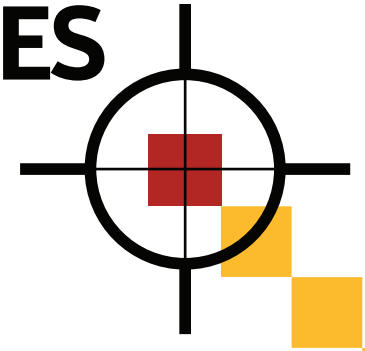
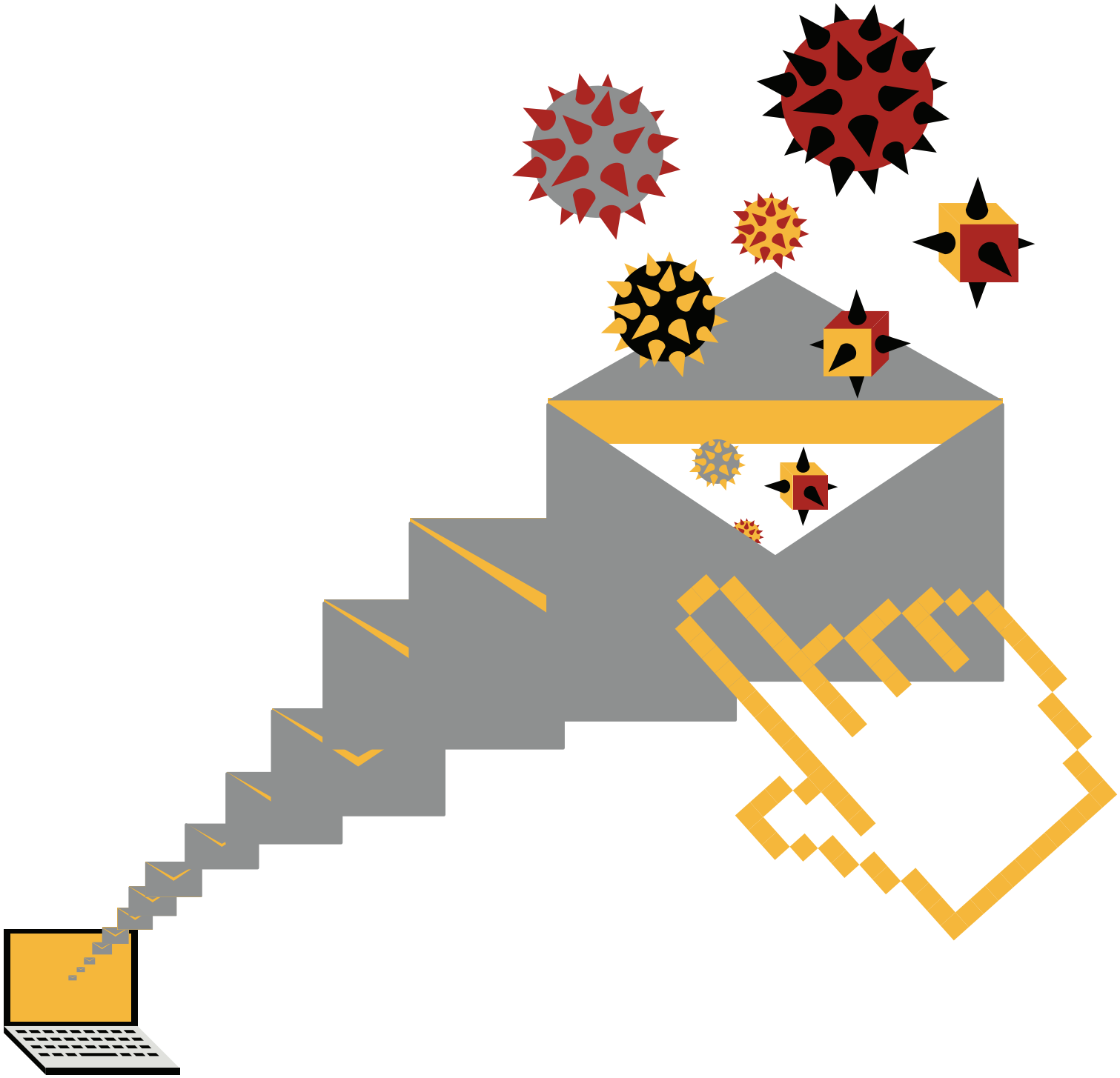
RELATÓRIO SOBRE AMEAÇAS À SEGURANÇA NA INTERNET PRINCIPAIS CONCLUSÕES



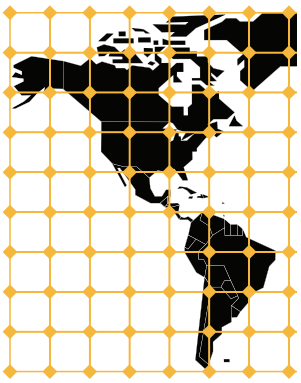
Região das Américas

Abril 2012

Symantec™



Conteúdo



Introdução

A Symantec desenvolveu algumas das mais abrangentes fontes de dados do mundo sobre ameaças da Internet através da Symantec™ Global Intelligence Network, que é composta por mais de 64,6 milhões de sensores de ataques e registros milhares de eventos por segundo. Essa rede monitora a atividade de ataques em mais de 200 países e territórios por meio de uma combinação de produtos e serviços da Symantec, como o Symantec DeepSight™ Threat Management System, o Symantec™ Managed Security Services e os produtos de consumo Norton™; bem como fontes de dados de terceiros.

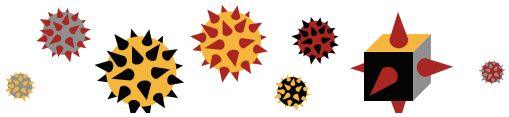
Além disso, a Symantec mantém um dos mais completos bancos de dados do mundo sobre vulnerabilidades, atualmente com mais de 47.662 itens registrados (abrangendo mais de duas décadas) a partir de mais de 15.967 fornecedores representando mais de 40.006 produtos.

Dados de spam e phishing são capturados através de uma variedade de fontes, incluindo a Symantec Probe Network - um sistema de mais de 5 milhões de contas de chamariz, a Symantec.cloud bem como outras tecnologias de segurança da Symantec. A Skeptic™, tecnologia heurísitica proprietária da Symantec.cloud é capaz de detectar novas e sofisticadas ameaças direcionadas antes que elas alcancem as redes dos clientes. Mais de 8 bilhões de mensagens de e-mail e mais de 1,4 bilhão de solicitações da Web são processados diariamente em 15 data centers. A Symantec também coleta informações de phishing por meio de uma extensa comunidade antifraude que reúne empresas, fornecedores de soluções de segurança e mais de 50 milhões de consumidores.

Esses recursos dão aos analistas da Symantec incomparáveis fontes de dados para identificar, analisar e prover informações com comentários sobre as tendências emergentes na área de ataques, atividade de programas maliciosos, phishing e spam. O resultado é o Relatório da Symantec sobre Ameaças à Segurança na Internet, que fornece a empresas e consumidores informações essenciais para protegerem seus sistemas de forma eficaz, agora e no futuro. Além de coletar dados globais sobre ataques na Internet, a Symantec também analisa dados de ataques que são detectados pelos sensores eletrônicos em regiões específicas. Este relatório aborda os principais aspectos das atividades maliciosas que a Symantec observou na região das Américas em 2011.

Tendências em atividade maliciosa: Região das Américas

A próxima seção do Relatório da Symantec sobre Ameaças à Segurança na Internet para a Região das Américas (incluindo América do Norte e América Latina) fornece uma análise das atividades de ameaças, atividades maliciosas e violações de dados que a Symantec observou na região das Américas em 2011. A atividade maliciosa discutida nesta seção inclui não apenas a atividade de ameaças, mas também de phishing, códigos maliciosos, spam zombies, computadores infectados por bots e origens de ataques de rede. Define-se ataque como qualquer atividade maliciosa efetuada através de uma rede que foi detectada por um sistema de detecção de intrusões (Intrusion Detection System - IDS) ou firewall. As definições de outros tipos de atividades maliciosas podem ser encontradas em suas respectivas seções neste relatório. Esta discussão baseia-se em atividades maliciosas de ameaça detectadas pela Symantec na região das Américas em 2011.



Background

Essa métrica avalia os países da região das Américas (incluindo América do Norte e América Latina) nos quais ocorre ou se origina o maior volume de atividades maliciosas. Em geral, as atividades maliciosas afetam computadores que estão conectados à Internet de alta velocidade, porque essas conexões são alvos atraentes para os invasores. A banda larga apresenta capacidades maiores do que outros tipos de conexão, velocidades mais altas, a possibilidade de manter os sistemas sempre conectados e, em geral, uma conexão mais estável. A Symantec classifica as atividades maliciosas como a seguir: :

- **Código malicioso** - Isso inclui vírus, worms e Cavalos de Tróia que são secretamente inseridos em programas. Os propósitos do código malicioso são destruir dados, executar programas destrutivos ou invasivos, roubar informações confidenciais, comprometer a segurança ou a integridade dos dados do computador da vítima.
- **Spam Zombies** - É um sistema invadido, controlado remotamente e usado para enviar grandes volumes de mensagens de e-mails inúteis ou não solicitadas. Esses e-mails podem ser usados para liberar códigos maliciosos e tentativas de phishing.
- **Hospedeiro de phishing:** - É um computador que provê serviços de site para tentar ilegalmente coletar informações confidenciais, pessoais e financeiras, passando-se por solicitação de uma organização confiável e bem conhecida. Esses sites são desenvolvidos para reproduzir sites de empresas legítimas.
- **Computador infectado por bots -** É um computador invadido, controlado remotamente por invasores. Normalmente, o invasor remoto controla um grande número de computadores através de um canal único e confiável em uma rede de bots (botnet), que é utilizado para lançar ataques coordenados.
- **Origens de ataques de redes** - Fontes que originam os ataques a partir da Internet. Por exemplo, alguns ataques podem ter como alvo os protocolos de SQL ou vulnerabilidades de buffer overflow.
- **Origens de ataques baseados na Web** - Fontes de ataque via Web ou através de HTTP. Normalmente, sites legítimos são invadidos e usados para atacar visitantes desavisados.

Metodologia

Para determinar atividades maliciosas por origem geográfica, a Symantec compilou dados geográficos sobre diversas atividades maliciosas, incluindo relatórios de códigos maliciosos, spam zombies, hospedeiros de phishing, computadores infectados por bots e origens de ataques de rede. A proporção de cada atividade originada em cada geografia é determinada, em seguida, dentro da região. A média das porcentagens de cada atividade maliciosa que se origina em cada geografia é calculada. Essa média determina a proporção de atividades maliciosas em geral que se origina na região geográfica em questão. Em seguida, determina-se o ranking, calculando a média das médias dessas atividades maliciosas originadas em cada geografia.

DADOS

Figura G.1

Atividade Maliciosa por Fontes: Ranking das Américas, 2011

País	Ranking regional 2011	Ranking mundial 2011	Ranking regional 2011 - Código Malicioso	Ranking regional 2011 – Spam Zombies	Ranking regional 2011 - Hosts de phishing	Ranking regional 2011 – Bots	Ranking regional 2011 – Ataques de Rede	Ranking regional 2011 – Ataques Web por País
Brasil	1	4	1	1	1	1	1	1
Estados Unidos	1	1	1	1	1	1	1	1
Argentina	2	22	5	2	3	2	2	4
Canadá	2	16	2	2	2	2	2	2
Colômbia	3	28	3	5	2	7	5	5
México	4	29	2	7	5	6	3	2
Chile	5	34	4	4	4	4	4	3
Perú	6	41	7	3	10	3	7	11
Venezuela	7	11	6	9	9	9	6	6
República Dominicana	8	54	9	6	25	5	9	15
Uruguai	9	61	20	8	15	13	8	9
Porto Rico	10	73	11	17	20	8	10	13

Fonte: Symantec *Países da América do Norte

Figura G.2

Atividade Maliciosa por Código Malicioso - Américas, 2011

País de Origem	Ranking Regional - Código Malicioso 2011	% Regional de Código Malicioso em 2011	Ranking Regional 2011	Ranking Mundial 2011
Estados Unidos	1	91.5%	1	1
Brasil	1	39.9%	1	4
Canadá	2	8.5%	2	16
México	2	21.0%	4	29
Colômbia	3	5.5%	3	28
Chile	4	5.4%	5	34
Argentina	5	4.7%	2	22
Venezuela	6	4.3%	7	52
Peru	7	2.7%	6	41
Jamaica	8	2.0%	16	96
República Dominicana	9	1.8%	8	54
Equador	10	1.5%	12	76

Fonte: Symantec *Países da América do Norte

Figura G.3

Atividade Maliciosa por Spam Zombies - Américas, 2011

País de origem	Ranking Regional – Spam Zombies	% Regional de Spam Sombies 2011	Ranking Regional 2011	Ranking Mundial 2011
Estados Unidos	1	93.9%	1	1
Brasil	1	40.4%	1	4
Canadá	2	6.1%	2	16
Argentina	2	14.9%	2	22
Perú	3	9.7%	6	41
Chile	4	8.8%	5	34
Colombia	5	6.7%	3	28
República Dominicana	6	4.6%	8	54
México	7	4.6%	4	29
Uruguai	8	3.5%	9	61
Venezuela	9	2.1%	7	52
Bolivia	10	1.2%	11	75

Fonte: Symantec *Países da América do Norte

Figura G.4

Atividade Maliciosa por Hosts de Phishing - Américas, 2011

País de origem	Ranking Regional – Host de Phishing 2011	% Regional de Host de Phishing 2011	Ranking Regional 2011	Ranking Mundial 2011
Estados Unidos	1	93.7%	1	1
Brasil	1	39.5%	1	4
Colômbia	2	32.7%	3	28
Canadá	2	6.3%	2	16
Argentina	3	8.2%	2	22
Chile	4	5.5%	5	34
México	5	4.8%	4	29
Panamá	6	2.1%	13	79
Ilhas Virgens (Britânicas)	7	1.1%	18	110
Equador	8	1.0%	12	76
Venezuela	9	0.9%	7	52
Peru	10	0.9%	6	41

Fonte: Symantec *Países da América do Norte

Figura G.5

Atividade Maliciosa por Bots - Américas, 2011

País de origem	Ranking Regional – Bots 2011	% Regional de Bots 2011	Ranking Regional 2011	Ranking Mundial 2011
Brasil	1	66.3%	1	4
Estados Unidos	1	88.6%	1	1
Canadá	2	11.4%	2	16
Argentina	2	16.6%	2	22
Peru	3	4.0%	6	41
Chile	4	3.5%	5	34
República Dominicana	5	2.2%	8	54
México	6	2.2%	4	29
Colômbia	7	1.4%	3	28
Porto Rico	8	1.0%	10	73
Venezuela	9	0.6%	7	52
Bolivia	10	0.5%	11	75

Fonte: Symantec *Países da América do Norte

Figura G.6

Atividade Maliciosa por Origens de Ataques Web - Américas, 2011

País de origem	Ranking Regional – Ataques Web por Geografia 2011	% Regional de Ataques Web por Geografia 2011	Ranking Regional 2011	Ranking Mundial 2011
Estados Unidos	1	96.6%	1	1
Brasil	1	42.6%	1	4
Canadá	2	3.4	2	16
México	2	12.9%	4	29
Chile	3	10.0%	5	34
Argentina	4	7.7%	2	22
Colômbia	5	6.7%	3	28
Venezuela	6	4.7%	7	52
Ilhas Virgens (Britânicas)	7	2.6%	18	110
Panamá	8	2.2%	13	79
Uruguai	9	1.6%	9	61
Equador	10	1.3%	12	76

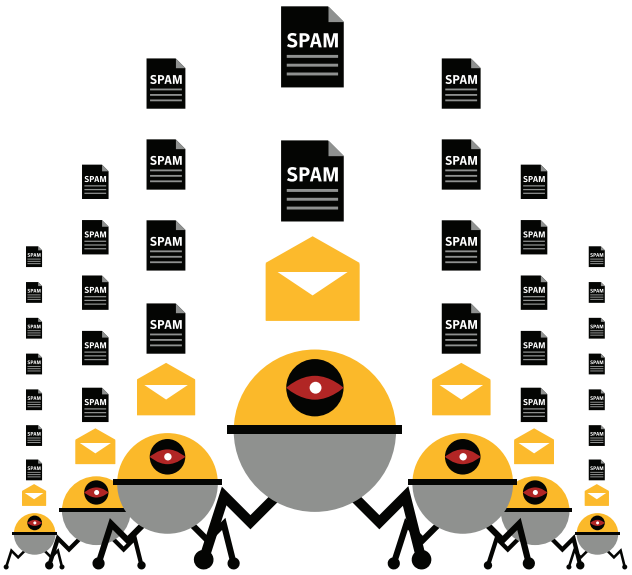
Fonte: Symantec *Países da América do Norte

Figura G.7

Atividade Maliciosa por Origens de Ataques a Redes - Américas, 2011

País de origem	Ranking Regional – Ataques de Rede por Geografia 2011	% Regional de Ataques de Rede por Geografia 2011	Ranking Regional 2011	Ranking Mundial 2011
Brasil	1	42.3%	1	4
Estados Unidos	1	88.5%	1	1
Canadá	2	11.5%	2	16
Argentina	2	14.1%	2	22
México	3	13.0%	4	29
Chile	4	7.0%	5	34
Colômbia	5	6.1%	3	28
Venezuela	6	4.9%	7	52
Peru	7	2.4%	6	41
Uruguai	8	2.0%	9	61
República Dominicana	9	1.6%	8	54
Porto Rico	10	1.2%	10	73

Fonte: Symantec *Países da América do Norte



Comentários

- As atividades maliciosas originadas em computadores infectados no Brasil levaram o país para o topo da tabela como fonte de atividades maliciosas na América Latina em 2011 e para o quarto lugar em nível mundial.
- Os Estados Unidos foram os primeiros na América do Norte e número um em nível global. Brasil e Estados Unidos foram a principal fonte de atividades maliciosas em todas as categorias em cada uma de suas respectivas regiões.
- A Argentina ocupou o segundo lugar geral na América Latina e o segundo lugar em spam zombies, bots, e como fonte de ataques de rede na América Latina.

Origem de ataques por país: Região das Américas

Background

Essa métrica avalia os principais países nos quais se originaram ataques direcionados para a região das Américas em 2011. Observe que, como o computador que ataca pode ser controlado remotamente, o invasor pode estar em um local diferente daquele em que está o computador usado para montar o ataque. Por exemplo, um invasor fisicamente localizado no Brasil pode lançar um ataque a partir de um sistema comprometido na Austrália contra uma rede no Japão.

Metodologia

Essa seção mede os principais países nos quais se originaram ataques direcionados para computadores na região das Américas em 2011. Em geral, considera-se um ataque malicioso de rede, qualquer atividade encontrada pelo sistema de detecção de intrusões (Intrusion Detection System - IDS), sistema de prevenção de intrusões (Intrusion Prevention System - IPS), ou firewall.

DADOS

Figura G.8

Principais Ataques por Fonte - Américas, 2011

País	Posição	% de Ataques contra a Região em 2011	% de Ataques contra a Região em 2010	Variação (%)
Estados Unidos	1	62.3%	n/a	-
China	2	10.1%	n/a	-
Tailândia	3	2.1%	n/a	-
Canadá	4	1.9%	n/a	-
Coreia do Sul	5	1.6%	n/a	-
Rússia	6	1.5%	n/a	-
Reino Unido	7	1.4%	n/a	-
Brasil	8	1.3%	n/a	-
Alemanha	9	1.2%	n/a	-
Taiwan	10	1.1%	n/a	-

Fonte: Symantec *Países da América do Norte

Figura G.8

Principais Ataques por Fonte – América do Norte, 2011

País	Posição	% de Ataques contra a Região em 2011	% de Ataques contra a Região em 2010	Variação (%)
Estados Unidos	1	62.0%	n/a	-
China	2	10.3%	n/a	-
Tailândia	3	2.2%	n/a	-
Canadá	4	1.9%	n/a	-
Coreia do Sul	5	1.7%	n/a	-
Rússia	6	1.5%	n/a	-
Reino Unido	7	1.4%	n/a	-
Brasil	8	1.3%	n/a	-
Alemanha	9	1.2%	n/a	-
Taiwan	10	1.1%	n/a	-

Fonte: Symantec *Países da América do Norte

Figura G.8

Principais Ataques por Fonte - América Latina, 2011

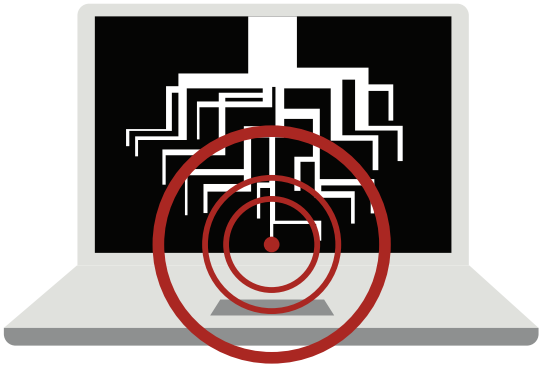
País	Posição	% de Ataques contra a Região em 2011	% de Ataques contra a Região em 2010	Variação (%)
Estados Unidos	1	88.1%	50%	31.8%
Brasil	2	2.3%	7%	-4.7%
México	3	2.1%	14%	-11.9%
China	4	2.0%	2%	0.0%
Reino Unido	5	0.8%	2%	-1.2%
Alemanha	6	0.8%	n/a	-
África do Sul	7	0.8%	n/a	-
Suécia	8	0.6%	n/a	-
Canadá	9	0.6%	1%	-0.4%
Rússia	10	0.6%	1%	-0.4%

Fonte: Symantec *Países da América do Norte

Comentários

- Os Estados Unidos continuam dominando os ataques na região das Américas: em 2011, os Estados Unidos foram o principal país de origem dos ataques contra alvos na região das Américas, respondendo por metade de todos os ataques detectados pelos sensores da Symantec na região.
- Provavelmente, esse resultado é devido ao alto nível de atividades de ataques originados nos Estados Unidos em geral, pois também foi o principal país de origem dos ataques Web globalmente, com 16,9 por cento do total. Ocupou ainda a segunda posição globalmente como fonte de ataques de rede, com 33,5 por cento dos ataques de rede originados nos Estados Unidos.
- Além disso, os Estados Unidos ficaram em primeiro lugar no quesito geral de atividades maliciosas, com 21,1 por cento do total. Os Estados Unidos também ficaram em primeiro lugar globalmente em computadores infectados por bots (12,6 por cento) e na segunda posição em código malicioso (13,3 por cento); grande parte das atividades de ataque que visaram países na região das Américas foi conduzida através dessas redes bot maliciosas.

Tendências de código malicioso: Região das Américas



A Symantec coleta informações sobre códigos maliciosos a partir de sua grande base global de clientes e através de uma série de programas opt-in de telemetria anônima, incluindo o Norton Comunidade Watch, o Symantec Digital Immune System e as tecnologias Symantec Scan and Deliver. Mais de 133 milhões de sistemas servidores, clientes e gateways contribuem ativamente com esses programas. Novas amostras de códigos maliciosos, bem como incidentes de detecção a partir de tipos já conhecidos são relatados à Symantec. Na ausência de software de segurança para detectar e eliminar ameaças, ataques maliciosos são considerados potenciais devido à possibilidade de infecção.

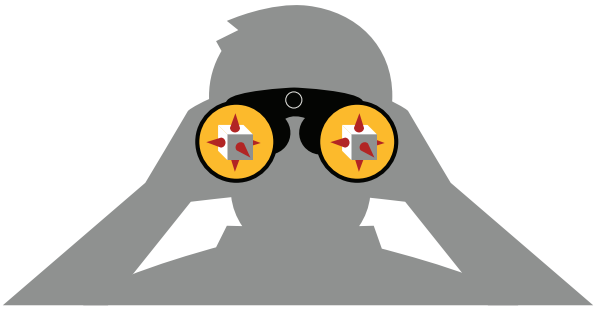
As ameaças de código malicioso são classificadas em quatro tipos principais — backdoor, vírus, worm e Cavalo de Tróia:

- **Backdoors** - permite que um invasor acesse remotamente os computadores comprometidos.
- **Cavalo de Tróia** - é um código malicioso que o usuário instala involuntariamente em seu computador, mais comumente ao abrir anexos de e-mail ou fazendo o download da Internet. Os Cavalos de Tróia também são muitas vezes transferidos e instalados por outro código malicioso. Eles se diferem dos vírus e worms, pois não se propagam.
- **Vírus** - Sse propaga infectando arquivos existentes em computadores afetados com código malicioso.
- **Worm** - é um programa malicioso que pode se replicar em computadores infectados ou de maneira a facilitar sua cópia para outro computador (por exemplo, via dispositivos de armazenamento USB).

Muitas ameaças de código malicioso têm características múltiplas. Por exemplo, um backdoor é sempre classificado em conjunto com outra característica de código malicioso. Normalmente, os backdoors também são Cavalos de Tróia. Por outro lado, muitos vírus e worms também incorporam funcionalidades de backdoor. Além disso, muitas amostras de código malicioso podem ser classificadas como worms e vírus devido à forma como se propagam. Uma razão para isso é que os desenvolvedores de ameaças tentam ativar o código malicioso com vários vetores de propagação para aumentar as chances de comprometer com sucesso os computadores nos ataques.

Essa discussão é baseada em amostras de código malicioso detectadas pela Symantec na região das Américas em 2011.

Principais amostras de código malicioso: Região das Américas



Background

Essa métrica avalia as principais amostras de código malicioso na região das Américas em 2011. A Symantec analisa amostras de código malicioso novas e já existentes para determinar que tipos de ameaças e vetores de ataque estão sendo empregados nas ameaças mais prevalentes. Essa informação também permite que os administradores e usuários ganhem familiaridade com as ameaças que os invasores podem favorecer em suas façanhas. Conhecer as novas tendências de desenvolvimento de ameaças pode ajudar a reforçar as medidas de segurança e reduzir a possibilidade de ataques futuros.

Metodologia

Para determinar as principais amostras de código malicioso, a Symantec classifica cada amostra com base no volume de fontes exclusivas de infecções potenciais observadas durante o período da pesquisa.

DADOS

Figura G.9

Principais Amostras de Código Malicioso nas Américas, 2011

Posição	Código Malicioso	% de Código Malicioso na Região
1	W32.Downadup.B	11.8%
2	W32.Sality.AE	11.1%
3	W32.SillyFDC	4.8%
4	W32.Almanahe.B!Inf	4.4%
5	W32.Almanahe.B!Ink	4.1%
6	Trojan.Maljava	3.8%
7	W32.Changeup	2.7%
8	W32.SillyFDC.BDP	2.3%
9	Trojan.FakeAV	2.3%
10	Trojan.ByteVerify	2.0%

Fonte: Symantec

Figura G.9

Principais Amostras de Código Malicioso na América do Norte, 2011

Posição	Código Malicioso	% de Código Malicioso ma Região
1	W32.Downadup.B	4.5%
2	Trojan.Maljava	3.5%
3	W32.SillyFDC.BDP!Ink	3.4%
4	Trojan.FakeAV	2.1%
5	W32.SillyFDC.BDP	2.0%
6	Trojan.ByteVerify	2.0%
7	Trojan.Malscript!html	1.3%
8	Trojan.Zefarch	1.2%
9	W32.Qakbot	1.0%
10	W32.Ramnit!html	0.9%

Fonte: Symantec

Figura G.9

Principais Amostras de Código Malicioso na América Latina, 2011

Posição	Código Malicioso	% de Código Malicioso ma Região
1	W32.Sality.AE	10.3%
2	W32.Downadup.B	7.3%
3	W32.SillyFDC	4.2%
4	W32.Almanahe.B!inf	3.6%
5	W32.changeup	2.3%
6	W32.Chir.B@mm(html)	1.5%
7	W32.Slugin.A!inf	1.5%
8	W32.Harakit	1.4%
9	W32.Virut.CF	1.4%
10	W32.Downadup!autorun	1.3%

Fonte: Symantec

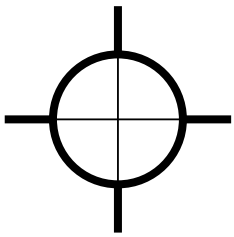
Comentários

- **W32.Downadup (também conhecido por Conficker) predomina na região das Américas:** O *W32.Downadup.B* foi classificado na primeira posição na região das Américas em 2011, respondendo por 7,3 por cento das potenciais infecções na América Latina e 4,5 por cento na América do Norte.
- A família Downadup de malware foi classificada na quarta posição mundial em 2011, apesar de perder o impulso, pois em 2010 foi a segunda família de código malicioso mais alta no ranking de volume de potenciais infecções em nível global.
- O Downadup se propaga através da exploração de vulnerabilidades, copiando-se para unidades de redes compartilhadas. Estima-se que o Downadup ainda esteja em mais de 3 milhões de PCs em todo o mundo até o final de 2011, em comparação com o volume de cerca de 5 milhões no final de 2010.
- Curiosamente, variantes do *Ramnit*, que foi o número um em famílias de malware globalmente em 2011, não se mostraram fortes entre os 10 principais malware identificados na região das Américas e responderam por menos de 1 por cento das potenciais infecções na América do Norte.
- O *W32.Sality.AE* foi classificado como número um na América Latina, mas não constou entre os 10 principais na América do Norte. A atividade reportada por esse vírus foi a principal contribuinte para que a família Sality ocupasse a segunda classificação mais alta entre as famílias de código malicioso globalmente em 2011.
- Descoberto em 2008, o *Sality.AE* tem sido parte proeminente no cenário de ameaças desde então, inclusive sendo a principal família de código malicioso em nível global identificada pela Symantec em 2009 e 2010.
- O Sality pode ser particularmente atraente para os invasores porque usa código polimórfico que pode dificultar a detecção. Também é capaz de desativar os serviços de segurança nos computadores afetados. Esses dois fatores podem levar a uma taxa mais elevada de instalações bem sucedidas para os invasores.

Melhores Práticas

EMPRESAS

- Adotar estratégias de defesa em camadas.
- Desativar serviços que não são necessários.
- Se algum código malicioso ou alguma outra ameaça explora um ou mais serviços de rede, desabilite ou bloqueie o acesso a esses serviços até que seja aplicado um patch. Isole os computadores infectados.
- Manter os patches atualizados (sistema operacional e aplicações).
- Considerar implementar soluções de acesso e conformidade com políticas de rede.
- Implementar políticas efetivas de senhas e controle de dispositivos.
- Adotar autenticação forte (OTP) para previnir ataques de Engenharia Social.
- Buscar entender, encontrar e controlar dados sensíveis a sua organização. Use criptografia para proteger essas informações.
- Assegugar que os procedimentos de emergência estejam atualizados e promover treinamentos sobre segurança na Internet para todos os funcionários. Eles são a primeira linha de defesa da organização.



CONSUMIDORES

- Adotar senhas com uma mescla de letras e números e trocá-las com frequência. As senhas não devem ser palavras conhecidas ou que constem no dicionário.
- Nunca ver, abrir ou executar arquivos anexos de e-mails a menos que os esteja esperando e que conheça o propósito dos mesmos.
- Mantenha as definições do antivírus atualizadas.
- Nunca revelar informação pessoal ou financeira confidencial ao menos que possa confirmar que esta solicitação de informação é legítima.
- Não realizar atividades de alto risco na web, como transações bancárias ou compras online, a partir de computadores públicos.
- Evite clicks em arquivos anexos e mensagens de e-mail ou mensagens instantâneas, uma vez que os mesmos também podem colocar os equipamentos em risco.
- Utilize uma solução de segurança de Internet que combine antivírus, firewall, detecção de invasão, reputação da nuvem e gestão de vulnerabilidades; possibilitando máxima proteção contra códigos maliciosos e outras ameaças.
- Mantenha seus patches de segurança atualizados e os aplique sempre que oportuno.

RECURSOS ADICIONAIS

Relatório sobre Ameaças à Segurança na Internet: www.symantec.com.br/gin
Outros relatórios da Symantec: www.symantec.com.br/relatorios
Soluções Symantec: www.symantec.com.br/empresas

Sobre a Symantec

A Symantec é líder mundial no fornecimento de soluções de segurança, armazenamento e gerenciamento de sistemas para ajudar consumidores e organizações a proteger e gerenciar suas informações no mundo conectado.
Nossos softwares e serviços protegem contra mais riscos, em mais pontos, de forma completa e eficiente, oferecendo segurança onde quer que a informação esteja sendo utilizada ou armazenada.
Mais informações em www.symantec.com.br.