1992: Histeria e Virus Machines

O ano de 1992 foi marcado por uma crise histérica. Se tornou evidente que a população pouco conhecia a respeito de vírus e que a mídia adorava alimentar o pânico a incentivar o bom senso. Um vírus descoberto em 1991 tinha se mantido obscuro até então. Seu payload podia apagar o disco rígido. A data de gatilho dele era 6 de Março, o dia do nascimento de Michelangelo. O nome pegou.

Em Janeiro de 1992, um grande fabricante de computadores anunciou que havia despachado 500 PCs contaminados com o vírus. Poucos dias depois outra empresa admitia que acidentalmente havia distribuído 900 disquetes infectados. Era o início de uma campanha histérica que ficaria na história dos vírus. A mídia divulgava a afirmação de que 5 milhões de computadores pelo mundo poderiam cair vítimas do Michelangelo. Os departamentos de marketing das empresas de antivírus tomavam suas providências a fim de captar a atenção da mídia e, oportunamente, promoviam a empresa distribuindo gratuitamente softwares de detecção.

Muitos pesquisadores tentavam desfazer a histeria, mas a mídia simplesmente não dava ouvidos. O pânico percorreu o mundo e as histórias sobre o Michelangelo raramente questionavam as astronômicas estimativas, algumas afirmando que um de cada quatro PCs existentes no mundo cairiam sob o ataque do Michelangelo.

Finalmente, quando o "dia-M" chegou, os cálculos divulgados indicavam que cerca de 10.000 a 20.000 computadores (5.000 a 10.000, segundo um especialista famoso) e não 5 milhões haviam sido vítimas do vírus. O Michelangelo havia se tornado um grande fiasco de alcance mundial. Durante dias não se falou mais sobre vírus na mídia e o fato abalou a reputação dos especialistas (aos quais se creditavam as afirmações e estatísticas alarmantes) e prejudicou o crédito daqueles que tentavam implantar estratégias de defesa contra os vírus.

Também em 1992, foram encontrados os primeiros pacotes destinados à autores de vírus. O VCL - **V**irus **C**reation **L**aboratory de Nowhere Man (do grupo NUKE) e a Dark Angel's Phalcon/Skism Mass-Produced Code Generator foram descobertos em Agosto. Esses pacotes eram "vírus machines" que permitiam a qualquer um que utilizasse computadores produzisse um vírus.

É claro, dúzias de vírus surgiram fabricados por essas máquinas. O próximo passo seria aperfeiçoar tais máquinas para que produzissem vírus realmente polimórficos, eficazes contra a detecção.

Um novo grupo de autores de vírus surgiu em 1993, na Holanda. Chamava-se Trident e o principal autor do grupo, Masouf Khafir produziu o Trident Polimorphic Engine e lançou um vírus utilizando-a, chamado Girafe. Ao contrário de uma polimorfic engine de Dark Avenger, a MtE, o TPE era muito mais difícil de se detectar. Nowhere Man, do NUKE lançou o Nuke Encryption Engine e Phalcon/Skism, da Dark Angel lançaram o DAME - **D**ark **A**ngel's **M**ultiple **E**ncryptor.

A Trident lançou a versão 1.4 do TPE, ainda mais difícil de detectar que a anterior, e em 1993 surgiu um vírus altamente polimórfico, chamado Tremor e, Lucifer Messiah, da Anarkick System lançou o PoetCode, usando a versão 1.4 do TPE.

A fácil produção de vírus e sobretudo de vírus polimórficos ia de encontro com a falta de especialistas de nível para desmontar um vírus e descobrir formas de detectá-lo. De certa forma, as crescentes facilidades em se criar vírus fazia com que a quantidade de vírus novos aumentasse mais do que a capacidade de analisá-los. E a possibilidade de se criar vírus polimórficos diferentes em larga escala dificultava ainda mais a capacidade de resposta dos produtores de antivírus em atender a demanda. Os vírus furtivos tentam enganar os checksummers, de forma que alterações nos arquivos não se tornem aparentes. Mas os vírus polimórficos visam os próprios scanners de vírus, de forma a inutilizar a pesquisa por strings. Detectar tais vírus implica em desenvolvimento de algoritmos de detecção, mais complexos do que a pesquisa de strings de detecção e, além disso, alarmes falsos são problemáticos no caso dos vírus polimórficos. Scanners buscando vírus polimórficos podiam acabar indicando alguns arquivos inocentes como suspeitos.