Stop Malvertising

Analysis of the Predator Pain Keylogger

Written by Kimberly on Sunday, 27 April 2014. Posted in Malware Reports Viewed 11403 times

The **Predator Pain Keylogger** incorporates Browser, Messenger, FTP and File stealers and is able of Clipboard and Screenhot logging, Bitcoin Wallet theft.

Predator Pain targets Steam, MineCraft and World of WarCraft usernames and passwords. A Runescape Pin Stealer is also available.

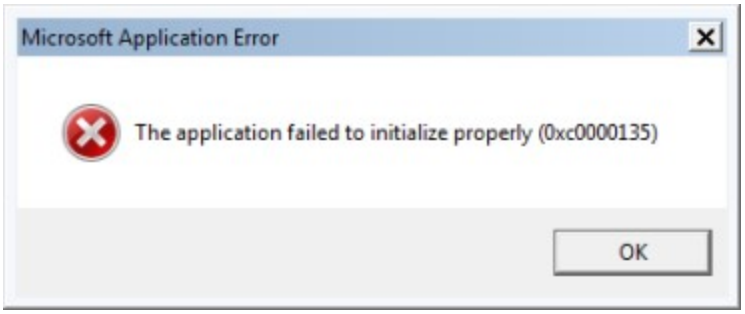
Predator Pain can disable several Windows features and spread via USB or P2P. **KazyLoader**, also known as **Karagany**, is used as the file downloader in this sample.

The Predator Pain Keylogger is advertised for 35$ on underground forums and comes with its own crypter.

Predator Pain is the payload of an unsolicited email from the IRS with the subject line "**Swift Transfer Confirmation**". No money at the horizon in this fake email but a swift transfer of all logins and passwords the Predator Pain Keylogger can possibly grab.

Predator Pain Keylogger

Upon execution SWIFTTRANSFERRECEPTS_FDP.EXE will display an error message stating that the application failed to initialize properly. The warning is a **fake error message** and part of the Predator Pain builder options.



In meanwhile SWIFTTRANSFERRECEPTS_FDP.EXE will create a copy of itself as WINLOGON.EXE in the %AppData%\Roaming folder and start the newly created process. WINLOGON.EXE will also create a global Low Level Keyboard hook and display the same fake error as above.

PID	Process Name	Operation	Path	Result	Detail
1792	swifttransferrecepts_fdp.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Desired Access: Generic Write, R
1792	swifttransferrecepts_fdp.exe	CloseFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	
1792	swifttransferrecepts_fdp.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Desired Access: Generic Write, R
1792	swifttransferrecepts_fdp.exe	QueryAttributeI...	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	FileSystemAttributes: Case Preser
1792	swifttransferrecepts_fdp.exe	QueryBasicInfor...	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	CreationTime: 26/04/2014 12:42:
1792	swifttransferrecepts_fdp.exe	QueryAttributeI...	C:\Users\MxAngel\Desktop\swifttransferrecepts_fdp.exe	SUCCESS	FileSystemAttributes: Case Preser
1792	swifttransferrecepts_fdp.exe	SetEndOfFileInf...	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	EndOfFile: 626,688
1792	swifttransferrecepts_fdp.exe	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\System	SUCCESS	Desired Access: Query Value
1792	swifttransferrecepts_fdp.exe	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Syste...	NAME NOT FOUND	Length: 20
1792	swifttransferrecepts_fdp.exe	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Syste...	NAME NOT FOUND	Length: 20
1792	swifttransferrecepts_fdp.exe	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\System	SUCCESS	
1792	swifttransferrecepts_fdp.exe	ReadFile	C:\Users\MxAngel\Desktop\swifttransferrecepts_fdp.exe	SUCCESS	Offset: 0, Length: 262,144, Priority
1792	swifttransferrecepts_fdp.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Offset: 0, Length: 65,536, Priority:
1792	swifttransferrecepts_fdp.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Offset: 65,536, Length: 65,536
1792	swifttransferrecepts_fdp.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Offset: 131,072, Length: 65,536
1792	swifttransferrecepts_fdp.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Offset: 196,608, Length: 65,536
1792	swifttransferrecepts_fdp.exe	ReadFile	C:\Users\MxAngel\Desktop\swifttransferrecepts_fdp.exe	SUCCESS	Offset: 262,144, Length: 262,144
1792	swifttransferrecepts_fdp.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Offset: 262,144, Length: 65,536
1792	swifttransferrecepts_fdp.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Offset: 327,680, Length: 65,536
1792	swifttransferrecepts_fdp.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Offset: 393,216, Length: 65,536
1792	swifttransferrecepts_fdp.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Offset: 458,752, Length: 65,536
1792	swifttransferrecepts_fdp.exe	ReadFile	C:\Users\MxAngel\Desktop\swifttransferrecepts_fdp.exe	SUCCESS	Offset: 524,288, Length: 102,400
1792	swifttransferrecepts_fdp.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Offset: 524,288, Length: 65,536
1792	swifttransferrecepts_fdp.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	Offset: 589,824, Length: 36,864
1792	swifttransferrecepts_fdp.exe	SetBasicInform...	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	CreationTime: 1/01/1601 10:00:0
1792	swifttransferrecepts_fdp.exe	CloseFile	C:\Users\MxAngel\Desktop\swifttransferrecepts_fdp.exe	SUCCESS	
1792	swifttransferrecepts_fdp.exe	CloseFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	SUCCESS	

Process Name	Operation	Path	Detail
swifttransferrecepts_fdp.exe	Process Create	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	PID: 1628, Command line: "C:\Users\MxAngel\AppData\Roamin...
swifttransferrecepts_fdp.exe	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session ...	Desired Access: Query Value
swifttransferrecepts_fdp.exe	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session ...	Desired Access: Query Value
swifttransferrecepts_fdp.exe	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot...	Desired Access: Query Value, Set Value
swifttransferrecepts_fdp.exe	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot...	Desired Access: Query Value, Set Value
swifttransferrecepts_fdp.exe	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer...	Desired Access: Query Value
swifttransferrecepts_fdp.exe	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\s...	Length: 80
swifttransferrecepts_fdp.exe	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\s...	Type: REG_DWORD, Length: 4, Data: 0
swifttransferrecepts_fdp.exe	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\s...	
swifttransferrecepts_fdp.exe	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer...	Desired Access: Query Value
swifttransferrecepts_fdp.exe	QuerySecurityFile	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	Information: Owner, Group, DACL, SACL, Label
swifttransferrecepts_fdp.exe	QueryBasicInfor...	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	CreationTime: 26/04/2014 12:42:23 PM, LastAccessTime: 26/04...
swifttransferrecepts_fdp.exe	Load Image	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	Image Base: 0x41e0000, Image Size: 0x9c000

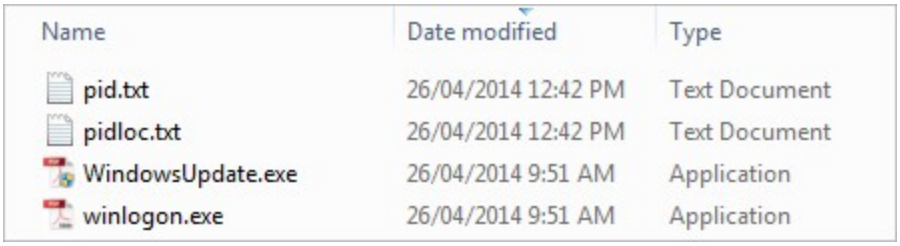
PID	Process Name	Operation	Path	Detail
1628	winlogon.exe	Process Start		Parent PID: 1792, Command line: "C:\Users\MxAngel
1628	winlogon.exe	Thread Create		Thread ID: 596
1628	winlogon.exe	Load Image	C:\Users\MxAngel\AppData\Roaming\winlogon.exe	Image Base: 0x340000, Image Size: 0x9c000

WINLOGON.EXE creates the following files in the %AppData%\Roaming folder:

- **pid.txt**: contains the PID of the Predator Pain Keylogger process - e.g. 1628
- **pidloc.txt**: contains the path to the Predator Pain logger executable - e.g. %AppData%\Roaming\winlogon.exe

PID	Process Name	Operation	Path
1628	winlogon.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\pid.txt
1628	winlogon.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\pid.txt
1628	winlogon.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\pid.txt
1628	winlogon.exe	CloseFile	C:\Users\MxAngel\AppData\Roaming\pid.txt
1628	winlogon.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\pidloc.txt
1628	winlogon.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\pidloc.txt
1628	winlogon.exe	WriteFile	C:\Users\MxAngel\AppData\Roaming\pidloc.txt
1628	winlogon.exe	CloseFile	C:\Users\MxAngel\AppData\Roaming\pidloc.txt

Predator Pain will also create a copy of itself as WINDOWSUPDATE.EXE in the %AppData%\Roaming folder. Predator Pain checks periodically for the existence of WindowsUpdate.exe. If the file is deleted a new copy is written to the HDD.



The following registry keys are created to ensure persistence:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Windows Update"
Type: REG_SZ
Data: C:\Users\MxAngel\AppData\Roaming\WindowsUpdate.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon "Shell"
Type: REG_SZ
Data: explorer.exe, C:\Users\MxAngel\AppData\Roaming\winlogon.exe

Before we go any further there are a few things that need clarification. When the Predator Pain binary - winlogon.exe in our analysis - is running, we can dump the strings contained in the different memory regions. The list is quite huge but for now we will focus on the three following elements:

- **WebBrowserPassView**: WebBrowserPassView.exe
- **Mail PassView**: mailpv.exe
- **CMemoryExecute**: CMemoryExecute.dll

WebBrowserPassView

WebBrowserPassView, developed by Nir Sofer, is a tool to recover lost passwords stored in your web browser.

WebBrowserPassView supports Internet Explorer,Mozilla, Google Chrome, Safari, and Opera and can be used to recover lost / forgotten passwords of any website, including Facebook, Yahoo, Google, and GMail, as long as the password is stored by the browser. The passwords can be saved to text / html / csv / xml files.

Mail PassView

Mail PassView, developed by Nir Sofer, allows extracting lost email passwords from the following email clients:

- Outlook Express
- Microsoft Outlook 2000 (POP3 and SMTP Accounts only)
- Microsoft Outlook 2002/2003/2007/2010/2013 (POP3, IMAP, HTTP and SMTP Accounts)
- Windows Mail
- Windows Live Mail
- IncrediMail
- Eudora

- Netscape 6.x/7.x (If the password is not encrypted with master password)
- Mozilla Thunderbird (If the password is not encrypted with master password)
- Group Mail Free
- Yahoo! Mail - If the password is saved in Yahoo! Messenger application.
- Hotmail/MSN mail - If the password is saved in MSN/Windows/Live Messenger application.
- Gmail - If the password is saved by Gmail Notifier application, Google Desktop, or by Google Talk.

CMemoryExecute - CMemoryExecute.dll

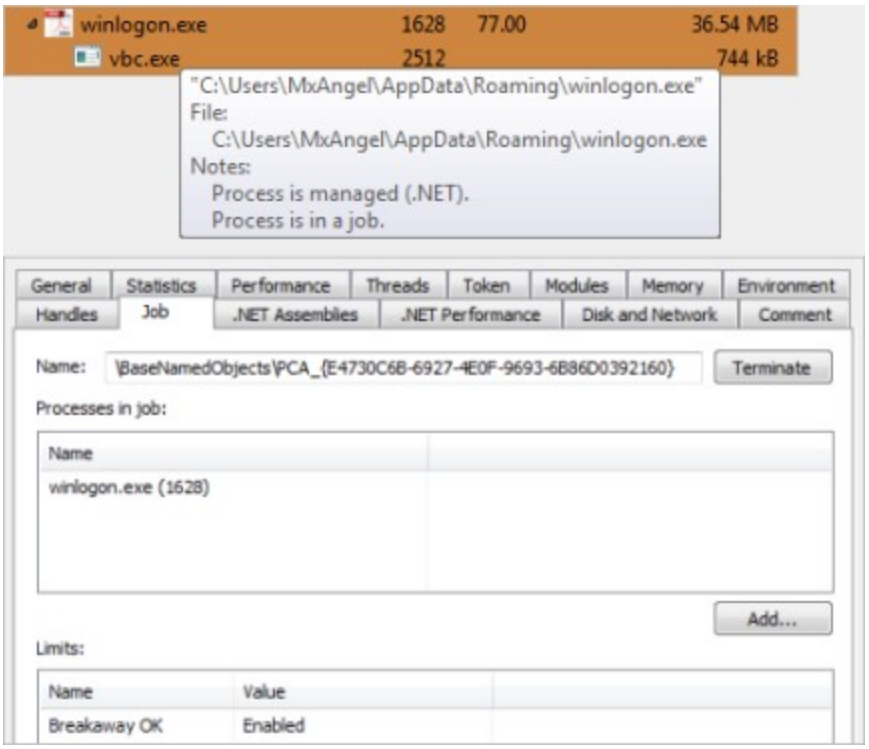
CMemoryExecute, written by **Affixiate**, is used to run a non .NET executable from memory without storing it on the hard-disk first. It uses the native WinAPI and the executable needs to be injected in VBC.EXE, the Visual Basic Command Line Compiler.

The syntax is as follows:

```
CMemoryExecute.Run(IO.File.ReadAllBytes("C:\run_me_in_memory.exe"),
"C:\inject_me_in_memory.exe", "(Optional) Command Line Parameters To Be Passed To
C:\run_me_in_memory.exe")
```

Predator Pain is thus able to harvest logins and passwords from several mail and browser clients with the help of two incorporated legit programs: WebBrowserPassView and Mail PassView.

Predator Pain will start up VBC.EXE, the Visual Basic Command Line Compiler, which is one of the requirements to run a PE from memory.



The Predator Pain Keylogger will:

- Run MAILPV.EXE from memory via VBC.EXE and dump the results to HOLDERMAIL.TXT.
- WINLOGON.EXE checks if HOLDERMAIL.TXT exists.
- WINLOGON.EXE reads HOLDERMAIL.TXT and uploads the harvested email credentials via mail - to This e-mail address is being protected from spambots. You need JavaScript enabled to view it in our analysis.

The same tasks will be performed using WEBBROWSERPASSVIEW.EXE & VBC.EXE to harvest stored passwords in browsers.

Process Name	Operation	Path
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\Mozilla\Profiles
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\Thunderbird\Profiles
vbc.exe	RegOpenKey	HKCU\Software\Qualcomm\Eudora\CommandLine
vbc.exe	RegOpenKey	HKCR\Software\Qualcomm\Eudora\CommandLine\current
vbc.exe	RegOpenKey	HKLM\Software\Mozilla\Mozilla Thunderbird
vbc.exe	CreateFile	C:\Program Files\Mozilla Thunderbird

Credentials saved in browsers are written to holderwb.txt

Process ...	Operation	Path	Detail
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History	Desired Access: Read Attribu
vbc.exe	QueryBasicInf...	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History	CreationTime: 7/01/2010 12:
vbc.exe	CloseFile	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History	
vbc.exe	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\KnownFolderSettings	Desired Access: Query Value
vbc.exe	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\KnownFolderSettings	Desired Access: Query Value
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History	Desired Access: Read Data/
vbc.exe	QueryDirectory	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History*	Filter: *, 1: .
vbc.exe	QueryDirectory	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History	0: ..., 1: desktop.ini, 2: History
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History\History.IE5	Desired Access: Read Data/
vbc.exe	QueryDirectory	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History\History.IE5*	Filter: *, 1: .
vbc.exe	QueryDirectory	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History\History.IE5	0: ..., 1: desktop.ini, 2: index.d
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	Desired Access: Generic Rea
vbc.exe	ReadFile	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	Offset: 0, Length: 32, Priority:
vbc.exe	QueryStandard...	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	AllocationSize: 49,152, EndO
vbc.exe	ReadFile	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	Offset: 20,480, Length: 8
vbc.exe	ReadFile	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	Offset: 20,480, Length: 256
vbc.exe	ReadFile	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	Offset: 20,736, Length: 8
vbc.exe	ReadFile	C:\Users\MxAngel\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	Offset: 20,864, Length: 8

Process ...	Operation	Path	Detail
vbc.exe	CreateFile	C:\Windows\System32\vaultcli.dll	Desired Access: Read Attributes, Disposition: Ope
vbc.exe	QueryBasicInf...	C:\Windows\System32\vaultcli.dll	CreationTime: 14/07/2009 9:37:00 AM, LastAcce
vbc.exe	CloseFile	C:\Windows\System32\vaultcli.dll	
vbc.exe	CreateFile	C:\Windows\System32\vaultcli.dll	Desired Access: Read Data/List Directory, Execut
vbc.exe	CreateFileMap...	C:\Windows\System32\vaultcli.dll	SyncType: SyncTypeCreateSection, PageProtecti
vbc.exe	CreateFileMap...	C:\Windows\System32\vaultcli.dll	SyncType: SyncTypeOther
vbc.exe	Load Image	C:\Windows\System32\vaultcli.dll	Image Base: 0x72540000, Image Size: 0xc000
vbc.exe	CloseFile	C:\Windows\System32\vaultcli.dll	

Process ...	Operation	Path	Detail
vbc.exe	CloseFile	C:\Program Files\Mozilla Firefox	
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\Mozilla\SeaMonkey\Profiles\	Desired Access: Read
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Local\Mozilla\SeaMonkey\Profiles\	Desired Access: Read
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Desired Access: Read
vbc.exe	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\seamonkey.exe	Desired Access: Read
vbc.exe	CreateFile	C:\Program Files\Sea Monkey\nss3.dll	Desired Access: Read
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Local\Google\Chrome\User Data\	Desired Access: Read
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Local\Google\Chrome SxS\User Data\	Desired Access: Read
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\Apple Computer\Preferences\keychain.plist	Desired Access: Read
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\Opera\Opera\wand.dat	Desired Access: Read
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\Opera\Opera7\profile\wand.dat	Desired Access: Read
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\Opera	Desired Access: Read
vbc.exe	CreateFile	C:\Users\MxAngel\AppData\Local\Temp\holderwb.txt	Desired Access: Gener
vbc.exe	WriteFile	C:\Users\MxAngel\AppData\Local\Temp\holderwb.txt	Offset: 0, Length: 2, Pr
vbc.exe	CloseFile	C:\Users\MxAngel\AppData\Local\Temp\holderwb.txt	
vbc.exe	Thread Exit		Thread ID: 2496, User

Below is a screenshot illustrating the flow of processes and services started by Predator Pain. The Protected Storage and Credential Manager services are started by the injected VBC.EXE process.

Message
Process created: swifttransferrecepts_fdp.exe (1792) started by explorer.exe (1944)
Process terminated: dllhost.exe (3948)
Process terminated: dllhost.exe (3988)
Process terminated: swifttransferrecepts_fdp.exe (1792)
Process created: winlogon.exe (1628) started by Unknown Process (0)
Process created: WmiPrvSE.exe (2452) started by svchost.exe (612)
Process created: vbc.exe (2512) started by winlogon.exe (1628)
Service started: ProtectedStorage (Protected Storage)
Process terminated: vbc.exe (2512)
Process created: vbc.exe (2544) started by winlogon.exe (1628)
Process terminated: dllhost.exe (4088)
Process created: dllhost.exe (2328) started by svchost.exe (612)
Service started: VaultSvc (Credential Manager)
Process terminated: vbc.exe (2544)

Besides harvesting various logins and passwords, Predator Pain reports the local Date and Time, the OS and the OS language, the internal and external IP address, installed antivirus and / or firewall. The external IP is obtained by querying whatismyipaddress.com.

In this sample all harvested information is send to This e-mail address is being protected from spambots. You need JavaScript enabled to view it . The interval and the chosen method (FTP / PHP / MAIL) can be set in the Predator Pain builder's options.

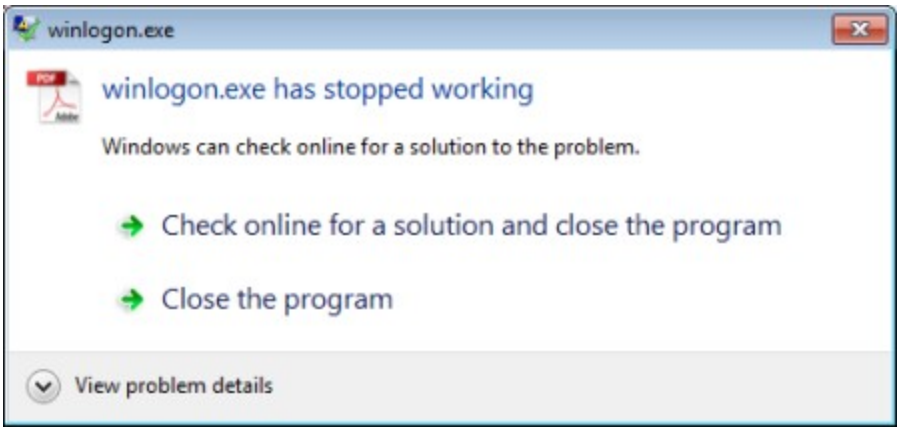
Protocol	Length	Info
DNS	81	Standard query 0xae92 A whatismyipaddress.com
DNS	298	Standard query response 0xae92 A 66.171.248.172

Protocol	Length	Info
DNS	87	Standard query 0x841c PTR 172.248.171.66.in-addr.arpa
DNS	201	Standard query response 0x841c PTR whatismyipaddress.com
DNS	86	Standard query 0xc2a0 A mail.facebookmarketers.net
DNS	163	Standard query response 0xc2a0 CNAME facebookmarketers.net A 65.19.143.222
TCP	66	49166 > smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

Predator Pain is also a Bitcoin Stealer. It steals the WALLET.DAT file that holds the users bitcoin currency.

Process Name	Operation	Path	Result
winlogon.exe	CreateFile	C:\Users\MxAngel\AppData\Roaming\bitcoin\wallet.dat	PATH NOT FOUND
winlogon.exe	Thread Create		SUCCESS
winlogon.exe	Thread Exit		SUCCESS
winlogon.exe	TCP Reconnect	MxAngel-PC:49167 -> 65.19.143.222:smtp	SUCCESS

After a while the WINLOGON.EXE process stopped working. It's hard to tell whether this is on purpose or simply because the logger is unstable.



When the WINLOGON.EXE process runs, the code in memory is unencrypted and its strings can be dumped from the different memory regions. I've posted a small snippet on our Pastebin.

Address	Length	Result	
0x2a138dd	72	This is an email notifying you that	
0x2a13928	262	has ran your logger and emails should be sent to you shortly and at interval choosen. Predator Logger Details: Server Name:	
0x2a13a30	42	Keylogger Enabled:	
0x2a13a5c	56	Clipboard-Logger Enabled:	
0x2a13a96	74	Time Logs will be delivered: Every	
0x2a13ae2	62	minutes Stealers Enabled:	
0x2a13b23	156	Time Log will be delivered: Average 2 to 4 minutes Local Date and Time:	
0x2a13bc1	44	Installed Language:	
0x2a13bef	40	Operating System:	
0x2a13c19	46	Internal IP Address:	
0x2a13c49	46	External IP Address:	
0x2a13c79	48	Installed Anti-Virus:	
0x2a13cab	44	Installed Firewall:	
0x2a13cd9	26	Disablenotify	
0x2a13cf5	60	Predator_Painv13_Notification_	
0x2a13d3d	68	Predator Pain v13 - Server Ran - [	
0x2a13d84	154	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	
0x2a13e2e	22	autorun.inf	
0x2a13e5a	24	open=Sys.exe	USB Spreading.
0x2a13e74	32	action=Run win32	
0x2a13ea6	90	Software\Microsoft\Windows\CurrentVersion\Run	
0x2a13f02	28	Windows Update	
0x2a13f20	28	CMemoryExecute	
0x2a13f46	106	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe	
0x2a13fd2	38	\bitcoin\wallet.dat	
0x2a13ffa	22	_wallet.dat	Bitcoin Stealer
0x2a14012	20	wallet.dat	
0x2a1403a	84	Microsoft.NET\Framework\v2.0.50727\vbc.exe	
0x2a140a2	30	holdermail.txt"	
0x2a140c2	28	holdermail.txt	
0x2a140e1	486	**********	Operating System Intel Recovery ...
0x2a142c9	46	Local Date and Time:	
0x2a142f9	30	Net Version:	
0x2a14319	58	Operating System Platform:	
0x2a14355	56	Operating System Version:	
0x2a14390	466	**********	WEB Browser Password Recovery ...
0x2a14565	468	**********	Mail Messenger Password Recovery ...
0x2a1473c	930	**********	Internet Download Manager Recovery ...

VirusTotal Results

swifttransferrecepts_fdp.exe

Additional information
MD5: 8ce71e40eda2d9304c1e127c60500e0c
SHA1: 93ef97529dcaa047d023456103827b6f97345caf
SHA256: e63b24adf9119f7d500167a62d62d3b8a35f4694f8488fc764523fd322fb2dce
File size: 612.0 KB (626688 bytes)
Detection ratio: 16 / 51
Analysis date: 2014-04-26 08:52:43 UTC

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Zusy.69824	20140426
AegisLab		20140426
Agnitum		20140425
AhnLab-V3	Trojan/Win32.Inject	20140425
AntiVir		20140425
Antiy-AVL		20140426
Avast	Win32:VB-AHWF [Trj]	20140426
AVG		20140426
Baidu-International		20140426
BitDefender	Gen:Variant.Zusy.69824	20140426
Bkav		20140425
ByteHero		20140426
CAT-QuickHeal		20140425

ClamAV		20140426
CMC		20140424
Commtouch		20140426
Comodo		20140426
DrWeb		20140426
Emsisoft	Gen:Variant.Zusy.69824 (B)	20140426
ESET-NOD32	a variant of MSIL/Injector.CUZ	20140426
F-Prot		20140426
F-Secure	Gen:Variant.Zusy.69824	20140426
Fortinet	MSIL/Injector.CSZ!tr	20140426
GData	Gen:Variant.Zusy.69824	20140426
Ikarus		20140426
Jiangmin		20140426
K7AntiVirus		20140425
K7GW		20140425
Kaspersky	Trojan.Win32.Fsysna.zcf	20140426
Kingsoft		20140426
Malwarebytes	Spyware.Zbot	20140426
McAfee	Artemis!8CE71E40EDA2	20140426
McAfee-GW-Edition	Heuristic.LooksLike.Win32.Suspicious.E	20140425
Microsoft		20140426
MicroWorld-eScan	Gen:Variant.Zusy.69824	20140426
NANO-Antivirus		20140426
Norman		20140426
nProtect		20140425
Panda		20140425

Qihoo-360	Win32/Trojan.53c	20140426
Rising		20140425
Sophos		20140426
SUPERAntiSpyware		20140426
Symantec		20140426
TheHacker		20140425
TotalDefense		20140426
TrendMicro		20140426
TrendMicro-HouseCall	TROJ_GEN.F47V0425	20140426
VBA32		20140425
VIPRE		20140425
ViRobot		20140426