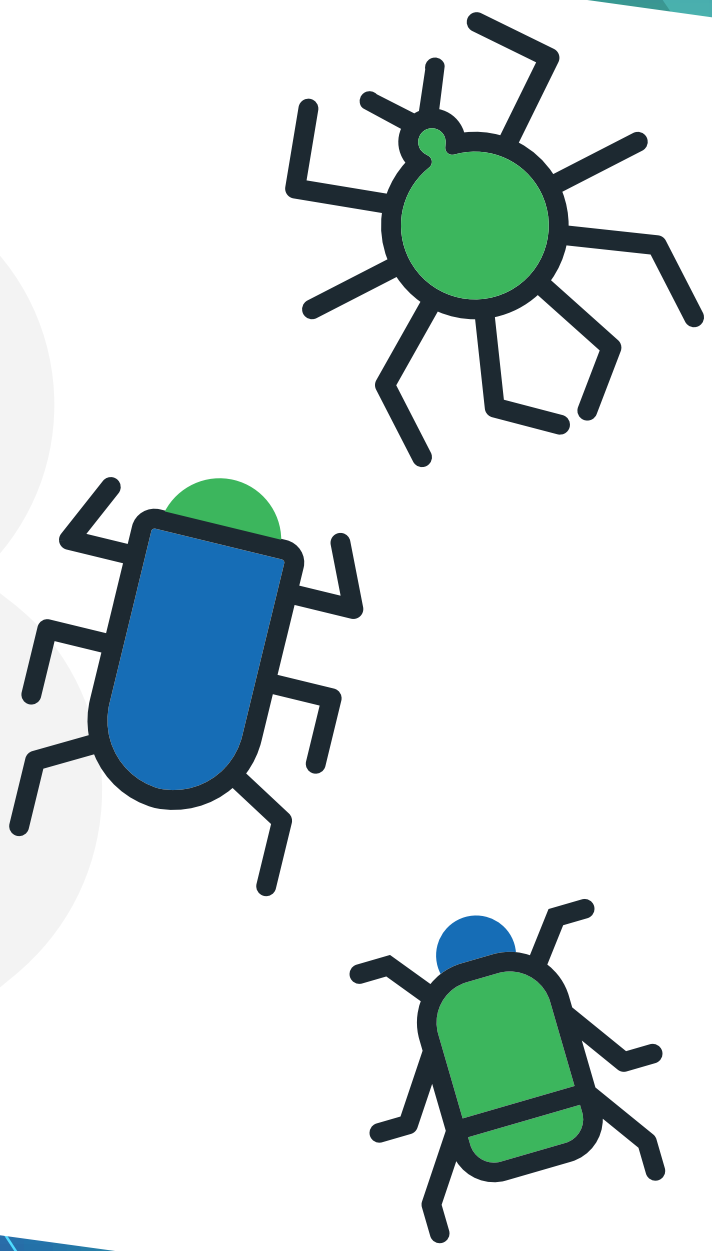
Blockbit

Você sabe como se proteger de uma **AMEAÇA AVANÇADA**?

Em meio a diversas modalidades de riscos cibernéticos e diferentes técnicas de contaminação, o cibercrime vem avançando na customização das ameaças. Ataques direcionados tendem elevar o grau de credulidade dos usuários, pois a organização criminosa busca conhecer seu alvo, criando meios de aproximação para cumprir seus objetivos.

Por isso, os alertas de segurança cibernética são mais urgentes no caso de identificação de ameaças persistentes avançadas (APT, Advanced Persistent Threat). São ataques sofisticados de espionagem, altamente direcionados, que usam diversas técnicas de entrada e exploração de informações. Em geral, são endereçados à coleta de dados valiosos, por exemplo, de negócios, financeiros e de propriedade intelectual.

Em geral, o ataque por APT busca implementar software para obter acesso remoto do ecossistema, permitindo ao cibercriminoso investigar o tráfego de informações em sistemas privados. Links maliciosos por email (phishing) ou o download de arquivos em websites desconhecidos, SQL Injection, são formas frequentes de distribuição de APTs.



São ataques persistentes

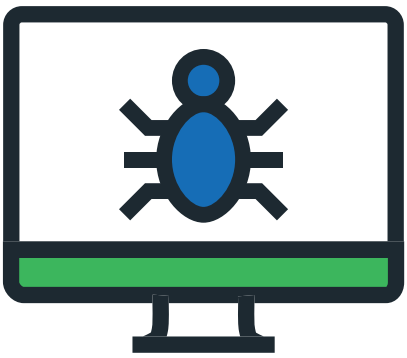
Tanto indivíduos como empresas podem ser alvo de ataques persistentes avançados. No entanto, muitos especialistas classificam APTs apenas aquelas aplicações desenvolvidas por ou endereçadas para fins políticos ou militares. De modo geral, são ameaças cuja tarefa é bastante específica, portanto sua vida útil será dedicada à execução daquela tarefa.

São ataques direcionados

Esse tipo de aplicação não está interessado em infecção em massa, mas sim em um alvo previamente definido. Isso significa que a aplicação é gerida por uma organização criminosa e continuamente monitorada para realizar a tarefa. Desse modo, o APT pode dedicar muito tempo explorando vulnerabilidades de sistema que lhe dê acesso aos dados. Seus objetivos podem ser: desabilitar certos serviços do alvo ou se apropriar de dados confidenciais.

São ataques sofisticados

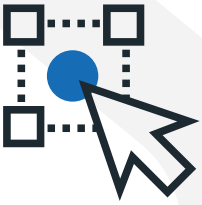
Para cumprir sua missão, um APT precisa manter-se anônimo por bastante tempo. Por isso, reúne diversas técnicas de exploração de sistemas e coleta de informações, de modo a dificultar que as ferramentas de segurança detectem sua ação criminosa. Brechas do tipo Zero-Day, são frequentemente exploradas por esse tipo de ataque.



Entenda como as APTs funcionam

1) Estudo

A primeira fase de uma ameaça persistente avançada é o planejamento. A rede de cibercriminosos que arquiteta o ataque busca entender previamente o comportamento de seu alvo – empresa ou usuário. As informações servem para desenvolver técnicas de aproximação – como spear phishing.



2) Acesso

Caso a técnica de engenharia social seja bem-sucedida - um usuário desavisado aciona um link ou arquivo malicioso – a APT ganha acesso ao ecossistema e pode instalar aplicativos com funções diferentes para garantir a sua permanência no ambiente: criar backdoors, multiplicar-se em ambientes de rede, copiar informações etc.

3) Investigação

Todo tráfego de informações é monitorado para identificar trilhas que apontem para dados confidenciais, credenciais para acesso a segmentos privados que podem armazenar as informações-alvo, além dos dados de gestão que permitam gerenciar privilégios de sistema.

Os APTs são responsáveis por diversos episódios de vazamentos de dados.

4) Captura

Durante todo o tempo em que a APT está infiltrada, o ataque é silencioso. O objetivo de sua missão é reunir os dados pré-definidos.

5) Exportação de Dados

As informações sequestradas são enviadas para a organização criminosa, que desenvolveu e gerencia a APT.

Detectando atividades suspeitas

Toda rede deve funcionar em acordo com as regras definidas pelo administrador. Isso significa, que atividades que não seguem esses padrões podem indicar a exploração de vulnerabilidades por artefatos externos, em especial se essas atividades acontecem em desacordo com o registro prévio – por exemplo, alto volume de transferência de dados.

Alguns sinais podem ajudar a identificar ameaças persistentes em seu ecossistema:

Tráfego inesperado: Com as ferramentas corretas, todo administrador de rede pode identificar fluxos imprevistos dentro da infraestrutura. Toda alteração no tráfego de dados precisa de atenção – procure por fluxos de dispositivos internos para outros dispositivos, sejam internos ou externos. Esse é uma das primeiras evidências a apontar para uma possível infecção por APT.

Acessos suspeitos: Um aumento repentino no volume de acessos de um usuário privilegiado a sistemas críticos também pode ser um indício de atividade suspeita. APTs se espalham rapidamente pelo ecossistema e recolhem todo tipo de informação disponível. Avaliando os tráfegos e os perfis do sistema, as aplicações são capazes de identificar usuários com maiores permissões e quais sistemas são mais protegidos. A partir daí, trabalham para coletar credenciais que darão acesso às informações privilegiadas. Quando você tem informações consolidadas dos locais, dispositivos e horários que determinado usuário acessa suas plataformas, qualquer alteração nesses padrões deve ser investigado.

Malware recorrente: APTs instalam códigos maliciosos para criar backdoor, ou seja, abrem brechas que podem ser exploradas em novas invasões. Caso o APT seja descoberto e mitigado, seus controladores podem usar vulnerabilidades previamente instaladas para retomar controle do sistema-alvo. Se um malware é mitigado, mas sempre consegue retornar ao sistema, esse é um sinal forte da existência de um backdoor. Por isso, é importante manter monitoramento ativo de todas as vias que permitam a entrada de intrusos.

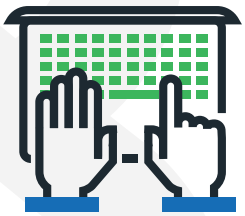
Dados deslocados: Antes de exportar dados para fontes externas, os APTs podem movê-los internamente, reunindo conjuntos de informações em locais inesperados. Grandes volumes de dados armazenados em locais inadequados representam um comportamento suspeito na rede e podem ter sido movidos em função de ação criminosa. Outro sinal suspeito é a compressão de dados em formatos não utilizados pela organização.

Construindo uma política contra vazamento de dados

A função central de uma ameaça persistente é explorar informações sigilosas. Por isso, é fundamental a construção de uma política de proteção contra o vazamento de dados. Três pilares devem sustentar essa política:

Cultura Organizacional

Apenas com educação corporativa pode haver sucesso dos objetivos da gestão de TI. Por isso, é importante a promoção de capacitações sobre segurança da informação para todos os níveis hierárquicos da empresa. Além de promover conhecimento sobre ameaças, ajuda a garantir que as políticas sejam seguidas.



Gestão de TI

Para evitar o vazamento de dados, é importante definir regras de segurança sólidas, para padronizar o uso dos recursos do ecossistema. Essa padronização permite identificar com base em dados, qualquer atividade suspeita em sua rede. Desse modo, o tempo de resposta diminui e o nível de segurança na gestão de incidentes aumenta.

Tecnologia

Com seus funcionários engajados, as ferramentas de cibersegurança ajudarão a manter o seu ambiente sempre monitorado. A tecnologia evoluiu bastante para evitar que APTs permaneçam anônimos em ecossistemas corporativos. Com ferramentas que prevejam vulnerabilidades, previnam ameaças, detectem de forma ativa os riscos e respondam a incidentes é fácil estar seguro.

Prevenindo as ameaças avançadas

Os ataques de ameaças avançadas podem aproveitar brechas internas ou externas, conhecidas ou desconhecidas, explorando informações em diferentes dispositivos e segmentos de rede.

Por isso, as ferramentas de proteção ativa de infraestruturas de TI são cruciais para mapear e detectar atividades suspeitas.

A Blockbit recomenda o uso de tecnologias de última geração para evitar que ataques direcionados tenham sucesso ao ganhar o controle de sistemas privados. Para que sua rede continue protegida, deve-se trabalhar e monitorar a coleta de credenciais que fornecem permissão de acesso às informações privilegiadas. Qualquer suspeita de entrada em uma plataforma, deve ser investigada a partir de dados consolidados do usuário, sejam eles local, hora ou dispositivo.

1. Procure todo tipo de vulnerabilidades

Ameaças internas
Sua rede é um conjunto de múltiplos dispositivos, segmentos e milhares de informações. Procure por brechas de segurança que possam ser exploradas por ameaças avançadas. Essas brechas podem ser sistemas desatualizados, permissões outorgadas de forma inadequada, senhas fracas ou que não são atualizadas periodicamente. A identificação destas vulnerabilidades internas pode ser automatizada com uma plataforma de Gerenciamento de Conformidades e Vulnerabilidades, que analise potenciais riscos e atribua o processo de remediação.

Ameaças externas
Não esqueça que a maioria das ameaças externas são catalogadas e possuem assinaturas de inteligência que alimentam as ferramentas com informações sobre os riscos e medidas de remediação. Por isso, é necessário que toda ferramenta de segurança adotada seja apoiada por uma Base de Inteligência Abrangente. No caso de vulnerabilidades desconhecidas, ou que não tenham assinaturas prévias, deve ser usado sistemas Sandbox, ou seja, sistemas que isolam a execução de aplicações para analisar seus processos. Assim, você será capaz de analisar o comportamento, as atividades e o impacto de ameaças, incluindo episódios Zero Day.

2. Ative mecanismos de proteção avançada

Vulnerabilidades desconhecidas
Para prevenir ameaças avançadas, você precisa usar plataformas avançadas. A plataforma de Proteção contra Ameaças Avançadas (ATP) permite detectar e defender sistemas contra ataques direcionados, ainda que não existam assinaturas prévias, como é o caso de vulnerabilidades Zero-Day. Esta capacidade é crucial para proteger os ativos da sua empresa contra novas modalidades de ataques, bloquear endereços IP com má reputação e bloquear ataques por geolocalização.

Vulnerabilidades conhecidas
Na proteção de ambientes de rede, monitorar tráfego é uma atividade crucial que ajuda a detectar a ocorrência de atividades suspeitas. Com o suporte de uma base de inteligência abrangente, um Firewall de Última Geração (NGFW) habilita o administrador de rede a identificar riscos de forma ágil, além de analisar o fluxo de dados, atividade de usuários e aplicações, o volume de banda em uso, tipos de arquivos utilizados e transmitidos pela rede etc. Todas estas informações instrumentaliza o gestor de TI a identificar e mitigar riscos.

3. Não esqueça as vias de contágio

Portas da frente
Em geral as técnicas de engenharia social serão exploradas como pontapé inicial dos ataques direcionados - os serviços de email são recursos frequentes para a esta distribuição de golpes. Proteger os servidores de correio com Análise Heurística - inteligência para aprender com os padrões das mensagens - e Anti-Malware pode ajudar a prevenir na ponta a circulação de ameaças direcionadas.

Portas do fundo
Caso um APT tenha sucesso em invadir sua rede, uma ação provável é a criação de backdoors, ou seja, um método não documentado de entrada em sistemas. O backdoor é uma das razões que qualifica o APT como persistente, pois permite que o atacante retorne ao seu ambiente. Mais uma vez, o Firewall será um grande aliado no monitoramento de portas ocultas. Combinado com um Sistema de Prevenção Contra Intrusos (IPS), você conseguirá identificar em tempo real atividades e ameaças suspeitas.