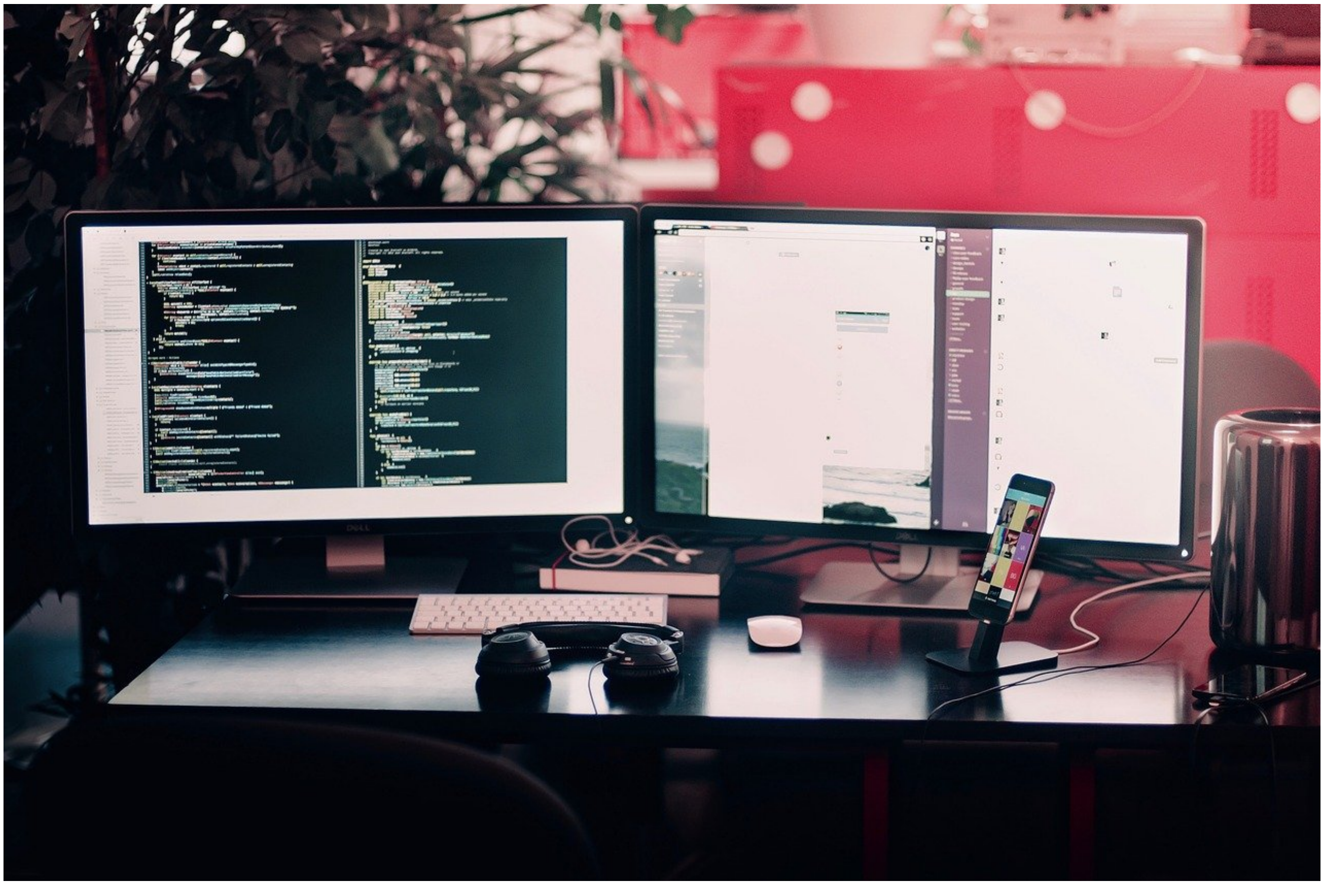
Operation StealthyTrident: corporate software under attack

welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop

December 10, 2020



LuckyMouse, TA428, HyperBro, Tmanger and ShadowPad linked in Mongolian supply-chain attack

Mathieu Tartare

10 Dec 2020 - 11:30AM

LuckyMouse, TA428, HyperBro, Tmanger and ShadowPad linked in Mongolian supply-chain attack

UPDATE (December 14, 2020): We have no reason to believe that Able Desktop updates or trojanized installers are still being used to distribute malware. The last instance we saw occurred in July 2020 as described in our blogpost.

On December 11th, Able Soft stated in an email to us that the trojanized installers and Able Desktop's updates have not been used since the incident was reported to them. They also stated that, as a precaution against further attacks, Able Soft halted the Able Desktop updates, and that the 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 Able Desktop, part of a business management suite popular in Mongolia and used by 430 government agencies in Mongolia (according to Able), was used to deliver the HyperBro backdoor (commonly used by LuckyMouse), the Korplug RAT (also known as PlugX), and a RAT called Tmanger (which was first documented by NTT Security and was used during Operation Lagtime IT campaigns attributed to TA428 by Proofpoint). A connection with the ShadowPad backdoor, which is now used by at least five different threat actors, was also found.

Two different trojanized installers, as well as a likely compromised update system, were used to deliver the payloads. According to our telemetry we think the Able update system has been compromised since at least June 2020 and trojanized installers delivered since at least May 2018.

Additionally, yesterday, Avast 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 East Asia and leveraged that compromise to deliver HyperBro by email. We believe that compromised company was Able, as the filename used in that malicious email attachment is probably AbleTimeAccess_Update.exe, and we observed such a file being used to drop the same HyperBro sample as described in Avast's blogpost.

A diagram summarizing the connections between LuckyMouse, TA428 and the ShadowPad backdoor C&C infrastructure is shown in Figure 1.

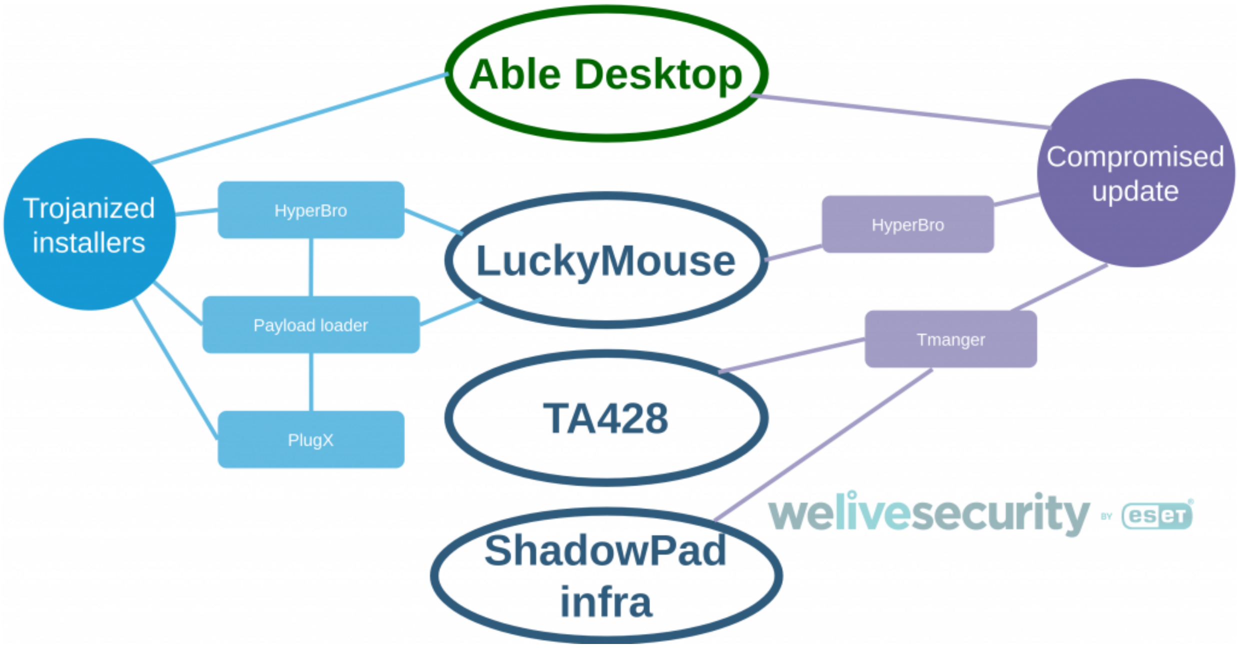


Figure 1. Summary of the connections between LuckyMouse, TA428 and the ShadowPad backdoor

Regarding the attribution of Operation StealthyTrident, considering that HyperBro is commonly attributed to LuckyMouse, that Tmanger was attributed to TA428 and that it uses one of the ShadowPad C&C servers, multiple competing hypotheses exist:

- LuckyMouse has access to Tmanger and ShadowPad.
- LuckyMouse share its access to the compromised Able Desktop update server with the TA428 group or some other group having access to Tmanger.
- HyperBro is now shared with TA428 or some other group having access to Tmanger and ShadowPad.
- LuckyMouse and TA428 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 2019, ShadowPad has been shared amongst multiple threat actors including the Winnti Group, CactusPete, TICK, IceFog and KeyBoy.

Additional elements regarding the connection between Tmanger and TA428 will be published in a second blogpost documenting another campaign where the attackers used both Tmanger and ShadowPad.

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

Compromised Able Desktop

Able Desktop is chat software included
as part of the Able business management suite used in Mongolia. It is a Chromium-based JavaScript app making use of the NodeJS library. According to Able, their software

suite is used by 430 government agencies in Mongolia.

In mid-2018, we observed a first occurrence of the legitimate Able Desktop application being used to download and execute HyperBro. HyperBro is a backdoor commonly attributed to LuckyMouse (also known as Emissary Panda or APT27). Able Desktop was also used to download and execute Tmanger; in that case, the Able Desktop software itself was not trojanized (i.e. it did not contain malicious code). The most likely hypothesis is that the Able Desktop update system was compromised.

In addition to legitimate Able Desktop applications used to drop and execute HyperBro, likely using its update system, we also found two Able Desktop installers that were actually trojanized and contained the HyperBro backdoor and the Korplug RAT. The first occurrence of this trojanized Able Desktop installer dates back to December 2017. A timeline of these events is shown in Figure 2.

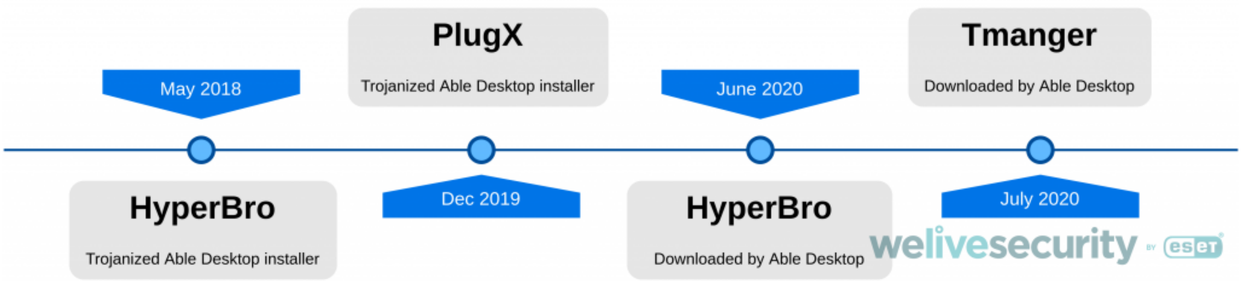
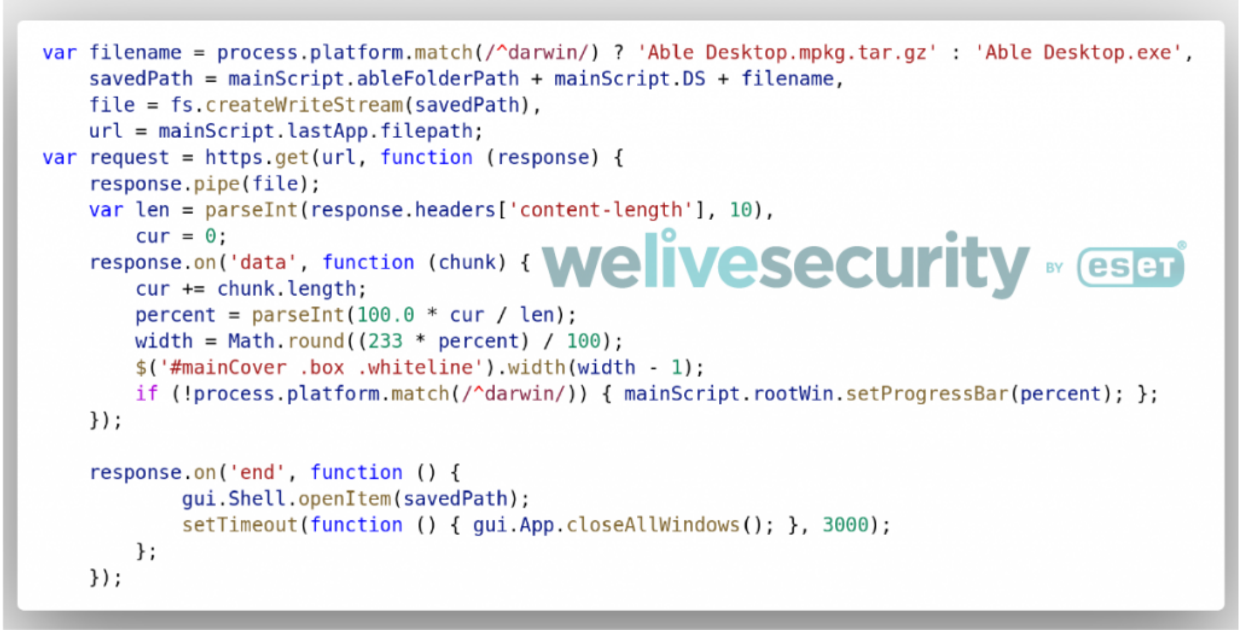

May 2018
HyperBro
Trojanized Able Desktop installer
PlugX
Trojanized Able Desktop installer
Dec 2019
June 2020
HyperBro
Downloaded by Able Desktop
Tmanger
Downloaded by Able Desktop
July 2020
welivesecurity by eset

Figure 2. Timeline of the various implants used with either a trojanized Able Desktop installer or likely delivered through Able Desktop update

We notified Able about these compromises.

Able Desktop update mechanism

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



```
var filename = process.platform.match(/^darwin/) ? 'Able Desktop.mpkg.tar.gz' : 'Able Desktop.exe',
    savedPath = mainScript.ableFolderPath + mainScript.DS + filename,
    file = fs.createWriteStream(savedPath),
    url = mainScript.lastApp.filepath;
var request = https.get(url, function (response) {
    response.pipe(file);
    var len = parseInt(response.headers['content-length'], 10),
        cur = 0;
    response.on('data', function (chunk) {
        cur += chunk.length;
        percent = parseInt(100.0 * cur / len);
        width = Math.round((233 * percent) / 100);
        $('#mainCover .box .whiteline').width(width - 1);
        if (!process.platform.match(/^darwin/)) { mainScript.rootWin.setProgressBar(percent); };
    });

    response.on('end', function () {
            gui.Shell.openItem(savedPath);
            setTimeout(function () { gui.App.closeAllWindows(); }, 3000);
        };
    });
```

Figure 3. JavaScript code responsible for Able Desktop updates

The downloaded update installer is saved to %USERPROFILE%\Documents\Able\Able Desktop.exe. Once downloaded, the installer is executed. In the case of a legitimate update installer, a new version of Able Desktop will be installed. We observed, however, that starting in mid-2018, the executable downloaded wasn't a legitimate installer, but rather the HyperBro backdoor. Since, in that case, the executable is not an Able Desktop installer but plain malware, no update installation takes place and HyperBro is executed instead —and Able 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 by the update system.
- The update is downloaded through HTTPS, so a man–in–the–middle attack is unlikely.
- HyperBro was dropped on all computers using Able Desktop during the same timeframe as previous legitimate updates.
- The malicious Able Desktop.exe is dropped by the real Able Desktop software and not malware masquerading as Able Desktop.
- No legitimate updates have been installed since the beginning of the campaign.

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

The list of update servers used by Able Desktop is shown in Figure 4. We can see from that list that Able Desktop is indeed used by several government entities such as the Mineral Resource Authority of Mongolia, the Ministry of Justice and Foreign Affairs, the Ministry of Construction and Urban Development, the Development Bank of Mongolia or the Mongolian State University of Education.

Figure 4. List of update servers that can be used with Able Desktop

```
var urls = [
'https://able[.]mn:8989',
'https://www.able[.]mn:8989',
'https://develop.able[.]mn:8989',
'https://release.able[.]mn:8989',
'https://mail.able[.]mn:8989',
'http://eoffice.police[.]gov:8000',
'http://e-office.dbm[.]mn:8000',
'http://192.168.10[.]37:8000', // Хөгжлийн банк
'http://172.16.200[.]16:8000', // Тээвэр хөгжлийн банк
'http://192.168.10[.]62:8000', // Миний локал
'https://eoffice.president[.]mn:8000',
'https://intranet.gov[.]mn:8000',
'https://intranet.mrpam.gov[.]mn:8080', // Ашигт малтмал
'https://able.audit[.]mn:8989', // Audit
'https://intranet.mojha.gov[.]mn:8989', // Хууль зүйн яам
'https://office.msue.edu[.]mn:8989',
'https://mcud.able[.]mn:8989', //Барилга хот байгуулалтын яам
'https://able.tog[.]mn:8989' // Улаанбаатар цахилгаан түгээх сүлжээ ХК
```

Then, in July 2020, we saw a shift from HyperBro being delivered by the update system to a backdoor attributed to TA428 and called Tmanger.

Trojanized Able Desktop

In addition to HyperBro and Tmanger being downloaded by legitimate Able Desktop software, we also found two different trojanized installers. It is unknown to us whether these installers were downloadable from the Able website or from another source.

Able Desktop installers, both legitimate and trojanized, are 7-Zip SFX installers and are not signed. In the case of trojanized installers, the legitimate Able Desktop software is bundled with either HyperBro or Korplug. The payload and its side–loading host are packaged in a data1.dat file which is a 7-Zip SFX archive while Able Desktop is packaged in a data.dat file which is an Advanced Installer. The content of the trojanized installer is summarized in Figure 5. The same IntgStat.exe side–loading host and pcalocalresloader.dll are used in both the root of the Able Desktop.exe archive and data1.dat archive.

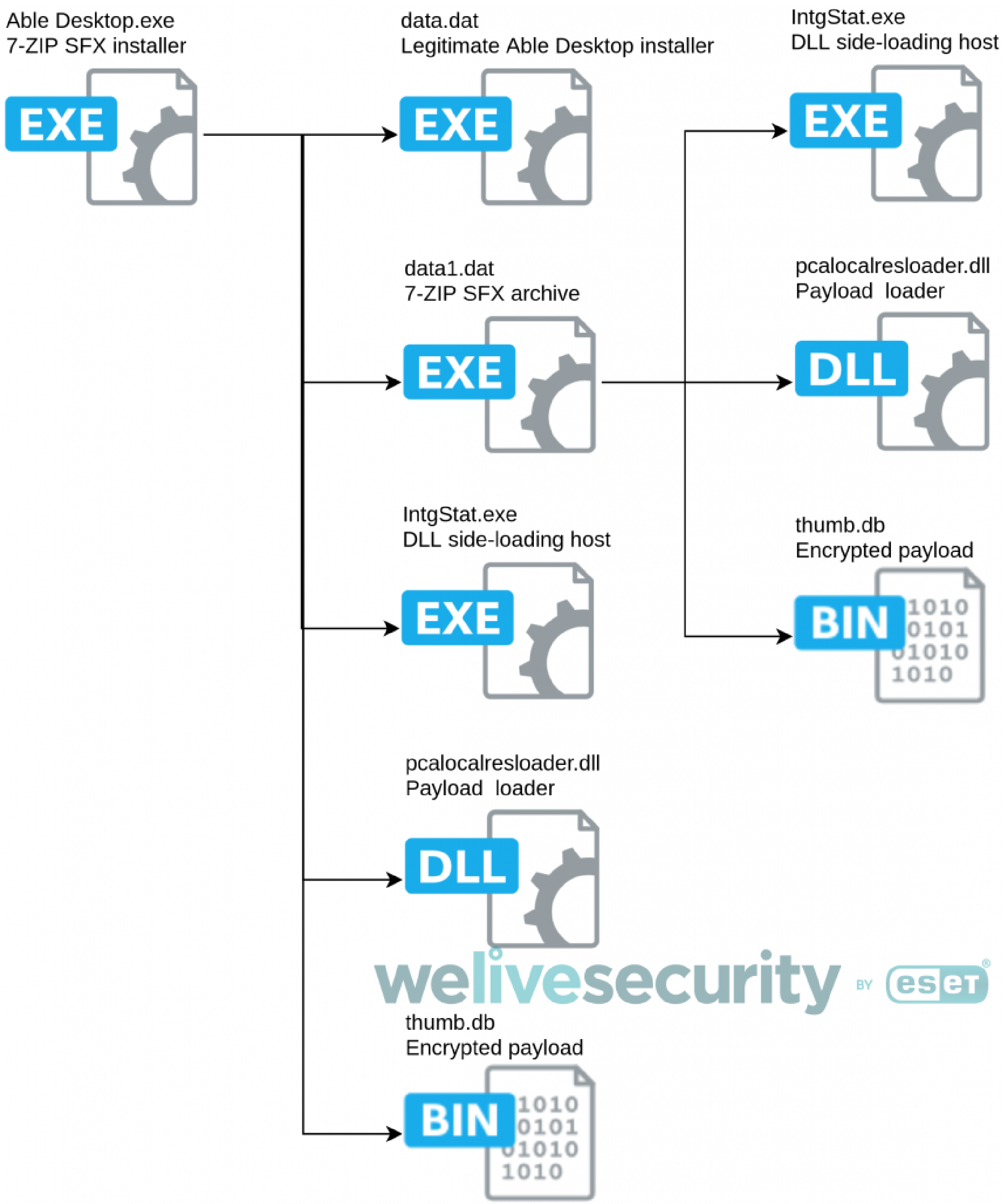


Figure 5. Trojanized Able Desktop installer content

The 7-Zip SFX installer first executes IntgStat.exe, a legitimate Symantec executable, which is a DLL side–loading host used to load pcalocalresloader.dll. This DLL is used to decrypt and load the XOR-encoded payload stored in thumb.db. This payload, XOR encoded with 0x04, once mapped into memory by the payload loader, will decompress and execute an embedded, LZNT1–compressed PE executable that is used to rename data.dat (the legitimate installer) and data1.dat (the malicious payload) as Able Desktop.exe and data1.exe respectively, and then execute them.

Once executed, the newly renamed data1.exe 7-Zip SFX archive will extract its contents and execute the second IntgStat.exe side–loading host, which then loads pcalocalresloader.dll. Again pcalocalresloader.dll is used to load the XOR-encoded payload stored in the thumb.db file. As before, this payload will decompress and execute an embedded LZNT1–compressed PE executable, which is actually HyperBro.

Note that, in the case of the Able Desktop installer trojanized with Korplug, the same side–loading host and DLL are used to execute data1.dat, while the side–loading host used to execute Korplog itself is not IntgStat.exe, but siteadv.exe – a legitimate executable from McAfee – and the loader DLL is called siteadv.dll. Apart from this change of side–loading host, the payload delivery mechanism is the same.

HyperBro

The HyperBro backdoor is LuckyMouse's custom backdoor used since at least 2013 and in continuous development. The variant being used here is similar to the variant described by Palo Alto Networks and Kaspersky. HyperBro was delivered to victims by both the legitimate Able Desktop software and a trojanized Able Desktop installer.

Similar to the version used with the trojanized Able Desktop installer, in the case of the HyperBro implant downloaded by the legitimate Able Desktop, its first stage consists in a 7-Zip SFX containing:

- thinprobe.exe, a legitimate Symantec executable used for DLL side–loading
- thinprobe.dll, a HyperBro loader
- thumbs.db, the XOR-encoded payload

HyperBro's loader DLL, thinprobe.dll, is executed by DLL side–loading using the thinprobe.exe executable, which is a legitimate, signed Symantec executable. While the side–loading host used with the downloaded HyperBro is different, the DLL used to decode and execute the thumbs.db payload is exactly the same.

This technique is very similar to the three–pronged trident attack reported by a Kaspersky researcher. Both thinprobe.exe and Intgstat.exe side–loading hosts were previously used by LuckyMouse to load HyperBro.

Note, however, that contrary to previously documented HyperBro droppers employing such a trident, the payload here is not Shikata Ga Nai encoded but XOR encoded with the value 0x04.

The C&C URL of the HyperBro implant used with the trojanized Able Desktop installer is https://developer.firefoxapi[.]com/ajax, while the C&C URL used by the one downloaded by the legitimate Able Desktop is https://139.180.208[.]225/ajax.

Considering HyperBro's compilation timestamps, the version used with the trojanized installer was compiled Fri Dec 08 05:22:23 2017 while the version downloaded by Able Desktop was compiled Mon Mar 11 03:23:54 2019. This suggests that the trojanized installer was used before the version downloaded by the Able Desktop updater. The trojanized installer was first seen in our telemetry in May 2018, while the version downloaded by Able Desktop was first seen in June 2020 (see the timeline in Figure 2).

Korplug

The Korplug RAT (also known as PlugX) is used by multiple different threat groups. In this case, it was only delivered via the trojanized Able Desktop installer and we have seen no occurrence of Korplug being downloaded by legitimate Able Desktop software.

As mentioned previously, and similar to installers trojanized with HyperBro, Korplug is bundled in the installer with the legitimate Able Desktop and executed twice via the trident model by DLL side–loading using IntgStat.exe as host executable and then siteadv.exe. The identical DLL is used to decode and execute the thumbs.db XOR-encoded payload as the one used with the installer trojanized with HyperBro, providing a strong link between these two trojanized installers.

The C&C address used by Korplug is 45.77.173[.]124:443. Interestingly, this address was also used by a CobaltStrike implant targeting a school in Mongolia during the same timeframe.

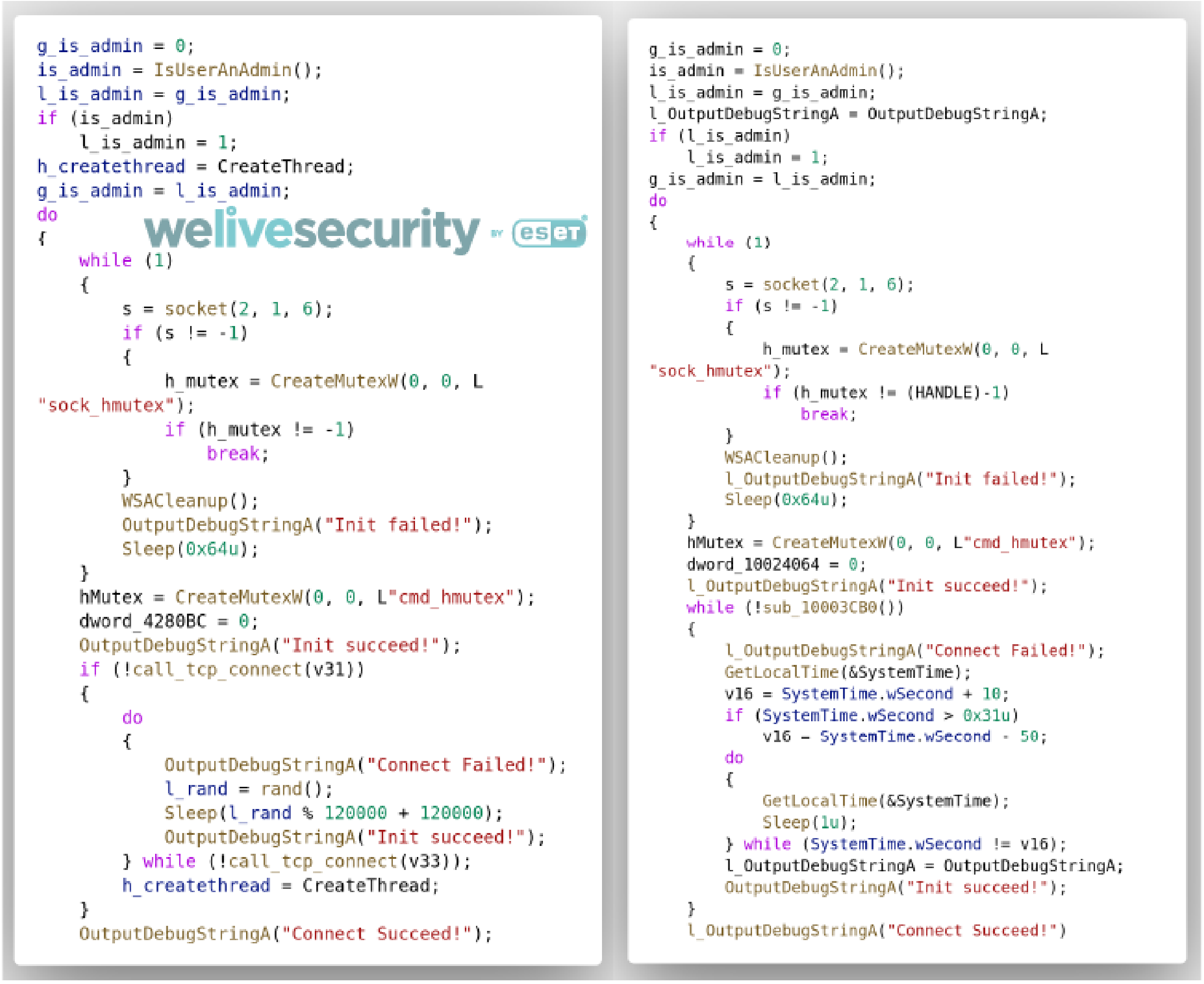
Its compilation timestamp (Sun Dec 08 06:22:34 2019) as well as the compilation timestamp of the installer (Wed Sep 04 16:52:04 2019) suggest that it was used after the Able Desktop installer trojanized with HyperBro and before HyperBro was downloaded by legitimate Able Desktop software. See the timeline in Figure 2.

Tmanger

Tmanger is a RAT that was first documented by NTT Security and that was used in Operation Lagtime IT which was attributed to TA428 by Proofpoint. It is called Tmanger because it is apparently the name given by its developer, as we can see from its PDB path, as an example:

c:\users\waston\desktop\20190403_tmanger\20191118 tm_new 1.0\release\mloaddll.pdb

Considering the variant we observed during Operation StealthyTrident no PDB path was present but it is still very similar to the one documented by NTT Security in their blogpost. As an example of similarity between the two samples, the connection procedure used by one of the Tmanger samples documented by NTT Security (14140782A68FF20000C7E9F58336620A65D4D168) and the one dropped by Able Desktop are shown side-by-side in Figure 6.



```
g_is_admin = 0;
is_admin = IsUserAnAdmin();
l_is_admin = g_is_admin;
if (is_admin)
    l_is_admin = 1;
h_createthread = CreateThread;
g_is_admin = l_is_admin;
do
{
    while (1)
    {
        s = socket(2, 1, 6);
        if (s != -1)
        {
            h_mutex = CreateMutexW(0, 0, L
"sock_hmutex");
            if (h_mutex != -1)
                break;
        }
        WSACleanup();
        OutputDebugStringA("Init failed!");
        Sleep(0x64u);
    }
    hMutex = CreateMutexW(0, 0, L"cmd_hmutex");
    dword_4280BC = 0;
    OutputDebugStringA("Init succeed!");
    if (!call_tcp_connect(v31))
    {
        do
        {
            OutputDebugStringA("Connect Failed!");
            l_rand = rand();
            Sleep(l_rand % 120000 + 120000);
            OutputDebugStringA("Init succeed!");
        } while (!call_tcp_connect(v33));
        h_createthread = CreateThread;
    }
    OutputDebugStringA("Connect Succeed!");
```

```
g_is_admin = 0;
is_admin = IsUserAnAdmin();
l_is_admin = g_is_admin;
l_OutputDebugStringA = OutputDebugStringA;
if (l_is_admin)
    l_is_admin = 1;
g_is_admin = l_is_admin;
do
{
    while (1)
    {
        s = socket(2, 1, 6);
        if (s != -1)
        {
            h_mutex = CreateMutexW(0, 0, L
"sock_hmutex");
            if (h_mutex != (HANDLE)-1)
                break;
        }
        WSACleanup();
        l_OutputDebugStringA("Init failed!");
        Sleep(0x64u);
    }
    hMutex = CreateMutexW(0, 0, L"cmd_hmutex");
    dword_10024064 = 0;
    l_OutputDebugStringA("Init succeed!");
    while (!sub_10003CB0())
    {
        l_OutputDebugStringA("Connect Failed!");
        GetLocalTime(&SystemTime);
        v16 = SystemTime.wSecond + 10;
        if (SystemTime.wSecond > 0x31u)
            v16 = SystemTime.wSecond - 50;
        do
        {
            GetLocalTime(&SystemTime);
            Sleep(1u);
        } while (SystemTime.wSecond != v16);
        l_OutputDebugStringA = OutputDebugStringA;
        OutputDebugStringA("Init succeed!");
    }
    l_OutputDebugStringA("Connect Succeed!")
```

Figure 6. Comparison of the connection routine in Tmanger sample dropped by legitimate Able Desktop (left) and one of the samples documented by NTT SecurityOne notable difference is that in the case of the Able Desktop variant, Tmanger is packaged is one single executable, while the variant described by NTT Security consists of three DLLs.

ESET telemetry shows the first download of this Tmanger variant by the legitimate Able Desktop software in July 2020. Tmanger replaced HyperBro on that system and HyperBro was not seen downloaded to it after that.

The C&C addresses used by this Tmanger implant, downloaded by Able Desktop, are stored in an RC4-encrypted configuration and are the following:

- 45.77.55[.]145:80
- 45.77.55[.]145:443
- 45.77.55[.]145:8080

The communication protocol is TCP and the messages are RC4 encrypted.

Interestingly, the first address is part of the ShadowPad network infrastructure and, to the best of our knowledge, none of these addresses are overlapping with LuckyMouse infrastructure.

Conclusion

ESET Research discovered a campaign targeting Mongolian organizations that relied on compromised Able Desktop installers and compromises to the Able update system to deliver HyperBro, Korplug and Tmanger malware.

This campaign shows a connection with the ShadowPad backdoor, as we observed network infrastructure overlaps between the ShadowPad C&C network infrastructure and one of the Tmanger C&C addresses.

Apart from the use of HyperBro, developed and commonly used by LuckyMouse, we found no significant overlap with the LuckyMouse toolset or network infrastructure. Does this mean that LuckyMouse has access to ShadowPad and Tmanger or did LuckyMouse share their access to a compromised Able Desktop update server with the TA428 group? Another hypothesis could be that, similarly to ShadowPad, HyperBro is now shared with other threat actors. Finally, one last hypothesis could be that LuckyMouse and TA428 are closely related threat actors or are actually the same.

Indicators of Compromise can also be found on GitHub. For any inquiries, or to make sample submissions related to the subject, contact us at: threatintel@eset.com.

Acknowledgment

The author would like to thank Matthieu Faou, who contributed to this research.

IoCs

ESET detection names

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

Trojanized Able 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 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	One of the Able update servers was likely compromised in order to deploy HyperBro and Tmanger.

Tactic	ID	Name	Description
Execution	T1204.002	User Execution: Malicious File	Able 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 And 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-Application Layer Protocol	Tmanger communicates using raw TCP.	
T1071.001	Application Layer Protocol: Web Protocols	HyperBro communication protocol is HTTP.	
Exfiltration	T1041	Exfiltration Over C2 Channel	Tmanger can exfiltrate files via a dedicated command.

10 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