Operation StealthyTrident: corporate software under attack

LuckyMouse | KJR, Hyperbro, Trisping and StealthyPetal linked to Mongolian supply-chain attacks

Matthieu Faraux

14 Dec 2020 · 9 min. read

Share
f
tw
in
✉

LAST: 19 December 2020 We have no reason to believe that the StealthyPetal infrastructure mentioned in this blog post was used in distributed malware. The last instance we saw occurred in July 2020 as described in our Blogspot.

On December 9th, we built a dataset as a result so as that the impacted victims number and the Destroy's updates have had been stopped. We have also found a new variant of Trisping. This also stated that it was signed using Symantec certificates. We built hashes and the DestroyUpdate.exe, and that this last occurrence they observed of such attacks was in July 2020.

ESET has no information that allows us to corroborate or dispute these statements.

ESET researchers discovered that chat software called Ole Desktop, part of a business management suite popular in Mongolia and used by ESET government agencies in Mongolia (according to ISO), was used to deploy a previously undocumented backdoor we have named StealthyTrident. We have also found KJR, Hyperbro and A. T. Calyst (Trisping) malware that has been discovered by ESET. StealthyPetal was used during Operation Lagrant (if campaigns attributed to T. KJR by ProofPoint). connection with the StealthyPetal backdoor, which is now used for at least two different threat actors, was also found.

Two different Trojanized installers, as well as a thirty-compromised update system, were used to deliver the payloads. According to our telemetry we think the Ole update system has been compromised since at least June 2020 and impacted installers delivered since at least May 2020.

Additionally, yesterday, eset published a blogpost documenting a campaign targeting government agencies and a national data center in Mongolia. During that campaign the attackers compromised an unknown company that was providing government institutions in Eastern Asia, and leveraged that compromise to deliver Hyperbro by email. We believe that compromised company was Ole, as the Remarkar used in those malicious email attachments probably DocumentSecurity.exe and the observed such a file being used to drop the same Hyperbro samples as described in ESET blogpost.

Diagram summarizing the connections between LuckyMouse, T. KJR and the StealthyPetal backdoor. C&C infrastructure is obscured in figure 1.

Figure 1. Summary of the connections between LuckyMouse, T. KJR and the StealthyPetal backdoor

Regarding the attribution of Operation StealthyTrident, considering that Hyperbro is commonly attributed to LuckyMouse that Trisping was attributed to T. KJR and that it uses one of the StealthyPetal C&C servers, multiple competing hypotheses exist:

- LuckyMouse has access to Trisping and StealthyPetal
- LuckyMouse shares its access to the compromised Ole Desktop update server with the T. KJR group or some other group having access to Trisping
- Hyperbro is now shared with T. KJR or some other group having access to Trisping and StealthyPetal
- LuckyMouse and T. KJR are subgroups of the same threat actor

Although originally only known to be used by the Winnti Group, it should also be noted here that since at least October 2018, StealthyPetal has been shared amongst multiple threat actors including the Winnti Group, CeroPurple, TA2726, LuCrip and Andariel.

Additional elements regarding the connection between Trisping and T. KJR will be published in a second blogpost documenting another campaign where the attackers used both Trisping and StealthyPetal.

We called this campaign Operation StealthyTrident because the attackers make extensive use of a three-pronged "trident" side-loading technique.

Compromised Ole Desktop

Ole Desktop is that software included as part of the Ole business management suite used in Mongolia. It is a Chromium-based JavaScript app making use of the Nodejs library. According to Ole, their software suite is used by 450 government agencies in Mongolia.

In mid 2019, we observed a first occurrence of the Hyperbro backdoor. Ole Desktop application being used to download and execute Hyperbro. Hyperbro is a backdoor commonly attributed to LuckyMouse (also known as Emissary Panda or APT27). Ole Desktop was also used to download another malware Trisping¹. In that case, the Ole Desktop software itself was not trojanized (i.e. it did not contain malicious code). The most likely hypothesis is that the Ole Desktop update system was compromised.

In addition to legitimate Ole Desktop applications used to drop and execute Hyperbro, likely using its update system, we also found two Ole Desktop installers that were actually trojanized and compared the Hyperbro backdoor and the Trisping. 1 The first occurrence of this trojanized Ole Desktop installer dates back to December 2019. Overview of these events is shown in Figure 2.

Figure 2. Timeline of the events involving Hyperbro, Trisping, PlugX, Trenger and Ole Desktop

We notified Ole about these compromises.

Ole Desktop update mechanism

To update itself, Ole Desktop downloads the update installer through HTTPS. The code responsible for the update is shown in Figure 3.

```
var filename = process.platform.toLowerCase() + '-ole-desktop.exe';
var tmpdir = require('os').tmpdir();
var fullpath = tmpdir + '\\' + filename;
var file = fs.create(fullpath, {mode: 0777});
var fileSize = 0, lastTime = 0, lastSize = 0;
var bytes = 0, total = 0, response, request;
var updateFile = function
var lastTime = parseInt(response.headers['content-length'], 10);
var bytes = 0;
response.on('data', function (chunk) {
var bytes = bytes + chunk.length;
var percent = parseInt(bytes * 100 / lastTime);
var now = parseInt(Date.now() / 1000);
if (percent != lastPercent && now != lastNow) {
lastPercent = percent;
lastNow = now;
console.log('Downloaded %d%% (%d/%d) - %s', percent, bytes, lastTime, speed);
});
response.on('end', function () {
console.log('Download finished');
console.log('Executing: [%s %s]', cmd.toUnicode(), [], [object Object]);
});
```

Figure 3 Javascript code responsible for Ole Desktop updates

The downloaded update installer is saved in %TEMP%\filename-of-the-ole-desktop.exe. Once downloaded, the installer is executed. In the case of a legitimate update installer, a new version of Ole Desktop will be installed. We assumed however that starting in mid-2019, the executable downloaded wasn't a legitimate installer, but rather the Hyperbro backdoor. Since, in that case, the executable is not an Ole Desktop installer, the update process would create installation-state files and Hyperbro's exec.exe instead – and Ole Desktop is not updated anymore.

Multiple elements support the hypothesis of a compromise of the update server:

- The filename and the path used to download Hyperbro are the filename and path used for the update system.
- The update is downloaded through HTTPS, at least on the middle attack in January.
- Hyperbro was dropped on all computers using Ole Desktop during the same timeframe as previous legitimate updates.
- The malicious ole-desktop.exe is signed by the real Ole Desktop software and not malware-masquerading as Ole Desktop.
- No legitimate updates have been created since the beginning of the campaign.

We believe this is enough to state that the update mechanism was compromised. It should be noted that Ole Desktop has multiple update servers, some of them hosted at customer organizations. Since we have no information on which update server was used for these victims, we don't know whether Ole was compromised or one of its customer's update servers.

The list of update servers used by Ole Desktop is shown in Figure 4. We can see from that list that Ole Desktop is related used by several government entities such as the Mineral Resource Authority of Mongolia, the Ministry of Labor and Social Welfare, Plans for Ministry of Construction and Urban Development, the Development Bank of Mongolia or the Mongolian State University of Education.

```
http://ole.mt/
https://ecloud.jus.mn/
https://ecloud.mrta.mn/
https://desktop.ptnet.jus.mn/
https://ole.ub.edu.mn/
https://ecloud.mcud.gov.mn/
http://ecloud.pdf.gov.mn/
http://ecloud.mlsp.gov.mn/
https://ole.ub.ac.mn/ ← Mongolian Univ.
https://ecloud.ub.edu.mn/ ← Mongolian Univ.
http://ole.mn.gov.mn/ ← Mongolian Univ.
http://ecloud.mnet.mn/ ← Mobile Network Provider
https://ecloud.pdf.gov.mn/ ← Pension Fund of Mongolia
https://ecloud.ub.ac.mn/ ← Mongolian Univ.
https://ecloud.gov.mn/ ← Mongolian Government
https://ecloud.mnet.mn/ ← Mobile Network Provider
https://ecloud.mnet.mn/ ← Mobile Network Provider
https://ecloud.mnet.mn/ ← Mobile Network Provider
```

ESET detection names

Win32/HyperBro. D
Win32/LuckyMouse.BL
Win32/Korplug.ND
Win32/Korplug.QD
Win64/Spy.Tmanger.

Trojanized ble Desktop

```
0B0CF4ADA30797B0488857F9A3B1429F44335FB6
B51835A5D8DA77A49E3266494A8AE96764C4C152
```

Payload loader

```
23A227DD9B77913D15735A25EFB0882420B1DE81
2A630E25D0C1006B6DBD7277F8E52A3574BEFFEC
```

HyperBro

```
8FFF5C6EB4DAEE2052B3578B73789EB15711FEEE
0550AAE6E3CEABCEF2A3F926339E68817112059A
```

Korplug

```
5D066113534A9E31F49BEFDA560CF8F8890496D0
```

Tmanger

```
ED6CECFDAAEB7F41A824757862640C874EF3F7AE
```

C&C domains

```
developer.firefoxapi[.]com
```

C&C IP addresses

```
45.77.173[.]124
45.77.55[.]145
139.180.208[.]225
```

C&C URLs

```
https://developer.firefoxapi[.]com/ajax
https://139.180.208[.]225/ajax
```

MITRE TT&CK techniques

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

Tactic	ID	Name	Description
Initial ccess	T1195.002	Supply Chain Compromise: Compromise Software Supply Chain	One of the ble update servers was likely compromised in order to deploy HyperBro and Tmanger.
Execution	T1204.002	User Execution: Malicious File	ble Desktop trojanized installer is executed by the user.
Persistence	T1574.002	Hijack Execution Flow: DLL Side-Loading	HyperBro, Korplug and Tmanger are executed via DLL side-loading.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	HyperBro and Korplug payloads are XOR encoded.
			Tmanger configuration is RC4 encrypted.
	T1574.002	Hijack Execution Flow: DLL Side-Loading	HyperBro and Korplug side-loading hosts are legitimate, signed executables from trusted security vendors.
Collection	T1056.001	Input Capture: Keylogging	Tmanger supports keylogging.
	T1113	Screen Capture	Tmanger supports screen capture.
Command nd Control	T1573.001	Encrypted Channel: Symmetric Cryptography	Tmanger messages are RC4 encrypted.
	T1008	Fallback Channels	Tmanger can fallback to a secondary C&C.
	T1095	Non- pplication Layer Protocol	Tmanger communicates using raw TCP.
	T1071.001	pplication Layer Protocol: Web Protocols	HyperBro communication protocol is HTTP.
Exfiltration	T1041	Exfiltration Over C2 Channel	Tmanger can exfiltrate files via a dedicated command.

Mathieu Tartare

10 Dec 2020 - 11:30 M

Newsletter

Email... Submit

Similar rticles

Watering hole deploys new macOS malware, DazzleSpy, in sia

Virus Bulletin: Old malware never dies – it just gets more targeted

natomy of native IIS malware

Some URL shortener services distribute ndroid malware, including banking or SMS trojans

Discussion

What do you think?
11 Responses

Upvote Funny Love Surprised Angry Sad

0 Comments WeLiveSecurity.com Disqus' Privacy Policy Login

Favorite 2 Tweet Share Sort by Best

Start the discussion…

LOG IN WITH OR SIGN UP WITH DISQUS

Name

Be the first to comment.

Subscribe Add Disqus to your site Do Not Sell My Data DISQUS

Copyright © ESET, ll Rights Reserved

Cookies make a website a better place

We use cookies to give you the best optimized online experience and consistent information. You can agree to the collection of all cookies by clicking on the Accept & Close button or adjust your cookies settings by clicking on Manage Cookies. For more information please see our Cookie Policy.

ACCEPT ALL AND CLOSE

MANAGE COOKIES