Relatório Anual de Incidentes de Segurança na Rede Brasileira de Ensino e Pesquisa

2017

CAIS

RNP

Sumário

SOBRE

1

RNP

A RNP – Rede Nacional de Ensino e Pesquisa foi criada em 1989 pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTI), com o objetivo de construir uma infraestrutura de rede de Internet nacional para a comunidade de ensino e pesquisa [1]. Como primeira rede de acesso à Internet no Brasil, a RNP atualmente conecta 1.197 campi e unidades de mais de 900 instituições de ensino e pesquisa nas capitais e interior dos 26 estados da federação, mais o Distrito Federal.

A RNP oferece conexão à internet para as instituições federais de ensino superior ligadas ao Ministério da Educação (MEC), unidades de pesquisa federais ligadas ao Ministério de Ciência, Tecnologia e Inovação (MCTI), agências de ambos os ministérios e outras instituições de ensino e pesquisa públicas e privadas.

Um total estimado em mais de 4 milhões de usuários da comunidade acadêmica brasileira se beneficiam dessa infraestrutura que estimula o progresso da educação superior, ciência e inovação no Brasil.

1.197
Campi e unidades

900
Instituições de ensino e pesquisa nas capitais e interior

26
Estados da federação
\+ Distrito Federal

1 +

Rede Ipê

A rede Ipê, como é chamado o backbone da RNP, é uma infraestrutura de rede de Internet voltada para a comunidade de ensino, pesquisa e inovação no Brasil. Nela, conectam-se as principais universidades e institutos de pesquisa do país, servindo como um canal de comunicação rápido e com suporte a serviços e aplicações avançadas.

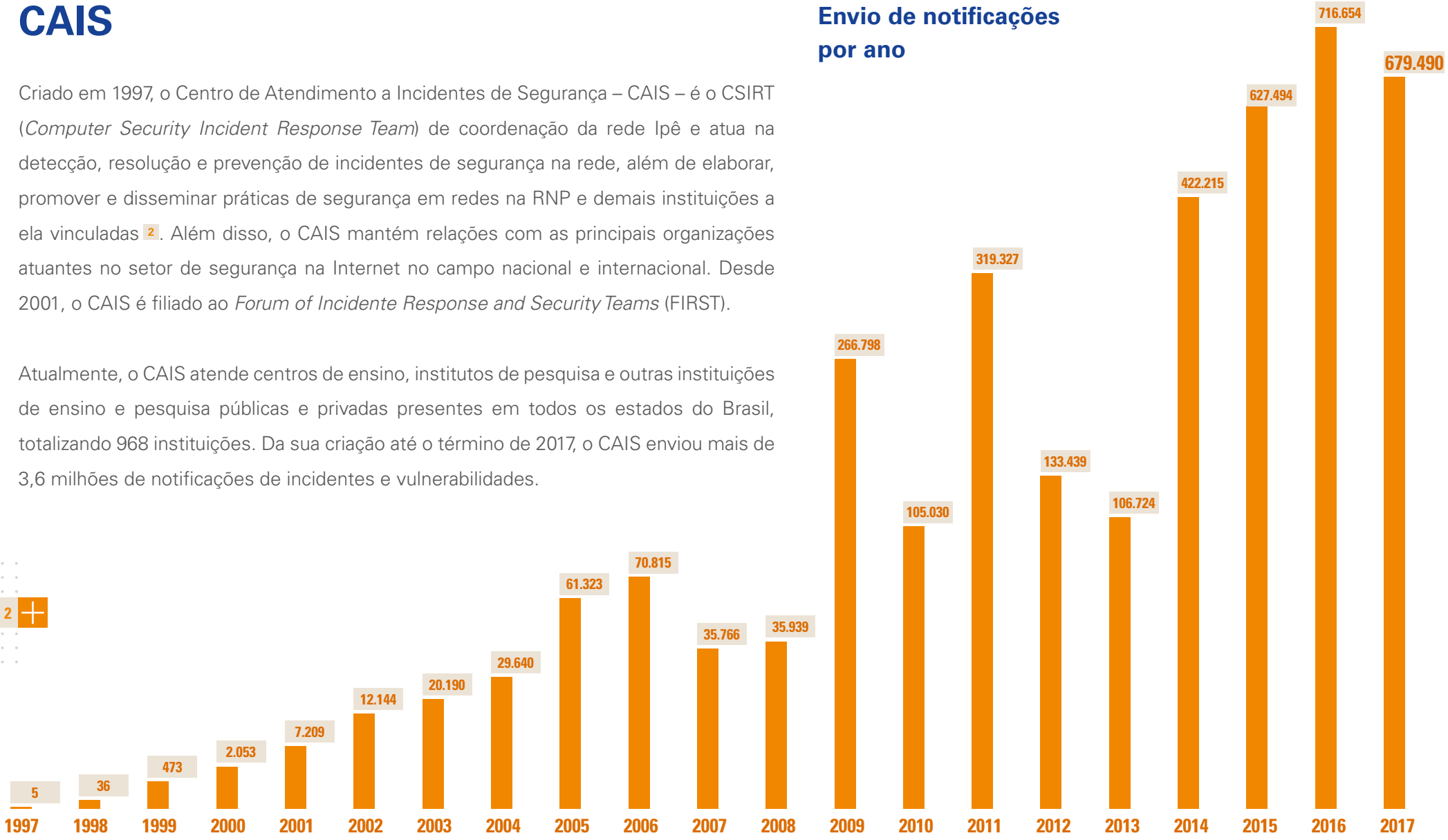
Baseada em tecnologia de transmissão óptica, a rede Ipê está entre as mais avançadas do mundo e possui conexão com redes acadêmicas estrangeiras, tais como RedCLARA, na América Latina, Internet2, nos Estados Unidos e a Géant, na Europa.

CAIS

Criado em 1997, o Centro de Atendimento a Incidentes de Segurança – CAIS – é o CSIRT (*Computer Security Incident Response Team*) de coordenação da rede Ipê e atua na detecção, resolução e prevenção de incidentes de segurança na rede, além de elaborar, promover e disseminar práticas de segurança em redes na RNP e demais instituições a ela vinculadas [2]. Além disso, o CAIS mantém relações com as principais organizações atuantes no setor de segurança na Internet no campo nacional e internacional. Desde 2001, o CAIS é filiado ao *Forum of Incidente Response and Security Teams* (FIRST).

Atualmente, o CAIS atende centros de ensino, institutos de pesquisa e outras instituições de ensino e pesquisa públicas e privadas presentes em todos os estados do Brasil, totalizando 968 instituições. Da sua criação até o término de 2017, o CAIS enviou mais de 3,6 milhões de notificações de incidentes e vulnerabilidades.

Envio de notificações por ano



2 +

RESUMO EXECUTIVO

2

Quem está no dia a dia da segurança da informação deve ter em mente a importância de estar conectado ao que acontece no mundo da tecnologia, inclusive no que diz respeito às ameaças e incidentes. Por isso, olhar para o presente com vistas para o futuro pode ajudar a impedir ataques, minimizar impactos e garantir a segurança de informações importantes para negócios e organizações.

A questão é: as equipes de segurança podem ver além do horizonte? Sim, é possível. Olhar para fatos, destaques e estatísticas podem nos dar valiosas pistas do que está por vir. Um bom exemplo foram os ataques de *ransomware* que ocorreram no primeiro semestre de 2017. Ter a ciência de que ocorreram, entender como e porque tomaram as proporções alcançadas ajudam a criar estratégias de como evitar novas ocorrências e, assim, salvar as organizações de prejuízos e perdas à sua imagem e às suas finanças.

O Relatório Anual de Segurança do CAIS em 2017 traz de início um levantamento dos fatos mais relevantes que ocorreram no ano anterior e os impactos que trouxeram ao backbone Ipê e à comunidade de segurança em geral, como por exemplo, os outbrakes de *ransomwares*, a vulnerabilidade crítica no protocolo de comunicação sem fio WPA2 e falhas em sistemas gerenciadores de conteúdo.

Em seguida, são analisadas as principais notificações de vulnerabilidades e incidentes de segurança da informação enviadas pelo CAIS às instituições usuárias da

rede brasileira de ensino e pesquisa, gerenciadas pela ferramenta SGIS (Sistema de Gestão de Incidentes de Segurança), sobre a ótica dos tipos de atividade maliciosa identificados. Entre outras análises, pode-se observar que 2017 foi um ano de ligeira queda, em números gerais, das notificações enviadas, em comparação com o ano de 2016, motivada por uma maior preocupação dos administradores de redes e sistemas na correção e mitigação das vulnerabilidades e incidentes, bem como também pela mudança de cenário a nível nacional e algumas mudanças de metodologia de monitoramento e notificação por parte do CAIS.

Uma novidade neste relatório é um artigo que traz importantes considerações acerca do esgotamento de blocos de endereços IPv4 e a importância da adoção de IPv6 nas redes das universidades e institutos federais, e instituições de pesquisa no Brasil, trazendo breves considerações sobre quais configurações relativas à segurança na implantação devem ser levadas em conta.

Também são apresentados os principais resultados das participações da RNP em congressos, seminários, fóruns e outros eventos de segurança no Brasil e no mundo. Assim como também são apresentadas outras realizações da Também são apresentadas outras realizações da RNP na área de segurança da informação, como a produção de uma campanha técnica, na seção "Atualize-se", como, por exemplo, a produção da Campanha Técnica para 2018.

Por fim, são apresentados ao final as tendências observadas para 2018, e como as organizações podem se preparar para evitar e combater as ameaças, ou se preparar para as batalhas pela segurança da informação com as armas e inovações que o mercado pode trazer.

Nós encorajamos a leitura deste relatório como uma forma de conhecer melhor o cenário da segurança da informação na comunidade acadêmica brasileira, os incidentes e vulnerabilidades que foram destaque e merecem atenção não somente aos profissionais de segurança, mas também aos administradores de redes e sistemas e a todos os usuários. O usuário final tem um papel cada vez mais importante nesse cenário, como co-responsável pela proteção das informações em seus computadores, seus dispositivos móveis, laptops, tablets e celulares, ou até mesmo nos serviços em nuvem.

Os casos de *ransomwares* são o maior exemplo dessa tendência. Os usuários não podem ser mais indiferentes aos dados que lidam no dia-a-dia, seja no ambiente profissional, seja em casa ou em outros ambientes pessoais. A maior parte das informações são armazenadas em diferentes formatos digitais e em muitos lugares diferentes que vão além das fronteiras de seus próprios sistemas.

3 DESTAQUES DO ANO

Ataques massivos de *ransomwares*

O primeiro semestre de 2017 foi marcado pela ocorrência massiva e a nível global de casos de *ransomwares*, um tipo de malware que cifra os arquivos do computador de um usuário e libera somente mediante pagamento de resgate. Em junho, houve os ataques do WannaCry (ou Wannacryptor) e NotPetya, e meses depois do BadRabbit, com imensa repercussão pública, operações de negócios interrompidas no mundo todo e, consequentemente, grandes prejuízos. O CAIS enviou alertas no período de ataques destes *ransomwares* [3] [4] [5]. No Brasil, foram registrados casos de infecção por alguns desses *ransomwares* em alguns órgãos do serviço público e também em instituições conectadas à rede de ensino e pesquisa.

A principal característica desses ataques foi a capacidade de propagação que eles tiveram, graças à exploração de uma vulnerabilidade no protocolo SMBv1 do sistema operacional Microsoft Windows utilizado para compartilhamento de arquivos e impressoras, que permitia ao *malware* acesso administrativo ao sistema e a execução de comandos para infectar outros hosts e se propagar. Um *exploit* (código destinado a exploração de vulnerabilidades) denominado EternalBlue, desenvolvido pela Agência Nacional de Segurança dos Estados Unidos (NSA) [6], foi a base utilizada pelo ransomware WannaCry para sua propagação em massa. Já o NotPetya se utiliza de brechas nas permissões administrativas nas ferramentas PSEXEC e WMIC, funções do Windows que permitem à contas do sistema operacional Windows gerenciar computadores remotamente e em massa. O ransomware BadRabbit infecta usuários que acessam sites comprometidos solicitando que seja realizado o download de uma atualização falsa do Adobe Flash Player, que, se executado, realiza a cifragem dos dados do computador e tenta se propagar através da rede.

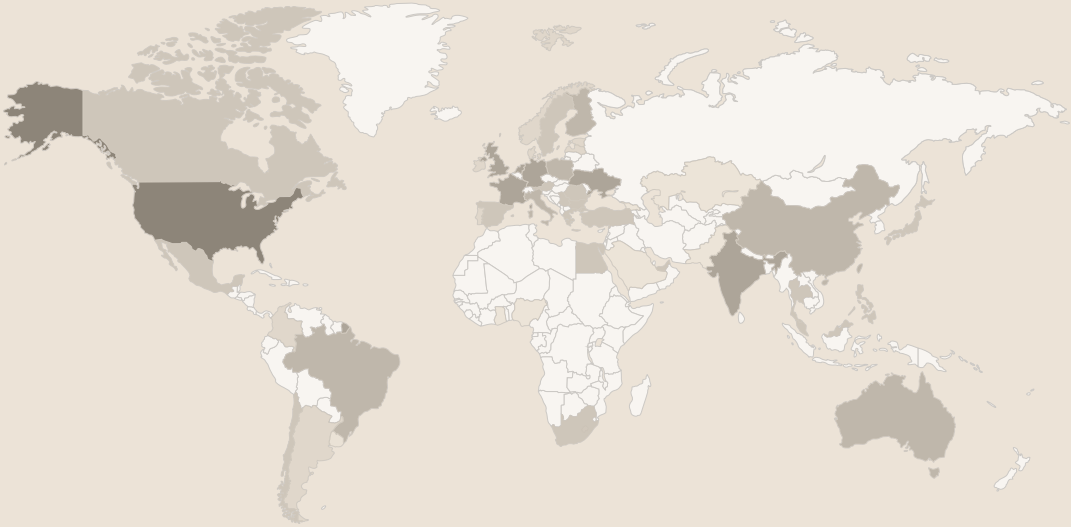
Em todos os casos, bastou que privilégios administrativos de contas estivessem mal configurados ou que os computadores não estivessem com as últimas atualizações de segurança do sistema operacional

3
4
5
6

para que organizações estivessem sujeitas a ter suas redes inteiras comprometidas por esses ransomwares. Somente em um dia, mais de 300 mil computadores foram infectados em mais de 150 países [7]. Apesar das ameaças de ransomwares não serem recentes, esses ataques expuseram a criticidade do uso de sistemas operacionais desatualizados e da ausência de políticas de aplicação de patches de segurança por parte das organizações.

Países afetados pelo ransomware NotPetya

Fonte: McAfee Labs



Na rede acadêmica:

1.150

Notificações de casos envolvendo IPs públicos

48

Instituições comprometidos pelo *ransomwares Wannacry*

7

Para não se tornar vítima desses ataques, o CAIS recomenda:

- Usar softwares e sistemas operacionais originais e licenciados (nos casos de SO proprietários, como o Microsoft Windows).
- Sempre aplicar as atualizações de segurança do sistema operacional e dos softwares instalados.
- Conscientizar os usuários sobre o uso seguro dos recursos computacionais, tais como não acessar sites maliciosos e não abrir anexos ou links suspeitos.
- Manter cópias de segurança sempre consolidadas, com políticas e rotinas de backup definidas, executando periodicamente testes de restauração do conteúdo do backup.
- Manter o firewall local e recursos de segurança do Microsoft Windows ativos.
- Usar software *antimalware* nos computadores e mantê-lo atualizado.
- Limitar as chamadas via PSEXEC e WMI somente a sistemas Microsoft Windows que necessitem desse recurso.

Vulnerabilidades no Windows em evidência

Em 2017, foram descobertas ainda outras falhas críticas no sistema operacional Microsoft Windows que causaram forte impacto no cenário da segurança da informação a nível mundial. Além da vulnerabilidade no protocolo SMBv1 já citada acima, outras também permitiam a execução de códigos remotos e o controle administrativo do computador.

As principais vulnerabilidades relativas ao Windows alertadas pelo CAIS dizem respeito a vulnerabilidades no kernel, publicada no mês de abril [8], no tratamento de arquivos de extensão. LNK (atalhos), em junho [9], e, em dezembro, na engine de proteção contra *malwares*, a qual inclui softwares como Windows Defender, Microsoft Endpoint Protection, Security Essentials, entre outros [10]. Em todos eles foram desenvolvidos códigos de exploração das vulnerabilidades, entre eles o EternalBlue, que foi utilizado no ataque dos ransomwares WannaCry e NotPetya, já comentados acima.

A Microsoft lançou patches de correção para todas as vulnerabilidades citadas. É imprescindível que os usuários de computadores e administradores de rede apliquem as atualizações de segurança disponibilizadas pela Microsoft através do Windows Update. Após a instalação das atualizações e dos patches de segurança, é recomendada a reinicialização do sistema para sua aplicação.

8 +

9 +

10 +

Redes sem fio vulneráveis

Em outubro de 2017, foi divulgada uma falha grave de segurança no protocolo WPA (Wi-FI Protected Access), um dos mais usados para proteger o acesso e tráfego de dados em equipamentos que fazem a conexão à rede sem fio [11].

Denominada de KRACK (Key Reinstallation Attacks), essa vulnerabilidade permite a um atacante, dentro do alcance da rede, interceptar informações entre dispositivos conectados e o ponto de acesso da rede sem fio (roteador ou ativo wireless). Dessa forma, o tráfego da conexão pode ser monitorado, assim como também é possível obter dados sensíveis como credenciais de acesso, conteúdo de mensagens, e-mails, números de cartões de crédito, fotos, entre outras informações enviadas. Em casos específicos, a depender das configurações da rede e dos dispositivos, é possível ainda o sequestro de conexão, redirecionamento de tráfego e manipulação de dados que pode permitir a injeção de códigos maliciosos [12].

Ataque KRACK à rede sem fio

Fonte: www.krackattacks.com

11

12

A falha está presente no processo de 4-*way handshake* usado para a troca de chaves criptográficas. Esse processo é executado quando um dispositivo cliente solicita ingresso em uma rede sem fio protegida, onde o ponto de acesso e o cliente verificam se as credenciais para estabelecimento da conexão estão corretas e, caso estejam, negociam as chaves de criptografia que serão usadas para cifrar o tráfego durante a conexão. É justamente nessa fase de negociação das chaves, a terceira do *handshake*, que o ataque é possível de ser realizado, quando o ponto de acesso não recebe uma resposta de confirmação da mensagem enviada para o cliente e então retransmite as informações da chave criptográfica para que o cliente possa recebê-la e instalá-la. O atacante pode se posicionar entre um cliente e o ponto de acesso e manipular as informações do *handshake* para que as chaves possam ser reutilizadas. De posse das chaves, o atacante consegue ter acesso aos dados trafegados nessa conexão que não estejam cifradas por outros protocolos de segurança, como SSL ou TLS, por exemplo.

A vulnerabilidade afeta os protocolos WPA e o WPA2, com qualquer tipo de criptografia que esteja sendo utilizada, TKIP, AES ou GCMP. Todos os dispositivos que tem comunicação wireless e usam o protocolo WPA são afetados. Isso porque a vulnerabilidade está na especificação do padrão 802.11 feita pelo IEEE para conexão em redes sem fio e, para permitir a interoperabilidade entre todos os dispositivos, os fabricantes desenvolvem a implementação do protocolo baseado neste padrão. Entre os fabricantes de dispositivos afetados estão Apple (iOS e macOS), Windows, MediaTek, Linksys e outros, sendo que os ataques realizados contra dispositivos Linux e Android são mais graves, pois permitem reinstalar uma chave de criptografia com relativa simplicidade.

É importante destacar que os ataques que exploram esta falha não são direcionados aos pontos de acesso, e sim aos clientes que se conectam à rede sem fio no momento em que o processo de 4-*way handshake* é realizado. Logo, estar conectado à rede não garante a segurança do tráfego. Da mesma forma, de nada adianta alterar a chave pré-compartilhada (PSK) configurada no ponto de acesso [13].

Logo após publicada a prova de conceito que evidenciou a falha na implementação do protocolo WPA, os fabricantes disponibilizaram patches de correção para correção da vulnerabilidade. Portanto, devem-se instalar as versões mais atualizadas dos sistemas operacionais e firmwares instalados nos pontos de acesso e nos equipamentos que usam a rede sem fio [14] [15].

+13
+14
+15

Outras formas de se proteger de ser alvo dessa vulnerabilidade são:

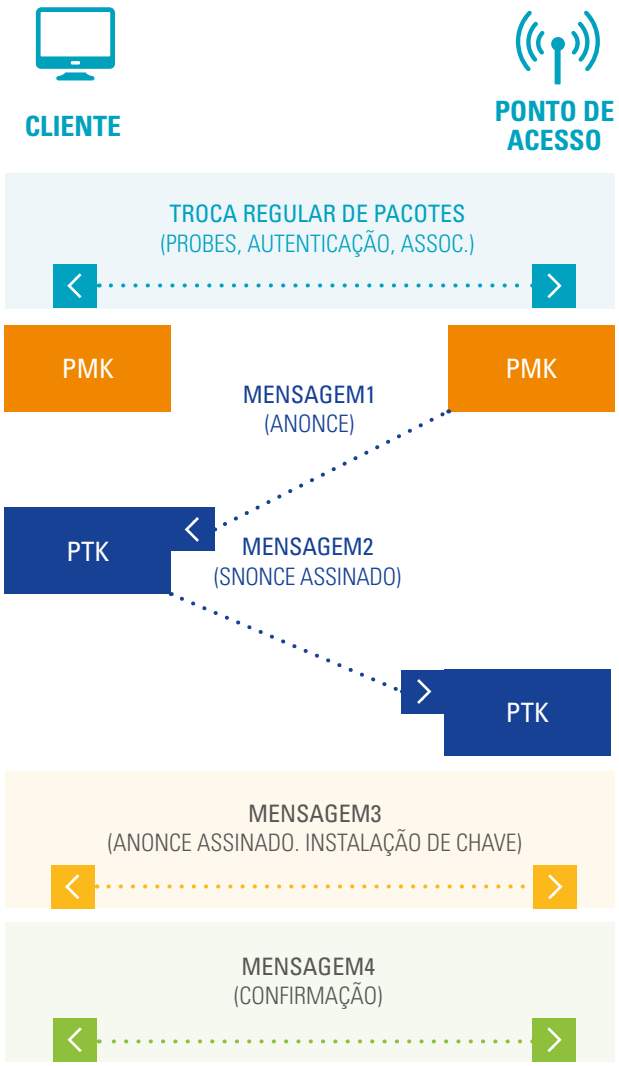
Utilizar na navegação protocolos de segurança, como SSL/TLS, usados em conexões HTTPS em navegadores, por exemplo.

Evitar utilizar redes sem fio abertas e desconhecidas.

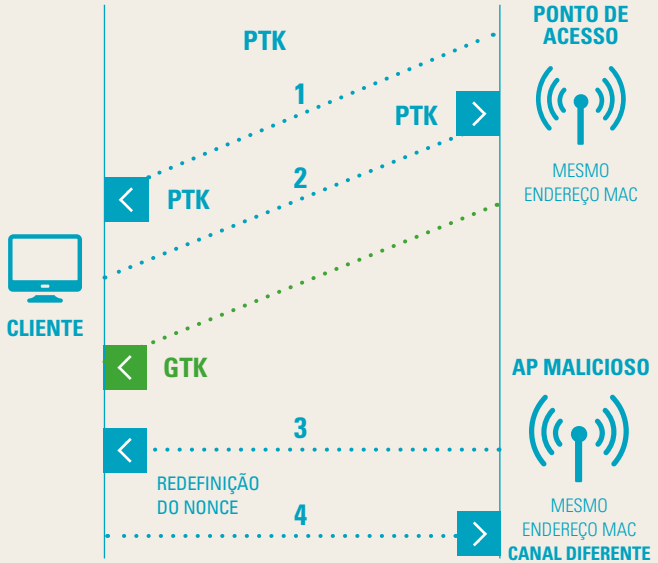
Caso utilizar redes públicas, jamais usar para trafegar dados sensíveis, como operações bancárias ou acesso a sistemas que contenham informações críticas.

Atualizar todos os dispositivos que acessam redes sem fio, desde laptops, tablets, celulares ou qualquer outro dispositivo.

Processo do *4-way handshake*



Como funciona o ataque KRACK



1. AP (ponto de acesso) envia valor nonce para o cliente e este deriva a chave PTK.
2. Cliente envia valor nonce para o AP e este deriva a chave PTK.
3. AP retransmite a mensagem 3 se não receber uma resposta apropriada de confirmação, o cliente redefine o valor nonce e retransmite, atacante obtém a chave.
4. AP malicioso recebe o valor nonce, deriva chave PTK e envia para cliente, que instala chaves PTK e GTK do atacante.

Fonte: cysreport.com

4 ESTATÍSTICAS

Após altas crescentes desde o ano de 2014, houve uma redução no número de notificações enviadas pelo CAIS em 2017 – um total de 679.490 notificações entre incidentes de segurança e vulnerabilidades – cerca de 5,2% menor se comparado ao mesmo período de 2016, quando foram enviadas 716,654.

Essa queda pode ser explicada por dois motivos principais:

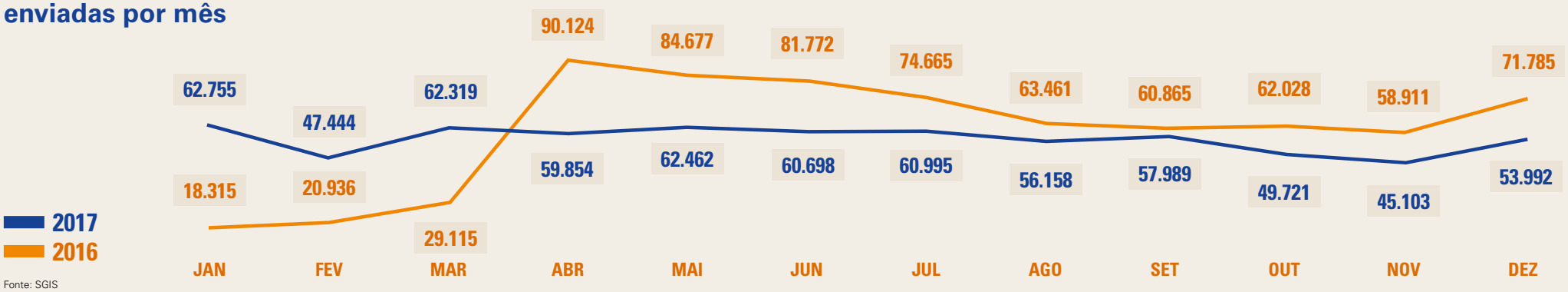
Os Jogos Olímpicos realizados na cidade do Rio de Janeiro em 2016 colocaram o Brasil nos holofotes das atenções a nível mundial, o que provocou uma maior ocorrência de atividades maliciosas na Internet no ano anterior tendo como meio ou alvo de ataques redes e organizações no Brasil, incluindo as instituições de ensino e pesquisa.

Uma mudança na metodologia feito pela RNP na detecção de eventos de DoS para garantir mais clareza e assertividade nas notificações.

Porém, mesmo com o registro de queda em números absolutos, a ainda alta incidência de ataques de negação de serviço, aliada ao alto grau de exposição de serviços vulneráveis expostos para a Internet por parte das instituições clientes do backbone Ipê, continuam sendo o grande desafio a ser enfrentado no combate a atividades maliciosas na rede brasileira de ensino e pesquisa.

Esta sessão aborda, de forma detalhada, os principais cenários acerca do panorama da segurança da informação no backbone Ipê no ano de 2017.

Quantidade de notificações enviadas por mês

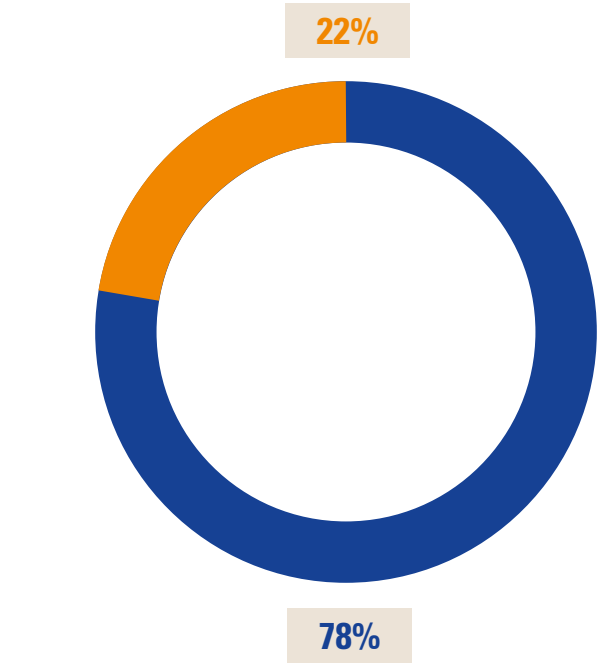


Fonte: SGIS

Alto índice de vulnerabilidades

Do total de 679.490 notificações enviadas pelo CAIS, cerca de 654 mil se referem a vulnerabilidades, ou seja, 96%. Desse total, somente 22% foram respondidas pelas instituições como resolvidas. Isso significa que o ano de 2017 se encerrou com quase 510 mil ocorrências de vulnerabilidades identificadas sem tratamento. Isso evidencia um campo de melhorias e investimentos a serem feitas pelas instituições de ensino e pesquisa clientes da RNP que deve ser trabalhado ao longo dos anos seguintes.

Percentual de resposta às notificações de vulnerabilidades em 2017



Não devemos esquecer que vulnerabilidades não tratadas tem um grande potencial de se gerar incidentes de segurança da informação, os quais podem comprometer as operações das instituições, causando prejuízos à sua imagem, aos seus funcionários e ao trabalho da comunidade acadêmica que utilizam seus recursos de tecnologia da informação. As consequências podem ser tão graves que, inclusive, podem impactar a utilização e o tráfego do backbone como um todo, prejudicando outras organizações da região ou do país.

Um problema recorrente chamado POODLE

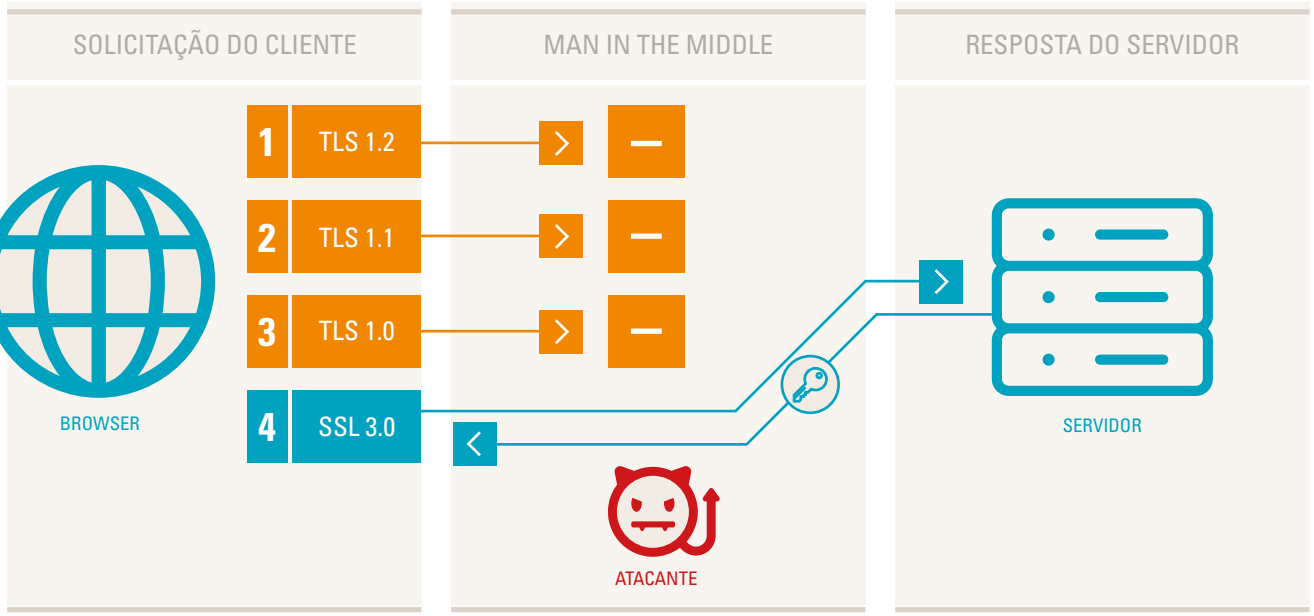
A vulnerabilidade no protocolo para navegação segura SSL – conhecida como Poodle (*Padding Oracle On Downgraded Legacy Encryption*) –, assim como em 2016, continua sendo a vulnerabilidade de mais incidência na rede de ensino e pesquisa.

Divulgada em 2014 [16], essa vulnerabilidade permite que um usuário malicioso intercepte e decifre as conexões, tendo, dessa forma, acesso a informações sensíveis, tais como usuários e senhas de sistemas, transações entre clientes e servidores, mensagens de e-mail, entre outros dados trafegados por sistemas que utilizam o protocolo legado.

16+

O CAIS segue recomendando que sejam desabilitados o uso do protocolo SSLv3 e TLS versões 1.0 e 1.1, tanto no cliente (browsers) quanto nos servidores – quando for estritamente necessário manter o suporte a esse protocolo, a recomendação é usar o SCSV (Signaling Cipher Suite Value) – passando a utilizar o TLS versão 1.2 nas configurações de certificado SSL nos servidores de navegação web.

Como funciona o ataque POODLE



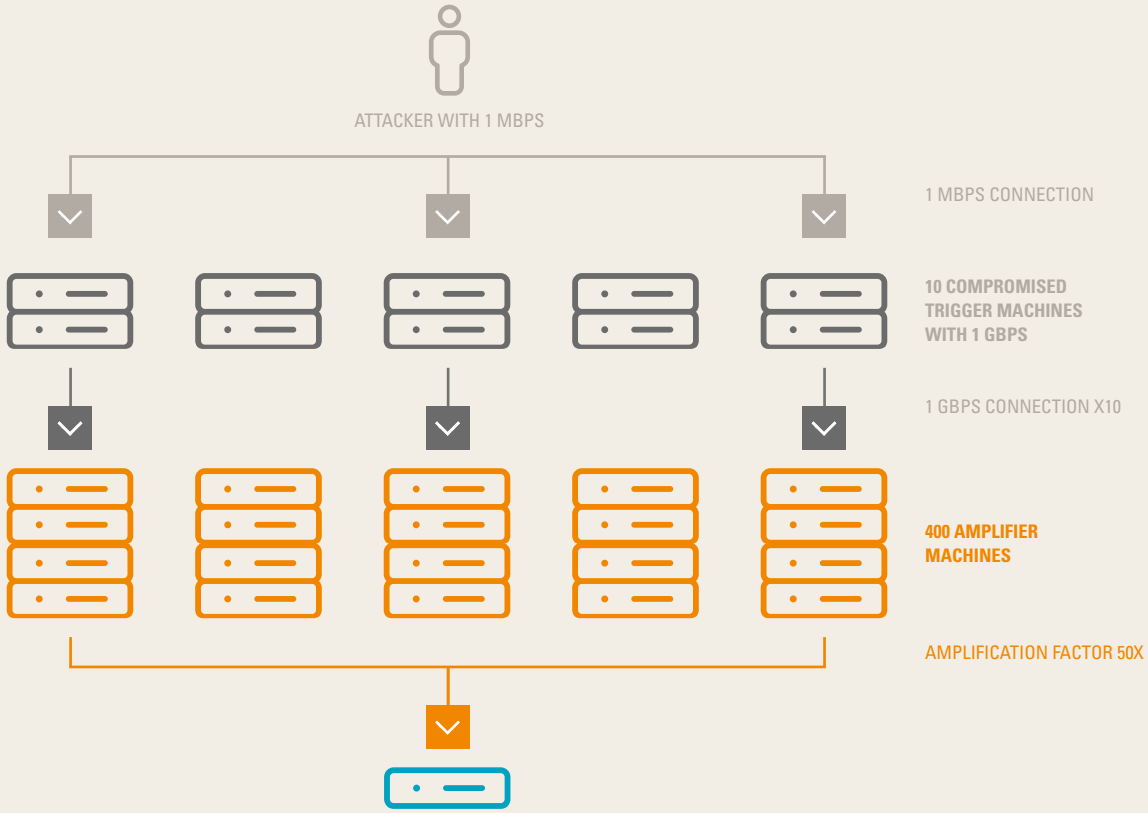
Fonte: Cais em Resumo nº 3

Serviços vulneráveis abertos para a internet

Outra grande parcela das vulnerabilidades notificadas ao longo do ano de 2017 diz respeito à serviços abertos para a Internet com potencial de gerar grandes volumes de tráfego amplificado e refletido, ataque conhecido como DRDoS (do inglês *"Distributed Reflection Denial of Service"* – negação de serviço distribuído e reflexivo).

Este tipo de ataque utiliza um host vulnerável acessível através da Internet que, ao receber uma requisição através de um host cujo endereço de IP de origem foi mascarado por parte do atacante, técnica esta conhecida como *IP Spoofing,* dispara uma resposta de tamanho várias vezes maior – que pode variar de acordo com o serviço vulnerável – gerando assim um tráfego não-requisitado para o alvo, consumindo seus recursos computacionais ou a largura de banda da rede, de modo a derrubar serviços e comunicação de dados do alvo específico.

Ataque de amplificação



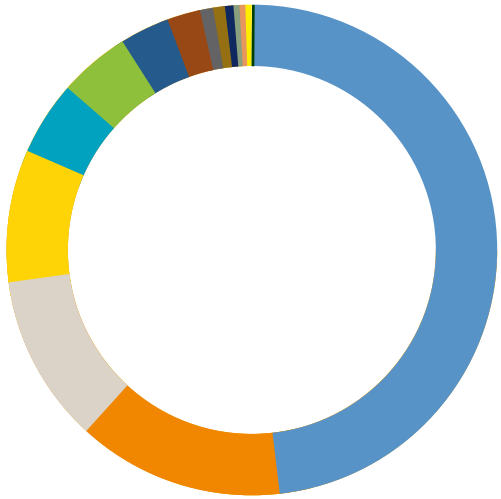
Fonte: Cloudfare.com

No conjunto das notificações enviadas em 2017, quase metade são referentes a vulnerabilidades em serviços que podem ser explorados para uso em ataques de DRDoS.

VULNERABILIDADE	NOTIFICAÇÕES	%
Servidores SSL vulneráveis que podem ser utilizados para roubo de informações	310.863	45.75
Host vulnerável usando o serviço PortMapper	86.244	12.69
Hosts vulneráveis que podem ser utilizados em ataques DRDoS envolvendo o protocolo SNMP	71.374	10.50
Host vulnerável executando o protocolo mDNS	35.670	5.25
Host(s) aparentemente com o serviço de NetBios Aberto	32.797	4.83
Servidores NTP vulneráveis que podem ser utilizados em ataques DDoS	29.525	4.35
Host vulnerável usando o serviço SMB	20.384	3.00
Host(s) aparentemente com o serviço de DNS Recursivo Aberto	19.030	2.80
Host vulnerável usando serviço TFTP	16.253	2.39

Na rede acadêmica, os principais protocolos vulneráveis e abertos para a Internet foram SSL, Portmapper, DNS, SNMP, NTP, SMB, TFTP, Memcached, bancos de dados – como MongoDB e MS-SQL Server – entre outros.

Protocolos vulneráveis detectados na rede acadêmica em 2017



SSL	310997	SSDP	5615
PORTMAPPER	86244	MS-SQL	4942
SNMP	71471	IPMI	4266
DNS	54937	MONGODB	1961
NETBIOS	32797	MEMCACHED	1507
NTP	29525	ELASTICSEARCH	896
SMB	20384	OUTROS	
TFTP	16253		

Fonte: SGIS

Tabela de amplificação de banda em ataques

VULNERABILIDADE	FATOR DE AMPLIFICAÇÃO DE BANDA	COMANDO VULNERÁVEL
DNS	28 a 54	ver: TA 13-088A
NTP	556.9	ver: TA14-013A
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 a 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 a 28	Malformed request
LDAP	46 a 55	Malformed request
CLDAP	56 a 70	–
TFTP	60	–
Memcache	10,000 a 51,000	–

Fonte: US-CERT

A depender do serviço vulnerável explorado, o fator de amplificação do ataque pode chegar a mais de 50 mil vezes o tamanho do pacote original [17]. Isso pode causar um impacto muito crítico no uso da rede das instituições, assim como também no próprio backbone da rede Ipê.

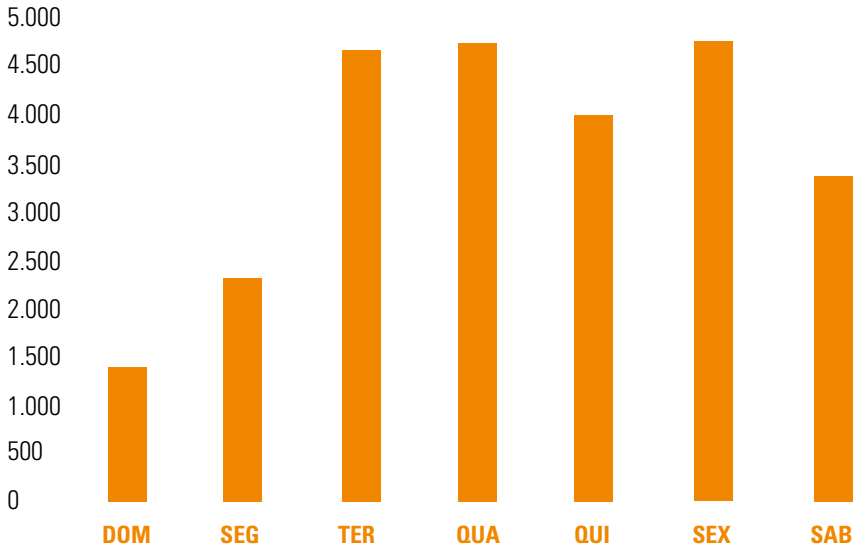
Por isso, o CAIS ressalta a importância de todas as organizações usuárias da rede de ensino e pesquisa tratarem as vulnerabilidades notificadas, a fim de reduzir do uso do backbone para atividades maliciosas e contribuir para a melhoria do uso dos recursos da rede Ipê.

+ 17

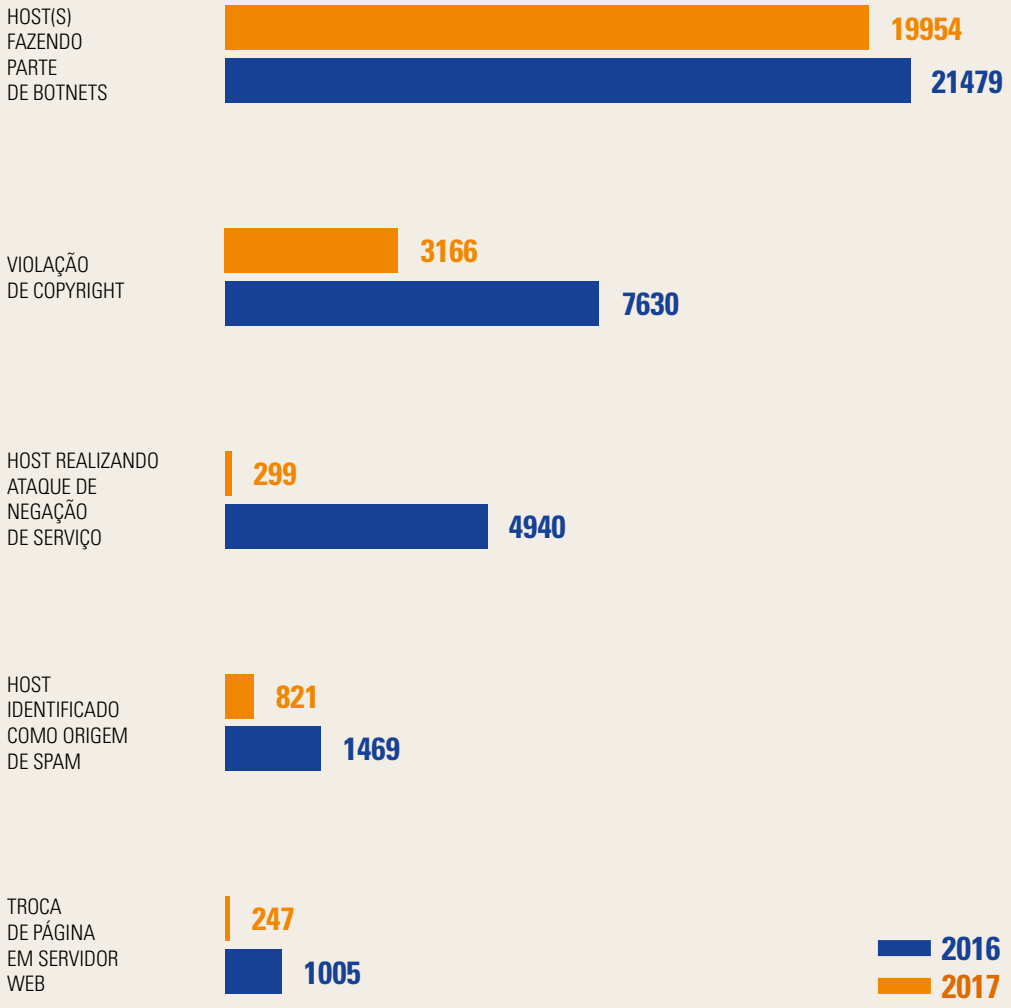
Incidentes

Em 2017, houve uma redução de 31% no total de notificações enviadas pelo CAIS às instituições de ensino e pesquisa no Brasil. O principal motivo foram as quedas no registro de ataques de negação de serviço e defacement.

Relação de notificações de incidentes por dia da semana



Fonte: SGIS



Botnets: velhos conhecidos x mesmos desafios

Bot é um software malicioso executado em um computador comprometido que permite controle administrativo e remoto deste por parte de um atacante, sem o conhecimento ou consentimento do proprietário. Uma *botnet* é um conjunto destes computadores infectados por *bots* semelhantes, os quais formam uma rede distribuída de controle para uso em atividades maliciosas na internet, como, por exemplo, ataques de negação de serviço, envio de spam, propagação de códigos maliciosos, roubo de informações confidenciais, entre outros.

Assim como no ano de 2016, em 2017 os incidentes de segurança da informação relacionados à botnets continuaram sendo a principal ocorrência na rede acadêmica brasileira. Foram registradas cerca de 20 mil notificações de hosts realizando atividades maliciosas típicas de computadores infectados por *bots* (robôs) ou de comando e controle (C&C).

Botnets comumente são utilizadas para realizar ataques distribuídos de negação de serviço (DDoS), seja enviando um ataque diretamente, seja usando ataques reflexivos (DRDoS), mascarando o IP da máquina infectada com *bot* para um alvo específico e disparando requisições para serviços vulneráveis conhecidamente abertos na internet.

Um monitoramento do tráfego da rede pode indicar à instituição se computadores em sua rede podem estar fazendo parte de uma *botnet*.

Alguns indícios são:

- Identificação de tráfego de IRC (comumente nas portas 6667 ou 6697, mas podem ser utilizadas outras portas).
- Verificação de tráfego de rede constantemente alto ou identificação de picos de tráfego repetidamente originados de hosts específicos.
- Identificação de tráfego SMTP (25/tcp) desconhecido e identificação de mensagens de e-mail não enviadas por usuários (spams).
- Verificação de problemas no acesso à Internet, aliado a lentidão no processamento e alto uso de CPU no computador.

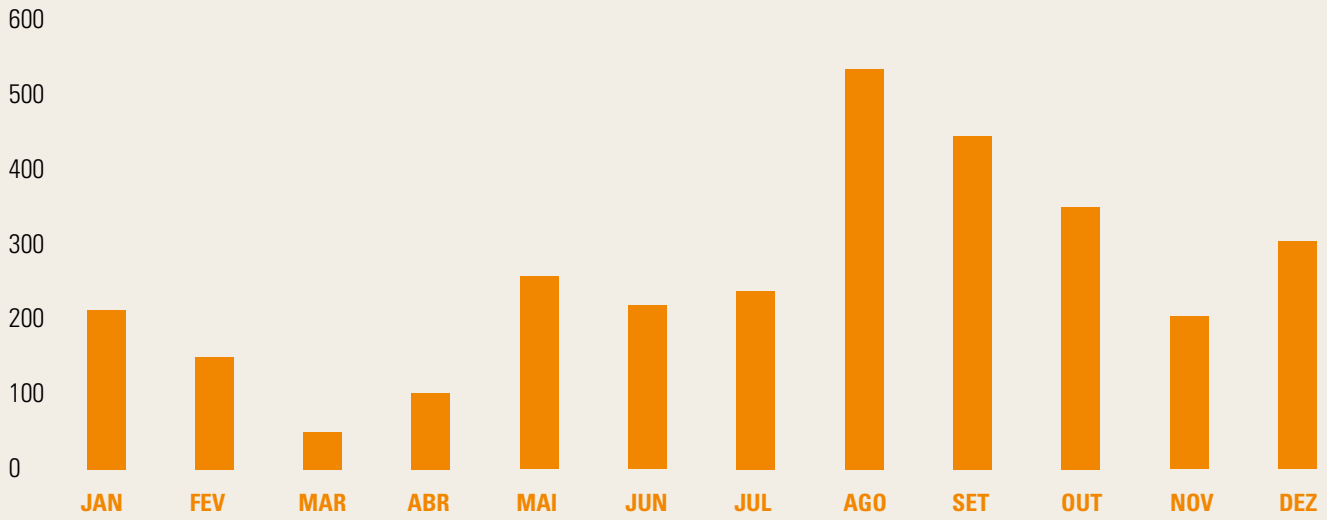
Uma boa prática para evitar que computadores sejam infectados por bots é manter os computadores com seus sistemas operacionais sempre atualizados, realizar auditoria e controle na instalação e execução de softwares e programas executáveis nas estações de trabalho, ter uma boa solução de anti-malware gerenciável, sempre atualizado com as últimas engines e vacinas, e, igualmente importante, conscientizar os usuários de computadores sobre o uso seguro de recursos e sistemas, para evitar que se tornem vetores de infecção e propagação de malwares.

Copyrights

A ocorrência de casos envolvendo transferência de arquivos protegidos por direitos autorais teve uma redução significativa, um total de 3.166 notificações, menos da metade dos casos em comparação com 2016.

Este tipo de notificação está relacionado ao *download* de arquivos de arquivos protegidos por direitos autorais, o que é caracterizado como um incidente de segurança da informação, haja visto que viola a Política de Uso da Rede Ipê, assim como a legislação vigente no país.

Notificações de incidentes relacionados à violação de direitos autorais por mês do ano



Fonte: SGIS

Conteúdos abusivos

Spam é um termo utilizado para caracterizar mensagens de e-mail enviadas em massa sem consentimento do usuário que recebe. Inicialmente relacionado a propagandas ou conteúdo comercial, atualmente os spams tem evoluído e se tornado mais perigosos, sendo um vetor de ataques à segurança da informação que pode envolver a propagação de malwares, golpes e roubo de informações pessoas e confidenciais.

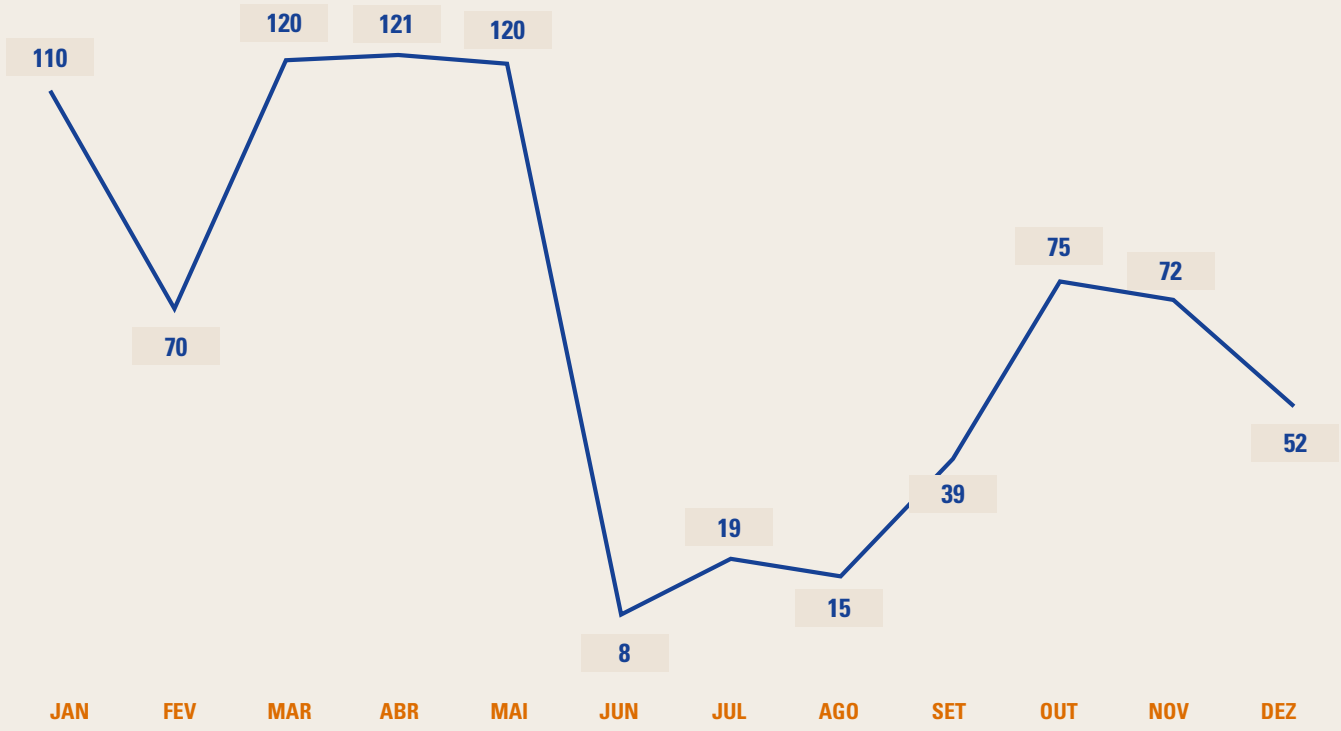
Também houve uma queda expressiva no total de spams notificados no ano de 2017, pouco mais de 800 casos. Os principais assuntos dos spams enviados pelas máquinas comprometidas foram:

Falsos pedidos de doação

Venda de produtos e medicamentos

Pedido de credenciais de acesso para renovação de cadastro

Notificações de hosts enviando Spam por mês do ano



Fonte: SGIS

O CAIS notifica incidentes na categoria Spam aqueles relacionados a servidores de e-mail comprometidos que enviaram uma grande quantidade de mensagens não requisitadas a domínios e usuários na Internet. Não são contabilizadas as ocorrências de spams recebidas por usuários das instituições em suas respectivas caixas de correio eletrônico.

Desfiguração de página web

Em 2017, foi registrada uma significativa redução nos casos de desfiguração de páginas web, chegando a ser 75% menor que em 2016. Estes incidentes estão relacionados a ataques que exploram vulnerabilidades em servidores, frameworks e aplicações – tais como gerenciadores de conteúdos (CMS) Drupal, Joomla, Open Journal, entre outros – com o objetivo de modificar o texto e imagens originais de websites.

O CAIS publicou alertas em março, abril e junho vulnerabilidades relativas ao Apache e Drupal, as quais permitiam a execução de códigos remotamente, sendo esta a principal causa de incidentes de desfiguração de páginas [18] [19] [20] [21].

[18]
[19]
[20]
[21]

5 EVENTOS

Nesta seção, serão abordadas as contribuições do CAIS nos eventos de segurança nacionais e internacionais.

LACNIC 27

O CAIS participou do maior fórum latino americano de provedores de infraestrutura e serviços, o LACNIC, em sua 27ª edição, realizado na cidade de Foz do Iguaçu, entre os dias 22 a 26 de maio. Neste evento, foram aceitas duas apresentações no LACSEC – Evento de Segurança em Redes para a América Latina e o Caribe: 22

- **i.** O serviço de apoio ao estabelecimento de novos CSIRTs na Rede de Ensino e Pesquisa.
- **ii.** Os resultados do projeto da Rede de Sensores Distribuídos, implementado nos 27 PoPs e em mais 17 organizações.

Ainda no LACNIC27, o CAIS participou do LAC-CSIRTs, a reunião de equipes de resposta a incidentes que atuam no contexto da Internet na América Latina e do Caribe. Nessa reunião, foram apresentados os números relativos aos dois anos de uso do SGIS e encaminhadas futuras parcerias com outras organizações da região.

22

Seminários online

O CAIS realizou, ao longo de 2017, três webinares sobre temas relacionados à segurança da informação. O primeiro, realizado em abril e ministrado pelo analista de segurança da informação da RNP, Rildo Souza, abordou as principais formas de ataques de negação de serviços distribuídos e reflexivos que ocorrem no cenário atual, destacando aqueles que ocorreram na rede de ensino e pesquisa do Brasil, além das principais vulnerabilidades utilizadas para a execução desses ataques e as respectivas contramedidas para evitar suas explorações.

O segundo webinar foi realizado no mês de Junho e conduzido pela analista Mirian von Zuben, do CERT.br. Tendo como tema a importância do backup, a palestra abordou a necessidade de realização de cópias de segurança nos dias atuais frente às ameaças de comprometimento de dados dos usuários, sobretudo pelo crescimento dos ransomwares, além de técnicas e boas práticas para realização do backup e testes periódicos de integridade dos dados das cópias de segurança. O terceiro e último webinar ocorreu em Setembro e teve como tema a preservação de evidências, triagem e comunicação às autoridades de incidentes de segurança relacionadas a condutas criminosas. O palestrante convidado Ivo Peixinho, especialista em Gestão de Segurança da Informação e perito criminal do Departamento da Polícia Federal, falou de aspectos relevantes das normas legais brasileiras, sobretudo aquelas que instituem a necessidade da guarda de logs, como a Instrução Normativa Nº 1 e as normas complementares associadas, e o Marco Civil da Internet. Abordou também as os requisitos, formas e procedimentos para repassar informações relacionadas às condutas cibercriminosas às autoridades competentes, quando necessárias ou solicitadas.

As três palestras online tiveram um total de audiência de 574 pessoas, compostas por usuários de computadores e também administradores de redes, sistemas e segurança em mais de 100 instituições clientes da rede Ipê. Os vídeos dos webinares podem ser encontrados na plataforma Video@RNP 23 24 25.

+23
+24
+25

Conferência Anual do FIRST

O CAIS participou da 29ª Conferência Anual do FIRST – Forum Mundial dos Times de Resposta a Incidentes de Segurança da Informação – realizada na cidade de San Juan, Porto Rico, em junho. Nessa edição, o CAIS apresentou na plenária os resultados do projeto de Sensores Distribuídos, além de realizar articulações com outras equipes para realização de projetos conjuntos 26.

TICAL 2017

Em julho, entre os dias 3 e 5, aconteceu a Conferência TICAL 2017, organizada pela RedCLARA – Cooperação Latino-Americana de Redes Avançadas – e CONARE – Conselho Nacional de Reitores da Costa Rica. Foi submetido um artigo produzido pela Universidade Federal da Bahia e o CAIS intitulada "Estabelecimento de CSIRTs e Processo de Tratamento de Incidentes de Segurança em Instituições Acadêmicas Brasileiras: estudo de caso da parceria CAIS/RNP e UFBA". Este artigo teve como objetivo apresentar à comunidade acadêmica da América Latina o projeto da RNP para apoiar o estabelecimento de novas equipes de tratamento de incidentes de segurança da informação em instituições de ensino e pesquisa no Brasil e os principais resultados obtidos pela UFBA na aplicação deste projeto para revisão e aperfeiçoamento do ETIR-UFBA e do processo organizacional da segurança da informação e comunicação da universidade 27.

Como principal resultado desta participação, foram feitos contatos importantes para divulgação, ampliação e colaboração do projeto com outras universidades que manifestaram interesse nos processos apresentados, como a Universidad de Costa Rica (UCR), bem como nas ferramentas utilizadas pela UFBA em seu processo de tratamento de incidentes de segurança da informação.

LACNIC 28

Realizado entre os dias 18 e 22 de setembro na cidade de Montevidéu, no Uruguai, o 28º Fórum do LACNIC também contou com a participação do CAIS durante o Colóquio Técnico Regional do FIRST, o FIRST-TC. Nesta ocasião, foi feita uma apresentação em parceria conjunta da ETIR-UFBA e do CAIS, intitulada "Estratégias de segurança da informação para CSIRTs Acadêmicos: as experiências e resultados da parceria do CAIS/RNP e ETIR-UFBA" 28. Esta apresentação abordou o desafio do tratamento de incidentes e adoção de proteções em um ambiente heterogêneo e flexível para as necessidades de ensino, pesquisa e extensão típicos das universidades, sob o aspecto de três dimensões da segurança da informação: processos, tecnologias e pessoas.

O CAIS também participou da reunião do LAC-AAWG, Grupo de trabalho Anti-Abuso da América Latina e Caribe, onde se deu início ao trabalho de desenvolvimento de um documento de boas práticas "BCOP – Requisitos mínimos de segurança para aquisições de CPEs". Este documento tem por objetivo relacionar um conjunto de requisitos de segurança que devem ser especificados na compra de CPEs – equipamentos utilizados para conectar usuários à rede do provedor de Internet (ISP), como modems, roteadores wi-fi, entre outros, visando o uso de equipamentos nativamente mais seguros e, com isso, reduzir a possibilidade comprometimento da rede através da degradação ou indisponibilidade de serviços.

+ 28

DISI

Foi realizada em 19 de outubro de 2017 a 12ª edição do Dia Internacional de Segurança em Informática – DISI, na cidade de Brasília-DF. Realizado anualmente pela RNP, com organização do CAIS em parceria com a OEA (Organização dos Estados Americanos) e a RedCLARA, o DISI reúne especialistas para compartilhar conhecimentos e promover a conscientização dos usuários de Internet sobre segurança da informação.

Nesta edição, o tema foi "Ransomware: não seja vítima de sequestro virtual" 29. Dentro da programação composta por 6 palestras, os expectadores puderam entender os conceitos básicos de criptografia e como a cifragem de arquivos é usada de forma maliciosa pelos criadores de ransomwares. Também foram exemplificados de forma prática como vetores de infecção são utilizados para enganar os usuários e torná-los vítimas de sequestro dos seus arquivos, como a conscientização do uso seguro dos computadores e dispositivos móveis é uma ferramenta importante para evitar novos casos de ransomwares, finalizando com uma análise das tendências e desafios futuros perante esta ameaça.

29

WTRs

Realizado pelos Pontos de Presença da RNP (PoPs) em cada estado da federação como parte do Programa SCI da RNP, os WTRs – Workshops em Tecnologia de Redes – são eventos voltados para gestores e equipes técnicas da área de TIC das principais instituições públicas e privadas de ensino e pesquisa no país, criando um espaço para capacitação, aprendizagem, troca de experiências e divulgação de novas tecnologias.

O CAIS participou de 10 WTRs ao longo de 2017 em diversos estados. Dentre os temas abordados, foi trazido o panorama da segurança da informação em cada região, avaliando tecnicamente os acontecimentos mais importantes. Foi apresentado também o novo serviço do CAIS para o estabelecimento de novas equipes de resposta a incidentes, ressaltando a importância das instituições clientes da rede Ipê possuírem seus CSIRTs internos e a estruturação dos procedimentos para tratamento, mitigação e prevenção de incidentes de segurança da informação. Como resultado, cerca de 14 instituições acadêmicas de 6 estados estarão em processo de estabelecimento de suas equipes de resposta a incidentes durante o ano de 2018.

EnCSIRTs

O Encontro de CSIRTs Acadêmicos Brasileiros – EnCSIRTs – em sua 12ª edição, aconteceu na cidade de São Paulo-SP 30. Contando com a presença de representantes de mais de 90% das equipes de resposta a incidentes que operam na rede brasileira de ensino e pesquisa, o encontro destacou a importância e necessidade de ações colaborativas entre as equipes. Foram estabelecidos grupos de trabalho que irão desenvolver ao longo de 2018 planos de ações em três tópicos principais: vulnerabilidades, gestão de incidentes, comunicação e disseminação da cultura em segurança da informação. Dentro do tradicional workshop de trabalhos técnicos, as palestras trouxeram temas como autenticação para redes de cabeamento físico e boas práticas na implantação de *firewall*.

30+

O 12º EnCSIRTs também foi marcado pelo lançamento da Campanha Técnica de Segurança da Informação para 2018. Outro destaque foi a realização de uma festa de assinatura de chaves (*PGP party key signing*), onde os participantes puderam anunciar suas chaves criptográficas e disponibilizá-las para os seus pares presentes assinarem, confiando assim na chave do respectivo membro do CSIRT.

6 ATUALIZE-SE

Campanha técnica

Durante o segundo semestre de 2017, foi desenvolvido pelo CAIS os materiais e documentações relativas à Campanha Técnica em Segurança da Informação, iniciativa inédita da RNP que será realizada durante o ano de 2018.

A campanha técnica terá como público alvo os administradores de redes e sistemas das instituições clientes da rede Ipê, mas também amplia o seu objetivo em ajudar toda a comunidade técnica da Internet. Tendo como tema Antispoofing, os materiais produzidos têm como objetivo trazer ao conhecimento o que é a técnica de IP Spoofing, como ela é utilizada para gerar tráfego malicioso nas redes e na internet, sobretudo em ataques de negação de serviços distribuídos e reflexivos (DRDoS), e as contramedidas que podem ser utilizadas.

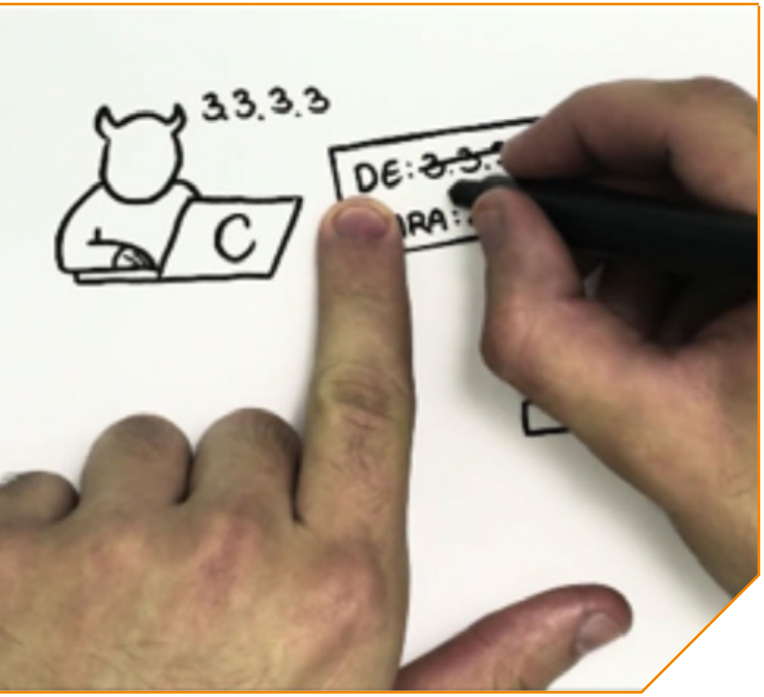
Na campanha, serão utilizadas cartilhas, tutoriais e um vídeo explicando conceitos e contramedidas.

AQUI TEM PROTEÇÃO
ANTI-SPOOFING

APOIO RNP

Campanha técnica de Anti-Spoofing

Exemplos de configurações seguras de equipamentos de rede estarão presentes em tutoriais técnicos, os quais serão divulgados durante o período de realização da campanha técnica.



Os materiais da campanha podem ser encontrados na seção de "Educação e Conscientização" no site da RNP [31].

31

RNP se posiciona com relação ao Marco Civil da Internet

No mês de agosto, a RNP lançou um position paper relativa ao Marco Civil da Internet no Brasil (Lei nº 12.965/14). Como provedora de serviços avançados de rede e de TIC, a RNP, através do artigo, propõe uma ação conjunta com a comunidade acadêmica brasileira com vistas ao fomento dos princípios do Marco Civil, visando facilitar a disseminação das melhores práticas a serem adotadas pelos administradores de redes acadêmicas no Brasil e promover a cultura em segurança da rede.

No artigo, são propostas diretrizes para a guarda, uso e responsabilidade sobre os registros de atividades e também sobre a garantia da liberdade de expressão, privacidade e neutralidade da rede.

VEJA O ARTIGO

ARTIGO

7

O Esgotamento do IPv4 e adoção do IPv6 na rede acadêmica

Por Guilherme Ladvocat,
Gerência de Operações da RNP.

A escassez de blocos IPv4 na internet é uma realidade para provedores de acesso e de conteúdo, como também para usuários de Internet. As entidades de registro, responsáveis pelas alocações em suas respectivas regiões, têm adotado medidas que visam prolongar a vida útil do IP versão 4. Em fevereiro de 2017, o NIC.br anunciou o início da última fase da "terminação gradual" do estoque de endereços IPv4 para a região da América Latina. A partir de então, Sistemas Autônomos existentes não poderão solicitar blocos IPv4 adicionais à entidade de registro. Em consequência disto, a RNP atualizou sua política de alocação de blocos IPv4, limitando pedidos a um período mínimo de seis meses e a um tamanho máximo de 128 hosts (/25), após justificativa iminente. Esta medida foi tomada visando estender a vida útil do protocolo IPv4 na rede acadêmica brasileira. Em consonância com a escassez de endereços IPv4, a Gerência de Operações da RNP tem trabalhado em ações de disseminação do protocolo IPv6. Entre 2016 e 2017, 783 instituições clientes foram contempladas por um projeto que consistiu em alocar proativamente blocos IPv6 e roteá-los até os roteadores de borda destas instituições.

Segurança na implantação do protocolo IPv6

É aconselhável a configuração de RA guard na camada de acesso, prevenindo ataques "man in the middle". Atenção também para não quebrar o Path MTU discovery. Configurações de endereços ULA e filtros a pacotes ICMPv6 podem quebrar o envio mensagens "packet too big". Isto torna-se crítico especialmente em IPv6, pois só é possível a fragmentação de pacotes na origem.

Uma boa prática é criar um plano de endereçamento estruturado, trivial para a implantação do protocolo, prevenindo retrabalho numa migração futura. No mais, as mesmas preocupações acerca de controle de acesso e uso de protocolos podem ser transportadas do IPv4 para IPv6.

8 O QUE O ANO DE 2018 RESERVA

O ano de 2017 trouxe à tona um problema recorrente: a falta de atualização e aplicação de patches de segurança e correção de vulnerabilidades por parte dos administradores de redes e sistemas. Pode-se, inclusive, afirmar que esta foi a principal causa dos maiores incidentes de segurança da informação registradas, como, por exemplo, os ataques massivos dos ransomwares Wannacry e NotPetya. E, se continuar não havendo ações proativas de administração segura de redes e sistemas, a tendência é que esse cenário continue em 2018.

Várias ameaças despontam para tornar o ano de 2018 um dos mais críticos em termos de segurança da informação no Brasil. Algumas tendências são muito fortes e merecem destaque:

Aumento de abuso de dispositivos IoT (Internet das Coisas)

Já em 2018, o número de dispositivos de Internet das coisas vai ultrapassar os aparelhos celulares como a maior categoria de ativos conectados. A expectativa é que o crescimento seja de, pelo menos, 23% em relação a 2017. Segundo relatório do Gartner [32], até 2020 serão mais de 20 bilhões de dispositivos conectados à Internet. Porém, o investimento em segurança no armazenamento e comunicação desses dispositivos não cresce na mesma proporção. Os dispositivos são essencialmente vulneráveis a ações de usuários maliciosos, o que se torna um risco à segurança e privacidade dos dados, além da possibilidade de serem usados em ataques de negação de serviço. Vale a pena lembrar que um dos maiores ataques de negação de serviços já registrados usaram dispositivos IoT que faziam parte de botnets [33]. Há uma expectativa de que a indústria nos próximos anos passe a olhar com mais cuidados para as questões de segurança da informação em dispositivos IoT, mas, a curto prazo, o cenário é que a adoção de uma arquitetura com forte segurança nos dispositivos ainda não seja economicamente viável.

+ 32

+ 33

Ataques massivos de botnets

Segundo relatório da Kaspersky [34], o Brasil foi o país da América Latina que mais realizou ataques a partir de dispositivos infectados fazendo parte de uma botnet em 2017. E com o crescimento constante de produção e uso de equipamentos IoT, essas ocorrências devem ficar ainda maiores e piores em 2018. Além da já conhecida Mirai, outras botnets estão sendo criadas e vem crescendo exponencialmente, tendo como alvo dispositivos conectados à Internet das coisas, a exemplo da Reaper, considerada uma evolução em sua forma de infecção e uso dos dispositivos comprometidos [35]. Os ataques são direcionados não somente aos dispositivos IoT comumente conhecidos, como câmeras IP, lâmpadas inteligentes, gravadores digitais (DVRs), impressoras, etc., mas também modems e roteadores domésticos e outros CPEs.

O método de ataque é quase sempre o mesmo: busca de dispositivos vulneráveis e configurados com usuário e senha padrão; após o acesso, é feito o download e execução do código malicioso, associando-o à rede para ser usada em futuros ataques. Neste cenário, o risco de ataques massivos de negação de serviço distribuídos (DDoS) a partir da rede de ensino e pesquisa é gigantesco.

Crescimento de redes baseadas em softwares (SDN)

Uma tendência forte é a utilização de redes definidas por software (SDN), assim como também de tecnologias de virtualização das funções de rede (NFV). Esta mudança já está em andamento e reorientando a forma como as organizações arquitetam suas redes WANs para ampliar seus serviços. Na rede acadêmica brasileira, tem crescido o número de testbeds locais em operação nas universidades e centros de pesquisa que compõem a plataforma Fibre [36].

Com isso, é preciso acompanhar a maturidade do Openflow, principal protocolo utilizado em redes SDN, com vistas ao surgimento de falhas de implementação ou vulnerabilidades que podem comprometer a segurança e o uso da solução [37].

34 35 36 37

Ataques a dados em nuvens

O uso de computação em nuvem já é uma realidade tanto para empresas, quanto para usuários de TIC. O uso de dispositivos IoT, que enviam os dados para serem armazenados e/ou processados na Internet, serviços e soluções em nuvem, como IaaS (infraestrutura como serviço), PaaS (plataformas com serviço) e SaaS (software como serviço) são só os exemplos mais comuns e que continuarão sendo amplamente consumidas por pessoas e organizações. Com isso, a escolha dos cibercriminosos por esses alvos também aumentará. No ano de 2017, por exemplo, foram registrados grandes ataques à Azure (Microsoft), tentativas de ataque ao Google Docs usando phishing, ameaça de vazamentos de senhas do iCloud da Apple e mineração de criptomoedas usando a infraestrutura em nuvem da Tesla hospedada na Amazon (AWS).

Em 2018 certamente haverá mais tentativas de comprometimento dos serviços em nuvem, em busca de roubo de credenciais de acesso, sobretudo as que tem acesso administrativo ou que proporcionam acesso mais amplo aos serviços, quebra de privacidade, acesso a dados sensíveis de usuários, negação de serviço e interrupção de acesso à nuvem, ataques de ransomwares, entre outros. Por outro lado, o investimento em soluções de segurança para nuvens também tem crescido, como a utilização de biometria e autenticação em múltiplos níveis, implementação de maiores controles de segurança que dependam menos dos usuários, criptografia e verificação de integridade dos dados e técnicas de prevenção de perda dos dados são só alguns exemplos do que pode vir a ser implementado pela grande maioria das soluções de computação em nuvem ao longo dos próximos anos.

Maior complexidade dos casos de ransomwares

2017 foi o ano que os ataques de ransomware se tornou notícias de jornais com os casos do WannaCry e NotPetya. Mas a expectativa é que tenha sido só o começo. De acordo com o relatório da TrendMicro [38], a tendência é que os ataques de ransomware em massa cresçam ao longo de 2018. E os alvos preferenciais serão organizações da área de educação, saúde e indústrias, em busca do comprometimento de documentos corporativos e de equipamentos de linha de montagem.

Uma outra tendência é que os ransomwares atinjam os dispositivos IoT. Espera-se que carros conectados, casas inteligentes, equipamentos médicos e dispositivos vestíveis (wearables) sejam o foco dos próximos alvos [39].

38

39

Aumento do hacktivismo em virtude das eleições

2018 é ano de eleição tanto para cargos majoritários, quanto para proporcionais, a nível nacional e estadual. O cenário de polarização política e dos debates já existente nos últimos anos tende a se acirrar ainda mais com a aproximação do pleito. A conectividade proporcionou uma mudança no comportamento nos eleitores usuários da Internet, que passaram a utilizar as redes sociais como uma das principais fontes de informação e consumo de notícias [40]. Dessa forma, as mídias sociais abriram caminho para jornalistas, colunistas e veículos considerados independentes em alternativa aos grandes grupos de comunicação, proporcionando mais democracia no acesso à informação. Porém, esse mesmo cenário é propício para a ação de cibercriminosos, ao usar esses mesmos meios como vetores de atividades maliciosas, tanto em relação à veiculação e viralização de notícias falsas, quanto também à propagação de softwares maliciosos através de phising sites, como bots, worms, ransomwares, entre outros.

Além disso, é esperado um aumento no número de casos de negação de serviços, roubo e divulgação de dados sensíveis e desfiguração de páginas em sites ligados a organizações estatais – incluindo universidades federais, institutos federais e organizações de pesquisa, por grupos de hacktivistas para defender ou promover uma causa política. Desta forma, é necessária toda a atenção por parte de administradores de redes e sistemas para implementação de medidas preventivas e correção de vulnerabilidades, a fim de evitar prejuízos aos dados e à imagem da organização.

Maior adoção de blockchain

Blockchain tem se tornado mais conhecido popularmente por causa das criptomoedas, sendo o Bitcoin a mais conhecida entre elas, geralmente usada como opção de solicitação de pagamento de resgate em casos de ransomwares. Porém, as aplicações de blockchain vão mais além e as organizações tem estudado o uso dessa tecnologia para realizar e facilitar transações entre empresas, oferecer um portfólio de serviços baseadas em blockchain e rastrear ativos IoT através do registro digital, reduzindo as chances de sucesso de um ataque malicioso.

Além disso, a partir de 2018 já será possível a realização de provas de conceito em defesas baseadas em tecnologia criptografada e surgimento de soluções de segurança como proteção de domínios, descentralização de autoridades certificadoras, proteção da integridade das informações, entre outras, baseadas em blockchain [41].

40

41

REFERÊNCIAS

1 www.rnp.br/institucional/quem-somos

2 www.rnp.br/servicos/seguranca

3 https://www.rnp.br/sites/default/files/alerta_ataque_ransomware.pdf

4 https://www.rnp.br/sites/default/files/cais-alerta_-_ataque_massivo_ransomware_notpetya.pdf

5 https://www.rnp.br/sites/default/files/alerta_ransomware_bad_rabbit.pdf

6 https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/

7 http://www.bbc.com/news/world-us-canada-42407488

8 https://www.rnp.br/sites/default/files/vulnerabilidade_kernel_windows.pdf

9 https://www.rnp.br/sites/default/files/vulnerabilidade_lnk.pdf

10 https://www.rnp.br/sites/default/files/vulnerabilidade_critica_no_sistema_malware_protection_0.pdf

11 https://papers.mathyvanhoef.com/ccs2017.pdf

12 https://www.rnp.br/sites/default/files/cais_alerta_wpa2.pdf

13 https://thehackernews.com/2017/10/wpa2-krack-wifi-hacking.html

14 https://www.kb.cert.org/vuls/byvendor

15 https://www.bleepingcomputer.com/news/security/list-of-firmware-and-driver-updates-for-krack-wpa2-vulnerability/

16 https://www.us-cert.gov/ncas/alerts/TA14-290A

17 https://www.us-cert.gov/ncas/alerts/TA14-017A

18 https://www.rnp.br/sites/default/files/apache_remote_code_execution.pdf

19 https://www.rnp.br/sites/default/files/cais-alertavulnerabilidades_no_cms_drupal_-_drupal_core.pdf

20 https://www.rnp.br/sites/default/files/vulnerabilidade_drupal8.pdf

21 https://www.rnp.br/sites/default/files/vulnerabilidade_no_core_do_drupal.pdf

22 http://www.lacnic.net/2675/4/evento/presentaciones-_-slides

23 http://video.rnp.br/portal/video/webinar-EvolucaoDoS

24 http://video.rnp.br/portal/video/webinar-backup

25 http://video.rnp.br/portal/video/incidentes-e-condutas-criminosas

26 https://www.first.org/conference/2017/program#pimplementing-a-country-wide-sensor-infrastructure-for-proactive-detection-of-malicious-activity

27 https://documentos.redclara.net/handle/10786/1256

28 https://www.first.org/events/colloquia/montevideo2017/program

29 https://disi.rnp.br/

30 http://encsirts.rnp.br/

31 https://www.rnp.br/servicos/seguranca/educacao-e-conscientizacao-seguranca

32 https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

33 https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices

34 https://latam.kaspersky.com/blog/33-ataques-por-segundo-kaspersky-lab-registra-un-aumento-de-59-en-ataques-de-malware-en-america-latina/11265/

35 https://research.checkpoint.com/new-iot-botnet-storm-coming/

36 https://www.rnp.br/pesquisa-e-desenvolvimento/internet-futuro

37 https://www.theregister.co.uk/2018/05/10/openflow_switch_auth_vulnerability/

38 https://blog.trendmicro.com/3-reasons-the-ransomware-threat-will-continue-in-2018/

39 https://www.acronis.com/en-us/blog/posts/ransomware-forecast-2018-expect-cars-homes-medical-equipment-and-wearables-be-targeted

40 http://www.valor.com.br/valor-investe/casa-das-caldeiras/5200923/tv-e-principal-fonte-de-informacao-mas-internet-avanca

41 https://www.infochain.com.br/o-blockchain-e-seguro-desmistificando-a-seguranca-no-blockchain-e-entendendo-o-potencial/

Nelson Simões
Diretor-geral

José Luiz Ribeiro Filho
Diretor de Serviços e Soluções

Realização
CAIS
Centro de Atendimento a Incidentes de Segurança

Edilson Lima
Gerente de Segurança da Informação

Redação
Yuri Alexandro
Revisão
Rildo Souza
Rodrigo Facio
Edição Final
Edilson Lima
Diagramação
Flávia da Matta Design

RNP
MINISTÉRIO DA DEFESA
MINISTÉRIO DA CULTURA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
GOVERNO FEDERAL