CAIS EM RESUMO é uma publicação periódica do Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa (CAIS/RNP), que tem como objetivo apresentar os principais acontecimentos relacionados à área de segurança da informação que impactaram a rede acadêmica e de pesquisa no último semestre, bem como as principais realizações do CAIS no período.

DESTAQUE

Ransomwares causam uma das maiores crises cibernéticas a nível mundial

Ransomware é um tipo de malware que se utiliza do recurso da criptografia para bloquear acesso de um usuário a arquivos e sistemas de seu computador e/ou dispositivo móvel, os quais são (ou, pelo menos, tem a promessa de serem) liberados somente mediante pagamento de resgate. Apesar de estarem atualmente com frequência nas manchetes de jornais e televisões, esta não é uma ameaça recente. O primeiro *malware* com as mesmas características dos *ransomwares* que conhecemos atualmente foi desenvolvido em 1989. De lá para cá, a sofisticação do uso malicioso da criptografia tem cada vez mais comprometido computadores e sistemas, afetando usuários, serviços e economias ao redor do mundo. Somente em 2016, foram descobertas quase 200 novas famílias de *ransomwares* e o número de novas variantes cresceram cerca de 600%. O CAIS também destacou os riscos e a tendência do aumento desse tipo de ataque na versão do CAIS EM RESUMO N.5, que foi publicado em setembro de 2015. Na época, vários especialistas já alertavam a comunidade para as medidas preventivas necessárias a serem adotadas por administradores de redes, equipes de segurança e usuários em geral.

Os mais recentes casos de *ransomware*, conhecidos como WannaCry, ou WannaCryptor, e o NotPetya causaram grandes prejuízos no primeiro semestre de 2017, comprometendo milhares de computadores em mais de 150 países, incluindo o Brasil (figura 1). Foram registrados casos de infecção por esses *ransomwares* em órgãos do serviço público e também em instituições que fazem uso da rede brasileira de ensino e pesquisa.

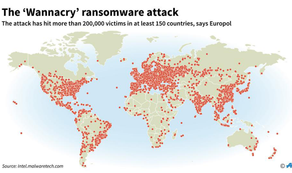

Figura 1 | Fonte: intel.malwaretech.com

Apesar de o NotPetya ser mais agressivo que o WannaCry e bloquear o acesso total ao computador quando da sua reinicialização, por cifrar a tabela de inicialização do sistema operacional e substituir o conteúdo da MBR (*Master Boot Record*) pela mensagem de pedido de resgate, o *modus operandi* dos dois são semelhantes: exploram vulnerabilidades de sistemas operacionais Microsoft Windows para se propagar pela rede local, sendo este o principal motivo deles terem tomado dimensões tão grandes. Tanto o WannaCry quanto o NotPetya exploram uma vulnerabilidade do protocolo SMBv1, usado para compartilhamento de arquivos e impressoras no Windows. Essa vulnerabilidade foi alertada pelo CAIS em abril, quando foi disponibilizada a correção pela Microsoft. Entretanto, o NotPetya ainda é capaz de utilizar as ferramentas PSEXEC e WMI – funções do Windows que permitem a administradores gerenciar computadores remotamente – para se propagar em massa e infectar outros hosts. Assim, basta que computadores não estejam atualizados ou que as ferramentas citadas acima estejam habilitadas em um computador comprometido para que organizações tenham suas redes inteiras sob o risco iminente de serem afetadas por esses *ransomwares* (Figura 2).

Figura 2 | Fonte: Fonte: www.symantec.com

O CAIS recomenda as seguintes ações para evitar ser vitima desse tipo de ataque:

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

ESTATÍSTICAS

O primeiro semestre de 2017 foi marcado pelo aumento de notificações a *hosts* vulneráveis ao ataque POODLE (*Padding Oracle On Downgraded Legacy Encription*), que explora uma vulnerabilidade do protocolo SSL em sua versão 3.0. Se consumado, o ataque pode permitir que um usuário malicioso, utilizando a técnica *man-in-the-middle*, seja capaz de interceptar e decifrar o tráfego da comunicação entre uma vítima e o servidor vulnerável, colocando em risco os dados sensíveis de usuário, tais como *login* e senha, compras, pagamentos pela internet, entre outros (figura 3). Contabilizou-se um aumento de 10 mil notificações, em comparação com o primeiro semestre de 2016. Notou-se também que grande parte dessas notificações se refere a hosts que estão vulneráveis desde 2016, mas que não foram corretamente tratadas até o fim do primeiro semestre de 2017. A vulnerabilidade do SSLv3 é séria e põe em grave risco dados sensíveis, porém é simples de ser resolvida. O CAIS recomenda que seja desabilitado o uso do protocolo SSLv3 tanto nos clientes, pela atualização das versões dos browsers de navegação web, quanto nos servidores, pela utilização do TLS versão 1.2 nas configurações de SSL.

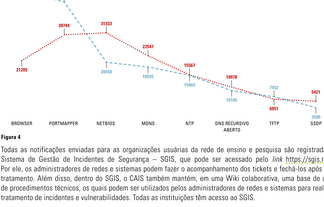

Figura 3

Mantendo o histórico de 2016, o primeiro semestre de 2017 registrou um alto índice de notificações a hosts que hospedam serviços que podem ser usados como vetor de ataques DDoS e DRDoS. Mais de 50% das notificações, entre incidentes e vulnerabilidades, se referem a esses serviços vulneráveis e abertos à internet, tais como DNS recursivo, NTP, SNMP, NetBIOS, SSDP, entre outros. Boa parte dessas vulnerabilidades provêm da configuração incorreta de segurança nos servidores, permitindo que atacantes utilizem essas aplicações para gerar ataques de volumetria com origem na rede acadêmica (figura 4).

Figura 4

Todas as notificações enviadas para as organizações usuárias da rede de ensino e pesquisa são registradas no Sistema de Gestão de Incidentes de Segurança – SGIS, que pode ser acessado pelo *link* https://sgis.rnp.br. Por ele, os administradores de redes e sistemas podem fazer o acompanhamento dos tickets e fechá-los após o seu tratamento. Além disso, dentro do SGIS, o CAIS também mantém, em uma Wiki colaborativa, uma base de dados de procedimentos técnicos, os quais podem ser utilizados pelos administradores de redes e sistemas para realizar o tratamento de incidentes e vulnerabilidades. Todas as instituições têm acesso ao SGIS.

ATUALIZE-SE

O CAIS alterou a sua chave pública PGP

O ID da nova chave é 0x7CDEAD34B8F8F498 (D382 6A1E 6CF1 B485 EBAC 261A 7CDE A034 B8F8 F498). A atualização da chave foi uma ação do CAIS para adequar-se às melhores práticas de segurança. A chave anterior era do tipo RSA 1024 bits, formato na qual foi descoberta recentemente uma vulnerabilidade na biblioteca *Libgcrypt* que permite um atacante extrair a chave privada usada para cifrar dados. A nova chave utiliza RSA 4096 bits e já pode ser encontrada nos servidores de chave PGP na internet.

Segurança na conectividade da rede acadêmica

O CAIS participou do piloto do projeto de segurança dos roteadores da rede Ipê. O objetivo do projeto consistiu em identificar e tratar vulnerabilidades de segurança existentes nos roteadores de borda de clientes, visando ao fortalecimento da segurança da rede de ensino e pesquisa brasileira.

O piloto foi feito com clientes da RNP no estado de Minas Gerais. Contou com o apoio técnico do PoP-MG e da Gerência de Operações da RNP. Como resultado dessa ação, foi produzido um conjunto de recomendações a serem aplicadas por todos os Pontos de Presença da RNP nos clientes da RNP em seus respectivos estados.

O CAIS em eventos internacionais

O CAIS, juntamente com outras áreas da RNP, participou ativamente em dois grandes eventos internacionais no primeiro semestre de 2017. No Lacnic 27, realizado em maio na cidade de Foz do Iguaçu (PR), o CAIS esteve presente na reunião do LAC-CSIRTs, que reúne as 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. Já na programação do evento, durante o LACSEC – seção destinada à segurança da informação – foi apresentado o Guia de Estabelecimento de CSIRTs na Rede de Ensino e Pesquisa, desenvolvido pelo CAIS em 2015 e os resultados da sua utilização em pilotos com clientes da RNP ao longo do ano de 2016. Ainda nessa seção, foram apresentados os resultados do projeto da Rede de Sensores Distribuídos, implementado nos 27 PoPs e em mais 17 organizações. Esse mesmo trabalho também foi apresentado pelo CAIS na Conferência Anual do FIRST – Fórum Mundial das Equipes de Resposta a Incidentes, realizado em junho na cidade de San Juan, em Porto Rico.

Seminários online sobre segurança

O CAIS realizou, neste primeiro semestre, dois seminários online sobre temas relacionados à segurança da informação. O primeiro tratou da evolução de ataques de negação de serviço. Ministrado pelo analista Rildo Souza, a palestra abordou os principais ataques de DoS distribuídos e reflexivos identificados na rede de ensino e pesquisa no Brasil, além das principais vulnerabilidades utilizadas para a execução desses ataques e as respectivas contramedidas para evitar as suas explorações.

O segundo webinar teve "Backup" como tema e foi ministrado pela analista Mirian Von Zuben, do CERT.br. Durante a palestra, foi ponderado a necessidade da realização de cópias de segurança nos dias atuais frente às ameaças de comprometimento dos dados de usuários, sobretudo pelo crescimento da ocorrência de casos de *ransomwares*, além de técnicas e boas práticas para realização e testes das cópias de segurança dos dados.

REFERÊNCIAS

Segue uma lista de documentos utilizados como referência nesta publicação. Recomendamos a sua leitura para complementar os conceitos aqui tratados.

[1] CAIS-Alerta:Vulnerabilidades no serviço SMBv1 da Microsoft
https://www.rnp.br/sites/default/files/vulnerabilidade_servico_smbv1_da_microsoft.pdf

[2] CAIS-Alerta:Ataque massivo do Ransomware WannaCry
https://www.rnp.br/sites/default/files/alerta_ataque_ransomware.pdf

[3] CAIS-Alerta:Ataque massivo do Ransomware NotPetya
https://www.rnp.br/sites/default/files/cais-alerta_-_ataque_massivo_ransomware_notpetya.pdf

[4] This PODDLE Bites: Exploiting The SSL 3.0 Fallback
https://www.openssl.org/~bodo/ssl-poodle.pdf

[5] SSL 3.0 Protocol Vulnerability and PODDLE Attack
https://www.us-cert.gov/ncas/alerts/TA14-290A

[6] PODDLE Vulnerability Puts Online Transactions At Risk
http://blog.trendmicro.com/trendlabs-security-intelligence/poodle-vulnerability-puts-online-transactions-at-risk/

[7] Chave pública do CAIS
http://pgp.rnp.br:11371/pks/lookup?op=vindex&search=0x7CDEAD34B8F8F498

[8] Webinar – A Evolução dos Ataques de DoS
http://video.rnp.br/portal/video/webinar-EvoluacaoDoS

[9] Webinar – Backup: O básico cada vez mais essencial
http://video.rnp.br/portal/video/webinar-backup

RNP
Rede Nacional de Ensino e Pesquisa

Nelson Simões
Diretor-geral

José Luiz Ribeiro Filho
Diretor de Serviços e Soluções

Realização:
CAIS
Centro de Atendimento a Incidentes de Segurança da RNP

Edilson Lima
Coordenador de Segurança da Informação

Redação:
Yuri Alexandro

Revisão:
André Landim, Carla Freitas

Edição Final:
Edilson Lima

Diagramação:
Flavia da Matta Design