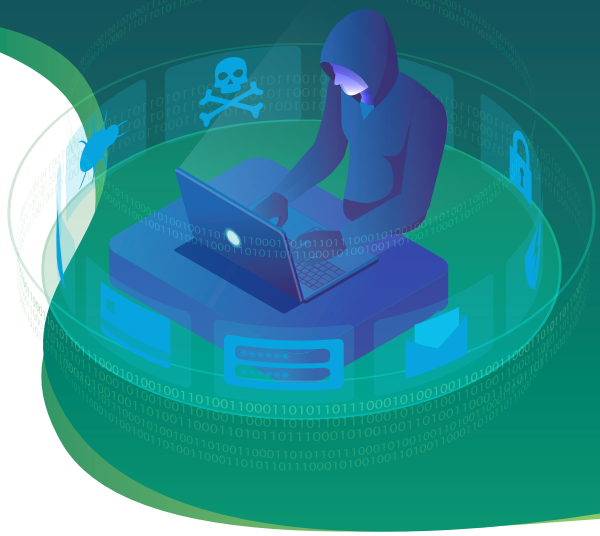
minitel NEXT WEBROOT Smarter Cybersecurity



RANSOMWARE, CRYPTOJACKING E OUTROS MÉTODOS DE ATAQUE EM 2019

O QUE DEVE SABER?

Com um valor de cerca de 11,5 mil milhões de dólares*, o ransomware é um negócio que vale muito dinheiro e, por isso, todos sabemos que não vai desaparecer tão cedo.

Mas, os dados mais recentes recolhidos pelo Webroot em 2019, apontam para algumas mudanças que é importante conhecer.

CRYPTOJACKING EM DECLÍNIO

O cryptojacking, um dos principais métodos de ataque, constituiu cerca de 35% das ameaças na primeira metade de 2018 (Webroot Threat Report 2018) e registou um declínio em 2019.

Isto não significa, infelizmente, que tudo está melhor e que as empresas podem sentir-se mais seguras. Para os cibercriminosos é um negócio e, assim sendo, estão sempre a surgir novas variantes que, com a possibilidade de compra/venda de malware na dark web, espalham-se em pouquíssimo tempo e podem ser devastadoras.

O RANSOMWARE TEM NOVAS FORMAS

Os ataques de ransomware na sua forma "tradicional" também diminuíram ligeiramente, mas foram substituídos por ransomware mais direcionado, com alvos específicos, capaz de se introduzir de forma ainda mais subtil nos sistemas de IT empresariais.

As PMEs estão no topo dos ataques. Os ataques através da porta RDP (Remote Desktop Protocol) também aumentaram, porque muitas empresas deixam este acesso desprotegido. Após um ataque bem-sucedido, os hackers tomam total controlo das máquinas e servidores, o que pode ter um enorme impacto nas PMEs.

Um ataque a uma fábrica, por exemplo, pode interromper as operações e a produção, bloqueando informações importantes, o que leva a que muitas empresas paguem o ransom para as recuperar.

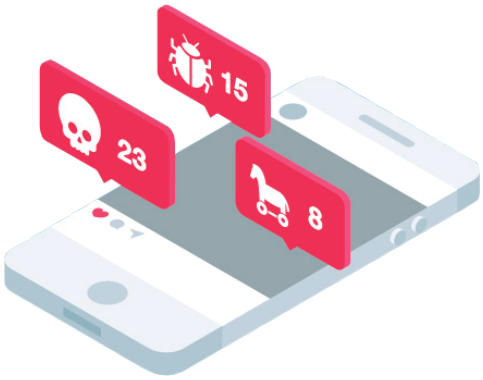
*Cybersecurity Ventures

Tudo isto é agravado porque os cibercriminosos não perdem tempo a desenvolver o malware, que pode ser adquirido na dark web apenas pelo preço de um café.

NOVO FOCO: O ROUBO DE INFORMAÇÃO

O roubo de dados é uma tendência corrente: o trojan bancário concebido para roubar informação sensível e credenciais bancárias online, procura obter dinheiro rápido.

As fugas de dados aumentaram 424% no último trimestre de 2018 (Inforsecurity Magazine). Os cibercriminosos focaram-se mais em pequenos negócios e dispõem de ferramentas mais sofisticadas, com maior automação e praticamente sem intervenção humana, que permitem atacar um maior número de PMEs.



MAIOR AUTOMAÇÃO

Quando falamos de alvos selecionados, podemos pensar em envolvimento humano. Mas, na prática o ataque é codificado sem a intervenção humana. O malware decide rotineiramente não correr se se tratar de um ambiente virtualizado, ou se existirem ferramentas de análise instaladas nas máquinas.

Os malwares Emotet e TrickBot utilizam automação para manter os botnets a funcionar e espalhar os ataques, utilizando credenciais roubadas. As fugas através de RDP são mais fáceis que nunca, devido aos processos automáticos que varrem a internet para encontrar vulnerabilidades. Num futuro próximo, vamos encontrar malware ainda mais inteligente e com maior automação.

O QUE PODEMOS FAZER?

Adotar uma tecnologia de segurança eficaz e sempre atualizada, como o Webroot, permite proteger contra as ameaças zero day, detetar e parar o ransomware. Utilizar uma solução como o Webroot DNS Protection, torna a navegação web dos seus clientes mais segura e bloqueia as ameaças.

As soluções do Webroot para endpoints, rede e utilizadores aproveitam a tecnologia Next Generation para parar as ameaças next gen:

- 100% cloud, eficaz, fácil de gerir e totalmente integrado. Todas as soluções utilizam a inteligência de ameaças do Webroot, a plataforma BrightCloud Threat Intelligence, uma das maiores redes mundiais de deteção de malware, que utiliza machine learning e AI para proteção em tempo real. Esta plataforma é utilizada por empresas líderes em segurança em todo o mundo – incluindo a Citrix, Cisco, F5 Networks e Palo Alto Networks –para melhor proteção dos clientes contra ciberataques.

A melhor parte, é o facto destas soluções abrangentes serem geridas remotamente, de forma simples e fácil, através de uma única consola baseada na Web, sem necessidade de um servidor de gestão local e sem ter de se preocupar com a localização dos endpoints.

WEBROOT BUSINESS ENDPOINT PROTECTION

- Deteta em tempo real
- Utiliza sempre a inteligência mais atualizada
- Faz o levantamento pesado na cloud (não nos sistemas dos clientes)
- Instala-se e faz scans em segundos

WEBROOT DNS PROTECTION

- Detém 88% das ameaças antes de atingirem a rede
- Poupa tempo e dinheiro na remediação
- Ajuda a controlar a largura de banda
- Minimiza a utilização pouco produtiva da web
- Permite personalizar políticas (por IP, grupo ou dispositivo)

WEBROOT SECURITY AWARENESS TRAINING

- Cumpre a legislação
- Implementa as melhores práticas
- Detém os ataques de phishing e social engineering
- Oferece formação constante para defesa constante

3 CAMADAS DE SEGURAÇA GERIDAS NA MESMA CONSOLA

QUER SABER MAIS OU TESTAR ESTAS SOLUÇÕES? CONTACTE-NOS E PEÇA-NOS UM TRIAL!

NEXT@MINITEL.PT

21 381 09 00