Report on Whitefly

Overview

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.

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

Whitefly has set its sights on various identities, including those belonging to unknown media, defense and telecommunications entities, in addition to locations such as Myanmar, South Korea and Singapore. In order to carry out these attacks, the group employs malwares such as ShimRAT and Vcrodat, as well as tools like S0002 - Mimikatz and Termite. The attack pattern used by Whitefly is identified as T1204.002 - Malicious File.

S0002 - Mimikatz

The tool operates within the INFR_MF infrastructure and serves the needs of the Operation Wocao campaign, as well as the intrusion-sets Turla, APT1 and APT28.

Mitre Matrix

Source	Name	Tactic	ATT&CK Code	Description
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 and permissions.

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.