New Loki Variant Being Spread via PDF File

blog.fortinet.com/2017/05/17/new-loki-variant-being-spread-via-pdf-file

May 17, 2017

Threat Research

By Xiaopeng Zhang and Hua Liu | May 17, 2017

Background

The Loki Bot has been observed for years. As you may know, it is designed to steal credentials from installed software on a victim's machine, such as email clients, browsers, FTP clients, file management clients, and so on. FortiGuard Labs recently captured a PDF sample that is used to spread a new Loki variant. In this blog, we will analyze how this new variant works and what it steals.

The PDF sample

Figure 1. Content of the PDF sample

The PDF sample only contains one page, shown above, which includes some social engineering content to entice users to download and run the malware.

```
000003d0h: 38 20 30 20 6F 62 6A 0D 3C 3C 2F 54 79 70 65 2F ; 8 0 obj.<</Type/
000003e0h: 41 6E 6E 6F 74 2F 53 75 62 74 79 70 65 2F 4C 69 ; Annot/Subtype/Li
000003f0h: 6E 6B 2F 52 65 63 74 5B 37 32 2E 37 32 20 34 35 ; nk/Rect[72.72 45
00000400h: 39 2E 33 35 39 39 39 20 35 31 32 2E 36 34 30 30 ; 9.35999 512.6400
00000410h: 31 20 37 33 38 5D 2F 42 6F 72 64 65 72 5B 30 20 ; 1 738]/Border[0
00000420h: 30 20 30 5D 2F 43 5B 30 20 30 20 30 5D 2F 46 20 ; 0 0]/C[0 0 0]/F
00000430h: 34 2F 50 20 31 20 30 20 52 2F 41 20 39 20 30 20 ; 4/P 1 0 R/A 9 0
00000440h: 52 2F 48 2F 4E 3E 3E 0D 65 6E 64 6F 62 6A 0D 39 ; R/H/N>>.endobj.9
00000450h: 20 30 20 6F 62 6A 0D 3C 3C 2F 53 2F 55 52 49 2F ;  0 obj.<</S/URI/
00000460h: 55 52 49 28 68 74 74 70 3A 2F 2F 31 39 34 2E 38 ; URI(http://194.8
00000470h: 38 2E 31 30 35 2E 32 30 32 2F 7E 6E 69 6E 6A 61 ; 8.105.202/~ninja
00000480h: 67 72 6F 2F 70 64 66 73 2F 51 55 4F 54 41 54 49 ; gro/pdfs/QUOTATI
00000490h: 4F 4E 2E 65 78 65 29 3E 3E 0D 65 6E 64 6F 62 6A ; ON.exe)>>.endobj
```

Figure 2. Objects inside the PDF sample

According to the sample content (Figure 2), an annotation object in the sample includes an URI action, where the malware is downloaded.

Add itself to Startup folder

When this malware is executed the very first time, it copies itself to “%AppData%\subfolder”, and renames it as “citrio.exe” in my test enviroment. It then creates a VBS file which can start “citrio.exe”. Figure 3 shows its code. The VBS file is added into the system Start Menu so it can automatically run whenever the system starts. After all these actions are complete, “citrio.exe” is started.

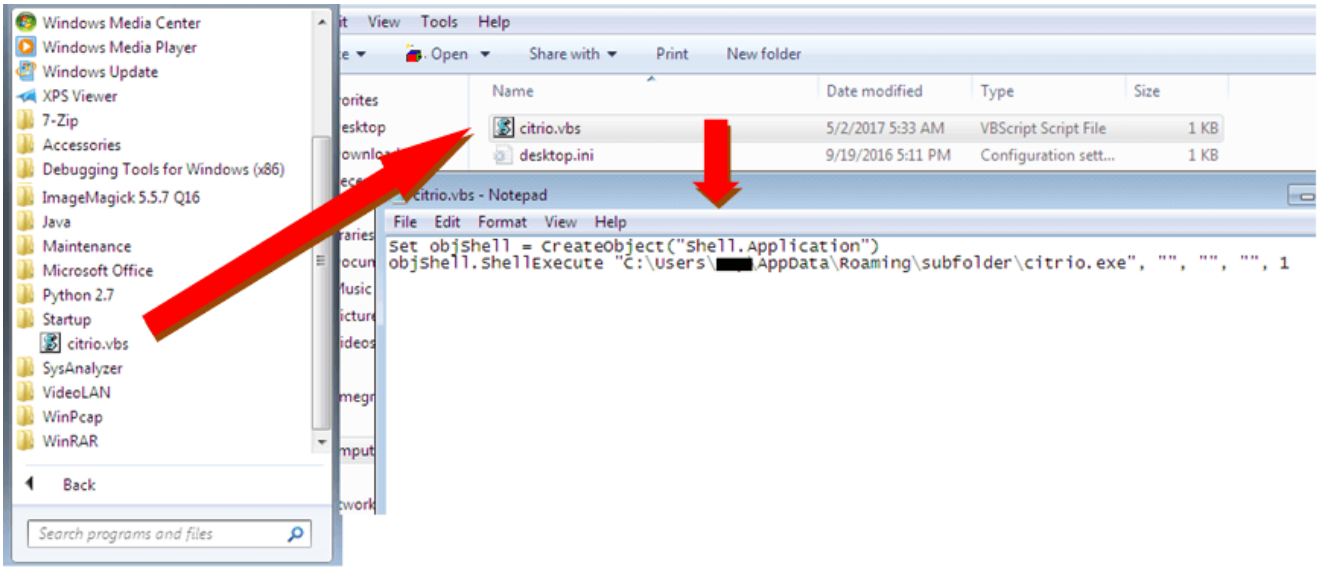

Figure 3. The VBS file in Startup with its code

How the new Loki variant works

All the APIs being called in this malware are hidden, which will be restored before calling. This increases the difficulty for researchers to analyze it. Figure 4 shows an example. After calling the sub_4031E5 function with the hash(C5FA88F1h) and DLL number (0Ah), eax points to the API "CommandLineToArgvW".

```
00:00413838 sub_413838      proc near               ; CODE XREF: st
00:00413838
00:00413838 arg_0           = dword ptr  8
00:00413838 arg_4           = dword ptr  0Ch
00:00413838
00:00413838       push    ebp
00:00413839       mov     ebp, esp
00:0041383B       push    0
00:0041383D       push    0
00:0041383F       push    0C5FA88F1h
00:00413844       push    0Ah
00:00413846       call    sub_4031E5
00:0041384B       push    [ebp+arg_4]
00:0041384E       push    [ebp+arg_0]
00:00413851       call    eax   ;==>CommandLineToArgvW
00:00413853       pop     ebp
00:00413854       retn
00:00413854 sub_413838      endp
```

Figure 4. Restoring the hidden API

The author of the malware has written a number of functions for stealing credentials from a victim's machine. There is an array that is used to store the function pointers. Figure 5 shows part of the function pointers.

```
mov     [ebp+var_19C], 80h
mov     [ebp+var_198], 81h
mov     [ebp+var_194], offset sub_4092CC ; ;;Mozilla Firefox
mov     [ebp+var_190], offset sub_4091F6 ; ;;IceDragon
mov     [ebp+var_18C], offset sub_40C9C2 ; Safari
mov     [ebp+var_188], offset sub_40922A ; ;;K-Meleon
mov     [ebp+var_184], offset sub_409A77 ; Mozilla SeaMonkey
mov     [ebp+var_180], offset sub_40910D ; Mozilla Flock
mov     [ebp+var_17C], offset sub_409046 ; ; NETGATE Black Hawk
mov     [ebp+var_178], offset sub_40929E ; ;Lunascape
mov     [ebp+var_174], offset sub_4070A2 ; Comodo Dragon
mov     [ebp+var_170], offset sub_407D6E ; Opera Next
mov     [ebp+var_16C], offset sub_40C5DF ; QtWeb
mov     [ebp+var_168], offset sub_40C71A ; QupZilla
mov     [ebp+var_164], offset sub_408952 ; ;Internet Explorer
mov     [ebp+var_160], offset sub_40C509 ; ;Opera
mov     [ebp+var_15C], offset sub_4090AA ; 8pecxstudios
mov     [ebp+var_158], offset sub_4094E7 ; Mozilla Pale Moon
mov     [ebp+var_154], offset sub_409CAE ; Mozilla Waterfox
mov     [ebp+var_150], offset sub_40DB78 ; ; IM Pidgin
mov     [ebp+var_14C], offset sub_410676 ; SuperPutty
mov     [ebp+var_148], offset sub_40F44A ; ;FTPShell
mov     [ebp+var_144], offset sub_40F73D ; NppFTP
mov     [ebp+var_140], offset sub_40F6A3 ; oZone3D MyFTP
mov     [ebp+var_13C], offset sub_40F3B3 ; FTPBox
mov     [ebp+var_138], offset sub_410611 ; sherrod FTP
mov     [ebp+var_134], offset sub_40F420 ; FTP Now
mov     [ebp+var_130], offset sub_40F705 ; NexusFile
mov     [ebp+var_12C], offset sub_410CD1 ; NetSarang xftp
mov     [ebp+var_128], offset sub_40ED17 ; EasyFTP
mov     [ebp+var_124], offset sub_410410 ; SftpNetDrive
mov     [ebp+var_120], offset sub_40F49E ; ;AbleFTP
mov     [ebp+var_11C], offset sub_40F561 ; JaSFtp
mov     [ebp+var_118], offset sub_40F4AA ; ;Automize
mov     [ebp+var_114], offset sub_40ECDE ; Cyberduck
mov     [ebp+var_110], offset sub_40F45F ; FullSync
mov     [ebp+var_10C], offset sub_40F3E8 ; FTPInfo
mov     [ebp+var_108], offset sub_40F56D ; LinasFTP
mov     [ebp+var_104], offset sub_40F12F ; ;FileZilla
mov     [ebp+var_100], offset sub_41064C ; Staff-FTP
mov     [ebp+var_FC], offset sub_40E97C ; ;BlazeFtp
mov     [ebp+var_F8], offset sub_40F6E7 ; Fastream NETFile
mov     [ebp+var_F4], offset sub_40F489 ; ;GoFTP
mov     [ebp+var_F0], offset sub_40E8A3 ; Estsoft ALFTP
mov     [ebp+var_EC], offset sub_40F474 ; DeluxeFTP
mov     [ebp+var_E8], eax ; ;;GHISLER
mov     [ebp+var_E4], offset sub_40F3C5 ; FTPGetter
mov     [ebp+var_E0], offset sub_410C98 ; WSFTP
mov     [ebp+var_DC], offset sub_40E8B8 ; ;site.xml
```

Figure 5. Array with function pointers

As you may have noticed, I added the comment behind each function to show you which software it steals credentials from. The malware calls those functions one by one in a loop. Here is the list of most of the software whose credentials can be stolen.

Browser software:

Mozilla Firefox, IceDragon, Safari, K-Meleon, Mozilla SeaMonkey, Mozilla Flock, NETGATE Black Hawk, Lunascape, Comodo Dragon, Opera Next, QtWeb, QupZilla, Internet Explorer, Opera, 8pecxstudios, Mozilla Pale Moon, Mozilla Waterfox.

IM software:

Pidgin.

FTP software:

FTPShell, NppFTP, oZone3D MyFTP, FTPBox, sherrod FTP, FTP Now, NetSarang xftp, EasyFTP, SftpNetDrive, AbleFTP, JaSFtp, Automize, Cyberduck, FTPInfo, LinasFTP, FileZilla, Staff-FTP, BlazeFtp, FTPGetter, WSFTP, GoFTP, Estsoft ALFTP, DeluxeFTP, Fastream NETFile, ExpanDrive, Steed, FlashFXP, NovaFTP, NetDrive, SmartFTP, UltraFXP, FTP Now, FreshFTP, BitKinex, Odin Secure FTP Expert, NCH Software Fling, NCH Software ClassicFTP, WinFtp Client, WinSCP, 32BitFtp, FTP Navigator.

Game software:

Full Tilt Poker, PokerStars.

File manager software:

NexusFile, FullSync, FAR Manager, Syncovery, VanDyke SecureFX, Mikrotik Winbox.

SSH/VNC client software:

SuperPutty, Bitvise BvSshClient, VNC, KiTTY.

Password manager software:

mSecure, KeePass, EnPass, RoboForm, 1Password.

Email client software:

Mozilla Thunderbird, foxmail, Pocomail, IncrediMail, Gmail Notifier Pro, DeskSoft CheckMail, Softwarenetz Mailing, Opera Mail, Postbox email, Mozilla FossaMail, Internet Mail, MS Office Outlook, WinChips, yMail2, Flaska.net Trojita, TrulyMail.

Notes/Todo list software:

To-Do DeskList, Stickies, NoteFly, Conceptworld Notezilla, Microsoft StickyNotes.

Stealing Microsoft Outlook Credentials and Stickies Pictures

From the above analysis, it is clear that this new Loki variant is capable of stealing credentials from more than 100 different software tools (if installed.) In this section, we are going to present how it steals the credentials of Microsoft Outlook and pictures from Stickies.

To do this, It goes through three sub-keys (for three different versions) in the system registry to get saved email accounts, email addresses, username, password, SMTP, POP3, IMAP related information, and so on.

The three sub-keys are:

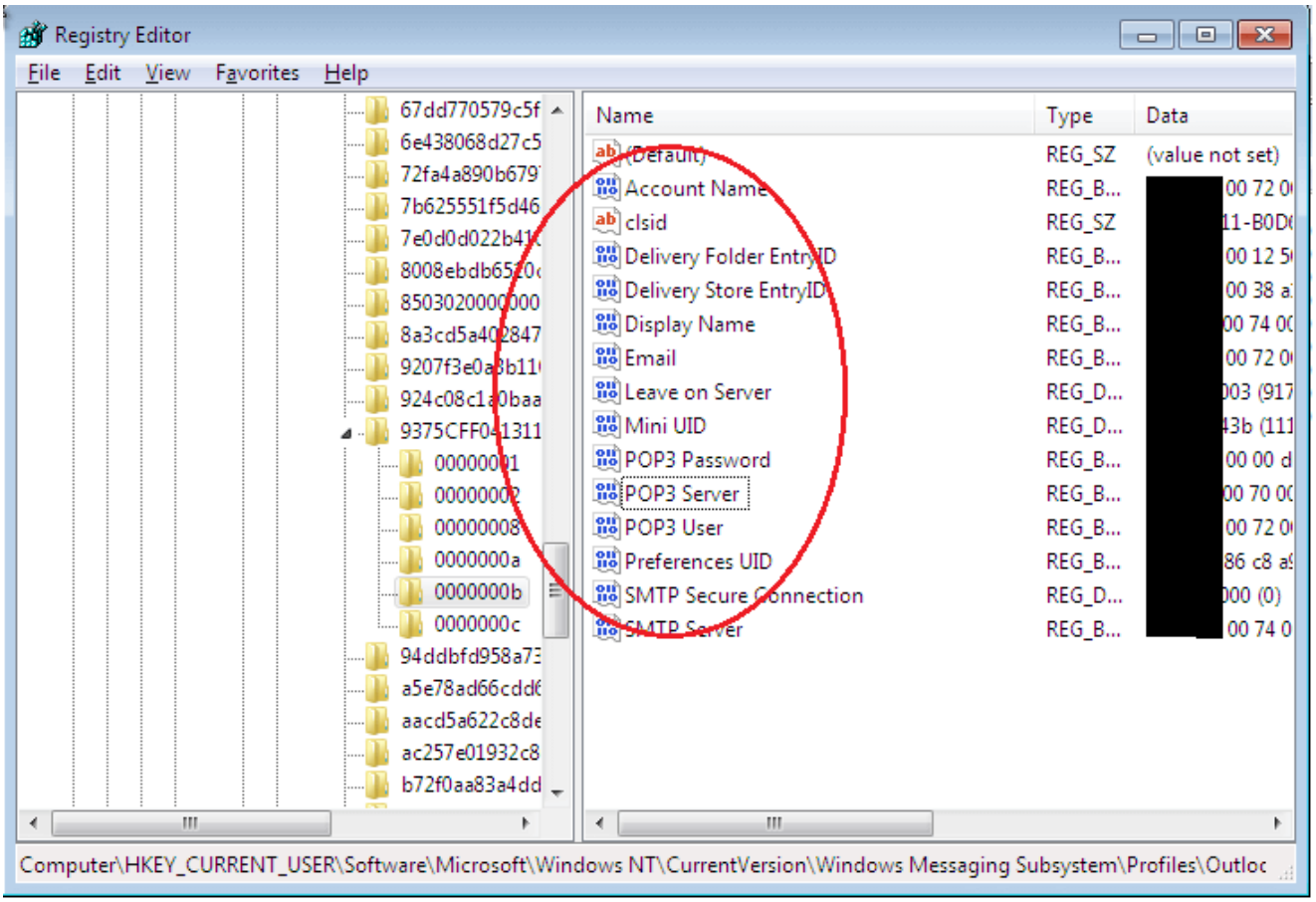

Figure 6. Microsoft Outlook saves credentials in the registry

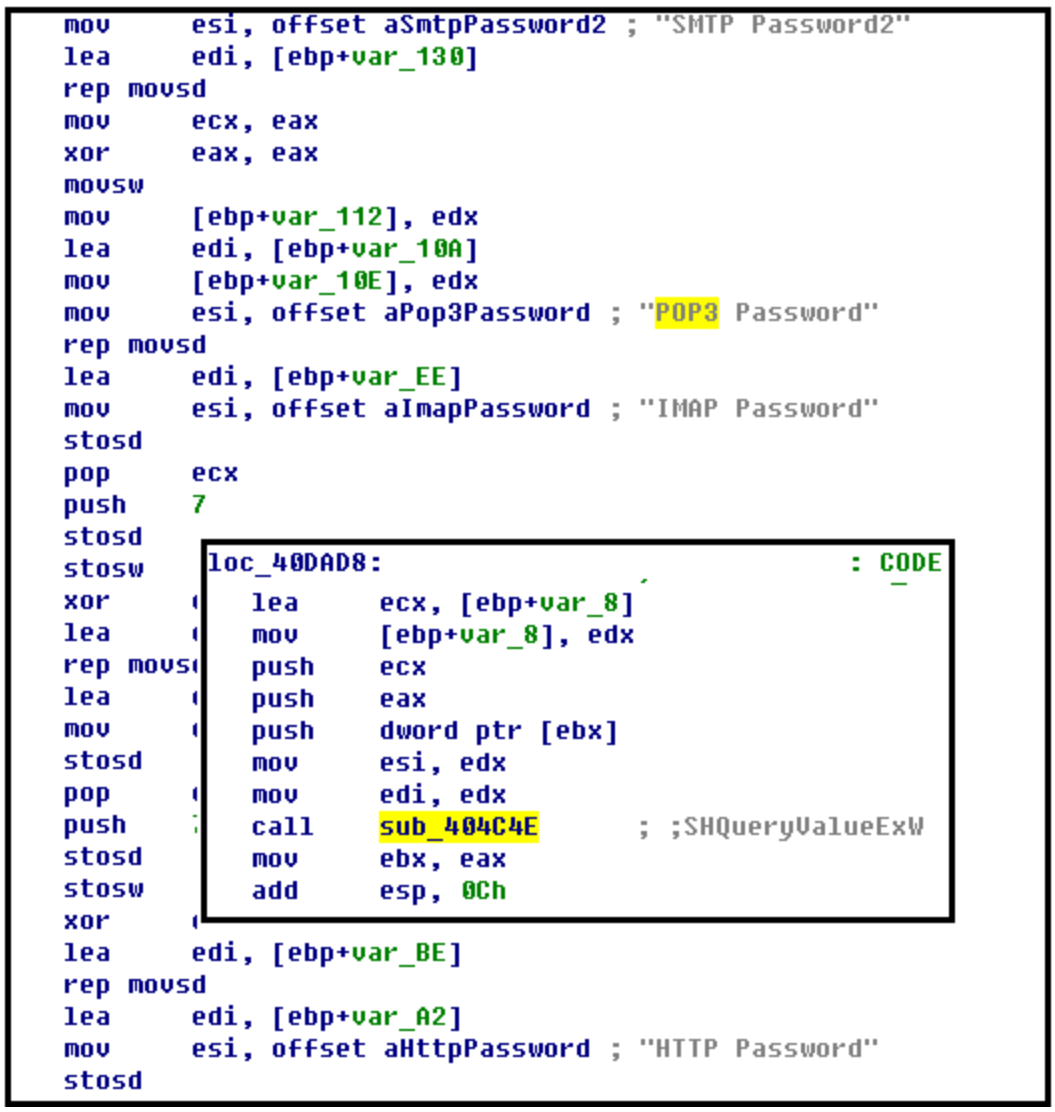

Figure 7. Copying sub-key “POP3 Password”

What you can see in the above figures are the Outlook credentials in the system registry of my test enviroment. The malware is able to read them from here by calling the API “SHQueryValueExW”. All stolen information is stored in a global buffer. See Figure 8.

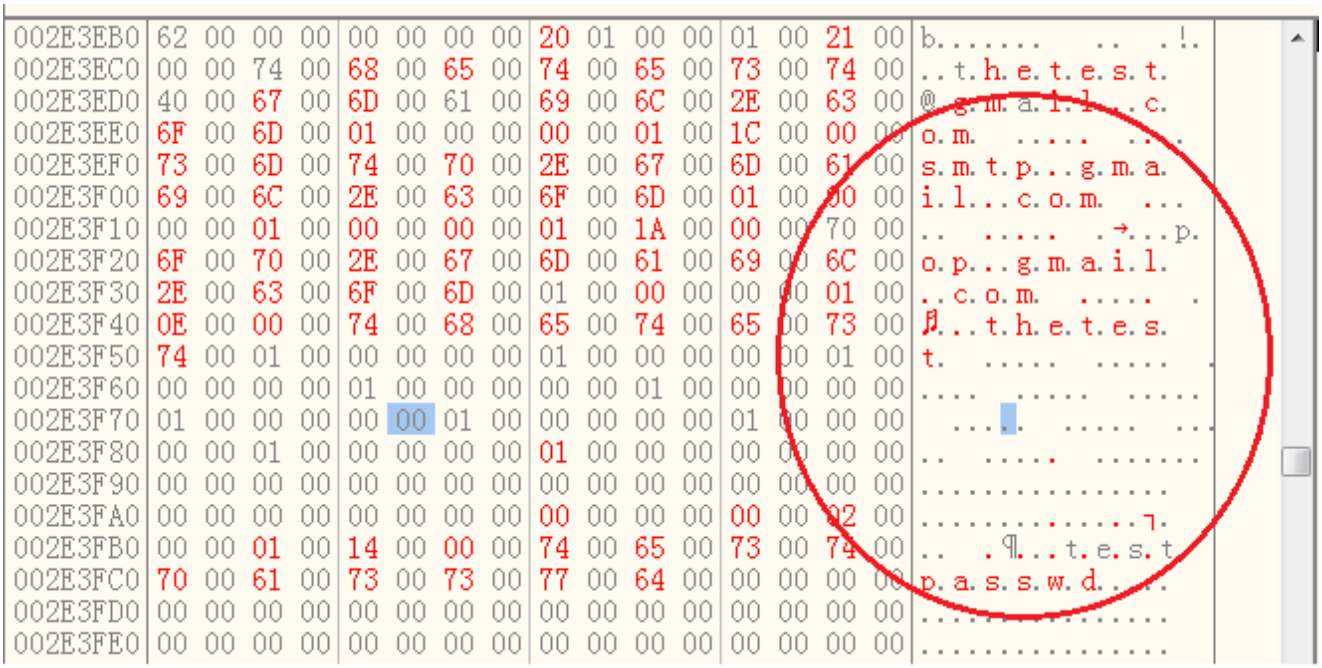

Figure 8. Stolen Outlook credentials in global buffer

For the Stickies attack, since I didn't have that software installed I simply modified my test machine to simulate that it was installed. Here we go.

Figure 9 shows part of the code for Stickies. It gets the strings "*.png", "*.rtf", "%s\stickies\images" dynamically created before using. The malware steals png and rtf files from the sub-folders "\stickies\images" and "\stickies\rtf" in several system directories, such as %AppData%, %UserProfile%.

```
004110CB   push    eax
004110CC   mov     [ebp+var_2A], di
004110D0   mov     [ebp+var_20], dx ; ;;*.png   %s\stickies\images
004110D4   mov     [ebp+var_1C], cx
004110D8   call    sub_412093      ; ;;go through all directories.
004110DD   push    offset sub_41113E ;read file
004110E2   push    esi
004110E3   push    esi
004110E4   lea     eax, [ebp+var_38]
004110E7   push    eax
004110E8   lea     eax, [ebp+var_18]
004110EB   push    esi
004110EC   push    eax             ; ;;*.rtf %s\stickies\rtf
004110ED   call    sub_412093      ; ;;go through all directories.
004110F2   push    esi
004110F3   push    esi
004110F4   push    ds:dword_49FC64
004110FA   call    sub_413ACA      ; ;;;;write data to global buffer.
004110FF   push    ds:dword_49FC64
00411105   call    sub_405695      ; ;;memset and HeapFree
0041110A   add     esp, 40h
0041110D   xor     eax, eax
0041110F   inc     eax
00411110   pop     edi
00411111   pop     esi
00411112   pop     ebx
```

Figure 9. Code snippet for Stickies

I created a sub-folder “%AppData%\stickies\images” and put a .png file into it. Loki reads the png file into that global buffer behind the Outlook data. It also collects system information from the victim’s machine, such as computer name, user name, processor property, etc. After all collected information is ready, it sends them to its C&C server using a HTTP POST request, the body of which is the data stolen from the victim’s machine. And the data is delivered in a kind of compression format. Figure 10 shows a screenshot of the packet in WireShark.

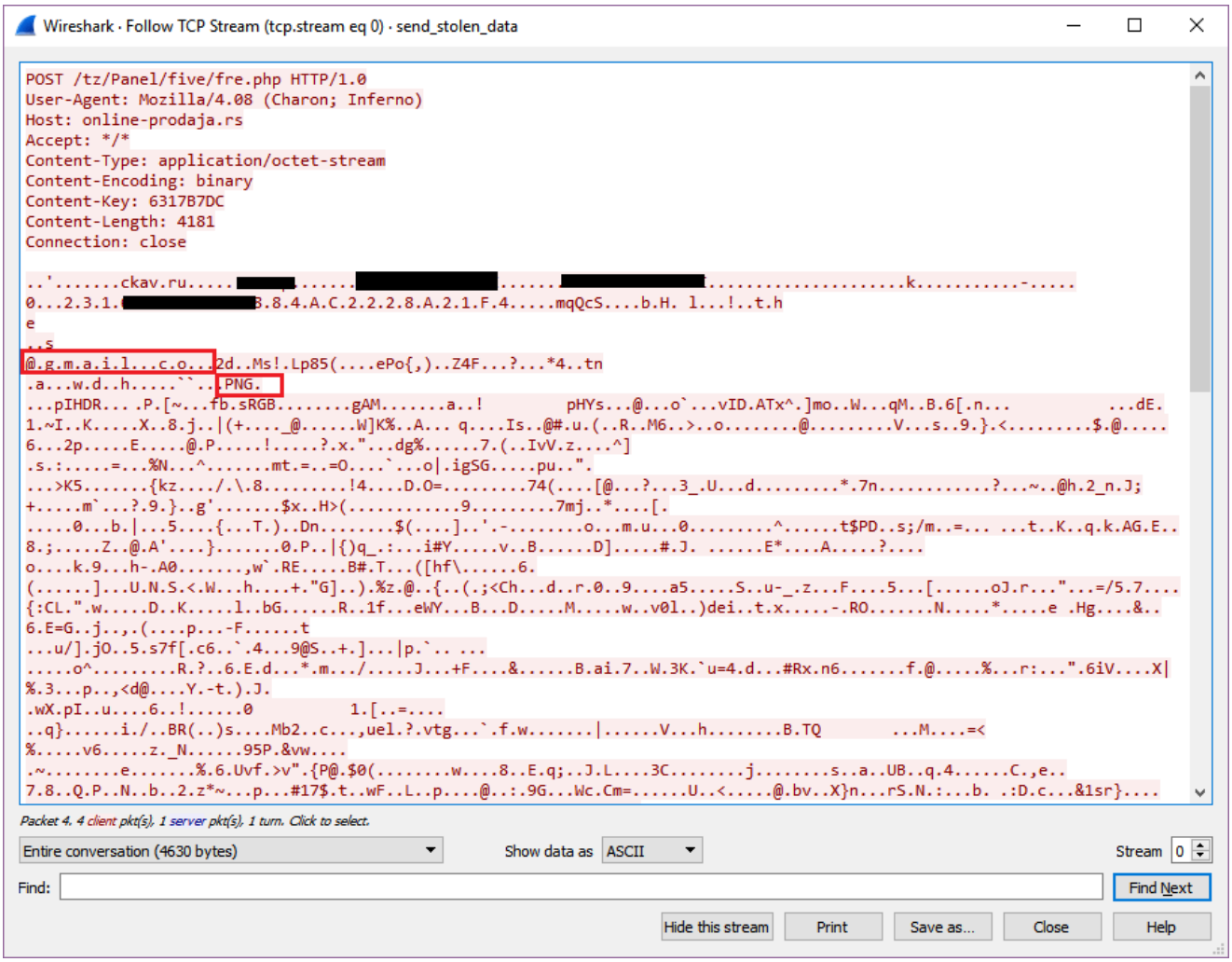

Figure 10. Send the data stolen from Outlook and Stickies to the C&C server

Solution

The URL “194.88.105.202/~ninjagro/pdfs/QUOTATION.exe” has been rated as **Malicious Websites** and “online-prodaja.rs/tz/Panel/five/fre.php” as **Phishing** by the FortiGuard Webfilter service.

The downloaded exe file has been detected as **W32/Injector.DONO!tr** and the PDF file as **Data/Loki_Phish.A!tr** by the FortiGuard Antivirus service.

IoC

URL:

"194.88.105.202/~ninjagro/pdfs/QUOTATION.exe"

"online-prodaja.rs/tz/Panel/five/fre.php"

Sample SHA256:

QUOTATION (1).pdf

E71379A53045385C4AC32E5BE75A04E3D2A9FC7B707FB4478CE90FE689F66D19

QUOTATION.exe

FA417E0B42362C40301750809DF9F0C9BDBF333269F50F74832D4F471358AAED