CTA Adversary Playbook: Goblin Panda

November 1, 2018

Adversary Playbook: The FortiGuard SE Team is releasing this new playbook on the threat actor group known as Goblin Panda as part of its role in the Cyber Threat Alliance. For more information regarding this series of adversary playbooks being created by CTA members, please visit the Cyber Threat Alliance Playbook Whitepaper.

Active since 2014, Goblin Panda is a threat actor that is focused on interests in Southeast Asia. Goblin Panda has been documented by various organizations, including Fortinet, over the past several years. Due to non-standardized naming conventions within the industry, Goblin Panda is also known as APT 27, Hellsing, Cycledek, and perhaps 1937CN. Goblin Panda is primarily active in South and Southeast Asia, with activity seen primarily in Cambodia, Indonesia, Philippines, Myanmar, Malaysia, Thailand, and Vietnam. India has also been targeted in the past, albeit in limited numbers.

Not much has been documented on this group for various reasons. This is primarily due the fact that its tactics, techniques, and procedures have evolved over the years, and also because rather than engaging in the sort of broad-brush attacks most cybercriminal gangs engage in, their targets and campaigns have been quite specific in nature. We hope that the information contained within our playbook is informative for responders who encounter one of their attacks, or for anyone interested in Goblin Panda.

Overview

Favorite methodologies of Goblin Panda include the use of remote access Trojans, including the infamous PlugX/Korplug, NewCore, and Sisfader RAT tools. Distribution of infected samples are often used by attackers such as Goblin Panda through weaponized Microsoft Office documents containing malicious macros, or by exploiting known vulnerabilities—most recently CVE-2012-0158 and CVE-2017-11882. Even though CVE-2012-0158 is over five years old, attackers are quite aware that many organizations, especially up and coming organizations in developing areas of the world, do not follow a regular patching schedule for various reasons, such as lack of resources or awareness, and therefore remain vulnerable to know exploits for long periods of time.

Methodology

Observed instances of Goblin Panda activity have generally started with a spearphishing attacks via a maliciously crafted Microsoft Office document. When the document is opened by the victim, various files are dropped into different locations of the victim's PC. Dropped files include legitimate software vendor files, an encrypted binary blog containing the payload, and DLL files containing the decryptor and loader for the payload.

During the installation of the malware, a DLL hijacking technique to evade traditional antivirus detections is used whereby a variety of legitimate DLL files from different vendors are hijacked using a Trojanized version of a malicious DLL file. Once the malicious DLL file is side loaded, it then downloads the Trojan downloader, which in turn sets a run key in the registry for persistence. Typically, a legitimate program requires libraries to properly execute. DLL sideloading/hijacking attacks makes the legitimate program think it is loading the correct DLL, when in reality it is loading the malicious DLL instead. Finally, it also checks to determine if it is running in a VM environment.

Once it is finished with those tasks, it then sends various parameters to a C2 server, including:

- OS version
- Processor speed
- Number of processors
- Physical memory size
- Computer name

- User name
- User privilege
- Computer IP address
- Volume serial number

When all of those parameters are deemed ok, it then downloads a payload. In most recent cases, that payload has been the NewCore RAT (Korplug/Plugx and Sisfader were seen in prior campaigns). The NewCore RAT is a malicious DLL file. However, executing the DLL without using the downloader will not work as the C&C server string is not embedded within the DLL file. Based on the strings found in its body, this malware may have been derived from the PcClient and PcCortr backdoors whose source codes are publicly available, especially on Chinese language coding forums.

NewCore RAT has the following attributes:

- Copy files
- Delete files
- Execute files
- Search files
- Download files
- Upload files
- Retrieve disk list
- Retrieve directory list
- Retrieve file information
- Retrieve disk information
- Rename files
- Screen monitoring
- Start command shell
- Shutdown/Reboot

We have also encountered several new NewCore RAT samples that may have been used by the Goblin Panda threat actors. However, due to time constraints we were unable to analyze them further to see if there is an absolute connection to the threat actor group. The following IOCs have been provided for information purposes. Please see the Indictors of Compromise section below for further details, along with our playbook viewer, which contains the tactics and techniques defined by the Mitre ATT&CK knowledge base.

For a detailed technical overview, read our previous blog: *Rehashed RAT Used in APT Campaign Against Vietnamese Organizations*

Indicators of Compromise

All samples (IOCs) have been provided in good faith. These samples had not been analyzed at the time of publication due to time restrictions. As a result, there are no guarantees made about the samples below with respect to Goblin Panda or any attributions to any threat actor.

(NewCoreRat Samples)

9d4ffae7a398a3aef1cef30da784ded0764c50099d3891291f4688aec35fe48

1d8ad2bf967aff93c713a729d5e9447700a236bde1af616bbe6f51e21bdad8c5

3720c608b82dc52f2f6099bd0d6b30701c8689f5ae6e8249f7a04964b2970ec4

59462ce5c9fccf55efade4784d9ef995905260df1c649894c5500702f46ea4f4

8930c8ca404ffbfe969c0d8efd6d2fce352e584a78bf11fb80ed3a0d35c06eeb

8a14b3a3d9da0ea72e40c48ac6fd29bf1c3427917d8ceeb0b81ff7aa1924f68b

a8efd9835cdd2cff2cdca61039f4d62990d4109f794e25d84250a0738d5f25de

af1d44b272cb2650f525879e772817f5bb4bf823c36a6e1f5c842f2fcc749930

af5301411e507dc142e671fc9a42f2fe32959add3a81fce2742dbf90536eebbd

cb5e090a867e76214897efcb55a7d8908a36e874229c508ad97c0ebc437d79d8

de42dcc2f9094efbd37d65821992865eab1ef9b66e83c76f3fc8c1a800b54350

f910c0b18b5af4359e7354475add9f622aa92f945739a1c3b3bfc3704a037561

fce7a763c05711bc0ba110ed23651c0f18aceddae5ada6e8042a2664a35d18ec

e5a170755ab090e944d1d24faef67ae1f80bac847f2a501937c9f03b888615c8

a270058cef51b49905d7ceb3df7b8b5bb7b60ebfb5099d8b177dc19a2064145c c9fb110ec68fd7fde1b72c5d92be5f6f03559d11a5d863e2179ebecc8fce2aee

5cef63d737153624211a6c408ef6b9ae008837f54f0ba44cbaefa57d8fde34f8

c8f19e0f7bbb63919df67f93d3c334e9564bf3aea910951d9ba644ae30783439

79ede3b7133d9edef0c14a6c8914113f7cfe2e45f76d216efbf1fc731f46e561

32946f137deb4d2abb7c71c021984e0d5364b6ee80560e09de133d8c11a5cf72

c299841e17b621db7a386c24f426a0a74912758b19ecfc368fabc8fb4742ab9c

c1b9d0639d416232995d5eef2515c9d9be0f694e67b1136d7c5d37ca2af2dacd

471c075d5e3c9cb009fa6ef1f8ec9c0ecf61251b4dab6eea161abec6935272bf

5e488198c47befc49a08fec6f19c3c7d8e0e955589465d4e83ba87b46b3d80df

22b0f774379c0e28211ffb53722d8cd5727da8e02aada3507be81d888864770f

b88cd263828b9856c1cee7eeecdd6da22eb9c892cbbd38c5bdab284f2a007582

79ede3b7133d9edef0c14a6c8914113f7cfe2e45f76d216efbf1fc731f46e561

8023c060d49479466b6595c72f07d89a6e598b8bde6805cdffcc52d1169d0304

e7def95e889704343557431aa30914faafeb5318bb2f0f6e7a00c6b319a5edd7

c9b96665e6962ccb47fb9963c3db6b0d9aebaedf717c42ac6ba321d7981dd69e

78ce3dcbe9b828b9be0c1a74757eb8f32052db171cde2f2e2fe897a8096f1140

8485d9ecfa94f3cd316057c97e13629973b7e110bdee288087f98338b67d8b48

dacb62e6a86a4ecd4f8f5e1685de018258b36372bad5d58bc9745725e2d04f8f

195ffc2123b3e601f36698584c032c6e429d4d20ea9bcc66ee7f8e4918c9106e

1185b1b983908f39d6885329e83f6349683716f9d056f56a22a86d8014cf0aac

471a980082a9fd1dfc66d068a4658df3b8e9552edac55e14622bd59e3093fd8d

d28ce94db53318bf951adf3a60af74ca6924291274f5474ae7bd77cbbeef581a

2b73a808c9a9b12f807c2282e30858acdcb6251e040c97c37037e78af1e99b3b

bceaf0be831e0a633ec204c70800a6827e0a9871167e812a6331b09c70c81a12

db4085acc3de63994186425d11c354879527ddd448a9f2cf5f830855d2c8257b df46fe83dab8fc1c4cfcff9b75d3ebf3b7390db6ebff09b74cb3c485300e8a78

79b57b487ea7e5dc6276a9028584a7fcc015a547c1ec221f10314ecec8a384fc

1cb80eed2cd06aa0a419f808e05efc29e5c63c3c6134b2f4d8b36fd2aeb49887

14daa0e0db8759568e5d49986d12ae8a1289efd308bdd41634448be543dd7c76

6b7dbf0a03b0e41a327bd7de2e26645a220465d7be68e8c3c70b8a1da534adcf

9fa5cc69aaa023a54ee7497b0f04b8d90960b276427d870b1782fb524d20c535

ca0e90a60c21bff48c02a17f73023c8813f5ddf0c9231878c6ade4c8e6ad8a1c

a65e0ef3d70bd891f0d077972fb86652bbb4132b276504cdd1b75882523bcf30

e5a31524fc95da517342bd1accc783e088fed42db33cb9caf7b60a39918ebdc2

a65e0ef3d70bd891f0d077972fb86652bbb4132b276504cdd1b75882523bcf30

281f3ce73e434f7616ce1600e0d6cab335ecdff2778dac0f916cc0e65224a753

b93b7ad0e27d95665b699c3f6cf49129cff410555defd2c56cd3ec8a112bf1c9

Read and learn more about the Cyber Threat Alliance (CTA).

Sign up for our weekly FortiGuard Threat Brief.

Know your vulnerabilities – get the facts about your network security. A Fortinet Cyber Threat Assessment can help you better understand: Security and Threat Prevention, User Productivity, and Network Utilization and Performance.