New Espionage Campaign Targets South East Asia

By About the Author

Archived: 2026-04-05 15:33:17 UTC

An espionage campaign using a previously undocumented toolset has targeted a range of organizations in South East Asia. Among the identified targets are organizations in the defense, healthcare, and information and communications technology (ICT) sectors. The campaign appears to have begun in September 2020 and ran at least until May 2021.

The toolset used by the attackers includes loaders, a modular backdoor, a keylogger, and an exfiltration tool designed to abuse cloud storage service Dropbox.

Attacker toolbox

The initial infection vector employed by the attackers remains unknown. The earliest sign of attempted compromise is a loader that decrypts and loads a payload from a .dat file. At least two different file names have been observed for the .dat file: sdc-integrity.dat and scs-integrity.dat. The loader also calls the DumpAnalyze export from the decrypted payload.

The payload has yet to be identified but is almost certainly a modular backdoor. This can be inferred from one of the modules identified. This "Orchestrator" module points to the existence of a separate DLL module that exposes at least 16 functions, as well as the existence of a custom binary command and control (C&C) protocol used by Orchestrator but implemented separately.

This module appears to be a core component of the backdoor. It runs as a Windows service and a large part of its functionality is implemented in a separate DLL that is loaded from registry (located in HKEY_CLASSES_ROOT\.z\OpenWithProgidsEx\<value_name_resolved_at_runtime>).

The module is expected to export the following functions:

- Construct
- ConnectHost1
- ForceCloseSocket
- Accept
- Recv
- RecvEx
- Send
- SendEx
- BindShell
- TransmitData_htran
- KillChildenProcessTree (sic)
- ExtractIPToConnect

- ExtractIPToConnect1
- GetDeviceInfoString1
- GetPseudoSocketInfo
- Decrypt_ByteToByte

The module loads a configuration either from a file (CSIDL_COMMON_APPDATA\Microsoft\Crypto\RSA\Keys.dat) or from the registry (HKEY_CLASSES_ROOT\.z\OpenWithProgidsEx\CONFIG). The configuration is encrypted. The module uses the function Decrypt_ByteToByte from the separate DLL to decrypt the configuration. The configuration is expected to contain the following options (stored in XML format):

- FLAG
- Ip
- Dns
- CntPort
- LstPort
- Blog
- DropboxBlog
- SvcName
- SvcDisp
- SvcDesc
- SvcDll
- OlPass
- OlTime
- SelfDestroy

The module also uses the hardcoded mutex name, Global\QVomit4.

Other tools used in the campaign include a keylogger, which shows signs of being authored by the same developer, sharing unique strings with other tools and string obfuscation techniques. The attackers also used 7zr, a legitimate tool that is a lightweight version of the 7-Zip archiver, in addition to a data-exfiltration tool that sends stolen data to Dropbox.

Possible false flags

The nature of the targets and the tools used have all the hallmarks of an espionage operation. Symantec has yet to attribute the attacks to a known actor and it appears that the attackers took some steps to complicate attribution. For example, it is not clear what language the group speaks and samples of the backdoor module found contained strings in what appeared to be both Cyrillic and Urdu scripts.

The only potential clue found to date is that one of the organizations attacked was also targeted by a tool used by the China-linked Leafhopper group (aka APT30) during the same time period. However, there is no evidence as yet to tie the tool to this campaign.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise
