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
This tool, known as Mimikatz, is designed to extract plaintext Windows account logins and passwords, as well as offering a range of other features that make it an excellent resource for testing network security.

malware: ShimRAT
ShimRat, a custom-built Remote Administration Tool (RAT) malware, was created by Fox-IT and first detected in 2012. Over the years, its capabilities have been expanded, including standard functionalities for file system interaction. The presence of multiple PDB paths in the early versions of ShimRat suggests that the project was initiated in 2012. However, in the latest versions of ShimRat, these paths are either removed or replaced with different paths during sample preparation, making them invisible.

tool: Termite
Termite is a versatile tool that can serve as a SOCKS proxy to redirect traffic, as well as a lightweight backdoor that enables file uploads and downloads, shell command execution, and more. It is compatible with a variety of operating systems and architectures, including x86, ARM, PowerPC, Motorola, SPARC, and Renesas.

malware: Vcrodat
In certain attacks, Whitefly has been observed using a second custom malware, known as Trojan.Nibatad, in addition to Vcrodat. Similar to Vcrodat, Nibatad is a loader that exploits search order hijacking to download an encrypted payload onto the compromised computer, with the goal of stealing information. Although Vcrodat is typically delivered through a malicious dropper, the delivery method for Nibatad remains unknown. The reason why Whitefly uses these two different loaders in some of their attacks remains unclear. While we have discovered both Vcrodat and Nibatad within individual victim organizations, there is no evidence to suggest that they were 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
Whitefly is an intrusion group, also known as Whitefly, whose main objective is to steal sensitive information through espionage. It was first observed on May 26, 2020, and its most recent activity was detected on October 12, 2021. This cyber espionage group has been in operation since 2017, targeting various organizations in Singapore from different sectors. Their primary focus is to obtain a significant amount of confidential data. Whitefly has been connected to an attack against SingHealth, Singapore's largest public health organization.

intrusion-set: Turla
The group, also known as Turla, IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, VENOMOUS BEAR, Snake, Krypton, and Venomous Bear, was first observed on May 31, 2017, and most recently on March 9, 2022. Since 2004, Turla, a Russian-based threat group, has targeted victims across 45 countries, including those in government, military, education, research, and pharmaceutical industries. Despite a peak in activity in mid-2015, Turla continues to conduct watering hole and spearphishing campaigns, using a

variety of in-house tools and malware. While their espionage platform is primarily used against Windows machines, instances of attacks on macOS and Linux machines have also been observed.

intrusion-set: APT28
This group, also known as APT28, IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, and TG-4127, has been primarily motivated by information theft and espionage. First observed on May 31, 2017, and most recently on March 16, 2022.

intrusion-set: APT1
This group, also known as APT1, Comment Crew, Comment Group, Comment Panda, Kumming Group (Dell SecureWorks), Comment Panda (CrowdStrike), Comment Crew (ThreatConnect), and Comment Crew (Internet), has primarily been motivated by information theft and espionage. First observed on May 31, 2017, and most recently on May 26, 2021, the group has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known as Unit 61398.

On 4 November 2022, 1 campaign had been published.

campaign: Operation Wocao

This cyber espionage campaign, known as Operation Wocao, targeted organizations worldwide, including those in Brazil, China, France, Germany, Italy, Mexico, Portugal, Spain, the United Kingdom, and the United States. Suspected China-based actors compromised government organizations, managed service providers, and companies in a range of industries, including aviation, construction, energy, finance, health care, insurance, offshore engineering, software development, and transportation. Researchers discovered that the actors behind Operation Wocao utilized similar tactics, techniques, and tools as those of APT20, suggesting a possible overlap. The campaign was named after a command line entry observed by one of the threat actors, possibly out of frustration from losing webshell access. The first activity related to the campaign dates back to December 1, 2017, with the last known activity seen on December 1, 2019.ion Wocao

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

attack-pattern: T1204.002 - Malicious File
Malicious File (T1204.002) is a technique used by adversaries to gain execution by relying on users to open a file that leads to code execution. This behavior is often the result of social engineering tactics like spearphishing, and adversaries may use various file types that require user interaction to execute, such as .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. To increase the likelihood of success, adversaries may use masquerading and obfuscation techniques, such as familiar naming conventions or password-protected files, and may

provide instructions on how to open the file. While malicious file execution often occurs shortly after initial access, it can also occur at other phases of an intrusion. For example, adversaries may place a file in a shared directory or on a user's desktop, hoping that the user will click on it. This activity may also be seen shortly after internal spearphishing attempts.

attack-pattern: T1098 - Account Manipulation
Account Manipulation (T1098) is a technique used by adversaries to maintain access to victim systems by manipulating accounts. This may involve modifying credentials or permission groups to preserve adversary access to a compromised account. Adversaries may also perform account activity designed to subvert security policies, such as iterative password updates to bypass password duration policies and preserve the life of compromised credentials. 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 ?!.