Threat Spotlight: Flokibot PoS Malware

cylance.com/en_us/blog/threat-spotlight-flokibot-pos-malware.html

The BlackBerry Cylance Threat Research Team

RESEARCH & INTELLIGENCE / 03.01.17 / The BlackBerry Cylance Threat Research Team

Introduction

Much has been written in recent years about point-of-sale (PoS) data breaches, most notably attacks against Target in late 2013, Home Depot in mid to late 2014, Wendy's in early 2016 and most recently Arby's in January of this year. Generally, malware used in PoS attacks is designed to identify payment card data residing in memory, then exfiltrate that data to an off-site, attacker controlled server.

Background

According to a 2016 report published by the Federal Reserve, non-cash payments increased in 2016 to an estimated total value of $178 trillion, with an estimated total non-cash payments increase of 5.3 percent per year since 2012. Given these statistics, it is not surprising to learn that there exists a thriving market for stolen payment card information on the dark web.

In a 2015 study, BitGlass discovered that fake financial information they generated and tracked was viewed almost 1,100 times from 22 different countries. Recent reports released by Arbor Networks and Flashpoint mentioned a recent campaign involving PoS malware called Flokibot that has recently targeted endpoints in Brazil, specifically those with

Portuguese language versions of Windows 7 installed. Both reports have excellent breakdowns of the files and attack chain analysis which will not be repeated here.

Testing RAM Scraping Protection

CylancePROTECT® actively blocks RAM scraping techniques used by this type of PoS threat, so the Cylance Threat Guidance Team set out to discover how CylancePROTECT would react to Flokibot in a test environment.

First, a brief introduction to what kind of data is encoded on a credit or debit card. The magnetic stripe on the back of a financial payment card contains three “tracks” of data: Track 1, Track 2 and Track 3 (which is rarely used). Track 1 contains, among other things, the account holder's name, account number, expiration date and CVV number. Track 2 contains much of the same information, except for the account holder's name and some of the other checks, and is ultimately less data over all, while still possessing enough data to generate a fake payment card. This makes the information contained on Track 2 a prime target for attackers. The format of the information contained within Track 2 is illustrated below:


Fig1_Floikibot

Figure 1. Track 2 Data (image by Duo Security: https://duo.com/blog/pos-malware-a-pci-nightmare)

We located a recent sample of Flokibot and copied it into a test environment with CylancePROTECT v1400 installed and online, where it was quarantined pre-execution:


Fig2_Floikibot

Figure 2. Malware Quarantined Pre-execution

Then, we took CylancePROTECT offline and again discovered the same results: the file was quarantined pre-execution, seen below:


Fig3_Floikibot

Figure 3. Malware Quarantined Pre-execution in Offline Mode

It was at this point that we got curious to see what would happen if we removed every protection within CylancePROTECT's arsenal except for Memory Defense. So, we created a test environment with Portuguese language version of 32-bit Windows 7 Professional with CylancePROTECT installed.

There are several websites that allow a user to generate credit card numbers that adhere to the Luhn Algorithm, a checksum formula that is used to validate, among other things, credit and debit card numbers. The team leveraged one of these sites to generate fake credit card numbers for testing:

VISA	**MASTERCARD**
4556920012834452	5341701240865907
4929028434080223	5301666338130225
4532321332286920	5414957219825866
4916294386558609	5181854712024975

These numbers were used to generate strings that adhered to the formatting structure of the information contained on Track 2, an example is shown below:

*;xxxxxxxxxxxxxxxx=yymm120012340000000?**

Where 'x' represents the 16-digit account number and 'yymm' represents the card's expiration date, as year and month.

When the file is executed, it injects explorer.exe and as a result, any credit card number that lies within the memory space of that process should be susceptible to memory scraping by Flokibot. This means that we should be able to generate a string that adheres to the formatting above and enter it into an open Notepad document, then execute the file. The RAM scraping protection built into CylancePROTECT will recognize Track 2 data in memory and trigger an alert.

We disabled all protections in our test environment, except for Memory Defense. The pre-execution setup of the test is shown below (again, note that we are using the Portuguese language version of 32-bit Windows 7 Professional):


Fig4_Floikibot

Figure 4. Pre-execution Setup

At this point, we executed the file. With the properly formatted Track 2 data in memory, we will expect to see the RAM scraping protection trigger an alert when the malware is executed, which is exactly what happens. In the screenshot below, the alert (Violation: TrackDataRead) can be seen:


Fig5_Floikibot

Figure 5. Post-execution, TrackDataRead Violation Alert

Conclusion

This demonstration shows that not only did CylancePROTECT quarantine the threat in both online and offline modes, the RAM scraping protection built within the Memory Defense protection is effective in mitigating Flokibot point of sale malware attacks by recognizing Track 2 payment card data residing in memory. It is important for end users to enable Memory Defense on their endpoints to aid in defending against PoS memory scraping attacks.

If you use our endpoint protection product, CylancePROTECT, you were already protected from this attack. If you don't have CylancePROTECT, contact us to learn how our AI based solution can predict and prevent unknown and emerging threats.

Indicators of Compromise

SHA-256 Hash:

23E8B7D0F9C7391825677C3F13FD2642885F6134636E475A3924BA5BDD1D4852

MD5 Hash:
DCBF3A8BFEC2B5A062F68DE4EEE4B717

C2:
https://extensivee(dot)bid/000L7bo11Nq36ou9cfjfb0rDZ17E7ULo_4agents/gate(dot)php

The BlackBerry Cylance Threat Research Team

About The BlackBerry Cylance Threat Research Team

The BlackBerry Cylance Threat Research team examines malware and suspected malware to better identify its abilities, function and attack vectors. Threat Research is on the frontline of information security and often deeply examines malicious software, which puts us in a unique position to discuss never-seen-before threats.

Back