40d
bb1464e75c750d90c0c49d148c9e64eefe0c29b2f670d708c8085ddd3104dbfe
314fe9383a2d78cbd2bf0f8014210c53c346b7995d1e86f72ec4d666b43586c9
7213da4c9a6a8cbf1d0e90ac3bfc082c8c92d4147ccc7fbc45c0a96270a36b0d
0b1ca7ed4460ba1fa8e6a0fbbca8dba4ff9e0a148521a3c79b6a14aef157f0ae
4575e0cc175fe8062123d5043ac3e40b3f8d7834305b87be392bf545f4e06151
6404ac4cac4d53dbbe19c6cef158ea1e2d1e263710058c140cee70b6881efacf
b90e166ad379671547a1ca303474d2d91773cc8bfce72e59344ac91ff3d51eb4
34918278f6eb6b5e3afa8da406eb3c5a4cc3b7c4a1cee55320fecdbef4e0a463
079caeb8f65bf60f958ed97244bc86fce83765614b22e4122d76435e50c23432
741b85f17765f4f17c342195642a39a34c8274c01e436b97b4e9294538310fd4
f158ce347d17fc8ad7504d5eb54cfb894237228dc9da46be26a5159fc07df94f
876c6f4d85012dc4c8a34598efe8f29c9f238a7b2a55444f45b062df258837ba
a32c1877d61900c22bd203158c18662cdfe360c88d3fc48b03532b1b935a1781

```
026b74331d4a67543a6ed4e636ef15ed5bc582daa3d143a8d4413b77801987b6
e62ba1c16c87313e0ae8a6c4ccf31eebca0927009c31e2317458aa09777a6ff8
5773216e3a9c0120fb5b08108b22ca4e175b2d4aa66107e33e72c95e283e8280
f9bdf078977c7fc938d3d0b4d4788f810af4791d502a7dbb5fee05bb633019da
e8a5b628a7fa45595eecb1f92d353d8b5d175d94f7befac803f11b1ffaf24e21
e53705f07a3a1ac7ca56ab495ba6d8fac9667d1a5a53eba3806f3acef2354ed1
6135bdbcfd9f824b3da0bef2ba73018a998967e20c5d0274c6a1c0433649b017
cbdaaf3f0cee70700df7c69c015fb98f5a69fb374cb1b9f57b8136813468b9db
e36bbdf75e56c4d0562ba5aba9e78d483a6196fe1ec891cc71ef9db5556c9c81
f9d1a3b43fdeca1691af785f6bdfb445c224e46e58be9d27ba4d77801ef2183f
99bd6ee7da4edad447fba55a6b11538927013586ef617e70a0ff4765adae22db
3005dac31220c8a2abef6fa332ef2a7e37843364c8ba5e1636e6679ec17febdb
6df2f4ce49b4fe7ef70623f25367380e14ce6f4a01fd06d8278bde1c712a9df0
b5bc03acaeb80ef98945cc3e0e7726276feb68e05b4e4811727b6d500cd67e37
d03e607e00e4e7dc4e5709a5ba73c21c923cdec0387cf3d7f2ec0c2d9979e370
2fc82bf903409c53ed2b488b7920be9df0c60835d12bb21c45c27384e4a1ff38
5c109b1d10f6969c8f4c6073180b15464c91937f33765bcbd2890d8dc0ca9220
7a03776b44cd724c05d692c4d78b09e9b8a1ea7e2c049d448dc79cf5d3d753f3
22beb0b11f2d0af021ed7514b2a382e2bd1f7e02e6a811fd4c903a75fce19d93
60cc28ae765bee54fb21f9291765a8930c9e18fe0e8f61ffc35996c6e72c5410
e5cc2137f5d4b69307e0a08ec5da4e35dc74648f262ed649c086d823cceb073f
0a8d8d26ed46de316efab3e7b31e46c5afb1fa67bfe950e1a8a27d79c78912b8
1fd5d4bbe948c9c60602392c338ea07fdbe44dea6216013a62c180aea97d2c1f
2003e381ae90e155ee9e413ecb9d696b5e01b0774a619fd72a02d31b85e74177
57acff4f016a60dde891df70d69d020853e679e2a5c99e4d3a605f1e11f33bd3
c0bdfba4ce1dd72f3c9b18459eaefdc17bb3612f2bb71888f9da5239ff84cc24
618fa764a0ab38d55e9904b562cc33408ff870eee38fef0897fbce8ad4c0ed0b
eaede80aa7400cd537e6a02385b397f38e76884b4d2122f05e7e6f021846f6a6
760a286108560faeb1f7f08b428d96aa1a88b17cc80d5d48847451efc0ed33cb
8088aedd53e360cee68378465155fa95aab5b583ac863a2e83cb5817f90c47ab
37017880268199de83a2080d1e23abd021f1ce76c2bbf68f95b1905f672c172f
9c6c64d5df68dc25fdb0c4ad021c9ecae9388f33717227eb9c8cd956b20e531d
4112161c45eae51019c33c6b5f5c3fb3024681ecf925d1c1af1f9c95066d428c
1f25fcaab335b52fe140bdedbce4e86a9e1b7bc0f31a9553ef55fa680d05cb37
9a97d52df9c7434cc01b4a26500b6584765fe7fb4ab1f9761724daba07948f6d
0a27c79559df172c25afb1d7ff16c0c220fb75925e5d61ec9ed54b83b0d71863
0218063602407eab13b71f311ed1be489c95f7dd2a6f8681871cb9025158ba8f
bd86b97948754903efe08cdb8b90c045e2fd10b6a7be88f94453e2489b2313c3
f4c0791bfc731d2774477d3b5e5164df302dbe2c732d4937be818ba712753e14
f2efe88c8041ccc776859c8b80fb981cf1cf9805b80fc66500738c223a88c713
35a70792a57447358477e5ca678420f14f577ed8e7956c9ee9013b8633d7feac
d94ffbeb0ca3a1ed919281dc57e95cd34064bc053f59ec69d9cdbb5d6a714b36
2fb0ca131bf1578752451e129c0e0de79a1eb58315e807949eb5dcedf68d750b
469789801593b0582e7da5acaf9e17c02776f6783d378ce42e90a817be5aedc6
8dca5512413cc1620911c1be69ae058e5040aba01178170ad0eb46f95667f51a
c27cba4a291c6dacc6d0c941b7bc0420e20a575902b207dd15f289509ba29314
7587be1d73dd90015c6200921d320ff0edcec19d7465b64d8ab8d12767c0f328
10ac0976b8f00ee4cdc65d473236a881a44c91a0d3ccdd5210c7a5bb3c41f920
9827f74e7c31c2399da388ff8f1039455b1739542dbaa16bf86bf23d38e8f07b
643d2764447b953c2203f53263ea1d66a361ceda7b72c3cdac7d633413596647
bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf
cff554d01ac17319ba2fec1acd8a3262386b3a01592741194b4fb05924e302e1
141ee34a8afb8f5a9d47e4910395bc70098a40ab46eb65bf3fb0b8e7c415c956
93510385e8c133675c386fec3e080fb27c536f6e8bbb640f766d09de65351cff
2bce0f081ce235caa11d047b750271c636b394c20e2188659edbeb7ffc591aba
1b0215062992174a807e9203688e5727a27c8aaf8a1b5dbdcd10d0d0ea89f7aa
df97eb504ed5a3298737f83d418d70025f3be0daf56d6ccae35ec0d2ef813b20
22a728ef7efea571769b481eaa224b4ae1f0151ae899ac2f30f3493e8e8166ee
bab017ca2aa472dc3b0370dba0bd356939a62947f4ff83ef4810a70a68fab1df
14a61d65ae287dde9da0482d7abda0fc32f116b16ed9fdeef56f35b3d6cf27fb
```

67825f431a99f551c9d75539be11907c3bcf91e9d55b6a91be221e4193eba49e c1680857ca2993539b1cf3040f144cd26e324c0091ef7e4e500a390584c98b66 819fff43c92af475d74a65fec08f8477df6c3f36c5c746c794d79d71f8c97dda

Table 10: *Rhadamanthys IoCs (Source: Recorded Future)*

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com