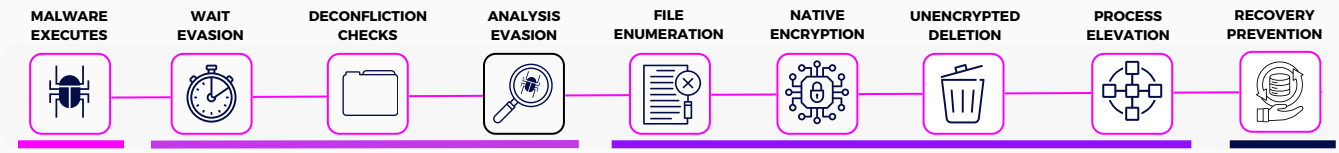
VIVA SECURITY

halcyon

DATA SHEET

ANTI RANSOMWARE

Nossa solução ao longo da cadeia de execução do Ransomware



Bloqueio Pré-Execução

Utilizando **modelos de ML/AI** proprietários enriquecidos por fontes de dados exclusivas, a plataforma possui uma nuvem totalmente habilitada que fornece **visibilidade** ao ponto de extremidade, **permitindo que decisões sejam tomadas** neste, mesmo quando não conectado à internet.

Exploração

Utilizando técnicas que os atacantes inserem em ransomwares para impedir que estes sejam executados em sistemas durante suas verificações, **bloqueando a criptografia** com um mecanismo que consegue **enganar o ransomware**.

Isolamento e Resiliência

Primeiro produto a defender ativamente sua solução de Proteção de Ponto de Entrada (EPP) existente **contra desativação em um ataque avançado**, visando proporcionar a melhor proteção, considerando que camadas podem apresentar falhas.

Comportamental de última Geração

Análise de todas as dimensões de um programa, incluindo procedência, comportamento e os sistemas com os quais se comunica, para criar uma pontuação integrada **a fim de evitar a ação de executáveis maliciosos**.

Desvendando os detalhes do Halcyon

BLOQUEIO DE PRÉ-EXECUÇÃO

Juntamente com o EPP existente, o Halcyon é a última linha de defesa proativa contra ransomware (e outros códigos maliciosos/evasivos) para concluir com sucesso suas rotinas ou funções no sistema. O Bloqueio de Pré-Execução atua quando o aplicativo/executável/binário é chamado primeiro pelo sistema para ser carregado na memória e antes que as primeiras linhas de código sejam executadas. A camada de pré-execução inclui o mecanismo de atribuição e a primeira implementação de nossa lógica de ML (machine Learning).

A Atribuição utiliza os seguintes componentes para analisar o processo antes de sua execução:

- Feeds de ameaças comerciais, bem como proprietários.
- PE análise estática.
- Digitalização do disco rígido.

Função para:

- Determinar 'ruim conhecido' para encerrar o processo antes da execução.
- Determinar 'bom conhecido' para permitir que os processos continuem sem intervenção.
- Determine o nível de suspeita ou peso da confiança que permeia ao longo do ciclo do processo e impulsiona a análise, monitoramento e interação subsequente pelo agente Halcyon.

EXPLORAÇÕES

Os processos suspeitos cuja execução é permitida são direcionados à camada de Exploração, onde o Halcyon utiliza uma variedade de técnicas para aproveitar as declarações condicionais, frequentemente escritas no código do ransomware, para realizar funções como evitar análises (explorando suas técnicas anti-análise ou de evasão), impedir o comprometimento de sistemas em seus países hospedeiros (apresentando arquivos de idioma/teclado/endereço IP/etc.) ou evitar o comprometimento de sistemas já criptografados (criando conflitos através de chaves de registro ou outros IOCs).

Ao injetar artefatos que tornam essas condições presentes na visualização do processo em execução/suspeito, podemos aproveitar as rotinas já incorporadas ao código do ransomware para evitar a detonação inicial. Por outro lado, em vez de acionar uma saída do processo, o segundo mecanismo na camada de Exploração, é projetado para acionar o pior cenário de mau comportamento que o código está programado para fazer.

Os mecanismos comportamentais são capazes apenas de detectar as ações de um processo malicioso. No caso do ransomware, muitos dos comportamentos só serão exibidos se certas condições estiverem presentes e, quando estas condições não estiverem presentes, as rotinas simplesmente não serão executadas. O Halcyon injeta artefatos (processos falsos, arquivos de isca, etc.) na exibição do processo em execução que atraem o máximo de comportamento ruim possível.

Função para:

- Fazer com que o processo acione uma saída e 'se mate' por meio de suas rotinas de anti-análise e evasão incorporadas ao código.
- Obter o pior cenário de comportamento 'ruim' ou suspeito para amplificar o sinal não apenas para o mecanismo comportamental do Halcyon, mas também para o EPP.

COMPORTAMENTO DE ÚLTIMA GERAÇÃO

A camada comportamental vincula-se ao mecanismo de exploração em uma camada anterior. O mecanismo comportamental é onde a maior parte dos recursos de ML do micromodelo Halcyon está alojada e é onde monitoramos e reagimos às atividades de processos suspeitos em tempo real. A maioria dos produtos modernos de proteção de endpoint aproveita a análise comportamental, normalmente na forma de redes neurais convolucionais e algoritmos de árvore de decisão.

Esses recursos convencionais de aprendizado de máquina, ainda sofrem falhas inerentes com base ao tamanho dos conjuntos de dados necessários para treiná-los e em sua capacidade de permanecer ciente do contexto.

A implementação contemporânea de modelos de ML/AI de endpoint não é capaz de fornecer aprimoramentos contínuos aos recursos de proteção do sistema e não pode incorporar novos dados aprendidos anteriormente pelo endpoint. O mecanismo comportamental Halcyon emprega uma arquitetura de micromodelo pioneira no setor, projetada com base no princípio do aprendizado de máquina baseado em rede de cápsulas, que permite amplos benefícios em relação aos métodos anteriores de análise comportamental.

- Permite mecanismos de aprendizado supervisionados e não supervisionados orientados por dados que funcionam juntos aos endpoints;
- Permite uma análise eficiente usando vários modelos, cada um treinado em conjuntos de recursos específicos, em paralelo, em oposição a um modelo de detecção monolítico.;
- Fornece decisões altamente precisas com um conjunto de dados limitado, pois cada micromodelo é especializado e atribui conjuntos de comportamentos que fornecem dados a outros micromodelos para avaliar suas decisões.;
- Permite um rastreamento de processos robusto para detectar e combater a injeção dos mesmos, protengendo ainda mais contra ataques aos produtos de segurança implantados no sistema.

Módulo de exfiltração

Fornece exame do comportamento da rede e dos dados, e correlações cruzadas com os dados do processo de endpoint, para verificar a sinalização de exfiltração de dados ilegítimos na empresa. O objetivo é observar os atributos comportamentais do solicitante, o processo e o destino para interromper a exfiltração e retornar a alavancagem de dados ao cliente.

ISOLAMENTO E RESILIÊNCIA

Por muito tempo, o setor de produtos de segurança teve como meta a eliminação de ameaças – soluções que mitigam 100% das ameaças 100% do Tempo. O Halcyon foi desenvolvido tendo em mente as vulnerabilidades, com o objetivo de reduzir o impacto nos negócios como o primeiro objetivo e a mitigação de ameaças em segundo lugar. Nossa experiência nas últimas décadas nos ensinou que a ameaça está sempre evoluindo e, embora devamos evoluir e nos adaptar continuamente a essa ameaça – mitigar o impacto nos negócios é a primeira prioridade.

Garantir que a empresa possa continuar funcionando é o primeiro objetivo do programa de segurança cibernética. E reduzir o impacto comercial de um evento de ransomware é a principal função da plataforma Halcyon.

A camada de isolamento e resiliência fornece proteção quando todas as outras lógicas de detecção e prevenção falham e fornece as seguintes funções:

- Proteção do Volume Shadow Service (VSS) do kernel MS
- Controle das regras de firewall do sistema local para fornecer a capacidade de colocar em quarentena o sistema afetado;
- Recuperação de chave de criptografia simétrica para eventos de criptografia;
- Atualmente, recuperando/duplicando chaves quando o ransomware está usando criptografia Microsoft AES nativa, que geralmente é aproveitada com base na força, velocidade e eficácia;
- Irá recuperar chaves de bibliotecas importadas (como salsa/chacha20) na versão Q3 2023.

Módulo de resiliência em tempo real

- Fornece retrocesso específico do processo de todas as atividades executadas no sistema em uma função fora do VSS. A capacidade de retroceder as alterações do sistema com base no rastreamento da árvore de processos, fornece a recuperação mais robusta e oportuna do mercado.

ORIENTADO POR API

As equipes de SOC modernas precisam de produtos que se integrem aos seus fluxos de trabalho, não outro console. O Halcyon é uma plataforma de segurança API-first (mas também possui um ótimo console da web!)

POWERED BY IA/ML

O Halcyon possui uma série de mecanismos de aprendizado de máquina treinados inteiramente em ransomware para tomar decisões altamente precisas quase em tempo real. Em vez de simplesmente utilizar um olhar binário, o Halcyon observa o contexto e o comportamento de todo o sistema.

CAMADAS DE PROTEÇÃO

O Halcyon combina defesa pré-execução com técnicas de engano e anti-detonação para bloquear novos ransomwares antes de serem executados. Caso o mecanismo não o detecte imediatamente, o Halcyon isola o nó afetado.

LEVE E LIVRE DE CONFLITOS

O agente é leve e desenvolvido para funcionar junto com sua solução NGAV/EPP/XDR existente sem problemas. O Halcyon é testado para trabalhar ao lado de Crowdstrike, SentinelOne e Windows Defender.

PROJETADO DESDE DO INÍCIO PARA DERROTAR O **RANSOMWARE!**

SOBRE NÓS.

A VIVA Security promove a democratização da cibersegurança para simplificar o dia-a-dia dos profissionais de TI por meio de soluções inovadoras e disruptivas.

VIVA SECURITY