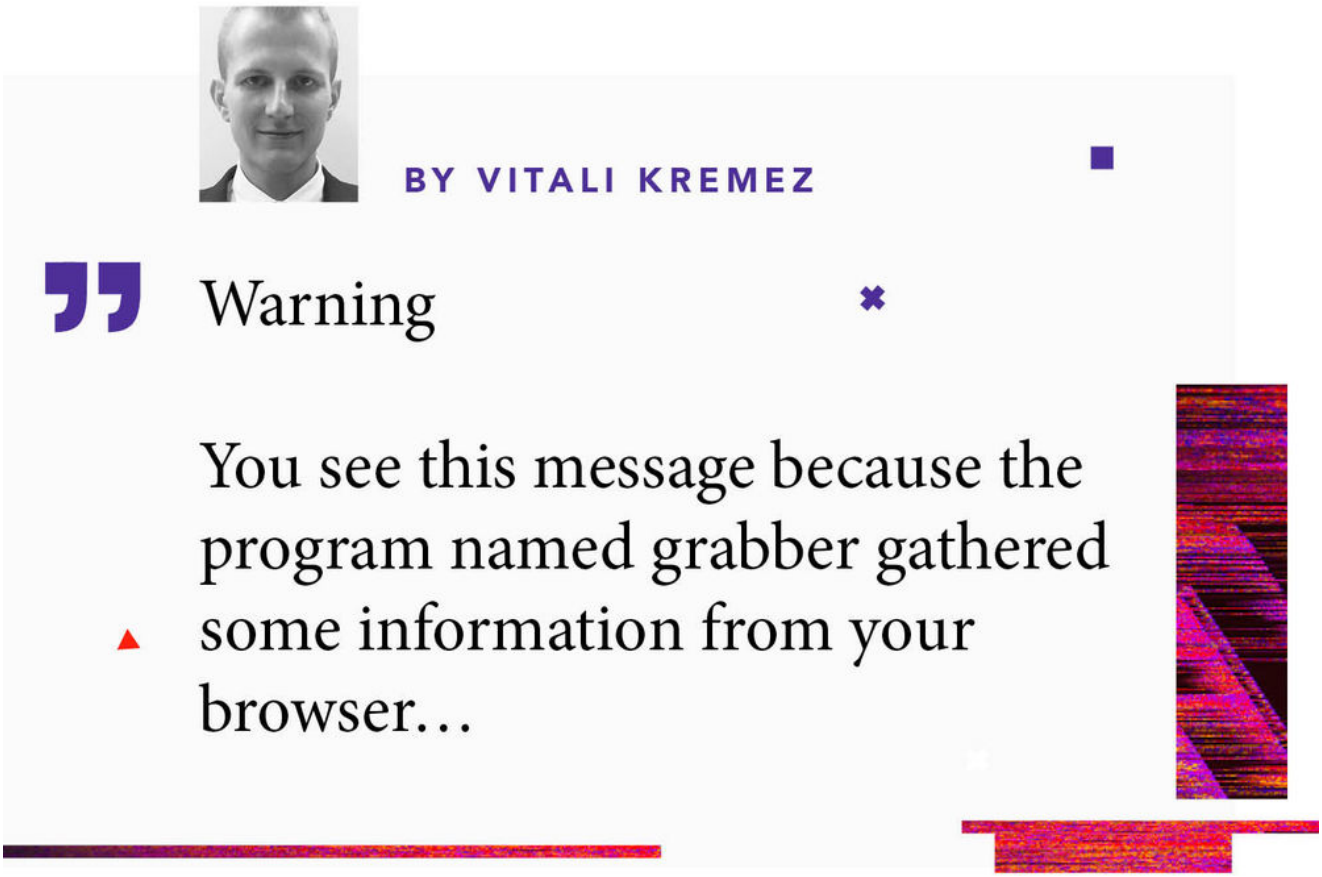
TrickBot Group Launches Test Module Alerting on Fraud Activity

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

July 11, 2020



- Jul 11, 2020
-
- 2 min read

Executive Summary

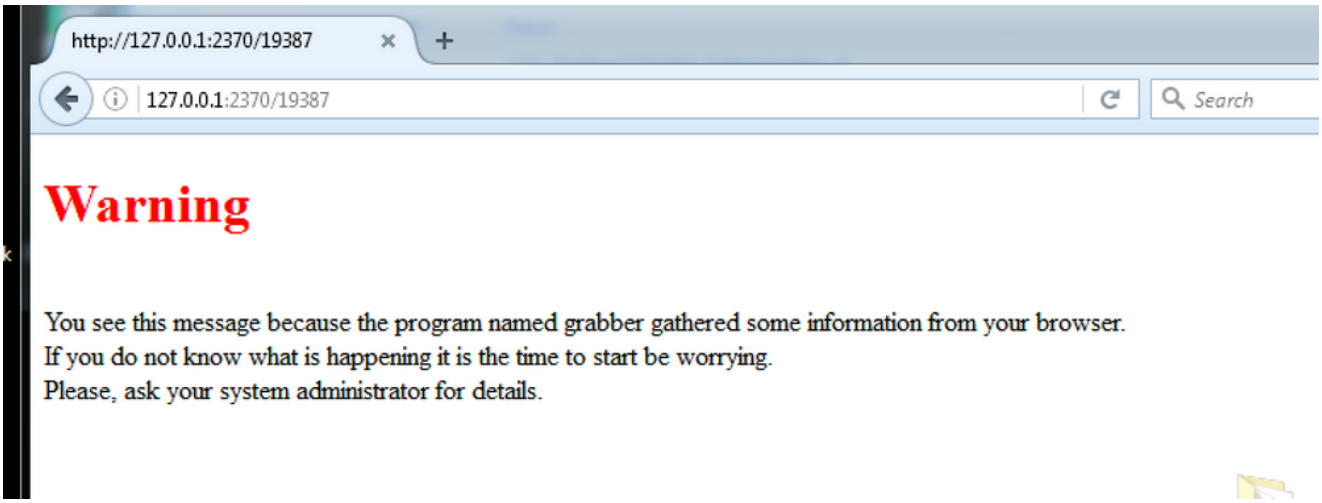
- On July 10, 2020, according to Advanced Intelligence's Vitali Kremez, it was revealed that sandboxed TrickBot banking malware activity related to the distribution group_tag "chil48" loaded a rather newer mysterious test module, known as "grabber.dll".

- 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.

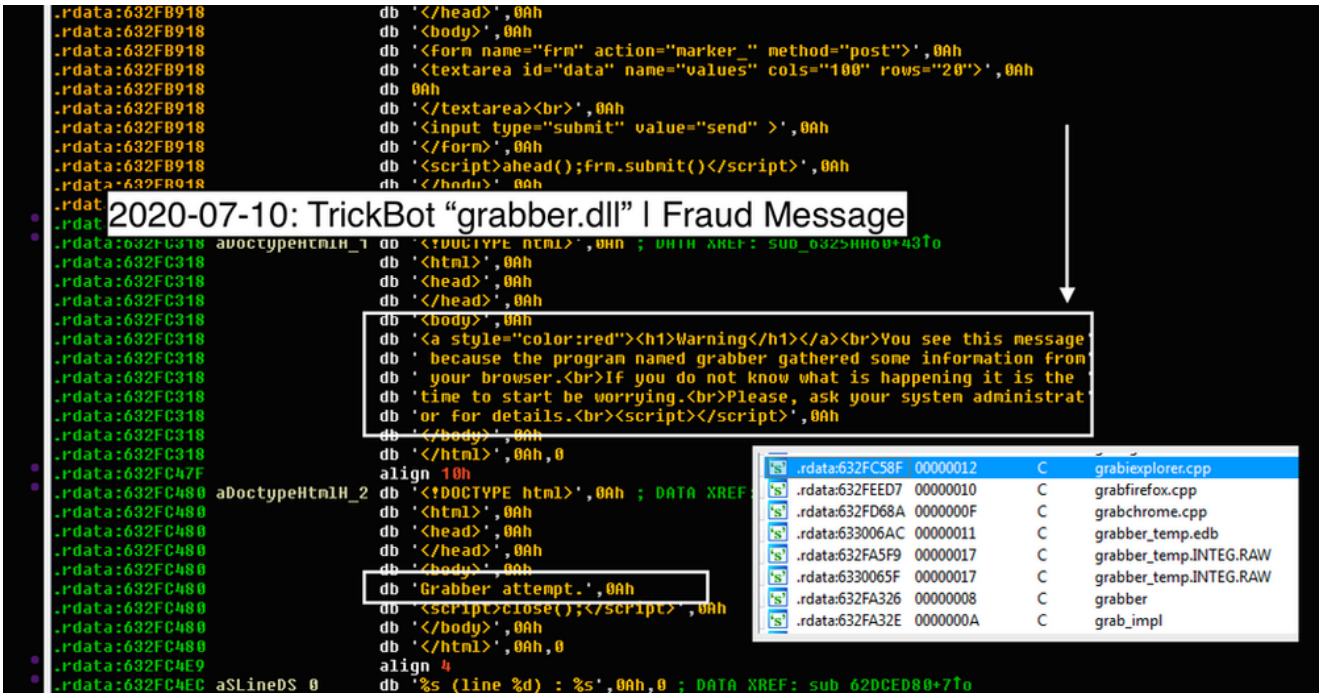
The signed malware sample that led to the discovery was originally found by MalwareHunterTeam (@malwrhunterteam).



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.



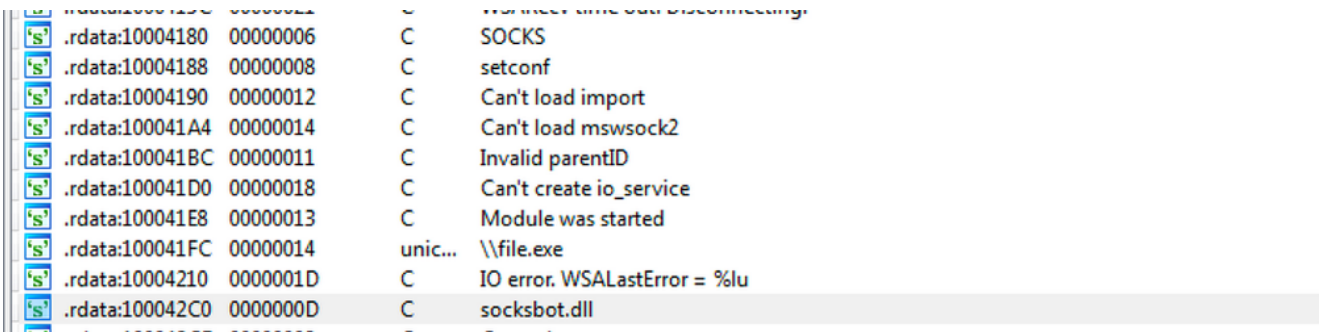
Notably, the malware contains the detailed verbose functionality prompt:

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.



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)