Inteligência de ameaças

1. Comunidade OTX
2. Informações VirusTotal
3. Inteligência de ameaças
4. Análise de malwares

HORIZON TECH

1. Primeira comunidade aberta de inteligência de ameaças do mundo

O compartilhamento de ameaças no setor de segurança permanece principalmente ad-hoc e informal, repleto de pontos cegos, frustração e armadilhas. Nossa visão é que empresas e órgãos governamentais coligam e compartilhem informações relevantes, oportunas e precisas sobre ataques cibernéticos novos ou em andamento o mais rápido possível para evitar violações graves (ou minimizar os danos de um ataque).

Como o OTX funciona

A OTX fornece acesso aberto a uma comunidade global de pesquisadores de ameaças e profissionais de segurança. Agora, possui mais de 100.000 participantes em 140 países, que contribuem com mais de 19 milhões de indicadores de ameaças diariamente. Ele fornece dados de ameaças gerados pela comunidade, permite pesquisa colaborativa e automatiza o processo de atualização de sua infraestrutura de segurança com dados de ameaças de qualquer fonte. O OTX permite que qualquer pessoa na comunidade de segurança discuta, pesquise, valide e compartilhe ativamente os dados, tendências e técnicas de ameaças mais recentes, fortalecendo suas defesas e ajudando outras pessoas a fazer o mesmo.

Acesso à comunidade aberta de inteligência contra ameaças

A pesquisa de segurança tende a ser um processo insular e raramente indivíduos ou grupos compartilham dados de ameaças entre si. Isso se deve à falta de confiança, políticas internas ou simplesmente à incapacidade de transmitir as informações às massas. A OTX ajuda a resolver esse problema com a capacidade de assinar ou seguir os pulsos mais confiáveis da comunidade.

- Disponibilizamos os pulsos e usamos o recurso DirectConnect para atualizar automaticamente nossos produtos de segurança.
- Seguimos os colaboradores da OTX e temos informações valiosas sobre as ameaças recentemente pesquisadas.

Pesquisamos e colaboramos abertamente sobre ameaças emergentes

O modelo tradicional de compartilhamento de ameaças é uma comunicação unidirecional entre pesquisadores / fornecedores e assinantes. Não há como os assinantes interagirem com colegas ou pesquisadores de ameaças em ameaças emergentes, pois cada destinatário é isolado um do outro. Por isso, existe o OTX - para mudar a maneira como todos criamos, colaboramos e consumimos dados de ameaças

2. Informações VirusTotal

O VirusTotal inspeciona itens com mais de 70 scanners antivírus e serviços de lista negra de domínios / URLs, além de uma infinidade de ferramentas para extrair sinais do conteúdo estudado. Qualquer usuário pode selecionar um arquivo do computador usando o navegador e enviá-lo para o VirusTotal. O VirusTotal oferece vários métodos de envio de arquivos, incluindo a interface principal da Web pública, uploaders de desktop, extensões de navegador e uma API programática.

Nossa plataforma faz de forma automática consultas de arquivos de URLs no VirusTotal, proporcionando um complemento das informações recebidas pelo OTX, formando uma gama completa de informações para análises de ameaças.

3. Inteligência de Ameaças

No ambiente de ameaças dinâmico e em evolução de hoje, as equipes de segurança de TI ocupadas não dispõem de tempo ou recursos para analisar por conta própria as ameaças emergentes. Em vez disso, eles podem recorrer à equipe de pesquisa de segurança da Horizontech e seus parceiros para fazer a pesquisa por eles com atualizações contínuas de inteligência de ameaças totalmente integradas à plataforma de segurança Horizontech provendo detecção e resposta de ameaças.

Nossa plataforma recebe atualizações a cada 30 minutos. Uma equipe dedicada passa inúmeras horas analisando os diferentes tipos de ataques, ameaças emergentes, comportamento suspeito, vulnerabilidades e explorações que eles descobrem em todo o cenário de ameaças.

Nossas vantagens:

A propriedade das fontes de dados integradas e da plataforma de gerenciamento que compõe a nossa plataforma oferece à uma vantagem exclusiva sobre outros produtos de pontos de segurança. O fornecimento de fontes de dados previsíveis permite que nossa equipe de pesquisa de ameaças tenha um entendimento abrangente das interações entre os diferentes tipos de dados que estão sendo coletados, correlacionados e analisados. Esse conhecimento profundo nos permite projetar a plataforma para fornecer controles de segurança eficazes e inteligência de ameaças perfeitamente integrada para qualquer ambiente.

Direcionamos os recursos de avaliação de ameaças da plataforma para equipes de pesquisa, identificando as ameaças mais recentes, resultando na visão mais ampla de vetores de ameaças, técnicas de ataque e defesas eficazes. Diferentemente das atualizações de uso único, focadas em apenas um controle de segurança, os parceiros fornecem regularmente nove atualizações de conjunto de regras coordenadas na plataforma. Essas atualizações eliminam a necessidade de você gastar um tempo precioso conduzindo sua própria pesquisa sobre ameaças emergentes ou alarmes acionados por suas ferramentas de segurança. Esses conjuntos de regras maximizam a eficiência do programa de monitoramento de segurança, fornecendo as seguintes atualizações:

- **Diretivas de correlação** - uma biblioteca extensa e crescente de regras predefinidas que convertem eventos brutos em informações de ameaças específicas e acionáveis, vinculando eventos diferentes de toda a sua rede
- **Assinaturas de IDS de rede** - detecta o tráfego malicioso mais recente na sua rede
- **Assinaturas de IDS do host** - identifica as ameaças mais recentes direcionadas aos seus sistemas críticos
- **Assinaturas de ameaças** - identifica novas forma de exploração e assinaturas que podem comprometer a segurança da sua empresa
- **Assinaturas de detecção de ativos** - detecta as informações mais recentes sobre sistemas operacionais, aplicativos e dispositivos
- **Assinaturas de avaliação de vulnerabilidades** - descubra as vulnerabilidades mais recentes em seus sistemas
- **Módulos de relatórios** - recebe novas visualizações de dados críticos sobre seu ambiente para gerenciar e atender às solicitações dos auditores
- **Modelos dinâmicos de resposta a incidentes** - orientação personalizada sobre como responder a cada alerta
- **Plug-ins de fonte de dados recém-suportados** - expande o espaço de monitoramento integrando dados de dispositivos e aplicativos de segurança herdados

Identificar as ameaças mais significativas que a sua rede enfrenta

As equipes de TI de todos os tamanhos sofrem com muitos dados de eventos de segurança e inteligência de ameaças acionável insuficiente. Muitas ferramentas de segurança geram um fluxo constante de alertas sobre atividades importantes (e não tão importantes), fazendo com que as equipes de TI sacrifiquem seu tempo valioso tentando correlacionar manualmente atividades diferentes em seus arquivos de log. Eles vasculham milhares de eventos aparentemente inócuos, na esperança de encontrar esses poucos indicadores que podem significar comprometimento do sistema ou violação de dados. Ao mesmo tempo, as técnicas de ataque se tornaram mais sofisticadas, dificultando a detecção de violações.

Os logs carregam informações importantes, como o que seus usuários estão fazendo, quais dados estão acessando, o desempenho de seus sistemas e a integridade geral da rede. Eles também conterão evidências de comprometimento do sistema e exfiltração de dados, se você soubermos onde procurar. No entanto, a leitura de logs brutos não é fácil, por vários motivos, incluindo:

- Os logs variam de sistema para sistema ou mesmo de versão para versão no mesmo sistema
- Eles geralmente são difíceis de interpretar e não são lidos facilmente pela equipe de TI
- Os logs são focados na gravação de eventos gerados por cada sistema e têm visibilidade limitada (por exemplo, um firewall vê pacotes e sessões de rede, enquanto um aplicativo vê usuários, dados e solicitações)
- Os logs são estáticos, pontos fixos no tempo, sem o contexto completo ou a sequência de eventos relacionados.

Nossa plataforma resolve esses problemas com seu poderoso mecanismo de correlação. Nossa extensa e crescente biblioteca de diretrizes de correlação pré-criadas analisa continuamente os dados do evento para identificar possíveis ameaças à segurança da sua rede. Detectamos e vinculamos automaticamente padrões de comportamento encontrados em eventos diferentes, ainda que relacionados, gerados em diferentes tipos de ativos, informando quais são as ameaças mais significativas que a sua rede enfrenta no momento.

Inteligência avançada para ameaças avançadas de combate

Análise de Artefato de Segurança

Usando uma ampla variedade de técnicas de coleta, incluindo sandboxing avançado para amostras de malware em quarentena, a equipe de pesquisa de ameaças dos parceiros Horizontech analisa mais de 10 milhões de artefatos de segurança exclusivos todos os dias. Essa análise fornece informações importantes sobre as mais recentes ferramentas e técnicas de invasor.

Implantação e análise Honeypot

Além de rodar armadilhas na rede local dos clientes, utilizamos armadilhas globais que são essencialmente “armadilhas virtuais para moscas venenosas” configuradas para detectar, capturar e analisar as mais recentes técnicas e ferramentas de ataque. Aproveitando o insight obtido pelos honeypots colocados em redes de alto tráfego, nossa equipe arma a proteção em nossos clientes com as mais recentes estratégias defensivas na forma de regras atualizadas de correlação de eventos, IDS, engano, assinaturas de vulnerabilidade e muito mais.

Análise do perfil do atacante

Nossos parceiros monitoram constantemente os fóruns de hackers e as redes undergrounds para obter perfis detalhados dos traços comuns de criminosos cibernéticos. Essas informações nos dão acesso incomparável para entender o "horizonte de ataque" e resultaram em grandes descobertas, como a evolução do Sykipot, o Red October e outros surtos de malware.

Colaboração aberta com agências estatais, academia e outras empresas de pesquisa de segurança

Graças ao amplo alcance de nossa comunidade de compartilhamento de inteligência de ameaças, conseguimos estabelecer fortes conexões parceiros de pesquisa de segurança que atuam com agências estaduais em todo o mundo, pesquisadores acadêmicos e outros fornecedores de segurança. Esses relacionamentos nos permitem obter acesso a atualizações de malware e vulnerabilidades pré-publicadas, bem como a verificação aprimorada de nossas próprias pesquisas. Reunindo informações sobre ameaças fornecidas pela comunidade a partir de uma base instalada diversificada, espalhada por vários setores e países e é composta por organizações de todos os tamanhos, podemos reduzir a capacidade de um invasor de isolar alvos por tamanho de setor ou organização.

4. Análises de Malwares com apoio da OTX e Virus Total

Com a comercialização do crime cibernético, as variações de malware continuam a aumentar a um ritmo alarmante, e os defensores se encontram em uma corrida constante para acompanhar. Mais do que nunca, as equipes de TI e os analistas de segurança precisam das ferramentas certas para identificar e analisar corretamente o malware, rapidamente. Seja fornecendo pontos de dados críticos para reforçar a inteligência do SOC ao responder a uma ameaça ativa ou filtrando os falsos positivos que podem consumir recursos e tempo valiosos, a análise de malware é um componente crítico do cenário de ameaças moderno.

Utilizando nativamente o OTX e Virus Total torna a análise de malware e vírus rápida e fácil! Com o clique de um botão, arquivos e URLs suspeitos podem ser carregados e analisados imediatamente. Estas fontes fornecem análises estáticas e dinâmicas rápidas, armando nossas equipes com as informações necessárias para agir e impedir atividades maliciosas antes que os danos em sua rede sejam causados.