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

Marcus Botacin[1,3], Vitor Afonso[1], Paulo Lício de Geus[1], André Grégio[1,2]

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

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

[3]Bolsista PIBIC-CNPq

5 de Novembro de 2014

Tópicos

Tópicos

Análise de *malware*

Tipos de análise

- **Análise estática**:
  - código-fonte;
  - executável (*disassembled*).
- **Análise dinâmica**:
  - execução controlada/temporizada;
  - extração comportamental (limitada).

Cenário Atual

Uso do Windows—Olhar Digital, 03/02/2014

O Windows 8.1 se tornou o quarto sistema operacional mais usado por computadores no mundo, deixando o Vista, o Mac OS X Mavericks e o Linux para trás.

Fonte: `http://olhardigital.uol.com.br/noticia/40085/40085`

Malware 64-bits—Securelist 11/12/2013

The more people switch to 64-bit platforms, the more 64-bit malware appears. We have been following this process for several years now. The more people work on 64-bit platforms, the more 64-bit applications that are developed as well.

Fonte: `https://www.securelist.com/en/blog/208214171/The_inevitable_move_64_bit_ZeuS_has_come_enhanced_with_Tor`

Tópicos

Técnicas de Análise

Técnicas de Análise

- ***System Service Dispatch Table (SSDT) Hooking***
  Ex.: BehEMOT (SBSeg 2010).
- ***Virtual Machine Introspection (VMI)***
  Ex.: Anubis (`anubis.iseclab.org`).
- ***Application Programming Interface (API) Hooking***
  Ex.: Cuckoo (`www.cuckoosandbox.org`),
  CWSandbox (`www.threattracksecurity.com`).
- ***Detour***
- ***Callback* e *Filters***
  Ex.: Capture-BAT (`www.honeynet.org/node/315`)

Tópicos

Novidades do Windows 64 bits

Novidades do Windows 64 bits

- ***Kernel Patch Protection (KPP)***.
  $\Rightarrow$ Apenas 64 bits.
- **Exigência de assinatura de *driver***.
  $\Rightarrow$ Inclui auto-assinados.
- **Sessões de aplicativos**.
  $\Rightarrow$ Impede criação de *threads* remotas entre sessões.
- **Mudanças na API**.

Tópicos

Considerações

Mecanismos de proteção vs. Análise dinâmica

- ***KPP***:
  - impede SSDT hooking.
- **Assinatura de *drivers***:
  - pode ser desligada;
  - *malware* geral atua em *userland*
    $\Rightarrow$ não carrega *drivers*!
- **Detours/Inline hooking**:
  - mesmo nível de privilégio do malware.
- **Proibição de *threads* remotas**:
  - dificulta *DLL hooking*.

Considerações

Requisitos de Projeto

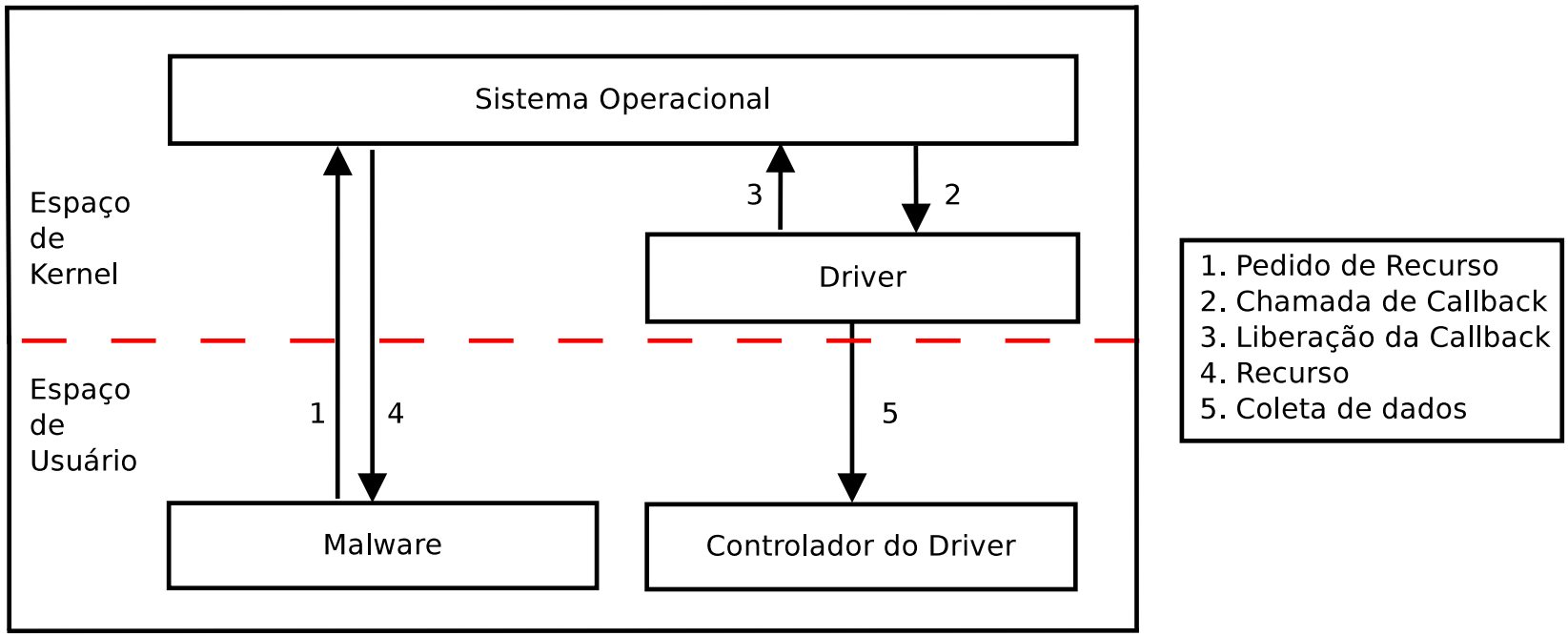
- Análise de *malware* moderno.
- Portabilidade e Escalabilidade
  $\Rightarrow$ incompatível com VMI.

Decisões de Projeto

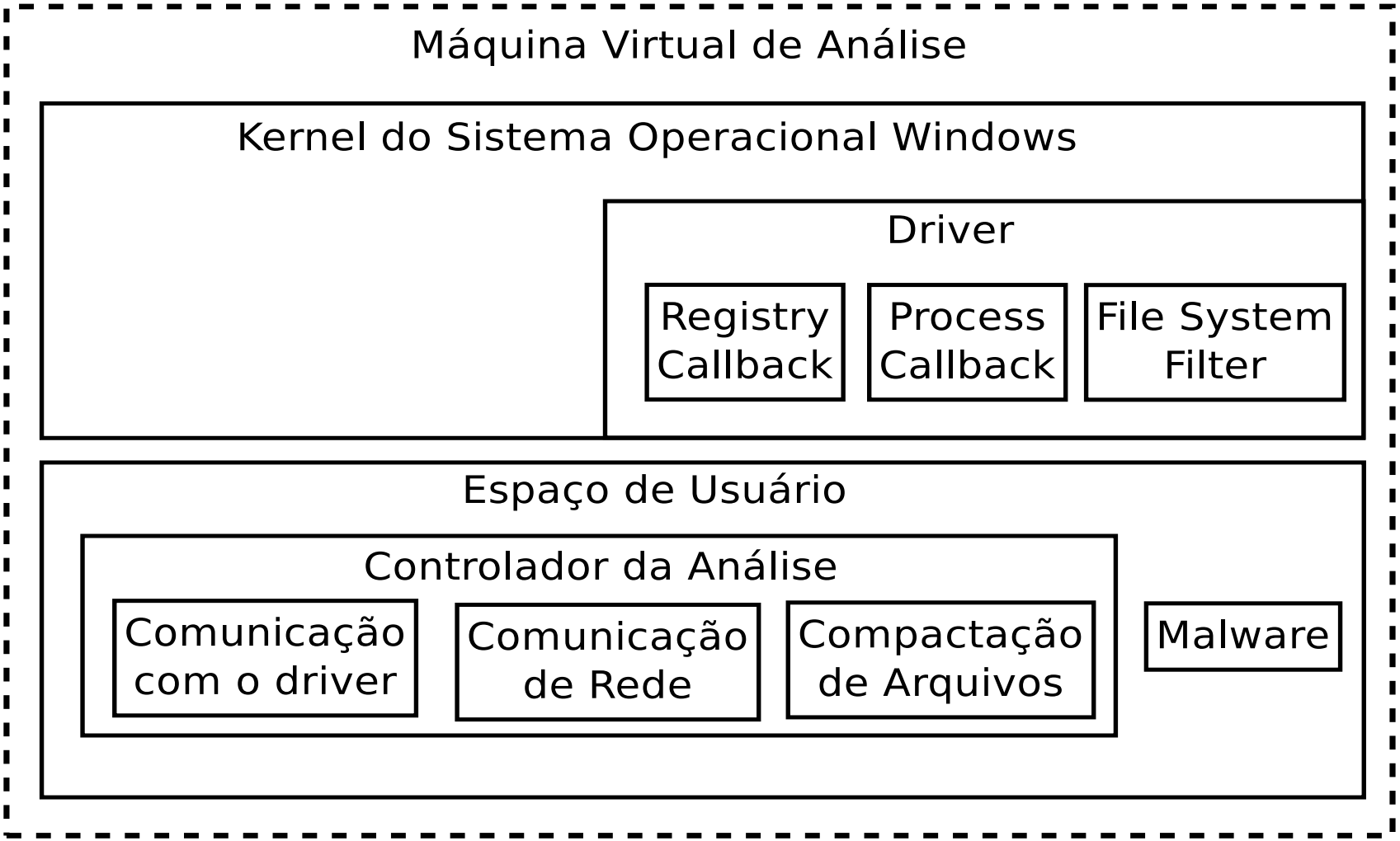
- Implementação Utilizando-se de *Callbacks* e *Filters*.
- Tráfego de rede capturado externamente ao ambiente de análise.

Tópicos

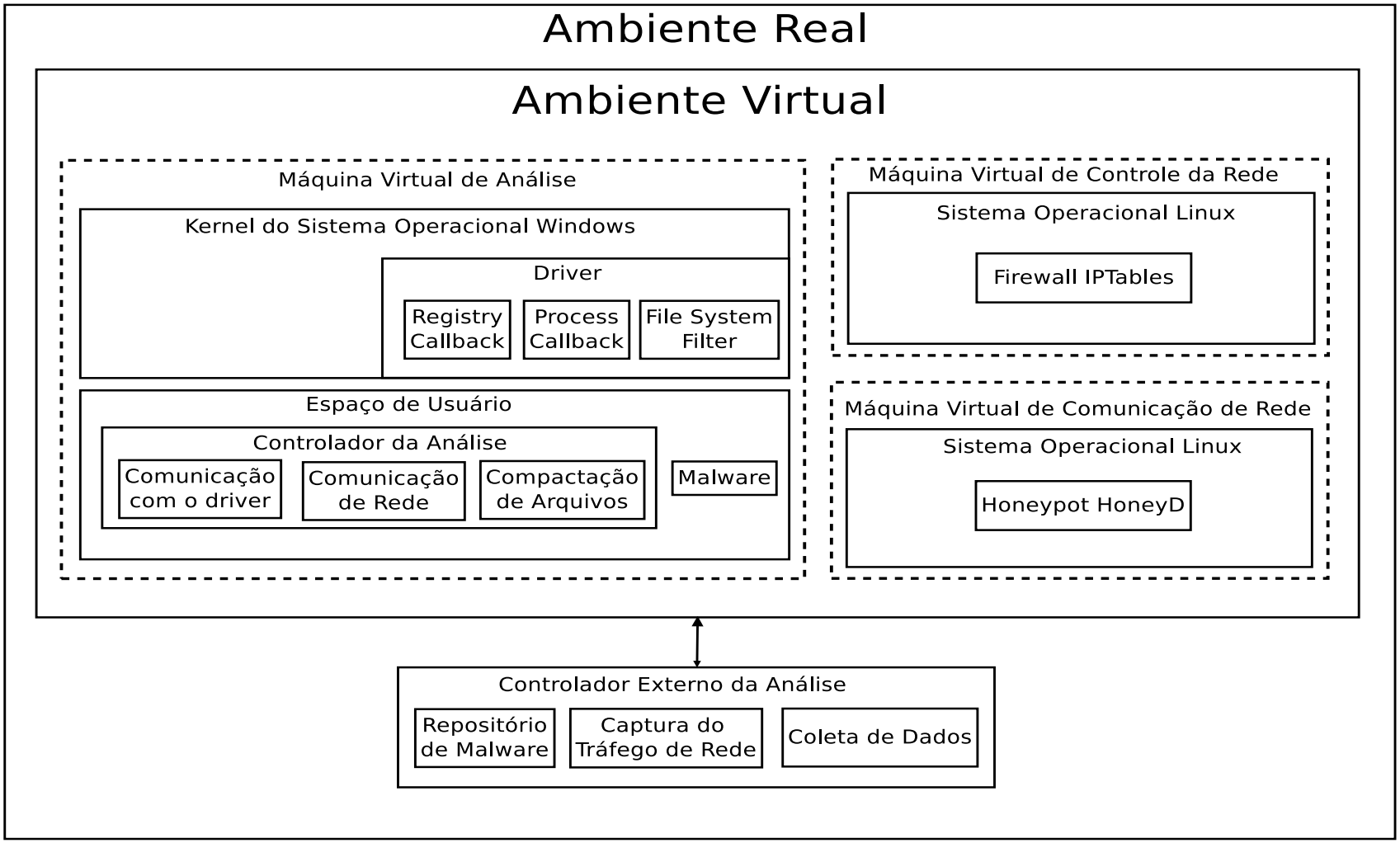
Callback


Sistema Operacional
Espaço de Kernel
Espaço de Usuário
Driver
Malware
Controlador do Driver
1
2
3
4
5
1. Pedido de Recurso
2. Chamada de Callback
3. Liberação da Callback
4. Recurso
5. Coleta de dados

Arquitetura do Sistema



Arquitetura do Sistema



Tópicos

Experimentos

Tipos de Experimentos

- Validação.
- Testes em maior escala.

Objetivo

1. Verificar se a monitoração das ações efetuadas sobre os subsistemas de arquivos, registro e processos é feita adequadamente.
2. Análise aprofundada de exemplares de *malware* em busca de comportamentos que indicam a presença de códigos maliciosos.

Validação

```
1  7/4/2014-13:3:48.793|SetValueKey|2032|C:\7G6C5n.exe
       |\REGISTRY\USER\S
       -1-5-21-3760592576-961097288-785014024-1001\
       Software\Microsoft\Windows\CurrentVersion\Run|
       SoftBrue|"C:\7G6C5n.exe"
```

```
1  7/4/2014-13:3:48.76|WriteOperation|3028|C:\
       visualizar.exe|C:\Windows\SysWOW64\dll.exe|
```

Validação

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

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

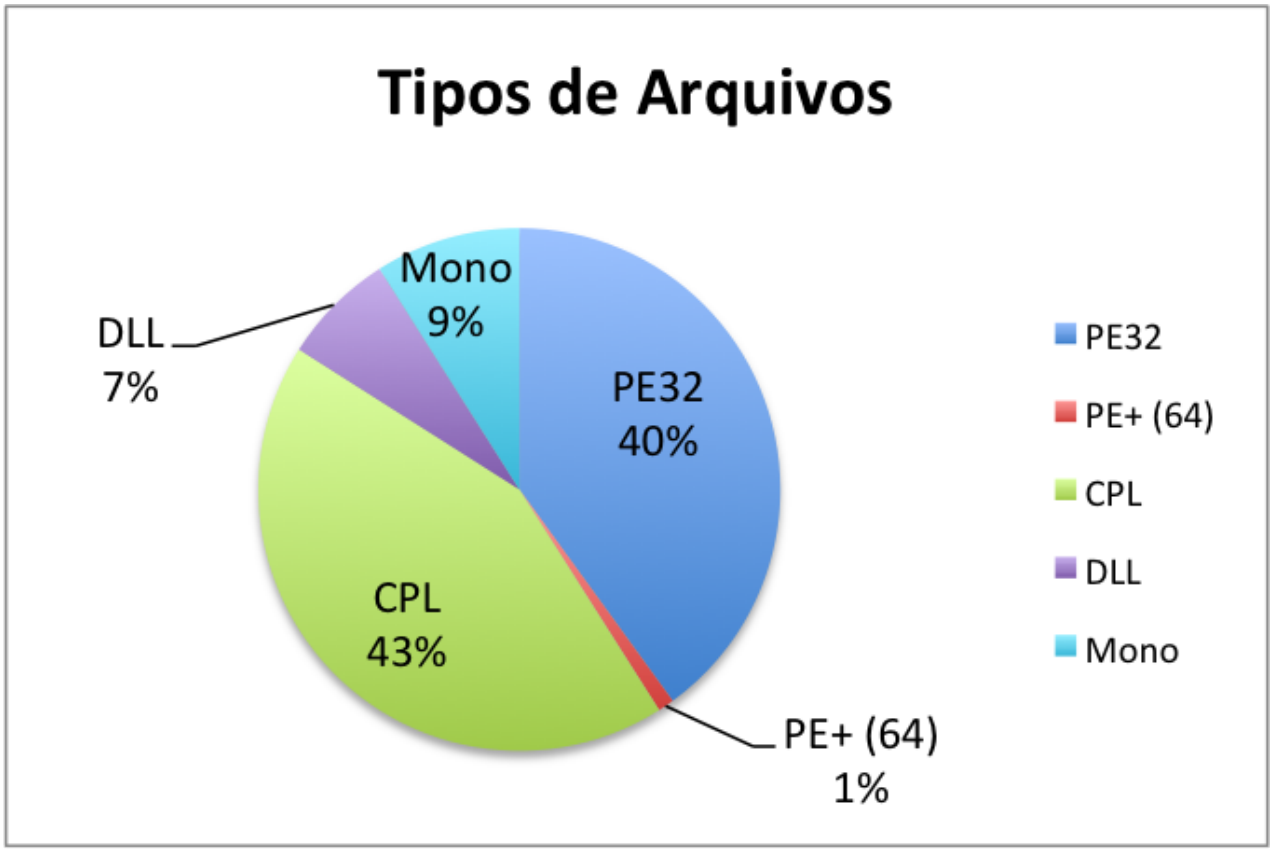
```
1 2014-05-14 20:02:40.963113 10.10.100.101 XX.
    YY.ZZ.121 HTTP 290 GET /.swim01/
    control.php?ia&mi=00B5AB4E-47098BC3 HTTP/1.1
```

Testes em maior escala

Amostras

1. Amostras coletadas no período entre 01/01/2014 e 21/05/2014.
2. 2.937 exemplares únicos (*hash* MD5).
3. Exemplares provenientes de *honeypots*, *phishing* e *downloads* de *links* contaminados.

Distribuição das Amostras



Comportamentos exibidos pelos exemplares

Tabela: Atividades monitoradas e quantidade de exemplares que as exibiram.

Atividade	**Qtde.**
Escrita no Registro	1073
Remoção de chave(s) do Registro	772
Criação de processo(s)	602
Término de processos	1337
Escrita em arquivo(s)	1028
Leitura de arquivo(s)	1694
Remoção de arquivo(s)	551

Comportamentos Observados

Detalhes dos comportamentos

- Finalização de mecanismos antívirus instalados no sistema operacional;
- Desligamento do *firewall* nativo do Windows;
- Criação de novos binários no sistema, seja por *download* ou por *dropping*;
- Desligamento do mecanismo de atualização automática do Windows;

Comportamentos Observados

Detalhes dos comportamentos

- Tentativa de persistência (sobrevivência a desligamentos e reinicializações);
- Injeção de *Browser Helper Objects* no Internet Explorer;
- Modificação no arquivo `hosts.txt` do sistema operacional;
- Sobrescrita de um arquivo (programa ou biblioteca) já presente no sistema;
- Remoção de seu próprio programa ou de outros artefatos.

Tráfego de rede

Tabela: 10 portas/protocolos mais utilizados pelos exemplares.

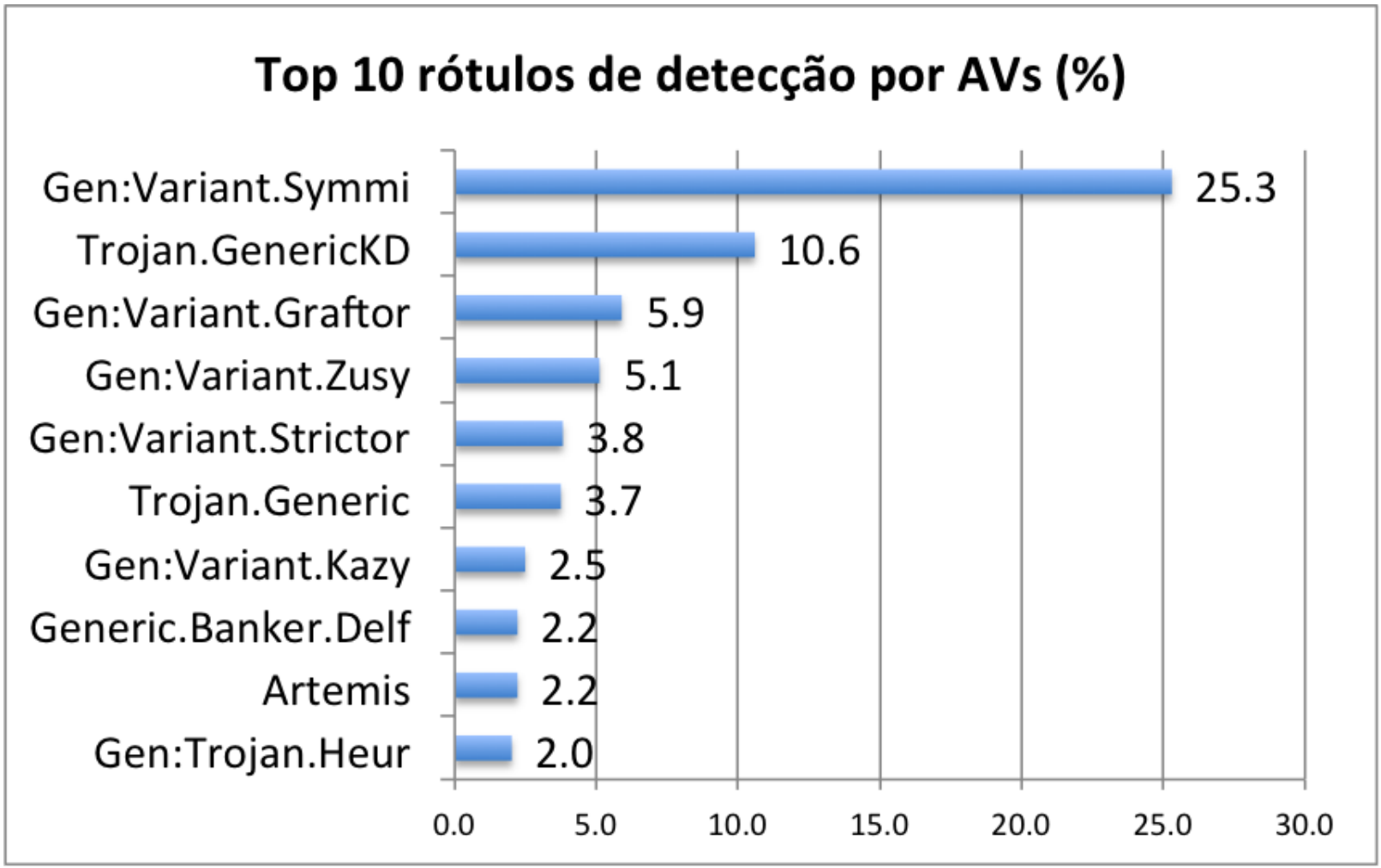
Protocolo	Porta	% dos exemplares
HTTP	80	44.4
HTTPS	443	6.5
MS-SQL	1433	2.6
-	8181	1.0
SMTP	587	0.8
-	82	0.7
MySQL	3306	0.5
-	720	0.3
-	2869	0.3
-	9000	0.2

Tráfego de rede

Tabela: Comportamentos suspeitos observados no tráfego de rede.

Comportamento	**Qtde. de *malware***
Download desconhecido	154
E-mail/Spam	25
Banker	22
Comunicação IRC	4
Dados do sistema	3
Obtenção de PAC	1
Portas de IRC	1

Virustotal


Top 10 rótulos de detecção por AVs (%)
Gen:Variant.Symmi
Trojan.GenericKD
Gen:Variant.Graftor
Gen:Variant.Zusy
Gen:Variant.Strictor
Trojan.Generic
Gen:Variant.Kazy
Generic.Banker.Delf
Artemis
Gen:Trojan.Heur
25.3
10.6
5.9
5.1
3.8
3.7
2.5
2.2
2.2
2.0
0.0
5.0
10.0
15.0
20.0
25.0
30.0

Discussão

Contribuições:

- Capaz de executar arquivos no formato PE+ (64 bits).
- Provê um ambiente "flexível" de 64 bits (Windows 8) para análise.

Ferramentas/sistemas avaliados:

- *Anubis* (`http://anubis.iseclab.org`)
- *Cuckoo* (`https://malwr.com/`)
- *ThreatExpert* (`http://www.threatexpert.com`)
- Camas Comodo (`http://camas.comodo.com`)
- CWSandbox (`http://www.threattracksecurity.com/resources/sandbox-malware-analysis.aspx`)

Discussão

Antivírus

- Rótulos de detecção baseiam-se em heurísticas genéricas.
  ⇒ Permitem que o usuário seja alertado sobre um evento ou processo suspeito.
  ⇒ Não provêem informações específicas sobre o tipo de dano causado.

Windows

- Retrocompatibilidade
  ⇒ Exemplares de 32 bits (Windows XP) infectam o Windows 8.

Tópicos

Limitações

Limitações

- Análise de *rootkits*
- Análise de tráfego criptografado
- Análise de *evaders* (*Reboot*, *VM detection*)
- Mecanismo de *callback* limitado a interface do S.O.

Trabalhos Futuros

Trabalhos Futuros

- Integração do ambiente *bare-metal* ao ambiente emulado.
- Implementação de técnicas para monitoração de outros subsistemas.
- Estudo e desenvolvimento de mecanismos de proteção para a ferramenta de monitoração.

Tópicos

Conclusões

Conclusões

- Introduziu-se um sistema de análise dinâmica de *malware* de 64 bits baseado em Windows 8.
- Avaliou-se o funcionamento do sistema por meio da execução de 2.937 exemplares de *malware*.
- Os resultados obtidos permitem uma maior compreensão da atuação de *malware*, possibilitando a criação de heurísticas de detecção, procedimentos de remediação e tomada de contra-medidas para resposta a incidentes.

Agradecimentos

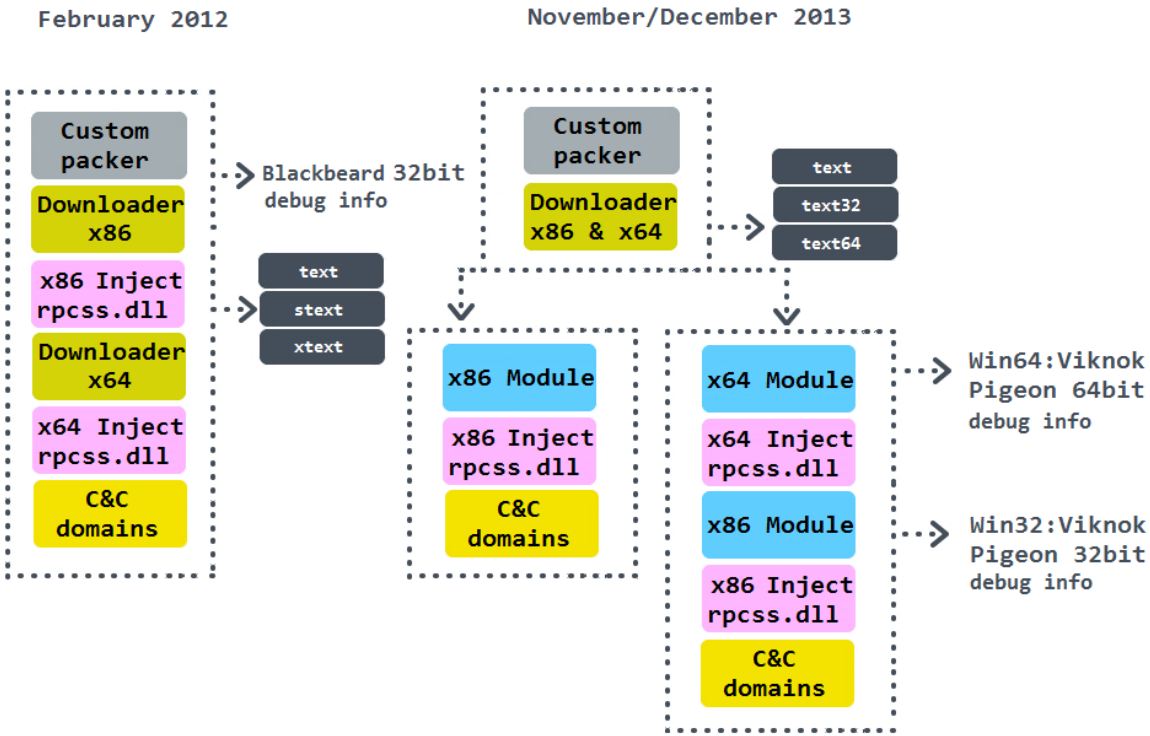
Os autores agradecem:

- CNPq
- Instituto de Computação/Unicamp
- CTI Renato Archer

Mais sobre *64-bit-malware*

Win32/64:Blackbeard & Pigeon

Fonte: `http://blog.avast.com/2014/01/15/win3264blackbeard-pigeon-stealthiness-techniques-in-64-bit-windows-part-1/`



Mais sobre *64-bit-malware*

TSPY64_ZBOT.AANP

Fonte: `http://about-threats.trendmicro.com/Malware.aspx?language=au&name=TSPY64_ZBOT.AANP`

- *It connects to the following URL(s) to get the affected system's IP address:* `http://checkip.dyndns.org`

Current IP Address: 187.35.196.227

Mais sobre *64-bit-malware*

TSPY64_ZBOT.AANP

- *It requires the existence of the following files to properly run: \Application Data\random folder name\random file name.exe*
- Nota: \Application Data\ é C:\Users\user name\AppData\Roaming do Windows Vista em diante.

```
1 29/6/2014 - 15:43:27.668|CreateOperation|1852|
    Trojan-Spy.Win64.Zbot.a|\Users\User_Windows_VM\
    AppData\Roaming\Gevoun|
2 29/6/2014 - 15:43:27.668|CreateOperation|1852|
    Trojan-Spy.Win64.Zbot.a|\Users\User_Windows_VM\
    AppData\Roaming\Gevoun\riod.exe|
3 29/6/2014 - 15:43:27.808|CreateOperation|1852|
    Trojan-Spy.Win64.Zbot.a|\Users\User_Windows_VM\
    AppData\Roaming\Arcole|
```