A ferramenta de segurança da Web de Cisco (WSA) fornece a proteção do malware/spyware?

Índice

Pergunta

A ferramenta de segurança da Web de Cisco (WSA) fornece a proteção do malware/spyware?

A ferramenta de segurança da Web de Cisco (WSA) fornece a defesa a mais detalhada do gateway da indústria contra o spyware e o malware com base na Web. Isto inclui tudo do adware (que causa a maioria de edições do supportability e consome recursos de rede significativos) a umas ameaças mais maliciosas tais como Trojan, objetos do ajudante dos piratas do ar do navegador, do navegador, phishing, Pharming, monitoramentos de sistema, Keyloggers, worms, etc.

Os diferenciadores de tecla da solução da Segurança da Web de Cisco incluem:

1. Um monitor de tráfego da camada integrada 4 (L4) faz a varredura de todas as portas na velocidade de fio, detectando e obstruindo a atividade do malware e do Phone Home. Seguindo todas as 65,535 portas de rede, o monitor de tráfego L4 para eficazmente o malware que as tentativas de contornear a porta 80 e igualmente impedem o P2P desonesto e o IRC atividade relativa.
2. Processamento da Proxy-camada: A ferramenta de segurança da Web de Cisco igualmente inclui um proxy da Web do desempenho extremamente alta, junto com pôr em esconderijo integrado & capacidades satisfeitas da aceleração. Construído no sistema operacional proprietário de Cisco, AsyncOS, o dispositivo do proxy da Web de Cisco pode apoiar até 100,000 conexões simultâneas tanto quanto os servidores proxy 10x baseados no Unix mais do que tradicionais. Ser um proxy da Web permite a inspeção satisfeita detalhada na camada de aplicativo - um requisito crítico para assegurar a precisão contra o malware com base na Web.
3. Filtros da reputação da Web da indústria os primeiros fornecem uma camada exterior poderosa de defesa. O ® Leveraging de SenderBase, filtros da reputação da Web de Cisco analisa sobre o tráfego de web 50+ diferente e parâmetros ligados à rede para avaliar exatamente a fiabilidade de uma URL. As técnicas sofisticadas da modelagem de Segurança são usadas para pesar individualmente cada parâmetro e para gerar uma única contagem numa escala de -10 a +10. As políticas configuradas administrador são dinamicamente aplicadas, com base em contagens da reputação.
4. Exploração acelerada da assinatura usando o motor dinâmico Vectoring & fluir (motor DV). Ao contrário das soluções da arquitetura do legado que confiam no ICAP e em um desenvolvimento da multi-caixa para assegurar a exploração do malware, o WSA de Cisco

introduziu o motor DV para uma solução integrada da exploração da em-caixa. Esta plataforma inovativa emprega objeto sofisticado que analisa gramaticalmente e que vectoring técnicas, junto com a exploração do córrego e a sentença que põem em esconderijo, tendo por resultado até um aumento da taxa de transferência da exploração 10x sobre soluções ICAP-baseadas primeira geração.

5. O sistema líder de mercado do Anti-malware de Cisco leverages o motor DV e os tipos múltiplos da assinatura de Webroot para fornecer o melhor da proteção da raça contra a variedade a mais larga de ameaças com base na Web. Estas ameaças podem variar do adware, dos piratas do ar do navegador, do phishing e dos ataques pharming a umas ameaças mais maliciosas tais como Trojan, monitoramentos de sistema e Keyloggers. WSA oferece o base de dados o maior da assinatura do malware da indústria no gateway.