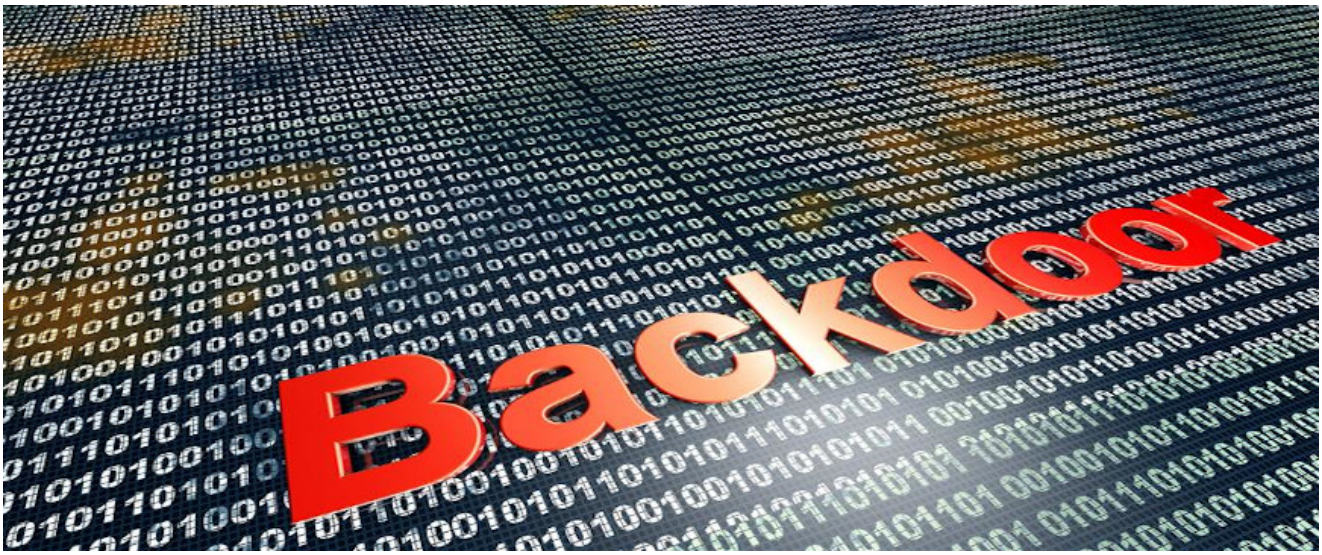
Trojanized TeamViewer Exploits its Users

blog.trendmicro.com/trendlabs-security-intelligence/unsupported-teamviewer-versions-exploited-backdoors-keylogging

June 15, 2016



Malware

We have evidence that trojanized an old version of TeamViewer installer packages have been used in a spam campaign that resulted in attackers gaining remote access to various systems.

By: Trend Micro June 15, 2016 Read time: (words)

Users of the TeamViewer remote-access service have been complaining in recent weeks about how their systems have been hacked into, unauthorized purchases made on their cards, their bank accounts emptied. Initially it was believed that this was due to a hack into TeamViewer itself, but the company has denied this. Instead, they have blamed password re-use, especially with millions of old passwords in the wild thanks to disclosed social network breaches.

Others have speculated that malware could be in use somehow, and that may be the case. We have evidence that trojanized TeamViewer installer packages have been used in a spam campaign that resulted in attackers gaining remote access to various systems. While this particular spam campaign used an old version of TeamViewer, we can't dismiss the possibility of other attacks using newer versions.

This spam campaign targeted users in Italy, using a variety of subject lines such as the following (English translation in parenthesis):

- Accesso dati (Data access)
- Il tuo ID e stato usato (Your ID was used)
- Prova gratuita 30 giorni (Free 30-day trial)
- Conferma dell'ordine (Order conformation)
- Il tuo conto informazione (Your account information)
- Finanziamento?????? (Financing)

A simple .JS (JavaScript) file was attached to these messages; when run this file downloads various files onto the system:

- A keylogger, detected as TSPY_DRIDEX.YYSUV
- A "Trojanized" version of TeamViewer, detected as BKDR_TEAMBOT.MNS.
- A batch file which executed the above two items, then deletes itself

This particular Trojanized version that the malware installs is very old - version 6.0.17222.0. TeamViewer 6 was first released in December 2010 and was superseded by version 7 in November 2011. Secondly, it is installed in an unusual location: *%APPDATA%\Div.* (Some variants installed their copy into *%APPDATA%/Addins* instead.) This behavior is consistent across all the various permutations of this attack we have seen.

This version of TeamViewer was Trojanized, but not by modifying the legitimate version. Instead, it *includes* an additional DLL - *avicap32.dll*. (This malicious DLL is detected as BKDR_TEAMBOT.DLL.) In a classic case of DLL search order hijacking; the legitimate TeamViewer applications loads two functions from this DLL; the legitimate version of which is a part of Windows. However, the presence of the malicious version allows an attacker to take control of the TeamViewer application.

This particular campaign targeted users in Italy for a month, ample time to gather all of a victim's usernames and passwords. The presence of a Trojanized TeamViewer version raises the possibility that a newer version may exist in the wild and account for some of the recent attacks.

One more thing to note is that the TeamViewer administrators *may* be able to limit the damage of old versions. All TeamViewer connections are initially mediated by company servers. It may be possible for connections from these unsupported versions to be disconnected at this handshake stage, preventing any malicious use from progressing. It would unfortunately also cut out any users of these old versions.

Trend Micro endpoint solutions such as Trend Micro™ Security, Smart Protection Suites, and Worry-Free™ Business Security can protect users and SMBs from this threat by detecting malicious files, and spammed messages as well as blocking all related malicious URLs. On the other hand, our Trend Micro Deep Discovery has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs. The following hashes are related to this attack:

- 0660CADEF21D2061E776E4BCAA6AA4FB48A778BE
- 14ABFE0FC2F84EB42177BE430AF72A291850F486
- 1AC5E11A48AA2162C6CD175403C7BFAF497000C0
- 3580F6974CBC30F6FC1C668EE2FEE6ED0C796B03
- 411ED021388DA1DA572529BA5AD6073761992800
- 47F539B76BEBE683B3ABEE001AE0605EC1ED4F25
- 4A2A77EB7B7C323E7F68ACF91014EC135C7B020F
- 4D68BE91DEE6291F3086F50599BBFF0DAF1B6509
- 5D47CD2D12DC6FDD49E2C14DFBDDBA17035A27B6
- 7CB82E53D9E803D2B5C98841E30411AD75C4866A
- 836446903F97A38EC4720299BA9D99CBAAFB31CE
- 8AD8A31A44FB65C6B3557F0A3AB9024B87994C0F
- 9521E5BDFE8EE780DE04979FDB450873227D7867
- 96C3BB27C89FC9C4ACF7AD9F89C3E06CF4F033F3
- 98D63628220AC630DFD0FD1033914473DB1D7306
- 9D9F80A1100914F5083DE5040B1B71C6EAD2DCF0
- AC5F7D9312BDAE4F82615333F939F92C78995F83
- B204D3EE95E83793EB9D3B1ACF89FB6726B6315F
- BFE8F9FEC531CF6D8AA23BD6B3B9ED85E46003E2
- C69A19298CAED379A1063593ACA25A0432E4D0FE
- E841CE2EF5847A87131EA1D9CBA135ED92D68E82
- F08BF9D0B028005090434983D78624D048CFBF42
- F2EC9C134AE52418DC6251FA7D2EF6E4F86C39CC

Tags

Malware | Endpoints | Research