

A Fortinet revelou os resultados da primeira análise de dados do Programa de Avaliação Global de Ameaças Cibernéticas da Fortinet (CTAP). Os resultados indicam que empresas de todos os tamanhos e verticais continuam enfrentando um cenário constante e consistente de riscos, com mais de 32 milhões de tentativas de ataques em cinco meses (outubro de 2015 a fevereiro de 2016).

"As empresas sofrem ataques cibernéticos constantemente. Com o substancial aumento da superfície de ataques e um ecossistema maduro de ameaças, as empresas têm de estar cada vez mais vigilantes em relação a todos os seus ativos de TI", diz John Maddison, vice-presidente sênior de Soluções e Produtos da Fortinet.

Devido aos lucrativos dados financeiros obtidos quando essas redes são infiltradas, as organizações bancárias e financeiras são alvo de 44,6% de toda a atividade maliciosa. Os hackers confiam em ataques de alta velocidade e concentram seus esforços em trojans sofisticados.

As companhias do setor de Educação representam 27,4% de todos os eventos de ataque neste relatório e são a segunda vertical de maior risco. Botnets representam a ameaça dominante para instituições de ensino, com 7 das 10 principais infecções, enquanto o XcodeGhost, o amplamente divulgado malware do iOS, divide a lista das Top 10 vulnerabilidades na área de educação.

Já o setor de Saúde ficou em terceiro lugar na lista de atividades maliciosas globais, com 10,6% dos eventos de ataque e destaque em exploit kits automatizados, com foco em inúmeras vulnerabilidades no Flash, Silverlight e Internet Explorer, para comprometer sistemas por meio de ações de drive-by-download ou websites infectados.

Atividades de mídias sociais e de streaming multimídia são responsáveis por 25,65% de todo o tráfego de rede, expondo os sistemas e dados corporativos sensíveis a riscos de infecção a partir de downloads, engenharia social e publicidades maliciosas. O Facebook é o mais dominante, representando 47,27% de todo o tráfego de mídia social, com o YouTube contribuindo para 42,29% do conteúdo transmitido.

O conteúdo publicitário contabiliza 19,1% do tráfego da rede e tem demonstrado ser uma fonte potencial de malware, uma vez que redes de publicidade de terceiros são subvertidas para fornecer anúncios maliciosos. O controle de aplicações surge como um desafio contínuo para os administradores. Uma quantidade significativa de tráfego ponto-a-ponto, principalmente Bittorrent e jogos, expõe a rede a um conteúdo malicioso que pega carona com aplicações e arquivos baixados por meio desses sites populares. As empresas devem ter cuidado ao construir políticas de controle de aplicativos em suas redes.

Fonte: [RISK REPORT](#), em 10.03.2016.