CAIS EM RESUMO SET14 N.2

Alertas, vulnerabilidades e incidentes de segurança

CAIS EM RESUMO é uma publicação periódica do Centro de Atendimento a Incidentes de Segurança (CAIS/RNP), que tem como objetivo apresentar, de forma reduzida, os principais alertas, vulnerabilidades, tipos de ataque e demais acontecimentos da área de segurança da informação, que impactaram a rede acadêmica e de pesquisa no último quadrimestre.

DESTAQUE

Protocolo UDP utilizado em ataques de amplificação - DRDoS

Com o recente crescimento da exploração do protocolo UDP em ataques de amplificação (DRDoS do inglês: *Distributed Reflection Denial of Service*), a atenção aos serviços que utilizam esse protocolo para comunicação deve ser maior. Diante disto e com o intuito de apoiar as organizações conectadas à rede Ipê a identificar e corrigir sistemas vulneráveis, o CAIS adicionou em seus sistemas a notificação dessa vulnerabilidade, o que causou um aumento considerável no número total de notificações.

Para se entender melhor como acontece este tipo de ataque, é necessário notar que uma das características do protocolo UDP é o fato dele não ser orientado à conexão, isto é, os serviços que utilizam este protocolo para comunicação não estabelecem uma conexão entre origem e destino antes de iniciar a transferência de dados. Isso não acontece com o protocolo TCP devido ao processo *three-way handshake*, que pede uma validação do destino para estabelecer uma conexão, dificultando a realização de pacotes com origem falsificada, o que impossibilita esse tipo de ataque.

Vale ressaltar que a não existência do *three-way handshake* no protocolo UDP não caracteriza uma vulnerabilidade em si. Algumas aplicações, como VoIP e *streaming* e aplicativos, como jogos *online,* por exemplo, não requerem a presença deste mecanismo.

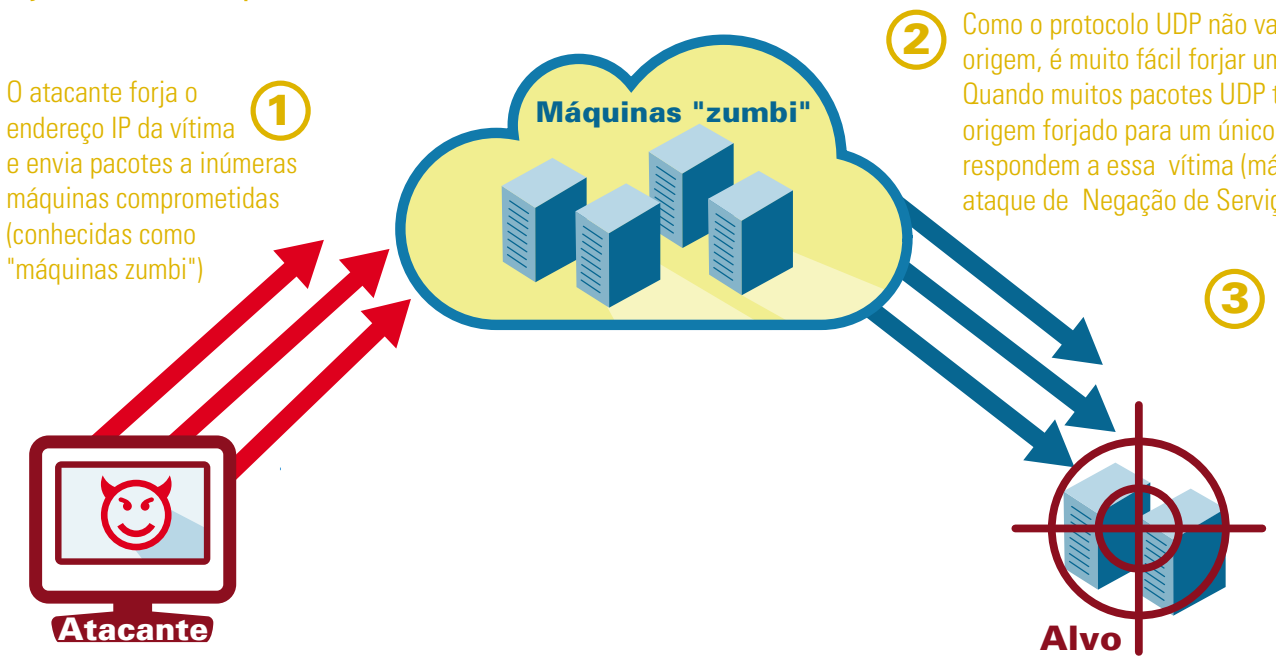
Um ataque de Negação de Serviço Distribuído (DRDoS) é uma forma de ataque de Negação de Serviço Distribuído (DDoS), que baseia-se na utilização de servidores UDP acessíveis ao público, bem como os fatores de amplificação de banda, para sobrecarregar o sistema da vítima com tráfego UDP.

Veja como o ataque funciona:

1 O atacante forja o endereço IP da vítima e envia pacotes a inúmeras máquinas comprometidas (conhecidas como "máquinas zumbi")

2 Como o protocolo UDP não valida os endereços IP de origem, é muito fácil forjar um endereço IP arbitrário. Quando muitos pacotes UDP têm o seu endereço IP de origem forjado para um único endereço, os serviços UDP respondem a essa vítima (máquina "zumbi"), criando um ataque de Negação de Serviço Distribuído (DDoS).

3 A vítima é inundada por todos os dados enviados a partir dos serviços UDP. Adicionalmente, onde antes os atacantes eram limitados pelo número de pacotes enviados diretamente para o alvo, para realizar um ataque de Negação de Serviço, agora um único pacote pode gerar dezenas ou centenas de vezes a largura de banda em sua resposta. Isto é chamado de ataque de amplificação e, quando combinado com um ataque Reflexivo de Negação de Serviço em grande escala, faz com que seja relativamente fácil realizar ataques DDoS.



Violação de direitos autorais

Até agosto de 2014, o número de incidentes envolvendo download de material protegido por direitos autorais ultrapassou o total de incidentes desta categoria, em relação ao ano inteiro de 2013. O CAIS notificou 3.346 incidentes de violação de direitos autorais nesse ano, 164% de aumento comparado ao número total de incidentes dessa categoria em 2013 (1268 incidentes). Esse aumento está diretamente relacionado a novas parcerias e sensores utilizados pelo CAIS para a detecção.

O *download* de arquivos protegidos por direitos autorais caracteriza um incidente de segurança, pois viola a Política de Uso da rede Ipê, além da legislação vigente no país.

ESTATÍSTICAS

Com mais de 226 mil notificações, no segundo quadrimestre de 2014, um novo recorde na história do CAIS é alcançado.

Veja o que contribuiu para esse fato:

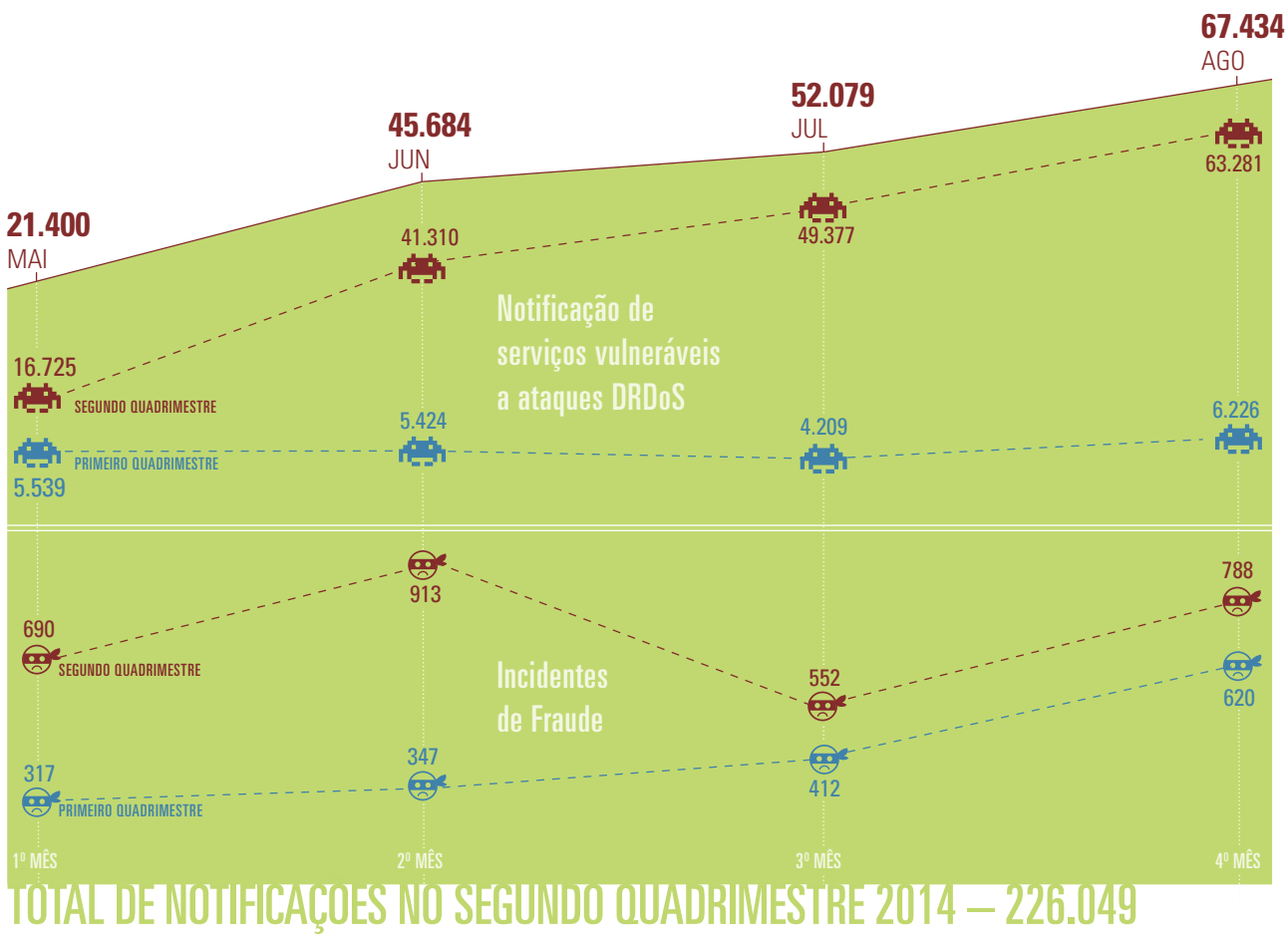
Inclusão de notificação de serviços vulneráveis a ataques DRDoS

O aumento na detecção de servidores vulneráveis aos ataques de reflexão (DRDoS – *Distributed Reflection Denial of Service*) na rede Ipê é o fator de maior relevância para esse resultado. A média do primeiro quadrimestre de 2014 foi de 5.349 notificações, no segundo quadrimestre a média aumentou **697%**, alcançando o número de 42.673.

Incidentes de fraude

O registro de incidentes de violação de direitos autorais também teve um aumento significativo, com um aumento médio de 74% incidentes desta categoria.

Conforme citado na seção "Destaques", novas parcerias estabelecidas pelo CAIS contribuíram com o aumento da detecção de incidentes.



TOTAL DE NOTIFICAÇÕES NO SEGUNDO QUADRIMESTRE 2014 – 226.049

ATUALIZE-SE

DISI e Mês de Segurança 2014

Segurança na nuvem foi o tema da 9ª edição do Dia Internacional de Segurança em Informática (DISI), promovido pela Rede Nacional de Ensino e Pesquisa (RNP), por meio do seu Centro de Atendimento a Incidentes de Segurança (CAIS) como uma ação internacional para o Mês de Segurança.

Realizado em Brasília, no dia 5 de setembro, o evento contou com a abertura do diretor da RNP, Nelson Simões (RNP), e dos representantes dos parceiros OEA e RedCLARA, Gonzalo Garcia-Belenguer e Florencio Utreras, respectivamente.

As palestras abordaram diversos aspectos relacionados a segurança na nuvem, como a segurança no uso de aplicações, termos de uso e ataques relacionados aos serviços na nuvem, segurança nas redes sociais, o armazenamento seguro dos dados na nuvem e o futuro dos dados armazenados na nuvem após a morte.

Além do evento presencial, várias instituições no Brasil e na América Latina transmitiram o DISI, como uma ação para o Mês de Segurança. O evento é um conjunto de celebrações que acontece anualmente durante todo o mês de setembro, com o intuito de fomentar a cultura de segurança da informação.

Até o fechamento desta edição, 98 instituições no Brasil e na América Latina inscreveram-se no Mês de Segurança com a finalidade de realizar atividades de conscientização em segurança da informação em suas instituições. Participe também com sua instituição!

Saiba mais sobre o DISI e o Mês de Segurança.

REFERÊNCIAS

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

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

http://www.prolexic.com/knowledge-center-white-paper-series-dns-reflection-amplification-drdos-attacks-ddos.html

http://www.rnp.br/sites/default/files/cais-alerta-maio-2014.pdf

http://www.rnp.br/sites/default/files/cais_alerta_ntp_0.pdf

http://www.rnp.br/sites/default/files/cais-alerta-junho-2014.pdf

http://www.rnp.br/sites/default/files/cais-alerta-openssl-junho.pdf

http://www.rnp.br/sites/default/files/cais-alerta-julho-2014.pdf

http://www.rnp.br/sites/default/files/cais-alerta-agosto-2014.pdf

http://www.rnp.br/sites/default/files/cais-alerta-agosto-2014-adendo.pdf

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

Liliana Velásquez Solha
Gerente de Segurança da Informação

Redação:
Alan Santos, Ana Carolina Fukushima, Edilson Lima e Rildo Souza

Projeto visual e Diagramação:
Tecnodesign