Timeline of the graph

From 10 December 2020 to 7 December 2022: 2 malwares, 1 indicator, 2 attack-patterns, 1 campaign, 3 identities, 1 infrastructure, 2 tools, 3 locations and 4 intrusion-sets had been published.

On 10 December 2020, 2 malwares and 2 tools had been published.

tool: S0002 - Mimikatz
The tool's 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. .

malware: ShimRAT
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..

tool: Termite
The tool's 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..

malware: Vcrodat
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.

While Vcrodat is delivered via the malicious dropper, we have yet to discover how Nibatad is delivered to the infected computer. Why Whitefly uses these two different loaders in some of its attacks remains unknown. And while we have found both Vcrodat and Nibatad inside individual victim organizations, we have not found any evidence of them being used simultaneously on a single computer..

On 20 October 2021, 3 identities had been published.

identity: [Unknown Media]

identity: [Unknown Defense]

identity: [Unknown Telecommunications]

On 28 February 2022, 1 location had been published.

location: Singapore
The location's associated country is SG.

On 1 March 2022, 2 locations had been published.

location: South Korea
The location's associated country is KR.

location: Myanmar
The location's associated country is MM.

On 17 June 2022, 1 indicator had been published.

mac-addr: 00-08-74-4C-7F-1D

On 10 October 2022, 4 intrusion-sets had been published.

intrusion-set: Whitefly
The set's aliases are Whitefly. The primary motivation of the group is information theft and espionage. The group was observed for the first time on 26 May 2020 and for the last time on 12 October 2021. 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..

intrusion-set: Turla
The set's aliases are Turla, IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, VENOMOUS BEAR, Snake, Krypton and Venomous Bear. The group was observed for the

first time on 31 May 2017 and for the last time on 9 March 2022. 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..

intrusion-set: APT28
The set's aliases are APT28, IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127 and TG-4127. The primary motivation of the group is information theft and espionage. The group was observed for the first time on 31 May 2017 and for the last time on 16 March 2022. The intrusion-set's description is: esempio di modifica.

intrusion-set: APT1
The set's aliases are APT1, Comment Crew, Comment Group, Comment Panda, Kumming Group (Dell SecureWorks), Comment Panda (CrowdStrike), Comment Crew (ThreatConnect) and Comment Crew (Internet). The primary motivation of the group is information theft and espionage. The group was observed for the first time on 31 May 2017 and for the last time on 26 May 2021. 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. .

On 4 November 2022, 1 campaign had been published.

campaign: Operation Wocao
The campaign's aliases are Operation Wocao. 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 activity related to the campaign dates back to 1 December 2017, last campaign's activities were seen on 1 December 2019.

On 7 December 2022, 2 attack-patterns and 1 infrastructure had been published.

attack-pattern: 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]..

attack-pattern: 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]..

infrastructure: INFR_MF
The infrastructure's description is: test ma com'è che funziona "prova" con @ e ?!.