Deep analysis of KPOT Stealer

By S2W

Published: 2021-07-07 · Archived: 2026-04-05 18:14:08 UTC

Detailed Analysis

Malware Information

- Filename : klfile.exe
- MD5 : 9dc97eaed4e61901afc327ce9f122262
- SHA-1 : 41881d3463f4246d4d0146faf39703354bab83e9
- SHA-256 : 4412624d06991fa64f684fcc6d66c787d040eaa12356885cf0a0919c732c82a3
- File type : PE32 executable (GUI) Intel 80386, for MS Windows
- PDB path : N/A
- Original name : hita.exe
- Certificate : N/A

`C&C : kpotuvorot10[.]bit, dolboeb1701[.]com`

Behavior

1) Packed with DerpLoader

This binary is packed with DerpLoader, which is also used for packing Raccoon stealer, Vidar stealer and REvil ransomware. It’s almost impossible to cover every polymorphic variant of this loader with a static method like Yara, since each packed binary has a unique stub built with dummy API calls and exported functions. This packer has 3 stages — decryption, decompression, and execution with process hollowing.

2) Using Murmurhash3 for string comparison & importing procedures

This stealer calculates 32-bit Murmurhash3 of a given string with a specific seed and compares it against the hash value of the target string, which is hardcoded in binary, to check the value of the given string. For this sample, `-794794744` (`D0A06508` in unsigned hexadecimal) is used for seed value, but it can be changed for other builds. This string comparison technique prevents exposure of some keywords like process name or folder name, which makes analysis harder. Murmurhash3 is also used for importing procedures from libraries by calculating the hash of the procedure name and get the address of the procedure only if it matches the target hash value. We can write a simple code to brute force these hashes with pre-built word lists.

3) XOR-encoded string

If plaintext is required to accomplish the job, then the stealer uses XOR encoded strings. Each string is encoded with 1-byte XOR key, and these keys are stored along with string length and pointer to the encoded string.

Following IDAPython script will decode the string stored at the given index in the table.

4) Resolve domain name of C2 with Blockchain DNS

`.bit` and `.lib` TLD is managed by a decentralized blockchain called Namecoin and Emercoin. This stealer can resolve these blockchain-based domain names by using blockchain DNS services like Blockchain-DNS, dotBit.me, or OpenNIC DNS servers. During the initialization step of the stealer, it tries to resolve `kpotuvorot10[.]bit`, and if it fails to resolve `.bit` or `.lib` C2 domain then it falls back to other address `http://dolboeb1701[.]com`. Unfortunately, those C2 servers are not available at this time. Querying `dolboeb1701[.]com` on RiskIQ shows that the domain was last seen at 04-01-2021.

The stealer tests the availability of C2 by sending HTTP GET requests to `{resolved_addr}/bgczXibj92HSlSCK`. If it succeeds, then the whole URL is stored in memory and used for other C2 communications.

5) Using volume serial number for mutex name & victim ID generation

The stealer calculates a simple hash using the volume serial number of `C:\` drive for mutex name and victim ID. Following code is hash algorithm ported to Python.

6) Download configuration from C2

The stealer sends HTTP GET request to `{resolved_addr}/bgczXibj92HSlSCK/util.php?id={vsn_hash}`. The response should be a configuration of the stealer, which is encrypted with XTEA and encoded to the base64 string. The stealer decodes the downloaded base64 string, and decrypts it with key `TezTfpjNMdcP6FNE`, which is stored in XOR encoded format.

Decrypted configuration is slightly changed from the older version of KPOT 2.0. Now there's a slot for a shell command between feature flags and the victim's external IP address.

7) Collect system information

After downloading the configuration, the stealer collects some system information.

- Privilege status of the current process (elevated or not)
- Integrity level of the current process
- Windows version
- Victim ID (generated with volume serial number)

Then, the stealer performs 'CIS check' by querying the user's default language ID. If the language ID belongs to CIS, the stealer won't steal information from this computer.

If the victim's computer passes a CIS check, then it collects more system information.

- Windows product name (with bitness)
- MachineGuid
- IP (use external one retrieved from C2 server)
- CPU (Model, number of cores)

- RAM
- Screen size
- Computer name & Username
- Local time
- GPUs
- Keyboard layout
- Installed softwares

All pieces of information are written to the stream, which minimizes footprint.

Get S2W's stories in your inbox

8) Steal application data

The stealer steals data from some apps by default and additional features can be enabled by configuration. Applications and feature flags annotated with bold characters can be applied to other users in victim PC, if the stealer process has required privileges. Some stealer functions require registry access for HKCU or HKU.

Stealing data from these applications are enabled by default.

- NordVPN
- mRemoteNG
- RDP connection profiles
- EarthVPN (Registry access required)
- Outlook
- Windows Mail

The first 16-bit digit of the stealer configuration controls the optional feature of the stealer. Bit 0~13 enables or disables info-stealing functions.

flag[0]: Steal data from Chromium-based browsers

flag[1]: Steal data from Firefox-based browsers and Mozilla products

flag[2]: Steal wininet cookies

flag[3]: Steal cryptocurrency wallets (Registry access required for Namecoin and Monero)

flag[4]: Steal Skype database

flag[5]: Steal Telegram database (Registry access required)

flag[6]: Steal Discord database

flag[7]: Steal Battle.net configuration files (including auto-login information)

flag[8]: Steal data from IE (including FTP accounts and Windows Vault)

flag[9]: Steal Steam accounts (loginusers.vdf and SSFN files)

flag[10]: Take a screenshot

flag[11]: Steal accounts from Total Commander, SmartFTP, Filezilla, WS_FTP, and WinSCP (Registry access required for WinSCP)

flag[12]: Steal Windows user credentials and Pstore (for the older version of Windows)

flag[13]: Steal XMPP(Jabber) accounts from Psi, Psi+, Pidgin, and libpurple based clients

If the stealer process has a high integrity level, SeDebugPrivilege is enabled to duplicate SeCreateTokenPrivilege from other processes.

After acquiring SeCreateTokenPrivilege, the stealer process creates a new process token with SeBackupPrivilege enabled which allows accessing other users' folders and files by ignoring ACL.

9) Exfiltrate & drop files

The stealer can be configured to exfiltrate files from the victim's PC. Configuration can contain multiple file grabber settings delimited by keyword `__DELIMM__`, and each element of grabber settings like filter or path is delimited by keyword `__GRABBER__`. The path can be set as `%FULLDISK%` to exfiltrate files from all drives of the system, or `%NETWORK%` to exfiltrate files from all resources on the network. If the stealer process has SeCreateTokenPrivilege, it can exfiltrate files owned by other users by creating a new process token with SeBackupPrivilege enabled.

The stealer can drop files after exfiltration based on configured URLs. If the downloaded file is DLL, then it is manually loaded by a custom PE mapper and the entry point of DLL will be called with DLL_PROCESS_ATTACH. If it's not a DLL, then it is executed by ShellExecuteW with `open` command.

10) Send collected information to C2

The stream of stolen data is encrypted with Chacha20 using with hard-coded key and nonce. If the victim PC belongs to one of CIS countries, then the data is limited to privilege & integrity level of the current process, Windows version, and victim ID generated with VSN. Otherwise, the data would also contain stolen information like accounts, cookies, browsing history, crypto wallets, and exfiltrated files.

- Key: `TezTfpjNMdcP6FNE` (Same as XTEA key used for config decryption)
- Nonce: `OX8Qe3j7BczD`

The stealer uploads encrypted data to C2 by sending an HTTP POST request to `{resolved_addr}/bgczXibj92HSlSCK/util.php`, with Content-Type set as `application/octet-stream` and Content-Encoding set as `binary`.

11) Execute shell command

Shell command parsed from configuration is executed after the information is uploaded to the C2 server. The only condition determining the execution of the command is the existence of command, which means that the command will be executed even on CIS machines.

12) Cleanup

The stealer destroys the input stream by filling the stream with zeros, which makes it hard to be detected by scanning memory. It also closes the handle for a mutex, frees allocated memory, and calls WSACleanup to terminate Winsock2. Finally, the stealer checks bit 14 of the feature flag and executes the shell command for self-destruction if it is enabled.

Attribution

In November 2020, the Source code of KPOT was sold to REvil ransomware gang. It’s not clear that these updates for KPOT were done by the original authors or REvil operators.

Conclusion

Stealers are becoming more evasive thanks to packers and new technologies like blockchain-based domain names. Not only applying security patches and updates but also awareness of social engineering techniques can help to minimize the risk of becoming a victim of this malware.

Appendix 1. Actionable Items

C2 domains

kpotuvorot10[.]bit
dolboeb1701[.]com

Hashes of unpacked binary

MD5: 989b32b7094ccb9493e6c2ca58696c1a
SHA1: f4d8ab987da7e199b62cac0ffd3d2ccab1634a61
SHA256: b8ceee160c1b674d336fed3027425cbd6228475c1a738d7a41cf176fc42fd1f2
