Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia

welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/

December 17, 2020

ESET researchers have uncovered a supply-chain attack on the website of a government in Southeast Asia.

Just a few weeks after the supply-chain attack on the Able Desktop software, another similar attack occurred on the website of the Vietnam Government Certification Authority (VGCA): ca.gov.vn. The attackers modified two of the software installers available for download on this website and added a backdoor in order to compromise users of the legitimate application.

ESET researchers uncovered this new supply-chain attack in early December 2020 and notified the compromised organization and the VNCERT. We believe that the website has not been delivering compromised software installers as of the end of August 2020 and ESET telemetry data does not indicate the compromised installers being distributed anywhere else. The Vietnam Government Certification Authority confirmed that they were aware of the attack before our notification and that they notified the users who downloaded the trojanized software.

Supply-chain attack in Vietnam

In Vietnam, digital signatures are very common, as digitally-signed documents have the same level of enforceability as “wet” signatures. According to Decree No. 130/2018, the cryptographic certificates used to sign documents must be granted by one of the authorized certificate providers that include the VGCA, which is part of the Government Cipher Committee. That committee, in turn, depends on the Ministry of Information and Communication.

In addition to issuing certificates, the VGCA develops and distributes a digital signature toolkit. It is used by the Vietnamese government, and probably by private companies, to sign digital documents. The compromise of a certification authority website is a good opportunity for APT groups, since visitors are likely to have a high level of trust in a state organization responsible for digital signatures.

As shown in Figure 1, it seems that these programs are deployed in the Party and State agencies.

Figure 1. Screenshot of ca.gov.vn

According to ESET telemetry, ca.gov.vn was compromised from at least the 23rd of July to the 16th of August 2020. Two of the installers available for download, gca01-client-v2-x32-8.3.msi and gca01-client-v2-x64-8.3.msi, were modified to include a piece of malware known as PhantomNet or SManager and recently analyzed by NTT Security. We were able to confirm that those installers were downloaded from ca.gov.vn over the HTTPS protocol, so we believe it is unlikely to be a man-in-the-middle attack. The URLs pointing to malicious installers were:

- https://ca.gov[.]vn/documents/20182/6768590/gca01-client-v2-x64-8.3.msi
- https://ca.gov[.]vn/documents/20182/6768590/gca01-client-v2-x32-8.3.msi

This is also confirmed by data from VirusTotal as shown in Figure 2.

Figure 2. Screenshot of VirusTotal. It shows the URL where the trojanized installer was downloaded from.

The trojanized installers are not properly signed, but we noticed that clean GCA installers are also incorrectly signed (*The digital signature of the object did not verify*). Both the official and trojanized MSIs use a certificate assigned to the Safenet company.

Figure 3 is a summary of the supply-chain attack. To be compromised, a user would have to manually download and execute the compromised software hosted on the official website.

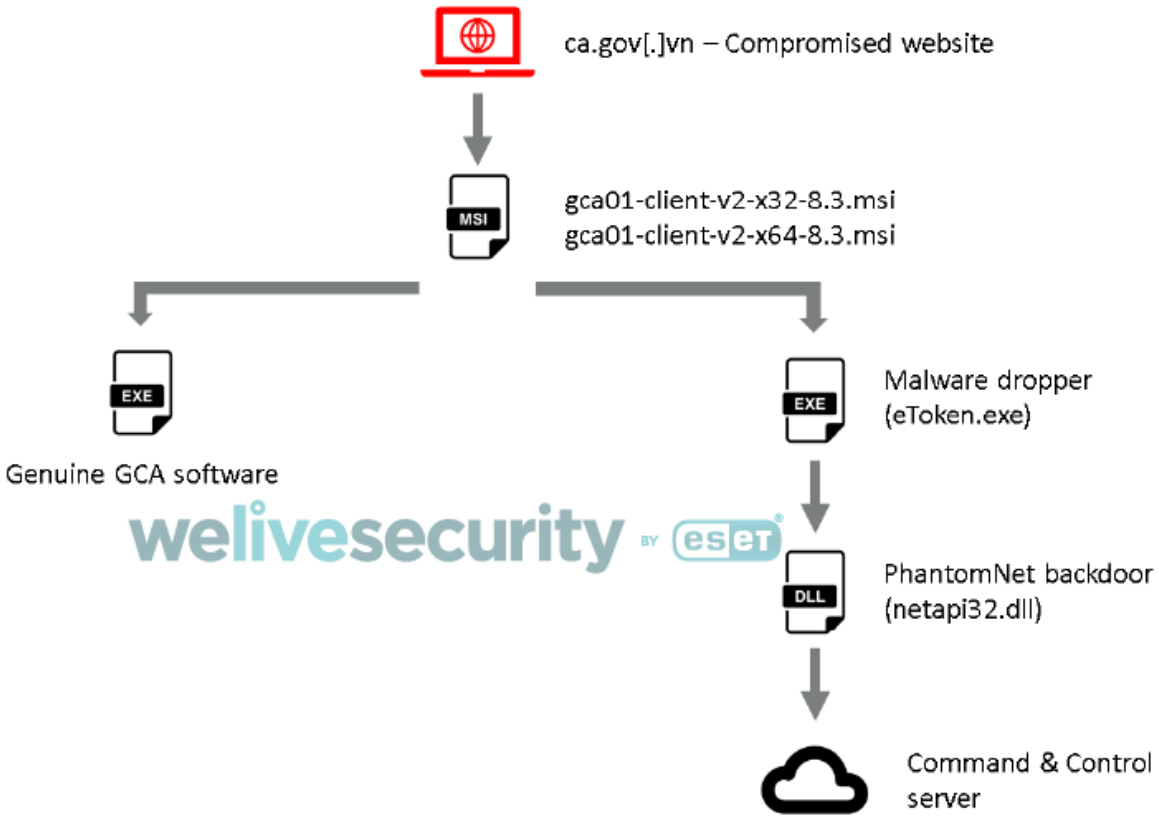

Figure 3. Simplified scheme of the supply-chain attack.

Once downloaded and executed, the installer starts the genuine GCA program and the malicious file. The malicious file is written to C:\Program Files\VGCA\Authentication\SAC\x32\eToken.exe. By also installing the legitimate program, the attackers make sure that this compromise won't be easily noticed by the end-users.

This malicious file is a simple dropper that extracts a Windows cabinet file (.cab) named 7z.cab and that contains the backdoor.

If the dropper runs as an admin, the backdoor is written to C:\Windows\apppatch\netapi32.dll and for the persistence, the dropper registers the malicious DLL as a service.

If run as a regular user, the backdoor is written to %TEMP%\Wmedia\<GetTickCount>.tmp and for the persistence, the dropper creates a scheduled task that calls the export Entery of the malicious DLL. It's interesting to note that the Entery export was also seen in versions of TManger used by TA428, as detailed by NTT Security.

PhantomNet

The backdoor was named Smanager_ssl.DLL by its developers but we use PhantomNet, as that was the project name used in an older version of this backdoor. This most recent version was compiled on the 26th of April 2020, almost two months before the supply-chain attack. In addition to Vietnam, we have seen victims in the Philippines, but unfortunately we did not uncover the delivery mechanism in those cases.

This backdoor is quite simple and most of the malicious capabilities are likely deployed through additional plugins. It can retrieve the victim's proxy configuration and use it to reach out to the command and control (C&C) server. This shows that the targets are likely to be working in a corporate network.

PhantomNet uses the HTTPS protocol to communicate with its hardcoded C&C servers: vgca.homeunix[.]org and office365.blogdns[.]com. In order to prevent a man-in-the-middle attack, PhantomNet implements certificate pinning, using functions from the SSPI library. The certificate is downloaded during the first connection with the C&C server and then stored in the Windows certificate store.

In addition to the use of dynamic DNS providers, it is interesting to note that the name of the first subdomain, vgca, was chosen in order to mimic the name of the Vietnam Government Certification Authority.

The implant can be controlled by the attackers using these five commands:

Command ID	Description
0x00110020	Get victim information (computer name, hostname, username, OS version, user privileges (admin or not), and the public IP address by querying ipinfo.io).
0x00110030	Call the export DeletePluginObject of all installed plugins.
0x00110040	Plugin management (install, remove, update). The plugins have the following exports (including the typo in the first one): GetPluginInfomation, GetRegisterCode, GetPluginObject, DeletePluginObject.
0x00110070	Set a value of a given field in the main structure of the backdoor.
0x547CBA78	Generate and set a password using the SSPI functions. The final purpose is unknown.

On VirusTotal, we found one plugin that matches the exports above. It is a debug build and is named SnowballS according to its PDB path and other debug paths:

- E:\WorkCode\AD_Attacker\Server\EXE_DEBUG\SnowballS.pdb

- e:\workcode\ad_attacker\server\plugins\plugins\snowballs\cdomainquery.cpp

An initial, cursory analysis suggests that this tool might be used for lateral movement, as it embeds Invoke-Mimikatz. It can also collect information about the victim machine and user accounts. This shows that PhantomNet can receive additional and complex plugins that are probably only deployed on machines of particular interest to the malware operators.

In the case of the attack in Vietnam, we were not able to recover data about post-compromise activity and thus we don't have visibility into the end goal of the attackers.

Conclusion

With the compromise of Able Desktop, the attack on WIZVERA VeraPort by Lazarus and the recent supply-chain attack on SolarWinds Orion, we see that supply-chain attacks are a quite common compromise vector for cyberespionage groups. In this specific case, they compromised the website of a Vietnamese certificate authority, in which users are likely to have a high level of trust.

Supply-chain attacks are typically hard to find, as the malicious code is generally hidden among a lot of legitimate code, making its discovery significantly more difficult.

For any inquiries, contact us as threatintel@eset.com. Indicators of Compromise can also be found in our GitHub repository.

IoCs

Files

SHA-1	ESET detection name	Description
5C77A18880CF58DF9FBA102DD8267C3F369DF449	Win32/TrojanDropper.Agent.SJQ	Trojanized installer (gca01-client-v2-x64-8.3.msi)
B0E4E9BB6EF8AA7A9FCB9C9E571D8162B1B2443A	Win32/TrojanDropper.Agent.SJQ	Trojanized installer (gca01-client-v2-x32-8.3.msi)
9522F369AC109B03E6C16511D49D1C5B42E12A44	Win32/TrojanDropper.Agent.SJQ	PhantomNet dropper
989334094EC5BA8E0E8F2238CDF34D5C57C283F2	Win32/PhantomNet.B	PhantomNet
5DFC07BB6034B4FDA217D96441FB86F5D43B6C62	Win32/PhantomNet.A	PhantomNet plugin

C&C servers
office365.blogdns[.]com
vgca.homeunix[.]org

MITRE ATT&CK

Note: This table was built using version 8 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Initial Access	T1195.002	Supply Chain Compromise: Compromise Software Supply Chain	Attackers modified the installer of the GCA01 software that is hosted on ca.gov.vn and added a backdoor to the MSI installer.
Execution	T1204.002	User Execution: Malicious File	The victim needs to manually execute the trojanized installer.
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task	If the user doesn't have admin privileges, PhantomNet persists via a scheduled task.
T1543.003	Create or Modify System Process: Windows Service	If the user has admin privileges, PhantomNet persists via a Windows service.	
Discovery	T1033	System Owner/User Discovery	PhantomNet implements a function to retrieve the username.
T1082	System Information Discovery	PhantomNet implements a function to retrieve the OS version.	
Command and Control	T1090.001	Proxy: Internal Proxy	PhantomNet can retrieve the proxy configuration of the default browser and use it to connect to the C&C server.
T1071.001	Application Layer Protocol: Web Protocols	PhantomNet uses HTTPS.	
T1573.002	Encrypted Channel: Asymmetric Cryptography	PhantomNet can add a certificate to the Windows store and use it for certificate pinning for its HTTPS communications.	

17 Dec 2020 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion