McAfee Labs Threat Advisory

LusyPOS

June 22, 2018

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.secure.mcafee.com/signup_login.

Summary

LusyPOS is malware that targets point of sale (POS) systems. Upon infection it searches the running processes' memory for bank card numbers. LusyPOS uses the Tor network to securely communicate with its command and control server, which is implemented as a Tor hidden service.

McAfee detects this threat under the following detection name:

- PWS-FBYT!partialMD5

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

Infection and Propagation Vectors

The malware targets only POS systems and as such is not spread via spam or any other mass-spreading mean. It is sold on specialized forums and installed on compromised POS systems.

Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL could be achieved at various layers of McAfee products. Browse the product guidelines available here (click Knowledge Center, and select Product Documentation from the Support Content list) to mitigate the threats based on the behavior described below in the Characteristics and symptoms section.

Refer the following KB articles to configure Access Protection rules in VirusScan Enterprise:

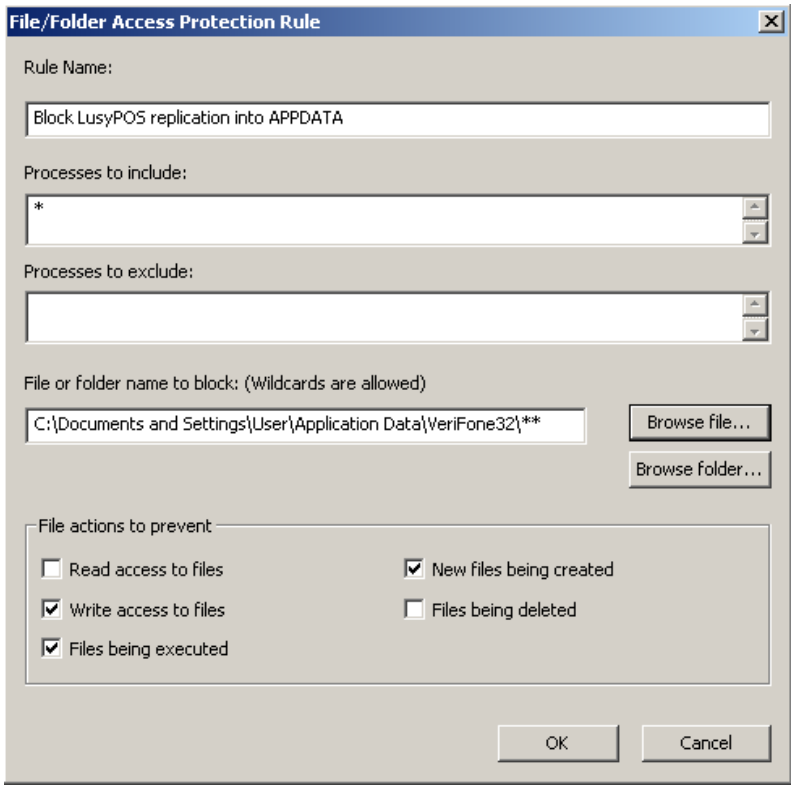
KB81095 - How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Users can configure and test Access Protection Rules to restrict the creation of new files and folders when there are no other legitimate uses.

LusyPOS copies itself into the following folder upon infection:

- <OS drive>:\Documents and Settings\<logged in user>\Application Data\VeriFone32 [Windows XP]
- <OS drive>:\Users\<logged in user>\AppData\Roaming\VeriFone32 [Windows 7]

Users can create an Access Protection Rule to prevent the malware from copying itself into the %APPDATA% folder. The folder to block is one of the aforementioned folders, depending on the Windows version. Checking the checkboxes “Write access to files”, “Files being executed” and “New files being created” will prevent LusyPOS from updating, executing, and installing itself into the %APPDATA% folder.

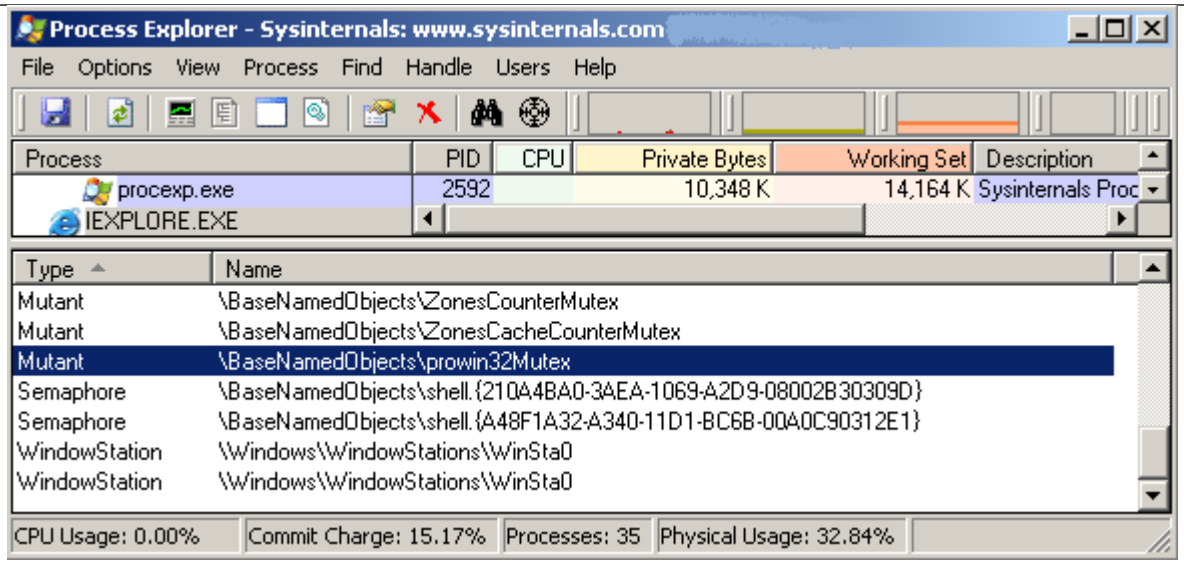


HIPS
To blacklist applications using a Host Intrusion Prevention custom signature refer to KB71329.
To create an application blocking rules policies to prevent the binary from running refer to KB71794.
To create an application blocking rules policies that prevents a specific executable from hooking any other executable refer to KB71794.

*** Disclaimer: Usage of *.* in access protection rule would prevent all types of files from running and being accessed from that specific location. If specifying a process path under “Processes to Include”, the use of wildcards for Folder Names may lead to unexpected behavior. Users are requested to make this rule as specific as possible.

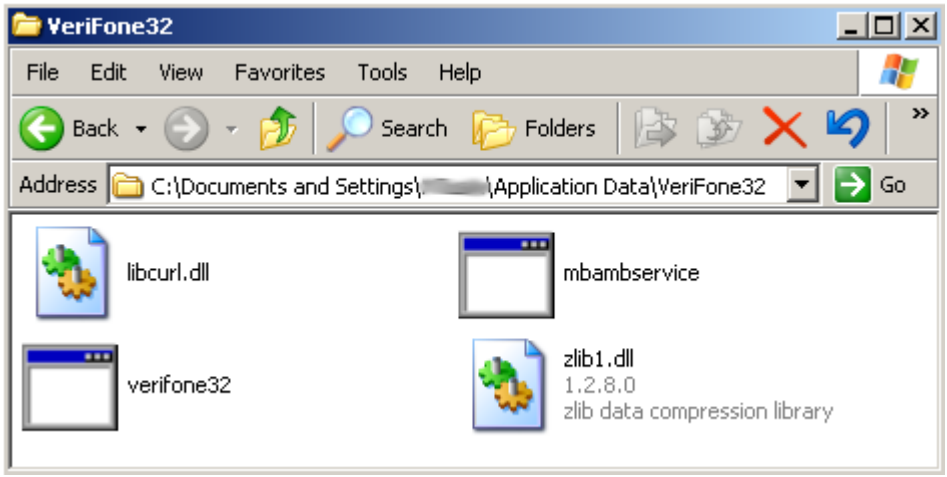
Characteristics and Symptoms

Description
LusyPOS hides itself into an Internet Explorer process and creates a mutex named “prowin32Mutex” to avoid multiple infections. This behavior can be seen on the following screenshot:



The malware copies itself into a directory named “VeriFone32” created into the %APPDATA% folder. Three other files are created into this folder:

- libcurl.dll - a clean library used to handle network operations
- mbambservice.exe - a clean Tor client
- zlib1.dll - a clean data compression library



LusyPOS searches the memory used by running processes for bank card numbers. However it does not scan the following processes:

- mbambservice.exe
- wmiprvse.exe
- LogonUI.exe
- svchost.exe
- iexplore.exe
- explorer.exe
- System
- smss.exe
- csrss.exe
- winlogon.exe
- lsass.exe
- spoolsv.exe
- alg.exe
- wuauclt.exe
- firefox.exe
- chrome.exe
- devenv.exe

For all other processes, LusyPOS retrieves their memory content by calling the Windows API ReadProcess(). This data is then searched for any series of digits whose length would match that of a bank card number.

```
ReadProcessMemory:                      ; CODE XREF: ExtractCa
                mov     [ebp+NumberOfBytesRead], 0
                mov     ecx, dword_408900
                mov     [ebp+lpBuffer], ecx
                lea     edx, [ebp+NumberOfBytesRead]
                push    edx             ; lpNumberOfBytesRead
                mov     eax, [ebp+nSize]
                push    eax             ; nSize
                mov     ecx, [ebp+lpBuffer]
                push    ecx             ; lpBuffer
                mov     edx, [ebp+lpBaseAddress]
                push    edx             ; lpBaseAddress
                mov     eax, [ebp+hObject]
                push    eax             ; hProcess
                call    ds:ReadProcessMemory
                mov     ecx, [ebp+NumberOfBytesRead]
                push    ecx
                mov     edx, [ebp+lpBuffer]
                push    edx
                call    ExtractCardNumbersFromBuffer
```

When a series of digits has been found, LusyPOS checks that it is a valid bank card number by taking advantage of the Luhn algorithm.

```
check_Luhn:                             ; CODE XREF: I
                mov     eax, [ebp+len]
                add     eax, [ebp+card_number_length]
                mov     [ebp+len], eax
                mov     ecx, [ebp+card_number_length]
                mov     [ebp+var_28], ecx
                mov     edx, [ebp+card_number_length]
                push    edx             ; length
                lea     eax, [ebp+card_number]
                push    eax             ; number
                call    IsValidLuhn
```

The malware periodically contacts its command and control server through the Tor network in order to receive new commands. These commands may trigger one of the following actions:

- Download and run a remote file
- Update itself from a remote location
- Delete itself and remove all traces of infection
- Change the time span between two requests to the command and control server
- Change the time span between two memory scans

```
lea     eax, [ebp+download]
push    eax             ; decrypted_string
push    26h             ; string_index
call    decrypt_string  ; download-
add     esp, 8
lea     ecx, [ebp+update]
push    ecx             ; decrypted_string
push    27h             ; string_index
call    decrypt_string  ; update-
add     esp, 8
lea     edx, [ebp+checkin]
push    edx             ; decrypted_string
push    28h             ; string_index
call    decrypt_string  ; checkin:
add     esp, 8
lea     eax, [ebp+scanin]
push    eax             ; decrypted_string
push    29h             ; string_index
call    decrypt_string  ; scanin:
add     esp, 8
lea     ecx, [ebp+uninstall]
push    ecx             ; decrypted_string
push    2Ah             ; string_index
call    decrypt_string  ; uninstall
add     esp, 8
lea     edx, [ebp+val]
push    edx             ; decrypted_string
push    23h             ; string_index
call    decrypt_string  ; &val=
```

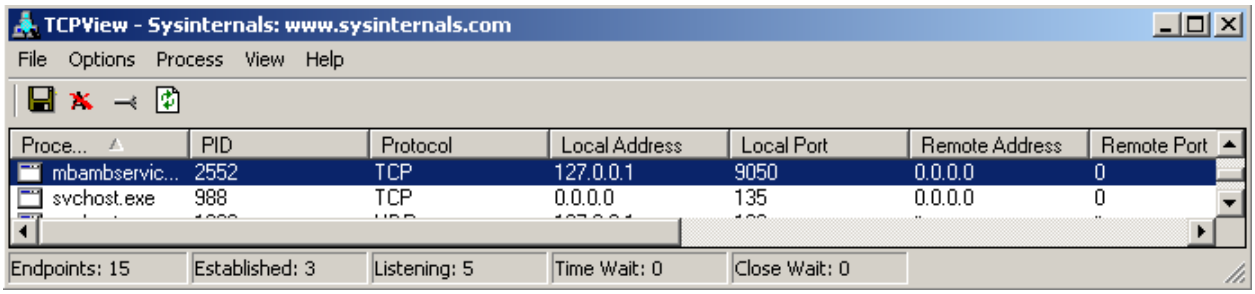
LusyPOS runs several threads in charge of restarting the Tor client if it is stopped and re-infecting the Windows registry if needed.

The malware generates a unique identifier and stores it into the following Windows registry value:

- HKEY_CURRENT_USER\Software\Verifone32\Digitb00 “<unique ID>”

Network Connections

LusyPOS communicates with its server through the Tor network. The Tor client is renamed to mbambservices.exe by the malware and infected machines would have this program listening on local port 9050 which is the default port of the Tor client.



mbambservices initiates multiple outbound TLS connections.

These are some Tor hidden services that LusyPOS has been seen communicating with:

- http://kcdjqxk4jjwzjopq.onion/d/gw.php
- http://ydoapqgxeqmvsugz.onion/d/gw.php

Restart Mechanism

In order to be automatically restarted upon reboot, the malware adds itself into the following Windows registry values:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\VeriFone32
  - "<OS drive>:\Documents and Settings\<logged in user>\Application Data\VeriFone32\verifone32.exe" [Windows XP]
  - "<OS drive>:\Users\<logged in user>\AppData\Roaming\VeriFone32\verifone32.exe" [Windows 7]
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\VeriFone32
  - "<OS drive>:\Documents and Settings\<logged in user>\Application Data\VeriFone32\verifone32.exe" [Windows XP]
  - "<OS drive>:\Users\<logged in user>\AppData\Roaming\VeriFone32\verifone32.exe" [Windows 7]

Indicators of Compromise (IOC)

The following indicators can be used to identify potentially infected machines in an automated way.

The presence of the following process running and listening on local port 9050:

- mbambservices.exe

The presence of the following folder:

- %APPDATA%\VeriFone32

The presence of the following mutex:

- prowin32Mutex

The presence of the following registry value:

- HKEY_CURRENT_USER\Software\Verifone32\Digitb00

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.

McAfee™
Together is power.