Spyder Loader: Malware Seen in Recent Campaign Targeting Organizations in Hong Kong

Symantec has observed a likely continuation of the Operation CuckooBees activity, this time targeting organizations in Hong Kong.

Operation CuckooBees was first documented in May 2022 by researchers at Cybereason, who said the intelligence-gathering campaign had been operating under the radar since at least 2019, stealing intellectual property and other sensitive data from victims.

The victims observed in the activity seen by Symantec were government organizations, with the attackers remaining active on some networks for more than a year. We saw the Spyder Loader (Trojan.Spyload) malware deployed on victim networks, indicating this activity is likely part of that ongoing campaign. While we did not see the ultimate payload in this campaign, based on the previous activity seen alongside the Spyder Loader malware it seems likely the ultimate goal of this activity was intelligence collection.

Background to Operation CuckooBees

The Spyder Loader malware was first discussed publicly in a March 2021 blog by SonicWall, with the researchers saying at the time that the malware was “being used for targeted attacks on information storage systems, collecting information about corrupted devices, executing mischievous payloads, coordinating script execution, and C&C server communication.”

These initial findings were expanded on substantially in a detailed Cybereason investigation published in May 2022, which detailed a long-running campaign that the researchers dubbed Operation CuckooBees. They said that this campaign had been ongoing since at least 2019. The researchers said that the attackers exfiltrated hundreds of gigabytes of information and that they “targeted intellectual property developed by the victims, including sensitive documents, blueprints, diagrams, formulas, and manufacturing-related proprietary data.” They also stole data that could be leveraged for use in future cyber attacks — such as credentials, customer data, and information about network architecture.

Among the tools used in that campaign was the Spyder Loader malware, which is what was also observed in the activity seen by Symantec researchers.

Spyder Loader - Technical Details

The loader sample analyzed by Symantec researchers is compiled as a 64-bit PE DLL.

It is a modified copy of sqlite3.dll, with the following malicious export added:

- sqlite3_prepare_v4

The sqlite3_prepare_v4 export expects a string as its third argument. Reportedly, whenever an export is executed by rundll32.exe, the third argument of the called export should contain part of the process command-line. When this loader is executed, it extracts the file name from its third argument, and the referred file is expected to contain a sequence of records. Each record has the following structure:

Offset	Size	Description
0	DWORD	blob_id
4	DWORD	blob_size
8	DWORD	blob_cksum
0x0c	blob_size BYTEs	encrypted_blob

At minimum, the malware sample requires records storing blob_ids 1 and 2. The sample also checks for the optional blob_ids 3 and 4. For blob_ids 1 and 2, the content of encrypted_blob is encrypted using the AES algorithm in Ciphertext Feedback (CFB) mode with segment_size of 0x80 bits.

The encryption key is based on the name of an affected computer per GetComputerNameW() API:

```
def generate_aes_key():
    computer_name = [obtained via GetComputerNameW()]
    hash = hashlib.sha256(computer_name.upper())
    digest = hash.digest()
    return digest[: 0x10]
```

And the initialization vector (IV) is derived from the corresponding record header:

```
def generate_aes_IV():
    return struct.pack("<IIII", blob_id, blob_size, blob_cksum, 0)
```

Then the sample creates FileMapping with the following parameters:

- hFile = INVALID_HANDLE_VALUE,
- dwMaximumSizeLow = sum of blob_sizes for blob_ids 2, 3 and 4,
- lpName = "Global\{94803275-9AEA-474E-A8F7-904EDE192BF4}"

Next, it populates the created FileMapping with:

- a copy of record storing blob_id 2, but decrypting the content of field encrypted_blob,
- (if present) copy of record storing blob_id 3, and
- (if present) copy of record storing blob_id 4.

Then it checks the status of service IKEEXT and stops the service, if running.

Next, it drops the decrypted content of blob_id 1 as the following file, before starting the service:

- *[SystemDirectory]\wlbsctrl.dll*

This is apparently intended to execute the created wlbsctrl.dll file. It is likely that this file acts as a next-stage loader that executes the content of blob_id 2 from the created FileMapping. It is possible that the remaining optional blobs could then be used for follow-up stages and/or configuration data. However, as Symantec researchers did not observe these additional content blobs being executed, this is speculative.

As previously mentioned, AES encryption is used where the sample uses the CryptoPP C++ library, but ChaCha20 algorithm encryption is also used to obfuscate one of the strings. The malware also cleans up created artifacts, overwriting the content of the dropped wlbsctrl.dll file before deleting it, for example. These steps are most likely taken in order to prevent the activity being analyzed.

Debug strings also indicated that the source code location of the malware was the following:

- *e:\works\2021\stonev4-legacy\cryptopp_5_6_4\cryptopp\secblock.h*

Similarities between this activity and the Spyder Loader activity described by Cybereason include:

- Use of a modified version of sqlite3.dll
- rundll32.exe command-line example seen in Cybereason's research seems consistent with how the third parameter of malicious export is used in this sample
- Use of the CryptoPP C++ library

These various similarities led us to conclude that this sample was also a version of the Spyder Loader malware. We saw various variants of Spyder Loader on victim networks, all displaying largely the same functionality.

Other Activity on Victim Networks

We saw assorted other malware samples that carried out various other types of activity on victim networks, including a modified SQLite DLL with the malicious export *sqlite3_extension_init,* which creates and starts a service named GeneralManintenanceWork for a file named data.dat. We also saw Mimikatz being executed on victim networks, as well as a Trojanized ZLib DLL that had multiple malicious exports, one of which appeared to be waiting for communication from a command-and-control (C&C) server, while the other would load a payload from the provided file name in the command-line.

Another sample installs and runs the below component of winpcap as a service:

- It accepts either -i or -v as a parameter
- -i installs and runs a service

- -v checks if winpcap is already installed

Files with the names *npf.sys* and *packet.dll* are then installed.

Intelligence Gathering the Likely Goal

While we do not see the final payload delivered in this campaign, the use of the Spyder Loader malware and crossover with the activity previously identified by SonicWall and Cybereason, combined with the victims seen in this recent activity, make it most likely that the motivation behind this activity is intelligence gathering.

The fact that this campaign has been ongoing for several years, with different variants of the Spyder Loader malware deployed in that time, indicates that the actors behind this activity are persistent and focused adversaries, with the ability to carry out stealthy operations on victim networks over a long period of time. Companies that hold valuable intellectual property should ensure that they have taken all reasonable steps to keep their networks protected from this kind of activity.

Protection

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

Indicators of Compromise (IOCs) – Spyder Loader

00634e46b14ba42c12e35a367f1c7a616fb8e8754ebb2e24ae936377a3ee544a

033313b31fbea64a1a0a53b38c74236f7af2e49018faa2be6c036427c456ef6d

06ed28c4ae295dec0bd692cd7fcecb5fa9de644968d281f5e4bf48eb72bc4b63

091e3e806b6d66cf1eccbd57a787eec65df5f07ad88118c576b3ae06c08af744

0cdbde55b23b26efd5c4503473bd673e3e5a75eae375bae866b6541edb8fcc84

181a25cbcd050c1b42839a5d32df4f59055e27377e71eaa3eb9230a43667f075

228784cc7dad998f1f8b7395bf758827eff9b27762a7056d9e8832bb8a029aad

260d54c2fcf725a8b6d030c36ca26f65ba3d01f707fa0e841cac0166d06218c0

2879253c8c8dd3ee53525c81801d813594bb657ad4f7478ba4288112f0315c9e

2da683d54f12d83f0f111b5c57f7f78016cad5860b2604d38b2aba37ab3d5c55

3196e74004816227323d6864448361fb173b3c96cf3d1b0aa26dfcd259a61505

33aa5df5470ae59cd30c7ea4c2ad1e13901a8fd13ea6b4b5584d10ffdba31ee4

396e35b2a4f920182d3148c834cf70f00b6094600e51e030d6fc297cb0ca5c06

3b3df3ada05e521ec8ce2f0deaeb6fd4359a2de9cadb0dd51c0d9d7a835473a4

3d96132412d8587849aa5dfd35c968755b30a08b100ec42eb810ff1f042e9fd0

3e10500c3779e56d2daa05da920d014becf33597f5ccb67c069320c5c43d40d2

4164cfc533621e37c8ad910f29d4afa92d0180c1697b7970746243574029a1f1

417a65be8ef81cb36021dbe56b07bf5dd65b7355e61b7a94bc988aaa335b22da

4221362bba10aedbb2d09729567d090f543c5de8543ec55ca4a6516815202064

438dddd93333ccfce4499558c92b20341166a134a8451ffc60ebf6ec5e0890dc

48658c800b724197cb91cbfd064df060221bc72bd77301707cb30b2f7c2b81fb

4a9cd0c32d6992077d3140917928f1b931bb2bf28e88f0dd8e4c92cd5d9cbe00

4bc3a4e4d74b81acf19621da7c8304527fff954747ab3393b78e0758306b3fa6

4d8784b957d826acc00e5a87d7317bbaeb63c7f9f86a5f446a41a5a355de437e

4dfae8301a9284eea4e975476ceaa652d5d3c799879dec7c5c9e18bbc2930885

54bcd44d4606e0fdb1b7c2110684f429f9e234269d213ddb60c9665e7b8679c7

551794bd7c66fb064d81230161b25ed81a714aa9377f2a9a1af69626dc99d385

5bf03354d708d3c87e82a50d3f4c948fc8c6e8186537b0463edafd9546b51333

5cf6bca323851a509120399a975edc759a9d2c5c21aff18ee6cae506b0f93d67

5deab41977d5d6217b3e35cfab81015d83f270650ccc170dfb948e55e92478dd

5f477c03a689b4aeed28dcb2f8bab3dfa7fc834223062f16eddb5426c2cfa2e6

6741a9ea57e38d1e9d6014bd191b0ac517d2bfa2d79cb091c64fb8011c8521d3

69d927abbacdfcdcad0a1d878e8c0a8543a940a101447b9127365034f7a2d773

6d07ce2ca82489599ae609c6ed18f587059ed5cf2d32a513c5ea6d35861695e9

6d689996a8721f8417de46d645dc6b66b261afdf8ee30b4a0853ff94ec87d3b0

72424e99c1814a1d741508c198eac3e3e84626ce39d961c014718e7f8abb6fe5

7443e17e80dec2db6cfffc0a272fd8a27b2a98a42ffc15fb9065c072dc5904f7

74ff4db3af082d73dcba597cacfd4cae64e00c68169a64be2f3715a0f06535ae

7ccb9cdaff8c6c7785ee1422aa70723c976f62795593b02fbf0923f09c6b647d

7ecd5ec38db31cfb7146ac684eb75912e418c3fbb69a2562478b5fce2ae2c615

8344fcc55534f0b0e08f48f44607771d7cfad130f749ddcc434ffc6fd9012eaa

8535a6e49afa4057e504fa8f4a21a06f535f51bbafff0631c662d7ade5aabfb9

8648bb183abf8aa2111f4d98ecc386e5bcdfa614033efdd124d61ee155261a13

86a45d92282ed3c4f82687eb1d6cfa6a906d6fc5033014bdc6c57da07db1b1b2

892c1f324fa5c2370b06dedf691bd60fa0aa70a4bd6502b9c615cdcd3d5e698a

8a42bee7190e23f76e46e66f9194c33f33a60903a28d267acebf4fd8dead15e8

8a8109f2af10898cdf7259467d18410f2b61a89d5f0d7031b5e45e1bd3b8678a

8eeba9d12cd01b8eb245c76ff16e34eb0455001243fcf1889f28655e55c1d1ed

8fe7cc990ffaf4f156c0868b41e1e92d09c1270e11b96c7320498e0390cc93c6

9138916b9630c81a0b7b6597f4be72ca46c7e3dc1e6fd89d14ddb12f1deb7fdc

95bc468f50483f337d3ef6e1c5d1765beffee4db9c057d6e49713b3a099b2eef

96e22da2b69f599cba297a9aafc971a09c99433bf7f51ec37446c34ed3701d12

9b114bfec2561e76fd8d0c9b31633c2089abec8f3a99c297f0f6416838567452

9b7d8827685b71e92438355872f10c2364d7e3a3811df884eb41e371bcda8f6d

9daa43c1204184634b9833718155404d6c0366fcdd524f945eacfc3e5760c116

a43c9dbfd2a9c1a065eb7a9212f2125ea6e6a73256081bc2deacd50913162a6a

a7f291bde213d9eb4fa60fb3517a6ec6fb7a057457534afe895c1684db0ba21d

b02c10d8a83857352c99f09548397bf8e0ee0548b8e050e138b82eb08b98e938

b13bc2986f098580e2432dac7004a9dca2254c6756dafa3b7f67aff743ee060f

b382824cbb11c60da6c733855c825dcbdf2bbfb8104a517d27af56b56625ba9f

b4703af681c75d2d16c555f008bc4308a4d03767ceed55c02d1a892341444304

b4841104c663f4f013b467220d576035fd2187a92c84451709abff47c8fb162e

b4cdc814f1536264cc5e469cebcbf351ee9d1b9620248bc0a6b14725fe38d5a0

b82a19a06270f37e3b12047a1382796678895fe1c58a9ef799cf5250f6c96dcf

c01f402b942502889aa854326405b29a4d33947547074fbb9eab7c4c4a896d77

c276300d47daff9cc1e486e4ea3d776d82fa9b3f8161eccfe49fc3218afdfbe9

c3d41387bcc9c9f2d9858b1286ed51369a06ed12abe7623344a31a0e0f18f36a

c57236c2e7fe84334d5bdef6420cbf121ab9f918f5d8e4323d7055b12947abb6

c862f2cdbf817f6d7c5568a4af2d8766a30719297e31a71620503e50176fceb2

ccaa5186451c0658b6294f5d8a78b3ec02505164c1ddec2b418259564cd7b23b

cd5a53fc5bb675b47bb4055d8f3e4c45902a8245df2300ccf03d7da6464add78

cdaaf781557e85582dd42ff6a58ecbbb68a7cb2e0dc7c7aa49b1d5df5391330b

d06730e1d07491a70b4b18b52e8f35c92509b5049239e3794a6be73ce160e2c0

d2939897865906fb339e878f620f928bff36c7dead15bb6ed94f7a9df16300e9 d3a163a7313629cc380b9405aafb847247d2a256ae48b60bffd0bfbe3082c19c

d76e32647c3890100fe994a9a0f84a3e6957af08195366e86299e4033c2551f1

dbc60a4878ae9f1a2184c44837db9968a157f2008a16e3a350909a598f918dd9

dc4218b67f99196fb5d71c4bd5ce762e9b8950d8206e198a755650c5e6d17fd0

dc647ce87c62b0ac76530362694d1dafdca5ca414e5abb18c324dfd24f0e9644

deb0e05adad48b90a534beabe2ef4261d2a864112945907fbd2d020b90f24507

e1af76d84f98eb4cd7af04d35030e37ffaa8120a7d048fafe0cbcb2a7f86c460

e3b82ac4870a2ae86dfe88cf7ecf9bc0dc6ed653af0ad1aaa20194cae8aff411

e4f4b3a554c8a0fd693201333e8d634f8ef1fa4ca4445ca556492bb9d0d486c4

ef24840ccde8c7547b3329c7854fdd22d2178c7ad7f931303da2e6eacbf16d1c

f17278d4eaafff971864c02efdc0e4435defad96e7f5203e580a4e32c64681d8

f8ebd94779851fbeca029db4ae938457c7ccf4e010b09f025ea5394b715b1838

f90dc76a9500ee2bb3380d5f4589289ec7ffa647be4262ee7674d37ce02283b7

5d868bfbfc767515c35ced7b0da36f41ed4728914ba081f132a9d9c54564ebf0