Timeline Overview.

From December 10, 2020 to December 7, 2022, 2 tools, 3 identities, 2 malwares, 1 indicators, 4 intrusion sets, 3 locations, 1 campaigns and 2 attack patterns had been published.

December, 2020.

In December, 2020, 2 tools and 2 malwares had been publicly released.

Termite

Termite has been published on December 10, 2020. Its description is

> Termite can act as a SOCKS proxy to bounce traffic, as well as a lightweight backdoor that can upload and download files, and execute shell commands, and is available for a range of different operating systems and architectures including x86 ARM, PowerPC, Motorola, SPARC and Renesas.

Vcrodat.

Vcrodat has been publicly released on December 10, 2020. The malware's description is

> (Symantec) In some attacks, Whitefly has used a second piece of custom malware, Trojan.{{Nibatad}}. Like Vcrodat, Nibatad is also a loader that leverages search order hijacking, and downloads an encrypted payload to the infected computer. And similar to Vcrodat, the Nibatad payload is designed to facilitate information theft from an infected computer.

Its kill chain phase is not provided.

ShimRAT.

ShimRAT has been published on December 10, 2020. The malware's description is

> (Fox-IT) ShimRat is a custom developed piece of malware known as a ‘RAT’, Remote Administration Tool. It has among others standard capabilities for filesystem interaction. The malware was originally built in 2012 and its features were expanded over the years. The artifacts left in the first samples, are a good indicator that the project has been started in 2012. Multiple pdB paths were seen in the early versions of ShimRat. These PDB paths are not visible in the latest

> versions of ShimRat, due to how the samples are prepared. The PDB paths are either stripped or filled with different paths.

The malware's kill chain phase is not provided.

S0002 - Mimikatz

S0002 - Mimikatz has been published on December 10, 2020. Its description is

> [Mimikatz] is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.

October, 2021.

In October, 2021, 3 identities had been published.

[Unknown Media].

[Unknown Media] has been published on October 20, 2021. Its identity class is not provided. Its sector is media. The identity's description is not provided.

[Unknown Defense].

[Unknown Defense] has been released on October 20, 2021. Its identity class is not provided. The identity's sector is defense. Its description is not provided.

[Unknown Telecommunications].

[Unknown Telecommunications] has been released on October 20, 2021. Its identity class is not provided. The identity's sector is telecommunications. Its description is not provided.

February, 2022.

In February, 2022, 1 location had been publicly released.

Singapore

The location has been publicly released on February 28, 2022. Its description is not provided.

March, 2022.

In March, 2022, 2 locations had been published.

South Korea

South Korea has been publicly released on March 1, 2022. The location's description is not provided.

Myanmar

Myanmar has been publicly released on March 1, 2022. Its description is not provided.

June, 2022.

In June, 2022, 1 indicator had been publicly released.

"MAC address: 00-08-74-4C-7F-1D".

It has been released on June 17, 2022. The indicator's indicator type is not provided. The indicator's description is not provided.

Its pattern type is not provided. Its pattern is not provided.

The indicator's "valid from" time is not provided. Its "valid until" time is not provided.

The indicator's kill chain phase is not provided.

August, 2022.

In August, 2022, 1 campaign had been published.

Operation Wocao.

Its alias is not provided. Its objective is not provided. Its description is

> [Operation Wocao] was a cyber espionage campaign that targeted organizations around the world, including in Brazil, China, France, Germany, Italy, Mexico, Portugal, Spain, the United Kingdom, and the United States. The suspected China-based actors compromised government organizations and managed service providers, as well as aviation, construction, energy, finance, health care, insurance, offshore engineering, software development, and transportation companies. Security researchers assessed the [Operation Wocao] actors used similar TTPs and tools as APT20, suggesting a possible overlap. [Operation Wocao] was named after an observed command line entry by one of the threat actors, possibly out of frustration from losing webshell access.

First events associated with the campaign have been observed on December 1, 2017. It has been last seen on December 1, 2019.

October, 2022.

In October, 2022, 4 intrusion sets had been published.

Whitefly

Whitefly has been released on October 10, 2022. The set is also known as "Whitefly". The intrusion set's description is

> [Whitefly] is a cyber espionage group that has been operating since at least 2017. The group has targeted organizations based mostly in Singapore across a wide variety of sectors, and is primarily interested in stealing large amounts of sensitive information. The group has been linked to an attack against Singapore’s largest public health organization, SingHealth.

The set has been first observed on May 26, 2020. The intrusion set's last activity dates back to October 12, 2021. Its resource level estimation is not provided.

APT28

APT28 has been publicly released on October 10, 2022. The intrusion set is also known as "APT28", "IRON TWILIGHT", "SNAKEMACKEREL", "Swallowtail", "Group 74", "Sednit", "Sofacy", "Pawn Storm", "Fancy Bear", "STRONTIUM", "Tsar Team" and "Threat Group-4127". The set's description is

> esempio di notifica

First events related to the set date back to May 31, 2017. The intrusion set's last events date back to March 16, 2022. Its resource level estimation is not provided.

Turla

Turla has been publicly released on October 10, 2022. It is also known as "Turla", "IRON HUNTER", "Group 88", "Belugasturgeon", "Waterbug", "WhiteBear", "VENOMOUS BEAR", "Snake", "Krypton" and "Venomous Bear". The intrusion set's description is

> [Turla] is a Russian-based threat group that has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies since 2004. Heightened activity was seen in mid-2015. [Turla] is known for conducting watering hole and spearphishing campaigns and leveraging in-house tools and

> malware. [Turla]’s espionage platform is mainly used against Windows machines, but has also been seen used against macOS and Linux machines.

The set has been first observed on May 31, 2017. Last activity associated with the intrusion set dates back to March 9, 2022. Its resource level estimation is not provided.

APT1

APT1 has been publicly released on October 10, 2022. The intrusion set is also known as "APT1", "Comment Crew", "Comment Group", "Comment Panda", "Kumming Group (Dell SecureWorks)", "Comment Panda (CrowdStrike)", "Comment Crew (ThreatConnect)" and "Comment Crew (Internet)". The set's description is

> The intrusion-set's description is: [APT1] is a Chinese threat group that has been attributed to the 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.

First activity related to the intrusion set dates back to May 31, 2017. Last activity related to it dates back to May 26, 2021. The set's resource level estimation is not provided.

December, 2022.

In December, 2022, 2 attack patterns had been publicly released.

T1098 - Account Manipulation

T1098 - Account Manipulation name is "T1098 - Account Manipulation". The attack pattern's description is

> Adversaries may manipulate accounts to maintain access to victim systems. Account manipulation may consist of any action that preserves adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain. However, account manipulation may also lead to privilege escalation where modifications grant access to additional roles, permissions, or higher-privileged [Valid Accounts].

T1204.002 - Malicious File

T1204.002 - Malicious File name is "T1204.002 - Malicious File". The attack pattern's description is

> An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment]. Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading] and [Obfuscated Files or Information] to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it. While [Malicious File] frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing].