Protege o teu PC contra ameaças online!

Em Novembro de 2014, a Symantec revelou que foi descoberto um código malicioso utilizado para espiar computadores em todo o mundo, designado por Regin. A equipa conclui que o Regin foi criado por uma entidade governamental há mais de 5 anos para espiar vários países. Este *malware* permitia tirar *printscreens* ao ecrã, roubar *passwords* ou recuperar ficheiros apagados.
É importante que saibas mais sobre estas ameaças e que aprendas a defender-te delas.
Os vírus são um tipo de *malware*, tal como o *spyware*, *adware*, *scareware* e *ransomware*. Um *spyware* regista a atividade do utilizador sem o seu conhecimento, reenviando-a ao criador. Um *adware* é uma aplicação que bombardeia o utilizador com publicidade. Um *scareware* faz o utilizador acreditar que o seu PC está contaminado por um vírus, permitindo assim a execução de um programa inútil ou com *malware*. E um *ransomware* limita as funcionalidades do sistema operativo ou o acesso a determinados ficheiros, pedindo um resgate pela reposição do sistema.

Já ouviste falar sobre estes vírus?

ILOVEYOU – Assumia o formato de anexo de e-mail com a mensagem "uma mensagem do teu admirador secreto". Ao ser aberto o anexo, o vírus era copiado para várias pastas do computador da vítima, substituía programas existentes e descarregava uma ferramenta de spyware (que reenviava informação pessoal e privada das vítimas para o cibercriminosos);

KLEZ VIRUS - Infetava computadores através de e-mail, replicando-se pela lista de contactos. Dentro do vírus, estavam contidos uma série de malwares que podiam tornar um computador inoperável;

Code Red I e II – Um computador infetado com este vírus, deixava de responder à vítima. Ao ser ativado criava uma porta no sistema que permitia o acesso remoto ao computador. Os cibercriminosos podiam aceder aos ficheiros das vítimas ou utilizar o computador para realizar crimes;

Leap-A/Oompa-A – Este vírus para Mac, propagava-se através do iChat. A vítima que descarregasse um ficheiro no formato .jpg, ativava o vírus que enviava uma mensagem automática para todas as pessoas da lista, contendo o mesmo ficheiro;

Storm Worm – Este cavalo de troia tinha várias versões. Algumas das versões tornavam os computadores em bots – PC's que quando ficavam infetados, podem ser utilizados via acesso remoto pelo responsável do ataque. O vírus era publicitado através de vários links falsos para outros serviços.

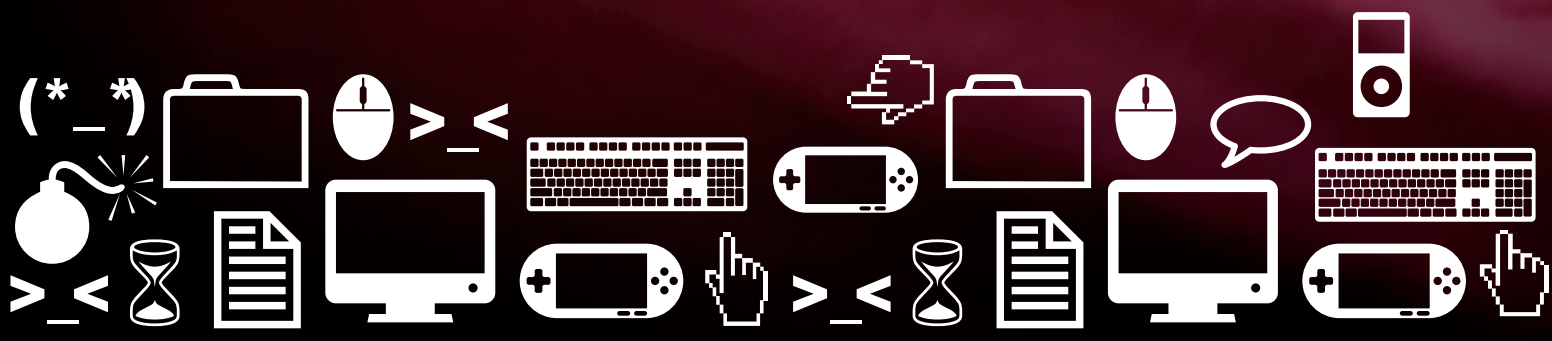
Pode ser mentira!

Como se não bastassem os *malwares*, também tens de te preocupar com boatos de vírus. Estes vírus ou não existem ou não são perigosos. Em vez disso, os criadores destes boatos pretendem que as pessoas e os media divulguem a sua existência. Isto pode ter uma consequência negativa (lembra-te da história do Pedro e do Lobo). Boatos desses podem fazer com que as pessoas ignorem avisos sobre ameaças reais.

Protege-te das ameaças!

Dificilmente vais estar 100% protegido. Mas as hipóteses do teu computador ser contaminado serão muito reduzidas se seguires estes passos:

1) Atualiza regularmente o teu sistema operativo. Se possível ativa as atualizações automáticas;



2) Instala e atualiza frequentemente o antivírus. Nunca utilizes mais que um pacote (suites) de antivírus - múltiplos antivírus podem interferir com o funcionamento do sistema;
3) Não instales *softwares* de websites pouco confiáveis, nem abras anexos suspeitos (com executáveis, ou cujo remetente desconheças);
4) Mantém uma cópia de segurança (backup) atualizada dos teus dados. Pode vir a ser necessária;

Acho que tenho um vírus... O que faço?

Depende do vírus. Muitos antivírus conseguem remover um vírus de um sistema. No entanto, se o vírus danificar os teus ficheiros, terás de os restaurar através de backups. É muito importante realizares regularmente cópias de segurança. Com um vírus como o Code Red, é uma boa ideia formatar completamente o disco rígido e começar de novo. Alguns vírus abrem portas para que outros *softwares* maliciosos sejam carregados na tua máquina e uma simples análise de antivírus não é suficiente.

Não te estás a esquecer do telefone, certo?

O tablet e o smartphone não só estão vulneráveis a *malwares, como* contam com muito menos defesas que um PC normal. Deverás, por isso, aplicar os mesmos cuidados que tens com o teu PC, no teu telemóvel.
A maior parte dos *malwares* existentes para estes dispositivos envolvem o roubo de informação, SPAM e adesão a serviços de valor acrescentado. Para evitares estes perigos, descarrega aplicações dos mercados oficiais e utiliza uma aplicação antivírus credível. Se tiveres dúvidas sobre qual escolheres, contacta-nos!