Overview of Whitefly intrusion set.

The set has been publicly released on October 10, 2022. The intrusion set's alias is "Whitefly". The 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 intrusion set has been first observed on May 26, 2020. It has been last seen on October 12, 2021. The intrusion set's resource level estimation is not provided.

Motivation.

Its primary motivation is information theft and espionage. The set's secondary motivation is not provided. Its goal is not provided.

Associated campaigns.

No entities found.

Associated victims.

[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.

Associated MITRE ATT&CK TTPs.

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].

Overview of S0002 - Mimikatz.

The tool 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.