Brazil Automation
ISA 2012

ANTIVIRUS É EFICIENTE PARA A PROTEÇÃO DE REDES INDUSTRIAIS?

Marcelo Branquinho & Jan Seidl

Novembro de 2012

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Apresentação

Marcelo Branquinho
(marcelo.branquinho@tisafe.com)

- Diretor executivo da TI Safe. Membro sênior da ISA e integrante do comitê da norma ANSI/ISA-99. Pesquisador em tecnologias de segurança para proteção de infraestruturas críticas.

Jan Seidl
(jan.seidl@tisafe.com)

- Coordenador técnico da TI Safe. Especialista em análise de riscos em sistemas de automação e pesquisador na área de engenharia de Malware.

Brazil Automation
ISA 2012

Siga a TI Safe nas Redes Sociais

- Twitter: @tisafe
- SlideShare: www.slideshare.net/tisafe
- Facebook: www.facebook.com/tisafe
- Flickr: http://www.flickr.com/photos/tisafe

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Não precisa copiar...

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Agenda

- Malware em redes de automação
- Demonstração de infecção em planta química
- Objetivo do trabalho
- Metodologia utilizada
- Ataques desenvolvidos
- Resultados dos testes
- Conclusão
- Treinamento e conscientização

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Malware em redes de automação

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Malware

- *Malware*, ou software malicioso, é um termo relativamente novo para o mundo da tecnologia da informação.
- Agrupa todo software ou programa criado com a intenção de abrigar funções para:
  - penetrar em sistemas
  - quebrar regras de segurança
  - servir de base para operações ilegais e/ou prejudiciais

Brazil Automation
ISA 2012

Exemplos de Malware

- Virus
  - Funções de cópia e dispersão
- Worms
  - Propagam independente das ações do usuário
- Trojans
  - Fingem executar uma tarefa, enquanto executam outra, indesejada
- Zumbis DDoS / BOTs
  - Abrem o computador para processar por terceiros
- Spyware e Adware
  - Originalmente, suportavam o desenvolvimento de programas
- Pranks
  - “Implicam” com o usuário

ISA América do Sul
Distrito 4

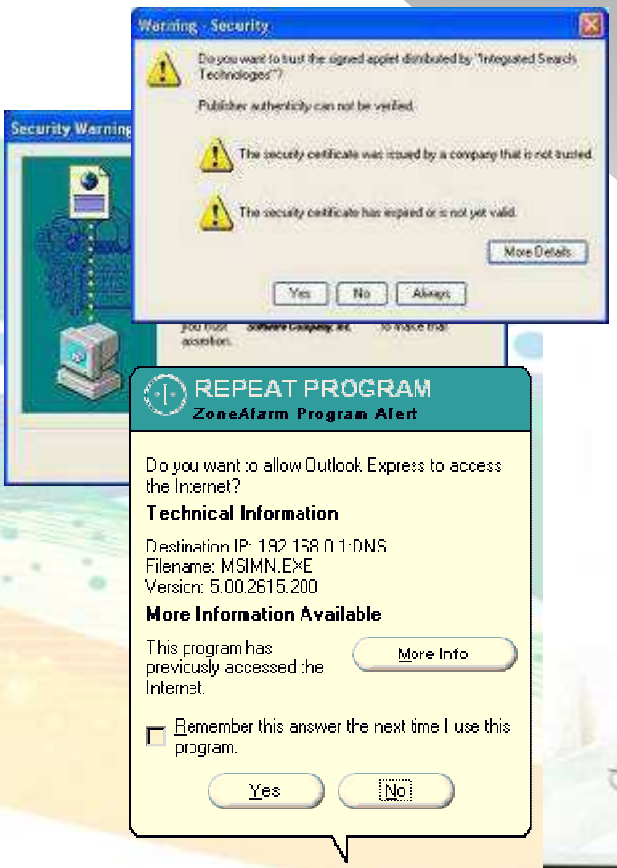
Brazil Automation
ISA 2012

Vetores de infecção

- Exploits
- Mídias removíveis (Pen Drives, HD Externos)
- Compartilhamentos na rede
- Redes externas (conexões com redes de outras empresas)
- Redes 3G
- VPNs
- Funcionários insatisfeitos
- Falta de perícia do usuário (clicar no anexo...)

Brazil Automati
ISA 2012

Usuário “Clicador Feliz”



Acho que tenho que clicar em “sim”!

Brazil Automation
ISA 2012

Incidentes no Brasil

- Na maioria dos casos de contaminações que observamos em nossos clientes existia uma solução de antivírus instalada na rede que foi infectada.
- Esta solução não foi capaz de detectar e impedir o alastramento da infecção por toda a rede.

Incidentes	# Casos
Malware	**5**
Erro Humano	**14**
Falhas em dispositivos	**7**
Outros	**4**

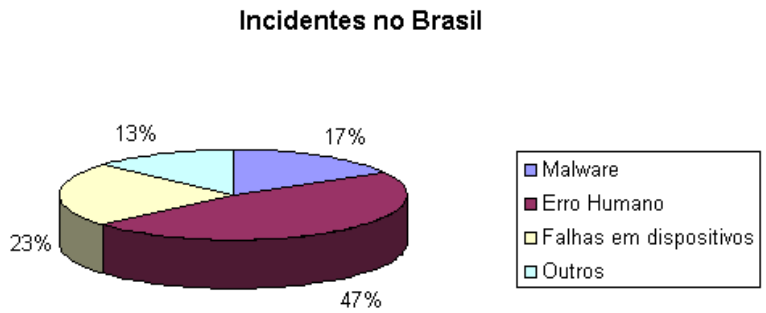


Figura: Incidentes em sistemas de automação no Brasil (*TI Safe Knowledge Base*)

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Demonstração de infecção em planta química

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Ataques por vírus a uma indústria química

Utilizando a plataforma TSSS, serão apresentados dois ataques em sequência através de infecção por vírus:

1)No primeiro ataque a visibilidade da IHM será cortada e o operador não conseguirá mais receber dados do campo.

2)No segundo ataque a programação dos set points das bombas hidráulicas será alterada pelo vírus provocando o transbordamento do tanque químico.

Brazil Automation
ISA 2012

Objetivo do trabalho

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Objetivo do Trabalho

- Análises de soluções de antivírus encontradas na Internet e em revistas especializadas avaliam a efetividade na prevenção de contaminação em computadores pessoais ou de redes corporativas, mas não são adequadas para serem usadas como base para a escolha de soluções para redes SCADA.
- Buscando orientar melhor os nossos clientes sobre qual a melhor solução de antivírus a ser usada em uma planta de automação, resolvemos investigar de forma independente e sem nenhuma influência de qualquer fabricante, até que ponto as soluções de antivírus de mercado são eficazes na detecção e combate de ameaças.
- Este trabalho apresenta uma série de testes realizados em nossos laboratórios visando medir a eficácia de cada solução de antivírus contra ataques de baixo e médio nível de complexidade utilizando ferramentas de ataque baixadas da Internet.

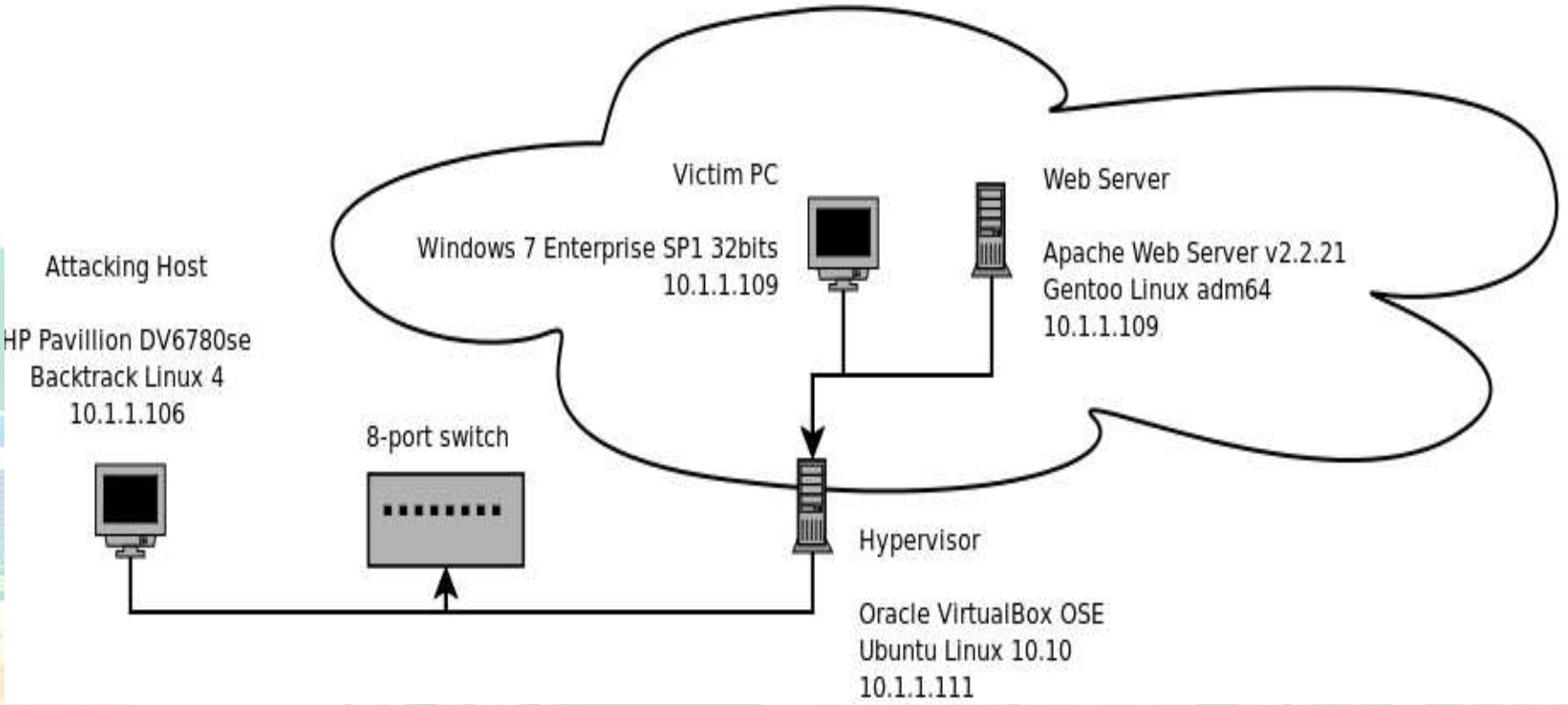
Brazil Automation
ISA 2012

Metodologia utilizada

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

A rede virtual de testes



Brazil Automation
ISA 2012

Metodologia dos testes

A metodologia empregada para a realização dos testes obedece à sequencia de passos detalhada abaixo:

a) Configuração da máquina vítima com a solução de antivírus a ser testada: A partir da máquina virtual em seu 'Estado Inicial', instalamos e configuramos a solução de antivírus a ser testada. Após a instalação, registro da licença (quando disponível) e completa atualização da base de assinaturas da solução de antivírus, foi obtido um novo *snapshot* da máquina chamado de 'Estado Protegido'.

b) Execução de ataque: a máquina vítima em 'Estado Protegido' é submetida ao primeiro ataque da lista e são anotados os resultados.

c) Restauração da máquina vítima: após o ataque ter sido testado, é restaurado o snapshot da máquina vítima em 'Estado Protegido' e o próximo ataque é realizado. Esta sequência é repetida até que todos os ataques tenham sido realizados com o antivírus em testes. Finalizados os testes para este antivírus a sequência é repetida para o próximo antivírus.

Brazil Automation
ISA 2012

Soluções de antivírus testadas

- McAfee Antivirus Plus 2012
- Kaspersky Antivirus 2012
- Panda Antivirus Pro 2012
- Trend Titanium Maximum Security 2012
- Norton Antivirus 2012
- F-Secure Antivirus 2012
- avast! Pro Antivirus 6
- AVG Anti-Virus FREE 2012
- Sophos Anti-Virus 7
- Microsoft Security Essentials
- E-SET NOD32 Antivirus 5

Todos os softwares de antivírus testados (excetuando-se os gratuitos) foram obtidos a partir dos *websites* de seus fabricantes em suas versões para avaliação em versões 32 bits e em idioma inglês. Todos foram instalados na opção 'Recomendada'.

Brazil Automation
ISA 2012

Ataques realizados

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Descrição dos ataques

As amostras de malware utilizadas nos testes foram em parte geradas pelo *Metasploit Framework* através da árvore oficial Subversion (SVN), parte injetada por vetores web, parte utilizada de injetores de código *open source* e parte fabricada internamente pela equipe de segurança SCADA da TI Safe. As 16 amostras de malware utilizadas nos testes foram as seguintes:

1)“EICAR”: Arquivo de testes de Antivírus EICAR.

2)“Metasploit EXE Default Template (no encryption)”: Binário gerado pelo Metasploit Framework com payload Meterpreter (interpretador nativo do MSF) com template de binário padrão, sem criptografia de payload.

Brazil Automation
ISA 2012

Descrição dos ataques

3) “Metasploit EXE Default Template (shikata_ga_nai)”: Binário gerado pelo Metasploit Framework com payload Meterpreter (interpretador nativo do MSF) com template de binário padrão e criptografia de payload shikata_ga_nai.

4) “Metasploit EXE Notepad Template (no encryption)”: Binário gerado pelo Metasploit Framework com payload Meterpreter (interpretador nativo do MSF) com template do Bloco de Notas (notepad.exe) original do Windows 7 Turco, sem criptografia de payload.

Brazil Automation
ISA 2012

Descrição dos ataques

5) "Metasploit EXE Notepad Template (shikata_ga_nai)": Binário gerado pelo Metasploit Framework com payload Meterpreter (interpretador nativo do MSF) com template do Bloco de Notas (notepad.exe) original do Windows 7 Turco e criptografia de payload shikata_ga_nai.

*6) "*Metasploit EXE SkypePortable Template (shikata_ga_nai)": Binário gerado pelo Metasploit Framework com payload Meterpreter (interpretador nativo do MSF) com template do instalador do Skype Portable (SkypePortable_online.paf.exe), com criptografia de payload shikata_ga_nai.

7) "Metasploit LOOP-VBS Default Template (no encryption)": Script VBS gerado pelo Metasploit Framework com payload Meterpreter (interpretador nativo do MSF), sem criptografia de payload.

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Descrição dos ataques

8) “Metasploit LOOP-VBS Default Template (shikata_ga_nai)”: Script VBS gerado pelo Metasploit Framework com payload Meterpreter (interpretador nativo do MSF), com criptografia de payload.

9) “Shellcodexec Default w/ VBS launcher”: Injetor de código ShellcodeExec[5] com launcher em VBS e payload alfanumérico gerado pelo MSF. O injetor de código ShellCodeExec funciona recebendo o payload alfanumérico como argumento na linha de comando.

10) “TI Safe Modded Shellcodeexec (w/ VBS launcher)”: Injetor de código ShellcodeExec modificado pela TI Safe com launcher em VBS e payload alfanumérico gerado pelo MSF.

Brazil Automation
ISA 2012

Descrição dos ataques

11) “TI Safe Modded Shellcodeexec (Custom EXE w/ embedded payload)”: Injetor de código ShellcodeExec modificado pela TI Safe com payload alfanumérico gerado pelo MSF embutido.

12) “TI Safe Custom Payload Launcher”: Injetor de código criado em laboratório pela equipe da TI Safe com payload alfanumérico gerado pelo MSF embutido e sistema rudimentar de evasão de máquinas virtuais de softwares antivirus.

13) “Metasploit PDF (adobe_utilprintf)”: Meterpreter embutido em exploit de PDF adobe_util.printf6

Brazil Automation
ISA 2012

Descrição dos ataques

14) “Metasploit PDF (adobe_pdf_embedded_exe)”: Meterpreter embutido em exploit de PDF adobe_pdf_embedded_exe7

15) “Metasploit PDF (adobe_pdf_embedded_exe_nojs)”: Meterpreter embutido em exploit de PDF adobe_pdf_embedded_exe_nojs8

16) “Metasploit Java Applet”: Meterpreter embutido em Java Applet via ataque Web. Utilizamos o SET (Social Engineering Toolkit) para gerar um ataque web clonando um website existente.

A descrição técnica completa e o as-built de todos os ataques poderá ser obtida a partir do trabalho técnico que faz parte dos anais do congresso.

Brazil Automation
ISA 2012

Resultados dos testes

ISA América do Sul
Distrito 4

Matriz de resultados

		Soluções de Antivirus Testadas										
	Ataques Executados	McAfee Antivirus Plus 2012	Kaspersky Antivirus 2012	Panda Antivirus Pro 2012	Trend Titanium Maximum Security	Norton Antivirus 2012	F-Secure Antivirus 2012	avast! Pro Antivirus 6	AVG Anti-Virus FREE 2012	Sophos Anti-Virus 7	Microsoft Security Essentials	E-SET NOD32 Antivirus 5
1	EICAR	EICAR test file	EICAR-Test-File	EICAR-AV-TEST-FILE	Eicar_test_file	EICAR Test String	Trojan.Generic.6567028	EICAR Test-NOT virus!!!	EICAR_Test	EICAR-AV-Test	DOS/EICAR_Test_File	Eicar test file
2	Metasploit EXE Default Template (no encryption)	Swrort.f	Trojan.Win32.Generic	Suspicious File	TROJ_SWRORT.SME	Packed.Generic.347	Backdoor.Shell.AC	Win32:SwPatch	Win32/Heur	Mal/EncPk-ACE	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AA trojan
3	Metasploit EXE Default Template (shikata_ga_nai)	Swrort.d	Trojan.Win32.Generic	Suspicious File	TROJ_SWRORT.SME	Packed.Generic.347	Backdoor.Shell.AC	Win32:SwPatch	Win32/Heur	Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AH trojan
4	Metasploit EXE Notepad Template (no encryption)	Swrort.f	Trojan.Win32.Generic	Trj/Genetic.gen	-	-	Backdoor.Shell.AC	Win32:SwPatch	-	Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AA trojan
5	Metasploit EXE Notepad Template (shikata_ga_nai)	Swrort.d	Trojan.Win32.Generic	Trj/Genetic.gen	-	-	Backdoor.Shell.AC	Win32:SwPatch	Win32/Heur	Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AH trojan
6	Metasploit EXE SkypePortable Template (shikata_ga_nai)	Swrort.d	Trojan.Win32.Generic	-	-	-	Backdoor.Shell.AC	Win32:SwPatch	-	Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AH trojan
7	Metasploit LOOP-VBS Default Template (no encryption)	Swrort.f	Trojan.Win32.Generic	Script Blocked	TROJ_SWRORT.SME	Packed.Generic.347	Backdoor.Shell.AC	Win32:SwPatch	-	Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AA trojan
8	Metasploit LOOP-VBS Default Template (shikata_ga_nai)	Swrort.f	Trojan.Win32.Generic	Script Blocked	TROJ_SWRORT.SME	Packed.Generic.347	Backdoor.Shell.AC	Win32:SwPatch	-	Mal/Swrort-C	Trojan.Win32/Swrort.A	a variant of Win32/Rozena.AH trojan
9	Shellcodexec Default w/ VBS launcher	Generic.tfr!i	Trojan.Win32.Genome .vrrg	Trj/CI.A	-	Trojan.Gen	Trojan.Generic.6567028	Win32:Malware-gen	Trojan Generic22.KPM	Mal/Generic.L	-	Win32/ShellcodeRunner.A trojan
10	TI Safe Modded Shellcodeexec (w/ VBS launcher)	-	-	Script Blocked	-	-	-	-	-	-	-	-
11	TI Safe Modded Shellcodeexec (Custom EXE w/ embedded payload)	-	-	-	-	-	Backdoor.Shell.AC	-	Trojan Generic22.SND	-	Trojan.Win32/Swrort.A	-
12	TI Safe Custom Payload Launcher	-	-	-	-	-	-	-	-	Mal/FakeAV-FS	-	-
13	Metasploit PDF (adobe_utilprintf)	Exploit.PDF.bk.gen	Exploit.JS.Pdfka.cil	-	HEUR_PDFEXP.B	Bloodhound.Exploit.213	Exploit.PDF-JS.Gen	JS:Pdfka-gen	Script/Exploit	Troj/PDFJs-B	Trojan.Win32/Swrort.A	JS/Exploit.Pdfka.NOO trojan
14	Metasploit PDF (adobe_pdf_embedded_exe)	Swrort.f	Trojan.Win32.Generic	Suspicious File	TROJ_SWRORT.SME	Bloodhound.PDF.24	Exploit.PDF-Dropper.Gen	Win32:SwPatch	Exploit.PDF	Mal/Swrort-C	Trojan.Win32/Swrort.A	PDF/Exploit.Pidief.PFW trojan
15	Metasploit PDF (adobe_pdf_embedded_exe_nojs)	Swrort.f	Trojan.Win32.Generic	Suspicious File	TROJ_PIDIEF.SMEO	Bloodhound.PDF.24	Exploit.PDF-Dropper.Gen	PDF:Launchr-C	Exploit	Mal/Swrort-C	Trojan.Win32/Swrort.A	PDF/Exploit.Pidief.PFT trojan
16	Metasploit Java Applet	-	-	-	-	-	-	-	-	-	-	-

Brazil Automation
ISA 2012

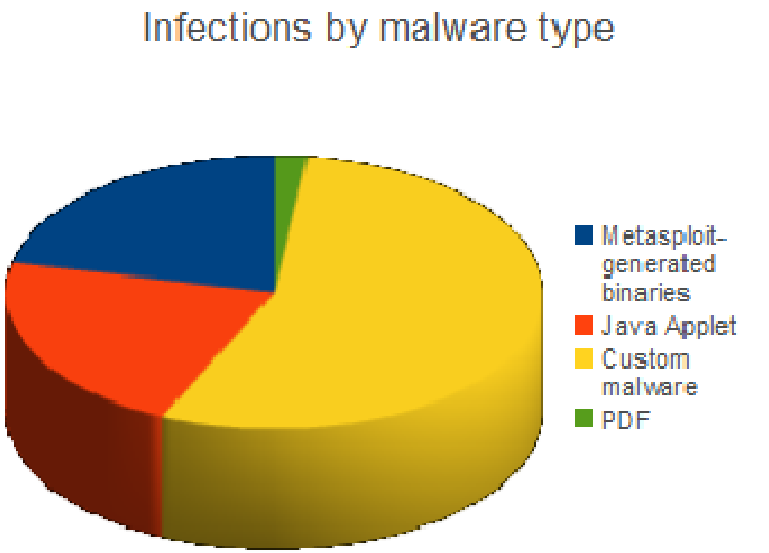
Análise de resultados

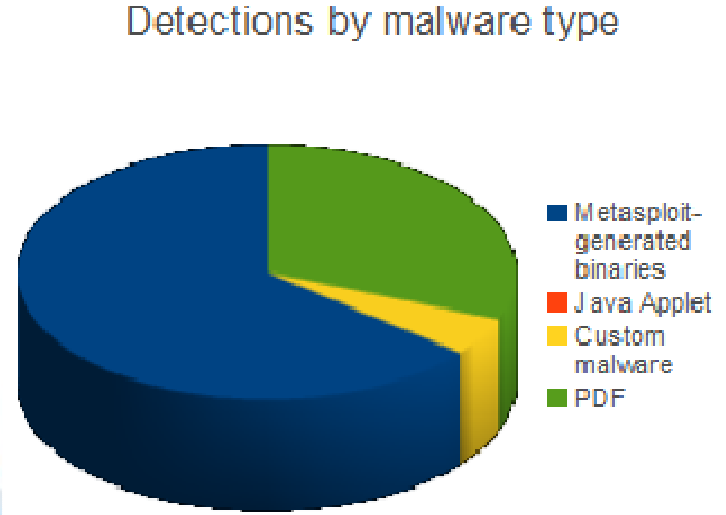
A partir da análise da matriz de resultados foi possível observar que:

- A grande maioria das detecções foi baseada em heurística.
- A grande maioria das soluções de antivírus não foi capaz de detectar a ameaça na memória.
- Apenas duas soluções reagiram por comportamento.
- Nenhuma solução que conseguiu detectar um ataque foi capaz de pará-lo.
- Nenhuma das soluções conseguiu a nota máxima.
- Nenhuma das soluções conseguiu detectar mais de uma amostra de malware criada em laboratório pela equipe da TI Safe (ataques 10,11 e 12).
- Em termos de heurística, há soluções comerciais que tiveram desempenho inferior a soluções gratuitas e outras que tiveram desempenho equivalente.
- Todos os candidatos falharam em prevenir o ataque pelo applet Java (ataque 16).

Brazil Automation
ISA 2012

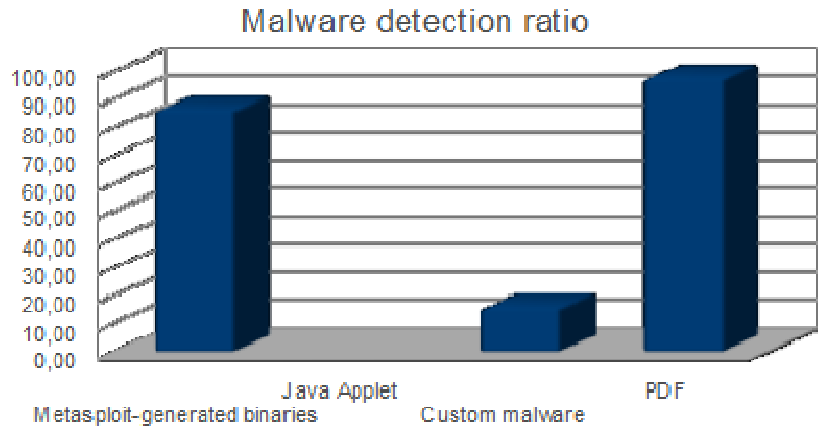
Infecções e detecções por tipo de Malware

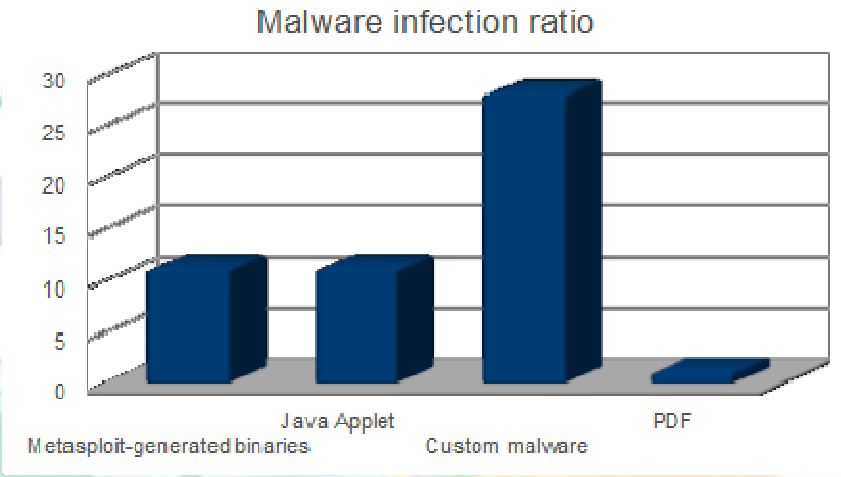




Brazil Automation
ISA 2012

Taxas de detecção e de infecção





Brazil Automation
ISA 2012

Ranking das soluções testadas

#	Produto	Score
1	F-Secure Antivírus 2012	13
	Sophos Antivírus 7	
2	McAfee Antivírus Plus 2012	12
	Kaspersky Antivírus 2012	
	avast! Pro Antivírus 6	
	Microsoft Security Essentials	
	E-SET NOD32 Antivírus 5	
3	Panda Antivírus Pro 2012	11
4	Norton Antivírus 2012	9
	AVG Antivírus FREE 2012	
5	Trend Titanium Maximum Security	8

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Conclusão

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Conclusão

- Nossos testes mostraram que quando o malware é um pouco mais sofisticado ou explora vulnerabilidades Windows desconhecidas (*zero-day*), os antivírus de mercado são muito pouco eficientes para a proteção.
- Podemos afirmar que nenhuma solução de antivírus de mercado é capaz de fornecer completa proteção às redes de automação e levam as empresas a terem uma "falsa sensação de segurança".
- Soluções de antivírus são recomendáveis, mas não fornecem toda a segurança necessária em sistemas de controle de uma planta de automação. É necessário o uso de controles complementares.

Brazil Automation
ISA 2012

Conclusão

- Recomendamos as seguintes práticas de segurança em complemento ao uso do antivírus:
  - Segmentar a rede de automação segundo o que recomenda a norma ANSI/ISA-99 em seu modelo de zonas e conduítes. Na entrada de cada zona de segurança deve haver equipamento de segurança de borda como Firewalls e sistemas de detecção e prevenção de intrusões (IDPSs) com assinaturas contra ataques SCADA.
  - Revisão periódica da configuração das regras dos firewalls que protegem a rede de automação orientada pelas melhores práticas do mercado.
  - O Rígido controle sobre qualquer dispositivo que seja conectado à rede SCADA (laptops de terceiros, mídias removíveis, modems e outros) e a inspeção profunda de novos programas antes de eles serem instalados pode aumentar e muito o nível de segurança e evitar infecções.
  - Não permitir o uso de e-mail e acesso à web de dentro da rede de automação e, na medida do possível, atualizar os patches de segurança dos computadores mais críticos.

Brazil Automation
ISA 2012

Conclusão

- Além da prevenção as empresas devem estar preparadas para o pior e possuir um plano de contingência para o caso de tudo dar errado e a planta de automação ser infectada.
- É essencial ter ferramentas de backup automatizado instaladas além de redundância nos servidores críticos da rede de automação.
- Nossa experiência mostra que o processo de desinfecção de uma rede de automação contaminada é bastante oneroso, complexo e depende da colaboração dos fabricantes para o sucesso, o que torna o processo lento.
- Incentivamos a comunidade internacional a criar um guia de boas práticas para a desinfecção de plantas de automação que possa servir como linha base para orientar as empresas que estejam passando por este problema a retomar o controle sobre seus sistemas de controle e supervisão de uma forma planejada e preferencialmente rápida.

Brazil Automation
ISA 2012

Treinamento e conscientização

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Formação em segurança de automação industrial

- Baseada na norma ANSI/ISA-99
- Escopo:
  - Introdução às redes Industriais e SCADA
  - Infraestruturas Críticas e Cyber-terrorismo
  - Normas para segurança em redes industriais
  - Introdução à análise de riscos
  - Análise de riscos em redes industriais
  - Malware em redes industriais e ICS
  - Desinfecção de redes industriais contaminadas por Malware
  - Uso de firewalls e filtros na segurança de redes industriais
  - Uso de Criptografia em redes industriais
  - Segurança no acesso remoto à redes industriais
  - Implementando o CSMS (ANSI/ISA-99) na prática

- Aulas ministradas nas instalações da TI Safe ou na empresa (mínimo de 10 alunos)
- Alunos recebem material didático em formato digital
- Formação com 20h de duração
- Instrutor membro da ISA Internacional e integrante do comitê da norma ANSI/ISA-99, com anos de experiência em segurança de automação industrial
- Objetiva formar profissionais de TI e TA:
  - ⇨ Apresenta, de forma teórica e prática, aplicações reais da segurança de acordo com o CSMS (Cyber Security Management System) preconizado pela norma ANSI/ISA-99
  - ⇨ Totalmente em português, adequada ao perfil do profissional de segurança requerido pelas empresas brasileiras
- Calendário com próximas turmas disponível em http://www.tisafe.com/solucoes/treinamentos/

ISA América do Sul
Distrito 4

Brazil Automation
ISA 2012

Dúvidas?

Marcelo.branquinho@tisafe.com

Jan.seidl@tisafe.com

(21) 2173-1159 / (11) 3040-8656

Twitter: @tisafe

Skype: ti-safe

ISA América do Sul
Distrito 4