Unveiling activities of Tropic Trooper 2023: deep analysis of Xiangoop Loader and EntryShell payload

Thursday 5 October 16:30 - 17:00, Red room

Suguru Ishimaru (ITOCHU Cyber & Intelligence), **Hajime Yanagishita** (MACNICA) & **Yusuke Niwa** (ITOCHU Cyber & Intelligence)

The Tropic Trooper (also known as KeyBoy and Pirate Panda) [1] is an infamous APT actor that has been highly active since 2011, according to Trend Micro [2]. This group has previously targeted various sectors, including government, healthcare, transportation and high-tech industries in Taiwan, the Philippines, and Hong Kong.

Interestingly, our investigation has revealed that in 2023, they conducted persistent campaigns targeting the offices of specific industries in China for over two months. Through our extensive long-term investigation, we discovered new malware and tactics, techniques, and procedures (TTPs).

In November 2022, we observed this actor focusing on targeting overseas branch offices of manufacturing industries, particularly in China. The initial infection method involved SMS, and the malware was a variant of the KeyBoy malware, which we named 'EntryShell malware'. In May 2023, a local office in China was attacked with EntryShell and a Cobalt Strike beacon delivered via spear-phishing emails.

Additionally, we encountered an intriguing mystery initial infection that suggests the actor may have exploited a local branch's Wi-Fi access point in an undisclosed manner in July 2023.

Throughout our investigation, we collected and analysed nearly 200 samples, including loader modules, payloads, second-stage malware, and post-exploitation tools related to this campaign. The group primarily utilizes a legitimate McAfee executable file and a malicious DLL file, 'McVsoCfg.dll', employing side-loading techniques to infect fileless malware like EntryShell and the Cobalt Strike beacon.

We have named the malicious DLL file 'Xiangoop Loader', which contains two malicious functions: an installer and a loader. Furthermore, it utilized a simple, yet effective and unconventional obfuscation technique involving an extensive amount of junk code. The astonishing aspect lies in the quantity; for example, the data size of the function responsible for initializing AES SBOX in this sample amounts to 586,784 bytes, including noise,

equivalent to 218,309 lines. When attempting to open this function in IDA Pro, a tool favoured by reverse engineers, the program flow exceeds 20,000 nodes, making it challenging to analyse easily.

In the second-stage sample that follows, additional obfuscation with Control Flow Flattening (CFF) [3] was applied, rendering it unreadable for humans. Furthermore, we have discovered a new approach to DLL side loading, involving the implementation of separate Export functions in individual DLLs for specific loader functions. These functions are then loaded from the main malicious DLL file. This technique aims to evade security products and obstruct research. Even if some DLLs are acquired for analysis, malware analysts must fully analyse all DLL files, making investigation and analysis challenging.
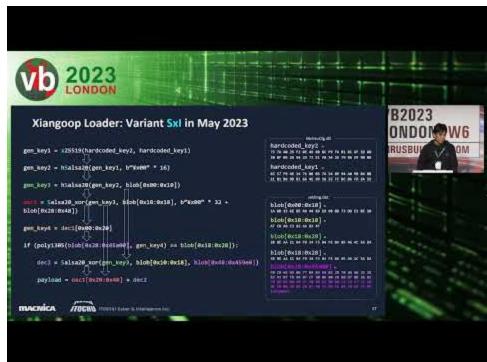
We are particularly interested in the implemented cryptographic algorithms, such as X25519 (Elliptic Curve Cryptography) for key generation, Salsa20 for key generation and payload decryption, and Poly-1305 for check digits for successful decryption.

Regarding payloads, we have named the fileless malware 'EntryShell', a variant of the KeyBoy malware, due to similarities in backdoor command IDs and debug messages with old KeyBoy samples. The embedded malware config was encrypted with a unique algorithm, which is also intriguing.

Furthermore, our DFIR results from a compromised host revealed a different type of malware as the third-stage malware, which is a variant of SparrowDoor, and we have named it 'Crowdoor' malware. We will also provide details about indicators of compromise (IoCs), malware samples, logs, commands, and post-exploitation tools in this presentation.

In summary, based on our two-month investigation of Tropic Trooper, we will present a detailed analysis of the malware, highlight differences from previous operations as new TTPs, and delve into the tools and commands used in the lateral movement stage.

[1] https://attack.mitre.org/groups/G0081/

[2] https://www.macnica.co.jp/business/security/security-reports/143962/ (in Japanese)

[3] https://github.com/obfuscator-llvm/obfuscator/wiki/Control-Flow-Flattening

Watch Video At:

https://youtu.be/s6vYp7YsWBs

Download slides for this talk

Suguru Ishimaru

In 2023, Suguru entered ITOCHU Cyber & Intelligence (ICI) as a senior cybersecurity researcher to analyse malware, to research Advanced Persistent Threats (APTs), to review security solutions and to handle incident response. Before moving to ICI, he worked for around 15 years as a senior researcher at Global Research and Analysis Team (GReAT) in Kaspersky. Based on his investigations, he posted technical blogs in securelist.com and given presentations at security conferences including AVTokyo, HITCON pacific, JSAC, FIRST TC Bali, Internet Week, HITCON community, Botconf, Objective by the sea and GReAT Ideas Green Tea Edition.

Hajime Yanagishita

Hajime is a security researcher at MACNICA. His major areas of research include APT campaign tracking and malware analysis for fighting cyber threats to protect users. Some of his work has been presented at several security conferences such as JSAC2018, JSAC2021, JSAC2022, HITCON Pacific 2018 and CONFidence 2020.

Yusuke Niwa

Yusuke is a senior security researcher at ITOCHU Cyber & Intelligence (ICI), protecting the cybersecurity of ITOCHU and its group companies as a member of ITOCHU CSIRT(ITCCERT). He also specializes in researching and analysing emerging threat trends such as email spam, APT attacks and cybercrime. Prior to joining ITCCERT, he worked as a security analyst for Symantec in threat monitoring for the APAC region. He has had the opportunity to present at JSAC2020, JSAC2021, JSAC2022 and GReAT Ideas Green Tea Edition (2021) conferences and is a contributor to MITRE ATT&CK v9. CISSP, GCFA, GCFR, GREM, GCIH and GCIA.

Other VB2023 papers