NOTA DE SOLUÇÃO

INFOBLOX DOSSIER™

Respostas mais rápidas. Mais contexto. Melhores decisões.

MAIS DO QUE IoCS

Antigamente, a Threat Intelligence (TI) envolvia pouco mais do que hashes de malware, URLs maliciosos e outros IoCs (Indicadores de Comprometimento). No entanto, os defensores de hoje frequentemente necessitam de conhecimentos muito mais profundos de uma ameaça e dos atores por trás dela para preparar defesas, detectar ataques, investigar, caçar ou responder de forma eficaz a ataques cibernéticos modernos, complexos e em múltiplas etapas. Para isso, eles frequentemente dependem de um pequeno arsenal de portais, uma variedade de fontes de TI e muito tempo para filtrar e correlacionar dados dessas fontes díspares na esperança de encontrar a percepção necessária sobre a ameaça atual de interesse.

TORNANDO O SECOPS MAIS EFICIENTE

BloxOne® O BloxOne Threat Defense oferece uma poderosa ferramenta de pesquisa de ameaças, o Dossier, para facilitar e simplificar o trabalho de analistas, pesquisadores de ameaças, equipe de segurança e outros membros da equipe do SOC. Ele automatiza a coleta e a correlação de threat intelligence de dezenas de recursos de código aberto, proprietários ou comerciais premium de sua escolha. Apresenta todas essas informações em uma única consulta, possibilitando que sua equipe se desloque pelos dados disponíveis para receber os insights necessários para concluir as investigações mais rápido e gerar respostas mais rápidas e eficazes.

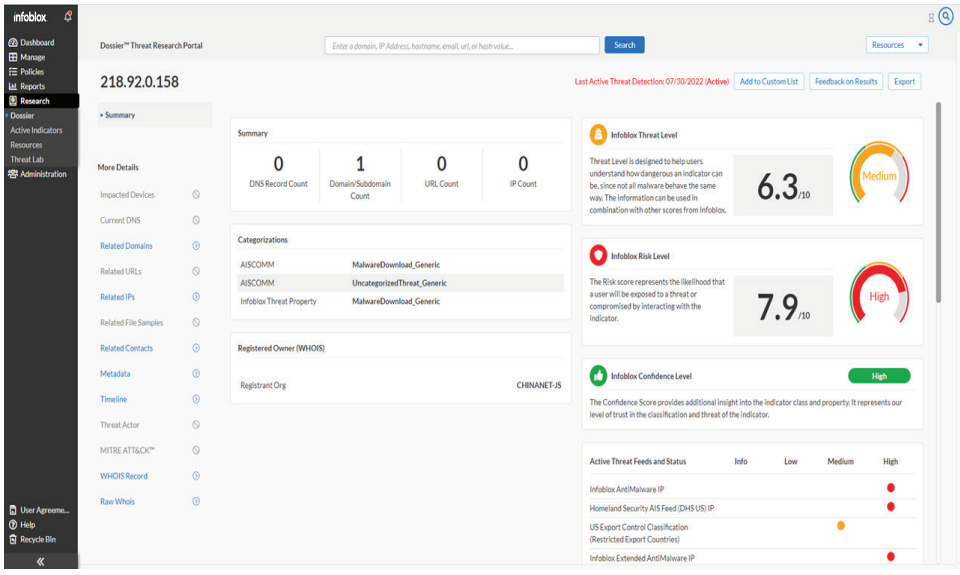

Figura 1: Resumo do dossiê de uma ameaça emergente com links para fácil navegação pelos dados disponíveis

FATOS E DADOS

- O Dossier melhora a velocidade, a qualidade e a precisão de pesquisa, investigação e esforços de resposta em até 67 por cento.
- O Dossier possibilita decisões mais rápidas e imediatamente acionáveis com maior confiança.
- Cerca de 74% dos líderes de segurança e risco reclamam que a investigação média de ameaças leva mais de quatro horas.
- Cerca de 64% dos profissionais afirmam que a investigação de segurança consome muitos recursos.

*Fonte: Forrester Research April 2020, Ponemon Institute 2019, ISC2 Cybersecurity Workforce Study, 2019

CASOS DE USO PODEROSOS UTILIZAM DADOS ACIONÁVEIS

A funcionalidade Infoblox Dossier do BloxOne Threat Defense torna os dados de pesquisa diretamente utilizáveis no nível do DNS através da integração nativa com o BloxOne Threat Defense. A integração direta do Dossier permite que os pesquisadores, a qualquer momento, adicionem imediatamente a ameaça a uma lista de bloqueio. Veja a seguir quatro casos de uso importantes para ilustrar a velocidade, a facilidade de uso e a alta utilidade do Infoblox Dossier:

Caso de Uso nº 1

Compreenda o nível relativo de ameaça e risco para um indicador de ameaça específico

A equipe de operações de segurança do seu banco identificou um URL suspeito associado a um e-mail de spam recebido por várias pessoas em diversos departamentos. Você deseja compreender os possíveis níveis de ameaça e risco. Você insere a URL no Dossier e navega rapidamente para outros dados contextuais importantes sobre o indicador. Este URL foi relatado como um site malicioso por algumas das fontes de threat intelligence do Dossier e associado a cavalos de Troia bancários. A ameaça e o risco são altos, portanto você deve tomar medidas para mitigar essa ameaça. Você adiciona o domínio à sua lista de bloqueio em uma etapa simples. O BloxOne Threat Defense protege imediatamente todos os usuários e dispositivos em qualquer lugar contra o acesso acidental a este domínio malicioso.

Caso de Uso n.° 2

Descubra a penetração de uma ameaça identificada a partir de um alerta da CISA

A Agência de Segurança Cibernética e de Infraestrutura (CISA) emitiu um alerta e advertiu sobre ataques a hospitais por um grupo específico de agentes de ameaças. Existem vários indicadores de ameaça no alerta. Você precisa saber o mais rápido possível se essa ameaça impactou o seu hospital. Você recorre ao Dossier para pesquisar indicadores de ameaças e descobre que ele já foi identificado por vários de seus feeds de threat intelligence e bloqueado. Você navega até os dispositivos afetados do Dossier e vê que nenhuma instância desses indicadores de IP foi utilizada em sua organização. Você percebe imediatamente que sua organização não foi afetada por essa ameaça até o momento.

Caso de Uso #3

Diferencie rapidamente entre registro de domínio e hospedagem de domínio para avaliar o risco

Sua equipe notou um malware aparente se comunicando com o site de uma pequena empresa acessado por um dos membros da sua equipe. O URL deste site não está identificado em nenhum dos seus feeds de ameaças. Ao acessar informações contextuais sobre dados de localização, você descobre que o site dessa pequena empresa local tem um domínio registrado em um país, mas hospedado em outro. Esses dados de localização parecem confirmar a validade de uma ameaça possivelmente perigosa e você adiciona o domínio à sua lista de vigilância imediatamente.

Caso de Uso nº 4

Rastreie a atividade histórica de uma ameaça dentro da sua empresa

Recentemente, você descobriu várias instâncias de um infostealer de malware na sua empresa. Sua equipe realiza pesquisas adicionais no Dossier para compreender quanta atividade já pode ter ocorrido. Os agentes de ameaças frequentemente monitoram a expiração de domínios e agem rapidamente para registrar novamente os sites quando o registro normal não é realizado pelo proprietário legítimo. O Dossiê permite que você acesse a linha do tempo do Dossiê para revisar os principais eventos associados à ameaça. E você pode revisar o registro do domínio e identificar mudanças na propriedade que possam indicar um risco.

Caso de Uso nº 5

Alinhe rapidamente as atividades de resposta com o MITRE ATT&CK™ Framework

Em resposta a uma violação real ou para apoiar um exercício de caça a ameaças, o Dossier apresenta orientações disponíveis do framework MITRE ATT&CK, uma maneira poderosa de classificar e estudar as técnicas dos adversários e entender suas intenções. Esta orientação pode ajudar a acelerar e otimizar a contenção e outras atividades de resposta a incidentes. Somente as ferramentas do MITRE ATT&CK correspondentes à pesquisa atual são exibidas para você usar o MITRE ATT&CK para aprimorar, analisar e testar seus esforços de caça e detecção de ameaças.

PESQUISAS E INVESTIGAÇÕES MAIS EFETIVAS

Navegue facilmente pelos dados coletados e organizados automaticamente pelo Dossier para investigar diferentes aspectos de uma ameaça, seguindo a trilha, para compreender melhor como proteger, detectar ou responder à ameaça de forma mais eficaz. Veja a seguir algumas das principais áreas de dados coletados e disponibilizados para acesso sob demanda.

Dispositivos afetados

Esta lista é criada ao executar uma consulta para o indicador que você está pesquisando. Os dados são provenientes dos logs de relatórios. A exibição está limitada a consultas realizadas nos últimos 30 dias. Se você encontrar uma ameaça, é altamente útil identificar quais dispositivos entraram em contato com o host remoto.

Listas personalizadas

Além dos feeds de threat intelligence predefinidos que a sua assinatura oferece, você pode criar listas personalizadas (contendo domínios e endereços IP) para definir listas de permissão e listas de bloqueio para proporcionar proteção adicional. Você pode usar uma lista personalizada para complementar feeds existentes ou substituir a ação Bloquear, Permitir, Registrar ou Redirecionar atualmente definida para um feed existente. O Dossier permite a edição de listas personalizadas com apenas dois cliques.

Detecção por semelhança

Domínios semelhantes são identificados para os mil principais domínios globais rastreados pela Infoblox. Com o BloxOne Threat Defense Advanced, você pode expandir este recurso para adicionar outros domínios personalizados que deseja monitorar para atividades de imitação.

Contatos Relacionados

Contatos Relacionados mostra os contatos registrados de acordo com os detalhes de registro do domínio. Embora muitos domínios mostrem detalhes limitados, o endereço de e-mail ou número de telefone às vezes é útil para vincular vários domínios a um único proprietário. Um atacante bem-sucedido geralmente conta com centenas de domínios.

Metadados

Os relatórios exibem conteúdo da web relacionado ao indicador de toda a web. Eles podem ser maliciosos, pois não são filtrados e são listados para apresentar uma perspectiva geral sobre a natureza desse indicador.

Cronograma

Este recurso exibe eventos significativos na atividade de ameaças e no histórico de registro de domínios. Você pode identificar alterações na titularidade. As fontes são WHOIS (registros reais), PDNS (DNS passivo observado a partir do tráfego real) e vários feeds, como o SURBL, que rastreiam domínios quando recém-criados.

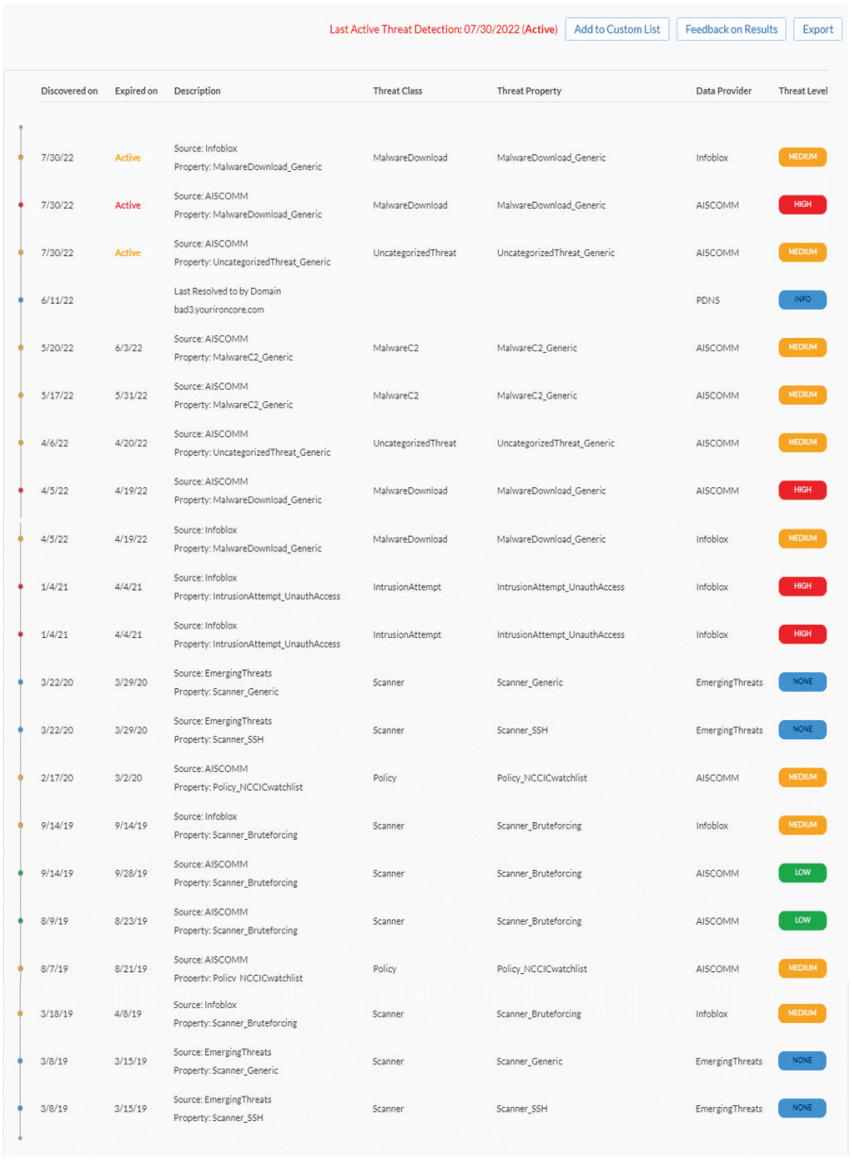

Figura 2: O longo histórico de atividade maliciosa é revelado em torno da origem da atividade de ameaça detectada

Registros DNS atuais

Uma rápida nos tipos comuns de registros DNS pode informar muito sobre os serviços em um host remoto. Mail Exchanger (MX) e ausência de site (A), campos DNS estendidos todos contam uma história sobre a finalidade do host/domínio remoto.

Domínios Relacionados

Esses domínios foram associados ao indicador que está sendo pesquisado com base em várias associações possíveis, como malware que utiliza múltiplos domínios.

URLs relacionadas

Esses sites foram associados ao indicador que está sendo investigado com base em várias possíveis associações, incluindo malware ou spam.

IPs relacionados

Estes são endereços IP que foram associados a este domínio.

Amostras de arquivos relacionados

Essas amostras são baseadas em arquivos possivelmente maliciosos diretamente associados ao domínio/IP. A fonte mais comum seriam os mecanismos de malware (vírus) que relatam arquivos originados de ou comunicados ao domínio.

MITRE ATT&CK™

MITRE ATT&CK™ é uma base de conhecimento acessível globalmente sobre táticas e técnicas de adversários, baseada em observações do mundo real. Apenas as ferramentas do MITRE ATT&CK relevantes para a pesquisa atual são exibidas para você utilizar o MITRE ATT&CK para aprimorar, analisar e testar seus esforços de caça e detecção de ameaças.

Agente de ameaça

Se houver dados disponíveis sobre um agente de ameaça relacionados ao indicador, eles serão exibidos e destacados. Isso ajuda você a aprender sobre eles, suas ferramentas, métodos e possíveis motivações para ataque.

Registro WHOIS

O registro WHOIS baseia-se em registros públicos obtidos de múltiplos registros de domínios e autoridades de IP da Internet. Diversas autoridades entregam mais ou menos dados e, em alguns casos, possibilitam o registro quase anônimo. Se utilizar o registro WHOIS para pesquisar domínios ou IPs, preste muita atenção a dados como o e-mail de contato de “abuso” e os servidores de domínio, pois essas informações podem indicar o proprietário real.

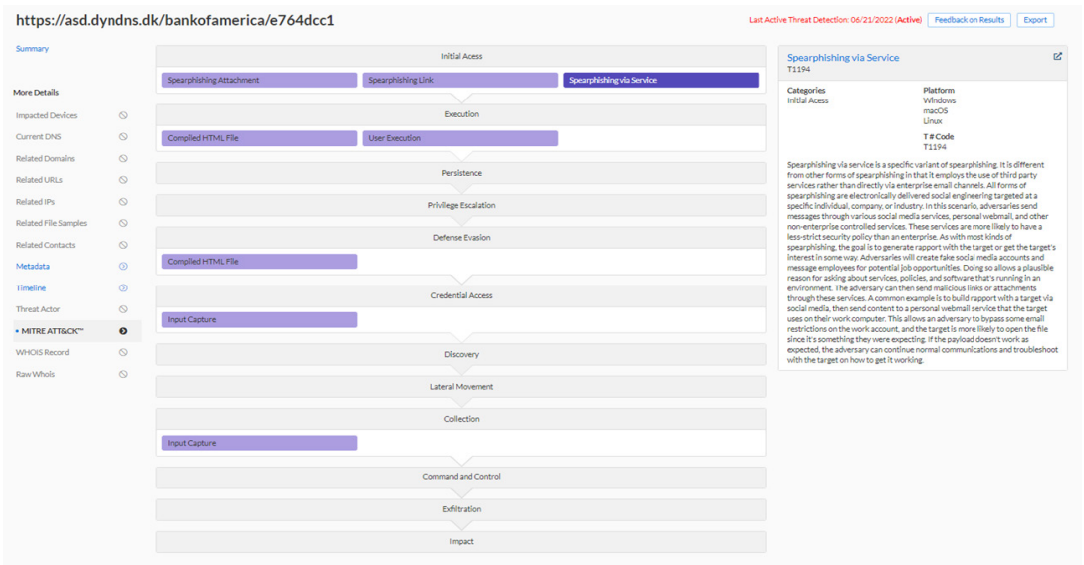

Figura 3: Com base na ameaça sob investigação, o relatório apresenta orientações do framework MITRE ATT&CK.

DESCRIÇÕES DAS FONTES DO DOSSIER

A ferramenta de pesquisa de indicadores de ameaças do Dossier utiliza múltiplas fontes. Utilizando o conjunto de ferramentas do Dossier, os usuários podem tomar decisões precisas mais rápido e com maior confiança com base nas informações contextuais obtidas de uma dezena de fontes simultaneamente. As descrições de origem do dossiê são:

Unidade de Inteligência Cibernética da Infoblox (CIU)

A CIU é a equipe de pesquisa de ameaças da Infoblox responsável pela pesquisa de ameaças (caça, investigação, etc.), tecnologias de detecção (IA, aprendizado de máquina, etc.) e pela agregação e curadoria de threat intelligence de dezenas de fontes para oferecer aos clientes da Infoblox. Esse trabalho potencializa as capacidades de investigação do Dossier, assim como as capacidades defensivas do BloxOne Threat Defense.

DNS atual

Os resultados da pesquisa do Current DNS apresentam todas as informações disponíveis sobre um determinado nome de host a partir dos servidores de nomes DNS.

Metadados

Esta ferramenta apresenta uma visão única de artigos relacionados da web que mencionam ou fazem link para o indicador pesquisado. Os analistas recebem um ambiente seguro para acessar essas informações sem o risco de seguir links potencialmente maliciosos.

Geolocalização

A ferramenta de geolocalização traça as coordenadas identificadas em um mapa, oferecendo precisão no nível de cidade. Outras informações são ISP, cidade, região, latitude/longitude e país.

Google Safe Browsing

O Google Safe Browsing, ou GSB, possibilita que os aplicativos verifiquem URLs em listas constantemente atualizadas do Google de páginas suspeitas de phishing, malware e software indesejado.

Infoblox InfoRanks

A lista InfoRanks oferece os domínios de segundo nível (SLDs) mais populares, atualizados diariamente a partir de um conjunto de dados agregado com base em registros de DNS de várias fontes de dados. O processo para determinar a classificação de cada domínio utiliza informações de contagem com técnicas de inferência estatística para estimar com precisão as classificações verdadeiras dos SLDs ao longo do tempo, tornando-se um substituto poderoso para a agora extinta classificação Alexa. Você pode filtrar os resultados por Domínio ou Classificação clicando no cabeçalho da coluna.

DNS passivo

O DNS passivo é o registro histórico de DNS para nomes de host. Pesquisando um nome de host, o Passive DNS retornará todos os IPs para os quais o nome de host foi resolvido e aqueles capturados pelos sensores do Passive DNS nos últimos 12 meses. Ao pesquisar um IP, o Passive DNS retornará todos os nomes de host que apontaram para esse IP. Observe que nem todas as alterações de DNS são capturadas, portanto haverá informações ausentes.

Reverse DNS

A ferramenta de DNS reverso faz uma consulta reversa de DNS de um endereço IP, pesquisando nas tabelas de registro de nomes de domínio e de registradores.

Whois reverso

Esta ferramenta apresenta dados sobre domínios, como nome, endereço, número de telefone, endereço de e-mail ou endereço físico do registrante listado nos registros Whois atuais ou históricos.

Análise de Malware

A coleta de dados de conteúdo malicioso é identificada pela agregação de mecanismos de antivírus e scanners de sites.

Whois

O Whois é um registro da Internet que lista os proprietários dos domínios e suas informações de contato. Os registros Whois são um recurso essencial para manter a integridade do processo de registro de nomes de domínio e de propriedade de sites. Eles podem revelar informações que ajudam a determinar qualquer risco associado a um domínio.

APIS DO DOSSIER

O Dossier oferece APIs para automatizar a conexão entre soluções relacionadas, como o gerenciamento de informações e eventos de segurança (SIEM) e a orquestração, automação e resposta de segurança (SOAR), aprimorando a experiência geral e melhorando a eficiência da investigação e resposta.

ACESSO PRIORITÁRIO À PESQUISA DE AMEAÇAS DA INFOBLOX

O Dossier oferece o acesso rápido às pesquisas e notícias mais recentes da Unidade de Inteligência Cibernética da Infoblox (CIU) sobre ameaças emergentes, incluindo avisos de ameaças, notas de pesquisa e relatórios de acompanhamento de analistas. E, como um portal nativo da nuvem, seus analistas e pesquisadores podem acessar essas informações em qualquer lugar, a qualquer momento para referência rápida online ou para download como PDFs para facilitar o compartilhamento.

TIDE (INTERCÂMBIO DE DADOS DE THREAT INTELLIGENCE)

O TIDE é outro recurso do BloxOne Threat Defense que pode aprimorar ainda mais a threat intelligence por trás do Dossier e aumentar a eficácia de toda a pilha de segurança.

Assuma o controle de sua threat intelligence e faça o TIDE ingerir e normalize automaticamente a threat intelligence das fontes que você escolher. O Dossier terá acesso instantâneo à sua combinação ideal de threat intelligence para caça e investigação de ameaças. Mas o TIDE também pode distribuir automaticamente sua escolha de feeds de ameaças para outras soluções na pilha de segurança, melhorando suas capacidades de detecção e outras, ajudando-o a obter mais do seu investimento geral em segurança.

Sede Corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1,408,986,4000
www.infoblox.com

Versão: 20230915v1