Alerta da Setic: entenda tudo sobre o 'supervírus' Flame

Praga é considerada "uma das mais complexas ameaças já descobertas"

Praga está atacando máquinas no Oriente Médio e é considerada "uma das mais complexas ameaças já descobertas".

Um assustador vírus de computador batizado de Flame está à solta no Irã e outras partes do Oriente Médio, infectando PCs e roubando informações. E agora a International Telecommunications Union, um órgão ligado às Nações Unidas, alerta que outros países podem estar correndo risco de sofrer um ataque.

Mas o que é exatamente o Flame? Ele é uma ameaça aos usuários domésticos de PCs? Veja a seguir tudo o que você precisa saber sobre o que a Kaspersky chama de "uma das mais complexas ameaças já descobertas".

O bê-a-bá do Flame

A Kaspersky descreve o Flame como um backdoor e Trojan com características de um Worm. Ou seja, ele permite que a máquina seja controlada remotamente, se infiltra "disfarçado" no PC e pode se propagar sozinho através de uma rede. O ponto de entrada do vírus é desconhecido - ataques de "phishing" (quando o usuário é enganado e convencido a baixar o programa) e sites infectados são duas das possibilidades. Após a infecção inicial, ele pode se espalhar entre máquinas através de pendrives ou circulando por redes locais.

O Flame não causa danos ao PC: ele foi projetado para roubar informações das máquinas infectadas. Vitaly Kamlyuk, especialista chefe em malware da Kaspersky, disse ao site RT que o vírus pode coletar informações de campos de texto, incluindo senhas representadas por asteriscos, gravar áudio usando o microfone do computador e capturar imagens de aplicativos considerados interessantes, como um cliente de e-mail ou programa de bate-papo. Ele também pode coletar informações sobre aparelhos Bluetooth "descobríveis" nos arredores. Toda essa informação é enviada a servidores de comando e controle, e há cerca de uma dúzia deles espalhados pelo mundo.

O vírus lembra o worm Stuxnet que causou prejuízos no Irã em 2010, mas

segundo a Kaspesky o Flame é muito mais complexo, com um conjunto de módulos que pode ocupar mais de 20 MB de espaço em disco. “Considere isto: levamos vários meses para analisar os 500KB de código do Stuxnet, e o Flame é mais de 40 vezes maior. Provavelmente levará um ano para que possamos entender completamente seu código”, disse a empresa.

De onde o Flame veio?

O Flame está à solta desde 2010, de acordo com a Kaspersky, mas sua data de criação é incerta. Ele foi descoberto há cerca de um mês após o Ministério do Petróleo do Irã descobrir que os servidores de várias empresas haviam sido atacados. Esta descoberta levou à evidência de mais ataques a outros ministérios e indústrias iranianas.

O Irã alega que os ataques também apagaram os HDs de algumas máquinas, mas a Kaspersky diz que o malware responsável por isso, chamado Wiper, não é necessariamente relacionado ao Flame. Os ataques do Wiper foram isolados ao Irã, enquanto o Flame foi encontrado em outros países.

O criador do Flame é desconhecido, mas é provável que uma nação esteja por trás dele. O vírus não foi projetado para roubar dinheiro de contas bancárias, e é muito mais complexo do que qualquer coisa comumente usada por “hacktivistas”, então esta é a única possibilidade que faz sentido.

Quem corre perigo?

A International Telecommunications Union está avisando a outros países para “ficar em alerta” quando ao vírus, que potencialmente poderia ser usado para atacar infraestrutura crítica. Em uma declaração à Reuters, o Departamento de Segurança Nacional do governo dos EUA disse que “foi notificado sobre o Malware e está trabalhando com seus parceiros federais para determinar e analisar seu impacto potencial nos EUA”

Empresas de segurança não alertam sobre nenhum risco direto ao usuário comum da Internet. Graham Cluley, da Sophos, lembra que o Flame só foi encontrado em algumas centenas de máquinas. “Certamente, é bastante insignificante quando comparado aos 600.000 Macs infectados com o malware Flashback no início deste ano”, disse Cluley em um post em um blog da empresa.