Cinco ameaças cibernéticas que burlam o antivírus tradicional

eBook

Cinco ameaças cibernéticas que burlam o antivírus tradicional

O primeiro vírus de computador documentado foi o Creeper, em 1971. Desenvolvido em um ambiente acadêmico, o vírus foi criado para demonstrar a capacidade de um arquivo de se propagar através de uma rede. Demorou seis meses até que os programadores desenvolvessem um programa de antivírus de sucesso que foi batizado de Reaper. Esse foi o primeiro registro de defasagem entre a ameaça e a defesa.

Desde então, profissionais de segurança e programadores vivem o jogo de gato e rato com os cibercriminosos. Como setor da indústria, detectamos ameaças, atualizamos nossas defesas, repetindo o ciclo quantas vezes necessário.

Muitos programas de antivírus (AV) tradicionais operam com base em assinaturas. Conforme um software malicioso é descoberto, uma assinatura que descreve esse arquivo é gerada, adicionada a um banco de dados e, em seguida, o banco de dados é enviado para a base de clientes. Se o antivírus descobrir um arquivo em sua máquina que corresponda a uma assinatura, esse arquivo é posto em quarentena e/ou removido. Em dezembro de 2018, o malware estava sendo identificado a uma taxa alarmante de 350.000 novas ameaças por dia1. Com esse número em franca expansão, é difícil para as soluções de AV baseadas em assinatura acompanharem esse volume, deixando os dispositivos, muitas vezes, vulneráveis.

Ao longo do tempo, temos visto o surgimento de novas defesas. No entanto, cada defesa desencadeia uma mudança correspondente nas táticas dos criminosos. Essas mudanças incluem malware projetado não apenas para explorar vulnerabilidades, mas também para enganar as defesas de um AV. Dada a nova realidade de trabalho em home office durante a pandemia de COVID-19, proteger dispositivos que estão literalmente fora das dependências da rede corporativa é agora crucial.

Brechas na cibersegurança são mais prováveis de ocorrer em um ambiente de home office com usuários sem formação adequada. Isso pode ter impacto não somente nos dados do usuário, mas de toda a corporação. E isso geralmente leva também à responsabilização dos provedores de serviços gerenciados (MSPs). E tende a ficar pior. A Morphisec constatou que 20% dos trabalhadores não receberam nenhuma orientação de TI ao migrarem do escritório para suas residências2. Uma boa postura de segurança tornou-se mais importante do que nunca.

Somando a esse perigo inerente, informações recentes esclarecem como o evento do coronavírus abriu oportunidades para novos ataques. De acordo com relatórios da RiskIQ, a cada minuto, 35 novos e-mails de spam são analisados e 14,6 hosts relacionados à COVID são criados3. Além disso, um domínio relacionado à COVID-19 é bloqueado a cada 15 minutos4.

[1] "Malware," AV-TEST. https://www.av-test.org/en/statistics/malware/ (acessado em setembro de 2020).

[2] "Increasing Cybersecurity Gaps and Vulnerabilities due to Remote Work During COVID-19," Security Magazine. securitymagazine.com/articles/92571-increasing-cybersecurity-gaps-and-vulnerabilities-due-to-remote-work-during-covid-19 (acessado em setembro de 2020).

3 "Evil Internet Minute 2020", RiskIQ. riskiq.com/resources/infographic/evil-internet-minute-2020/ (acessado em setembro de 2020).

4 "Evil Internet Minute 2020", RiskIQ. riskiq.com/resources/infographic/evil-internet-minute-2020/ (acessado em setembro de 2020).

Aqui estão cinco tipos de ataques que conseguem escapar das garras do AV tradicional.

1. Malware polimórfico

Como mencionado na introdução, muitos programas de AV tradicionais dependem da detecção baseada em assinatura. Isso envolve a comparação de um arquivo com uma entrada de dados conhecida, chamada de assinatura, em um banco de dados de ameaças identificadas.

Este estilo de proteção tem algumas falhas. Primeiro, o usuário do AV deve ter a lista mais recente de assinaturas, o que exige fazer atualizações frequentes. Se esse usuário não mantiver suas definições de vírus atualizadas, estará indefeso contra arquivos mais recentes. Além disso, esse método de proteção é puramente reativo. A empresa de AV deve conhecer a existência da assinatura antes que possa sinalizá-la para sua base de usuários. Além disso, o malware geralmente usa técnicas de evasão para evitar a detecção por empresas de AV.

A principal falha aqui é que muitas vezes há uma lacuna de conhecimento ou de tempo na cobertura. O malware polimórfico foi projetado para explorar essa falha. Se, por exemplo, o malware for detectado por um programa AV, ele se regenerará usando novas características que não correspondem a assinaturas conhecidas. Isso torna difícil para o AV baseado em assinatura realmente deter a infecção. Além disso, existem cerca de 350.000 novas variantes de malware sendo criadas a cada dia5. Isso garante que aqueles que usam AV baseado em assinatura estarão quase sempre a salvo.

2. Documentos armados

Os criminosos muitas vezes exploram falhas em diferentes formatos de documentos para comprometer um sistema. Esses documentos normalmente usam scripts incorporados. Os ofensores ofuscam o código ou script no interior desses documentos armados. Parece inofensivo até mesmo para um olhar experiente. Assim passará pelo AV, que só verifica o documento inicial, em vez do código ou script depois que este é executado. Após ser iniciado, o ataque é executado em segundo plano, sem o conhecimento do usuário.

Os criminosos podem usar os arquivos Adobe® PDF com JavaScript® incorporado para executar comandos do sistema operacional ou baixar arquivos executáveis para comprometer dispositivos e redes acessados. Os hackers costumam usar scripts incorporados para executar comandos PowerShell® e, devido a sua integração ao sistema operacional Windows®, esses ataques podem danificar terminais e até mesmo redes inteiras. No entanto, os PDFs não são os únicos tipos de arquivos vulneráveis. Documentos baseados em XML, HTML e do Office® podem geralmente carregar esses scripts maliciosos escondidos dentro deles. Uma solução de AV com base na comparação de assinaturas executáveis vai ignorar documentos armados, pois irá verificar apenas o documento inicial e não o código malicioso que o documento inicializará depois.

[5]"Malware," AV-TEST. av-test.org/en/statistics/malware/ (acessado em setembro de 2020).

3. Downloads induzidos por navegador

Downloads induzidos são arquivos baixados para o terminal, tirando proveito das vulnerabilidades do navegador ou de uma extensão de navegador. Isso faz o arquivo ser baixado, e o usuário e seu programa de AV nem percebem. O download pode vir de um site legítimo com um script comprometido ou serviço de publicidade, ou pode ser um site malicioso especificamente configurado para iniciá-lo. Esses ataques começam por um e-mail ou phishing social, anexos de e-mail ou links de pop-up bem disfarçados para atrair usuários para um determinado site. Os criminosos, em seguida, aproveitam-se de exploits em navegadores ou plugins para baixar malware e dar início ao ataque. Após essa etapa ser concluída, o criminoso pode começar a causar estragos, seja instalando um componente de criptomineração, um trojan de acesso remoto ou um ransomware.

4. Ataques sem arquivo

A maioria dos programas de antivírus fazem a inspeção dos arquivos quando são gravados no dispositivo. No entanto, se não há um arquivo, o programa de AV normalmente não pode detectar o comportamento malicioso.

Ataques sem arquivo ocorrem sem a instalação de uma carga útil real em um sistema, tornando-os extremamente difíceis de serem detectados pelo antivírus. Eles normalmente são executados na memória do terminal e usam PowerShell, rundll32.exe ou outros recursos incorporados do sistema para infectar máquinas.

Ataques sem arquivo muitas vezes podem começar com documentos ou scripts maliciosos em um site, mas isso certamente não é a única maneira com a qual eles infectam máquinas. Por exemplo, quando um terminal permite o protocolo de desktop remoto (RDP), cria uma porta aberta de escuta na máquina que permite a alguém se conectar a ela e começar a executar processos maliciosos, incluindo o download de malware baseado em arquivos, adulteração de registro ou roubo de dados.

Como se isso já não fosse assustador o bastante, a SentinelOne® detectou um aumento de 91% em ataques de malware sem arquivo no primeiro semestre de 20186. À medida que esses ataques tornam-se mais preponderantes, as empresas precisam ir além da detecção baseada em arquivos para proteger melhor seus ativos e dados.

[6] "Fileless Malware Attacks | How They Can Be Detected and Mitigated", SentinelOne. sentinelone.com/blog/fileless-malware-attacks-can-detected- mitigated/ (acessado em setembro de 2020).

5. Malware ofuscado

Anteriormente, abordamos como os profissionais de segurança e pesquisadores vivem constantemente um jogo de gato e rato com os criminosos. Empresas de AV fazem uso de diversos métodos para detectar a presença de malware. Um método de detecção comum envolve a execução de arquivos em ambientes sandbox e a observação de comportamento malicioso. Outro método de detecção comum envolve a verificação do código em busca de sinais comuns de intenção maliciosa.

Os cibercriminosos encontraram maneiras de contornar isso. Da mesma maneira que os profissionais de segurança implementam defesas para proteger seus dados e ativos, os hackers também têm maneiras de proteger a carga maliciosa dentro de uma porção de malware.

Malware mais recente detectará um ambiente sandbox e permanecerá benigno dentro dele, pronto para atacar somente em um cenário ao vivo. Isso pode tornar impossível para o AV detectar métodos comportamentais no ambiente sandbox.

Outro método para enganar o AV envolve “empacotadores”, que usam criptografia ou compressão para impedir que o interior do arquivo seja visualizado. Além disso, os desenvolvedores de malware podem empacotar o código malicioso dentro do código benigno em um arquivo, ocultando assim o código maligno.

Para começar, qualquer uma dessas técnicas torna difícil para os pesquisadores de segurança detectar (e entender) a natureza desses arquivos maliciosos. Além disso, se você usa um programa antivírus que executa varreduras heurísticas dentro de um ambiente sandbox, essas técnicas ajudam o malware a escapar da detecção antes de entrar em operação em uma máquina.