minitel
30 anos a distribuir valor

NÃO SEJA UM ALVO FÁCIL.

THREATTRACK: A SOLUÇÃO DE CIBERSEGURANÇA PARA ANALISAR, RESPONDER E DEFENDER A REDE DE ATAQUES DIRECIONADOS, SOFISTICADOS, MALWARE AVANÇADO E ZERO-DAY.

ThreatTrack

Comprovada e Eficaz.
A principal SandBox da indústria para análise de malware, conhecida pela sua performance eficiência e inovação.

Proteção de Confiança.
Há duas décadas a criar soluções inovadoras de cibersegurança utilizadas na defesa dos governos, organizações de inteligência e cumprimento de legislação assim como empresas em indústrias alvo de ataques tais como serviços financeiros, indústria, retalho e saúde.

Peça-nos uma demonstração com um técnico especializado:

info@minitel.pt
ou 21 381 09 00

Um dos assuntos que mais preocupa os governos é a cibersegurança.

Em Portugal, segundo o CNCS, Centro Nacional de Cibersegurança, é uma área em que há sempre mais a fazer, uma vez que a modernização tecnológica da sociedade aumenta a exposição de todas as organizações.

Nos EUA, passou a ser uma questão de segurança nacional. Os hackers tiraram partido das vulnerabilidades dos computadores e infiltraram-se nas redes governamentais para roubar dados sensíveis e causar danos.

- **Que opções de deteção e defesa contra estes ataques têm atualmente os organismos governamentais?**
- **Que inovações tecnológicas estão a ser disponibilizadas pelos fornecedores de soluções de segurança para manter as redes governamentais protegidas?**

O ThreatTrack, com décadas de experiência em cibersegurança, tem utilizadores no mundo inteiro, nos ambientes mais sensíveis, incluindo a segurança governamental, defesa e organismos de informação semelhantes ao nosso Serviço de Informação de Segurança (SIS) ou SIRP.

VEJA POR SI MESMO COMO FUNCIONA ESTA SOLUÇÃO:

- O ambiente de cibersegurança atual;
- Como é que as organizações governamentais estão a abordar os ciberataques emergentes e desafios;
- A estratégia de segurança da ThreatTrack, abordagem em layers, para capacitar os profissionais de segurança;
- Funcionalidades inovadoras que a ThreatTrack está a desenvolver para melhorar a segurança dos organismos do Estado.

Quer saber mais? Peça uma demonstração personalizada para a sua empresa, para os seus clientes e veja por si mesmo como foi já implementada por empresas, organismos estatais em Portugal.

Travessa Légua da Póvoa, 1A
1250-136, Lisboa
21 381 09 00
www.minitel.pt
info@minitel.pt

minitel
30 anos a distribuir valor

UMA ABORDAGEM GLOBAL À CIBERSEGURANÇA GOVERNAMENTAL

PERCEBER A ENVOLVENTE DA CIBERSEGURANÇA

As ferramentas utilizadas pelos hackers tornaram-se mais sofisticadas. Por exemplo, a tecnologia de encriptação, permite a atacantes encriptar parte do código malicioso para que as ferramentas de segurança não os consigam facilmente detectar.

O malware polimórfico é um problema e está a aumentar. Os atacantes podem alterar substancialmente partes do código malicioso, estes códigos passam a ser diferentes e, por isso, a deteção tradicional por assinaturas não pode ser usada para parar estes ataques. Para além disso, os atacantes estão a capitalizar na generalização do uso da comunicação por email. Os ataques de phishing, que se focam em grupos ou organizações especificas, para roubar propriedade intelectual, dados financeiros, segredos militares e outros dados confidenciais são tácticas favoritas dos cibercriminosos. No Spear Phishing, o malware é disfarçado como sendo de uma instituição de confiança, tornando difícil para quem recebe o email perceber que está comprometido. Uma alteração significativa é que o código malicioso faz um reconhecimento extensivo antes de corromper o sistema.

Significa construírem um sistema multi-direcionado, com que possam comprometer não só o alvo principal do ataque, mas também toda uma cadeia de fornecedores e clientes para, por exemplo atingir todas as empresas na área da indústria de defesa que trabalhem com o Ministério da Defesa.

As organizações governamentais e os responsáveis pela segurança enfrentam novos desafios.

ThreatTrack

ENFRENTAR AS CRESCENTES CIBERAMEAÇAS & DESAFIOS

A cibersegurança não é um problema novo e não vai ficar mais fácil, mas sim ainda mais complicado.

Em Portugal e nos outros países existem progressos nesta área, permitindo o acesso a ferramentas de segurança mais eficazes. Mas a modernização tecnológica, serviços cloud, maior abrangência do perímetro da rede, mobilidade e colaboradores remotos aumentam a exposição das organizações e exigem às entidades governamentais um constante acompanhamento. É precisamente nesta área que o ThreatTrack se destaca.

ESTRATÉGIA DE CIBERSEGURANÇA 'LAYERED'.

Face à frequência e sofisticação dos recentes ciberataques, as entidades estatais não podem depender de defesas de segurança reactivas. Precisam de soluções de segurança que garantam agilidade e adaptação aos ambientes IT e empresarias em mudança.

É necessária uma defesa de segurança em camadas, "layered", que garanta que estão preparados para detectar rapidamente e acabar com estes "actores maliciosos" antes de causaram estragos nas redes governamentais.

O termo "layered security" significa uma estratégia defensiva que apresenta múltiplas "layers" de defesa que abrandam ou retardam o ataque, estratégia que os militares chamam "defesa em profundidade, cavar fundo".

Este tipo de defesa não está exclusivamente dependente das ferramentas ou da experiência humana, mas sim de uma combinação de ferramentas com uma visão sólida, que garanta que os organismos estão suficientemente bem equipados para se defenderem da maior diversidade e alcance dos ciberataques. As soluções do ThreatTrack são adaptadas a este ambiente. O ThreatTrack sabe que está a lidar com ambientes híbridos, com um misto de serviços baseados na cloud e em serviços internos, assim como uma noção mais inconsistente da rede que não é apenas a rede do edifício, mas transcende a organização. As instituições estatais também devem ter em conta a explosão de dispositivos que se ligam à sua rede - tanto as disponibilizadas pelo Estado como dispositivos pessoais. As soluções do ThreatTrack oferecem uma cobertura completa, desde ambientes web, email e BYOD, até ao endpoint. É uma suite abrangente, que considera todas as facetas das organizações governamentais, em ambientes híbridos.

O ThreatTrack não disponibiliza apenas ferramentas de deteção e prevenção, mas também soluções que são por natureza proativas. e ajudam as organizações públicas a simular ataques e prever o tipo de risco que podem vir a ter antes de serem comprometidas.

O termo 'layerd security' descreve uma estratégia defensiva, com múltiplas camadas de segurança desenhadas para atrasar um atacante, tornando possível o bloqueio da ameaça.

A principal prioridade das organizações é determinar rapidamente e de forma clara quando é que está a ser levado a cabo um ataque. O problema com que se defrontam, é que muitas soluções param na fase de deteção. Em vez disso, o ThreatTrack examina a progressão do ataque e do que está a acontecer de forma a que as organizações não sejam surpreendidas se a atividade maliciosa tiver sido completamente eliminada da rede e mais tarde reaparecer noutra forma. Mostra a progressão do ataque, reduzindo o tempo de análise que de outra forma teria gasto a ir atrás de falso positivos. Se considerar a natureza da maior parte dos ataques direcionados, normalmente não envolvem um único actor malicioso que envia uma única peça de malware a um individuo.

Em muitos casos, os atacantes montam campanhas amplas de spear phishing, enviando emails que parecem legítimos a um conjunto de pessoas na mesma organização. Os atacantes lançam-se a uma rede mais alargada, mas frequentemente utilizam um tipo de malware especifico que tenta encontrar o caminho de menor resistência para penetrar a rede. Podem também utilizar vários

tipos de malware e direcionar o código malicioso para uma tarefa/função específica dentro da organização, tal como administrador de sistema ou diretor financeiro.

O ThreatTrack agrega dados sobre o tipo de ataques à medida que se desenvolvem e mostra a correlação entre o ataque corrente e os ataques anteriores com características similares. Oferece uma visão histórica, mas no contexto do tempo real. É importante ter esses dados à sua disposição, porque essa é a altura crítica em que pode impedir o ataque de se espalhar.

Queremos ter a certeza que, seja quem for que analise, consegue ter total visibilidade e distinguir as árvores da floresta. Muitas outras soluções focam-se demasiado nas árvores. O ThreatTrack eleva o padrão, permitindo olhar para a floresta e ter uma visão mais global do ambiente.

O conhecimento profundo e avançado do ThreatTrack na área da cibersegurança - especificamente na resposta a ameaças avançadas e malware – resulta de décadas de experiência e este conhecimento está embutido nas soluções da empresa. O beneficio para as organizações é que não têm de investir fortemente em serviços para reforçar estas soluções.

Para ajudar os organismos a ver o plano de fundo no que respeita à segurança de rede, as soluções da ThreatTrack oferecem avisos automatizados de eventos futuros e assuntos que devam ser abordados de imediato, com informação precisa e atempada, para que as pessoas a possam utilizar e tomar as melhores decisões.

O ThreatTrack desenvolveu as suas soluções tendo em mente dois grupos primários de utilizadores: analíticos de segurança e responsáveis IT.

Os dados são personalizados para responder às necessidades destes e outros grupos de utilizadores ou pessoas.

Por exemplo, o ThreatTrack pode disponibilizar aos analistas de segurança visões especificas, mostrando o que aconteceu, o que levou ao ciberataque e se este tipo de ataque foi alguma vez utilizado contra a organização. A possibilidade de visualizar os dados agregados num formato apropriado à função do colaborador pode poupar tempo que é vital para subverter um ataque.

O ThreatTrack construiu uma estrutura que disponibiliza dados sobre o que se está a passar, para além das tentativas de malware para atacar ou infiltrar, disponibilizando dados de forma simplificada, que todos consigam perceber.

Mas os esforços do ThreatTrack para capacitar e equipar a segurança do governo não param aqui. A equipa de peritos em cibersegurança da empresa está permanentemente a inovar para oferecer uma melhor visão e maior conhecimento aos responsáveis pela segurança da rede.

COMO É QUE O THREATTRACK INOVA NO CIBERESPAÇO?

Uma das poucas constantes no mundo da cibersegurança é a inovação.

As ferramentas de segurança e defesa devem evoluir na medida em que as ameaças são mais sofisticadas e destrutivas. Esta é a razão pela qual inovação na área da segurança deve ser uma prioridade para o governo e seus parceiros neste ecossistema.

Para o ThreatTrack, a inovação tem tomado várias formas nesta última década. Machine Learning dentro da rede é um exemplo. Hoje em dia, muitas empresas online e prestadores de serviços utilizam o machine learning para controlar a visão do utilizador e os hábitos de compra e utilizam essa informação para fazerem recomendações, baseadas nas preferências dos utilizadores. O ThreatTrack utiliza os algoritmos de machine learning à volta do malware e utiliza-os para observar o comportamento dentro da rede para identificar rapidamente atividades suspeitas ou anómalas e separá-las dos falsos positivos.

Ao utilizar estas técnicas de aprendizagem dinâmicas, utilizando o machine learning, o ThreatTrack pode controlar todas as atividades na rede e estabelecer um padrão de comportamento típico do utilizador. Se existir um desvio a esse padrão de comportamento, as organizações podem usar essa informação para saber mais sobre a rede e sobre ataques que possam vir a acontecer. Se uma atividade não for anómala, mas sim uma falha no sistema, também pode aprender mais com essa informação. Não se tratam só de anomalias, mas de limites do risco aceitável. O objectivo do ThreatTrack é ter todo este processo automatizado.

Para que as organizações sejam eficazes, a automatização e a visibilidade são fulcrais. Infelizmente, os profissionais de cibersegurança, na maior parte das empresas e organismos similares, nem sempre têm o nível de visibilidade necessário para fazer essas determinações. Da perspectiva da segurança, as organizações estão principalmente focadas na forma como o malware é entregue.

Ainda não estão focadas no facto de que todos vão ser infectados.

Então o que é que acontece a seguir?

Tradicionalmente, as ferramentas de segurança têm falhado na ligação deste tipo de informação de ameaças para a atividade da rede dentro da organização. Esta parte tem estado a faltar e é onde as nossas soluções de destacam.

É necessário olhar para os comportamentos que estão a acontecer, na perspectiva do utilizador de rede e do endpoint, para identificar as potenciais actividades maliciosas que estão a entrar para a rede da organização.

Estas soluções foram concebidas para trabalhar em conjunto e disponibilizar aos utilizadores uma visão abrangente da atividade na rede.

Hoje, os fabricantes desenvolvem soluções com novas capacidades resultantes de aquisições e fusões e um dos principais desafios é integrar estas soluções.

O ThreatTrack optou por uma estratégia diferente dos concorrentes, disponibilizando uma solução completa para os organismos, não estando essencialmente focada na forma como se encaixa na infraestrutura existente.

A cibersegurança requer coordenação e inovação entre o governo e a indústria, tanto agora e no futuro. A equipa de peritos do ThreatTrack percebe que a colaboração é a chave e pode ajudar a construir uma estratégia globalizante para as organizade segurança governamentais.

ThreatAnalyzer

Proteger a rede contra ataques zero-day, ataques direccionados e malware avançado continua a ser o maior desafio. Para defender os dados empresarias é preciso uma análise dinâmica do malware e analisar com maior profundidade.

O ThreatAnalyzer é uma Sand Box de análise do malware, personalizável e fácil de utilizar: permite recriar os ataques, executar amostras de malware que lhe permitem "cavar mais fundo", num ambiente protegido, revelar comportamentos maliciosos e ver o impacto dos mesmos, em minutos. O painel de controlo único mostra a informação chave, com possibilidade imediata de ver cirurgicamente os detalhes granulares, sem ser inundado por dados desnecessários.