Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 05
Antivírus

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

"Atitudes exageradas de um indivíduo significam, quase sempre, o contrário do que se declara."
(Hammed)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O que Aprenderemos?

- Aprender o conceito de antivírus;
- Entender o funcionamento;
- Compreender o conceito de assinaturas de vírus;
- Apresentar dicas e exemplos de antivírus.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

Os principais mecanismos de segurança são:

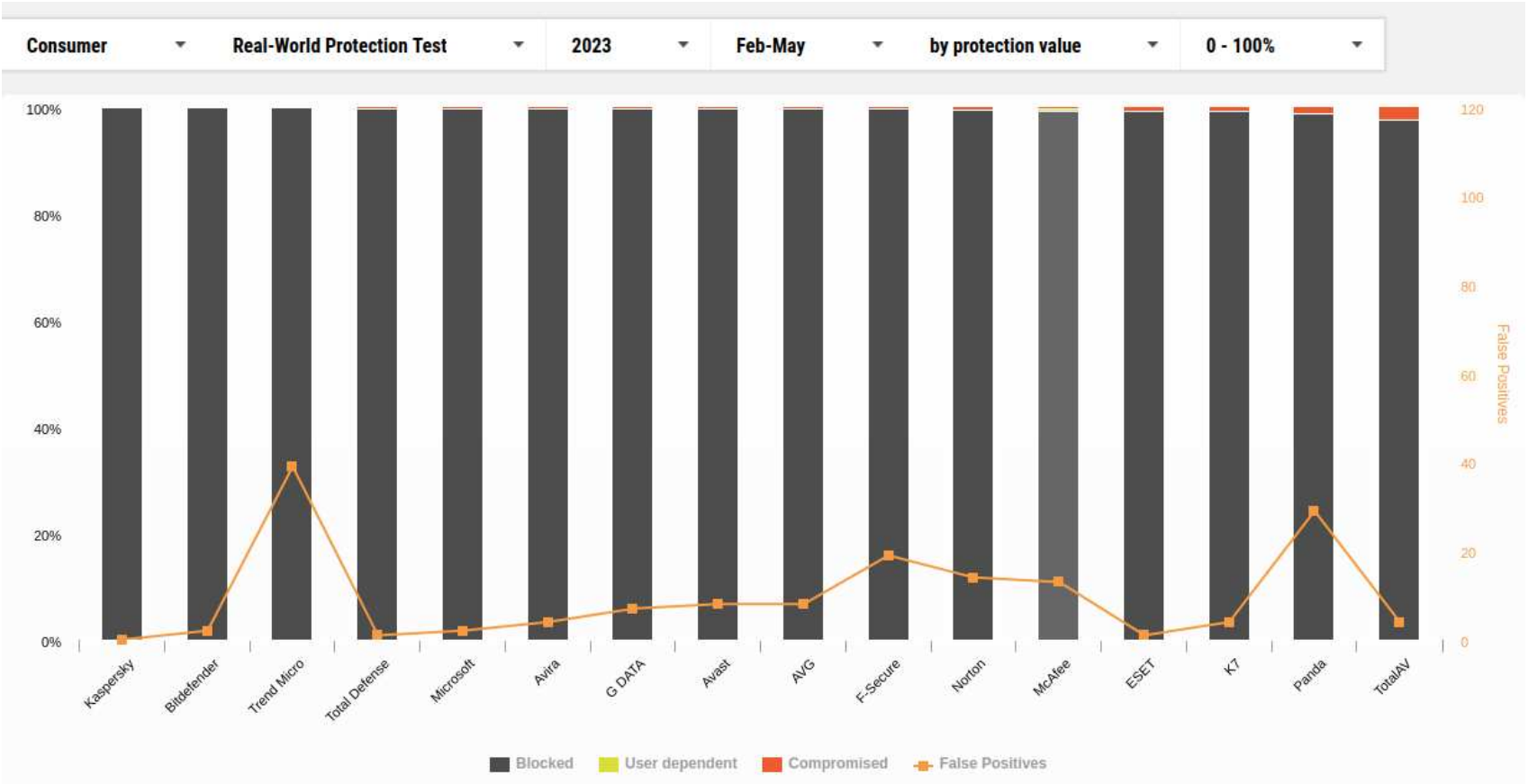
- Firewall;
- Antivírus;
- Criptografia;
- Autenticação;
- Assinatura Digital;
- Sistema de Detecção de Intruso;
- Rede Virtual Privada (VPN);
- Política de Segurança.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus

Antivírus, ou antimalwares, é um *software* que detecta, impede e atua na remoção de programas de *software* maliciosos (*malwares*). Ele varre arquivos ou monitora ações dos programas em busca de indícios de atividades maliciosas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE



O site `http://www.av-comparatives.org/` realiza comparações, através de testes, entre diversos antivírus.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus

Em geral, os antivírus detectam os *malwares* das seguintes formas:

- Assinatura: possuem um banco de dados de assinaturas que contém informações sobre padrões conhecidos de malware (bytes e/ou hash). Essas assinaturas são comparadas com os arquivos presentes no seu sistema para detectar se há alguma correspondência;
- Heurística: um arquivo sob análise é executado virtualmente em um emulador minimalista e os indícios de comportamento suspeito são avaliados a fim de se verificar a atividade realizada pelo programa, como alterações não autorizadas em arquivos do sistema, tentativas de modificar registros do Windows, entre outros;
- Comportamental: é feito uma análise do comportamento dos programas que são executados na máquina real e identificando se determinadas ações são suspeitas.

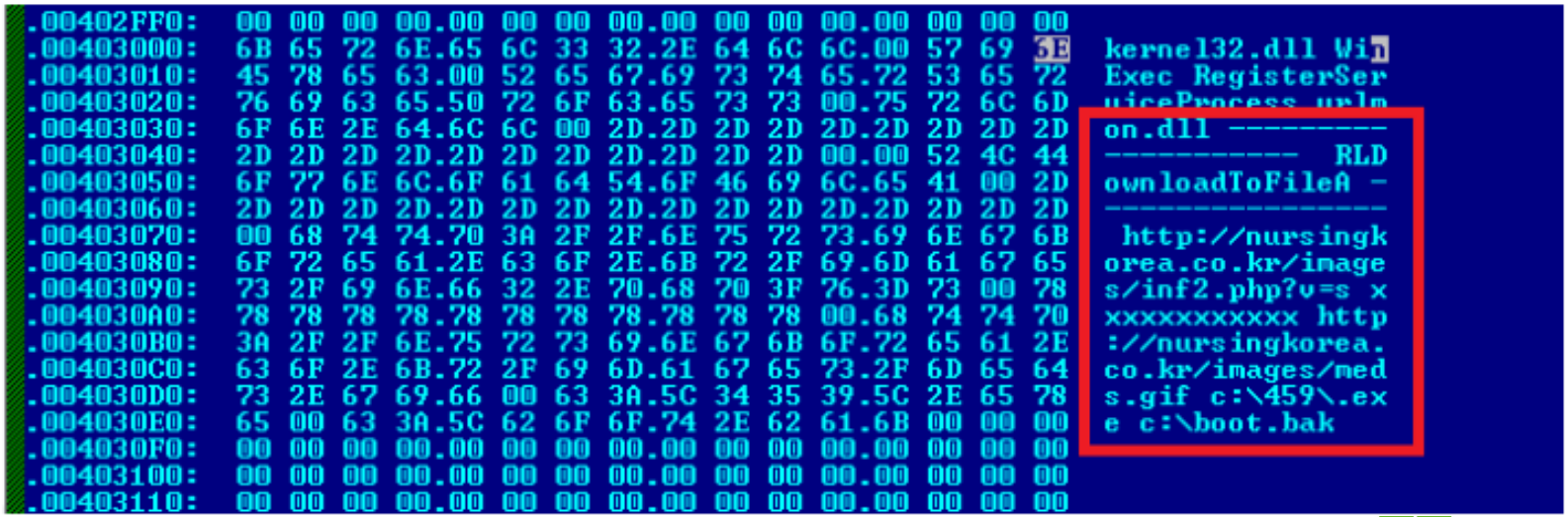
Antivírus

Tanto a detecção Heurística quanto a Comportamental são detecção proativa. Elas são importantes devido a quantidade de códigos maliciosos que aparecem todos os dias. Nelas para cada ação executada pelo arquivo é atribuída uma pontuação, por isso, se esse número for superior a um determinado valor, será classificado como um provável novo malware. Depois o antivírus manda uma amostra do arquivo para análise da empresa, e se confirmada geração de novas assinaturas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus

As assinaturas pode ser: um *hash* criptográfico e uma determinada cadeia de caractere, como URLs e endereços de correio eletrônico. Hoje, assinaturas estão longe de serem suficientes na hora de detectar arquivos maliciosos pois os *malwares* podem ofuscar (esconder) estas assinaturas visando burlar seus rastros.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Antivírus

O grande problema dos antivírus é o surgimento frequente e crescente de *malware*, cujas ações modificadas visam evitar a detecção. Desta forma, os antivírus precisam atualizar o banco de dados de assinaturas sempre. Entretanto entre o surgimento do malwares e a disponibilização das assinaturas requerem um período consideravelmente longo. Pois, primeiro é necessário a empresa receber a amostra, depois desenvolver uma detecção, enviá-la para o servidor e aguardar até que o computador do usuário seja atualizado com o novo banco de dados. Desta forma, os antivírus trabalham com a detecção por assinatura e comportamental. Alguns antivírus, mais sofisticados, apresentam também a detecção por heurística.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus – Dicas

- Escolha um antivírus confiável e respeitável de uma empresa reconhecida;
- Mantenha o antivírus atualizado;
- Ative a proteção em tempo real: isso permite que ele monitore continuamente o sistema em busca de ameaças enquanto você usa o computador.
- Execute verificações regulares: além da proteção em tempo real, realize verificações regulares (agendadas) do sistema para garantir que não haja malware oculto.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus – Dicas

- Configure para verificar automaticamente arquivos anexados aos e-mails e obtidos pela Internet, os discos rígidos e as unidades removíveis (como pen-drives, CDs, DVDs e discos externos);
- Nunca use dois antivírus no mesmo computador podendo causar instabilidade e não detectar vírus;
- Utilize antivírus *online* quando suspeitar que o seu antivírus esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião sobre um arquivo. O site `https://www.virustotal.com/` disponibiliza um antivírus online.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE