

TrickBot Group Launches Test Module Alerting on Fraud Activity

advanced-intel.com/post/trickbot-group-launches-test-module-alerting-on-fraud-activity

July 11, 2020



BY VITALI KREMEZ



Warning



You see this message because the program named grabber gathered some information from your browser...



- Jul 11, 2020
-
- 2 min read

Executive Summary

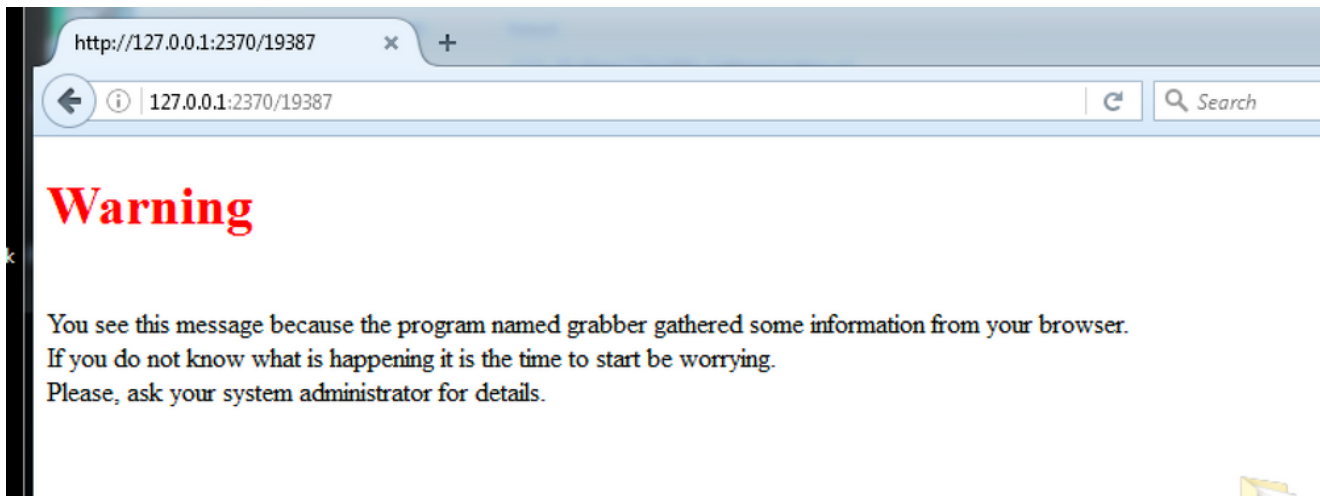
- On July 10, 2020, according to Advanced Intelligence's Vitali Kremez, it was revealed that sandboxed TrickBot banking malware activity related to the distribution group_tag "chil48" loaded a rather newer mysterious test module, known as "grabber.dll".

- The module version "0.6.8" is meant for browser stealer activity affecting Google Chrome, Internet Explorer, Mozilla Firefox, Microsoft Edge as well as browser cookies. The module immediately alerted the victim machine of the fraud by opening the browser with the alert message.
- Advanced Intelligence assesses with high confidence that this module was likely a test module deployed mistakenly alerting on the malware activity during the testing phase.
- Possible recommendations and mitigation steps include immediate disconnect and forensic investigation of the affected machines.

Background

On July 10, 2020, according to Advanced Intelligence's Vitali Kremez, it was revealed that sandboxed TrickBot banking malware activity related to the distribution group_tag "chil48" loaded a rather mysterious module, known as "grabber.dll". The module version "0.6.8" is meant for browser stealer activity affecting Google Chrome, Internet Explorer, Mozilla Firefox, Microsoft Edge as well as browser cookies.

The signed malware sample that led to the discovery was originally found by MalwareHunterTeam (@malwrhunterteam).



Discovery: New "grabber.dll" Test Module

Strangely enough, the module immediately alerted the victim machine of the fraud by opening the browser with the message:

The malware development module references a plethora of internal C++ code references such as "grabchrome.cpp." The module itself references the usual TrickBot grabber code patterns and functions.

```

.rdata:632FB918 db '</head>',0Ah
.rdata:632FB918 db '<body>',0Ah
.rdata:632FB918 db '<form name="frm" action="marker_" method="post">',0Ah
.rdata:632FB918 db '<textarea id="data" name="values" cols="100" rows="20">',0Ah
.rdata:632FB918 db 0Ah
.rdata:632FB918 db '</textarea><br>',0Ah
.rdata:632FB918 db '<input type="submit" value="send" >',0Ah
.rdata:632FB918 db '</form>',0Ah
.rdata:632FB918 db '<script>ahead();frm.submit()</script>',0Ah
.rdata:632FB918 db '</body>',0Ah
.rdata:632FC318 db '<?DOCTYPE html>',0Ah ; DATA XREF: sub_63254400+4370
.rdata:632FC318 db '<html>',0Ah
.rdata:632FC318 db '<head>',0Ah
.rdata:632FC318 db '</head>',0Ah
.rdata:632FC318 db '<body>',0Ah
.rdata:632FC318 db '<a style="color:red"><h1>Warning</h1></a><br>You see this message
.rdata:632FC318 db 'because the program named grabber gathered some information from
.rdata:632FC318 db 'your browser.<br>If you do not know what is happening it is the
.rdata:632FC318 db 'time to start be worrying.<br>Please, ask your system administrat
.rdata:632FC318 db 'or for details.<br><script></script>',0Ah
.rdata:632FC318 db '</body>',0Ah
.rdata:632FC318 db '</html>',0Ah,0
.rdata:632FC47F align 10h
.rdata:632FC480 db '<!DOCTYPE html>',0Ah ; DATA XREF:
.rdata:632FC480 db '<html>',0Ah
.rdata:632FC480 db '<head>',0Ah
.rdata:632FC480 db '</head>',0Ah
.rdata:632FC480 db '<body>',0Ah
.rdata:632FC480 db 'Grabber attempt.',0Ah
.rdata:632FC480 db '<script>close()</script>',0Ah
.rdata:632FC480 db '</body>',0Ah
.rdata:632FC480 db '</html>',0Ah,0
.rdata:632FC4E9 align 4
.rdata:632FC4EC db '%s (line %d) : %s',0Ah,0 ; DATA XREF: sub_62DCED80+770

```

2020-07-10: TrickBot "grabber.dll" | Fraud Message

Warning
 You see this message because the program named grabber gathered some information from your browser. If you do not know what is happening it is the time to start be worrying. Please, ask your system administrator for details.

.rdata:632FC58F	00000012	C	grabiexplorer.cpp
.rdata:632FEED7	00000010	C	grabfirefox.cpp
.rdata:632FD68A	0000000F	C	grabchrome.cpp
.rdata:633006AC	00000011	C	grabber_temp.edb
.rdata:632FA5F9	00000017	C	grabber_temp.INTEG.RAW
.rdata:6330065F	00000017	C	grabber_temp.INTEG.RAW
.rdata:632FA326	00000008	C	grabber
.rdata:632FA32E	0000000A	C	grab_impl

Notably, the malware contains the detailed verbose functionality prompt:

Assessment: TrickBot Group Distribution Mistake?

Advanced Intelligence assesses with high confidence that this module was likely a test module deployed mistakenly alerting on the malware activity during the testing phase due to the typical TrickBot module code patterns. Based on our assessment, it is hypothesized If developed by an outsider coder, this test module possibly reveals the nature of the TrickBot operations as leveraging coders with hiring coders under the ruse of legitimate anti-malware activity development.

As part of the chain, Advanced Intelligence discovered another rather unusually named module "socksbot.dll." This module is meant for Socks5 proxy activity of the TrickBot chain.

We continue closely monitoring for TrickBot activity and malware distributions.

.rdata:10004180	00000006	C	SOCKS
.rdata:10004188	00000008	C	setconf
.rdata:10004190	00000012	C	Can't load import
.rdata:100041A4	00000014	C	Can't load mswsock2
.rdata:100041BC	00000011	C	Invalid parentID
.rdata:100041D0	00000018	C	Can't create io_service
.rdata:100041E8	00000013	C	Module was started
.rdata:100041FC	00000014	unic...	\\file.exe
.rdata:10004210	0000001D	C	IO error. WSALastError = %lu
.rdata:100042C0	0000000D	C	socksbot.dll

Recommendations & Possible Mitigations

- The immediate disconnect of the affected machine from the network when observed the fraud message as displayed
- Full password reset from browsers for any internal and external assets
- Logged-in session reset to prevent reuse of stolen cookies

Indicators of Compromise (IOCs): grabber.dll (MD5: 57103CAE44BA3FA21804EBC9BF702B1F) socksbot.dll (MD5: 382A62908E86BB1F333EC99B17A38930) TrickBot loader (MD5: 4BE2C925E06F6CABB3D3761B8D3A3D11)