Operation NightScout: Supply-chain attack targets online gaming in Asia

ESET researchers uncover a supply-chain attack used in a cyberespionage operation targeting online-gaming communities in Asia

Ignacio Sanmillan

1 Feb 2021 - 11:30AM

During 2020, ESET research reported various supply-chain attacks, such as the case of WIZVERA VeraPort, used by government and banking websites in South Korea, Operation StealthyTrident compromising the Able Desktop chat software used by several Mongolian government agencies, and Operation SignSight, compromising the distribution of signing software distributed by the Vietnamese government.

In January 2021, we discovered a new supply-chain attack compromising the update mechanism of NoxPlayer, an Android emulator for PCs and Macs, and part of BigNox's product range with over 150 million users worldwide.

This software is generally used by gamers in order to play mobile games from their PCs, making this incident somewhat unusual.

Three different malware families were spotted being distributed from tailored malicious updates to selected victims, with no sign of leveraging any financial gain, but rather surveillance-related capabilities.

We spotted similarities in loaders we have been monitoring in the past with some of the ones used in this operation, such as instances we discovered in a Myanmar presidential office website supply-chain compromise on 2018, and in early 2020 in an intrusion into a Hong Kong university.

About BigNox

BigNox is a company based in Hong Kong, which provides various products, primarily an Android emulator for PCs and Macs called NoxPlayer. The company's official website claims that it has over 150 million users in more than 150 countries speaking 20 different languages. However, it's important to note that the BigNox follower base is predominantly in Asian countries.

BigNox also wrote an extensive blogpost in 2019 on the use of VPNs in conjunction with NoxPlayer, showing the company's concern for their users' privacy.

We have contacted BigNox about the intrusion, and they denied being affected. We have also offered our support to help them past the disclosure in case they decide to conduct an internal investigation.

Am I compromised?

- *Who is affected:* NoxPlayer users.
- *How to determine if I received a malicious update or not:* check if any ongoing process has an active network connection with known active C&C servers, or see if any of the malware based on the file names we provided in the report is installed in:
  - `C:\ProgramData\Sandboxie\SbieIni.dat`
  - `C:\ProgramData\Sandboxie\SbieDll.dll`
  - `C:\ProgramData\LoGiTech\LBTServ.dll`
  - `C:\Program Files\Internet Explorer\ieproxysocket64.dll`
  - `C:\Program Files\Internet Explorer\ieproxysocket.dll`
  - a file named `%LOCALAPPDATA%\Nox\update\UpdatePackageSilence.exe` not digitally signed by BigNox.
- *How to stay safe:*
  - In case of intrusion – standard reinstall from clean media.
  - For non-compromised users: do not download any updates until BigNox notifies that it has mitigated the threat.

Timeline

Based on ESET telemetry, we saw the first indicators of compromise in September 2020, and activity continued until we uncovered explicitly malicious activity on January 25th, 2021, at which point we reported the incident to BigNox.

Victimology

In comparison to the overall number of active NoxPlayer users, there is a very small number of victims. According to ESET telemetry, more than 100,000 of our users have Noxplayer installed on their machines. Among them, only 5 users received a malicious update, showing that Operation NightScout is a highly targeted operation. The victims are based in Taiwan, Hong Kong and Sri Lanka.

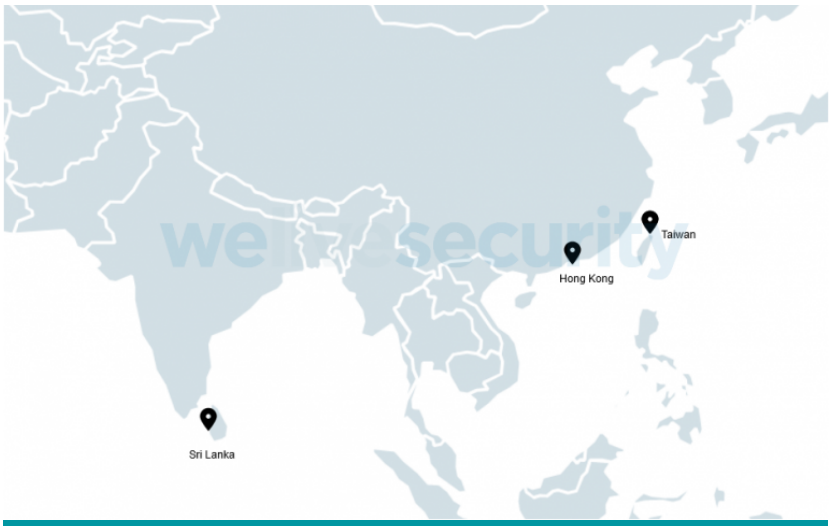


Figure 1. Asia victimology map

We were unsuccessful finding correlations that would suggest any relationships among victims. However, based on the compromised software in question and the delivered malware exhibiting surveillance capabilities, we believe this may indicate the intent of collecting intelligence on targets somehow involved in the gaming community.

It is important to highlight that, in contrast with similar previous operations such as the Winnti Group activity targeting the gaming industry in 2019, we haven't found indicators that would suggest indiscriminate proliferation of malicious updates among a large number NoxPlayer users, reinforcing our belief that this is a highly targeted operation.

Update mechanism

In order to understand the dynamics of this supply-chain attack, it's important to know what vector was used in order to deliver malware to NoxPlayer users. This vector was NoxPlayer's update mechanism.

On launch, if NoxPlayer detects a newer version of the software, it will prompt the user with a message box (Figure 2) to offer the option to install it.

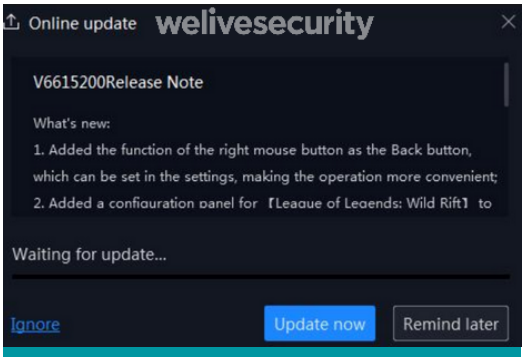


Figure 2. NoxPlayer update prompt

This is done by querying the update server via the BigNox HTTP API (`api.bignox.com`) in order to retrieve specific update information, as seen in Figure 3.

Figure 3. NoxPlayer client update API request

The response to this query contains update-specific information such as the update binary URL, its size, MD5 hash and other additional related information as seen in Figure 4.

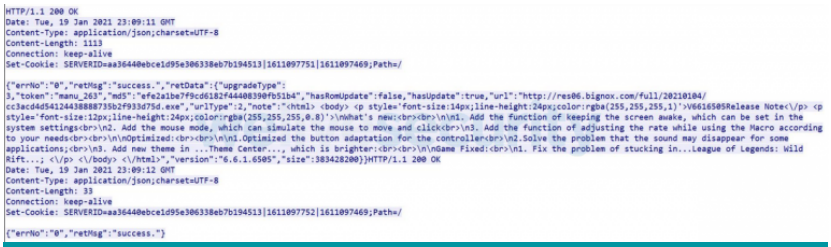


Figure 4. NoxPlayer server API reply

Upon pressing the "Update now" button from Figure 1, the main NoxPlayer binary application `Nox.exe` will supply the update parameters received to another binary in its toolbox `NoxPack.exe`, which is in charge of downloading the update itself, as can be seen in Figure 5.

Figure 5. NoxPlayer execution chain on update

After this is done, the progress bar in the message box will reflect the state of the download (Figure 6), and when completed the update has been performed.

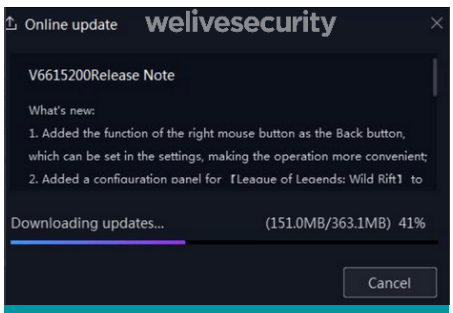


Figure 6. NoxPlayer update ongoing via `NoxPack.exe`

Supply-chain compromise indicators

We have sufficient evidence to state that the BigNox infrastructure (`res06.bignox.com`) was compromised to host malware, and also to suggest that their HTTP API infrastructure (`api.bignox.com`) could have been compromised. In some cases, additional payloads were downloaded by the BigNox updater from attacker-controlled servers. This suggests that the URL field, provided in the reply from the BigNox API, was tampered with by the attackers. The intrusion flow observed is depicted in Figure 7.

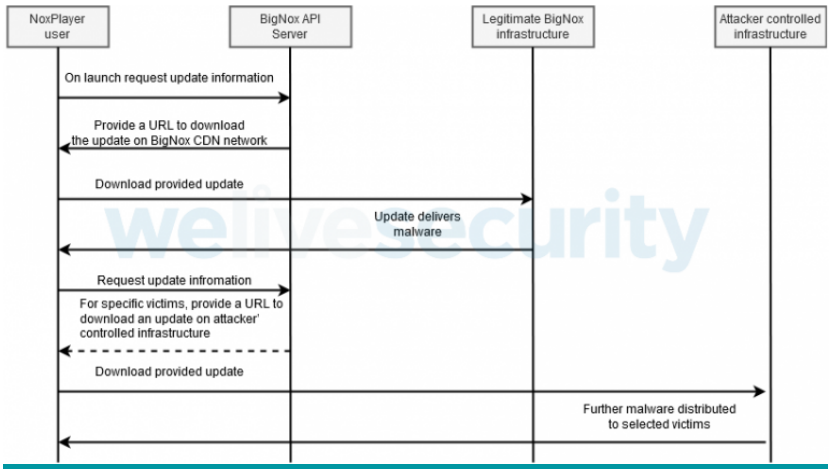


Figure 7. Intrusion flow sequence diagram

An overview of what's shown in the sequence diagram above is the following:

1. On launch, the primary NoxPlayer executable `Nox.exe` will send a request via the API to query update information.
2. The BigNox API server responds to the client request with specific update information, including the URL to download the update from BigNox legitimate infrastructure.
3. `Nox.exe` provides the appropriate parameters to `NoxPlayer.exe` to download the update.
4. The legitimate update stored in BigNox infrastructure could have been replaced with malware, or it may be a new filename/URL not used by legitimate updates.
5. Malware is installed on the victim's machine. Contrary to legitimate BigNox updates, the malicious files are not digitally signed, strongly suggesting that the BigNox build system was not compromised, but just its systems that distribute updates.
6. Some reconnaissance of the victim is performed and information sent to the malware operators.
7. The perpetrators tailor malicious updates to specific victims of interest based on some unknown filtering scheme.
8. `Nox.exe` will perform sporadic update requests.
9. The BigNox API server responds to the client with update information, which states that the update is stored in the attacker-controlled infrastructure.
10. Further malware gets delivered to selected victims.

With this information we can highlight several things:

- Legitimate BigNox infrastructure was delivering malware for specific updates. We observed that these malicious updates were only taking place in September 2020.
- Furthermore, we observed that for specific victims, malicious updates were downloaded from attacker-controlled infrastructure subsequently and throughout the end of 2020 and early 2021.

- We are highly confident that these additional updates were performed by `Nox.exe` supplying specific parameters to `NoxPack.exe`, suggesting that the BigNox API mechanism may have also been compromised to deliver tailored malicious updates.
- It could also suggest the possibility that victims were subjected to a MitM attack, although we believe this hypothesis is unlikely since the victims we discovered are in different countries, and attackers already had a foothold on the BigNox infrastructure.
- Furthermore, we were able to reproduce the download of the malware samples hosted on `res06.bignox.com` from a test machine and using https. This discards the possibility that a MitM attack was used to tamper the update binary.

It is also important to mention that malicious updates downloaded from the attacker-controlled infrastructure mimicked the path of legitimate updates:

- Malicious update to attacker-controlled infrastructure:
  `http://cdn.cloudfronte[.]com/player/upgrade/ext/20201030/1/35e3797508c555d5f5e19f721cf94700.exe`
- Legitimate NoxPlayer update:
  `http://res06.bignox[.]com/player/upgrade/202012/1b31bced0a564bed9f60264f061dcdae.exe`

Furthermore, registered attacker-controlled domain names mimicked the BigNox CDN network domain name, that being `cloudfront.net`.

These indicators suggest that attackers were trying to avoid detection so that they could remain under the radar and achieve long-term persistence.

Malware

A total of three different malicious update variants were observed, each of which dropped different malware. These variants are the following:

Malicious Update variant 1

This variant is one of the preliminary updates pointing to compromised BigNox infrastructure. Our analysis is based on the sample with SHA-1 `CA4276033A7CBDCCDE26105DEC911B215A1CE5CF`.

The malware delivered does not seem to have been documented before. It is not extremely complex, but it has enough capabilities to monitor its victims. The initial RAR SFX archive drops two DLLs into `C:\Program Files\Internet Explorer\` and runs one of them, depending on architecture, via `rundll32.exe`. The names of these DLLs are the following:

- `ieproxysocket64.dll`
- `ieproxysocket.dll`

It also drops a text file named `KB911911.LOG` to disk, into which the original name of the SFX installer will be written. The DLL attempts to open and read this log file, and if not found will stop execution, therefore implementing an execution guardrail.

The DLL will then check whether it has been loaded by any of the following processes; if it has, it will stop its own execution:

- `smss.exe`
- `winlogon.exe`
- `csrss.exe`
- `wininit.exe`
- `services.exe`
- `explorer.exe`

The IP address of the machine will be checked to verify that it is neither `127.0.0.1` nor `0.0.0.0`; if it is, it will be rechecked in an infinite loop until it changes. Otherwise, it will proceed to extract the UUID of the current machine via a WMI object query. This returned UUID is hashed using MD5 to serialize the current victim. Account name information will also be retrieved and saved.

An encrypted configuration will be retrieved from the DLL's resource. This configuration is encrypted using a two-byte XOR with 0x5000. The encrypted configuration is partially visible given the weakness of the key used:

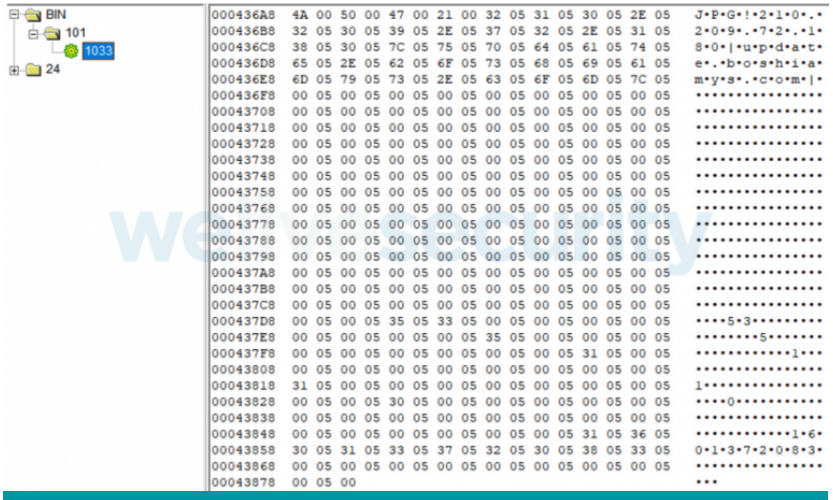


Figure 8. Encrypted configuration in resources

The format of this configuration is the following (roughly):

Offset	Size	Comment
0x00	0x08	Fake JPG header magic
0x08	0x12C	Buffer holding tokenized C&C information
0x134	0x14	Buffer holding port for C&C communication
0x148	0x14	Sleep time
0x15C	0x14	Operate flag; don't operate with network monitoring tools deployed or if this flag is set
0x170	0x14	N/A
0x184	0x14	DNS flag; append a token at the end of a hostname buffer with either `|UDP` or `|DNS`, depending on the value of this field
0x198	0x38	Variable holding offset start of decoded configuration buffer

After the configuration has been parsed, the backdoor will check several times for network monitoring processes before transferring execution to the C&C loop. Operation stops if the Operate flag is set or if either of the following processes is running:

- `netman.exe`
- `wireshark.exe`

The backdoor can use either a raw IP address or a domain name to communicate with the C&C server. After successful connection to the C&C, the malware will be able to perform the following commands:

Command ID	Specification
getfilelist-delete	Delete specified files from the disk
getfilelist-run	Run a command via the `WinExec` API
getfilelist-upload	Upload a file via `ScreenRDP.dll::ConnectRDServer`
getfilelist-downfile1	Download a specific file
getfilelist-downfile2	Download a specific directory
getfilelist-downfile3	Same as getfilelist-downfile2
<default>	\\tsclient drive redirection of certain directories (starting with `A:` for range(0x1A))

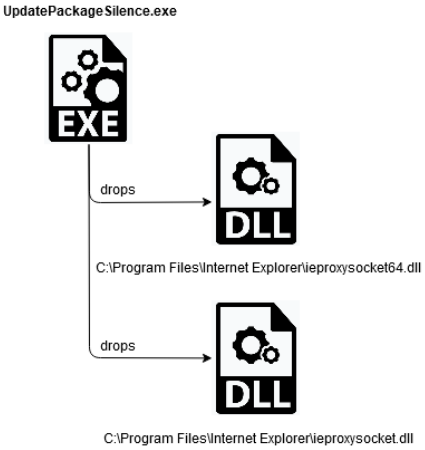


Figure 9. Anatomy of malicious update variant 1

Malicious Update variant 2

This malware variant was also spotted being downloaded from legitimate BigNox infrastructure. Our analysis is based on the sample with SHA-1 `E45A5D9B03CFBE7EB2E90181756FDF0DD690C00C`.

It contains several files comprising what is known as a trident bundle, in which a signed executable is used to load a malicious DLL, which will decrypt and load a shellcode, implementing a reflective loader for the final payload.

The theme for this trident bundle was to disguise the malware as Sandboxie components. The names of the bundled components are the following:

Filename	Description
`C:\ProgramData\Sandboxie\SandboxieBITS.exe`	Signed Sandboxie COM Services (BITS)
`C:\ProgramData\Sandboxie\SbieDll.dll`	Malicious hijacked DLL
`C:\ProgramData\Sandboxie\SbieIni.dat`	Malicious encrypted payload; decrypts a reflectively loaded instance of Gh0st RAT
`C:\Users\Administrator\AppData\Local\Temp\delself.bat`	Script to self-delete the initial executable
`C:\Windows\System32\wmkawe_3636071.data`	Text file containing the sentence `Stupid Japanese`

We have encountered other instances of this same text file, dropped by a very similar loader in a supply-chain compromise involving the Myanmar presidential office website in 2018, and in an intrusion into a Hong Kong university in 2020.

The deployed final payload was a variant of Gh0st RAT with keylogger capabilities.

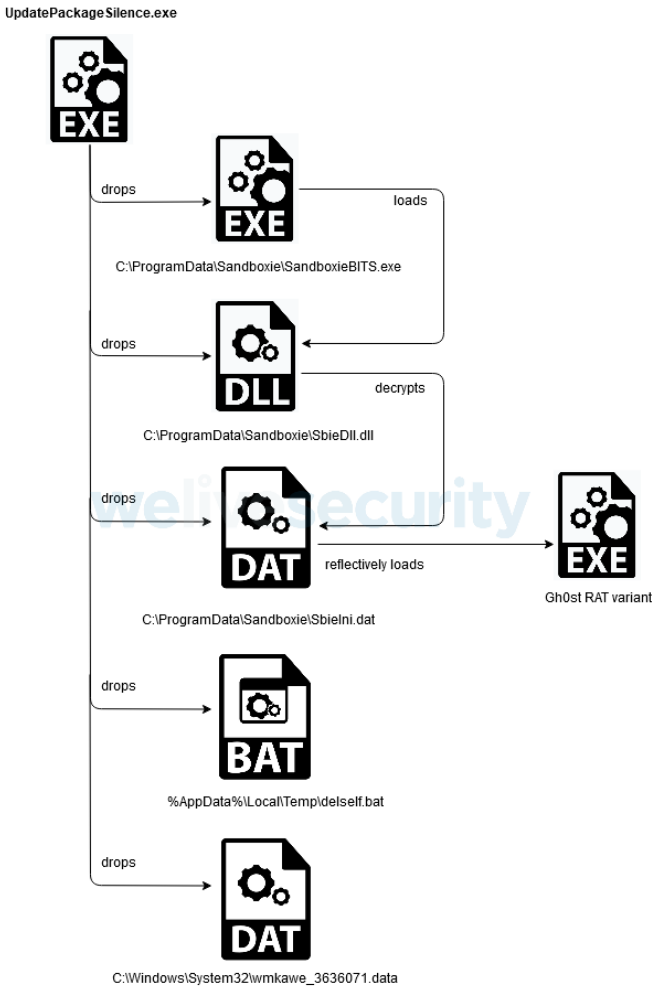


Figure 10. Anatomy of malicious update variant 2

Malicious Update variant 3

This update variant was only spotted in activity subsequent to initial malicious updates, downloaded from attacker-controlled infrastructure. Our analysis is based on the sample with SHA-1 `AA3D31A1A6FE6888E4B455DADDA4755A6D42BEEB`.

Similarly, as with the previous variant, this malicious update comes bundled in an MFC file, and extracts two components: a benign signed file and a dependency of it. The components are:

Filename	Description
`C:\ProgramData\LoGiTech\LoGitech.exe`	Signed Logitech binary
`C:\ProgramData\LoGiTech\LBTServ.dll`	Malicious DLL decrypts and reflectively loads an instance of PoisonIvy

On the most recently discovered victims, the initial downloaded binary was written in Delphi, while for previous victims the same attacker-controlled URL dropped a binary written in C++. These binaries are the initial preliminary loaders. Although the loaders were written in different programming languages, both versions deployed the same final payload, that being an instance of the PoisonIvy RAT.

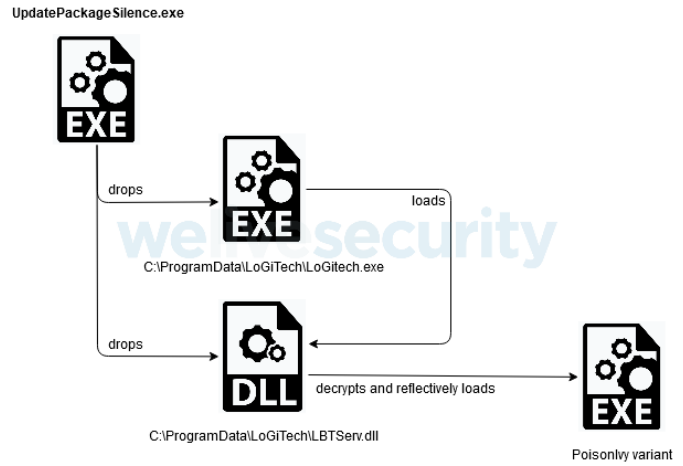


Figure 11. Anatomy of malicious update variant 3

Conclusion

We have detected various supply-chain attacks in the last year, such as Operation SignSight or the compromise of Able Desktop among others. However, the supply-chain compromise involved in Operation NightScout is particularly interesting due to the targeted vertical, as we rarely encounter many cyberespionage operations targeting online gamers.

Supply-chain attacks will continue to be a common compromise vector leveraged by cyber-espionage groups, and its complexity may impact the discovery and mitigation of these type of incidents.

For any inquiries, or to make sample submissions related to the subject, contact us at: threatintel@eset.com.

Acknowledgement

The author would like to give special credit to Matthieu Faou for his support and feedback during the investigation.

Indicators of Compromise (IoCs)

Files

SHA-1	ESET detection name	Decription
CA4276033A7CBDCCDE26105DEC911B215A1CE5CF	Win32/Agent.UOJ	Malicious Update variant 1
E45A5D9B03CFBE7EB2E90181756FDF0DD690C00C	Win32/GenKryptik.ENAT	Malicious Update variant 2
AA3D31A1A6FE6888E4B455DADDA4755A6D42BEEB	Win32/Kryptik.HHBQ	Malicious Update variant 3
5732126743640525680C1F9460E52D361ACF6BB0	Win32/Delf.UOD	Malicious Update variant 3

C&C servers

```
210.209.72[.]180
103.255.177[.]138
185.239.226[.]172
45.158.32[.]65
cdn.cloudistcdn[.]com
q.cloudistcdn[.]com
update.boshiamys[.]com
```

Malicious update URLs

```
http://cdn.cloudfronter[.]com/player/upgrade/ext/20201030/1/35e3797508c555d5f5e19f721cf94700.exe
http://cdn.cloudfronter[.]com/player/upgrade/ext/20201101/1/bf571cb46afc144cab53bf940da88fe2.exe
http://cdn.cloudfronter[.]com/player/upgrade/ext/20201123/1/2ca0a5f57ada25657552b384cf33c5ec.exe
http://cdn.cloudfronter[.]com/player/upgrade/ext/20201225/7c21bb4e5c767da80ab1271d84cc026d.exe
http://cdn.cloudfronter[.]com/player/upgrade/ext/20210119/842497c20072fc9b92f2b18e1d690103.exe
https://cdn.cloudfronte[.]com/player/upgrade/ext/20201020/1/c697ad8c21ce7aca0a98e6bbd1b81dff.exe
http://cdn.cloudfronte[.]com/player/upgrade/ext/20201030/1/35e3797508c555d5f5e19f721cf94700.exe
http://res06.bignox[.]com/player/upgrade/202009/6c99c19d6da741af943a35016bb05b35.exe
http://res06.bignox[.]com/player/upgrade/202009/42af40f99512443cbee03d090658da64.exe
```

MITRE ATT&CK techniques

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	Malware gets delivered via NoxPlayer updates.
Execution	T1053.005	Scheduled Task/Job: Scheduled Task	Malicious update variant 3 instances will be executed via Scheduled task.
Execution	T1569.002	System Services: Service Execution	Malicious update variant 2 instances will be executed via service execution.

Persistence	T1053.005	Scheduled Task/Job: Scheduled Task	Malicious update variant 2 instances will create a scheduled task to establish persistence.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	Malicious update variant 2 and 3 will be contained in "trident" bundles for evasion purposes.
	T1574.002	Hijack Execution Flow: DLL Side-Loading	Malicious updates shipped as "trident" bundles will perform DLL side loading.
Collection	T1056.001	Input Capture:Keylogging	Some of the final payloads such as PoisonIvy and Gh0st RAT have keylogging capabilities.
Command and Control	T1090.001	Proxy: Internal Proxy	The PoisonIvy final payload variant has capabilities to authenticate with proxies.
	T1095	Non-Application Layer Protocol	All malicious update instances communicate over raw TCP or UDP.
	T1573	Encrypted Channel	Both PosionIvy and Gh0st RAT use encrypted TCP communication to avoid detection.
Exfiltration	T1041	Exfiltration Over C2 Channel	Exfiltration in all malicious updates instances is done over a Command and Control channel.

Ignacio Sanmillan

1 Feb 2021 - 11:30AM

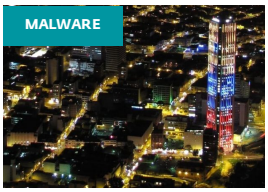
Newsletter

Email... Submit

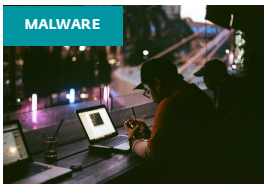
Similar Articles

Emotet botnet disrupted in global operation

Vadokrist: A wolf in sheep's clothing



Operation Spalax: Targeted malware attacks in Colombia



7 ways malware can get into your device

Discussion