53GUR4NC4 D4 INFORM4C40

M4LW4R3

J1y4n y4R1

M4LV4R3

MalWare = Malicious software

Código que infiltra em um sistema computacional de forma ilícita para causar danos, alterações ou roubo de informações (confidenciais ou não).

0000 0100

M4LV4R3

- Vírus
- Worm
- trojan (cavalo de Tróia)
- Spyware
- Adware
- Backdoor
- Keylogger
- Screenlogger
- Exploit
- Sniffer
- bot (botnet)
- Rootkit
- Etc.

0000 0100

M4LV4R3

Vírus

Programa de computador malicioso que se propaga via infecção;

Se replica e insere cópias de si mesmo se tornando parte de outros programas e arquivos de um computador;

Depende da execução do arquivos hospedeiros para que possa se tornar ativo e continuar o processo de infecção;

Geralmente altera e ou danifica arquivos, algumas vezes de forma devastadora e definitiva

M4LV4R3

O início ...

Caso McFee Lookhead - extra-oficialmente o primeiro vírus (1980);

Criado por um programador "paquistanês" que prestava serviço à empresa McFee Lookheed (aviação);

A empresa negou-se a pagar um serviço (software), então ele resolveu criar e enviar um código final;

Esse código na realidade era um malware e "contaminou" o sistema;

O programado exigiu então que se pagasse um valor para que ele removesse o malware;

A empresa se negou e contratou profissionais (John McAfee) para remover o malware – surgia então o primeiro anti-vírus (1987)!

PR1NC1P415 V1RU5

- Elk Cloner
- considerado o primeiro vírus;
- criado por Rich Skrenta, de 15 anos, em 1982;
- atacava computadores Apple 2 com MS-DOS;
- exibia um "poema" a cada cinquenta vezes que o computador era iniciado com um disquete infectado:

```
Elk Cloner:
The program with a personality

     It will get on all your disks
       It will infiltrate your chips
         Yes it's Cloner!

     It will stick to you like glue
       It will modify ram too
         Send in the Cloner!
```

PR1NC1P415 V1RU5

- Brain
- Considerado o primeiro vírus conhecido;
- Detectado pela primeira vez em janeiro de 1986;
- Executava no MS-DOS;
- O seu código fornecia o endereço e o telefone de contato dos seus desenvolvedores (Paquistaneses):

> Welcome to the Dungeon © 1986 Basit * Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination...

0000 0100

PR1NC1P415 V1RU5

Brain

Os desenvolvedores "alegaram" que criaram o programa para monitorar a distribuição de cópias piratas de um software médico de monitoramento cardíaco que haviam desenvolvido para o computador da Apple Inc.;

O código foi portado por outro programador para o sistema operacional MS-DOS, tornando-se um vírus;

A companhia foi alvo de ações judiciais e foi fechada;

O vírus se espalhava por disquetes e causava lentidão na operação dos discos;

Ocupava "preciosos" kilobytes de memória do MSDOS.

0000 0100

PR1NC1P415 V1RU5

Brain

Os desenvolvedores "alegaram" que criaram o programa para monitorar a distribuição de cópias piratas de um software médico de monitoramento cardíaco que haviam desenvolvido para o computador da Apple Inc.;

O código foi portado por outro programador para o sistema operacional MS-DOS, tornando-se um vírus;

A companhia foi alvo de ações judiciais e foi fechada;

O vírus se espalhava por disquetes e causava lentidão na operação dos discos;

Ocupava "preciosos" kilobytes de memória do MSDOS.

0000 0100

PR1NC1P415 V1RU5

Vírus de boot

- foi um dos primeiros tipos a surgirem no mundo;

- se alojava no primeiro setor do disquete e ocupavam cerca de 1k; - surgiu nos disquetes flexíveis de 5 ¼ de 360k, em 1988;

- na memória alojava-se no endereço 0000:7C00h do Bios, e quando o boot ocorria, o vírus se transferia para este endereço e depois se auto-executava;

- os principais virus de boot foram:

  - Ping-Pong;

  - Stoned;

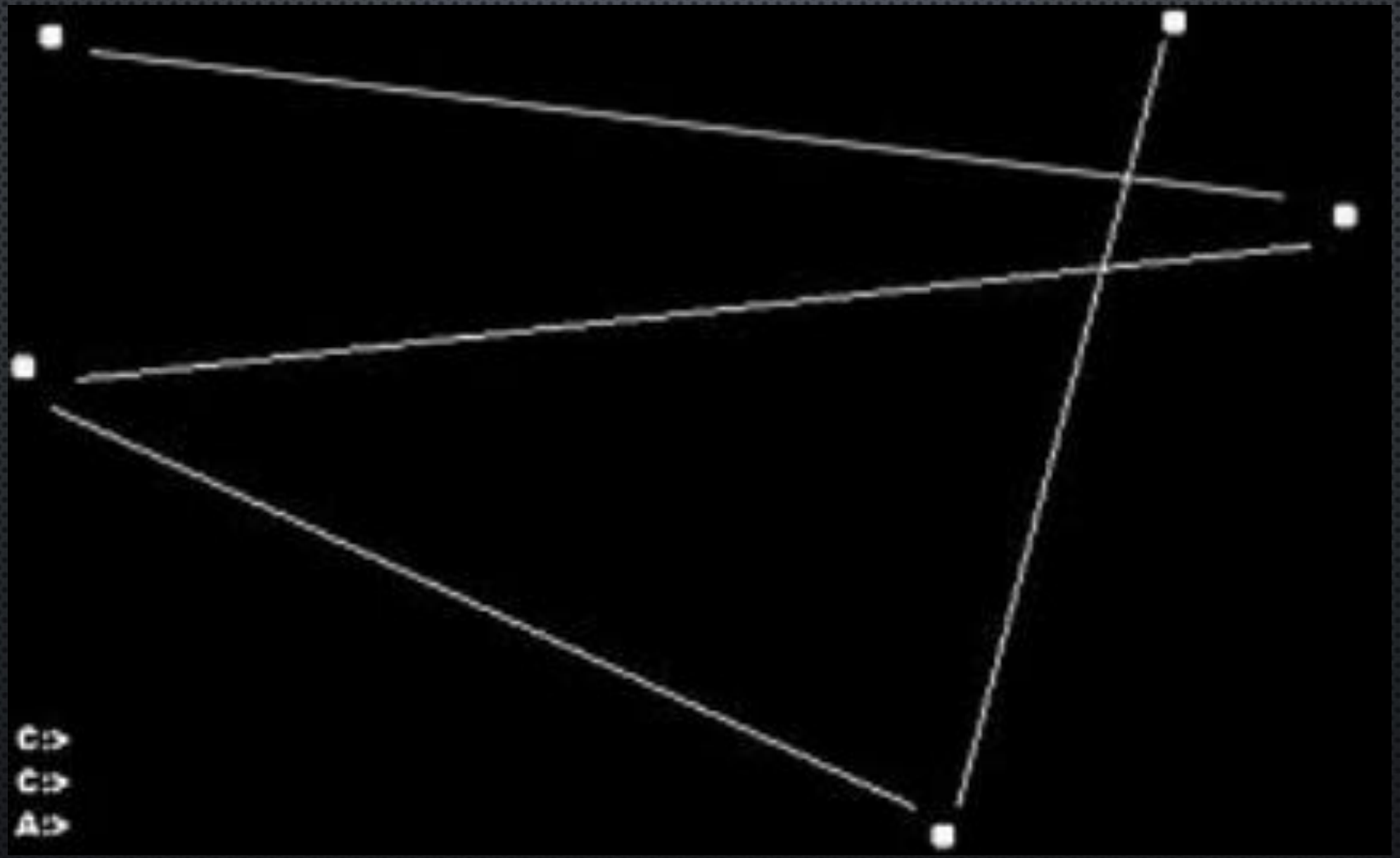
  - Jerusalem (Versão Boot).

PR1NC1P415 V1RU5

Ping Pong

- primeiro vírus a surgir com impacto no Brasil;
- afetava o Sistema Operacional MS-DOS/PC-DOS;
- se instalava na Interrupção 8 do BIOS do PC, seguindo o tick do relógio do PC;
- "pulava" de um lado para o outro na tela;
- também conhecido como Bouncing Ball ou Bouncing Dot.

0000 0100


C>
C>
A>

PR1NC1P415 V1RU5

STONED

- ANTES DA INTERNET, OS VÍRUS SE ESPALHAVAM PRINCIPALMENTE VIA DISQUETES;
- UM DOS PRIMEIROS A SURGIR EM 1987 E ERA CONHECIDO COMO STONED;
- O USUÁRIO INFECTADO RECEBIA A SEGUINTE MENSAGEM NA TELA:

"SEU COMPUTADOR ESTÁ AGORA SENDO APEDREJADO"

- DIVERSAS VARIANTES DELE FORAM CRIADOS, DANDO INÍCIO À PRÁTICA DOS HACKERS DE ATUALIZAREM O CÓDIGO DE UM VÍRUS EXISTENTE PARA CRIAR OUTROS.

0000 0100


Award Modular BIOS v6.00PG, An Energy Star Ally
Copyright (C) 1984-2007, Award Software, Inc.
Intel P35 BIOS for P35C-DS3R F2o
Memory Runs at Dual Channel Interleaved
Boot Disk failure. Type key to retry
Boot Disk failure. Type key to retryYour PC is now Stoned!
Non-System Disk or disk error
Replace and press any key when ready
Boot Disk failure. Type key to retry
Boot Disk failure. Type key to retry_
Your PC is now Stoned!
<DEL>:BIOS Setup/Q-Flash <F9>:XpressRecovery2 <F12>:Boot Menu <End>:Qflash
05/11/2007-P35-ICH9-6A79OG0BC-00

PRINCIPAIS VIRUS

JERUSALÉM

- SURGIU NO FINAL DE 1987;

- FOI MUITO MAIS DESTRUTIVO DO QUE O STONED, POIS INFECTAVA ARQUIVOS DOS TIPOS .EXE E .COM;

- COMO O ERA ATIVADO SEMPRE NAS SEXTAS-FEIRA 13, FICOU CONHECIDO TAMBÉM PELO NOME "SEXTA-FEIRA 13";

- SUA AÇÃO ERA MAIS LENTA COMPARADA AO STONED, MESMO ASSIM, DESTRUIU DEZENAS DE MILHARES DE PROGRAMAS DOS USUÁRIOS INFECTADOS.

PRINCIPAIS VIRUS

CONCEPT (POLIMÓRFICOS)

- OS ANOS 90 VIRAM O DESENVOLVIMENTO DE UMA SÉRIE DE NOVOS "CÓDIGOS BUGS" (QUE CAUSAM ERROS E DEFEITOS);

- SURGIRAM OS VÍRUS **POLIMÓRFICOS**, QUE PODIAM MUDAR DE FORMA A CADA NOVA INFECÇÃO, TORNANDO DIFÍCIL PARA O ANTIVÍRUS DETECTAR A PRESENÇA DA AMEAÇA;

- EM 1995 O VÍRUS CONCEPT INOVOU AO SER O PRIMEIRO A INFECTAR DOCUMENTOS DO MICROSOFT WORD;

- USUÁRIOS QUE COMPARTILHAVAM DOCUMENTOS INFECTADOS VIA E-MAIL AJUDARAM A TORNAR O VÍRUS UM DOS MAIS RÁPIDOS A SE DISSEMINAR NA ÉPOCA.

PR1NC1P415 V1RU5

CIH

- CONHECIDO COMO CHERNOBYL, FOI UM DOS VÍRUS MAIS DEVASTADORES JÁ CONHECIDOS (1988);

- DIFERENTEMENTE DOS OUTROS VÍRUS QUE CAUSAM DANOS LEVES E SÓ SE REPRODUZIAM, ESSE VÍRUS DESTRUÍA TODOS OS DADOS DO COMPUTADOR;

- SUA VERSÃO DESTRUTIVA (BRASIL) DESTRUÍA OS DADOS DA BIOS, TRANSFORMANDO QUALQUER PC EM SUCATA;

- SEU PODER DE SE PROPAGAR FOI NEUTRALIZADO COM UM UPDATE DA MICROSOFT, JÁ QUE ELE ATACAVA APENAS VERSÕES ANTIGAS DO WINDOWS, COMO O 95, 98 E MILLENIUM.

0000 0100

PR1NC1P415 V1RU5

MELISSA

- SURGIU EM MEADOS DE 1999;

- FOI O PRIMEIRO VÍRUS (WORM) PROJETADO PARA SE ESPALHAR DE COMPUTADOR PARA COMPUTADOR, SEM DEPENDER DA AÇÃO DOS USUÁRIOS;

- PARA CADA PC INFECTADO POR EMAIL, O VÍRUS IDENTIFICAVA OUTROS 50 USUÁRIOS DA LISTA DE CONTATOS DA VÍTIMA;

- O AUMENTO DO TRÁFEGO DE EMAIL FORÇOU EMPRESAS COMO A INTEL E A MICROSOFT A DESLIGAREM TEMPORARIAMENTE SEUS SERVIDORES DE EMAIL ATÉ QUE O VÍRUS FOSSE ELIMINADO.

0000 0100

PR1NC1P415 V1RU5

LOVE BUG (I LOVE YOU)

- CONSIDERADO UM DOS VÍRUS (WORM) MAIS DESTRUTIVOS QUE JÁ EXISTIRAM (2000);
- INFECTOU MAIS DE 50 MILHÕES DE COMPUTADORES EM APENAS NOVE DIAS;
- FUNCIONAVA COMO O MELISSA, USANDO O E-MAIL PARA AGIR E SE ESPALHAR PARA CONTATOS DO DESTINATÁRIO;
- ENVIAVA UMA SUPOSTA CARTA DE AMOR DE UM ADMIRADOR SECRETO ANEXADA NO E-MAIL;
- QUANDO A VÍTIMA ABRIA, O SCRIPT ANEXADO EXCLUÍA ARQUIVOS PESSOAIS E MUDAVA A PÁGINA INICIAL DO INTERNET EXPLORER;

PR1NC1P415 V1RU5

Love Bug (I Love You)

- criada nas Filipinas por um estudante deixado pela namorada;
- chegou em forma de worm
- programa independente, que faz cópias de si mesmo e os envia pela rede; - o vírus circulava pela internet por e-mail;
- o assunto da mensagem trazia uma carta de amor de um admirador secreto;
- no anexo um arquivo nomeado como:

LOVE-LETTER-FOR-YOU.TXT.vbs.

- extensão .vbs (Visual Basic Script).

0000 0100

ILOVEYOU - Message (Rich Text)

File Edit View Insert Format Tools Actions Table Help

Reply Reply to All Forward

From: John Doe Sent: Thu 5/4/00 11:29 AM

To: John Doe

Cc:

Subject: ILOVEYOU

kindly check the attached LOVELETTER

LOVE-LETTER-FOR-YOU.TXT.vbs

coming from me.

PR1NC1P415 V1RU5

Anna Kournikova (Engenharia Soial)

- circulou na internet em 2001;

- inaugurou a fase de uma tática comum (engenharia social): vírus que enganavam os destinatários prometendo imagem anexada de interesse sexual;

- Foi criado por um jovem programador da Holanda que foi identificado e se entregou às autoridades.

0000 0100

PR1NC1P415 V1RU5

Leap-A/Oompa-A

- atacava usuários do Mac/Apple e MacOS, que se vangloriavam da segurança dos seus sistemas;
- surgiu em 2006 o vírus Leap ou Oompa-A;
- utilizava o programa iChat para propagar-se em Macs vulneráveis;
- enviava um arquivo corrompido maquiado por uma imagem em JPEG

WORMS

- CÓDIGO CAPAZ DE SE PROPAGAR AUTOMATICAMENTE ATRAVÉS DE REDES, ENVIANDO CÓPIAS DE SI MESMO DE COMPUTADOR PARA COMPUTADOR;

- DIFERENTE DO VÍRUS, O WORM NÃO EMBUTE CÓPIAS DE SI MESMO EM OUTROS PROGRAMAS OU ARQUIVOS E NÃO NECESSITA SER EXPLICITAMENTE EXECUTADO (AÇÃO HUMANA) PARA SE PROPAGAR;

- SUA PROPAGAÇÃO SE DÁ ATRAVÉS DA EXPLORAÇÃO DE VULNERABILIDADES EXISTENTES OU FALHAS NA CONFIGURAÇÃO DE SOFTWARES INSTALADOS EM COMPUTADORES

PR1NC1P415 WORM5

Morris

- criado "sem más intenções" por Robert Morris para medir o tamanho da Internet;

- Foi capaz de mostrar como um simples código pode se tornar uma ameaça muito perigosa;

- disseminou-se a partir do MIT em 2 de Novembro de 1988;

- tinha um "erro" que infectava o computator várias vezes e também causava um ataque de negação de serviço (DoS);

- sobrecarregava as vias de comunicação do sistema, obrigando algumas instruções a "esperarem na fila de tarefas" para após um tempo inutilizar essas tarefas (deadlock).

PRINCIPAIS WORMS

Nimda (worm) surgiu em 2001;

- tem o nome formado pelo inverso da palavra admin;
- famoso por ter sido um dos Worms mais rápidos a se propagar;
- em apenas 22 minutos que ele "estava online" e já aparecia no topo da lista de ataques virtuais;
- seu principal alvo eram os servidores, já que seu objetivo consistia em tornar a navegação mais lenta.
- foi considerado o worm mais rápido, precisando de apenas 22 minutos para entrar na Internet e se tornar o malware "mais espalhado do mundo".

0000 0100

PR1NC1P415 WORM5

Blaster

- foi criado com a intenção de atacar os sistemas Windows da Microsoft;

- além de atacar o sistema operacional, o worm continha a seguinte mensagem para a empresa:

"Billy Gates why do you make this possible? Stop making money and fix your software!!"

Tradução:

“Bill Gates por que você fez isso ser possível? Pare de fazer dinheiro e corrija seu software!!”

0000 0100

PR1NC1P415 WORM5

Sasser

- atacou várias máquinas com o Windows;

- usou uma vulnerabilidade de segurança na porta de rede, conectando-se a outras máquinas e se espalhando pela Internet;

- afetou várias empresas, como a Delta Airlines, que teve que interromper seus voos por conta da infecção;

- a Guarda Costeira da Inglaterra teve seus serviços de mapas interrompidos;

- a agência de notícias France-Press também teve as suas comunicações com os satélites interrompidas.

0000 0100

PR1NC1P415 WORM5

Code Red

- aproveitava-se de uma vunerabilidade de estouro de buffer dos servidores Microsoft IIS;
- Dessa forma se replicava para outros servidores IIS.

Buffer é uma região da memória temporária utilizada para escrever e ler dados antes deles serem guardados permanentemente

PR1NC1P415 WORM5

Code Red

- quando acontecia o estouro do buffer, o servidor desligava;

- os sites guardados nesses servidores, que foram afetados pelo worm, passavam então a exibir a mensagem “Hacked by Chinese!” ("Hackeado por Chinês", em tradução literal);

- o nome Code Red surgiu quando os pesquisadores da eEye Digital Security descobriram o worm e naquele momento estavam tomando uma bebida chamada "Code Red Mountain Dew".

PR1NC1P415 WORM5

SLAMMER

- SE APROVEITAVA DE UMA VULNERABILIDADE DE ESTOURO DE BUFFER NO MICROSOFT SQL SERVER;

- UMA VEZ INSTALADO CAUSAVA UM ATAQUE DE NEGAÇÃO DE SERVIÇO (DOS) FAZENDO COM QUE OS BANCOS DE DADOS NÃO RESPONDESSEM E CAUSASSEM GRANDE LENTIDÃO NA INTERNET.

PR1NC1P415 WORM5

SLAMMER

- SE REPLICAVA E ATACAVA TODOS OS SERVIDORES SQL SERVER QUE TINHAM A MESMA VULNERABILIDADE, CAUSANDO UM EFEITO CASCATA;
- ESTIMA-SE QUE CERCA DE 75.000 SERVIDORES FORAM AFETADOS EM APENAS 10 MINUTOS;
- FOI TÃO AGRESSIVO E RÁPIDO QUE MUITOS NA ÉPOCA PENSARAM QUE ERA UM ATAQUE COORDENADO POR UM GRUPO HACKER.

PRINCIPAIS WORMS

Storm

- teve um modo de propagação curioso: mandava e-mails com assuntos polêmicos ou sensacinalistas, como "Genocídio de muçumanos britânicos" ou "Fidel Castro faleceu";

- por ser um worm mais moderno, o Storm construíu uma verdadeira "botnet", ou seja, usava o computador infectado para realizar açÕes programadas pelo worm, como ataques a determinados sites,

Obs: os computadores infectados comunicavam-se entre si para melhorar as formas de ataque.

PRINCIPAIS WORMS

MyDoom

- surgiu em 26 janeiro de 2004;
- em quatro horas a sua ação pôde ser sentida em todo o mundo;
- se espalhou em uma velocidade sem precedentes pela Internet;
- também conhecida como Norvarg, se espalhou em um arquivo anexado que parecia ser uma mensagem de erro, com o texto:

"Mail transaction failed"

- espalhava-se pelas redes P2P via compartilhamento de arquivos entre os usuários como o Kazaa.

PR1NC1P415 WORM5

MyDoom

- sua replicação foi tão bem-sucedida que especialistas em segurança calcularam que uma em cada dez mensagens de email enviadas durante as primeiras horas da infecção continham o vírus;

- foi programado para parar de agir depois de 12 de fevereiro;

- seu auge chegou a diminuir em 10% a performance global da Internet e aumentar o tempo de carregamento dos sites em 50%.

VÍRUS/WORMS

SASSER E NETSKY

- FORAM CRIADO POR UM ALEMÃO DE 17 ANOS CHAMADO SVEN JASCHAN;

- ELE CRIOU OS DOIS PROGRAMAS (2004) QUE ATACAVAM DE FORMAS DIFERENTES, MAS POSSUÍAM CÓDIGOS MUITO SIMILARES, O QUE LEVOU AS AUTORIDADES A DESCONFIAREM QUE ERAM DO MESMO AUTOR;

- O SASSER APROVEITAVA UMA VULNERABILIDADE DO WINDOWS QUE PROCURAVA ENDEREÇOS DE IP ALEATÓRIOS EM BUSCA DE OUTRAS VÍTIMAS;

- TAMBÉM CORROMPIA O SO PARA DIFICULTAR O DESLIGAMENTO DO COMPUTADOR PARA NÃO INTERROMPER A PROLIFERAÇÃO

VIRUS/WORMS

Sasser e Netsky

- o Netsky se espalhava por meio de e-mails e redes do Windows;

- causava um ataque DoS para causar colapso no sistema que tentava responder todo o tráfego gerado;

- Sven Jaschan foi condenado a um ano e nove meses de prisão, mas cumpriu a pena em liberada condicional.

VIRUS/WORMS

STUXNET

- WORM/VÍRUS DE COMPUTADOR PROJETADO ESPECIFICAMENTE PARA ATACAR O SISTEMA OPERACIONAL SCADA (SISTEMA DESENVOLVIDO PELA SIEMENS PARA CONTROLAR AS CENTRÍFUGAS DE ENRIQUECIMENTO DE URÂNIO IRANIANAS);

- DESCOBERTO EM JUNHO DE 2010 PELA EMPRESA BIELORRUSSA DESENVOLVEDORA DE ANTIVÍRUS VIRUSBLOKADA;

- PRIMEIRO WORM DESCOBERTO QUE ESPIONA E REPROGRAMA SISTEMAS INDUSTRIAIS;

- CONSIDERADO O MARCO ZERO DA CYBERGUERRA;

- FOI ESPECIFICAMENTE ESCRITO PARA ATACAR O SCADA, SENDO CAPAZ DE REPROGRAMAR CLPS E ESCONDER AS MUDANÇAS.

VÍRUS/WORMS

Flame

- considerado o vírus/worm mais letal da história dos computadores (2012);

- atingiu uma série de computadores ao redor do Oriente Médio para espionar e sabotar órgãos governamentais e militares;

- os alvos foram: Síria, Arábia Saudita, Irã, Egito, Líbano e os territórios palestinos, que levou os especialistas a acreditar que pode ter origem nos Estados Unidos ou no Israel;

- é capaz de coletar e de deletar informações e ativar microfones de outros computadores, que mesmo desligados seriam capazes de enviar conversas.

VÍRUS/WORMS

Flame

- A complexidade desse vírus espantou as empresas de segurança, que afirmam que devido à quantidade de códigos do vírus levariam cerca de dez anos para decodificar tudo;

- Foi tão bem escrito e tão silencioso que os especialistas demoraram dois anos para descobrir a sua existência;

- Se instala através de um programa de 6MB, antes de contaminar o computador;

- Ainda ninguém conseguiu descobrir a forma real como infecta os computadores-alvo;

- A Karpesky desenvolveu uma vacina.

0000 0100

Kaspersky Lab, uno de los mayores fabricantes de antivirus del mundo, descubrió un nuevo virus informático llamado "Worm.Win32.Flame", o simplemente "Flame", el software malicioso más complejo hallado hasta la fecha.

COMPLEJIDAD

Con un tamaño de casi 20 MB y unos 20 módulos de código, "Flame" es uno de los softwares maliciosos más grandes descubiertos hasta el momento.

ALCANCE

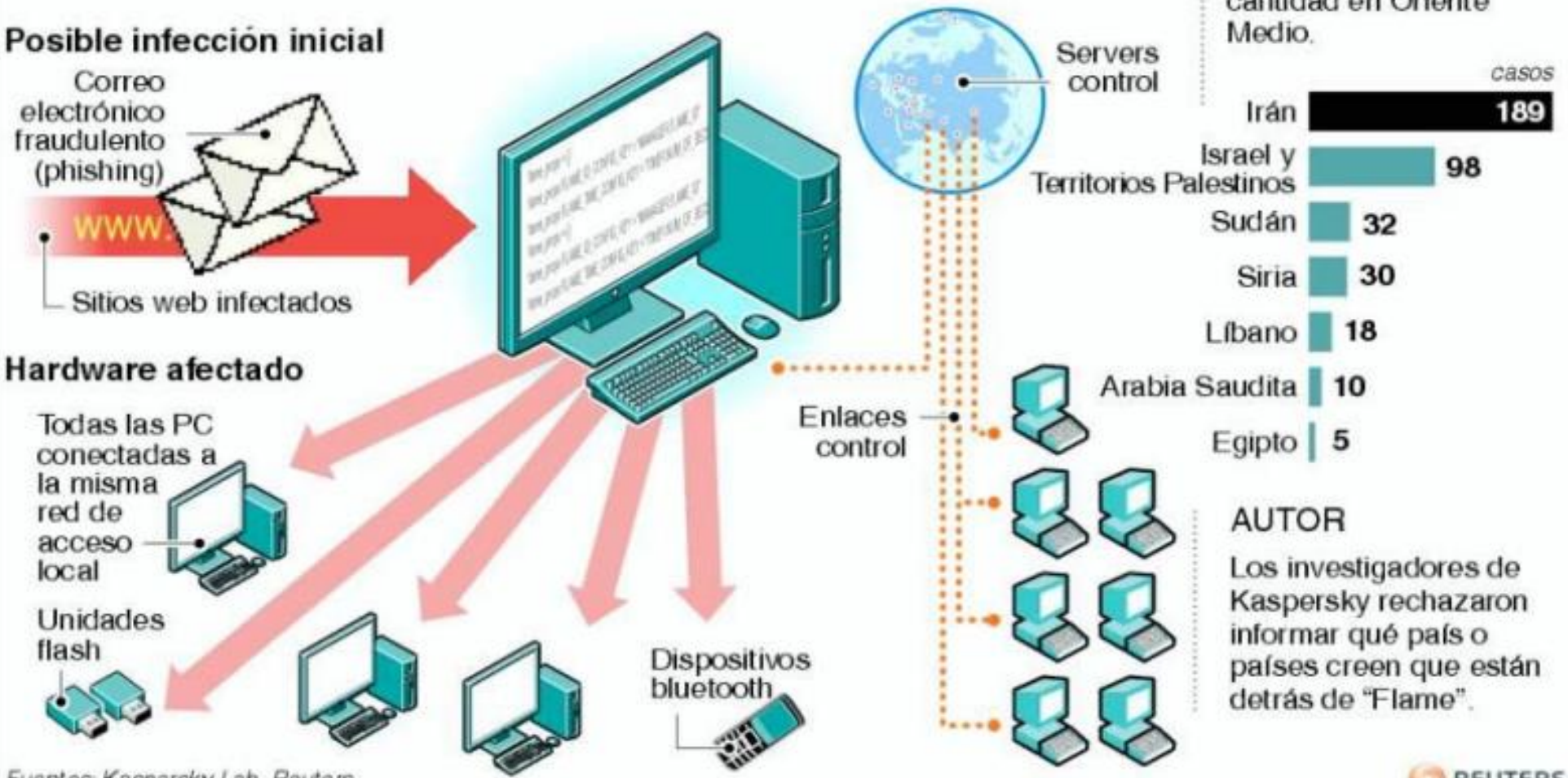
El virus puede grabar sonidos, acceder a comunicaciones bluetooth, realizar capturas de pantalla y registrar conversaciones en internet.

RED

Los creadores del virus usaron una red de unos 80 servidores a través de Asia, Europa y América del N. para controlar las máquinas infectadas a distancia.

VICTIMAS

Los investigadores estiman que un total de entre 1.000 y 5.000 máquinas están infectadas en todo el mundo, con la mayor cantidad en Oriente Medio.



AUTOR

Los investigadores de Kaspersky rechazaron informar qué país o países creen que están detrás de "Flame".

Fuentes: Kaspersky Lab, Reuters

REUTERS

```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
      __LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CH
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUE
      flame_props.BPS_KEY = "BPS"
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
```

7ROJ4N

BackDoor (Trojan backdoor)

permite que o atacante obtenha controle remoto do computador infetado.

Permite que se envie, receba, execute e delete arquivos e reiniciar o computador.

Os trojans backdoor são também podem ser utilizados para criar um grupo de computadores vitimizados de modo a formar uma rede zumbi ou botnet que possa ser utilizada para finalidades criminosas.

Alguns BackDoors famosos:

- BackOriffice;
- Brifost;
- c99Shell;
- WebShell
- RST.

0000 0100

3XPLO17

São programas que contêm dados ou código que tiram partido de uma vulnerabilidade no software do sistema operacional, serviço/servidor ou de uma aplicação em execução no computador.

ROOT KIT

São códigos que ocultam determinados arquivos ou atividades no seu sistema.

Geralmente permitem acesso ao sistema como um usuário com privilégios de administrador, como root (Linux/Unix) e Administrador (Windows).

O seu principal objetivo é evitar a detecção de programas maliciosos, de modo a prolongar o período em que os programas podem ser executados num computador infetado

5PYW4R3

São programas espiões.

Sua função é coletar informações sobre uma ou mais atividades realizadas em um computador.

Nem todo SpyWare é malicioso:

- Spyware não-prejudicial: só será instalado mediante a autorização do usuário;

- Spyware maligno: irá se instalar sem que o usuário perceba.

http://www.tecmundo.com.br/ubuntu/33888-richardstallman-chama-nova-versao-do-ubuntu-de-spyware.htm

0000 0100

5N1FF3R

Conhecida também como Packet Sniffer, Analisador de Rede, Analisador de Protocolo, Ethernet Sniffer ou Wireless Sniffer.

Intercepta e registra o tráfego de dados em uma rede de computadores.

Pode ser utilizado com propósitos maliciosos por invasores para capturar o tráfego da rede com diversos objetivos, como:

- obter cópias de arquivos durante sua transmissão;

- obter senhas ou ver conversações em tempo real.