Dyre - No Rest for the Wicked

Julia Karpin, 2015-11-11

Dyre malware requires little introduction as it had been the focus of many publications and it is a well-known threat in the financial malware world.

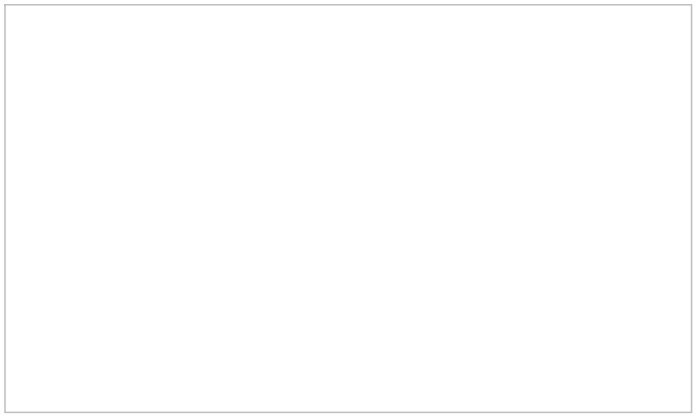
One of the reasons for it being so infamous is the frequent changes the authors incorporate in the code.

Recently, my colleague Gal Shilo and I noticed a few minor changes in Dyre's configuration file.

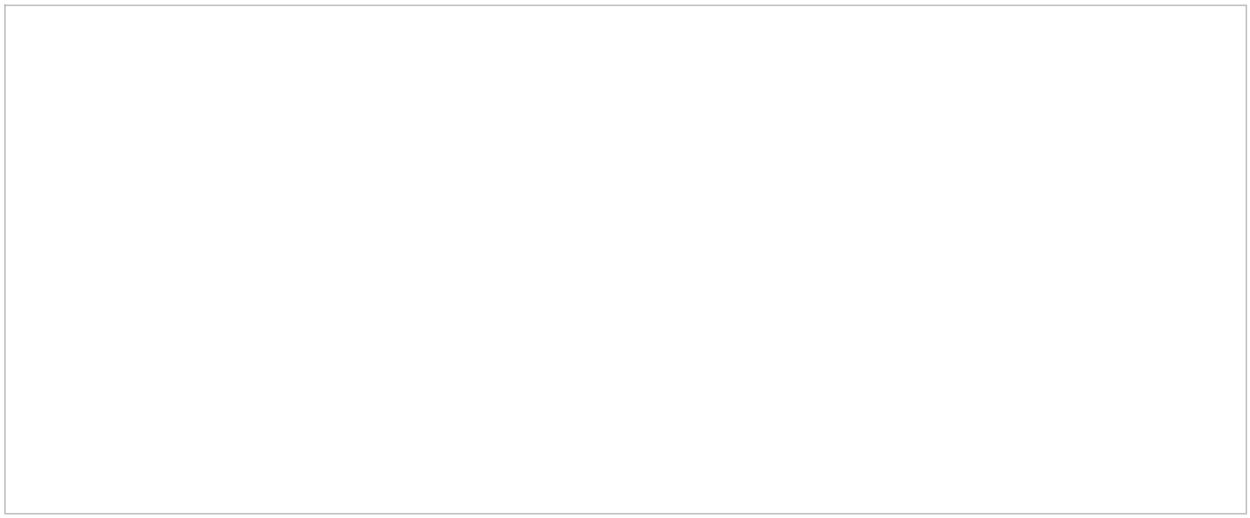
This triggered research that uncovered a significant evolution in the malware's behavior.

Windows 10 and Microsoft Edge Browser are Under Attack

While Windows 10 is gaining momentum, Dyre creators don't miss the opportunity to target the early adopters by also infecting the Edge browser that ships with this OS.



This is an example of the browser injection routine:



Renewed Dyre Commands

Dyre uses a windows pipe for inter-process communication, passing commands from the main module it injects into the "windows explorer" process to other processes. The commands are passed both to browsers launched by the user and stealthy worker-processes launched by the malware itself.

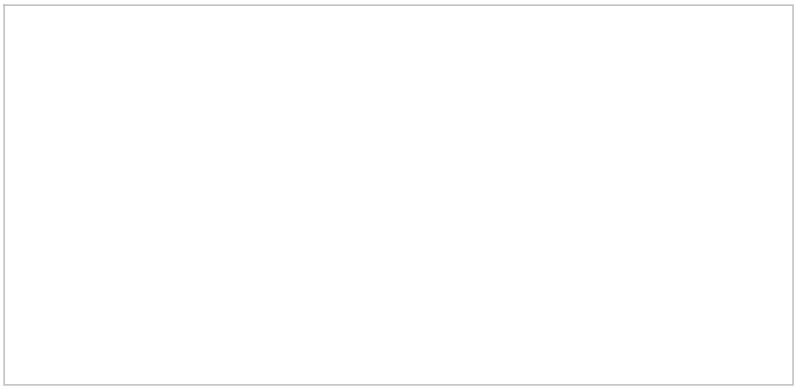
In the new sample, most of the commands discussed in previous F5 research have been replaced and a few new ones have been added, along with new functionality.

- The following is a list of new commands and their functions:
    - 0xF1"lli" – Get the botid name
    - srvv – Get the C&C IP
    - dpsr – Get the data POST server IP
    - grop – Get the botnet name
    - seli – Get the self-IP
    - gcrc – Get the fake pages configuration
    - gcrp – Get the server-side webinjects configuration
    - pngd – Get the account information stolen by the pony module
    - sexe – Among other jobs, it copies the droppee path and its content both to Dyre's special structure and the configuration file on disk. It also tries to get the anti-antivirus module from the C&C.
    - gsxe – Get the droppee path

Additional Protection Layers

Here is a list of new features designed to add protection from removal and detection:

- The pipe's name is no longer hardcoded (e.g. "\\\\.\\pipe\\3obdw5e5w4"). It is now based on a hash of the computer name and windows OS version

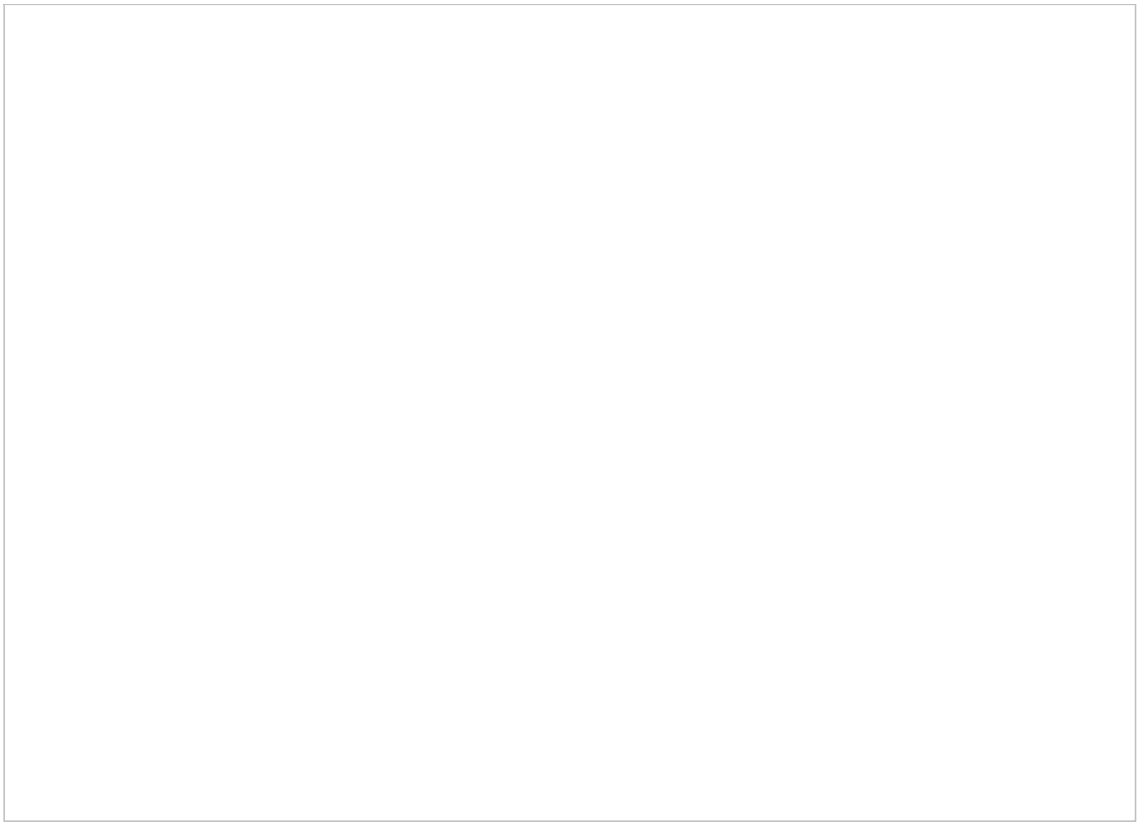


Although the purpose was to make the pipe harder to detect because it is unique per machine, the opposite was accomplished as the name can now be predicted for each machine.

- **Anti-antivirus module** – A new Dyre module dubbed aa32(or aa64 on 64 bit OS) by the malware, was observed. After receiving it from the C&C, it is injected to the "spoolsv.exe" process (the spooler service responsible for fax\print jobs). Its functionality is to locate anti-virus products on the machine and disable their activity (for example, by deleting their files or changing their configurations).

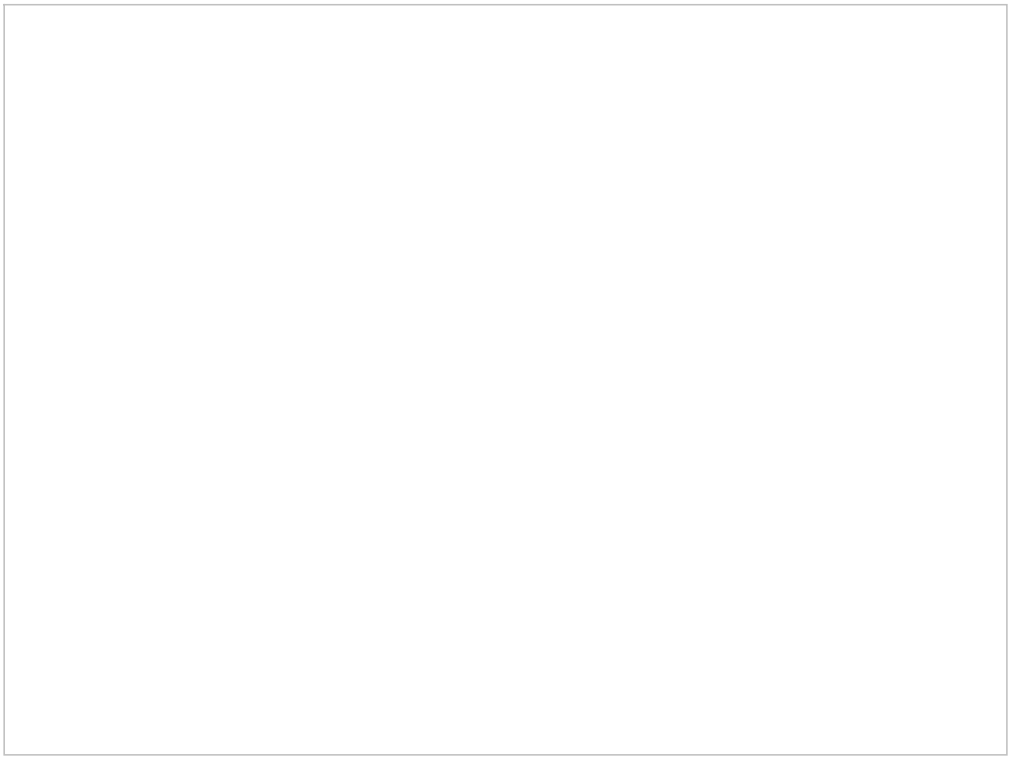
Some of the spotted vendors include: Avira, AVG, Malwarebytes, Fortinet and Trend Micro.

Looking for the product path in the registry:



- **Encrypted strings** – The hardcoded debug strings that used to make analysis much easier are now encrypted. They are decrypted only during runtime, so the static analysis reveals much less than before about the malware's behavior.

- In former versions of the malware, a runkey was set in order to maintain persistency after a reboot. However, in this version, a scheduled task is ran every minute.



- **Disable windows security center**

We conclude from the addition of these features that the authors of the malware strive to improve their resilience against anti-viruses, even at the cost of being more conspicuous. They also wish to keep the malware up-to-date with current OS releases in order to be “compatible” with as many victims as possible. There is little doubt that the frequent updating will continue, as the wicked require very little rest.

Sample MD5: 5f464d1ad3c63b4ab84092d2c1783151

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com