FIREEYE™

FICHA TÉCNICA

Serviços de resposta a incidentes

Investigue, contenha e corrija incidentes de segurança críticos com velocidade, escala e eficiência

ESTUDO DE CASO: IR DA MANDIANT NO TRABALHO

Uma empresa multinacional de serviços profissionais, com dezenas de milhares de computadores espalhados pelo mundo, entrou em contato com a Mandiant para responder a uma possível violação de dados críticos de clientes.

Dia 1 - Os consultores da Mandiant iniciaram a distribuição da tecnologia de terminal com base na nuvem em 18.000 sistemas no prazo do quatro horas após a notificação.

- A investigação começou no mesmo dia.
- Evidência de comprometimento confirmada identificada no prazo de quatro horas após o início da investigação.

Dia 6 - A maior parte do trabalho investigativo foi concluída. A análise foi realizada em mais de 18 mil terminais com análise de resposta detalhada e ao vivo em 80 sistemas.

Dia 7 - A contenção foi realizada sem interrupção dos negócios. Os especialistas da Mandiant continuaram a monitorar a rede para assegurar que não houvesse novas tentativas de comprometimento por parte do perpetrador da ameaça.

Dia 11 - Cliente voltou ao trabalho normalmente.

Todo o trabalho foi conduzido remotamente.

A FireEye Mandiant está na linha de frente da inteligência em segurança cibernética e ameaças cibernéticas desde 2004. Os responsáveis pela resposta a incidentes estiveram nas linhas de frente das violações mais complexas do mundo. Temos um profundo conhecimento sobre os agentes de ameaça existentes e emergentes, bem como sobre suas táticas, técnicas e procedimentos extremamente dinâmicos.

Combinamos conhecimentos investigativos e de correção, obtidos ao se responder a milhares de incidentes, com a avançada tecnologia de terminais e rede FireEye e a inteligência sobre ameaças da FireEye, que são líderes do setor.

O trabalho da Mandiant nos maiores e mais divulgados incidentes qualifica nossos especialistas para que ajudem os clientes em todos os aspectos da resposta a incidentes — da resposta técnica ao gerenciamento de crises.

Ajudamos os clientes a investigar e a corrigir com mais rapidez e eficiência, para que eles possam se dedicar ao que mais interessa: seus negócios.

Visão geral

O uso de soluções na nuvem e no local permite que as investigações comecem imediatamente, durante o gerenciamento das questões de privacidade dos dados do cliente. No prazo de horas, os responsáveis pela resposta a incidentes da Mandiant podem começar a analisar o tráfego de rede e as informações de milhares de terminais. O incomparável acesso à inteligência sobre ameaças obtida nas linhas de frente de pesquisas de ataques e outras fontes de inteligência informa as equipes de resposta a incidentes da Mandiant sobre as mais recentes táticas, técnicas e procedimentos (tactics, techniques and procedures, TTPs) dos atacantes.

Os especialistas da Mandiant entendem que uma resposta abrangente a incidentes e violações é mais do que investigação técnica, contenção e recuperação. Portanto, também ajudamos com comunicação executiva e gerenciamento de crises — incluindo considerações jurídicas, regulatórias e de relações públicas. O gerenciamento de crises é fundamental para controlar o dano à reputação e a vulnerabilidade jurídica.

Tabela 1. Tipos de incidentes que costumamos gerenciar.

Roubo de propriedade intelectual	Roubo de segredos comerciais ou outras informações confidenciais.
Crime financeiro	Roubo de dados de cartões de pagamento, transferências de dinheiro ACH/EFT ilícitas, extorsão e ransomware.
Informações de identificação pessoal (Personally identifiable information, PII)	Exposição de informações utilizadas para identificar indivíduos especificamente.
Informações protegidas de saúde (Protected Health Information, PHI)	Exposição de informações protegidas de atendimento médico.
Ameaças internas	Atividades inadequadas ou ilegais realizadas por funcionários, fornecedores e outros elementos internos.
Ataques destrutivos	Ataques cujo único objetivo é criar dificuldades para a organização visada, ao tornar irrecuperáveis informações e sistemas.

O DIFERENCIAL DA MANDIANT

- **Experiência investigativa:** os investigadores da Mandiant aprimoraram suas habilidades conduzindo e corrigindo as maiores e mais complexas investigações do mundo.
- **Inteligência sobre ameaças:** avançada inteligência montada a partir das linhas de frente da resposta a incidentes, extensa descoberta de métodos e tecnologias usadas por invasores e pesquisa por meio de fontes de dados de terceiros, FireEye Dynamic Threat Intelligence coletada pelas tecnologias da FireEye e outras fontes da FireEye Threat Intelligence.
- **Tecnologia:** os especialistas da Mandiant usam as mais recentes tecnologias da FireEye no local e na nuvem, permitindo que as investigações comecem imediatamente. Nossas tecnologias permitem resposta rápida em grande escala, dando visibilidade sobre o tráfego da rede e os terminais que executam Microsoft Windows, Linux e macOS X.
- **Gerenciamento de crises:** os responsáveis pela resposta a incidentes têm anos de experiência aconselhando clientes sobre comunicações relacionadas a incidentes, incluindo comunicações executivas, relações públicas e requisitos de divulgação.
- **Análise de malware:** a engenharia reversa da FireEye analisa malware e escreve decodificadores e analisadores personalizados para fornecer insight sobre os recursos e TTPs usados pelos atacantes.
- **Cobertura de resposta a incidentes 24h por dia, sete dias por semana:** análise de atividade de atacante 24h por dia, sete dias por semana, durante investigação e correção, fornecida pela FireEye Managed Defense.

Nossa abordagem

As investigações da Mandiant incluem análises com base em evento, rede e host para uma avaliação holística e abrangente do ambiente. Nossas ações de resposta são personalizadas para ajudar os clientes na resposta e na recuperação de um incidente, ao mesmo tempo que são gerenciados requisitos regulatórios e o dano à reputação. Durante as investigações, os consultores da Mandiant normalmente identificam:

- Aplicativos, redes, sistemas e contas de usuários afetados
- Software malicioso e vulnerabilidades exploradas
- Informações acessadas ou roubadas

Análise de incidentes

1. **Distribuição de tecnologia/ investigação de indícios preliminares:** distribuir a tecnologia mais apropriada para uma resposta a incidentes rápida e abrangente. Investigamos simultaneamente os indícios preliminares informados pelo cliente para começar a construir indicadores de comprometimento (Indicators of Compromise, IOC) que vão identificar a atividade do atacante durante a varredura do ambiente quanto a todos os indicadores de atividade maliciosa.
2. **Planejamento do gerenciamento de crises:** colaborar com executivos, equipes jurídicas, líderes de negócios e pessoal de segurança sênior para desenvolver um plano de gerenciamento de crises.
3. **Determinação do escopo do incidente:** monitorar a atividade do atacante em tempo real e procurar evidências forenses de atividade prévia do atacante para determinar o escopo do incidente.
4. **Análise detalhada:** analisar as ações tomadas pelo atacante para determinar o vetor de ataque inicial, estabelecer uma linha de tempo da atividade e identificar a extensão do comprometimento. Isso pode incluir:
   - Análise de resposta ao vivo
   - Análise forense
   - Análise de tráfego de rede
   - Análise de logs
   - Análise de malware
5. **Avaliação de danos:** identificar os sistemas, instalações, aplicativos afetados e a exposição de informações.
6. **Correção:** desenvolver uma estratégia personalizada de contenção e correção com base nas ações do atacante, adaptada às necessidades do negócio para eliminar o acesso por parte do atacante e melhorar a postura de segurança do ambiente, de modo a evitar ou limitar os danos decorrentes de futuros ataques.

Materiais entregues

Relatórios executivos, investigativos e de correção que possam ser submetidos ao crivo de terceiros.

- **Resumo executivo:** resumo de alto nível explicando a cronologia e o processo investigativo, as principais descobertas e as atividades de contenção/erradicação.
- **Relatório investigativo:** detalhes sobre a cronologia do ataque e seus caminhos críticos (como o atacante operou no ambiente). Os relatórios incluem uma lista de computadores afetados, localizações, contas de usuário e informações que foram roubadas ou colocadas em risco.
- **Relatório de correção:** detalhes sobre as medidas de contenção/ erradicação tomadas, incluindo recomendações estratégicas para melhorar a postura de segurança da organização.

Suspeita de um incidente? Envie-nos um e-mail para **investigations@mandiant.com** ou visite **https://www.fireeye.com/company/incident-response.html**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Sobre a FireEye, Inc.

A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência de ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e responder a ataques cibernéticos.