Malwarebytes

RESUMO DA SOLUÇÃO

Malwarebytes Endpoint Security vs. Ransomware

Derrotando a disseminação da ameaça do ransomware

O Ransomware é conhecidamente difícil de ser parado. Após infectar os dispositivos, suas vítimas enfrentam a difícil decisão entre pagar os violadores por uma chave para desbloquear os dados ou perder para sempre seus arquivos.

Um pesquisa global recente patrocinada pela Malwarebytes sobre profissionais de segurança demonstra a dimensão da ameaça comercial. Vinte e seis por cento das organizações pesquisadas foram afetados por ataques de ransomware nos últimos 12 meses.[1] Dentre os setores pesquisados, os ataques de ransomware foram mais comuns nos setores relacionados a serviços financeiros e assistência médica, incluindo bancos e seguros.

26% das organizações pesquisadas
foram impactadas por um ataque de ransomware durante os 12 meses anteriores.

Os custos decorrentes do ransomware são significativos, seja pela perda de ativos digitais ou por serem forçados a gastar mais do que o necessário. O FBI diz que ransomware é um negócio de bilhões de dólares e a Cybersecurity Ventures prevê que os custos com ransomware excederão $11,5 bilhões em 2019. Em todo o mundo quase 40% das vítimas de ransomware pagam o resgate.[2]

Contudo, o pagamento do resgate não garante que você recuperará seus dados.[3] Globalmente, cerca de 20 por cento das organizações pagaram o resgate mas perderam seus dados. Sendo assim, não é de surpreender que os profissionais de segurança estejam preocupados e digam que ransomware passou de quinta para a segunda maior preocupação entre todas as ameaças cibernéticas que tenham uma organização como alvo.[4]

Impacto econômico do ransomware

Ocupando a primeira posição na lista de custos financeiros, o ransomware representa um risco de segurança e econômico devido à interrupção das operações. Vimos o ransomware mutilar empresas: 20% das empresas param as operações imediatamente após descobrirem um ataque de ransomware. Salas de emergência em hospitais foram forçadas a negar o atendimento às pessoas; o transporte global e portos vivenciaram grandes oscilações; e mesmo o lançamento de um grande filme blockbuster teve que ser adiado por conta do resgate. A lista de vítimas é muito ampla.

Atacar organizações de saúde significa dinheiro fácil para os criminosos de ransomware. De acordo com o Ponemon Institute, os registros de assistência médica conseguem um alto preço na dark web, com registros individuais valendo em torno de $380. Isto porque os registros de saúde costumam conter dados de cartão de crédito, endereços de e-mail, número de serviço social, histórico médico e informações de emprego. Os ataques de ransomware costumam impedir o acesso aos sistemas da empresa de saúde até que o resgate seja pago. E caso o pagamento não ocorra, alguns invasores chegam a ameaçar vender o PHI no mercado negro.

Um evento pode ter um impacto catastrófico. A Hancock Health passou por isso. Eles foram atingidos pelo ransomware SamSam em 2018 e tiveram que pagar $47.000 de resgate para evitar uma interrupção em suas operações.[5]

Por que os criminosos cibernéticos o amam

Nada prospera tanto quanto o sucesso, e uma chuva de fatores de sucesso estimula o surgimento do ransomware. Como Adam Kujawa, Chefe de Inteligência de Malware da Malwarebytes, destaca: “O volume de atenção que o ransomware tem recebido da mídia é a relação mais precisa entre perigo e exposição que já experimentamos”

Em outras palavras, a alta incidência de ransomware e a ameaça real que ela representa não são exageros da mídia. Com base na análise estatística da Malwarebytes das contribuições de ransomware nos ataques de propaganda maliciosa, Kujawa diz, "os bandidos estão desistindo de outros tipos de malware e adotando o ransomware".

Simplificando, o ransomware é a arma preferencial do criminoso cibernético porque:

- **É rentável, exigindo um pagamento rápido para os criminosos, com gratificação instantânea.** Normalmente, os invasores exigem pagamento em criptomoedas, como Bitcoins. Essas moedas são, em sua maioria, anônimas e praticamente impossíveis de serem rastreadas, permitindo que os criminosos cibernéticos lavem seus ganhos ilícitos em sua moeda local. E assim como as grandes empresas legítimas, as empresas de ransomware às vezes oferecem "atendimento ao cliente", cujos prestativos representantes acompanham as vítimas no processo de compra de uma criptomoeda adequada.
- **É fácil de usar, e está ficando cada vez mais fácil.** Ransomwares desenvolvidos por criminosos experientes estão encontrando seu caminho no mercado on-line, oferecendo ransomware como um serviço (RaaS) para golpistas menos aptos tecnicamente. Na verdade, os desenvolvedores de ransomware estão terceirizando seu malware para uma rede de distribuição composta por script kiddies (hackers inexperientes), para que os aplicativos possam ser implementados de forma imediata, em troca de uma porcentagem da participação do desenvolvedor original do ransomware.[6]
- **Se defender de ransomwares é muito difícil.** De acordo com uma pesquisa patrocinada pela Malwarebytes sobre executivos em funções relacionadas a TI,[7] os entrevistados nos EUA estavam mais preocupados com a infiltração de malware por meio de e-mail e navegação na internet. Por exemplo, abrir um anexo de e-mail contendo um exploit permite que o malware se aproveite de todos os pontos fracos encontrados em softwares comuns no sistema e libere o ransomware. Propagandas maliciosas escondem armadilhas de código malicioso em sites confiáveis, que podem baixar ransomwares mesmo que os visitantes não cliquem nos anúncios infectados. Considere que em 2018, a Google reportou que removem 100 anúncios infectados por segundo, totalizando mais de 3.2 bilhões de anúncios no ano anterior.[8] Na verdade, de acordo com pesquisadores de ameaças da Malwarebytes, estima-se que 70 por cento das campanhas com propaganda maliciosa disseminam ransomware como payload.

Revidando com o Malwarebytes Endpoint Security

A maioria dos softwares de segurança de hoje oferecem eficácia limitada contra o ransomware. O ransomware não age como o malware tradicional: alguns tipos são atualizados automaticamente todos os dias e até usam código polimórfico (que mudam de forma) para desviar da detecção. Isso dificulta muito sua detecção, especialmente porque as soluções tradicionais e antigas de plataforma de proteção de endpoints usam tecnologias estáticas que dependem de assinaturas que simplesmente não conseguem identificar os comportamentos em evolução da atividade de ransomware. Além disso, o ransomware encontrado hoje é tão sofisticado que a criptografia avançada que ele usa torna impossível recuperar os arquivos sem pagar o resgate.

Infelizmente, os sistemas de backup online e conectados localmente usados como uma contra medida eficaz podem falhar, porque o ransomware procura intensamente por diferentes tipos de sistemas de backup e criptografa os arquivos salvos. No caso de backups on-line, o upload automático de arquivos pode corromper arquivos que o usuário acredita que permanecerão seguros.

Em contraste, o Malwarebytes Endpoint Security é projetado para combater—e derrotar—ransomwares avançados que outras soluções de segurança não veem. Ele é implantado pelas redes corporativas e protege endpoints contra malwares e outras ameaças avançadas graças a uma poderosa combinação de várias camadas de tecnologias pró-ativas heurísticas, sem assinatura e comportamentais.

Além disso, o Malwarebytes Endpoint Security oferece outra camada de proteção contra ataques baseados em ransomware, com uma nova tecnologia dedicada criada do zero para detectar e bloquear todos os ransomwares, conhecidos e desconhecidos, de criptografarem os arquivos dos usuários. Isso difere dos esforços anti-ransomware de outras soluções de segurança de endpoints, se é que elas existem, que normalmente consistem em tecnologias antigas costuradas uma na outra e que já se mostraram ineficazes.

Malwarebytes Endpoint Security quebra a cadeia de ataque do ransomware com uma abordagem de quatro camadas:

1. A camada anti-ransomware do Malwarebytes Endpoint Security monitora constantemente os sistemas de endpoint e elimina automaticamente os processos associados à atividade de ransomware. Ele possui um mecanismo dedicado de detecção em tempo real que não usa assinaturas nem requer atualizações. Além disso, ocupa um pequeno espaço no sistema e é compatível com soluções de segurança de terceiros.

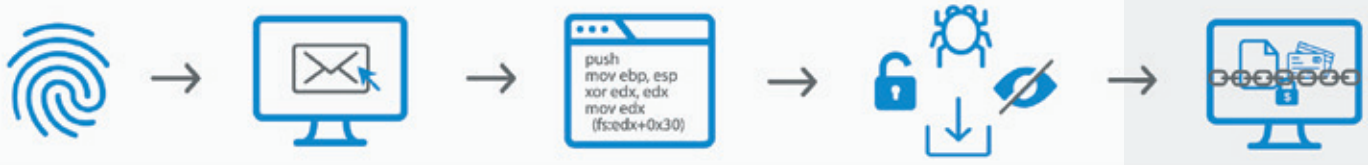
2. A camada anti-exploit bloqueia proativamente os exploits antes que possam liberar seu payload de malware. Ele envolve aplicativos e navegadores vulneráveis em camadas de defesa projetadas para interromper ataques de dia zero logo no início. Usando tecnologia sem assinatura que identifica comportamentos característicos de um exploit, o anti-exploit pode até mesmo proteger contra malwares e ransomwares não identificados que outras tecnologias não conseguem detectar porque não foram previamente expostas a eles.

3. A camada anti-malware da Malwarebytes Endpoint Security emprega regras heurísticas e comportamentais para detectar e remover em tempo real malwares de todo tipo, para que ele não possa executar seu código.

4. A camada de bloqueio de sites maliciosos interrompe o acesso a servidores conhecidos e suspeitos de comando e controle, para que o ransomware não consiga obter as chaves de criptografia ou acessar e baixar o arquivo .exe do ransomware.

Quebrando a cadeia de ataque do ransomware com Malwarebytes

Veja como as tecnologias do Malwarebytes Endpoint Security bloqueiam um ataque de ransomware enviado por exploit de propaganda maliciosa. A melhor maneira de explicar isso é observando as várias etapas da cadeia de ataque do ransomware:



1. Determinação de perfil
2. Entrega
3. Exploração
4. Execução de payload
5. Comportamento malicioso

Determinação de perfil
O invasor faz o reconhecimento do seu endpoint através de um banner de anúncio infectado, tentando identificar seu SO, tipo de navegador, endereço IP e programa de segurança de endpoint.

Tecnologia Malwarebytes: Proteção de aplicativos reduz a superfície da vulnerabilidade, tornando o computador mais resiliente, e detecta proativamente as tentativas de rastreio feitas por ataques de exploit avançados. (Sem assinatura)

Entrega
Como o invasor coloca seu exploit e payload no seu endpoint.

Tecnologia Malwarebytes: Proteção Web protege os usuários ao prevenir o acesso a websites maliciosos, redes de publicidade, redes scammer e "áreas perigosas".

Exploração
O invasor explora um código vulnerável em seu navegador, Adobe Flash, Microsoft Word, etc., para entregar e executar remotamente o payload do ransomware.

Tecnologia Malwarebytes: A mitigação de exploit detecta e bloqueia de forma proativa tentativas de abusar de vulnerabilidades e executar remotamente um código na máquina, que é um dos principais vetores de infecção hoje em dia. (Sem assinatura)

O comportamento da aplicação garante que as aplicações instaladas se comportem corretamente e impede que sejam utilizadas para infectar a máquina. (Sem assinatura)

Execução de payload
O invasor entrega e executa o payload do ransomware no seu sistema.

Tecnologia Malwarebytes: A análise de Payload é composta de regras heurísticas e comportamentais para identificar famílias completas de malware conhecidos e relevantes.

Comportamento malicioso
O ransomware é ativado no seu sistema. Ele entra em contato com um servidor de comando e controle para baixar as chaves criptográficas e, em seguida, criptografa seus arquivos.

Tecnologia Malwarebytes: Mitigação de ransomware é uma tecnologia de monitoramento do comportamento que detecta e bloqueia ransomwares de criptografar arquivos do usuário (sem assinatura). Proteção de retorno de chamada evita o acesso a servidores de comando e controle (C&C) e websites maliciosos.

Resumo

À medida que mais dispositivos são conectados ao vasto panorama de alvos conhecido como Internet das coisas (IoT), o ransomware representará uma ameaça cada vez maior às vítimas. Especialmente dado que os especialistas preveem que continuaremos observando várias novas variantes de ransomware por toda parte.

Malwarebytes Endpoint Security é uma plataforma de proteção de endpoint que protege proativamente seus endpoints contra ameaças conhecidas e desconhecidas. O Malwarebytes Endpoint Security adicionou uma camada adicional de proteção contra ataques baseados em ransomware com uma exclusiva tecnologia anti-ransomware que monitora, detecta e bloqueia o ransomware automaticamente antes mesmo que ele toque nos arquivos do usuário. Além de lidar com ameaças conhecidas, como Cryptolocker, CryptoWall ou CTBLocker, ele acaba com novos ransomwares no momento em que são lançados, protegendo proativamente os usuários contra ransomwares que nunca foram vistos antes.

Os benefícios do Malwarebytes Endpoint Security para os clientes empresariais são:

- Reduzir a vulnerabilidade a ataques de ransomware. Detecta e bloqueia automaticamente ransomwares desconhecidos e conhecidos, em vez de apenas alertar o usuário por meio de um e-mail automático de que há um ataque, como fazem alguns produtos de segurança.
- Bloqueia a criptografia em tempo real. Interrompe o ransomware antes que ele possa iniciar, eliminando a necessidade de ferramentas de descriptografia complicadas e, muitas vezes, ineficazes.
- Funciona contra ransomware de dia zero (não identificado anteriormente), empregando tecnologia especializada de monitoramento de comportamento que protege contra novos ransomwares que outras tecnologias não conseguem detectar porque não foram expostos a eles anteriormente.
- Emprega um projeto único feito do zero para derrotar o ransomware com mais rapidez e eficiência. A Malwarebytes construiu esta tecnologia a partir do zero para se defender contra o ransomware. Outras soluções ou recursos anti-ransomware dependem de tecnologias obsoletas ou de uma coleção de tecnologias adaptadas que foram originalmente montadas para fazer outra coisa.
- Usa tecnologia sem assinatura nas camadas anti-ransomware e anti-exploit, de modo que a proteção seja eficaz até mesmo contra novos ransomwares que ainda não possuem uma assinatura.
- Preserva a reputação de uma empresa, permitindo evitar o pesadelo de relações públicas que geralmente acompanha um ataque ou uma violação.
- Protege a receita da empresa, que seria utilizada para resgatar dados criptografados.

RECURSOS DO WEBSITE

Para mais informações sobre o Malwarebytes Endpoint Security e a nova tecnologia ransomware, acesse: br.malwarebytes.com/business/endpointsecurity/

Notícias recentes: br.blog.malwarebytes.com/

Referências

[1]*Pesquisa publicada em agosto de 2018 pela Osterman Research, Inc.*
[2]*CyberEdge Group. 2018 Cyberthreat Defense Report. 2018.*
[3]*CyberEdge Group. 2018 Cyberthreat Defense Report. 2018.*
[4]*CyberEdge Group. 2018 Cyberthreat Defense Report. 2018.*
[5]*HealthcareITNews. Hancock Health paga regate de $47.000 para desbloquear dados de pacientes. 2018.*
[6]http://www.techrepublic.com/article/ransomware-as-a-service-is-exploding-be-ready-to-pay/
[7]*Pesquisa realizada em junho de 2016 e publicada em agosto de 2016 pela Osterman Research, Inc.*
[8]*Google. Um ecossistema publicitário que funcione para todo mundo. 2018.*

br.malwarebytes.com/business corporate-sales@malwarebytes.com +55.11.4280.6661

A Malwarebytes protege de forma proativa as pessoas e as empresas contra as ameaças perigosas, tais como malware, ransomware e exploits que escapam à detecção das soluções tradicionais de antivírus. O Malwarebytes substitui completamente os antivírus com tecnologia respaldada por inteligência artificial que interrompe ciberataques antes que eles possam comprometer computadores domésticos e endpoints empresariais. Saiba mais em br.malwarebytes.com.