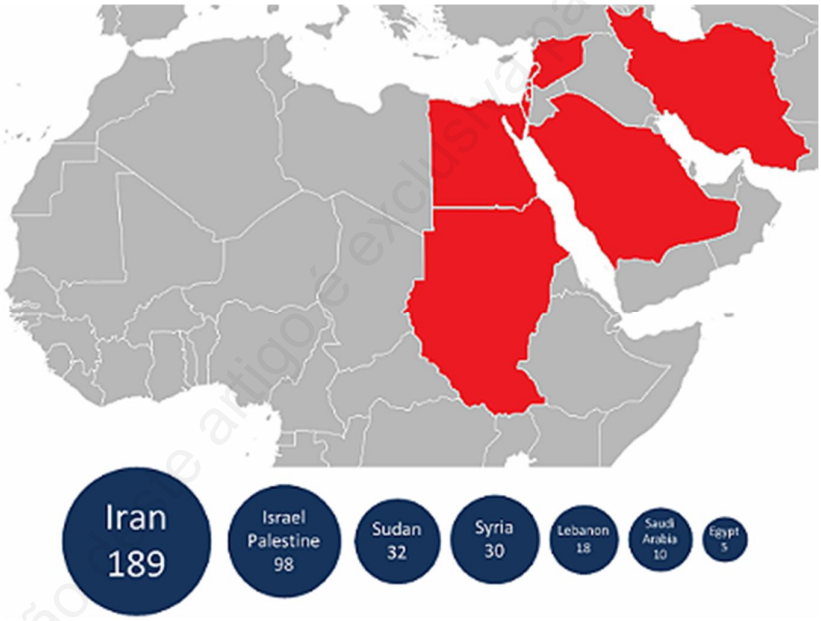
'Supervírus' espião é o mais complexo já descoberto

Pesquisadores da Kaspersky dizem que Flame é especializado em roubar dados e é tão sofisticado que age há dois anos sem ter sido detectado

Meses depois do Stuxnet, vírus que atingiu o programa nuclear do Irã, uma nova - e mais sofisticada - ciberarma foi descoberta. De acordo com pesquisadores da Kaspersky, a complexidade e a funcionalidade do programa malicioso recém-descoberto são superiores aos de todas as ciberameaças conhecidas até o momento. O malware foi identificado pelos especialistas da empresa russa durante uma investigação realizada para a International Telecommunication Union (ITU).

O programa malicioso, chamado de Worm.Win32.Flame pela companhia, é projetado para realizar espionagem virtual. Ele pode roubar informações valiosas, incluído, mas não limitado a, conteúdos de um computador, informações em sistemas específicos, dados de contatos e até conversas em áudio.

A pesquisa foi iniciada pela ITU e pela Kaspersky depois de uma série de incidentes com outro malware destrutivo, e ainda desconhecido,– apelidado de Wiper – responsável por apagar dados de um elevado número de computadores na região do Oriente Médio (veja mapa). As pesquisas sobre este malware ainda não foram concluídas. Porém, durante sua análise, os especialistas, em conjunto com a ITU, depararam-se com o novo malware, conhecido agora como Flame.



Países mais atingidos pelo vírus Flame

Resultados preliminares indicam que este programa malicioso está sendo disseminado há mais de dois anos, desde meados março de 2010. Devido à extrema complexidade, além da natureza de seus alvos, nenhum software de segurança tinha conseguido detectá-lo até agora, diz a empresa.

Embora as características do Flame diferem das primeiras ciberarmas, como o Stuxnet e o Duqu, a geografia dos ataques, o uso de vulnerabilidades em softwares específicos e o fato de que só computadores selecionados serem atacados indicam que este malware pertence à mesma categoria de "super-ciberarmas".

"O Stuxnet e o Duqu pertenciam a uma única cadeia de ataques, o que levantou preocupações relacionadas com a guerra cibernética no mundo inteiro. O malware Flame parece ser uma nova fase nesta guerra e é importante entender que as armas cibernéticas podem facilmente serem usadas contra qualquer país. Neste caso, ao contrário da guerra convencional, os países

mais desenvolvidos são realmente os mais vulneráveis", afirmou Eugene Kaspersky, CEO e co-fundador da Kaspersky Lab, sobre a descoberta do Flame.

O objetivo principal do Flame parece ser a ciberespionagem, roubando informações das máquinas infectadas. As informações então são enviadas para uma rede de servidores de comando e controle localizados em diferentes partes do mundo.

A diversidade das informações roubadas, que incluem documentos, imagens, gravações em áudio e interceptação de tráfego de rede, torna-o o kit de ataque mais avançado e complexo já descoberto. O exato vetor da infecção ainda não foi revelado, mas já está claro que o Flame tem a capacidade de se replicar numa rede local usando vários métodos, incluindo os mesmos métodos explorados pelo Stuxnet, explorando vulnerabilidades no serviço de impressão e de dispositivos USB.

"Os resultados preliminares da pesquisa, pedida com urgência pela ITU, confirmam a natureza altamente direcionada deste programa malicioso. Um dos fatos mais alarmantes é que este ciberataque está no auge da sua fase ativa e seu criador está vigiando constantemente os sistemas infectados, recolhendo informações e definindo novos sistemas para atingir os seus objetivos, ainda desconhecidos", explica Alexander Gostev, analista-chefe da Kaspersky.

Por enquanto, o que se sabe é que este malware é composto por vários módulos e vários megabytes de códigos executáveis – o que o faz cerca de 20 vezes maior do que o Stuxnet. Isto significa que analisar e reverter esta arma exige uma grande equipe de especialistas e engenheiros altamente qualificados e com vasta experiência em ciberdefesa.

Fonte: IDG Now. [Portal]. Disponível em: <http://idgnow.uol.com.br/internet/2012/05/28/supervirus-espiao-e-o-mais-complexo-ja-descoberto/>. Acesso em: 29 maio 2012.