Trickbot Shows Off New Trick: Password Grabber Module

blog.trendmicro.com/trendlabs-security-intelligence/trickbot-shows-off-new-trick-password-grabber-module

November 1, 2018

Trickbot, which used to be a simple banking trojan, has come a long way. Over time, we've seen how cybercriminals continue to add more features to this malware. Last March, Trickbot added a new module that gave it increased detection evasion and a screen-locking feature. This month, we saw that Trickbot (detected by Trend Micro as TSPY_TRICKBOT.THOIBEAI) now has a password grabber module (pwgrab32) that steals access from several applications and browsers, such as Microsoft Outlook, Filezilla, WinSCP, Google Chrome, Mozilla Firefox, Internet Explorer, and Microsoft Edge. Based on our telemetry, we saw that this Trickbot variant has affected users mainly in the United States, Canada, and the Philippines.

Analyzing Trickbot's modules

Malware authors continue to cash in on Trickbot's modular structure — its ability to continually update itself by downloading new modules from a C&C server and change its configuration make for a malware that's ripe for updating. To gain a better understanding of this threat, we analyzed Trickbot's different modules, starting with the new *pwgrab32* module that we saw this month.

pwgrab32 module

Trickbot’s new module, called pwgrab32 or PasswordGrabber, steals credentials from applications such as Filezilla, Microsoft Outlook, and WinSCP.

Figure 1. A screen capture of Trickbot’s new module, pwgrab32, in an affected system

Figure 2. A screen capture of the new module’s code that steals FTP passwords from FileZilla

Figure 3. A screen capture of the new module’s code that steals Microsoft Outlook credentials

Figure 4. A screen capture of Trickbot harvesting passwords from open-source FTP WinSCP

Aside from stealing credentials from applications, it also steals the following information from several popular web browsers such as Google Chrome, Mozilla Firefox, Internet Explorer, and Microsoft Edge:

- Usernames and Passwords
- Internet Cookies
- Browsing History
- Autofills
- HTTP Posts

Figure 5. A screen capture of Trickbot’s code that is structured to steal passwords from popular web browsers

It should be noted that this Trickbot variant is not capable of stealing passwords from third-party password manager applications. We are studying this malware further to see if it is able to steal passwords from password managers that have browser plugins.

shareDll32 module

Trickbot uses the shareDll32 module to help propagate itself throughout the network. It connects to a C&C server http[:]//185[.]251[.]39[.]251/radiance[.]png to download a copy of itself and save it as setuplog.tmp.

Figure 6. Trickbot’s shareDll32 module allows it to connect to a C&C server to download a copy of itself

Figure 7. The downloaded file is saved as *setuplog.tmp*

The shareDll32 module then enumerates and identifies systems connected on the same domain using *WNetEnumResource* and *GetComputerNameW*.

Figure 8. Screen capture of code that enumerates and identifies connected systems using WNetEnumResourceW and GetComputerNameW

The file *setuplog.tmp* is then copied in the administrative shares of the discovered machines or systems.

Figure 9. A screenshot of setuplog.tmp copied in the administrative shares

To make the malware more persistent, it has an auto-start service that allows Trickbot to run whenever the machine boots. This service can have the following display names:

- Service Techno
- Service_Techno2
- Technics-service2
- Technoservices
- Advanced-Technic-Service
- ServiceTechno5

wormDll module

The wormDll32 module attempts to identify servers and domain controllers in the network using NetServerEnum and LDAP queries. Trickbot’s worm-like propagation capability was first observed by security researchers from Flashpoint in 2017.

Figure 10. Screen capture of code that identifies workstations and servers in a domain using NetServerEnum

Figure 11. Screen capture of code that identifies domain controllers in a network using LDAP queries

Figure 12. Screen capture of code that identifies machines which are not domain controllers in a network using LDAP queries

We also discovered that there is a possible SMB protocol implementation using “pysmb,” utilizing the NT LM 0.12 query for older Windows operating systems and IPC shares. It should be noted that this function seems to still be in development.

Figure13. Screen capture of code showing possible SMB communication

networkDll32

Trickbot uses this encrypted module to scan the network and steal relevant network information. It executes the following commands to gather information on the infected system:

Figure 14. Screen capture of the commands executed by the networkDll32 module to gather network information

Wormdll32 module

Wormdll32 is an encrypted module that Trickbot uses to propagate itself via SMB and LDAP queries. It is used together with the module “wormDll” to propagate across the network.

importDll32 module

This module is responsible for stealing browser data such as browsing history, cookies, and plug-ins, among others.

systeminfo32 module

Once successfully installed in a system, Trickbot will gather system information such as OS, CPU, and memory information, user accounts, lists of installed programs and services.

mailsearcher32 module

This module searches the infected system’s files to gather email addresses for information-stealing purposes. Collecting email addresses for spam campaign-related needs is usual malware behavior, however, Kryptos Research recently reported that the Emotet banking trojan doesn't just steal email addresses; it also harvests emails sent and received via Microsoft Outlook on an Emotet-infected device. Emotet, according to previous research by Brad Duncan, is also responsible for delivering this password-grabbing Trickbot variant, as well as Azorult, to users.

injectDll32 module

This encrypted module monitors websites that banking applications might use. It's also used to inject code into its target processes using the *Reflective DLL Injection* technique.

The injectDll32 monitors banking-related websites for two different credential-stealing methods:

First, when a user logs in to any of the monitored banking websites on its list such as Chase, Citi, Bank of America, Sparda-Bank, Santander, HSBC, Canadian Imperial Bank of Commerce (CIBC), and Metrobank, Trickbot will then send a POST response to the C&C server to extract the user’s login credentials.

Second, Trickbot monitors if a user accesses certain banking-related websites on its list, such as C. Hoare & Co bank, St. James’s Place Bank, and Royal Bank of Scotland, and will redirect users to fake phishing websites.

The banking URLs Trickbot monitors include websites from the United States, Canada, UK, Germany, Australia, Austria, Ireland, London, Switzerland, and Scotland.

Trickbot’s other notable tricks

Trickbot is usually sent via malicious spam campaigns. The malware disables Microsoft’s built-in antivirus Windows Defender by executing certain commands and modifying registry entries. Additionally, it also terminates Windows Defender-related processes such as MSASCuil.exe, MSASCui.exe, and antispyware utility *Msmpeng.exe*. It also has an autostart mechanism (Msntcs) that is triggered at system startup and every ten minutes after it is first executed.

It disables the following anti-malware services:

- MBamService (Malwarebytes-related Process)
- SAVService (Sophos AV-related process)

Its anti-analysis capability checks the system and terminates itself when it finds certain modules, such as pstorec.dll, vmcheck.dll, wpespy.dll, and dbghelp.dll.

Defending against Trickbot’s tricks: Trend Micro solutions

Malware authors continue to update banking trojans like Trickbot and Emotet with new modules that make it more difficult to detect and combat. Users and enterprises can benefit from protection that use a multi-layered approach to mitigate the risks brought by threats like banking trojans.

Trend Micro Smart Protection Suites provide a cross-generational blend of threat defense techniques to protect systems from all types of threats, including banking trojans, ransomware, and cryptocurrency-mining malware. It features high-fidelity machine learning on gateways and endpoints, and protects physical, virtual, and cloud workloads. With capabilities like web/URL filtering, behavioral analysis, and custom sandboxing, XGen security protects against today's threats that bypass traditional controls; exploit known, unknown, or undisclosed vulnerabilities; either steal or encrypt personally identifiable data; or conduct malicious cryptocurrency mining. Smart, optimized, and connected, XGen security powers Trend Micro's suite.

Indicators of Compromise

Trickbot C&C servers

- 103[.]10[.]145[.]197:449
- 103[.]110[.]91[.]118:449
- 103[.]111[.]53[.]126:449
- 107[.]173[.]102[.]231:443
- 107[.]175[.]127[.]147:443
- 115[.]78[.]3[.]170:443
- 116[.]212[.]152[.]12:449
- 121[.]58[.]242[.]206:449
- 128[.]201[.]92[.]41:449
- 167[.]114[.]13[.]91:443
- 170[.]81[.]32[.]66:449
- 173[.]239[.]128[.]74:443
- 178[.]116[.]83[.]49:443
- 181[.]113[.]17[.]230:449
- 182[.]253[.]20[.]66:449
- 182[.]50[.]64[.]148:449
- 185[.]66[.]227[.]183:443
- 187[.]190[.]249[.]230:443
- 190[.]145[.]74[.]84:449
- 192[.]252[.]209[.]44:443
- 197[.]232[.]50[.]85:443
- 198[.]100[.]157[.]163:443
- 212[.]23[.]70[.]149:443
- 23[.]226[.]138[.]169:443
- 23[.]92[.]93[.]229:443
- 23[.]94[.]233[.]142:443
- 23[.]94[.]41[.]215:443
- 42[.]115[.]91[.]177:443
- 46[.]149[.]182[.]112:449
- 47[.]49[.]168[.]50:443
- 62[.]141[.]94[.]107:443
- 68[.]109[.]83[.]22:443

- 70[.]48[.]101[.]54:443
- 71[.]13[.]140[.]89:443
- 75[.]103[.]4[.]186:443
- 81[.]17[.]86[.]112:443
- 82[.]222[.]40[.]119:449
- 94[.]181[.]47[.]198:449

TSPY_TRICKBOT.THOIBEAI:

806bc3a91b86dbc5c367ecc259136f77482266d9fedca009e4e78f7465058d16