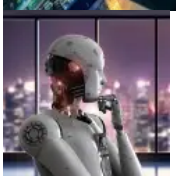
Whitefly: Espionage Group has Singapore in Its Sights

symantec.com/blogs/threat-intelligence/whitefly-espionage-singapore



Threat Hunter TeamSymantec

Group behind the SingHealth breach is also responsible for a string of other attacks in the region.

In July 2018, an attack on Singapore's largest public health organization, SingHealth, resulted in a reported 1.5 million patient records being stolen. Until now, nothing was known about who was responsible for this attack. Symantec researchers have discovered that this attack group, which we call Whitefly, has been operating since at least 2017, has targeted organizations based mostly in Singapore across a wide variety of sectors, and is primarily interested in stealing large amounts of sensitive information.

Whitefly compromises its victims using custom malware alongside open-source hacking tools and living off the land tactics, such as malicious PowerShell scripts.

"#Whitefly, the group behind the SingHealth breach, is also responsible for a string of other attacks in Singapore https://symc.ly/2X1RALf" Click to Tweet

Whitefly's targets

From mid-2017 to mid-2018, Whitefly launched targeted attacks against multiple organizations. While most of these organizations were based in Singapore, some were multinational organizations with a presence in Singapore.

To date, Whitefly has attacked organizations in the healthcare, media, telecommunications, and engineering sectors.

How Whitefly compromises its victims

Whitefly first infects its victims using a dropper in the form of a malicious .exe or .dll file that is disguised as a document or image. These files frequently purport to offer information on job openings or appear to be documents sent from another organization operating in the same industry as the victim. Given the nature of disguise, it's highly likely that they are sent to the victim using spear-phishing emails.

If opened, the dropper runs a loader known as Trojan.Vcrodat on the computer. Whitefly has consistently used a technique known as search order hijacking to run Vcrodat. This technique takes advantage of the fact that Windows does not require an application to provide a specific path for a DLL that it wishes to load. If no path is provided, Windows searches for the DLL in specific locations on the computer in a pre-defined order. Attackers can therefore give a malicious DLL the same name as a legitimate DLL but place it ahead of the legitimate version in the search order so that it will be loaded when Windows searches for it. Whitefly frequently delivers Vcrodat as a malicious DLL that has the same name as DLLs belonging to legitimate software from various security vendors. The group leverages search order hijacking to assure that its malicious DLLs will be executed. Targeting security applications could allow the attackers to gain higher privileges for the malware, since the vendor's component may be run with elevated privileges.

Once executed, Vcrodat loads an encrypted payload on to the victim's computer. The payload contacts a command and control (C&C) domain. Whitefly configures multiple C&C domains for each target. The payload sends system information about the infected computer to the C&C server and downloads additional tools.

> Whitefly usually attempts to remain within a targeted organization for long periods of time—often months—in order to steal large volumes of information.

Once the initial computer on the targeted organization's network is infected with Vcrodat, Whitefly begins mapping the network and infecting further computers. In order to carry out this operation, it uses publicly available tools, including Mimikatz (Hacktool.Mimikatz) and an open-source tool (SHA2: 263dc5a8121d20403beeeea452b6f33d51d41c6842d9d19919def1f1cb13226c) that exploits a known Windows privilege escalation vulnerability (CVE-2016-0051) on unpatched computers. The attackers rely heavily on tools such as Mimikatz to obtain credentials. Using these credentials, the attackers are able to compromise more machines on the network and, from those machines, again obtain more credentials. They perform this tactic repeatedly until they gain access to the desired data.

Whitefly usually attempts to remain within a targeted organization for long periods of time—often months—in order to steal large volumes of information. It keeps the compromise alive by deploying a number of tools that facilitate communication between the attackers and infected computers. These tools include a simple remote shell tool that will call back to the C&C server and wait for commands, and an open-source hacking tool called Termite (Hacktool.Rootkit), which allows Whitefly to perform more complex actions such as controlling multiple compromised machines at a time.

Additional malware used in selected attacks

In some attacks, Whitefly has used a second piece of custom malware, Trojan.Nibatad. Like Vcrodat, Nibatad is also a loader that leverages search order hijacking, and downloads an encrypted payload to the infected computer. And similar to Vcrodat, the Nibatad payload is designed to facilitate information theft from an infected computer.

While Vcrodat is delivered via the malicious dropper, we have yet to discover how Nibatad is delivered to the infected computer. Why Whitefly uses these two different loaders in some of its attacks remains unknown. And while we have found both Vcrodat and Nibatad inside individual victim organizations, we have not found any evidence of them being used simultaneously on a single computer.

Links to other attacks

Some of the tools that Whitefly has used in its attacks have also been deployed in other targeted attacks outside Singapore.

Between May 2017 and December 2018, a multi-purpose command tool (SHA2: 7de8b8b314f2d2fb54f8f8ad4bba435e8fc58b894b1680e5028c90c0a524ccd9) that has been used by Whitefly was also used in attacks against defense, telecoms, and energy targets in Southeast Asia and Russia. The tool appears to be custom-built and, aside from its use by Whitefly, these were the only other attacks where Symantec has observed its use.

In another case, Vcrodat was also used in an attack on a UK-based organization in the hospitality sector.

It's possible Whitefly itself performed these attacks but it’s more likely that they were carried out by one or more other groups with access to the same tools.

Adept attackers with a large toolset

It now appears that the SingHealth breach was not a one-off attack and was instead part of a wider pattern of attacks against organizations in the region. Whitefly is a highly adept group with a large arsenal of tools at its disposal, capable of penetrating targeted organizations and maintaining a long-term presence on their networks. Links with attacks in other regions also present the possibility that it may be part of a broader intelligence gathering operation.

Protection/Mitigation

Symantec has the following protection in place to protect customers against these attacks:

File-based protection

- Trojan.Vcrodat
- Trojan.Nibatad
- Hacktool.Rootkit
- Hacktool.Mimikatz

Indicators of Compromise

MD5	SHA2	Description
eab0a521aa7cac62d98d78ef845a8319	a196dfe4ef7d422aadf1709b12511ae82cb96aad030422b00a9c91fb60a12f17	Trojan.Vcrodat
79bef92272c7d1c6236a03c26a0804cc	d784a12fec628860433c28caa353bb52923f39d072437393629039fa4b2ec8ad	Trojan.Vcrodat
394df628b3c8977661c8bebea593e148	6e874ac92c7061300b402dc616a1095fa7d13c8a18c8a3ea5b30ffa832a7372c	Trojan.Nibatad
51862c3615e2f8a807b1d59f3aef3507	ed3cd71eaca603a00e4c0804dc34d84dc38c6c1e1c1f43af0568fb162c44c995	DLL Shellcode Loader
b4a7049b90503534d494970851bdda62	9d9a6337c486738edf4e5d1790c023ba172ce9b039df1b7b9720ed4c4c9ade90	DLL Shellcode Loader
	93c9310f3984d96f53f226f5177918c4ca78b2070d5843f08d2cf351e8c239d5	Mimikatz
	263dc5a8121d20403beeeea452b6f33d51d41c6842d9d19919def1f1cb13226c	CVE-2016-0051 privilege escalation
	b2b2e900aa2e96ff44610032063012aa0435a47a5b416c384bd6e4e58a048ac9	Termite
	dda22de8ad7d807cdac8c269b7e3b35a3021dcbff722b3d333f2a12d45d9908d	Simple command line remote access tool
	f562e9270098851dc716e3f17dbacc7f9e2f98f03ec5f1242b341baf1f7d544c	Simple command line remote access tool
	7de8b8b314f2d2fb54f8f8ad4bba435e8fc58b894b1680e5028c90c0a524ccd9	Multi-purpose command tool

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?