RELATÓRIO SOBRE AMEAÇA CIBERNÉTICA: RECONNAISSANCE 2.0

Os invasores desenvolveram um arsenal de ferramentas e técnicas para invadir as redes das organizações e roubar informações valiosas. Este relatório revela as táticas mais recentes usadas pelos agentes de ameaças para não serem detectados durante a realização de reconhecimento interno. Também explica como a automação permitiu que hackers amadores realizassem reconhecimentos avançados e acelerassem seus ataques.

Invasores em busca de dados valiosos

Os ataques direcionados geralmente começam nos pontos mais fracos das defesas das organizações: seus endpoints. A etapa inicial de um ataque direcionado pode ser tão simples quanto convencer um usuário a abrir um anexo de e-mail. Com 4% dos usuários que caem em qualquer campanha de phishing[1] e invasores capazes de enviar uma infinidade de e-mails de phishing, e também de executar outros inúmeros ataques (de explorações de dia zero a ataques de engenharia social), as intrusões podem atingir até as organizações mais bem fortificadas.

Depois de comprometerem o endpoint, os invasores estabelecem um canal de comunicação com um servidor de controle e comando (C2). Em seguida, começam a explorar o ambiente circundante, enquanto buscam ativos valiosos. Durante a fase de reconhecimento interno, eles podem buscar caminhos que levem a becos sem saída, mas continuarão tentando novos caminhos até atingir seu objetivo.

Para evitar a detecção, os agentes de ameaça atualizam continuamente suas ferramentas e métodos. Eles aproveitam novas técnicas para reconhecer o terreno e localizar os principais ativos, como servidores do Active Directory®, servidores de arquivos e bancos de dados.

Por anos, os invasores usaram uma combinação de scanners de porta, malware, ferramentas de hacking e tentativa e erro para mapear as redes visadas e ampliar seu acesso quando conseguem entrar em uma rede. Hoje, muitos invasores expandiram seus repertórios de técnicas de reconhecimento interno para incluir aquelas mostradas na Figura 1.

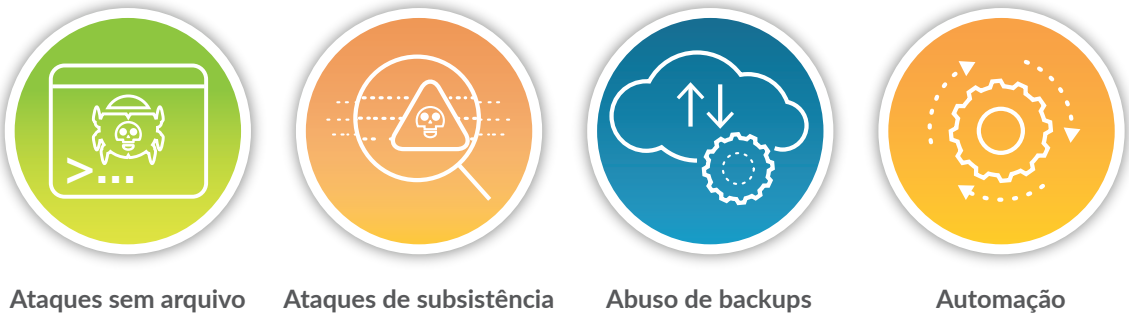

Figura 1: Algumas técnicas de reconhecimento interno

Essas técnicas de reconhecimento interno permitem que os agentes de ameaças encubram suas atividades e acelerem seus ataques. Então, como elas funcionam? Mais importante, podemos detectar e interromper esses ataques antes que o dano aconteça? Acreditamos que a resposta é um retumbante "sim".

Ataques sem arquivo

À medida que as tecnologias de segurança melhoram na detecção de malware, os agentes de ameaças recorrem a ataques sem arquivos para comprometer endpoints e realizar o reconhecimento interno sem ativar os alarmes. As técnicas de ataque sem arquivo incluem o seguinte:

- Malware apenas de memória
- Malware e ferramentas baseadas em script
- Incorporação de código malicioso em arquivos benignos

Os agentes de ameaça usam ataques sem arquivo, pois assim eles têm muito mais chances de sucesso do que com malwares tradicionais baseados em arquivos. Na verdade, de acordo com uma pesquisa recente, 77% dos ataques bem-sucedidos resultaram de ataques ou explorações sem arquivos, enquanto apenas 23% dos comprometimentos foram atribuídos a ataques baseados em arquivos.[2]

Os ataques sem arquivo podem evadir os controles de segurança porque o software antivírus tradicional foi projetado para analisar arquivos e buscar atributos ou funções de arquivos, a fim de determinar se são maliciosos. No entanto, com um ataque sem arquivo, não há um arquivo tradicional para o antivírus fazer a varredura ou análise, permitindo que um invasor drible a detecção estática baseada em disco.

__77%__ dos ataques bem-sucedidos foram resultado de ataques sem arquivo ou explorações.

Os invasores podem começar com uma exploração distribuída por meio do tráfego da Web ou de e-mail, como um arquivo do Adobe® Flash® malicioso, um macro em uma planilha ou até mesmo uma cadeia JavaScript especialmente desenvolvida, que aproveita uma vulnerabilidade do endpoint para executar um código malicioso.

1. "Relatório de investigações sobre violação de dados de 2018", Verizon, março de 2018, https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.
2. "Relatório sobre o estado de risco da segurança do endpoint 2017", Ponemon Institute, outubro de 2017, https://www.barkly.com/ponemon-2018-endpoint-security-statistics-trends#form.

Os invasores podem então abusar das ferramentas internas do Windows®, como PowerShell® e Windows Management Instrumentation, ou outras ferramentas, como Metasploit®, para transferir malware de um local remoto e carregá-lo na memória. O conteúdo do malware nunca é gravado no disco, mas reside em áreas voláteis do sistema, como processos em memória ou áreas de serviço. O malware apenas de memória é especificamente eficaz em servidores e dispositivos de rede que são reinicializados com pouca frequência.

Os invasores também usam malwares baseados em script, geralmente em conjunto com malwares apenas de memória, para executar comandos nas máquinas visadas. Como os scripts são arquivos de texto não estruturado, as ferramentas de segurança não podem usar facilmente as assinaturas de ataque para detectá-los. Os invasores podem facilmente modificar parâmetros, nomes ou a ordem do código de script para frustrar a detecção de assinatura.

Por fim, os invasores podem incorporar códigos maliciosos em arquivos bem conhecidos, especialmente aplicativos gratuitos ou de código aberto que não são assinados digitalmente. Eles podem até injetar código nos processos em execução. Se as ferramentas antivírus detectarem funções maliciosas nesses arquivos legítimos, os analistas de segurança geralmente presumem que os alertas são falsos positivos em vez de se concentrarem em ameaças aparentemente mais prioritárias. Depois que os invasores comprometerem um endpoint com um ataque sem arquivo, eles podem atravessar a rede para encontrar e transferir dados.

__30%__ de todos os ataques em 2017 foram sem arquivo. Em 2019, espera-se que seja __38%__.

Os kits e as estruturas de exploração pré-embalados tornaram os ataques sem arquivos muito mais fáceis de implantar e mais comuns no atual cenário de ameaças. De todos os ataques de 2017, 30% foram sem arquivo, e espera-se que esse número aumente para 38% em 2019.[3]

Ataques de subsistência

Depois que os invasores exploram um endpoint (geralmente com um ataque sem arquivo), eles tentam localizar, roubar, manipular ou destruir os dados. Em vez de chamar a atenção para si mesmos ao instalar malware ou ferramentas de ataque, os invasores furtivos usam aplicativos já existentes nas máquinas das vítimas para fazer o reconhecimento. Esses aplicativos são confiáveis e usados para atividades diárias legítimas, logo os invasores os podem usar em vários estágios durante o ciclo de vida do ataque, inclusive no reconhecimento interno, evitando a detecção.

O ataque de subsistência também consiste em abusar de serviços bem conhecidos, como GitHub®, Pastebin, Twitter®, Box ou mesmo Microsoft® Office 365®. Os invasores usam esses serviços para encontrar dados confidenciais em aplicativos online de e-mail e de compartilhamento de arquivos. Eles também usam esses serviços para C2, bem como para a transferência não autorizada de dados.

Para pesquisar a rede, os invasores perspicazes aproveitam os aplicativos da rede (como o Ping, o NetStat e o IPConfig), além de ferramentas da área de trabalho remota e utilitários de administração. Se, por acaso, os invasores comprometerem as máquinas dos administradores de TI, eles ganham a "bolada" de um "ataque de subsistência", e geralmente podem assumir o comando de vários aplicativos e credenciais que podem ajudá-los a atingir seus objetivos fraudulentos.

As equipes de segurança não conseguem desinstalar facilmente todos esses aplicativos. Agravando os riscos de segurança, os invasores de ataques de subsistência geralmente burlam o software de antivírus tradicional e as ferramentas de lista branca dos aplicativos, porque os invasores não instalaram novos arquivos no sistema. Como resultado, não há assinaturas para serem detectadas pelas ferramentas de antivírus e poucos vestígios de atividades que possam ser usados para a análise forense.

Abuso de backups

Muitas organizações investem quantias exorbitantes de recursos na proteção de seus aplicativos confidenciais. Elas implantam firewalls, autenticação forte, prevenção de ameaças, proteção de endpoint, e, muito mais, para proteger seus aplicativos e dados. No entanto, essas organizações preocupadas com a segurança normalmente não ampliam as práticas recomendadas de segurança cibernética aos servidores de backup. Eles geralmente consideram a proteção por senha e a correção regular como controles de segurança suficientes. Como resultado, os servidores de backup podem fornecer tesouros de dados facilmente acessíveis a hackers inescrupulosos.

Como exemplo, "Phineas Fisher", o autoproclamado hacker da HackingTeam, empresa de TI com sede em Milão, relatou que usou servidores de backup para obter acesso a várias máquinas virtuais, incluindo

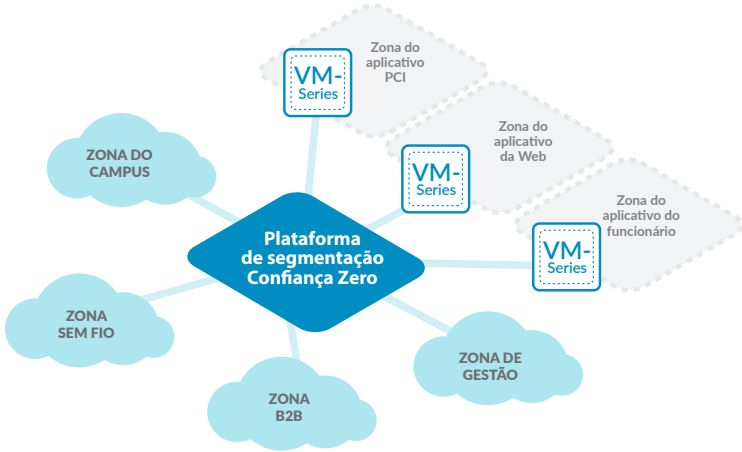

Figura 2: Modelo de Confiança Zero

3. "Relatório sobre o estado de risco de segurança do endpoint 2018", Ponemon Institute, acessado em fevereiro de 2019, https://www.barkly.com/ponemon-2018-endpoint-security-risk-report.

ao servidor de e-mail do Exchange da HackingTeam. Em seu guia Hack Back! Fisher afirmou: "Seus backups não protegidos foram a vulnerabilidade que abriu suas portas". O ataque da HackingTeam não foi o primeiro a explorar sistemas de backup desprotegidos, mas aumentou a conscientização entre a comunidade Black Hat sobre o uso de sistemas e serviços de backup para localizar e roubar dados.

Como os servidores de backup contêm versões anteriores de dados ativos, eles devem ser protegidos com o mesmo nível de segurança que os servidores e aplicativos ativos. As organizações devem implementar o modelo de Confiança Zero, usando políticas de segmentação e granulares de rede e firewall para limitar o acesso a usuários autorizados. Elas também devem implementar a autenticação multifatorial para impedir que invasores acessem dados de backup com credenciais roubadas. Por último, as organizações devem monitorar o acesso a dados de backup para detectar atividades incomuns, como um usuário fazendo download de um grande volume de dados ou o download de dados por um usuário sem fazer upload ou a sincronização de nenhum dado.

Automação

No passado, apenas os criminosos cibernéticos mais sofisticados e os invasores patrocinados pelo estado podiam realizar ataques direcionados. Agora, até mesmo o hacker mais principiante pode realizar ataques multifásicos usando uma combinação de ferramentas de ataque, scripts e compartilhamento de informações. A automação também permite que os invasores façam o reconhecimento mais rápido do que nunca.

As ferramentas de teste de penetração, como o Metasploit e o PowerShell Empire, simplificaram os ataques direcionados. Embora essas ferramentas não sejam realmente novas, o Metasploit foi introduzido pela primeira vez em 2003, novos recursos foram incluídos ao longo do tempo para explorar sistemas, descobrir novas vulnerabilidades e auxiliar hackers Black ou White Hat em cada etapa de um ataque. Com muitas dessas ferramentas sendo exaltadas em comunidades online ativas, elas estão sendo continuamente aprimoradas para incluir novos recursos e explorações.

```
+------------------+-------------------------------------------------+
|     Option       |                  Summary                        |
+------------------+-------------------------------------------------+
|1. Usage          | Display this informational message.             |
|2. Gather Hosts   | Query Shodan for a list of platform specific IPs.  |
|3. View Hosts     | Print gathered IPs/RHOSTS.                      |
|4. Exploit        | Configure MSF and Start exploiting gathered targets|
|5. Quit           | Exits AutoSploit.                               |
+------------------+-------------------------------------------------+
```

Figura 3: O AutoSploit simplifica o reconhecimento e a exploração do sistema

Mais recentemente, os desenvolvedores incluíram interfaces gráficas de usuário e recomendações sobre exploração com suas ferramentas, tornando os testes de penetração e o hacking mais fáceis do que nunca. Os desenvolvedores também incluíram scripts integrados que permitem que até mesmo os testadores de penetração mais principiantes e hackers executem seus ataques. Por exemplo, o AutoSploit, introduzido no início de 2018, automatiza muitas das etapas manuais de um ataque, permitindo que praticamente qualquer invasor execute um ataque multifásico. O AutoSploit combina Metasploit e Shodan®, um mecanismo de pesquisa para dispositivos conectados à Internet, permitindo que invasores localizem e explorem sistemas, como dispositivos inseguros da IoT.

Embora os especialistas em guerra cibernética possam preferir ataques furtivos e manuais, a automação de ataques coloca ataques avançados ao alcance de invasores menos sofisticados. Ela também permite que os invasores detectem e explorem vulnerabilidades recém-divulgadas muito rapidamente, obrigando as organizações a fazerem a correção dos sistemas com a mesma rapidez. Com os invasores usando cada vez mais automação, as equipes de segurança precisam fortalecer suas defesas e automatizar a detecção para ultrapassar os ataques.

Proteção da sua organização contra o reconhecimento

O reconhecimento interno da rede é um componente essencial da maioria dos ataques direcionados, entretanto também é quando os invasores ficam mais expostos. Para os agentes de ameaça, a invasão inicial é, frequentemente, apenas o primeiro passo. Depois de penetrarem em uma rede, eles precisam realizar milhares de ações individuais enquanto exploram a rede e se movimentam lateralmente até acessarem os dados visados. Se os defensores puderem coletar e analisar os sinais que essa atividade universal de invasores emite, eles poderão se antecipar aos agentes de ameaça.

Figura 4: A Palo Alto Networks bloqueia ameaças em todo o ciclo de vida do ataque

Com a tecnologia certa, acreditamos que as equipes de segurança podem impedir ataques cibernéticos bem-sucedidos. Ao caracterizar automaticamente o perfil do usuário e o comportamento do dispositivo, as equipes de segurança podem detectar comportamentos incomuns indicativos de reconhecimento interno e as outras fases de um ataque direcionado. As equipes de segurança só precisam detectar uma das muitas ações que os agentes de ameaças executam para identificá-los, bloqueá-los para que não entrem na rede e para interromper o ataque.

Proteger sua organização com o Cortex XDR

A detecção e resposta baseada em nuvem do Cortex XDR ™ é um aplicativo que permite que você interrompa ataques sofisticados e adapte as defesas para evitar futuras ameaças. O Cortex XDR descobre com precisão ameaças ao analisar seus dados de rede, endpoint e nuvem com o aprendizado de máquina. Ele fornece um retrato completo de cada incidente e revela a causa raiz para acelerar as investigações. A forte integração com pontos de aplicação acelera a contenção, permitindo que você interrompa os ataques antes que o dano aconteça.

O Cortex XDR encontra o reconhecimento interno mesmo quando os agentes de ameaças não usam malware, porque ele identifica mudanças no comportamento da rede. Como resultado, o Cortex XDR pode capturar invasores de ataques de subsistência, que abusem dos backups ou que realizam reconhecimento automatizado. O Cortex XDR também pode detectar invasores que usam ataques sem arquivos e scripts para se movimentarem de um host para outro dentro da rede.

O Cortex XDR integra os dados da rede, endpoint e nuvem para criar um retrato completo de cada incidente. Combinando dados de tráfego de firewalls de última geração e dados de endpoints da proteção e resposta de endpoints do Traps™, o Cortex XDR pode determinar a causa raiz dos ataques. Essa análise integrada de endpoint ajuda os analistas de segurança a identificarem quais aplicativos ou ferramentas, como o PowerShell ou o WMI, foram usados nos ataques à rede. O Cortex XDR também pode analisar dispositivos corporativos para encontrar processos raros. Se o Cortex XDR detectar ferramentas de hacking em um host, as equipes de segurança poderão investigar mais profundamente para determinar se o host foi comprometido.

O Cortex é a única plataforma de segurança contínua aberta e baseada em IA do setor. Ele oferece simplicidade radical para operações de segurança e melhora significativamente os resultados de segurança por meio da automação com uma precisão sem precedentes.

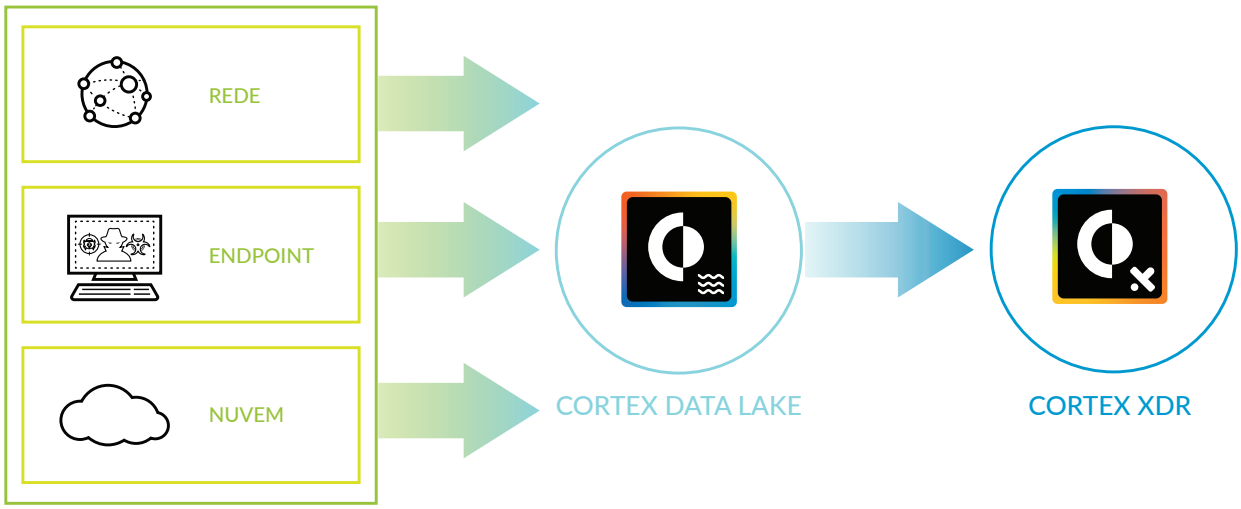

Figura 5: O Cortex XDR quebra os silos ao integrar os dados do endpoint, nuvem e rede

Ficar à frente dos invasores

Os métodos de ataque cibernético mudam continuamente. É apenas uma questão de tempo até que os invasores inventem novas maneiras de acelerar seus ataques e esconder suas atividades das ferramentas de segurança. As técnicas de reconhecimento atuais (ataques de subsistência, ataques sem arquivo, abuso de backups e automação) são perigosas, mas os invasores, em algum momento, as substituirão por novos métodos de ataque. No entanto, os invasores ainda precisarão coletar informações sobre os seus ambientes antes de localizarem e roubarem dados. Ao caracterizar o comportamento da rede dos usuários e do dispositivo, as equipes de segurança podem detectar o reconhecimento interno mesmo se os invasores mudarem suas ferramentas e técnicas no futuro.

3000 Tannery Way
Santa Clara, CA 95054

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com

cyberthreat report-reconnaissance2.0-wp-022219