

Derrotando o botnets do Futuro

O artigo seguinte é extraído do *Understanding and Blocking the New Botnets*, um relato pesquisado e escrito por Scott Pinzon, CISSP, e Corey Nachreiner, CISSP, da equipe WatchGuard @ LiveSecurity . Para saber como eles evoluíram, e como eles funcionam hoje, faça o download gratuito do arquivo em <http://www.watchguard.com/infocenter/whitepapers.asp>

Códigos Botnets executam quase todas as formas de malwares, de spywares para Downloaders, rootkits, spams e muito mais. Para ter um bom desempenho, os “antídotos” devem proteger múltiplas camadas de segurança. A boa notícia é que essas camadas são surpreendentemente eficazes contra botnets. Abaixo sugerimos contramedidas que ajudam a prevenir o risco de uma infecção por bots em sua rede.

1. Patch promptly

Bots podem recorrer a uma grande variedade de opções a fim de infectar as redes. No entanto, os maiores e mais bem sucedidos bots exploram vulnerabilidades que o técnico tenha se protegido de seis a dezoito meses mais cedo. Nos casos mais extremos, vimos bots tentando infectar máquinas que se protegeram até quatro anos atrás. Por isso não podemos inovar em um ritmo empolgante, ao passo que o bot usa 'exploits' que são conhecidos e antigos. O nosso melhor palpite é que os botmasters encontrem uma solução e, em seguida, a engenharia descubra onde foi a falha.

Nós esperamos que os botmasters se preocupem mais com os problemas recentes para que sejam solucionados rapidamente. Porém, isso é uma boa notícia para os administradores de rede.

2. Bloqueio de JavaScript

Um bot ataca uma vitima executando o JavaScript. Configurando navegadores antes de executar JavaScripts eliminará uma enorme faixa de infecções. É altamente recomendável que os usuários confiem no Firefox como seu principal navegador, usando o [plug-in para noscript](#) sempre que um script tentar executar.

3. Cuidado Especial com as Portas de Serviços

Essa é a segunda parte da recomendação

1) Embora os bots mais recentes se comuniquem através de portas que os administradores deixam abertas, a grande maioria dos bots ainda se comunicam usando IRC (porta 6667) e outras portas não usuais (tais como 31337 e 54321). Todas as portas acima de 1024 devem ser definidas para bloquear a entrada e saída, a não ser que sua empresa tenha um aplicativo personalizado ou a necessidade especial para a abertura de uma determinada porta. Mesmo assim, você pode abrir uma porta com cuidado, implementar políticas tais como "aberta apenas durante o horário comercial" ou "negar tudo, exceto o tráfego a partir da seguinte lista de endereços IP confiáveis." Essa simples medida evita a variedade de bots de chegarem ao seu Centro de Comando e Controle (C & C).

2) Botnets trafegam por portas 80 ou 7, quando não deveria haver nenhum tipo de tráfego nestas portas. Normalmente, botmasters atualizam entre 1h00-5h00. Tenha o hábito de verificar o seu servidor de logs na parte da manhã.

Administradores utilizando WatchGuard Firebox ® estarão satisfeitos por saber que a Firebox procura parar o tráfego não-padrão e tenta executar no padrão correto. Por exemplo, o spam Mega-D é executado fora do padrão, tráfego sobre HTTP porta 80. O Firebox's proxy HTTP local iria bloquear esse tráfego instantaneamente.

4. Redobrar o treinamento para sensibilizar os usuários

Alguns bots executam scans em massa na Internet, encontram máquinas vulneráveis e infectam-nas. Frequentemente, os bots de "engenharia social" infectam sua rede quando uma vitima clica em um link malicioso. Estes bots seguem as mesmas restrições que alguns lendários vampiros: eles não podem cruzar o seu limite, a menos que você convide-o.

Esta "isca" tem sido muito utilizada. Invasores utilizavam códigos executáveis maliciosos anexados em e-mails, mas essa técnica vem diminuindo. A maior parte dos ataques, agora, são feitos na web. E-mails maliciosos que traziam anexos há dois anos atrás, agora utilizam links para sites perigosos. Web sites podem ser infectados pelo Mpack ou outro malwares oculto para infectar os visitantes que clicam no link..

Essa é a sua dica para explicar aos usuários, em termos fáceis de entender, o porquê eles nunca deveriam convidar um 'vampiro' para sua rede. Informe-os para não abrir anexos que não possuem conhecimento ou que pareçam duvidosos; eles não devem clicar em links vindos em e-mails, ou devem pensar duas vezes antes de clicar. Se você precisar de um ponto de partida, apresente nosso vídeo que mostra como o "drive-by downloads" trabalha: <http://video.google.com/videoplay?docid=-4094518401580008932>.

5. Fique atento

Esta recomendação parece óbvia demais, é como falar, "Tente não ser infectado!" Nós continuamos encontrando administradores de TI que gastam muito tempo demitindo e mantendo um suporte (help desk) desfalcado, eles nunca observam seus históricos. Eles nunca monitoram o uso de sua banda de conexão. Eles não podem lhe dizer quem está conectado a sua rede.

Eles têm dispositivos conectados à sua rede que não possuem nenhum conhecimento.

Se isso serve para você, todos nós podemos dizer que você está implorando por apuros. Você pode até ter bots em sua rede que e nem sabe. Se você é um administrador que raramente verifica seus registros, você deve começar a lê-los. Trinta minutos por dia é tudo que você precisa para uma verificação no seu computador.

Se isso serve para você, não significa que você é preguiçoso, mas que você é limitado pela falta de recursos. Explique a ameaça ao seu chefe e veja se eles irão apoiá-lo na perda de meia hora cada manhã para verificar o estado da sua rede. Esta forma de seguro é quase nada em comparação com o custo de uma rede compromissada.

Nós acreditamos que com os avanços, inovações estão por vir. Como nunca ocorreu em anos, cada mês parece que são descobertas coisas que os investigadores não podem explicar.

Acontece que os botnets têm se misturado com ameaças, mas eles não foram misturados com ameaças finais. Botmasters agora complementam gratuitamente a tradicional arquitetura botnet com componentes adicionais que aumentam a automação, administração e evasão. Essa combinação de tecnologias é assustadoramente sofisticada e surpreendentemente eficaz. Qualquer observador pode seguramente prever que essa tendência não vai somente continuar, mas como crescer também.

Os "bad boys" estão ganhando? Evidentemente não, já que ainda fazemos operações bancárias e compras pela internet. Mas a onda de atividades de bot está crescendo, então nós deveremos recuar, represando a onda de bot e identificando suas técnicas. Um jeito simples de minar o poder dos botmasters é deixar difícil para que o código bot recrute vítimas

Os equipamentos de segurança WatchGuard utilizam inúmeras camadas de segurança, inteligência aplicada em vários protocolos com a poderosa tecnologia proxy, que analisam tanto as *entradas* quanto as *saídas* para manter sua rede segura.

Para obter informações sobre as soluções WatchGuard de segurança e proteção contra botnets e outras ameaças de rede, visite-nos em www.watchguard.com ou fale com nossos canais autorizados.