Report on Whitefly

Overview

Whitefly is an intrusion-set, which operates also under the name of Whitefly. The primary motivation of the group is information theft and espionage, followed by information theft and espionage. The set was observed for the first time on 26 May 2020 and for the last time on 12 October 2021. The description of Whitefly 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.

Stats

The group is related to these malwares:
- 2 loaders (Vcrodat and Nibatad)
- 2 downloaders (Vcrodat and Nibatad)
- 1 backdoor (ShimRAT)
- 1 info stealer (ShimRAT)
- 1 exfiltration (ShimRAT)

The group is related to these tools:
- 1 tunneling (Termite)
- 1 exfiltration (Termite)
- 1 backdoor (Termite)
- 1 downloader (Termite)
- 1 credential stealer (Mimikatz)
- 1 keylogger (Mimikatz)

It is related to these attack-patterns:
- 1 command-and-control (T1105 - Ingress Tool Transfer)
- 1 credential-access (T1003.001 - LSASS Memory)
- 1 resource-development (T1588.002 - Tool)
- 1 privilege-escalation (T1068 - Exploitation for Privilege Escalation and T1574.001 - DLL Search Order Hijacking)
- 2 executions (T1059 - Command and Scripting Interpreter and T1204.002 - Malicious File)
- 3 defense-evasions (T1027 - Obfuscated Files or Information, T1036.005 - Match Legitimate Name or Location and T1574.001 - DLL Search Order Hijacking)

Relationships

Whitefly

The group targets these identities [Unknown Media], [Unknown Defense] and [Unknown Telecommunications] and these locations Myanmar, Singapore and South Korea. The group uses these malwares ShimRAT and Vcrodat and these tools S0002 - Mimikatz and Termite. The group uses this attack-pattern T1204.002 - Malicious File.

S0002 - Mimikatz

The tool is hosted by this infrastructure INFR_MF. The tool is used by this campaign Operation Wocao and these intrusion-sets Turla, APT1 and APT28.

Mitre Matrix

Source	Name	Tactic	ATT&CK Code	Description
Whitefly	T1204.002 - Malicious File	execution		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](https://attack.mitre.org/techniques/T1566/001). 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](https://att

				ack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) 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.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) 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](https://attack.mitre.org/techniques/T1534).
S0002 - Mimikatz	T1098 - Account Manipulation	persistence		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](https://attack.mitre.org/techniques/T1078).

IOCs

Source	Type	Value
Whitefly	mac-addr	00-08-74-4C-7F-1D

Useful Resources

Useful material to know better the set can be found at: https://attack.mitre.org/groups/G0107 and https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/whitefly-espionage-singapore.