Tópicos Especiais em Segurança da Informação

TP7 - Análise de códigos maliciosos

Arthur do Prado Labaki

28-06, 2022

GBC 235

Informações adicionais

Nem todos os exercícios estão com imagem aqui no relatório, mas todas as imagens integradas nesse relatório, quanto códigos, planilhas ou gifs de demonstração estão em meu repositório no GitHub abaixo.
Link do meu GitHub

Parte 1)

Para facilitar a explicação do exercício, essa primeira parte será dividia em 5, sendo uma para cada *hash* solicitado e a última para explicações gerais dos antivírus analisados. Também foi criado uma planilha para registrar as detecções doa antivírus, que está disponível no link abaixo.
Link da planilha

196eb5bfd52d4a538d4d0a801808298faadec1fc9aeb07c231add0161b416807

Esse malware é comumente conhecido como RansomExx.
Seu nome em *hash* é:

- MD5: f7c4cb42780b03303ca4b8535bb27207
- SHA-1: 6429700e978385c27d4443b1174fdb0b8940c5f3
- SHA-256: 196eb5bfd52d4a538d4d0a801808298faadec1fc9aeb07c231add0161b416807
- Vhash: 6df0735396cce17fe6a590e3e95f9069

A classe do malware é Ransomware com Cavalo de Troia.
Sua família de Ransomware é RansomExx, RansomX, Target777 ou Defray777
O tipo do arquivo binário é ELF (*Executable and Linkable Format*).
Seu tamanho é 253.59 KB (259680 bytes).
Por ser um ELF, o sistema operacional relacionado predominante é o Linux.
Esse malware foi responsável por atacar diversas empresas brasileiras, como a Renner e até o Superior Tribunal de Justiça (STJ).

cd9c621c0398dd8935890ffbe48a6cb1ebf8e7170b58b2a4981d98813d121282

Esse malware é comumente conhecido como Mirai.
Seu nome em *hash* é:

- MD5: 9f5285d74c8e7ee2e900b89f850604ba
- SHA-1: 89a18a364ca2e4dd382c57f50cdb4402b92a2bfb
- SHA-256: cd9c621c0398dd8935890ffbe48a6cb1ebf8e7170b58b2a4981d98813d121282
- Vhash: 3a9557e5312dce5056e3f79cc0a82d61

A classe do malware é Botnet focada em ataques de negação de serviços.
Ainda alguns analisadores afirmam que esse malware é Backdoor.
Sua família de Botnet/Backdoor é Mirai.1.
O tipo do arquivo binário é ELF (*Executable and Linkable Format*).
Seu tamanho é 35.30 KB (36152 bytes)
Por ser um ELF, o sistema operacional relacionado predominante é o Linux.
O malware em questão foi inicialmente usado para atacar servidores do jogo Minecraft e empresas que ofereciam proteção contra DDos para esses servidores, utilizando ataques de negação de serviços.

7786483b897971c243102c6203d0f19608524cba52136ae5fa71803e74d55825

Esse malware é comumente conhecido como GoCryptoLocker.
Seu nome em hash é:

- MD5: 8f616ddebbce71e29951a6e9472f2ea6
- SHA-1: 0394adee22cc087a07b5f661eeb008fb4083163a
- SHA-256: 7786483b897971c243102c6203d0f19608524cba52136ae5fa71803e74d55825
- Vhash: 0260f7555d14547474747az25!z

A classe do malware é Ransomware com Cavalo de Troia.
Sua família de Ransomware é GoCryptoLocker, Filecoder ou Ransom Encoder.
O tipo do arquivo binário é Win32 EXE PE (*Portable Executable*).
Seu tamanho é 2.62 MB (2749952 bytes)
Por ser um EXE, o sistema operacional relacionado predominante é o MS Windows.
Esse malware é CriptoLocker, ou seja, ele criptografa e bloqueia o acesso aos arquivos, exigindo dinheiro (normalmente em criptomoedas) para o resgate deles.

a1b05e1fc423dd9540b3c34cec562626358f55213ca3b352052792eaf8a9c98a

Esse malware é comumente conhecido como Stuxnet.
Seu nome em *hash* é:

- MD5: 03dc793dcbc7f24a986d321777c3b350
- SHA-1: d9a4fcaf116641f3e107b980a18d530af1d68719
- SHA-256: a1b05e1fc423dd9540b3c34cec562626358f55213ca3b352052792eaf8a9c98a
- Vhash: 055056551d151d7bzdnz1ez8

A classe do malware é Worm com Cavalo de Troia.
Sua família de Worm é Stuxnet, NSAnti.
O tipo do arquivo binário é Win32 EXE PE (*Portable Executable*).
Seu tamanho é 505.50 KB (517632 bytes)
Por ser um EXE, o sistema operacional relacionado predominante é o MS Windows.
Pesquisando mais, Stuxnet é um Worm projetado especificamente para atacar o sistema operacional SCADA desenvolvido pela Siemens e usado para controlar as centrífugas de enriquecimento de urânio iranianas.

Analisando os antivírus

Analisando os resultados, conseguimos verificar que alguns antivírus conseguiram detectar os quatro malwares testados. Eles são:

1. Avast
2. AVG
3. BitDefender
4. DrWeb
5. Emsisoft
6. eScan
7. ESET-NOD32
8. Fortinet
9. GData
10. Ikarus
11. Kaspersky
12. MAX
13. McAfee-GW-Edition
14. Microsoft
15. Sophos
16. Tencent
17. Trellix (FireEye)

Também exitaram poucos antivírus que não conseguiram detectaram nenhum dos quatro *hashes* malignos testados. São eles:

1. Acronis (Static ML)
2. Bkav Pro
3. F-Secure
4. TACHYON

5. Zoner

Examinando esses dados, podemos concluir que grande parte dos antivírus utilizados pela ferramenta Vírus Total (VirusTotal, 2012) tem uma boa eficiência sobre esses malwares relativamente famosos, já que 17 analisadores conseguiram detectar códigos maliciosos, além de que o malware que teve menos detecções corretas (o Mirai) teve cerca de 25 detecções, o que é um número relevante.

Parte 2)

Nessa segunda parte, foi requisitado estudar os malwares, procurar e obter duas amostras de dois malwares estudados e escolhidos anteriormente. Porém, para adquirir melhor conhecimento do assunto, foi obtido um malware de cada um dos citados no exercício, somando 13 amostra das diferentes classes e famílias de malwares, que são:

Malwares citados	
Nome Comum	Classe
ILoveYou	Worm
MyDoom	Worm
Storm	Backdoor
CryptoLocker	Ransomware
WannaCry	Ransomware
CovidLock	Ransomware
LockerGoga	Ransomware
Emotet	Trojan
Petya	Ransomware
Stuxnet	Worm
Zeus	Trojan
Melissa	Virus
SQL Slammer	Worm

Algumas informações obtidas pelo Virus Share (Roberts, 2014), pelo Cuckoo online sandbox(Guarnieri et al., 2018) ou por outras fontes foram adicionadas em uma outra tabela na

mesma planilha já disponibilizada.

Analisando os binários de malwares no *Sandbox*, é possível confirmar que são códigos malicioso por diversos fatores. Um deles pode ser a nota que o próprio ambiente virtual atribui para o arquivo analisado, sendo de 0 até 10, sendo esse ultimo muito suspeito. Todos os arquivos analisados receberam nota máxima.

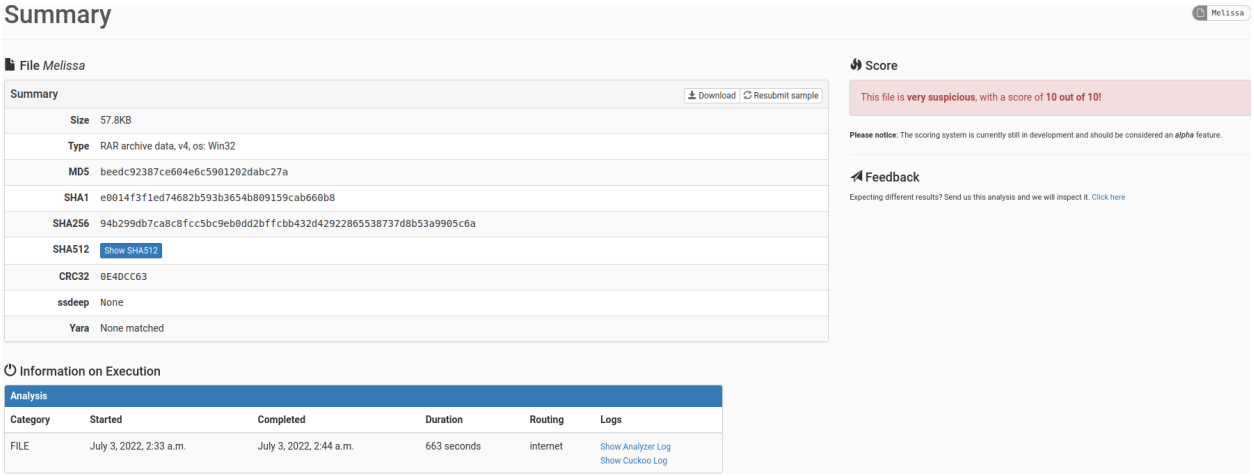

Figura 1: Resumo do malware Melissa no Cuckoo

Outra forma de analisa-los é lendo as strings deles. Nela é possível ver que diversos algumas ações dos códigos, como nos *criptomalwares*, que são malwares que criptografam os arquivos, ou *lockermalwares*, que bloqueiam o acesso do usuário aos arquivos, eles normalmente utilizam funções como *"CryptImportKey", "CryptDecrypt", "CryptGenRandom"* entre outros. Nas strings também é possível ver a linguagem que os códigos maliciosos utilizam, como *C++, HTML5, Python* e outros. Com essas informações, os antivírus podem obter essas strings em comum, utilizando algum algoritmo de aprendizado de máquina para impedir que arquivos com essas funções sejam executadas.

Também uma outra forma seria ver as analises de rede. Com ela é possível ver comunicações entre os malwares e outras máquinas, porém nas amostras capturadas, somente o *SQL Slammer* teve esse tipo de informação. Nele é possível ver algumas requisições HTTP para o site bdimg.share.baidu.com. Para também poder ver essas analises de rede, o *Behavioral Analysis* do Cuckoo na parte *network* pode auxiliar.

Além disso, podemos ver o *VM Memory Dump*, ou despejo da memória da maquina virtual.

Isso é o processo de pegar todo o conteúdo de informação na RAM e gravá-lo em uma unidade de armazenamento, realizado pelo arquivo executado. Com ele podemo ver que tipo de processos o malware executou na maquina virtual, como *"svchost.exe", "pythonw.exe", "SearchProtocol"ou "explorer.exe"*. Em alguns malwares não é possível visualizar esse despejo, pois provavelmente o malware executado deve ter em seu código fonte, funções para detectar se está sendo executado em um ambiente controlado, parando suas ações e não deixando o despejo da memória.

Com tudo isso, usuários mais experientes devem utilizar essas ferramentas para verificar se *URLs* ou arquivos desconhecidos são maliciosos, seja subindo eles no Vírus Total para verificar a analise dos antivírus, ou até testa-lo no ambiente controlado, para ver o comportamento dele em uma máquina virtual, impedindo do malware de prejudicar o usuário. Porem, nem todos os antivírus são capazes de identificar malwares, principalmente os recentes e também existem códigos maliciosos que detectam se estão em um ambiente controlado não executando. Com isso, mesmo com as ferramentas, ainda deve-se ter muito cuidado com links e arquivos desconhecidos.

Analisando os malwares individualmente

Com essas informações, binários de malwares e relatórios do ambiente Cuckoo, iremos analisar cada amostra, elencando suas características particulares. É importante ressaltar que todas as informações adicionais do malware estão indicadas na planilha, sendo a maioria do MalWiki. Ainda algumas amostras de malware que não tiveram resultados satisfatórios foram trocadas por outras amostras.

ILOVEYOU

Esse worm originalmente chamado de LOVE-LETTER-FOR-YOU.txt.vbs afetou mais de 50 milhões de computadores com Windows. Ele teve origem nas Filipinas e basicamente é um *script* do Visual Basic disfarçado. O malware quando executado danificava a máquina local e mandava uma cópia de si mesmo para todos os contatos do usuário no Outlook.

Analisando a sua execução, ele adiciona arquivos chamados *MSKERNEL32.VBS e WIN32DLL.VBS*. Pesquisando por esses nomes, temos que eles são adicionados na configuração do sistema alvo,

iniciando automaticamente junto com o sistema. Quando o alvo for iniciado, esse executável baixa e instala outro malware. Após isso, o malware pode agir de diferentes formas, como roubar dados do computador e enviar a um e-mail, pode modificar arquivos existentes no computador, e procurar a lista de e-mail do alvo para enviar esse malware para outros alvos. No caso da amostra obtida, é possível encontra o e-mail *ispyder@mail.com* além de algumas partes de um código HTML5 e do próprio código do Visual Basic.

Mydoom

Normalmente conhecido com W32.MyDoom@mm, Novarg, Mimail.R e Shimgapi é um worm de sistemas operacionais Windows que causou um prejuízo estimado de 38 bilhões de dólares. Esse malware se tornou na época o *worm* de mais rápida infeção através do e-mail. Ele, como o malware anterior, explora a falha humana (engenharia social), se passando de e-mails de erro, como *"Error", "Mail Delivery System", "Test"ou "Mail Transaction Failed"*.

No ambiente Cuckoo é possível verificar (principalmente no *Behavioral Analysis* e *VM Memory Dump*) que ele cria dois arquivos chamados de *Taskmon.exe e Shimgapi.dll*. Pesquisando melhor, esses arquivos adicionados são um backdoor que abre portas *TCP* variando de 3127 a 3198, permitindo baixar e executar arquivos arbitrários. Esses arquivos são adicionados na configuração do sistema para serem iniciados quando o computador alvo iniciar. Com esse acesso, ele consegue realizar qualquer ação na máquina hospedeira, como se enviar para os outros e-mails. Na amostra obtida não foi possível verificar esse espalhamento de e-mail característico de worm.

Storm

O Trojan Storm é um backdoor com cavalo de troia que afeta sistemas Windows. Pertencendo a família Peacomm dos Trojans, esse malware infectou milhares de computadores principalmente privados na Europa e nos Estados Unidos por meio de uma mensagem de e-mail característica "230 mortos por tempestade atinge a Europa", dai vem seu nome tempestade (Storm).

Ao ser executado, esse malware instala o serviço *wincom32* (possível de visualizar no Cuckoo) e injeta uma carga útil, passando pacotes para destinos codificados no próprio malware. Na amostra, é possível observar que o malware, após ser executado, baixa e executa um arquivo chamado *Launcher.exe*, provavelmente começando a sua segunda etapa. Nessa nova etapa, a máquina comprometida é mesclada em uma *botnet*, que é uma rede de computadores infectados que, sob o comando de um único computador principal, trabalham juntos para cumprir um objetivo, ou ainda instalando um *rootkit*, que é uma coleção de software de computador, projetada para permitir o acesso privilegiado a um computador ou a uma área do software que não é permitida.

CryptoLocker

Esse popular malware é um ransomware trojan que afeta sistemas Windows e que pode se espalhar por e-mail, característica de worms. Considerado um dos primeiros malwares ransomware, ele recebeu esse nome pela sua capacidade de criptografar os arquivos do usuário infectado e impedir o acesso a eles, sendo uma espécie de sequestro virtual de informação.

Ao ser executado, o código malicioso criptografa todos os arquivos do alvo usando um método de criptografia bastante difícil de decifrar ou descriptografar (RSA-2048). Assim, é cobrado um resgate, comumente em alguma criptomoeda para impedir seu rastreio, porém esse resgate nem sempre é garantido. Após algum tempo, normalmente 72 horas, o malware excluirá o código de descriptografia. Na amostra podemos observar que algumas strings são *"H:mm:ss dddd, MMMM dd, yyyy", "M/d/yy", "December", "Monday"* e provavelmente indicando que esse esse código utiliza algo relacionado ao tempo, como um temporizador. Também foi verificado que esse arquivo baixa e executa outro arquivo chamado {*CBEEB8AE-E184-322E-2C31-200C1D0F3521*}*.exe*, que deve ser um *script* em python para criar a tela de resgate, pois momentos antes de executa-lo, foi iniciado o processo *pythonw.exe*, que executa aplicativos de interface gráfica python sem iniciar um *shell* do sistema.

WannaCry

WannaCry, originalmente chamado WanaCrypt, também conhecido como Wana Crypt0r e Wana Decrypt0r, é provavelmente o mais famoso worm de ransomware que ataca sistemas Microsoft Windows. Ele se propaga através do EternalBlue, um *exploit* desenvolvido pela Agência de Segurança Nacional dos Estados Unidos (NSA) para sistemas Windows mais antigos, que foi roubado e vazado pelo grupo hacker The Shadow Brokers. O WannaCry causou estragos em aeroportos, bancos, universidades, hospitais e muitas outras instalações, se espalhando para cerca de 150 países em todo o mundo, principalmente Rússia, Ucrânia, EUA e Índia.

Como o CryptoLocker, o WannaCry utiliza o método de criptografia RSA-2048, sendo praticamente impossível de decifra-lo. Diferentemente do anterior, após algum tempo (normalmente 7 dias) o código malicioso começa a pagar os arquivos criptografados. Ao ser executado, ele baixará um cliente TOR para se comunicar com os servidores selecionados anonimamente. Após isso, ele obtém permissões completas do sistema, encerra processos de banco de dados e e-mail e começa a criptografar todos os arquivos possíveis, incluindo banco de dados e armazenamentos de correio, utilizando a extensão .WNCRY.

Em nossa amostra foi possível obter strings de funções utilizadas para criptografar os arquivos, como *"CryptAcquireContextA", "CryptImportKey", "CryptReleaseContext", "CryptDestroyKey"e "CryptDecrypt"*. Também é possível confirmar que ele usa RSA pois existe a *string "Microsoft Enhanced RSA and AES Cryptographic Provider"*. Pode ser visto também uma árvore de processos, sendo *WCry.exe, cmd.exe, cscript.exe, !WannaDecryptor!.exe, taskkill.exe e explorer.exe*. Também foi possível ler a nota de resgate utilizada pelo malware na figura 2.

Emotet

Trojan:Win32/Emotet ou Emotet é um trojan que afeta Windows. Esse malware consegue coletar credenciais bancárias e roubar dinheiro de contas bancárias usando ataques clandestinos MitB (*Man-in-the-Browser*). Ele também é usado para coletar credenciais para contas de mídia social, ou até mesmo soltar outro malware em *hosts* infectados.

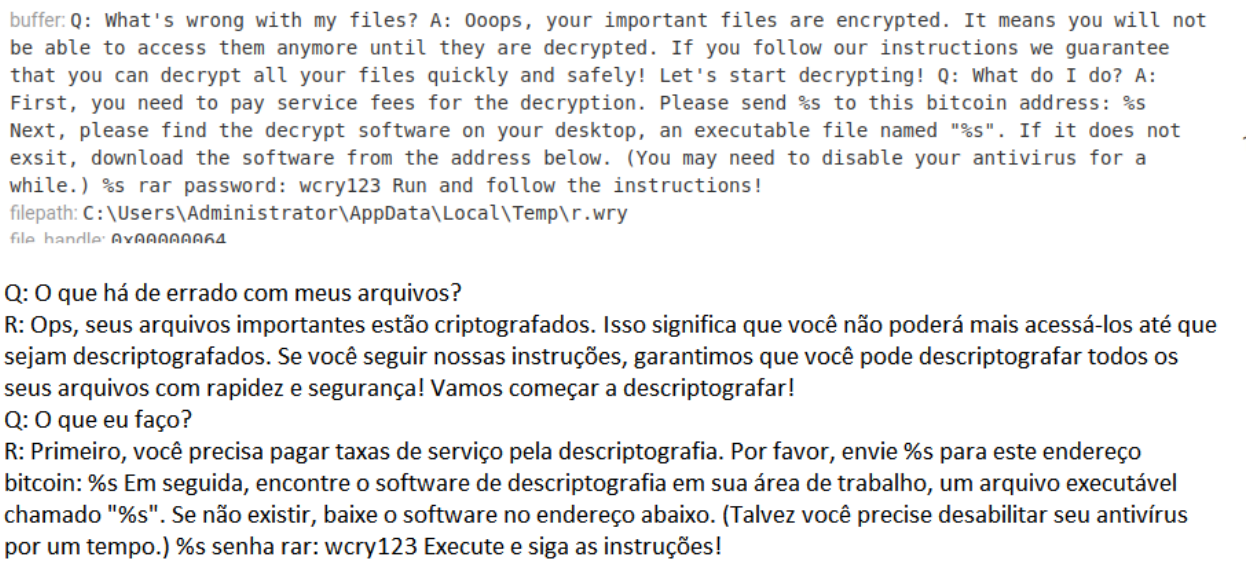

Figura 2: Carta de resgate do WannaCry

Ao ser executado, o malware instala um arquivo *DLL* que intercepta o tráfego de vários navegadores para obter os dados, principalmente bancários. Em seguida, ele envia os dados coletados para um servidor remoto, que é configurado pelo hacker. Na amostra, é possível ver strings das *dll* baixadas *"C://Windows//system32//uxtheme.dll", "dwmapi.dll"* e *"apphelp.dll"*. Ele também abre multi-processos, além de reabrir o *"explorer.exe"*.

Petya

Petya é uma família de ransomware que afeta o Microsoft Windows, ele infecta o registro mestre de inicialização (MBR) para executar uma carga que criptografa a tabela do sistema de arquivos de um disco rígido e impede a inicialização do Windows. O malware infecta principalmente computadores na Europa (especialmente Alemanha, Reino Unido, Bélgica e Dinamarca), mas começou a se espalhar pela Ásia, Austrália e América do Sul. O nome Petya é uma referência ao filme de James Bond GoldenEye de 1995, no qual Petya é um dos dois satélites de armas.

Os códigos maliciosos também são compactados e criptografados de maneira difícil de anali-

sar, o que torna o código difícil de detectar mesmo por meios heurísticos. Ao ser executado, o malware executara da memória (RAM) um arquivo *dll* e descriptografará sua seção .xxxx, incorporada no arquivo *DLL* como seção legível, e executará o código presente nela. O código presente na seção executará a *API DeviceIoControl* do Microsoft Windows no disco rígido principal. Na amostra, conseguimos encontrar funções de criptografia, como no WannaCry, além de pedaços de códigos escritos em C++ e Assembly. Também conseguimos observar que o malware realmente utiliza a tabela de registro mestre de inicialização, vemos *"Invalid partition tableError loading operating systemMissing operating systemc"*. Por fim, vale ressaltar que o Petya é realmente destrutivo, pois ele criptografa todo o disco rígido, impedindo o acesso do usuário, sendo demonstrado pois o *log* do Cuckoo afirma que foi possível gerar o *VM Memory Dump*, porém não tem nada nele, indicando que não existe arquivos visíveis.

Stuxnet

Stuxnet é um worm malicioso de computador descoberto pela primeira vez em 2010 e que se acredita estar em desenvolvimento desde pelo menos 2005. O malware tem como alvo sistemas de controle de supervisão e aquisição de dados (SCADA) e acredita-se ser responsável por causar danos substanciais ao programa nuclear do Irã. Embora nenhum país tenha admitido abertamente a responsabilidade, o worm é amplamente entendido como uma arma cibernética construída em conjunto pelos Estados Unidos e Israel em um esforço colaborativo.

Diferente de um worm típico, em vez de tentar roubar detalhes de cartão de crédito, senhas ou outras informações confidenciais, o Stuxnet é lançado contra sistemas industriais. Ele faz com que as centrífugas se autodestruam, criando muitos danos. Segundo especialistas em segurança, essa ameaça tinha um grande potencial para ser usada para destruição física. Parece que os invasores projetaram esse worm digital com muito cuidado para que ele não atinja os computadores e redes que não atendem a configurações específicas. Analisando os *logs* do Cuckoo, pode-se notar que após o malware ser executado, quase nenhuma ação é realizada, observando o *Behavioral Analysis*, ele usa argumentos para comparar strings e objetos, provavelmente buscando as configurações especificas do alvo.

Zeus

Zeus ou Zbot é um trojan que roda no Microsoft Windows. Foi identificado pela primeira vez em julho de 2007, originalmente usado para roubar informações do Departamento de Transportes dos EUA. Às vezes, ele era usado para instalar o CryptoLocker. O malware engana a vitima usando golpes de engenharia social de uma forma muito mais leve. Ele também é muito difícil de se detectar utilizando antivírus antigos e outros softwares de segurança antigos, pois se esconde com poderosas técnicas furtivas.

Quando instalado em um computador *host*, ele tenta induzir o usuário a pagar pelo suporte técnico por meio de anúncios *pop-up* e usa o visualizador de eventos ou o *prompt* de comando para manipular o usuário a pensar que seu computador está infectado. A amostra coletada provavelmente é recente e relativamente fraca, pois seu código fonte foi copiado em partes do Stack Overflow, sendo confirmado encontrando esse nome nas strings do malware. Também é possível ver que ele executa um processo de nome *"muuz.exe"*. Ele também se clona para a pasta Temp e Roaming do usuário administrador do computador, além de utilizar funções de tempo, provavelmente em um temporizador.

Melissa

Melissa é um vírus de macro muito perigoso que apareceu por volta de 1999. Ele visava sistemas baseados no Microsoft Word e Outlook e criava um tráfego de rede considerável. O vírus infectaria computadores via e-mail utilizando engenharia social, normalmente utilizando pornografia (seu nome, de acordo com o criador do malware, era de uma stripper).

Ao ser executado, ele enviaria um e-mail em massa para as primeiras cinquenta pessoas na lista de contatos do usuário e desabilitaria vários recursos de proteção no Microsoft Word e no Microsoft Outlook, permitindo se espalhar. O vírus desacelerou os sistemas de e-mail devido à sobrecarga dos servidores Microsoft Outlook e Microsoft Exchange. Logo de cara podemos ver que o arquivo do malware é uma arquivo do word (.doc). Observando as imagens, ao ser aberto o documento, o Microsoft Word nem chega a carrega-lo, travando. Nas strings, é possível ver o nome Harry H., uma senha com o nome de um site *"http://SuperBest.da.ru/"*, além de ter *string* do Visual Basic para abertura e execução de *scripts*.

SQL Slammer

SQL Slammer também conhecido como Helkern ou Sapphire é um worm que causou cerca de 1 bilhão de dólares em danos. Ele foi criado em 2003 e afeta o sistema operacional Microsoft Windows. A causa foi uma exploração com o *bug* de estouro de *buffer* nos produtos de banco de dados *SQL Server* e *Desktop Engine* da Microsoft. Ele causou uma negação de serviço em alguns *hosts* da Internet e reduziu drasticamente o tráfego geral da Internet.

Ele é um pequeno pedaço de código que faz pouco além de gerar endereços IP aleatórios e se enviar para esses endereços. Se um endereço selecionado pertencer a um *host* que esteja executando uma cópia não corrigida do *Microsoft SQL Server Resolution Service* escutando na porta UDP 1434, o *host* será infectado imediatamente e começará a espalhar mais cópias do programa worm pela Internet. Após algum tempo, ele foi desacelerando os sistemas do mundo inteiro, em que essa desaceleração foi causada pelo colapso de vários roteadores sob a carga de tráfego de bombardeio extremamente alto de servidores infectados. Na analise do Cuckoo da amostra, conseguimos ver que esse malware abre uma página local no navegador. Também é possível ver diversas requisições *GET* no site *"http://bdimg.share.baidu.com/"*. Nas strings é possível visualizar o código *HTML5* quase completo da página web. Também conseguimos ver que ele acessa diversas *dll* e impede outras de serem executadas.

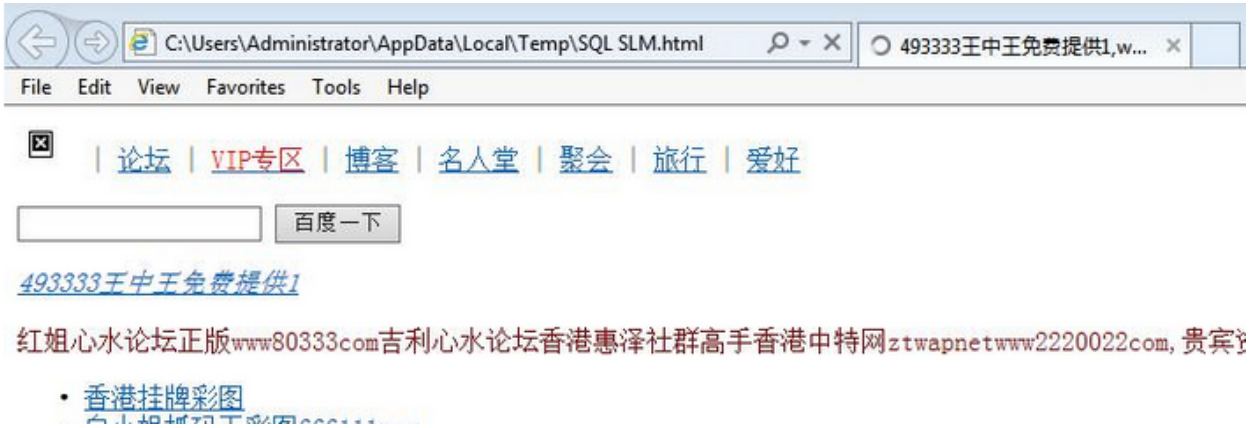

Figura 3: Site local aberto pelo SQL Slammer

Observações Importantes

Alguns malwares foram trocados por outras versões, pois alguns não executaram ou não obtiveram o resultado esperado. Ainda vale relembrar que todos os *logs* gerados, strings, *Memory Dump* e outras informações estão upados no Github mencionado.

Imagens de exemplos

Por fim, serão adicionado algumas imagens mostrando um pouco dos malwares explicados em ação.

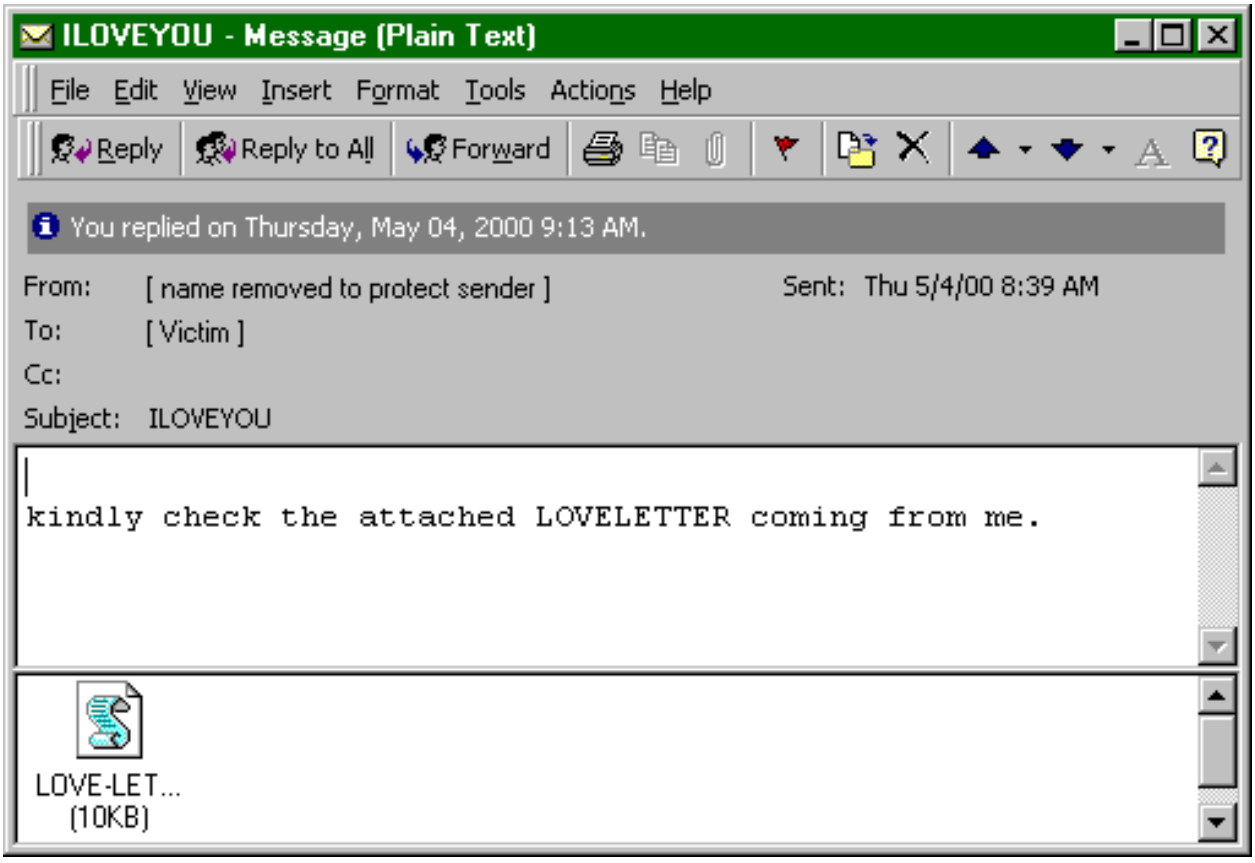

Figura 4: E-mail com o malware ILOVEYOU

Figura 5: E-mail com o malware Mydoom

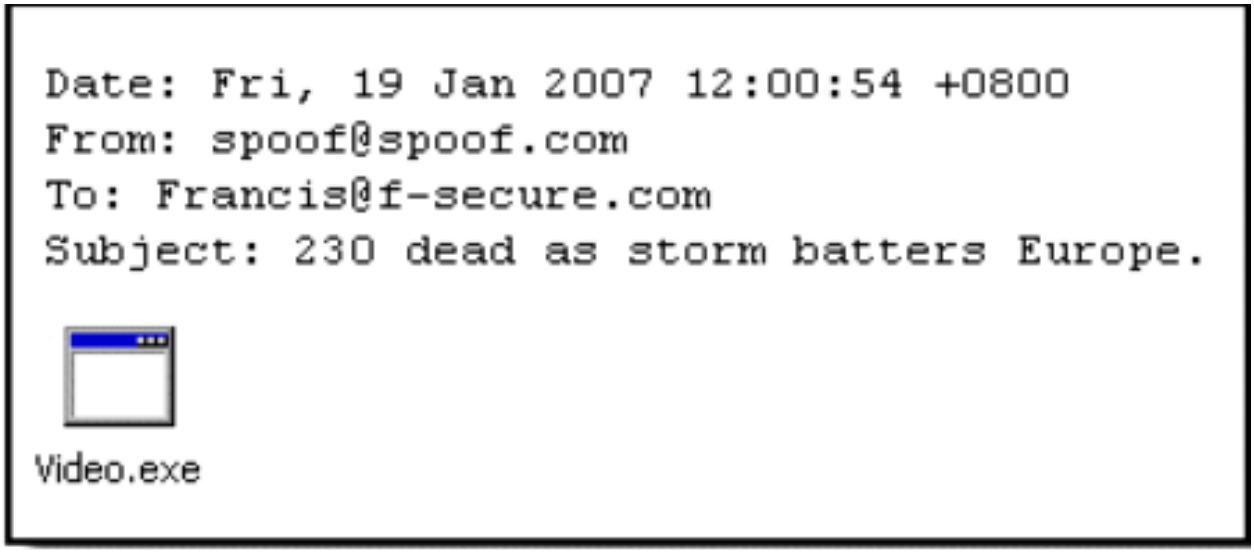

Figura 6: E-mail com o malware Storm Trojan

Figura 7: Tela de resgate do CryptoLocker

Figura 8: Tela de resgate do WannaCry

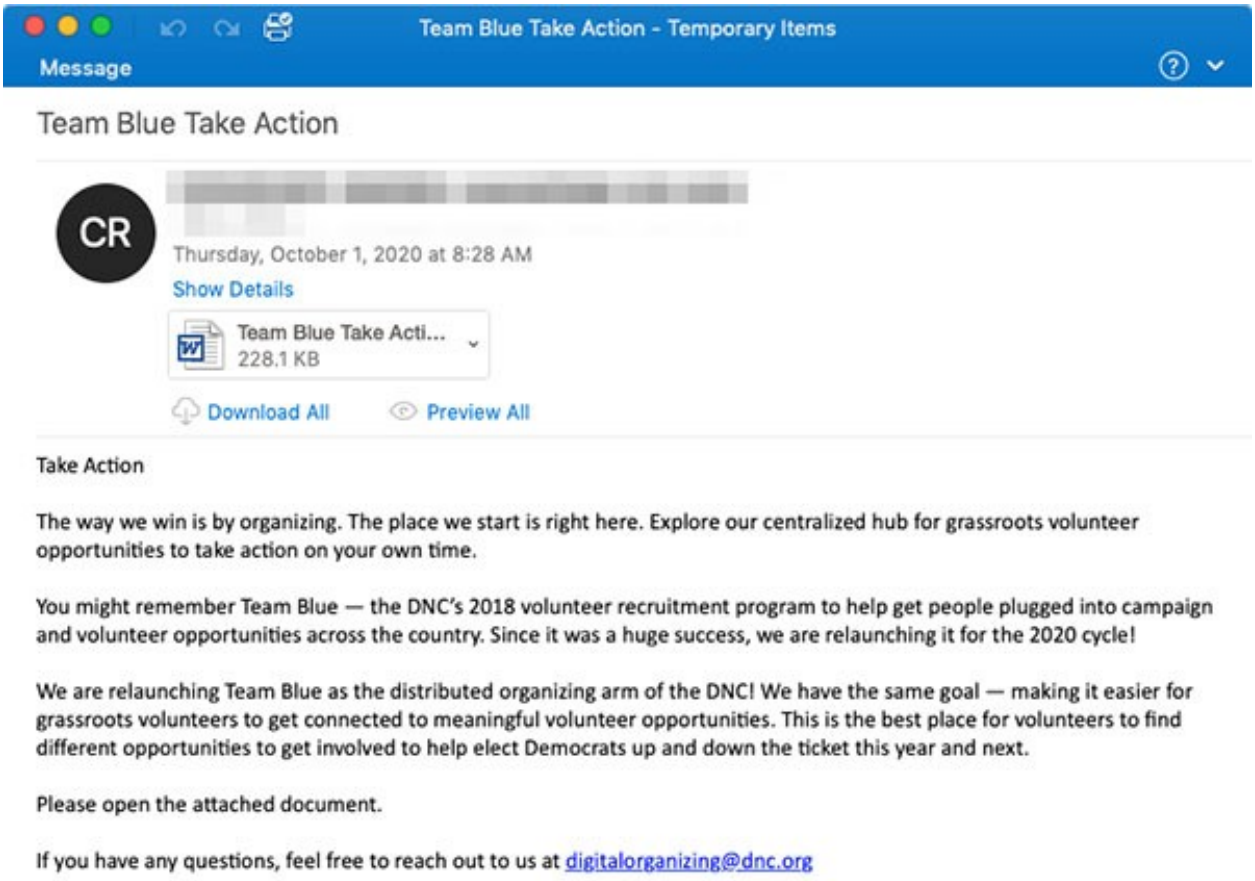

Figura 9: E-mail com o malware Emotet

Figura 10: Tela de resgate do Petya

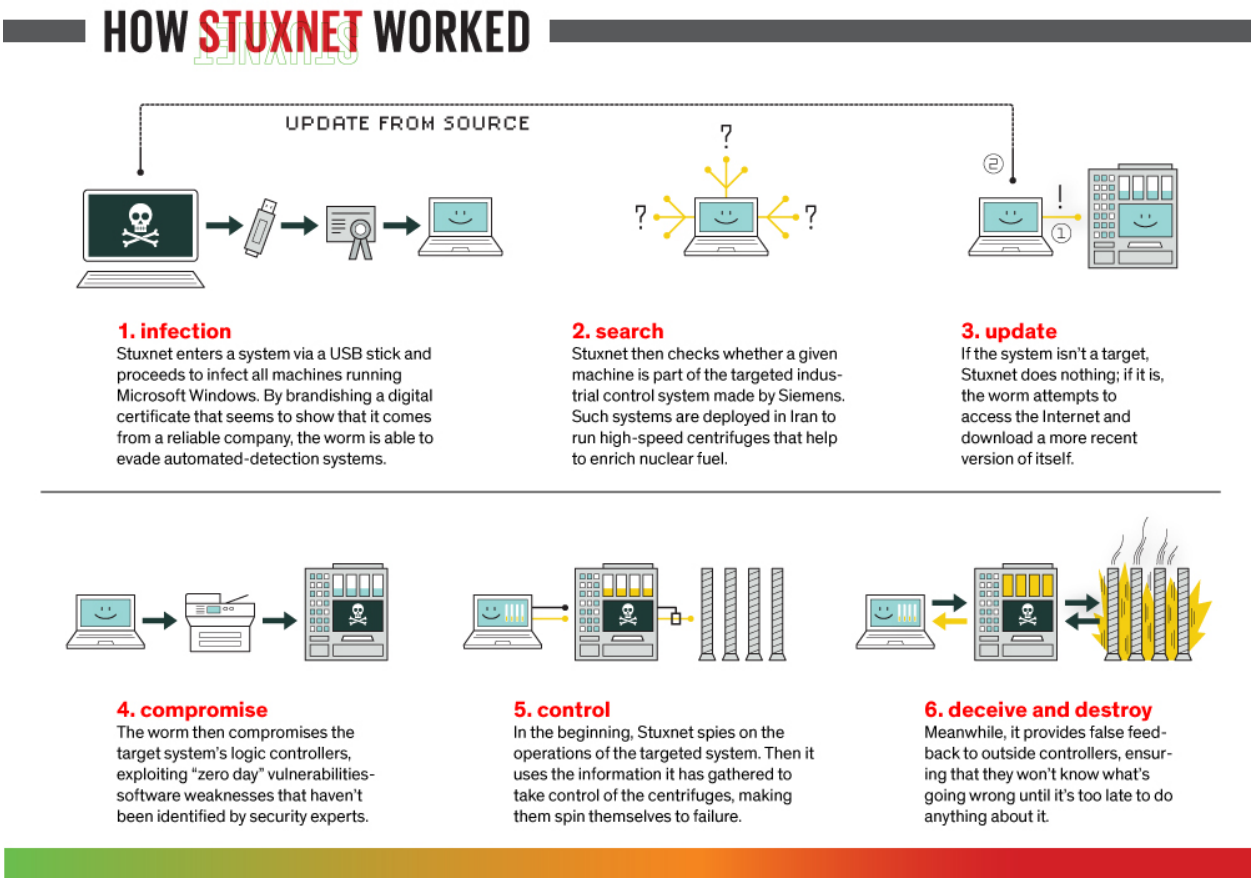

Figura 11: Explicando o funcionamento do malware Stuxnet

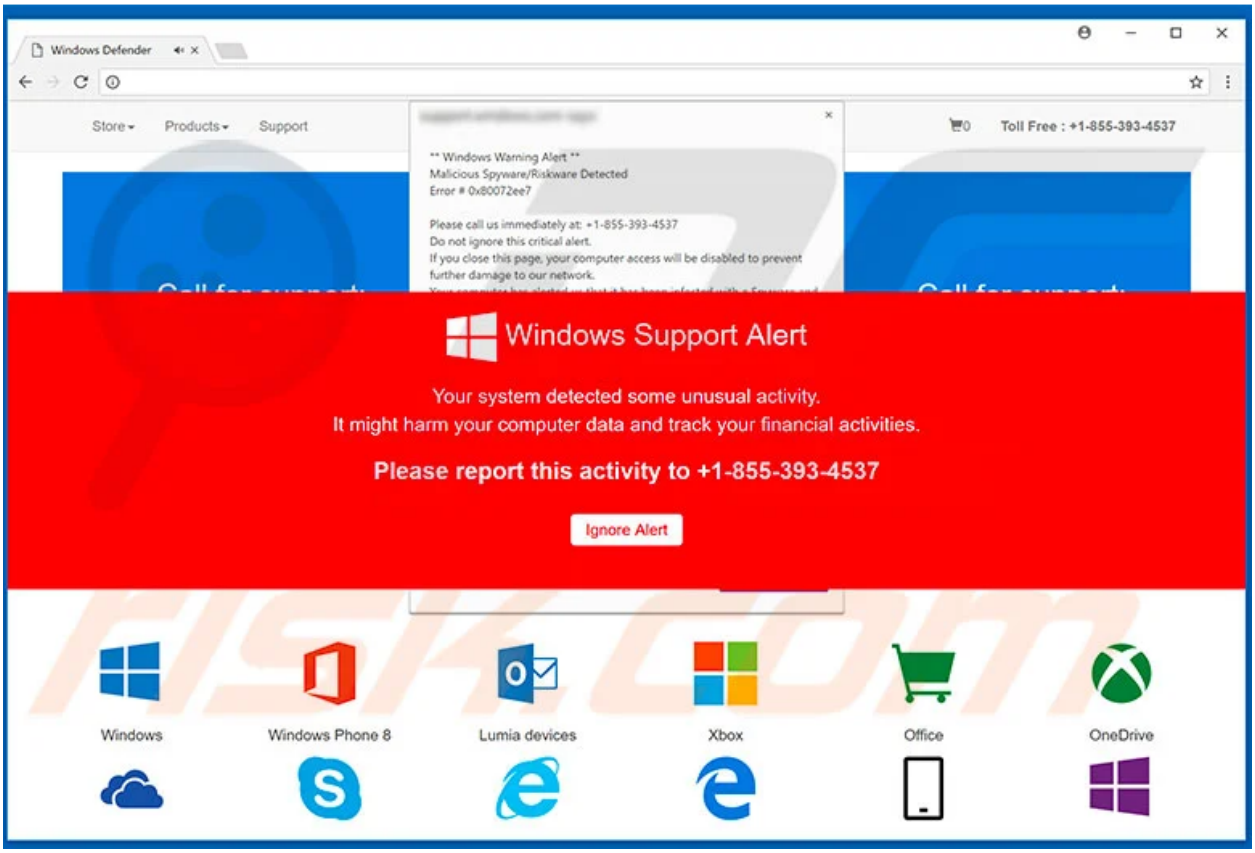

Figura 12: Funcionamento do malware Zeus

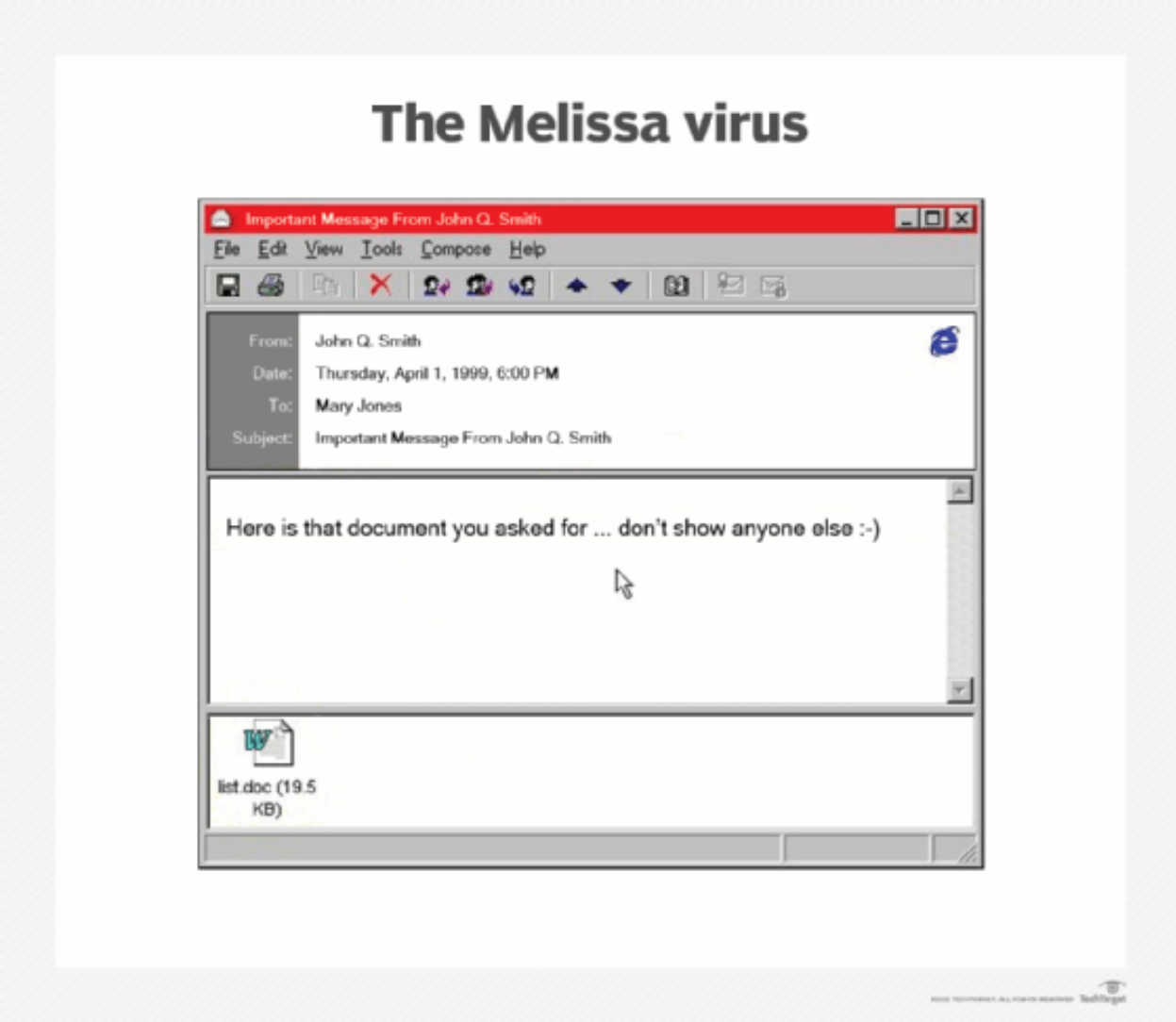

Figura 13: E-mail com o malware Melissa

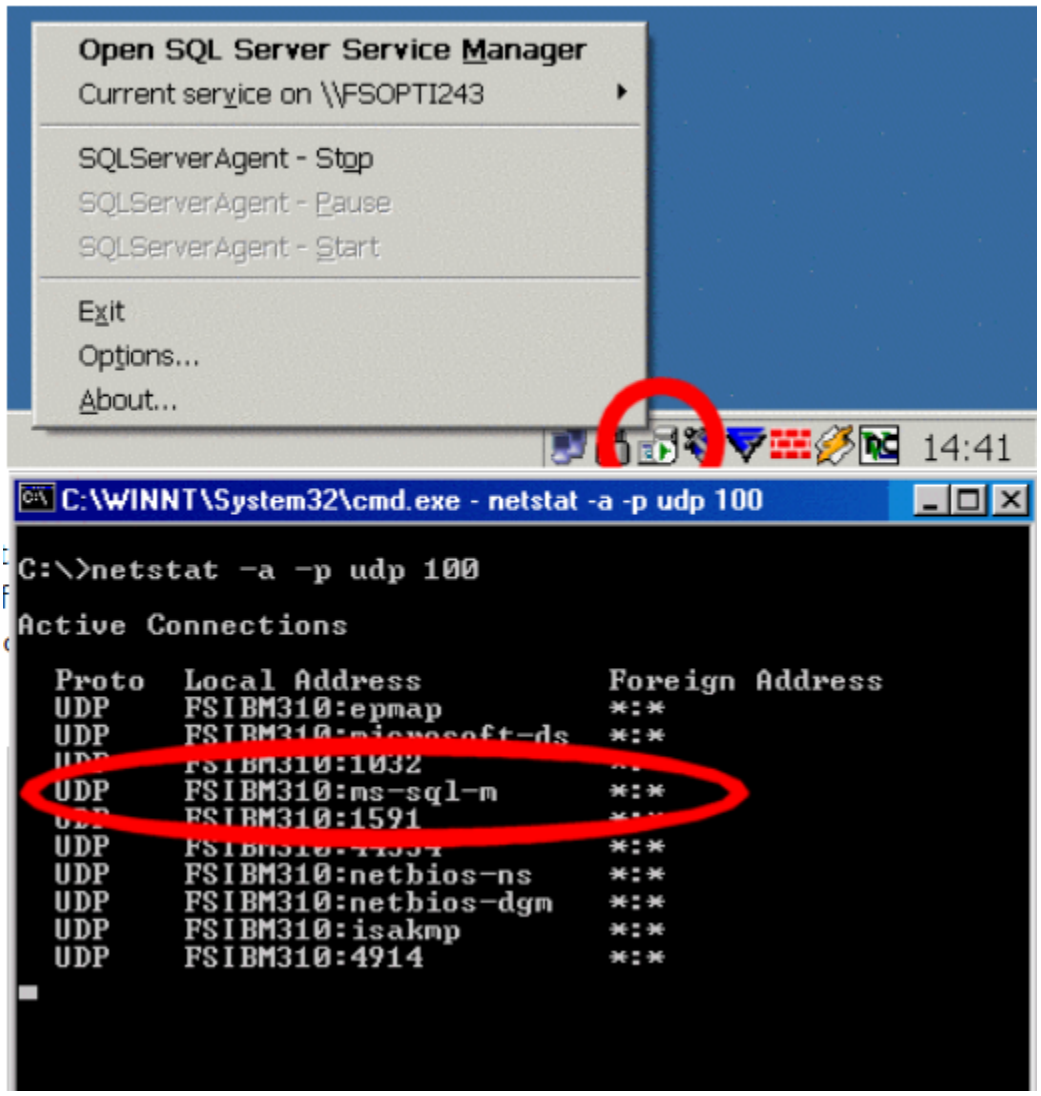

Figura 14: Demonstrando execução do malware SQL Slammer

Referências

Guarnieri C. n., Tanasi A. j., Bremer J. s. e Schloesser M. r. (2018). *Cuckoo Sandbox Online*.

Roberts J.-M. (2014). *Virus share*.

VirusTotal (2012). "Virustotal-free online virus, malware and url scanner". *Online: https://www. virustotal. com/en*.