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 group was observed for the first time on 26 May 2020 and for the last time on 12 October 2021. The description of the set 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.

Relationships

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

Stats

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

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

The set 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 (T1204.002 - Malicious File and T1059 - Command and Scripting Interpreter)
- 3 defense-evasions (T1027 - Obfuscated Files or Information, T1574.001 - DLL Search Order Hijacking and T1036.005 - Match Legitimate Name or Location)

Mitre Matrix

Name	Tactic	ATT&CK Code	Description
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://attack.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).

IOCs

Type	Value
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.

Report on S0002 - Mimikatz

Overview

S0002 - mimikatz is a tool. The description of S0002 - Mimikatz 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.

Relationships

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

Stats

The tool is related to these attack-patterns:
- 1 defense-evasion (T1207 - Rogue Domain Controller, T1550.003 - Pass the Ticket, T1550.002 - Pass the Hash and T1134.005 - SID-History Injection)
- 1 persistence (T1547.005 - Security Support Provider and T1098 - Account Manipulation)
- 2 lateral-movements (T1550.003 - Pass the Ticket and T1550.002 - Pass the Hash)
- 2 privilege-escalations (T1134.005 - SID-History Injection and T1547.005 - Security Support Provider)
- 11 credential-accesses (T1649 - Steal or Forge Authentication Certificates, T1555 - Credentials from Password Stores, T1552.004 - Private Keys, T1555.003 - Credentials from Web Browsers, T1558.002 - Silver Ticket, T1555.004 - Windows Credential Manager, T1003.001 - LSASS Memory, T1558.001 - Golden Ticket, T1003.002 - Security Account Manager, T1003.006 - DCSync and T1003.004 - LSA Secrets)

Mitre Matrix

Name	Tactic	ATT&CK Code	Description
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).

Useful Resources

Useful material to know better the tool can be found at: https://attack.mitre.org/software/S0002, https://github.com/gentilkiwi/mimikatz and https://adsecurity.org/?page_id=1821.