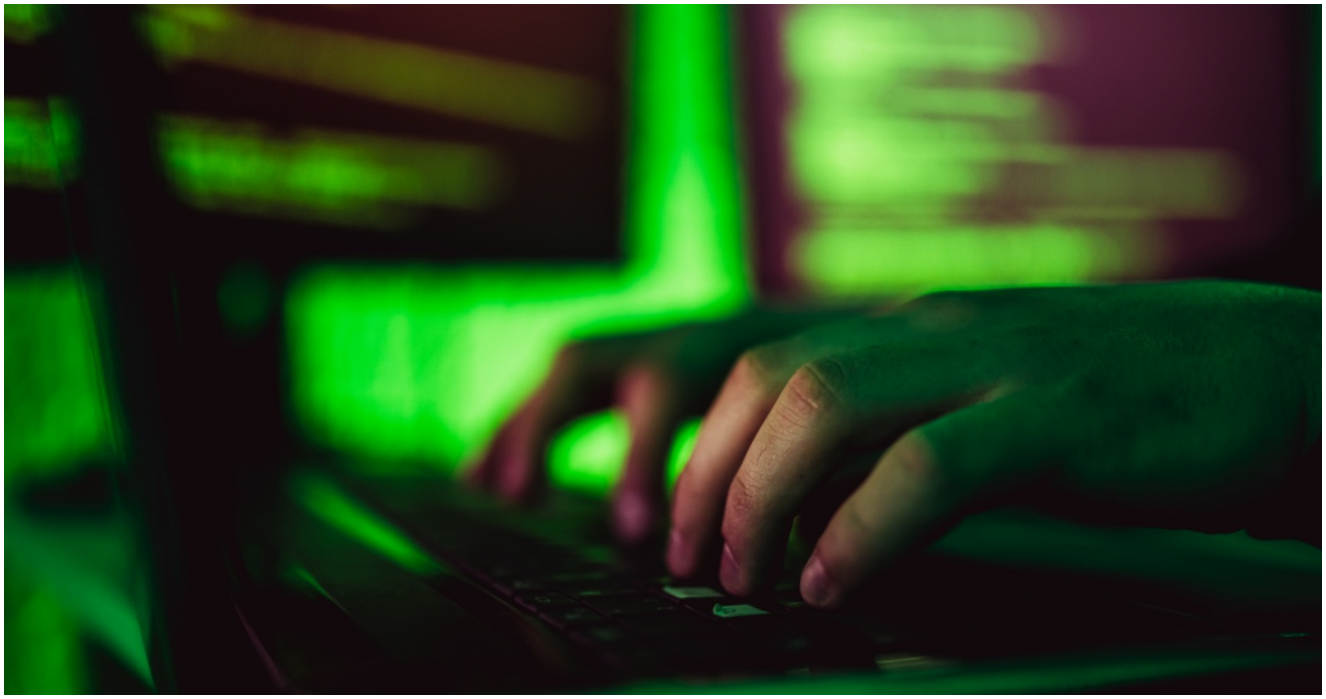
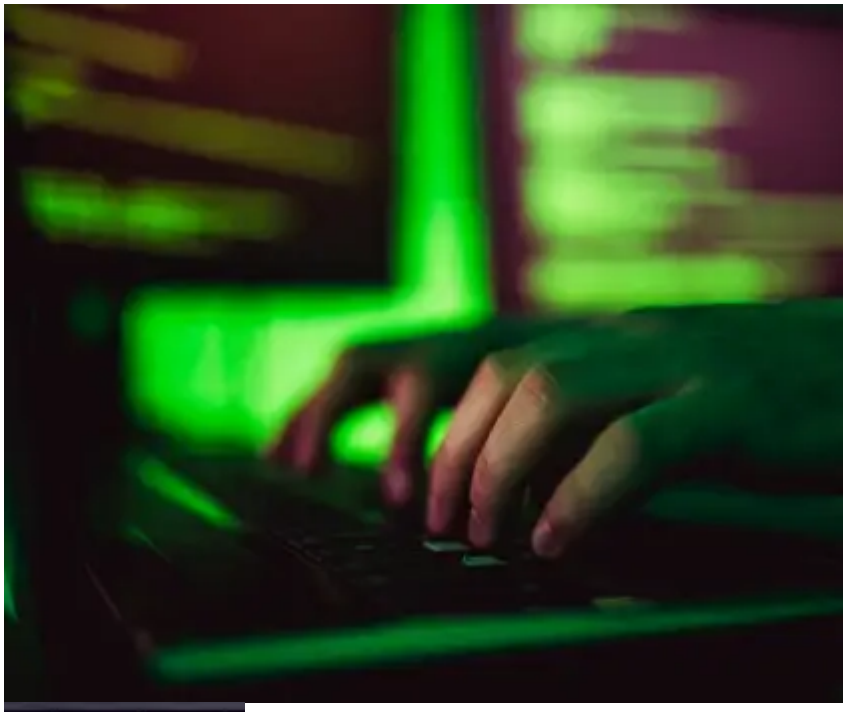
New Espionage Campaign Targets South East Asia

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-campaign-south-east-asia





Threat Hunter TeamSymantec

Unknown attacker using previously undocumented toolset targets defense, healthcare, and ICT sectors.

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

Hash	Description
ac4b50727c69ca7cc3c0a926bb1b75418a8a0eabd369a4f7118bb9bba880e06	Loader
b04be710feba6a070107ff276e1e17e348f534eb9be142271e1ea2fcffa1ef9b	Loader
b25f3e8d1b7fcef6a54fc959d7e82c6a4e2da3836e98766ae4a157484da0b9b1	Loader
1af5252cadbe8cef16b4d73d4c4886ee9cecddd3625e28a59b59773f5a2a9f7f	Orchestrator module
a6f75af45c331a3fac8d2ce010969f4954e8480cbe9f9ea19ce3c51c44d17e98	Orchestrator module
d1ff2ded43e2d9c2e6e07e71f0e3adb815ea0eef7ca391ee272b874807add4a	Orchestrator module
7904ce020b55a6343005db5a5dad7d841db8300fb270c78e8585903e1de13e2	Exfiltration tool
a15eda7c75cf4aa14182c3d44dc492957e9a9569e2d318881e5705da2b882324	Keylogger
967e8063bd9925c2c8dd80d86a6b01deb5af54e44825547a60c48528fb5f896d	Keylogger
64f036f98aad41185163cb328636788a8c6b4e1082ae336dad42b79617e4813d	Keylogger
91b3022e776d1ffb350e550911d08f10d30678bcb4c17d9c0ae5088f5e63146e	Unknown file
c3aee1f79e27af6ddc8ded38bfdfab004ad489c8f81f7928cfea5c05a3605338	Suspected loader
37d0c0afaa77c7363b6515eff9590eba546cce2a751a454d5200a25b7c24dfef	Unknown file

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?