GTS-16

Análise comportamental de *malware*

André Grégio, Dario Fernandes, Vitor Afonso, Paulo L. de Geus

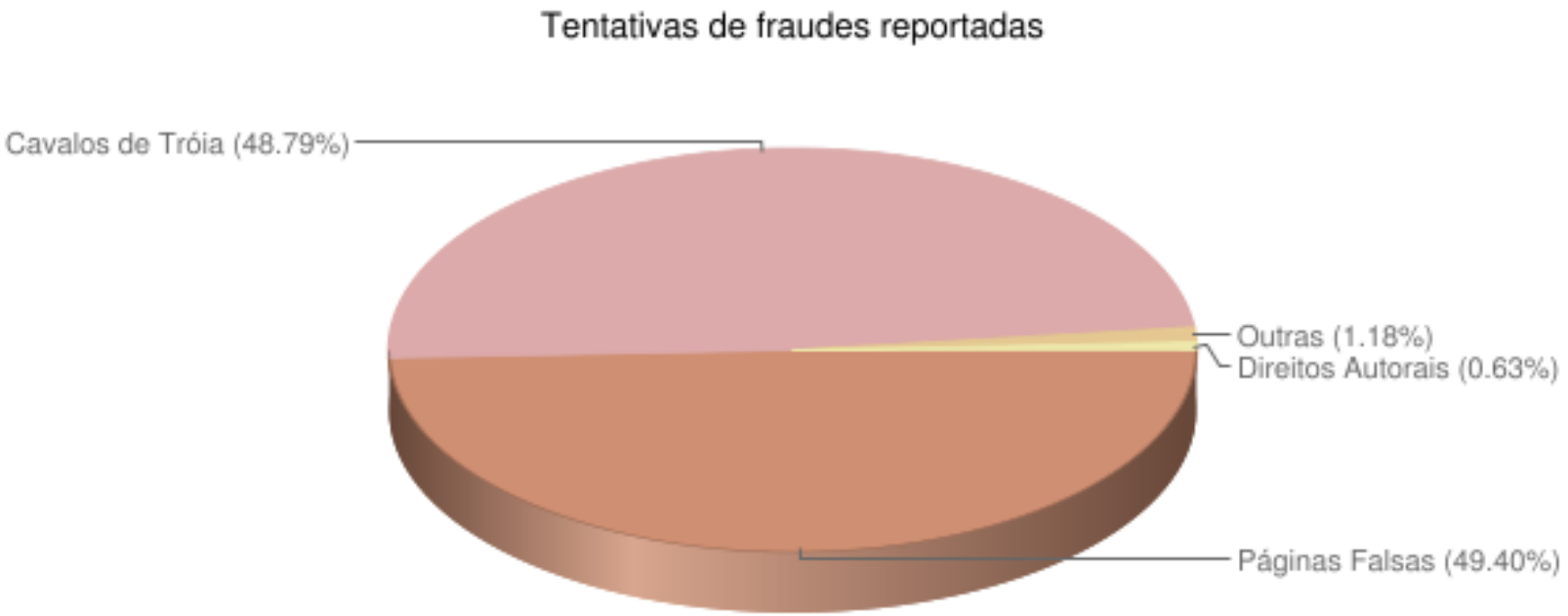
Agenda

- Motivação habitual
- Causos (não necessariamente nessa ordem)
  - Algumas técnicas de captura de comportamentos
  - Exemplos de comportamentos de malware
  - Trabalhos dos outros
  - Trabalhos próprios
  - Estudos de caso
  - Discussões acaloradas
- Agradecimentos

Estatísticas do CERT.br (jul-set/2010)

http://www.cert.br/stats/incidentes/2010-jul-sep/tipos-ataque.html

Estatísticas do CERT.br (fraude)



http://www.cert.br/stats/incidentes/2010-jul-sep/fraude.html

Aí o malware vem e…

- Faz download de um ".rar" com páginas falsas (ou não) de bancos azuis, amarelos, vermelhos, verdes, brancos…

- Muda o "hosts.txt":

```
[endereço IP]
bancoX.com.br
bancoY.com.br
bancoZ.com.br
```

- Sobrepõe telas de login com figuras/forms para "obter" os dados/credenciais de acesso.

Aí o malware vem?

- É. Vem, e se comporta de uma maneira.

- Análise comportamental:
  - O que o malware fez no sistema alvo?
    - Modificação de arquivos;
    - Carregamento de DLLs;
    - Criação de processos;
    - Mudança em registros;
    - Acesso à rede, etc.
  - O que o sistema alvo respondeu para o malware?

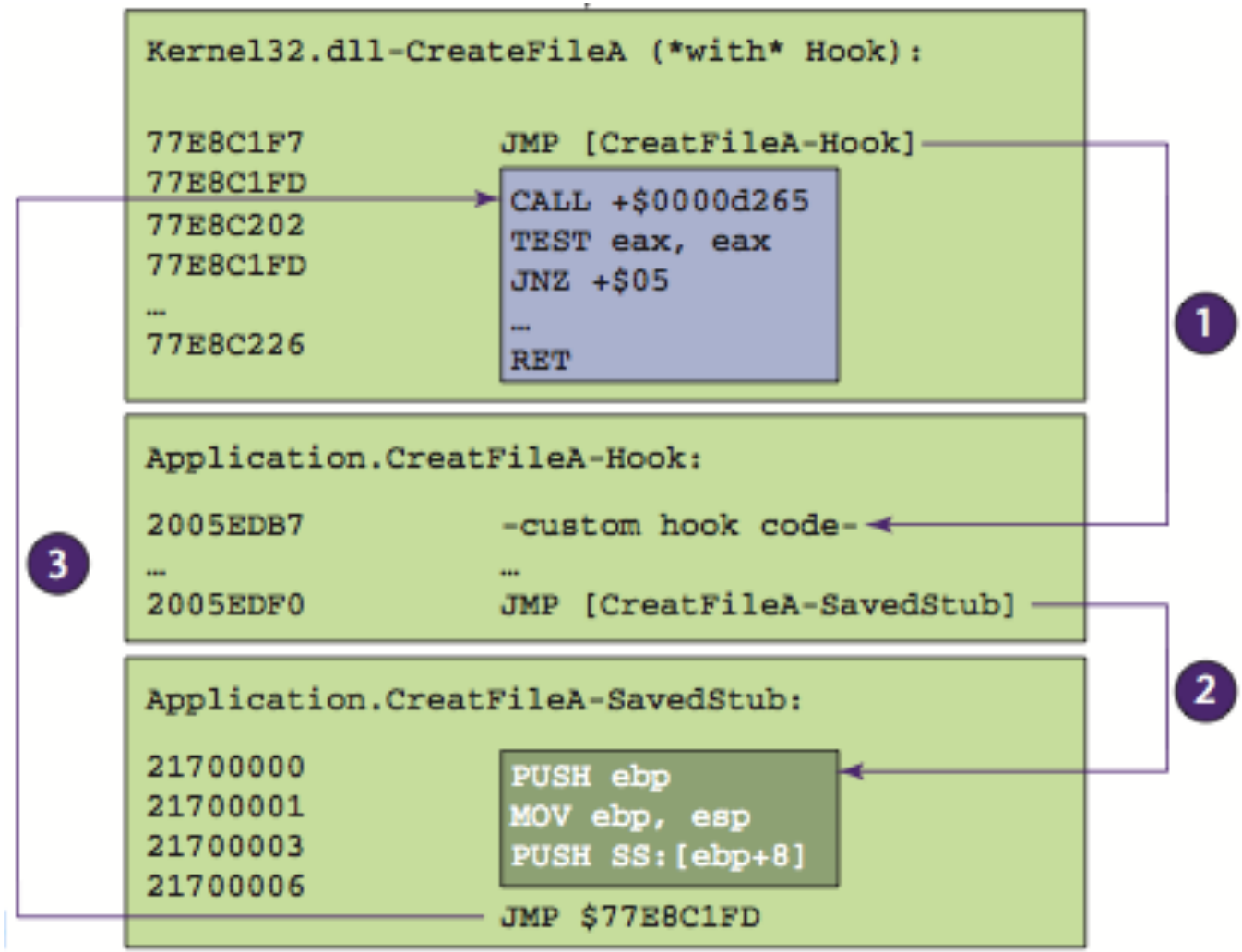
- Um comportamento ocorre em uma dada execução. Pode ser que em outra o malware atue de modo diferente.

Algumas técnicas…

…de análise comportamental:

- *Hooking*
  - *API (CWSandbox)*
    - *Modifica os endereços na IAT (import address table) do malware.*
  - *SSDT*
    - *Modifica a System Service Dispatch Table do sistema.*
- *Virtual Machine Introspection* (VMI)
  - Emulação (Anubis)
    - Modifica o emulador para extrair informações em uma camada intermediária (entre o host e o guest)

API Hooking



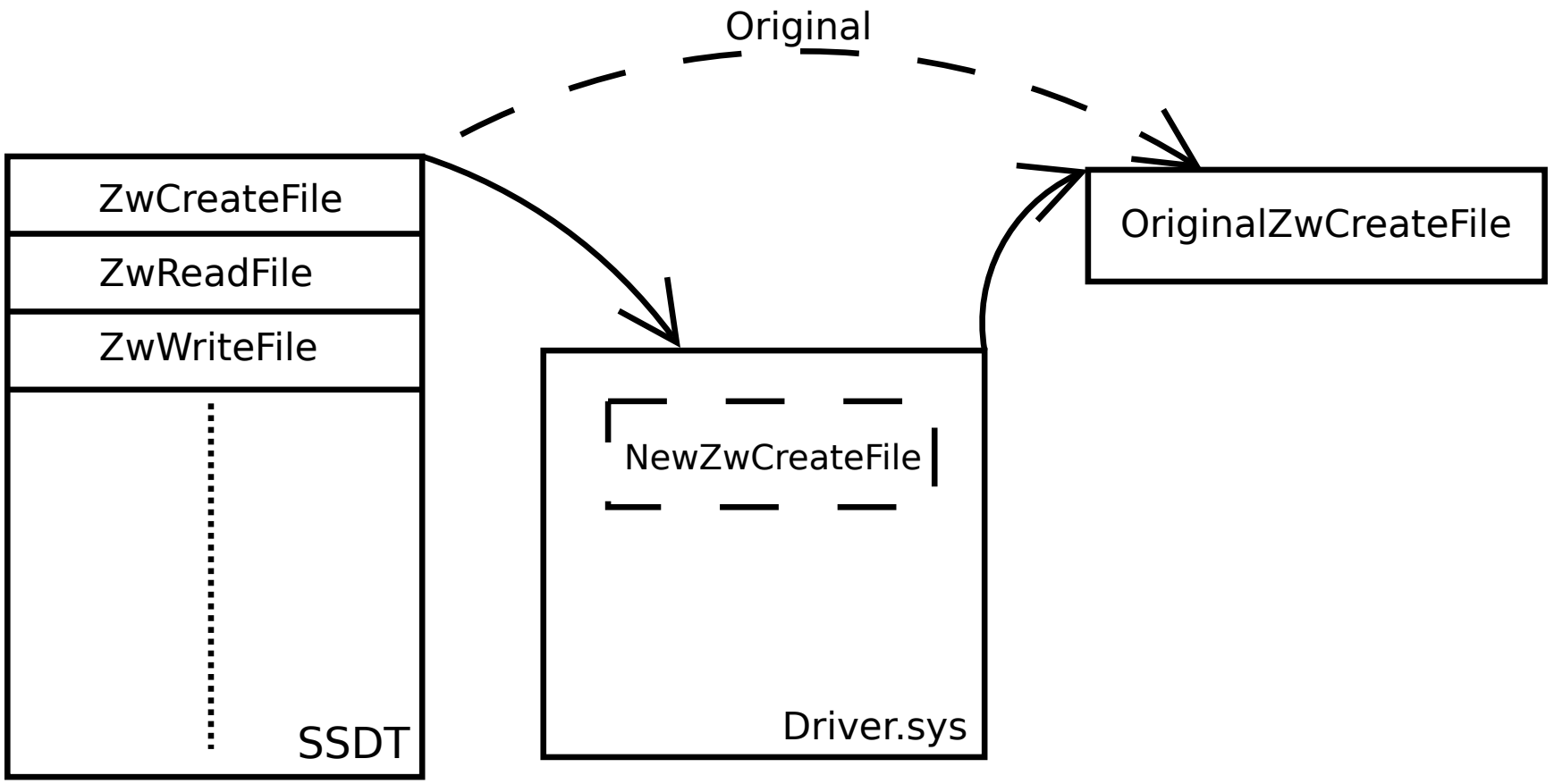
Fonte: Willems, C., Holz, T., Freiling, F. Towards Automated Dynamic Malware Analysis using CWSandbox. IEEE Security & Privacy Mar/Apr 2007.

API Hooking

- Vantagens:
  - Fácil de implementar;
  - Resultados mais precisos;
  - Malware "de prateleira" geralmente usa a Windows API.

- Desvantagens:
  - O malware pode fazer checagem de integridade que foi modificado;
  - Se o malware fizer chamadas diretas ao kernel, sem usar a Windows API, a técnica de monitoração é contornada.

SSDT Hooking



SSDT Hooking

- Vantagens:
  - Permite a interceptação de todas as chamadas de sistema;
  - Mais difícil de detectar, pois não modifica o processo.

- Desvantagens:
  - Conhecimento do sistema (versão, nível de patches/Serv. Pack);
  - Pode ficar instável na presença de outros programas que fazem a mesma coisa (antivírus, rootkits).

Para onde a coisa vai...

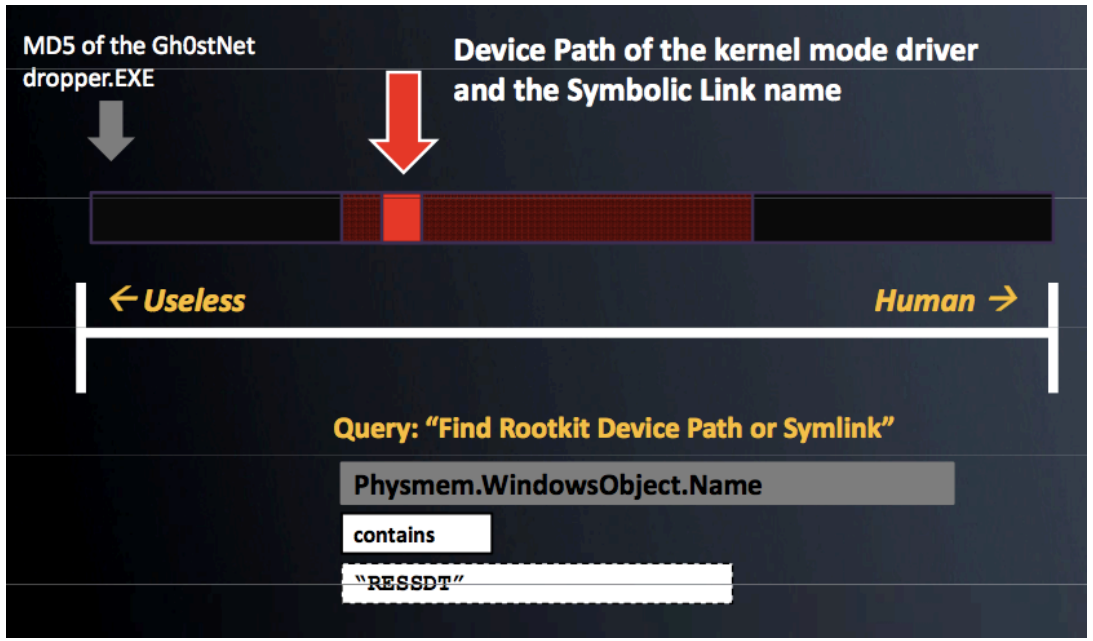
- Variações das técnicas apresentadas têm sido desenvolvidas.

- Melhor uso dos resultados de análise comportamental:
  - Classificação
  - Atribuição
  - Detecção

- Alguns exemplos (Black Hat 2010)
  - Malware Attribution – Greg Hoglund
  - Virt-ICE – Quynh Nguyen Anh, Kuniyasu Suzaki
  - Dirtbox – Georg Wicherski

Atribuição

- Foco no desenvolvedor do malware, fatores de influência;
  - Meio-termo entre ter o MD5 de uma variante e lançar um míssil na casa do atacante: assinaturas de longo prazo.



http://www.blackhat.com/html/bh-us-10/bh-us-10-archives.html#Hoglund

Atribuição

- Ex.: quatro *bankers* distintos, enviando POSTs após comprometimento por execução na vítima.

1. **praquem=**brasilverde2014@gmail.com**&titulo=**CHANGEME+**Suporte****&texto=**.:::.INFECT.:::.
2. **praquem=**dener.infects@gmail.com**&titulo=**CHANGEME-(windows+XP)+(IE+7+ou+8)+++**&texto=**Data..:+10/7/2010
3. **praquem=**sexototal2010@gmail.com**&titulo=**CHANGEME-(windows+XP)+(IE+7+ou+8)+++**&texto=**Data..:+10/7/2010
4. **praquem=**edunorauto@gmail.com**&titulo=**INFECT:+CHANGEME10/7/2010+1:16:28+AM**&texto=**&

Atribuição


KL BANK - COPA DO MUNDO
O key tem um systema pra deletar o GB, e o mesmo foi atualizado pra deletar todos os update dos AVS, e depois da vitima se infectar, os AVS vão ser impossivel de ter update para se atualizar e localizar o kl Bank.
Telas do Kl Bank
Bradesco Net Empresa: Superrrrrr Atualizaaaaaaaaaaaa.
Bradesco: Nova Tela, Super Atualizada, Pegando dentro, So info valida.
Banco do Brasil: Super Atualizada.
Caixa Economica: Super Atualizada.
Itaú Fisica: Nova Tela, Pedindo Token, Pedindo Tabela, So info valida.
Itaú Personalite: : Nova Tela, Pedindo Token, Pedindo Tabela, So info valida.
Itaú Juridica: Nova Tela, Pedindo Token, Pedindo Tabela, So info valida.
Santander: Nova Tela, Super Atualiza, Pegando dentro, So info valida.
Banrisul: Nova Tela Super Atualizada.
KL BANK - COPA DO MUNDO

Debugger (Virt-ICE)

- Debuggers são facilmente detectados por malware, e podem ser "contaminados" se ambos estão em ring 0.
- Virt-ICE faz VMI total através da modificação do Qemu, não inserindo nenhum programa ou driver no S.O. alvo e estando completamente fora do alcance do malware.
- Não tem problemas para lidar com rootkits.

http://media.blackhat.com/bh-us-10/whitepapers/Anh/BlackHat-USA-2010-Anh-Virt-ICE-wp.pdf

Emulador (Dirtbox)

- Novas assinaturas para antivírus são necessárias constantemente; análise dinâmica não escala bem.
- Emuladores dos antivírus => interpretadores de x86, com limitação de velocidade e de precisão nas Windows APIs.
- Dirtbox implementa *instruction level introspection:*
  - Instruções executadas na CPU do *host* em blocos;
  - Memória virtual separada da memória do emulador.

http://media.blackhat.com/bh-us-10/presentations/Wicherski/BlackHat-USA-2010-Wicherski-dirtbox-x86-windows-emulator-slides.pdf

Sobre tais avanços.

- Cenário favorável == problema resolvido?

- Problemas:
  - Atribuição necessita interação humana.
  - Abordagens com Qemu sempre são suscetíveis aos problemas do Qemu!
  - Todo emulador tem alguma limitação.

- Tem mais…
  - Alguns malware detectam aceleração do tempo;
  - Outros, dormem ou agendam horário para comunicar/atuar.

Algumas deficiências intrínsecas

Sandbox bypass

- Depende do que se usa para captura de eventos
  - *Debugger*
    - kernel32!IsDebuggerPresent
    - PEB!IsDebugged
    - http://www.symantec.com/connect/articles/windows-anti-debug-reference
  - Emulador
    - Emulação incompleta ou imprecisa permite detecção
  - VM "rootkits"
    - Identificação pelo tipo de VM utilizado ou por tipo de *hook*
    - www.damballa.com/downloads/r_pubs/BH08RoyalPres.pdf

Exemplo com emulador

- *Malware* com *packer tElock*.

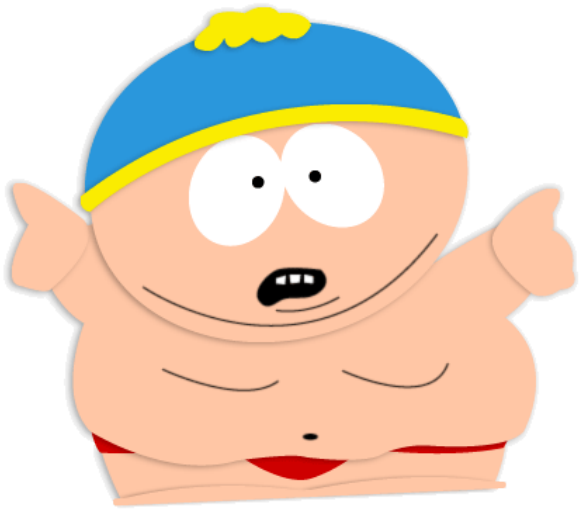
- *Em alguns sistemas emulados com Qemu, exceções não gerenciadas podem gerar análise incompleta ou nula.*

- *Sistema A (saída resumida).*
  - *Windows SEH exceptions:*
  - *[Exception 0x80000003 (STATUS_BREAKPOINT)]*
  - *[Exception 0xc000001d (STATUS_ILLEGAL_INSTRUCTION)]*
  - *[Exception 0xc0000094 (STATUS_INTEGER_DIVIDE_BY_ZERO)]*
  - *[Exception 0x80000004 (STATUS_SINGLE_STEP)]*

No mais,

- Analisadores comportamentais…
  - …analisam comportamento?
- E se
  - eu precisar de uma aplicação específica?
  - o malware conflita com meu monitor?
  - aguarda um gatilho (ou só aguarda)?
  - …
- A seguir, casos de confusão!

Boy oh boy



Antes dos casos de confusão

- Em resumo:
  - Os resultados podem ser confusos para leigos;
  - Podem causar uma interpretação errônea;
  - O objeto de análise pode atacar o analisador;
  - Packers como telock, armadillo, pecompact podem criar problemas;
  - Comportamento temporizado subverte o objetivo do analisador;
  - Aplicações adicionais demandam tratamento especial;
  - Caso nada saia para a Internet, atrapalha a análise de downloaders;
  - Se um repositório estiver indisponível, proibido ou não mais existir, o comportamento pode não ser obtido;
  - Gatilhos exigem tratamento (entrar em determinado site, enviar/receber um dado, form inputs, clicks em botões/pop-ups de erro, etc.)

Casos de confusão

- Cenário: comparar a execução de um binário em dois sistemas (A e C) para tomar uma decisão.

- Binário: nada.exe
  - PE32 executable for MS Windows (console) Intel 80386 32-bit

- nada.c:

```
int main(){
    return 0;
}
```

Casos de confusão (nada.exe)

- Saída do Sistema A (alguns trechos omitidos).

- Summary:
  - Performs Registry Activities:
    - The executable reads and modifies registry values. It also creates and monitors registry keys.

- [Load-time Dlls]
  - [C:\WINDOWS\system32\ntdll.dll]
  - [C:\WINDOWS\system32\kernel32.dll]
  - [C:\WINDOWS\system32\msvcrt.dll]

Casos de confusão (nada.exe)

- Sistema A:

"Performs Registry Activities"

- Onde?

Image Copyrighted by Historylink101.com & found at Egyptian Picture Gallery.

Casos de confusão (nada.exe)

- Saída do Sistema C (muitos trechos omitidos).

- Loaded DLL's:
  - **C:\WINDOWS\system32\ntdll.dll**
  - **C:\WINDOWS\system32\kernel32.dll**
  - **C:\WINDOWS\system32\msvcrt.dll**
  - C:\WINDOWS\system32\user32.dll
  - C:\WINDOWS\system32\GDI32.dll
  - C:\WINDOWS\system32\advapi32.dll
  - C:\WINDOWS\system32\RPCRT4.dll
  - C:\WINDOWS\system32\Secur32.dll
  - C:\WINDOWS\system32\oleaut32.dll
  - C:\WINDOWS\system32\ole32.dll
  - C:\WINDOWS\system32\IMM32.DLL
  - C:\WINDOWS\system32\pstorec.dll
  - C:\WINDOWS\system32\ATL.DLL

Casos de confusão (nada.exe)

Ainda o sistema C...

All Processes (28)

- Process ID **0**, File Name: **(SystemIdle)**,
- Process ID **4**, File Name: **(System)**,
- Process ID **128**, File Name: **C:\Program Files\Microsoft Office\Office\FINDFAST.EXE**, File Name Hash: **3C6B1E4410DC5BB2B3DA01ACE236F30063E2DD5E**.
- Process ID **376**, File Name: **C:\Program Files\Microsoft Office\Office\OSA.EXE**, File Name Hash: **B735358310B44C10CB80006851EF1E00B94DDC4A**.
- Process ID **476**, File Name: **C:\WINDOWS\System32\smss.exe**, File Name Hash: **33A0AB030064EFA6C69B00AD18ED030054CE3826**.
- Process ID **540**, File Name: **C:\WINDOWS\system32\csrss.exe**, File Name Hash: **B4E7351200C6D8C218E800665DD0AE001975146F**.
- Process ID **564**, File Name: **C:\WINDOWS\system32\winlogon.exe**, File Name Hash: **65AC26F6009EAAB8C01307D21BFA850005C731B9**.
- Process ID **608**, File Name: **C:\WINDOWS\system32\services.exe**, File Name Hash: **2C560F210066FD4CA85C016C25DE39002D329A6C**.
- Process ID **620**, File Name: **C:\WINDOWS\system32\lsass.exe**, File Name Hash: **09DB5EC900AF6D2D3445003B3C2E07008DAECC19**.
- Process ID **712**, File Name: **C:\12063271.exe**, File Name Hash: **C2B180D35BDE073D3CB8007E237FB400138636FD**.
- Process ID **780**, File Name: **C:\WINDOWS\system32\svchost.exe**, File Name Hash: **52BDB1F1005527D0384D00B1B6718300527EEB16**.
- Process ID **872**, File Name: **C:\WINDOWS\system32\svchost.exe**, File Name Hash: **52BDB1F1005527D0384D00B1B6718300527EEB16**.
- Process ID **940**, File Name: **C:\WINDOWS\System32\svchost.exe**, File Name Hash: **52BDB1F1005527D0384D00B1B6718300527EEB16**.
- Process ID **1000**, File Name: **C:\WINDOWS\system32\cmd.exe**, File Name Hash: **2751DD6A00570674F0080506F4B6C600B64FDB50**.
- Process ID **1072**, File Name: **C:\WINDOWS\System32\alg.exe**, File Name Hash: **B789899500A84BB2AEC2005EDE65FA004F6B7ADA**.
- Process ID **1096**, File Name: **C:\WINDOWS\system32\svchost.exe**, File Name Hash: **52BDB1F1005527D0384D00B1B6718300527EEB16**.
- Process ID **1172**, File Name: **C:\WINDOWS\system32\wscntfy.exe**, File Name Hash: **8FBFA6FA00E6E09B3694001AFC0EFA001CA5DA83**.
- Process ID **1184**, File Name: **C:\WINDOWS\system32\svchost.exe**, File Name Hash: **52BDB1F1005527D0384D00B1B6718300527EEB16**.
- Process ID **1244**, File Name: **C:\WINDOWS\system32\defrag.exe**, File Name Hash: **56453841008F9E9E6206004B549BE0001BED168F**.
- Process ID **1320**, File Name: **C:\WINDOWS\system32\WgaTray.exe**, File Name Hash: **881AAD6628B4C7FFFE9B0D4BF02E98004350C9D4**.
- Process ID **1340**, File Name: **C:\WINDOWS\system32\dwwin.exe**, File Name Hash: **E9B24CDF002D6A3DC06802B62E989F00335129CA**.
- Process ID **1352**, File Name: **C:\WINDOWS\Explorer.EXE**, File Name Hash: **7BA51796002B8BEEC6F00FDC583A42008EE45077**.
- Process ID **1476**, File Name: **C:\WINDOWS\system32\spoolsv.exe**, File Name Hash: **2C3E540B00AFB573E240000320EF83001114DA67**.
- Process ID **1564**, File Name: **C:\WINDOWS\system32\DfrgNtfs.exe**, File Name Hash: **812BD95000F634F29CBA0103CCF3BF009D5EB97B**.
- Process ID **1636**, File Name: **C:\WINDOWS\system32\cmd.exe**, File Name Hash: **2751DD6A00570674F0080506F4B6C600B64FDB50**.
- Process ID **1756**, File Name: **C:\WINDOWS\system32\rundll32.exe**, File Name Hash: **8F5576C400BCA32982A2003396ABA600A90A8D28**.
- Process ID **1820**, File Name: **C:\Program Files\Messenger\msmsgs.exe**, File Name Hash: **2AC9751E00467CB2DEE5194C868B040012D12CA7**.
- Process ID **1832**, File Name: **C:\WINDOWS\system32\ctfmon.exe**, File Name Hash: **CB94C76000E5509F3C0D00C310E23300C6DC8A05**.

Mais um exemplo

- Cenário: Um link ou arquivo recebido que o usuário leigo quer saber do que se trata antes de executar.

- Binário: WinPcap_4_1_2.exe
  - Biblioteca de captura de pacotes para windows

- Disponível em:
  - http://www.winpcap.org/

Mais um exemplo (WinPcap_4_1_2.exe)

- Sistema A.

- Summary:
  - Changes security settings of Internet Explorer:
    - This system alteration could seriously affect safety surfing the World Wide Web.
  - Performs File Modification and Destruction:
    - The executable modifiesand destructs files which are not temporary.
  - Performs Registry Activities:
    - The executable reads and modifies registry values. It also creates and monitors registry keys.

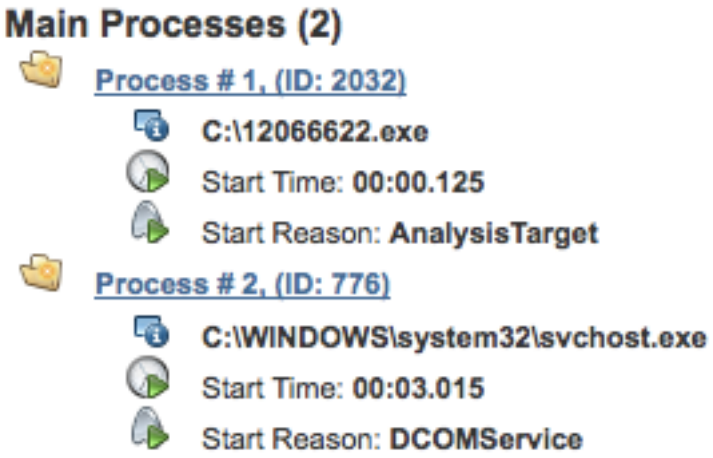
Mais um exemplo (WinPcap_4_1_2.exe)

- […] Muitos blahs depois no Sist.A […]

```
[=- Keyboard Keys Monitored: -=]
Virtual Key Code: [ VK_CONTROL (17) ], 5 times
Virtual Key Code: [ VK_ESCAPE (27) ], 23 times
Virtual Key Code: [ VK_MENU (18) ], 4 times
Virtual Key Code: [ VK_SHIFT (16) ], 10 times
Virtual Key Code: [ VK_LWIN (91) ], 4 times
Virtual Key Code: [ VK_RWIN (92) ], 4 times
Virtual Key Code: [ VK_LBUTTON (1) ], 30 times
Virtual Key Code: [ VK_LCONTROL (162) ], 2 times
Virtual Key Code: [ VK_RCONTROL (163) ], 2 times
```

Mais um exemplo (WinPcap_4_1_2.exe)

- Sistema C.



- Dezenas de processos em execução
- Muitas páginas de entradas relacionadas ao 'svchosts.exe'

- Filtros?

Análise comportamental

- Comportamento é o conjunto das ações efetuadas capturadas durante a execução do binário no alvo.

- Qual o comportamento principal?
  - Ações "interessantes" que o malware faz no alvo…

Behavior Evaluation through
Malware Observation Tool

http://www.las.ic.unicamp.br/paulo/papers/2010-SBSEG-dario.fernandes-andre.gregio-vitor.afonso-rafael.santos-mario.jino-analise.malware.pdf

Análise comportamental (stuxnet)

- O que ele faz *:
  - Registro:
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet
  - Arquivos:
    - %windir%\inf\mdmcpq3.PNF
    - %windir%\inf\mdmeric3.PNF
    - %windir%\inf\oem6C.PNF
    - %windir%\inf\oem7A.PNF
    - %windir%\system32\drivers\mrxcls.sys
    - %windir%\system32\drivers\mrxnet.sys

* http://www.f-secure.com/v-descs/trojan-dropper_w32_stuxnet.shtml

Análise comportamental (stuxnet)

Registro:

```
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxcls\description
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxcls\displayname
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxcls\errorcontrol
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxcls\group
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxcls\imagepath
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxcls\start
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxcls\type
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxcls\data

c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxnet\description
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxnet\displayname
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxnet\errorcontrol
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxnet\group
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxnet\imagepath
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxnet\start
c:\windows\system32\lsass.exe;WRITEREGISTRY;HKLM\system\controlset001\services\mrxnet\type
```

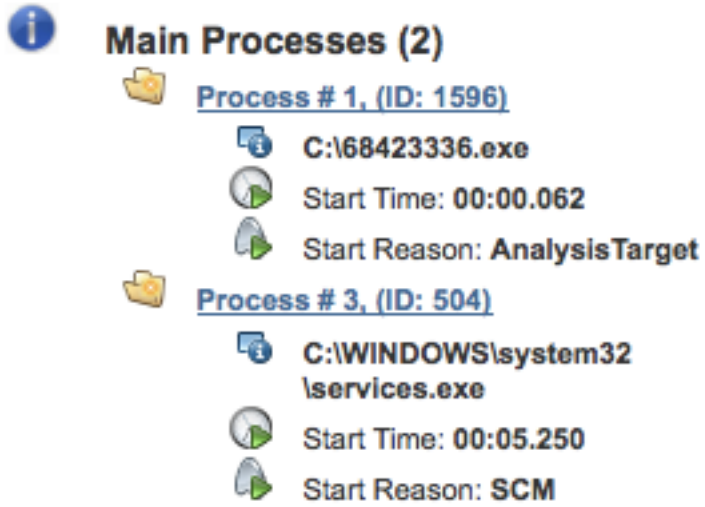
Análise comportamental (stuxnet)

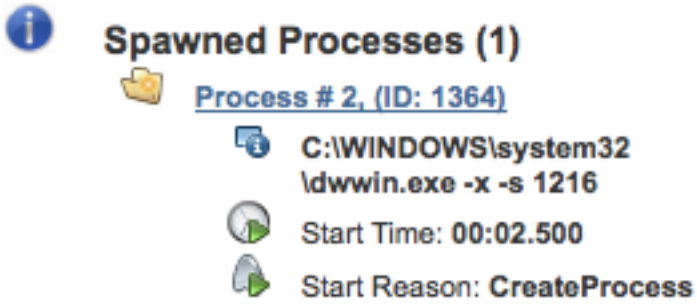
Arquivos:

```
c:\windows\system32\lsass.exe;CREATEFILE;c:\windows
  \inf\oem7a.pnf
c:\windows\system32\lsass.exe;CREATEFILE;c:\windows
  \inf\mdmeric3.pnf
c:\windows\system32\lsass.exe;CREATEFILE;c:\windows
  \inf\mdmcpq3.pnf
c:\windows\system32\lsass.exe;CREATEFILE;c:\windows
  \inf\oem6c.pnf
c:\windows\system32\lsass.exe;CREATEFILE;c:\windows
  \system32\drivers\mrxcls.sys
c:\windows\system32\lsass.exe;CREATEFILE;c:\windows
  \system32\drivers\mrxnet.sys
```

Outros relatórios disponíveis (C)

http://www.sunbeltsecurity.com/cwsandboxreport.aspx?id=68423336&cs=12A40DE4AE53E6CA8609D327E8267E91





- Nenhum dos registros mencionados apareceu.
- Tampouco os arquivos criados.
  - O programa deu erro durante a execução!

Outros relatórios disponíveis (A)

http://anubis.iseclab.org/?action=result&task_id=1e419ccc05bbe3104ddef15d3732ecc3a&format=txt

Arquivos:

```
File Name: [ C:\WINDOWS\inf\mdmcpq3.PNF ]
File Name: [ C:\WINDOWS\inf\mdmeric3.PNF ]
File Name: [ C:\WINDOWS\inf\oem6C.PNF ]
File Name: [ C:\WINDOWS\inf\oem7A.PNF ]
File Name: [ C:\WINDOWS\system32\Drivers
  \mrxcls.sys ]
File Name: [ C:\WINDOWS\system32\Drivers
  \mrxnet.sys ]
```

Outros relatórios disponíveis (A)

Registro:

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxCls**], Value Name: [Data], New Value: [0x8f1ff76d7db1c9099dcc247ac69ffb2390bd9dbff1d451922ab41f6a2ea6]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxCls**], Value Name: [Description], New Value: [MRXCLS]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxCls**], Value Name: [DisplayName], New Value: [MRXCLS]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxCls**], Value Name: [ErrorControl], New Value: [0]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxCls**], Value Name: [Group], New Value: [Network]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxCls**], Value Name: [ImagePath], New Value: [\??\C:\WINDOWS\system32\Drivers\mrxcls.sys]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxCls**], Value Name: [Start], New Value: [1]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxCls**], Value Name: [Type], New Value: [1]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxNet**], Value Name: [Description], New Value: [MRXNET]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxNet**], Value Name: [DisplayName], New Value: [MRXNET]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxNet**], Value Name: [ErrorControl], New Value: [0]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxNet**], Value Name: [Group], New Value: [Network]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxNet**], Value Name: [ImagePath], New Value: [\??\C:\WINDOWS\system32\Drivers\mrxnet.sys]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxNet**], Value Name: [Start], New Value: [1]

Key: [HKLM\SYSTEM\CurrentControlSet\Services**MRxNet**], Value Name: [Type], New Value: [1]

Discussões sobre análise comportamental

- Não basta mostrar um "caminhão" de informações para o usuário, tem de haver a análise.
- Deve-se aceitar que os sistemas tem limitações.
- É preciso se conformar que muitos malware comportam-se como programas legítimos.

Agradecimentos

- Obrigado.

André Grégio

andre.gregio **at** cti gov br

http://www.cti.gov.br

http://www.las.ic.unicamp.br

Centro de Tecnologia da Informação Renato Archer

UNICAMP