VÍRUS

LUCAS VINICIUS DIETZ

RESUMO: Com a atual organização global utilizamos a tecnologia em diversas formas no nosso dia a dia, principalmente através de redes sociais, desse modo estamos suscetíveis aos vírus, que atingem e modificam o funcionamento de nossas máquinas, com este artigo busca-se explanar sobre a história desses, o que são, e como podemos proceder quando um destes atingir algum dispositivo.

PALAVRAS-CHAVE: vírus, antivírus, computador.

ABSTRACT: With the current global organization we use technology in various forms in our daily life, mainly through social networks, thus we are susceptible to viruses, which affect and modify the operation of our machines, this article seeks to explain about history what they are, and how we can proceed when one reaches some device.

KEY WORDS: virus, antivirus, computer.

INTRODUÇÃO

Segundo Santos e Camargo (2013), estamos inseridos em um contexto moderno e dependente de computadores, e em meio a isso os vírus de computador e suas demais variáveis representam uma ameaça real onde todos de maneira direta ou indireta estão suscetíveis.

Com este trabalho objetiva-se fazer um breve apanhado sobre a história dos vírus de computadores, smartphones, tablets entre outros dispositivos eletrônicos, as maneiras como se apresentam e os meios utilizados para se proteger destes.

1.0 Vírus e principais acontecimentos ao longo da história

Desde que a primeira linha de código começou a rodar, milhões de vírus, códigos maliciosos e táticas hackers surgiram para roubar dados valiosos ou prejudicar indivíduos e negócios.

Em 1982, Rich Skrenta, um programador de 15 anos criou o primeiro código malicioso, para Apple 2 em DOS, não fazia mal algum, mas a um certo número de execuções ele exibia uma poesia criado pelo autor.

Ainda em 1983, houve o pesquisador Fred Cohen, que deu o nome a programas com códigos nocivos aos computador, de “Vírus de computador”, ainda nesse ano Len Eidelmen demonstrou em um seminário um programa que se replicava em vários locais do sistema. Em 1984 na 7th Annual Information Security Conference, o termo vírus passou para programa que infecta outros programas e os modifica para produzir novas cópias de si mesmo. Já em 1986 teve sim o primeiro vírus considerado, chamado Brain, que era um vírus de boot, danificava o setor de inicialização do disco rígido, se propagava através de disquetes contaminados. Foi elaborado pelos irmãos Basit e Amjad. A falha utilizada é que os endereços da memória eram físicos, então alterar o bloco que inicia o boot era simples. No ano seguinte foi criado o vírus Vienna, a cada execução ele infectava arquivos com extensão COM. Aumentavam o tamanho do executável em 684 bytes, os programas não tinham uma cópia dele só eram alterados. Foi criado o ThusFix queneutralizava o Vienna, não foi considerado um antivírus e sim somente uma correção

No sistema operacional Windows os vírus de pendrive se utilizam do arquivo autorun.inf para se autoexecutar e infectar a máquina. Sua limpeza é simples, existem alguns antivírus que alteram o conteúdo do autorun e tiram a permissão de gravação do arquivo, e alguns usuários criam um diretório com o nome autorun.inf e isso impede de criar o tal arquivo. Os vírus em si funcionam de forma interessante, temos por exemplo o conficker que após infectar o PC ele passa a infectar todo pendrive que nele for utilizado, assim como enquanto conectado a internet ele baixa diversos outros vírus e com isso acaba com o sistema e arquivos do usuário. Sua prevenção é simples e sua remoção é complicada. Ou seja se todos fossem informados de como o vírus funciona a prevenção seria óbvia e este tipo de vírus seria obsoleto.

Os vírus de macro são utilizados dentro de, aparentemente, inofensivos arquivos estilo "office" são scripts executados automaticamente para facilitar a visualização dos arquivos e fazer eles executarem o que teriam de executar, os criadores de vírus aproveitam que macros tem poder de execução e infectam os arquivos colocando dentre a macro código malicioso que o usuário previamente nem notará, e após execução do arquivo já estará infectado e infectará outros. A maior praga disso esta nas apresentações de slides, como foi muito difundido por e-mails para passar imagens.

Há também os vírus polimórficos, porém, ainda não existe uma forma eficaz para se detectar este tipo de vírus, eles não tem um padrão a ser identificado. O que se faz é criar um arquivo de vitima e este fica sempre sendo monitorado, mas o bom vírus polimórfico já está residente em memória e faz o sistema "ver"o arquivo como inalterado e com isso não há mais nada a ser feito. Seria uma limpeza manual, sem o auxilio de outra maquina seria inviável, enquanto o vírus se infecta o usuário tentaria localizá-lo e deletá-lo numa guerra perdida

O Brasil é o quarto pais com maior incidência de crimes de internet, sendo também um dos que está entre os que possuem maior prejuízo com esses crimes, somente em 2012, 28 milhões de pessoas foram vitimas, o que causou um prejuízo de 15 bilhões de reais. O que vem aumentando esses casos é o acesso cada vez maior da população à internet, principalmente por meio de smartphones e tablets, aos jovens tem utilizado cada vez mais as redes sociais, como o facebook que se tornou popular entre os usuários iniciantes o que os torna as principais vitimas pelo fato de não terem utilizado a tecnologia antes e não estarem familiarizados com vírus, worms, phishing entre outros. (SANTOS E CAMARGO, 2013).

Os autores relatam ainda que quase metade dos usuários não possuem o conhecimento de que um vírus pode passar despercebido sem causar danos aparentes ao sistema fazendo com que o usuário não perceba o vírus em seu aparelho, e não perceberiam o problema sem que o computador parasse ou ficasse mais lento, e mais da metade não tem certeza se seu computador está livre ou não de um vírus, há ainda aqueles que não compreendem o que é um vírus e que acreditam que não serão prejudicados por isso.

Em 1986 ocorreu a primeira “epidemia” cibernética para o PC da IBM, o Brain,. O malware foi criado por desenvolvedores do Paquistão como um esquema de gestão de direitos digitais que não deu certo, e acabou destruindo uma série de HDs, exigindo a formatação e a reinstalação completa de inúmeras máquinas.

Pouco tempo depois os hackers passaram a usar esses “precursores” e outros códigos maliciosos por shareware disponibilizados em sistemas BBS, onde vítimas buscaram softwares, aplicativos e informações.

Quando descobriam que o conteúdo que tinham baixado era, na verdade, um vírus, já não havia nada a ser feito além de remover além de formatar seus sistemas e começar do zero.

Em 1987, a infecção cibernética mais comum era conhecida como STONED Virus, que resultou em uma praga de diferentes variantes que diferiam apenas na mensagem exibida na tela da vítima.

O STONED e suas variantes tinham um nível mais elevado de sofisticação, pois usavam uma tecnologia chamada Terminate, Stay Resident (TSR), ou memória de vírus, que permitia a ele infectar qualquer disco próximo da máquina, mesmo que seus arquivos digitais fossem deletados.

Em 1989, os danos causados por malwares já não se restringiam “incômodos”. Eles já eram capazes de causar danos significativos aos dados e às máquinas de ambientes corporativos e domésticos. Após o surgimento do STONED Virus, um grupo chamado Virus-L passou a ser usado para atualizar indivíduos sobre segurança, com o compartilhamento de informações, ferramentas e shareware para remover infecções.

Entre os indivíduos que faziam parte do grupo estavam John McAfee e Eugene Kaspersky. Em 1989, McAfee deu início ao seu próprio negócio vendendo soluções para proteger hardwares e softwares. Foi neste momento que a história do antivírus começou e essa ferramenta ganhou cada vez mais importância.

Quando se ouve falar em código polimórfico, a primeira associação que se faz é com vírus de computador. No entanto, existem diversas aplicações legais do código polimórfico.Empresas que desenvolvem código de proteção contra cópia ilegal de software usam código polimórfico para dificultar a engenharia

reversa do software de proteção e do software protegido visando inibir a ação de crackers que criam patches para fazer com que o software pense que está registrado legalmente[2, 4]. Atualmente, todas as empresas de proteção contra cópia usam polimorfismo juntamente com compactação de dados e técnicas anti-debugging para proteger o software. Alguns usam também códigos metamórficos. O código metamórfico difere do polimórfico por usar técnicas de recompilação/reconstrução fazendo com que cada versão seja única não somente na aparência mas também no código binário executável.

Outro uso legal do código polimórfico seria para gerar uma marca digital do software, pois cada versão seria única tornando possível assim dizer quem é o dono da versão que está em circulação no caso de haver alguma cópia ilegal. A indústria fonográfica já usa algo semelhante a isso nas músicas com a finalidade de descobrir quem disponibilizou cópias ilegais. O mais importante é que esta medida não altera em nada a qualidade do áudio, passando totalmente despercebida pelo usuário. Também é usado este artifício em máquinas fotográficas e dispositivos de gravação. Cada dispositivo possui sua marca digital única fazendo assim sua ’assinatura’ em cada foto ou filme produzidos pelo dispositivo.

Um código polimórfico exige no mínimo duas partes: a rotina de encriptação e a rotina de decriptação. A criptografia pode ser algo super simples ou algo muito complexo.

2.0 Antivírus

A história do antivírus foi essencial para a cibersegurança, pois a ferramenta automatizou o processo de remover malwares, garantindo ainda que a máquina poderia retornar ao seu funcionamento normal, sem precisar de formatação e reinstalação de sistemas.

O departamento de TI que passava horas tentando eliminar uma infecção que podia se espalhar por toda a rede e depois tinha de começar tudo “do zero”, viu seu modo de trabalho mudar com os antivírus, pois a partir disso bastava abrir um arquivo, checar se havia indícios de que ele estava infectado e, se necessário, checar a base de dados de assinatura.

Uma assinatura era formada de algum texto ou outra parte do malware para identificar o que havia sido detectado, junto do tamanho, em que o número

exibido era o tamanho em bytes do fim do arquivo que continha o vírus em questão.

Hoje os antivírus são parte essencial de qualquer estratégia de segurança, mesmo que sua empresa conte com múltiplas camadas de softwares modernos de proteção. Os antivírus atuam checando cada arquivo aberto na máquina. Toda vez que abrimos um arquivo executável, o antivírus faz uma checagem para compará-lo com vírus, worms e outros tipos de malware conhecidos. Ele também é capaz de chegar programas em busca de comportamentos prejudiciais que indiquem algum vírus desconhecido.

CONSIDERAÇÕES FINAIS

Com a realização deste trabalho foi possível expandir o conhecimento à cerca dos vírus, as maneiras como se apresentam, e como evitar os mesmos, e quando necessário o que fazer quando uma máquina for infectada.

REFERÊNCIAS

http://www.proof.com.br/blog/historia-antivirus/ <acesso em 20 de novembro de 2014>

SANTOS, Loirto Alves dos. CAMARGO, Luis Henrique Pires de. **Vírus de computador Uma abordagem do código polimórfico.** Curitiba, 2013.