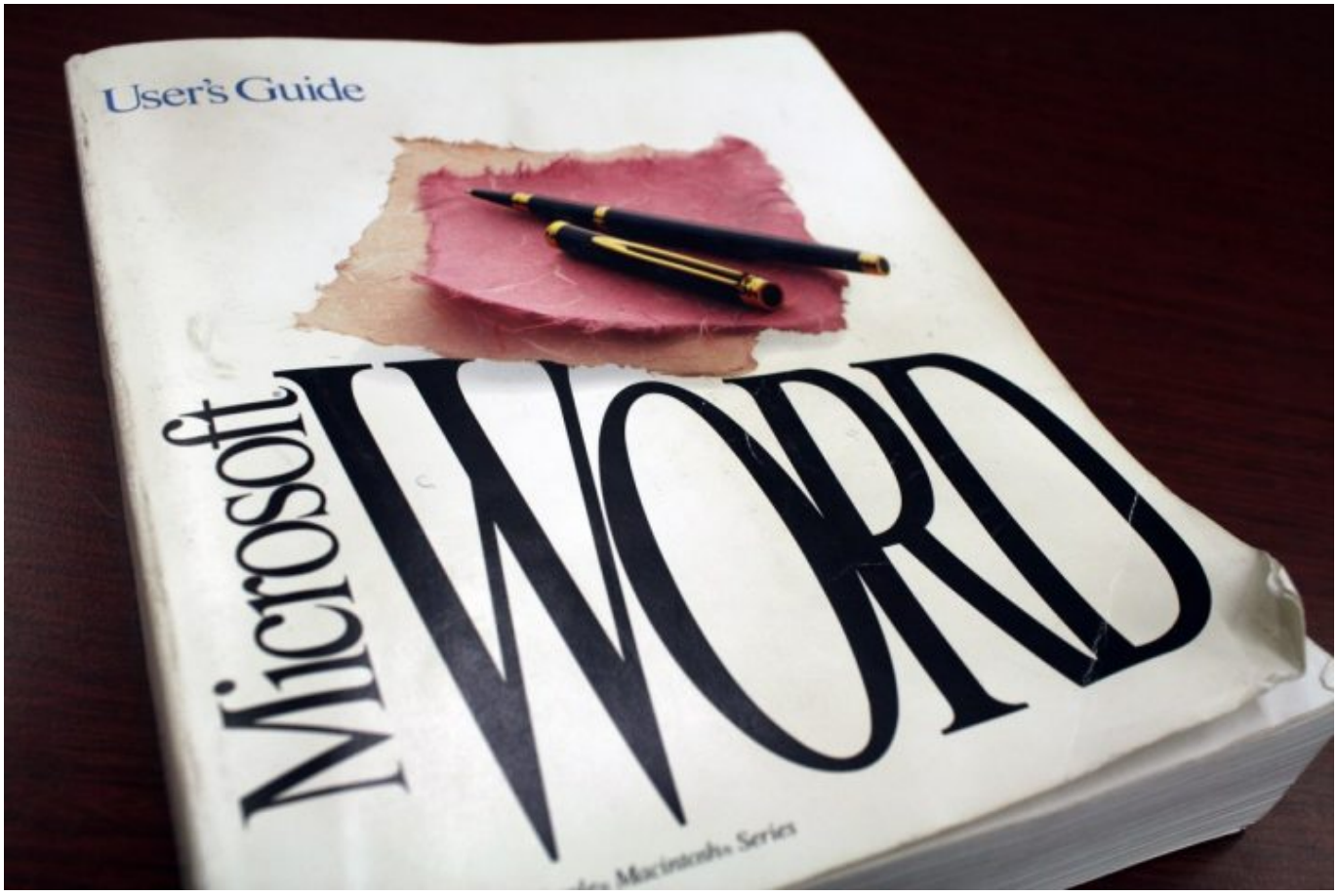
Hackers russos estão a usar Office para comprometer segurança

Date : 14 de Novembro de 2017

A segurança digital é um dos assuntos mais pertinentes junto dos utilizadores. Tendo em conta a quantidade e a profundidade da informação que estes dispõem e armazenam nos seus aparelhos eletrónicos, é essencial ter estes dados bem protegidos e salvaguardados.

Contudo, as brechas de segurança são uma realidade constante. Uma das mais recentes ocorreu proveniente de um grupo de hackers russos que estão a usar fragilidades em protocolos acoplados ao Office para atacar e espiar computadores Windows.



O grupo Fancy Bear é conhecido por ser um grupo de hackers russos que aparentemente esteve envolvido na polémica das eleições presidenciais americanas de há um ano.

Este mesmo grupo tem explorado fragilidades em protocolos usados no Office e com isto têm conseguido espiar e comprometer a segurança de vários utilizadores de equipamentos Windows.

O ataque consiste em usar o protocolo Dynamic Data Exchange (DDE) para inserir malware no computador e desta forma conseguir espiar e controlar o equipamento. O DDE é um protocolo acoplado ao Office que permite que este comunique e partilhe dados com outras aplicações instaladas no computador.

O procedimento que os hackers estão a realizar foca-se em, usando o e-mail, enviar um ficheiro .docx (Word) que contém uma ligação para um site onde será transferido o malware Seduploader e instalado no computador da vítima. O DDE é a arma que estão a usar para conectar o ficheiro com o esse site. Este tipo de manipulação usando o DDE não é propriamente recente mas ultimamente tem-se registado um crescente de casos reportados.

A Microsoft entretanto já reagiu ao sucedido e, em comunicado, expôs algumas técnicas e cuidados para os utilizadores evitarem cair neste tipo de dolos. A primeira advertência refere para os utilizadores terem cautela com a proveniência de documentos que transferem para os seus equipamentos.

Para além disso, nestes casos de ligações acopladas ao DDE, o Office apresenta uma mensagem de aviso para garantir que o utilizador tem consciência da proveniência do ficheiro e das implicações que este tipo de ligações podem causar no computador. O utilizador terá de autorizar a ligação nestas notificações, caso contrário esta não será feita.

Não ficando por aqui, a Microsoft acrescentou ainda técnicas para que os utilizadores possam desativar completamente a funcionalidade do protocolo DDE e outras técnicas mais elaboradas para lidar com o problema.

Não obstante, a Microsoft deixou a sua recomendação mais relevante: o mais importante nestes casos é ter sempre tudo atualizado para a versão mais recente, estando a referir-se ao sistema operativo e a todo o software.

Deste modo, violações e ameaças de segurança como esta poderão ser evitadas e prevenidas, se entretanto for erradicada pelo desenvolvedor.