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

Marcus Botacin[1], André Grégio[1,2], Paulo Lício de Geus[1]

[1]Instituto de Computação - UNICAMP
{marcus,paulo}@lasca.ic.unicamp.br

[2]Centro de Tecnologia da Informação Renato Archer (CTI)
andre.gregio@cti.gov.br

12 de Novembro de 2015

Tópicos

Tópicos

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]

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]

Objetivos

Objetivos

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

Coleta de dados I

Exemplares

- 2012 a mar/2015.
- 33.811 exemplares totais.
- 21.359 exemplares únicos.

Fontes de Coleta

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

Coleta de dados II

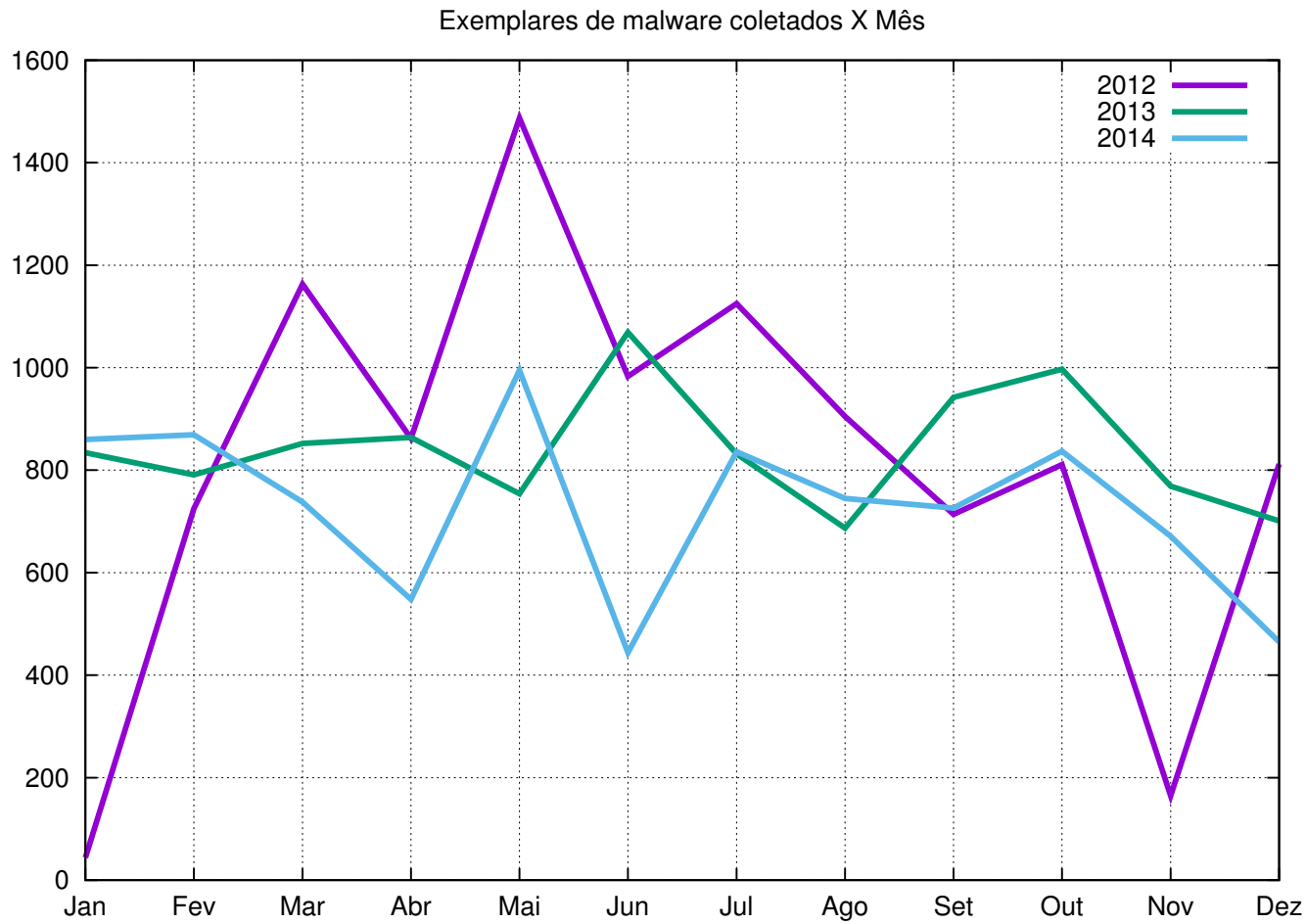


Figura: Coleta de amostras ao longo do período observado.

Análise Estática

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

Metodologia

Análise Dinâmica

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

Tráfego de Rede

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

Tópicos

Tipos de Arquivo

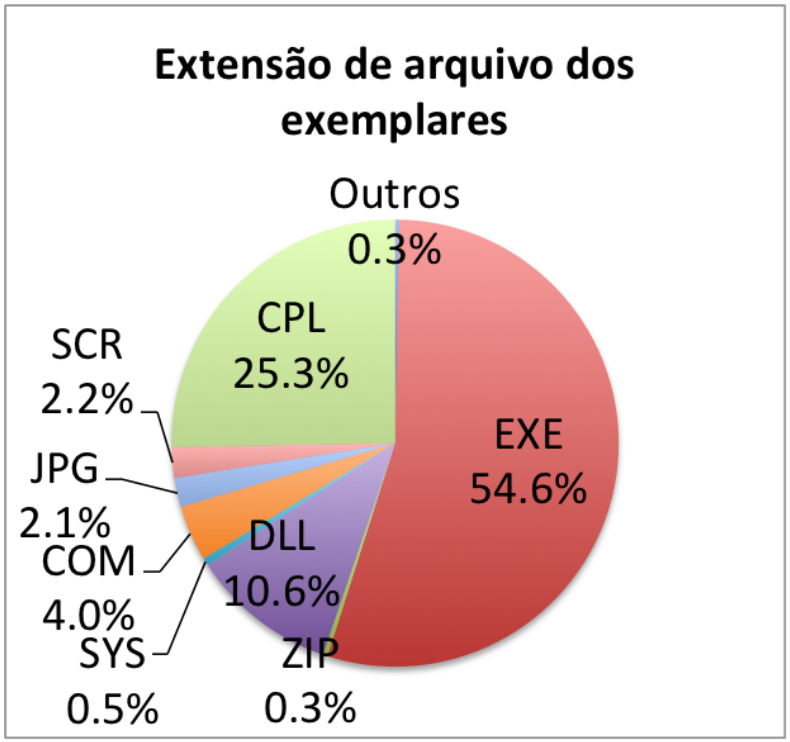


Figura: Distribuição por extensão.

Figura: Distribuição por tipo de arquivo.

Tipos de Arquivo

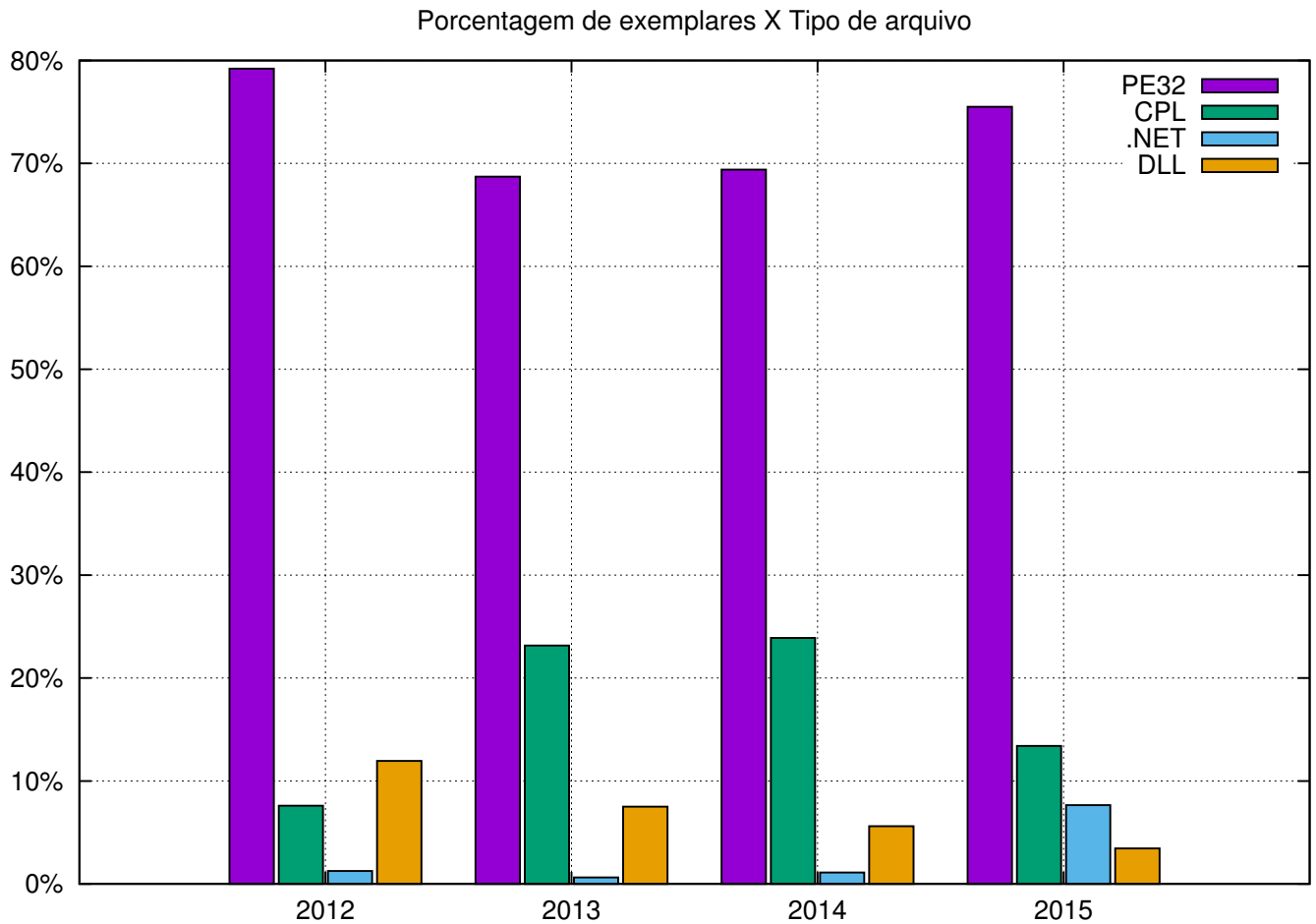


Figura: Evolução dos tipos de arquivo.

Chamadas de Função

Tabela: Chamadas de função mapeadas estaticamente.

Função	# Exemplares	Função	# Exemplares
GetProcAddress	17317 (81,08%)	RegOpenKeyExA	7599 (35,58%)
LoadLibraryA	16713 (78,25%)	LoadLibraryExA	7045 (32,98%)
VirtualAlloc	15032 (70,38%)	ExitThread	6916 (32,38%)
VirtualFree	15007 (70,26%)	FindResourceA	6216 (29,10%)
Sleep	11812 (55,30%)	GetCurrentProcess	5983 (28,01%)
WriteFile	11545 (54,05%)	VirtualProtect	5448 (25,51%)
UnhandledExceptionFilter	11049 (51,73%)	WinExec	5111 (23,93%)
GetTickCount	9977 (46,71%)	CreateFileW	4910 (22,99%)
CreateThread	9214 (43,14%)	**SetWindowsHookExA**	4883 (22,86%)
GetCurrentProcessId	8521 (39,89%)	**IsDebuggerPresent**	3511 (16,44%)
GetWindowThreadProcessId	8142 (38,12%)	**InternetCloseHandle**	4405 (20,62%)
GetCommandLineA	7659 (35,86%)	**InternetReadFile**	3777 (17,68%)

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)ranco**
2012	49,28%	34,97%
2013	56,59%	*ND*
2014	59,96%	37,53%
2015 (1^o trim.)	51,62%	*ND*

Ofuscação

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

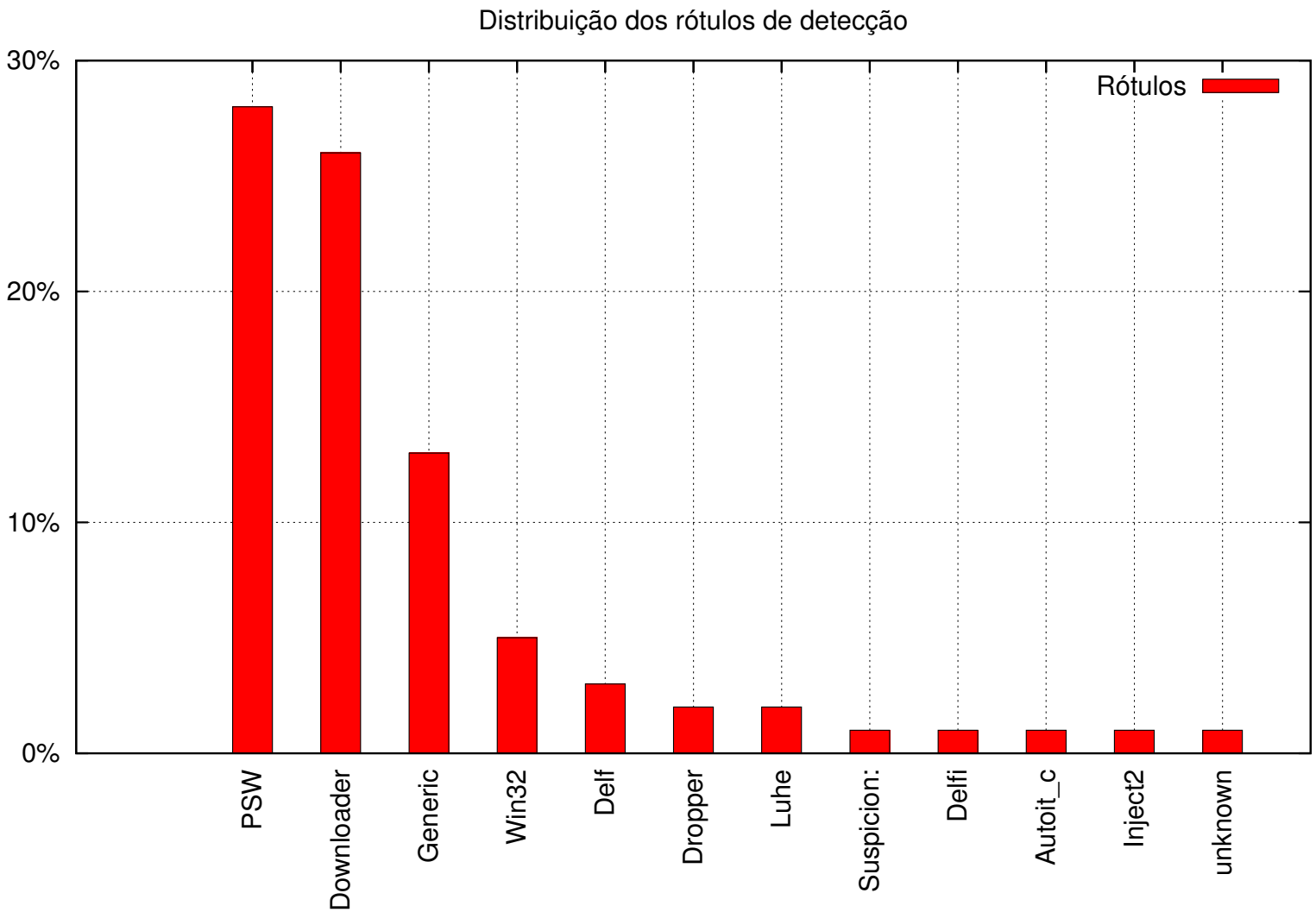
Packer	**Exemplares**	***Packer***	**Exemplares**
Borland Delphi	45,90%	NsPack	0,95%
UPX	24,83%	PKLITE32	0,86%
Microsoft C/C++	23,50%	Enigma	0,67%
ASProtect	2,31%	Dev-C++	0,50%
Themida/WinLicense	2,11%	Thinstall	0,47%

Ofuscação

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

Packer	**2012**	**2013**	**2014**	**2015**
Borland Delphi	35,19%	51,19%	49,66%	43,39%
UPX	31,11%	25,95%	17,36%	8,53%
Microsoft C/C++	22,03%	17,62%	25,97%	44,01%
Themida/WinLicense	5,00%	—	—	—
ASProtect	2,61%	1,54%	2,90%	1,23%
PKLITE32	1,34%	—	—	—
Dev C++	—	1,10%	—	—
NsPack	1,08%	—	1,16%	—

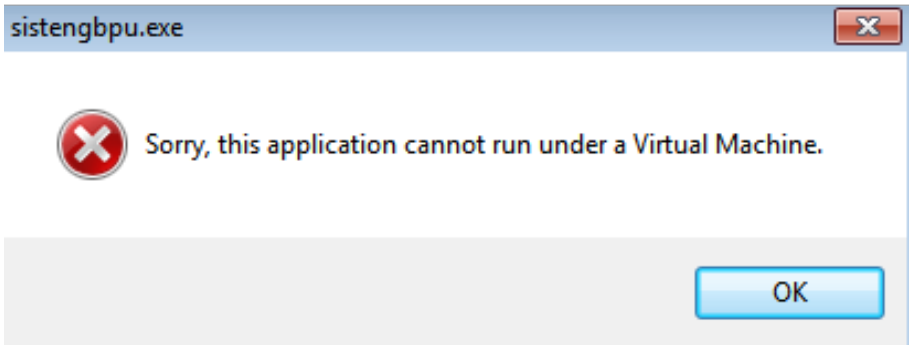
Rótulos de Detecção



Anti-Análise

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

Técnica	**# de exemplares**	**Técnica**	**# de exemplares**
VMCheck.dll	2.729 (12,77%)	Detecção de VirtualBox	306 (1,43%)
VMware *trick*	843 (3,95%)	Bochs & QEmu CPUID *trick*	267 (1,25%)



Evolução das Técnicas de Anti-Análise

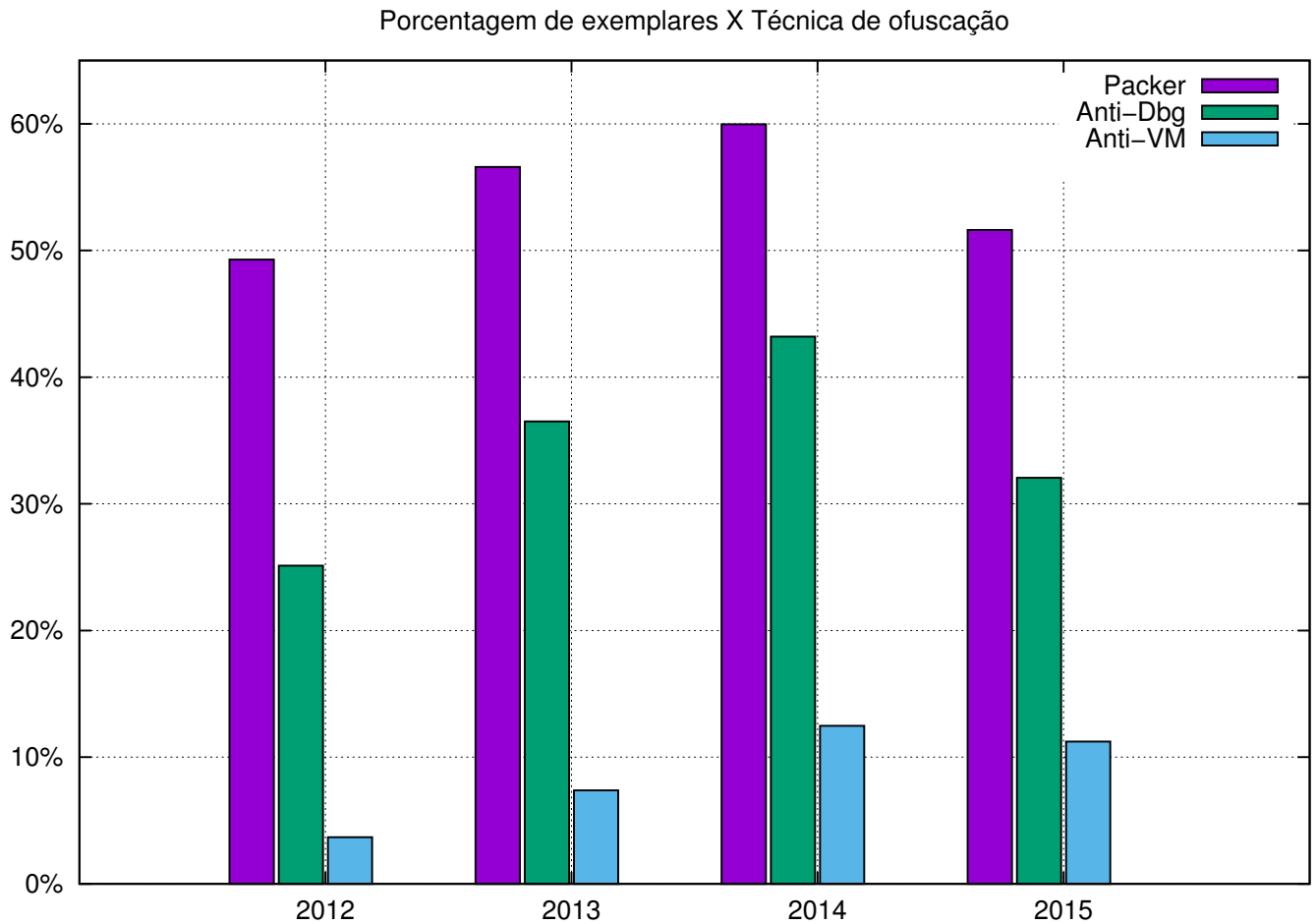


Figura: Evolução das Técnicas de Anti-Análise.

Tópicos

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*.

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 *hosts*	0,11%	1,97%
Criação de arquivo	26,23%	70,78%
Remoção de arquivo	13,71%	42,57%
Modificação em arquivo	17,37%	79,87%
Instalação de BHO no IE	1,26%	1,72%
Tráfego de rede	98,82%	55,18%
Criação de chave no Registro	33,67%	64,71%
Criação de Processo	18,79%	52,19%

Tópicos

Tráfego de Rede

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

Porcentagem de exemplares					
Tipo de tráfego	**2012 (T)**	**2013 (T)**	**2014 (T)**	**2015 (T)**	**Bayer et al.**
TCP	40,87%	41,24%	56,19%	65,10%	45,74%
UDP	52,76%	54,74%	52%	58,79%	27,34%
ICMP	1,28%	1,70%	1,33%	1,18%	7,58%
DNS	52,69%	54,73%	51,98%	58,79%	24,53%
HTTP	38,63%	39,69%	52,03%	58,96%	20,75%
SSL	5,30%	5,62%	4,64%	7,99%	0,23%

Tópicos

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.

Limitações

Limitações

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

Trabalhos Futuros

Trabalhos Futuros

- Expansão das análises.
- Análise *Bare-Metal*.
- Avaliação da eficácia das técnicas de anti-análise.

Tópicos

Conclusões

Conclusões

- Especificidades do cenário nacional.
- Identificação de tendências (CPL e .NET).
- Observação de técnicas de anti-análise.

Agradecimentos

- CNPq, pelo financiamento via Proj. MCTI/CNPq/Universal-A edital 14/2014 (Processo 444487/2014-0)
- Instituto de Computação/Unicamp
- Centro de Tecnologia da Informação Renato Archer

Contato:

marcus@lasca.ic.unicamp.br
paulo@lasca.ic.unicamp.br
andre.gregio@cti.gov.br

LASCA
LABORATORY OF SECURITY AND APPLIED CRYPTOGRAPHY