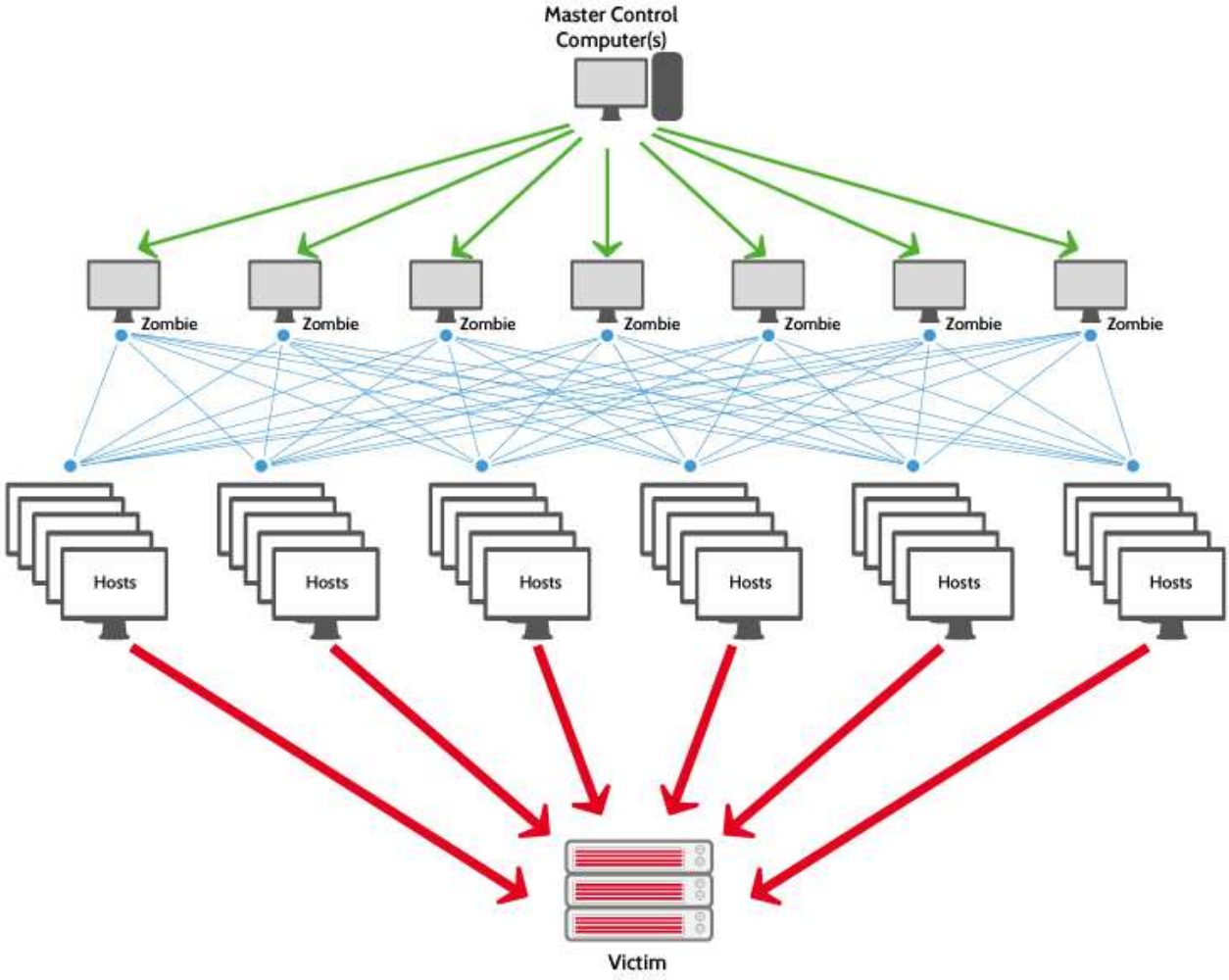
Ataque DDoS[1]

De forma bem resumida, num **ataque** distribuído de negação de serviço (também conhecido como **DDoS**, um acrônimo em inglês para Distributed Denial of Service), um computador mestre denominado master pode ter sob seu comando até milhares de computadores zombies, literalmente zumbis. Estes zumbis acessam um determinado serviço; página de web; cloud (nuvem); ou até mesmo um servidor em geral. Com um número de acessos enormes faz com que o sistema pare por falta capacidade de atender a todas as solicitações.

Alvos e tipos de ataque



[1] Wikipedia

Mais de 15 mil ataques DDoS atingiram 7 mil sites em 10 dias[2]

Há algumas semanas, aconteceu o maior ataque DDoS da história. Um ataque hacker foi detectado, no dia 28 de fevereiro, pela equipe do site GitHub, mais famoso repositório de códigos na internet, e teve picos de tráfego de até 135 Terabits por segundo.

Agora, segundo informações do The Hacks News, o ataque abriu espaço para que outros hackers se aproveitassem da situação. Nos últimos 10 dias, já foram registrados mais de 15 mil ataques DDoS que atingiram 7.113 sites.

O monitoramento da Qihoo 360's Netlab mostra que os ataques são baseados em Memcached e atingiram sites famosos, incluindo Google, Amazon, QQ.com, 360.com, PlayStation, OVH Hosting, VirusTotal, Comodo, GitHub, Royal Bank, Minecraft, RockStar, Avast, Kaspersky, PornHub, Epoch Times e Pinterest.

A equipe de monitoramento descobriu a vulnerabilidade Memcached em junho de 2017 e divulgou em novembro de 2017. Mesmo com os alertas, mais de 12 mil servidores com suporte UDP habilitado ainda estão vulneráveis, o que poderia alimentar mais ciberataques.

[2] Juliana Américo 09/03/2018 ciberataque Hackers

Operadora nos EUA resiste a maior ataque DDoS da história[3]

Na semana passada, o GitHub foi atingido pelo maior ataque DDoS já registrado até aquele momento. Mas infelizmente, o recorde durou pouco. A empresa de segurança digital Arbor Networks divulgou hoje que detectou um ataque DDoS com intensidade de 1,7 Tbps contra um cliente de uma operadora de telecomunicações dos EUA; apesar do ataque, a operadora resistiu e manteve o serviço funcionando.

O ataque contra o GitHub havia sido detectado pela Akamai, mas o ataque de segunda-feira, ainda maior, foi detectado pela rede ATLAS de monitoramento de tráfego de internet. Antes desse ataque, o maior golpe DDoS que a ATLAS já havia registrado foi um ataque de 650 Gbps que tinha como alvo um serviço hospedado no Brasil.

Nova era de DDoS

DDoS é uma sigla que, em inglês, significa "Distributed Denial of Sevice"; um ataque DDoS, portanto, é um ataque distribuído de negação de serviço. Ele acontece quando muitas máquinas tentam acessar um único site ao mesmo tempo; se o site não estiver preparado para receber esse tipo de tráfego, ele corre o risco de sair do ar, como aconteceu com o GitHub na semana passada.

Para levar muitas máquinas para o site ao mesmo tempo, os hackers normalmente se valem de "botnets". As "botnets" são redes de dispositivos infectados por programas que permitem que eles sejam manipulados a gerar tráfego para determinados IPs a partir do comando de outro computador. Um hacker ordena que a botnet ataque determinado site ou serviço e, em breve, milhares de dispositivos estão tentando acessá-lo ao mesmo tempo.

Mas tanto no caso do GitHub quanto no ataque de ontem, os hackers usaram mais um recurso. Trata-se do memcached (como já foi citado anteriormente e mais detalha ao final), um protocolo de cache de bases de dados cujo propósito original é acelerar o carregamento de páginas e conteúdos da rede colocando determinadas partes delas na memória RAM dos servidores. Abusando desse protocolo, os hackers conseguem aumentar em até 51 mil vezes a intensidade de seus ataques, segundo o ArsTechnica.

Sequestro

Embora ataques DDoS possam ser feitos só para tirar do ar determinado site, muitas vezes eles são feitos como parte de um "sequestro". Os atacantes ameaçam tirar do ar o site ou serviço de determinada empresa por meio de um ataque DDoS, e cobram uma quantia (geralmente em criptomoedas) para que o ataque não ocorra.

A Arbor Networks não esclareceu se foi esse o caso do ataque de segunda-feira. No entanto, a empresa deixou claro que, apesar do ataque, o site vitimado não saiu do ar. Mesmo assim, a empresa de segurança considera que ataques que exploram o protocolo

[3] Gustavo Sumares 06/03/2018 16h00 Empresas Hackers Segurança

memcached devem se tornar cada vez mais comuns, e por isso o recorde estabelecido por esse último golpe pode novamente ser batido em breve.

Memcached[4]

Em computação, **memcached** é um sistema distribuído de cache em memória de propósitos gerais. É frequentemente utilizado para acelerar sites dinâmicos orientados a banco de dados, cacheando dados e objetos na Memória (RAM) para reduzir o número de vezes que uma fonte de dados externa (como um banco de dados ou uma API) deve ser acessada. Foi originalmente desenvolvido pela Danga Interactive para o LiveJournal, mas é usado agora para muitos outros sites. O Memcached roda em Unix, Linux, Windows and Mac OS X e é distribuído sobre a licença Revised BSD license. No sistema computacional a memória pode ficar dentro processador ou na placa mãe, mas de qualquer forma seu acesso é muito mais rápido que a memória normal do computador. Esta cache é uma memória de uso temporário.

[4] Wikipedia e Pedro Ismar UFMS