AnyDesk Bundled with New Ransomware Variant

blog.trendmicro.com/trendlabs-security-intelligence/legitimate-application-anydesk-bundled-with-new-ransomware-variant/

May 1, 2018

We recently discovered a new ransomware (Detected as RANSOM_BLACKHEART.THDBCAH), which drops and executes the legitimate tool known as AnyDesk alongside its malicious payload. This isn't the first time that a malware abused a similar tool. TeamViewer, a tool with more than 200 million users, was abused as by a previous ransomware that used the victim's connections as a distribution method.

In this instance, however, RANSOM_BLACKHEART bundles both the legitimate program and the malware together instead of using AnyDesk for propagation.

Bundling a legitimate tool with ransomware

Although the specifics of how RANSOM_BLACKHEART enters the system remains unknown, we do know that users can unknowingly download the ransomware when they visit malicious sites. Once downloaded, RANSOM_BLACKHEART drops and executes two files:

- %User Temp%\ANYDESK.exe
- %User Temp%\BLACKROUTER.exe

Figure 1. The files dropped by RANSOM_BLACKHEART

Figure 1. The files dropped by RANSOM_BLACKHEART

As noted earlier, the first file contains AnyDesk, a powerful application capable of bidirectional remote control between different desktop operating systems, including Windows, macOS, Linux and FreeBSD, as well as unidirectional access on Android and iOS. In addition, it can perform file transfers, provide client to client chat and can also log sessions. Note that the version used by the attackers is an older version of AnyDesk, and not the current one.


Figure 2. The AnyDesk user interface on the sample we analyzed

Figure 2. The AnyDesk user interface on the sample we analyzed

It will also delete shadow copies via the following process:

```
"cmd.exe" /c vssadmin.exe delete shadows /all /quiet
```

The second file is the actual ransomware. Based on our analysis, we can determine that it's a fairly common ransomware, with a routine that encrypts a variety of files that use different extensions as part of its routine. The complete list can be seen below:

- .dbf
- .doc
- .docx
- .dt
- .dwg
- .efd
- .elf
- .epf
- .erf
- .exe
- .geo
- .gif
- .grs
- .html
- .ini
- .jpeg
- .jpg
- .lgf
- .lgp
- .log
- .mdb
- .mft
- .mkv
- .mp3
- .mp4
- .mxl
- .odt
- .pdf
- .pff
- .php
- .png
- .ppt
- .pptx
- .psd
- .rar
- .rtf
- .sln
- .sql
- .sqlite
- .st
- .tiff
- .txt
- .vrp
- .webmp
- .wmv
- .xls
- .xlsx
- .xml
- .zip
- 1cd

It will search out and encrypts all files with these extensions in the following folders:

- %Desktop%
- %Application Data%
- %AppDataLocal%
- %Program Data%
- %User Profile%
- %System Root%\Users\All Users
- %System Root%\Users\Default
- %System Root%\Users\Public
- All Drives except for %System Root%

Once it has found and encrypted a file, it will append the .BlackRouter extension to the affected file. When it has accomplished its encryption routine, RANSOM_BLACKHEART will then drop a ransom note, in which the attackers demand $50 or 0.006164 BTC for decryption, in the following locations:

- {All Drives}:\ReadME-BlackRouter.txt
- %Desktop%\ReadME-BlackRouter.txt
-

Figure 3. Screenshot of the ransom note

We believe bundling AnyDesk with the ransomware might be an evasion tactic. Once RANSOM_BLACKHEART is downloaded, AnyDesk will start running in the affected system's background — masking the true purpose of the ransomware while it performs its encryption routine. Cybercriminals may be experimenting with AnyDesk as an alternative because Teamviewer's developers have acknowledged its abuse, and have also included some anti-malware protection in some of its tools.

Note that we found another malicious sample that is very similar, but it's bundled with a keylogger (Detected as TSPY_KEYLOGGER.THDBEAH) instead of ransomware. AnyDesk has acknowledged the existence of the ransomware, and has stated that they will be discussing possible steps they can take.

Trend Micro Solutions

Trend Micro XGen™ security provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. It features high-fidelity machine learning to secure the gateway, endpoint data and applications, and protects physical, virtual, and cloud workloads. With capabilities like web/URL filtering, behavioral analysis, and custom sandboxing, XGen™ protects against today's purpose-built threats that bypass traditional controls, exploit known, unknown, or undisclosed vulnerabilities, and either steal or encrypt personally-identifiable data. Smart, optimized, and connected, XGen™ powers Trend Micro's suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

Related Hash detected as RANSOM_BLACKHEART.THDBCAH:

85173ef5572f316df839e63b4e1526e97e5f123ae73f898b872baa6a5a9711f

Ransomware

We recently discovered a new ransomware (Detected as RANSOM_BLACKHEART.THDBCAH), which drops and executes the legitimate tool known as AnyDesk alongside its malicious payload.

By: Raphael Centeno May 01, 2018 Read time: (words)

Content added to Folio