technology review.es
Published by MIT

Segunda-feira, 11 de agosto de 2014

Antes de Começarem os Conflitos Russo e Israelense, Houve Impresionante Aumento no Trafego de Malware

Aparentemente hackers do governo foram ao trabalho quando Israel e Rússia aumentaram suas atividades militares este ano.
Por Tom Simonite

Imagem: *Briefing de Segurança: Participantes assistem a uma apresentação na conferência Black Hat 2014.*

Um estudo sobre a operação de malware em redes corporativas e governamentais sugere que os padrões de comunicação destes programas poderia ser um aviso da chegada de grandes conflitos.

Pesquisadores da empresa de segurança FireEye monitoraram milhões de mensagens enviadas por malware ao longo dos últimos 18 meses e encontraram picos no tráfego entre Rússia e Ucrânia enquanto as tensões aumentavam entre os dois países no início deste ano. Um padrão semelhante foi observado no tráfego de malware para Israel à medida que se iniciavam as recentes hostilidades com o Hamas.

O estudo da FireEye se baseou em dados coletados de mais de 5.000 clientes corporativos e governamentais em todo o mundo. O software da FireEye captura mensagens de "*callback*" enviadas por malware dentro de uma rede - relatando seu status para seus operadores ou recebendo novos comandos. Essas mensagens foram usadas para determinar a localização do computador que estava controlando o malware.

A provável causa dos padrões deve ser agências do governo aumentando seus esforços para coletar informações ou atacar seus adversários, diz Kenneth Geers, que trabalhou no projeto. "No período que antecedeu a crise na Crimeia, vimos um aumento no numero de mensagens '*callback*' de malware tanto na Rússia quanto na Ucrânia", disse ele na conferência de segurança da computação, Black Hat, na quinta-feira.

Também é possível que a atividade tenha vindo de hackers simpatizantes, mas não apoiados pelos países envolvidos nos conflitos. Mas, hoje em dia, muitos países usam de forma rotineira ataques digitais para fins militares e de inteligência.

Geers disse que os padrões de comunicação de malware pode ser usado para prever quando os países estão se preparando para o conflito: "Se EUA, Coréia ou Japão estivessem prestes a entrar em guerra, você veria um aumento de *callbacks* - é apenas parte integrante do serviço

das empresas de segurança nacional de hoje". Geers, que recentemente deixou a FireEye para trabalhar como consultor independente, anteriormente trabalhava com segurança computacional internacional na Agência Nacional de Segurança (dos EUA) e na OTAN.

Operadores e malware as vezes escondem sua localização fazendo com eu mensagens viajem por computadores em diferentes países, mas o estudo da FireEye só conseguiu registrar a primeira parada. No entanto, os autores dos malware nem sempre instalam esse tipo de proteção, diz Geers. Logo, disse ele, com um conjunto de dados grande o suficiente, padrões geográficos reais são revelados.

Grande parte do tráfego para Israel enquanto se mobilizava para atacar o Hamas na Faixa de Gaza veio de malware instalado em computadores no Canadá e nos EUA "Você tem um indício de que organizações de segurança nacional israelenses talvez estejam aproveitando a infra-estrutura do Canadá e doa EUA", disse Geers.

Correspondência de tráfego de malware para eventos do mundo real também pode fornecer uma maneira de descobrir ferramentas que estão sendo usadas por Estados-nação. Parte do tráfego que sai do Canadá, por exemplo, parecia vir de malware que nunca tinha sido visto antes, que FireEye está investigando agora.

FireEye tem planos de continuar a pesquisa. "Podemos ver o equivalente digital a tropas na fronteira," disse Kevin Thompson, analista de risco da empresa, ao MIT Technology Review. "Mas nós gostaríamos de olhar para um ano inteiro de dados e tentar correlaciona-los a todos os eventos mundiais do mesmo período".

O uso de malware pelo governo está se tornando mais comum, de acordo com Mikko Hypponen, chefe de pesquisa da F-Secure, que estuda malware feito e utilizado por nações. Países de todos os tamanhos utilizam malware porque é relativamente barato e traz resultados, disse ele durante uma palestra na Black Hat na quarta-feira. "Há paralelos aqui com a corrida para o armamento nuclear", disse ele. "[Mas] o poder das armas nucleares estava na propagação do medo e não temos isso com as armas cibernéticas".

E, como Geers observou, há um conflito entre o entusiasmo dos governos com essas novas armas e sua obrigação de garantir a segurança da Internet. "O problema do malware em todo o mundo é muito difícil de resolver, mas os governos querem resolver isso?", disse. "Governos se beneficiam bastante protegendo a soberania e projetando poder através de ataques à rede".