SONICWALL

SEUS DADOS POR RESGATE

Por que ransomware é o exploit preferido dos hackes atuais

CAPTURE RANSOMWARE PERMANENTEMENTE

Os agentes de ameaças e hackers sempre foram habilidosos em violar redes e roubar dados. No entanto, geralmente era complexo e demorado converter esses dados em moeda forte.

A introdução do ransomware eliminou a necessidade da exfiltração de dados e a revenda em mercados clandestinos.

Atualmente, é mais fácil violar sua rede, criptografar os dados e mantê-los para resgate até que você pague. Sem uma estratégia de cibersegurança em tempo real e proativa implantada, as organizações ficam com poucas opções.

Explore este guia para entender melhor o ransonware e como uma solução de sandboxing baseada na nuvem pode diminuir os ataques, antes que eles violem seu ambiente e mantenham seus dados, e seu negócio, por resgate.

Visão geral

SONICWALL®

Ransomware: você está protegido contra o próximo ataque?

Você será a próxima vítima de ransomware? Os invasores podem criptografar seus dados e mantê-los reféns até que você pague um resgate?

As grandes e pequenas organizações de todos os setores em todo o mundo correm risco de um ataque de ransomware. Na maior parte das vezes, a mídia relata ataques em grandes instituições, como o Hollywood Hospital que ficou por mais de uma semana off-line em 2016, depois que um ataque de ransomware criptografou arquivos e exigiu resgate para descriptografar os dados.

Entretanto, pequenas empresas também são afetadas. Na realidade, uma pesquisa da Kaspersky relatou que as empresas de pequeno e médio porte foram as mais afetadas, 42% delas sendo vítimas de um ataque de ransomware em um período de 12 meses.

Dessas, uma em três pagou o resgate, mas uma em cinco nunca recebeu seus arquivos de volta, apesar do pagamento. Sendo parte de uma grande organização ou de uma pequena empresa, você corre risco.

CONCLUIR A HISTÓRIA >

SONICWALL®

Os sete hábitos de ataques de ransomware altamente eficazes

Em 2016, a SonicWall detectou um crescimento de 600% em famílias de ransomware. Vimos uma grande variedade de formas de ransomware e vetores de ataque no Relatório Anual de Ameaças 2017, alguns bem-sucedidos e outros nem tanto.

Portanto, o que está no núcleo de qualquer ataque bem-sucedido? Se você entender os sete componentes da estratégia de uma campanha de ransomware, poderá se defender melhor de uma das mais perniciosas formas de malware na história.

1. Pesquisa inteligente de destino

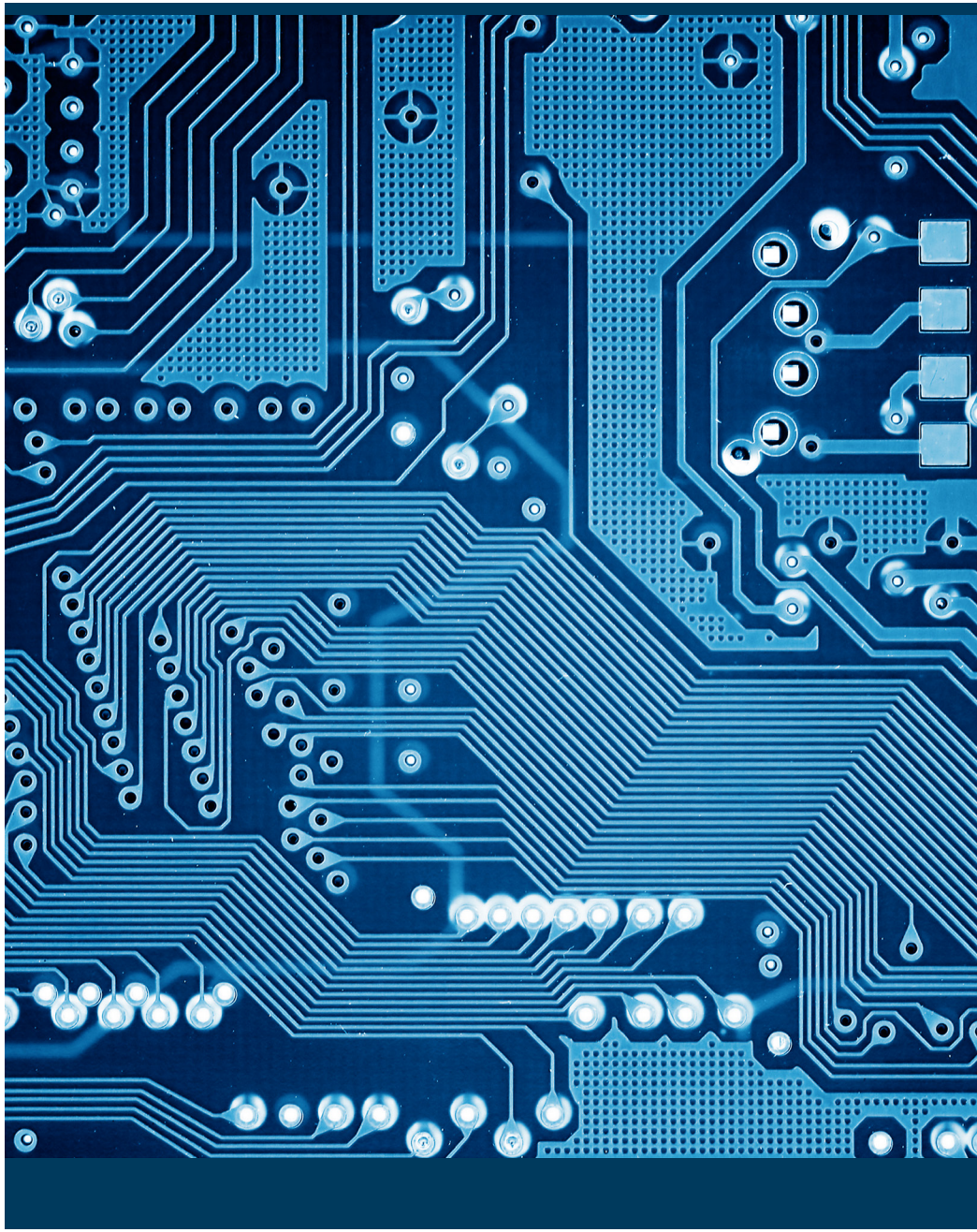
Qualquer bom golpista sabe como localizar as pessoas certas em uma organização para direcionar a mensagem certa. Os hackers sabem que organizações municipais e de saúde são opções propícias.

Embora as organizações forneçam educação de conscientização, as pessoas ainda clicam em postagens de mídia social e e-mails criados com inteligência. Além disso, os hackers podem acessar qualquer base de dados pública de geração de demanda e encontrar o conjunto certo de vítimas para uma campanha de phishing.

2. Fornecimento eficaz

Como 65% dos ataques de ransomware acontecem por meio de e-mail, um golpista pode facilmente enviar aquele anexo infectado para alguém em contas a pagar com a alegação de que uma fatura não foi paga. Um ataque semelhante derrubou a BWL de Lansing, Michigan, por duas semanas e custou à fornecedora de serviços públicos cerca de US$ 2,4 milhões.

VER A LISTA COMPLETA >



SONICWALL®

Ransomware-como-um-Serviço (RaaS) é a nova moda

Os modelos de negócios sempre têm de abordar o método de distribuição; as vendas serão diretas ou por meio de um canal de distribuidores, ou uma combinação de ambos? O mesmo vale para desenvolvedores de ransomware.

Muitos escolhem pegar seu código bem-sucedido e vendê-lo como um kit, o que elimina muitos riscos e o trabalho pesado de distribuição, ao mesmo tempo que recebem uma redução na recompensa.

Durante todo o ano passado, e mesmo até os ataques de WannaCry em grande escala, as flutuações entre os picos dos famigerados eventos são ataques em massa pequenos e focados de exploit kits reformulados. A SonicWall descobriu uma combinação de hobby de desenvolvedor/malware de caos, ransomware reformulado e ransomware RaaS reempacotado.

- Trumplocker
- AlmaLocker
- Jigsaw
- Lambda
- Derialock
- Shade
- Popcorn
- Jaff

Recentemente, um autor mostrou como é fácil lançar um ataque de ransomware dentro de uma hora... **sem nenhuma habilidade de hacking**.

Então, o que isso significa para uma organização com a sua? Isso deve assustar você? Simplificando, ataques de mais origens significam mais ataques. Mas a SonicWall lhe dá cobertura.

CONTINUAR A LER >

SONICWALL®

Por que é necessário sandboxing na rede para interromper ransomware

Os firewalls de próxima geração utilizam assinaturas e heurísticas de forma muito bem-sucedida. Mas ao defender contra os ataques mal-intencionados de hoje em dia, eles não são mais suficientes. Os desafios dos ataques direcionados e das ameaças de zero-day fazem da inclusão de sandboxing uma atividade essencial para uma postura de segurança eficaz.

O crescimento das ameaças externas hoje em dia é impressionante. Os invasores combinam a natureza oportunista da automação com um conceito de fornecedor de software para evoluir suas ameaças constantemente, tudo para ter a maior amplitude possível e sem serem detectados.

E dado o impacto negativo sofrido por uma organização que sofre uma violação de dados ou um ataque de ransomware, detectar códigos mal-intencionados antes que eles impactem a rede é de extrema importância para as organizações de TI.

O desafio real não é o ransomware que já se espalhou na Internet. Os desafios reais são os ataques direcionados e as ameaças zero-day.

Os ataques direcionados envolvem códigos nunca antes vistos e criados com o propósito específico para a organização atacada, enquanto as ameaças zero-day exploram vulnerabilidades recentemente descobertas para as quais os fornecedores ainda precisam emitir patches.

As organizações precisam se preocupar mais com esses tipos de ataques, que, geralmente, são mais bem-sucedidos do que seus antigos equivalentes. Então, qual é a melhor maneira de evitar ameaças provenientes de dentro da sua rede?

Faça download do relatório gratuito do IDC para entender como o sandboxing ajuda a mitigar as ameaças avançadas.

IDC

IDC ANALYST CONNECTION

Robert Ayoub
Research Director, Security Products

Addressing Advanced Threats Through Multiple Sandbox Options

November 2016

Organizations are investing in security solutions that provide additional protection over sensitive data and increase visibility into network traffic and endpoint activity. According to IDC research, 60% of organizations surveyed indicated that modern endpoint and network security products such as sandboxes are either a high priority or an extremely high priority over the next 12 months.

The following questions were posed by SonicWALL to Rob Ayoub, Certified Information Security Systems Professional (CISSP) and research director for IDC's Security Products service, on behalf of SonicWALL's partners and customers.

Q. **Hardly a day goes by without a major breach being reported through the media, yet we see continued investment in security products and services. Why are successful attacks still occurring?**

A. There are a number of reasons why these attacks are still successful. First and foremost, there are still many vectors for attackers to exploit today; in fact, there are more vectors than ever. We've seen attackers exploiting email, websites, and social media, plus a whole host of other applications that people use to communicate with each other.

Attackers can get into an organization in many ways, such as trying to trick users into clicking links and downloading things that give the attacker access. On top of that, software is still inherently insecure and patching is difficult. Even though software developers continue to release patches on a regular basis, it's hard for organizations to do the testing to patch machines on a regular basis and for end users to keep up with all the changes to their systems. For zero-day attacks, the patch may not be available at the time of attack. In the majority of organizations, patching does not occur quickly or consistently enough to address many of the vulnerabilities being used in the wild.

Finally, while security has certainly increased in importance, and we see more spending occur for security, it's still very complex and requires significant expertise to implement properly and to keep up with the latest threats. In addition, attackers have substantial financial motivation. The FBI is predicting that ransomware victims will pay over $1 billion this year, so attackers are incented to keep their attacks fresh and stay ahead of security defenses.

US41907416

Relatório gratuito do IDC

Endereçando ameaças avançadas através de várias opções de sandbox

FAZER DOWNLOAD DO RELATÓRIO >

SONICWALL®

Detenha o ransomware com Capture ATP

O serviço SonicWall Capture Advanced Threat Protection (ATP), ou Proteção contra Ameaças Avançadas, é um sandbox multimotor, baseado na nuvem, projetado para detectar e interromper ataques desconhecidos e zero-day (por exemplo, ransomware) no gateway com remediação automatizada.

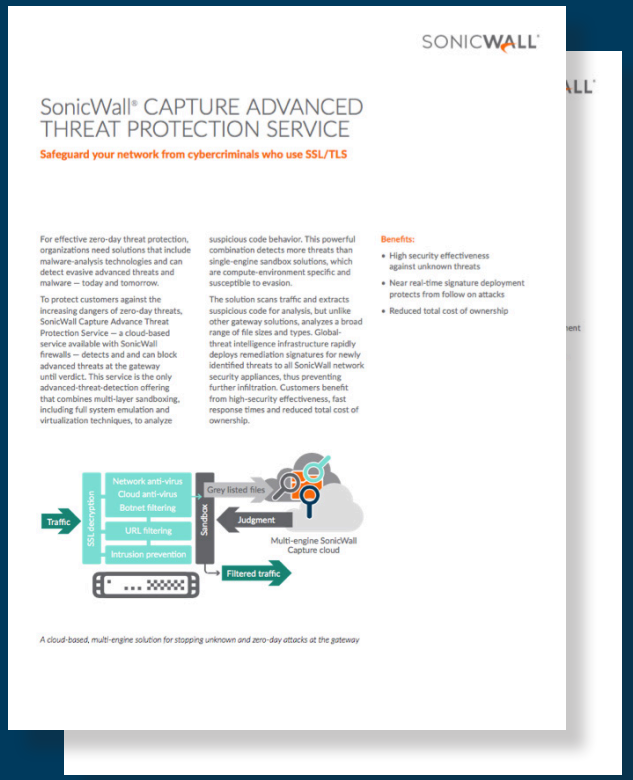
Esse serviço é a única oferta de detecção de ameaças avançadas que combina sandboxing multicamada, inclusive a emulação completa de sistema e técnicas de virtualização, para analisar o comportamento de código suspeito.

Essa eficiente combinação detecta mais ameaças do que soluções de sandbox de um único motor, que são específicas ao ambiente de computação e susceptíveis à evasão.

- **Interrupção de ransomware em tempo real**
- **Análise de uma ampla variedade de tipos de arquivo**
- **Análise de ameaças avançadas multimotor**
- **Implementação rápida de assinaturas de remediação**
- **Relatórios e alertas**
- **Bloqueio até o veredito**

Para saber mais sobre o serviço SonicWall Capture Advanced Threat Protection, faça download do datasheet ou acesse **sonicwall.com/capture**.

Como o Capture ATP funciona?


SONICWALL

SonicWall® CAPTURE ADVANCED THREAT PROTECTION SERVICE

Safeguard your network from cybercriminals who use SSL/TLS

For effective zero-day threat protection, organizations need solutions that include malware-analysis technologies and can detect evasive advanced threats and malware — today and tomorrow.

To protect customers against the increasing dangers of zero-day threats, SonicWall Capture Advance Threat Protection Service — a cloud-based service available with SonicWall firewalls — detects and and can block advanced threats at the gateway until verdict. This service is the only advanced-threat-detection offering that combines multi-layer sandboxing, including full system emulation and virtualization techniques, to analyze suspicious code behavior. This powerful combination detects more threats than single-engine sandbox solutions, which are compute-environment specific and susceptible to evasion.

The solution scans traffic and extracts suspicious code for analysis, but unlike other gateway solutions, analyzes a broad range of file sizes and types. Global-threat intelligence infrastructure rapidly deploys remediation signatures for newly identified threats to all SonicWall network security appliances, thus preventing further infiltration. Customers benefit from high-security effectiveness, fast response times and reduced total cost of ownership.

Benefits:

- High security effectiveness against unknown threats
- Near real-time signature deployment protects from follow on attacks
- Reduced total cost of ownership

A cloud-based, multi-engine solution for stopping unknown and zero-day attacks at the gateway

OBTER O DATASHEET >

SONICWALL®

Demonstração: SonicWall Capture ATP versus o mais recente malware

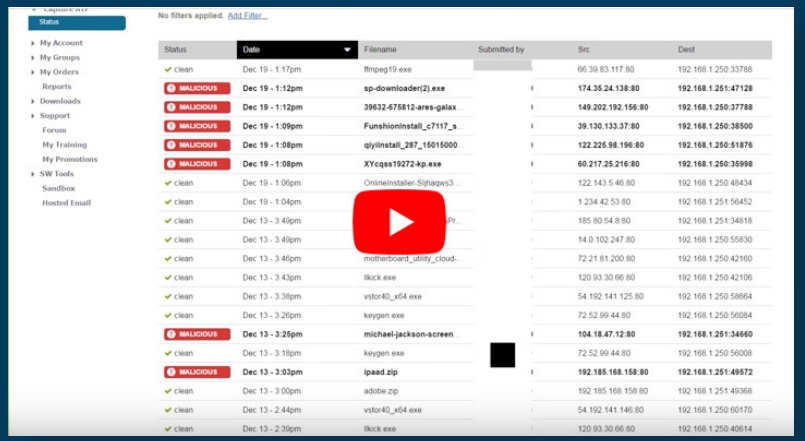
Para proteger clientes contra os perigos cada vez maiores de ameaças zero-day (por exemplo, ransomware), o SonicWall Capture Advanced Threat Protection, um serviço baseado na nuvem, disponível em todos os firewalls SonicWall, detecta e bloqueia, até o veredito, ameaças avançadas no gateway.

Quão eficiente é o Capture ATP? Pegamos os malwares mais perigosos e mais recentes de toda a Internet e os submetemos à tecnologia da SonicWall para mostrar como interrompemos ameaças avançadas do mundo real, que são implacáveis em atacar os negócios todos os dias.

Apenas com o Antivírus de Gateway (GAV) e o Capture ATP, demonstramos como o malware foi identificado e mitigado em tempo real. O Capture ATP descobre o que o malware deseja fazer, da aplicação para o sistema operacional, para o software e para o hardware.

Deste ponto, a infraestrutura global de threat intelligence rapidamente implanta assinaturas de remediação para ameaças recém-identificadas em todos os appliances de segurança de rede SonicWall, o que impede uma infiltração ainda maior.

Os clientes se beneficiam da eficácia de alta segurança, tempos de resposta rápidos e custo total de propriedade reduzido.



ASSISTIR À DEMONSTRAÇÃO COMPLETA >

SONICWALL®

Sobre nós

Em uma história de mais de 25 anos, a SonicWall tem sido a parceira de segurança confiável do setor. Desde a segurança de rede até a segurança de acesso e de e-mail, a SonicWall tem evoluído continuamente seu portfólio de produtos, o que permite que as organizações inovem, acelerem e cresçam. Com mais de um milhão de dispositivos de segurança em quase 200 países e territórios no mundo todo, a SonicWall permite que seus clientes digam sim com confiança para o futuro.

Se você tiver dúvidas sobre o possível uso deste material, entre em contato com:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Acesse o nosso site para obter mais informações.
www.sonicwall.com

Ebook-Your-Data-For-Ransom-US-IMAG-MKTG883

SONICWALL®