McAfee Labs

Attacks on SWIFT Banking System Benefit From Insider Knowledge

By Christiaan Beek on May 20, 2016

Email

In recent months, we've seen headlines about the compromise of a bank in Bangladesh from which cybercriminals attempted to steal US$951 million. The malware they used was able to manipulate and read unique messages from SWIFT (Society for Worldwide Interbank Financial Telecommunication), as well as adjust balances and send details to a remote control server. BAE Systems wrote a detailed analysis and concluded that the malware must be based on a framework of different modules that could be used for multiple targets.

This week SWIFT sent another warning without details about another bank, this time in Vietnam that was compromised. According to a bank spokesperson, they detected in a timely manner the fraudulent transfer of $1.13 million in December 2015. Because we know the attackers had some insight into the Bangladesh attack, Intel Security assumed the attackers also knew something beforehand about the Vietnamese bank. We investigated possible malware indicators for the latter attack.

Files used for the investigation:

- MD5: 0b9bf941e2539eaa34756a9e2c0d5343
- MD5: 909e1b840909522fe6ba3d4dfd197d93

We focused our analysis primarily on the first sample. The file's compile timestamp is 2015-12-

04 02:04:23. The first submission of the file from Vietnam was on December 22, 2015.

In the case of the Vietnamese bank, the file used for the attack is a fake version of the popular PDF reader Foxit. The malware installs itself in the original Foxit installation directory and renames the original file to FoxltReader.exe.

Once the user starts using the fake reader, the malware executes and writes to a log file in the temp directory C:\\Windows\temp\\WRTU\ldksetup.tmp. Analyzing this file, we see the log data is XOR encoded using the value 0x47.

As in the case of the Bangladeshi bank, the malware uses the configuration file Lmutilps32.dat, which can also be found in C:\\Windows\\temp\WRTU\. This file is also XOR encoded, with the

value 0x7C4D5978.

Was this malware part of a targeted attack? Yes, absolutely. As in the malware used against the Bangladeshi bank, we found the SWIFT code for the target in multiple places in the malware:

The code TPBVVNVX is the SWIFT code for the Tienphong Commercial Joint Stock Bank, in Hanoi.

We also noticed that there were more SWIFT codes in the code:

These banks are based in Australia, Singapore, Japan, Korea, Vietnam, Italy, and the United States. We wondered why the actors would put this particular list in the malware. Further analyzing the working of the malware, we discovered an interesting part in the code concerning ”Executing the real Foxit reader” and the next section in the code states “PDFmodulation success. ...” This hints of the manipulation of PDF files.

In the code, we found that the malware uses the original driver fpdsdk.dll from the Foxit SDK to execute the transformation of the files.

We discovered functionality in the code that converts PDF files to XML files, which are stored in the folder C:\Documents and Settings\Test\Local Settings\Temp\. The filenames start with XXX or RSP followed by a value between 0-F and finish with the extension .tmp.

Let's return to our list of SWIFT codes of other banks. The malware reads the SWIFT messages and checks if the sender of the message is one of the listed banks. Once it finds these messages, it reads their information: