SOLUTION NOTE

INFOBLOX DOSSIER™

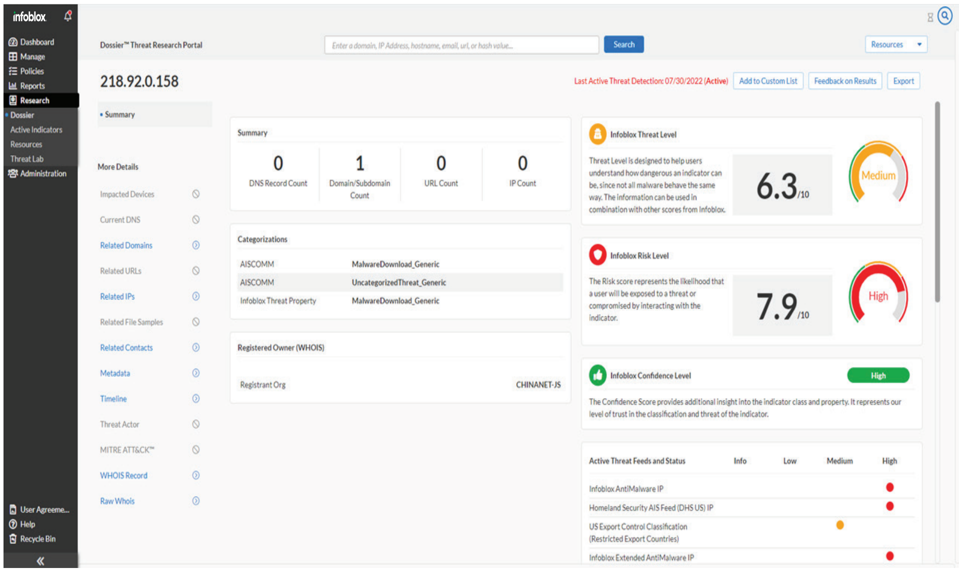
Faster answers. More context. Better decisions.

MORE THAN IoCS

Threat Intelligence (TI) once involved little more than malware hashes, malicious URLs, and other IoCs (Indicators of Compromise). But today's defenders often require a much deeper understanding of a threat, and the actors behind it, to effectively prepare defenses, detect attacks, investigate, hunt, or respond to modern, complex, multistage cyberattacks. To do this they often depend on a small arsenal of portals, a variety of TI sources, and a great deal of time to filter and correlate data from these disparate sources in the hope of finding the necessary insight into the current threat of interest.

MAKING SECOPS MORE EFFICIENT

BloxOne® Threat Defense offers a powerful threat research tool, Dossier, to ease and streamline the efforts of analysts, threat researchers, security staff and other SOC team members. It automates the collection and correlation of threat intelligence from the dozens of open source, proprietary or premium commercial resources of your choice. It presents all of this information in a single view, allowing your team to pivot around available data for the insights needed to complete investigations faster and drive more rapid and effective response.



218.92.0.158

Last Active Threat Detection: 07/30/2022 (Active)

Summary

0	1	0	0
DNS Record Count	Domain/Subdomain Count	URL Count	IP Count

Categorizations

AISCOMM	MalwareDownload_Generic
AISCOMM	UncategorizedThreat_Generic
Infoblox Threat Property	MalwareDownload_Generic

Registered Owner (WHOIS)

Registrant Org	CHINANET-JS

Infoblox Threat Level

Threat Level is designed to help users understand how dangerous an indicator can be, since not all malware behave the same way. The information can be used in combination with other scores from Infoblox.

6.3/10

Infoblox Risk Level

The Risk score represents the likelihood that a user will be exposed to a threat or compromised by interacting with the indicator.

7.9/10

Infoblox Confidence Level: High

The Confidence Score provides additional insight into the indicator class and property. It represents our level of trust in the classification and threat of the indicator.

Active Threat Feeds and Status	Info	Low	Medium	High
Infoblox AntiMalware IP				●
Homeland Security AIS Feed (DHS US) IP				●
US Export Control Classification (Restricted Export Countries)			●	
Infoblox Extended AntiMalware IP				●

Figure 1: Dossier summary of an emerging threat with links for easy pivoting around available data

FACTS & FIGURES

- Dossier improves the speed, quality and accuracy of threat research, investigation and response efforts by as much as 67 percent.
- Dossier empowers quicker and immediately actionable decisions with greater confidence.
- 74 percent of security and risk leaders complain that the average threat investigation takes over four hours.
- 64 percent of practitioners say security investigation is resource intensive.

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

POWERFUL USE CASES LEVERAGE ACTIONABLE DATA

The Infoblox Dossier feature of BloxOne Threat Defense makes research data directly actionable at the DNS level through native integration with BloxOne Threat Defense. Dossier's direct integration enables researchers at any point to immediately add the threat to a block list. Here are four important use cases to illustrate the speed, ease of use, and high utility of Infoblox Dossier:

Use Case #1

Understand the Relative Level of Threat and Risk for a Specific Threat Indicator

Your bank's security operations team has identified a suspicious URL associated with a spam email received by multiple people in several departments. You want to understand its possible threat and risk levels. You enter the URL into Dossier and quickly navigate to other important contextual data about the indicator. This URL has been reported as a malicious website by some of Dossier's threat intelligence sources and associated with banking Trojans. The threat and risk are high, so you must take action to remediate this threat. You add the domain to your block list in one simple step. BloxOne Threat Defense immediately protects all users and devices everywhere from accidentally accessing this malicious domain.

Use Case #2

Uncover the Penetration of an Identified Threat from a CISA Alert

The Cybersecurity and Infrastructure Security Agency (CISA) has sent out an alert and warned of attacks on hospitals by a specific group of threat actors. There are several threat indicators in the alert. You need to know as quickly as possible if this threat has impacted your hospital. You pivot within Dossier to research threat indicators and find that it already has been identified by several of your threat intelligence feeds and blocked. You navigate to the impacted devices within Dossier, and you can see that zero instances of these IP indicators have been used within your organization. You learn immediately that your organization has not been impacted by this threat at this time.

Use Case #3

Rapidly Differentiate between Domain Registration and Domain Hosting to Assess Risk

Your team has noted apparent malware communicating with a small business website accessed by one of your team members. This website URL is not identified on any of your threat feeds. Upon pivoting to contextual information on location data,you find that this local small business website has a domain registered in one country but hosted in another. This location data seems to confirm the validity of a potentially dangerous threat, and you add the domain to your watch list immediately.

Use Case #4

Trace the Historic Activity of a Threat within Your Enterprise

You have recently discovered several instances of a malware infostealer within your enterprise. Your team does additional research within Dossier to understand how much activity might have already occurred. Threat actors often watch for domain expiration and move rapidly to re-register the websites when the timely re-registration was not done by the legitimate owner. Dossier enables you to pivot to the Dossier timeline to review major events associated with the threat. And you can review the domain registration and identify changes in ownership that may indicate a risk.

Use Case #5

Quickly Align Response Activities with the MITRE ATT&CK™ Framework

In response to an actual breach or to support a threat hunting exercise, Dossier provides available guidance from the MITRE ATT&CK framework, a powerful way of classifying and studying adversary techniques and understanding their intent. This guidance can help speed and optimize containment and other incident response activities. Only MITRE ATT&CK tools relevant to the current search are displayed so you can use MITRE ATT&CK to enhance, analyze, and test your threat hunting and detection efforts.

MORE EFFECTIVE RESEARCH AND INVESTIGATIONS

Easily pivot around the data automatically collected and organized by Dossier to investigate different aspects of a threat, following the trail, to better understand how to protect, detect, or respond to the threat more effectively. Here are some of the key areas of data collected and made available for on-demand access.

Impacted Devices

This list is created by running a query for the indicator you are researching. The data comes from the reporting logs. The display is limited to queries made within the past 30 days. If you find a threat, it is highly useful to pinpoint what devices have come into contact with the remote host.

Custom Lists

In addition to the predefined threat intelligence feeds that your subscription offers, you can create custom lists (containing domains and IP addresses) to define allow lists and block lists for additional protection. You can use a custom list to complement existing feeds or override the Block, Allow, Log or Redirect action currently defined for an existing feed. Dossier allows editing of custom lists with two simple clicks.

Lookalike Detection

Lookalikes are identified for the top 1,000 global domains tracked by Infoblox. With BloxOne Threat Defense Advanced, you can expand this feature to add other custom domains that you want monitored for lookalike activity.

Related Contacts

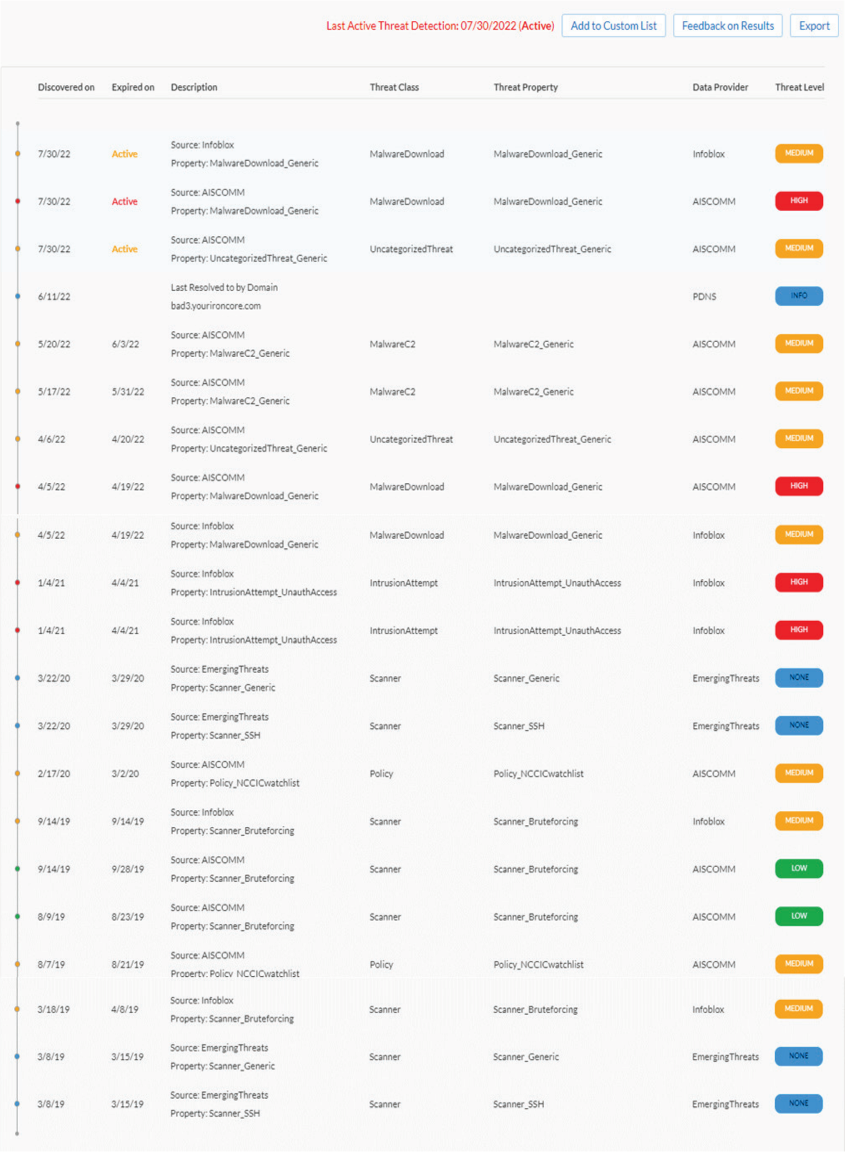
Related Contacts shows registered contacts according to the Domain registration details. While many domains will show limited details, the email address or phone number is sometimes useful to tie multiple domains to a single owner. A successful attacker commonly has hundreds of domains.

Metadata

Reports display web content related to the indicator from around the web. These may be malicious, as they are unfiltered and listed to give an overall perspective on the nature of this indicator.

Timeline

This feature shows significant events in threat activity and the domain registration history. You can identify changes in ownership. Sources include WHOIS (real records), PDNS (passive DNS observed from actual traffic), and various feeds such as SURBL, which track domains when they are newly created.



Discovered on	Expired on	Description	Threat Class	Threat Property	Data Provider	Threat Level
7/30/22	Active	Source: Infoblox Property: MalwareDownload_Generic	MalwareDownload	MalwareDownload_Generic	Infoblox	MEDIUM
7/30/22	Active	Source: AISCOMM Property: MalwareDownload_Generic	MalwareDownload	MalwareDownload_Generic	AISCOMM	HIGH
7/30/22	Active	Source: AISCOMM Property: UncategorizedThreat_Generic	UncategorizedThreat	UncategorizedThreat_Generic	AISCOMM	MEDIUM
6/11/22		Last Resolved to by Domain bad3.youríroncore.com			PDNS	INFO
5/20/22	6/3/22	Source: AISCOMM Property: MalwareC2_Generic	MalwareC2	MalwareC2_Generic	AISCOMM	MEDIUM
5/17/22	5/31/22	Source: AISCOMM Property: MalwareC2_Generic	MalwareC2	MalwareC2_Generic	AISCOMM	MEDIUM
4/6/22	4/20/22	Source: AISCOMM Property: UncategorizedThreat_Generic	UncategorizedThreat	UncategorizedThreat_Generic	AISCOMM	MEDIUM
4/5/22	4/19/22	Source: AISCOMM Property: MalwareDownload_Generic	MalwareDownload	MalwareDownload_Generic	AISCOMM	HIGH
4/5/22	4/19/22	Source: Infoblox Property: MalwareDownload_Generic	MalwareDownload	MalwareDownload_Generic	Infoblox	MEDIUM
1/4/21	4/4/21	Source: Infoblox Property: IntrusionAttempt_UnauthAccess	IntrusionAttempt	IntrusionAttempt_UnauthAccess	Infoblox	HIGH
1/4/21	4/4/21	Source: Infoblox Property: IntrusionAttempt_UnauthAccess	IntrusionAttempt	IntrusionAttempt_UnauthAccess	Infoblox	HIGH
3/22/20	3/29/20	Source: EmergingThreats Property: Scanner_Generic	Scanner	Scanner_Generic	EmergingThreats	NONE
3/22/20	3/29/20	Source: EmergingThreats Property: Scanner_SSH	Scanner	Scanner_SSH	EmergingThreats	NONE
2/17/20	3/2/20	Source: AISCOMM Property: Policy_NCCICwatchlist	Policy	Policy_NCCICwatchlist	AISCOMM	MEDIUM
9/14/19	9/14/19	Source: Infoblox Property: Scanner_Bruteforcing	Scanner	Scanner_Bruteforcing	Infoblox	MEDIUM
9/14/19	9/28/19	Source: AISCOMM Property: Scanner_Bruteforcing	Scanner	Scanner_Bruteforcing	AISCOMM	LOW
8/9/19	8/23/19	Source: AISCOMM Property: Scanner_Bruteforcing	Scanner	Scanner_Bruteforcing	AISCOMM	LOW
8/7/19	8/21/19	Source: AISCOMM Property: Policy_NCCICwatchlist	Policy	Policy_NCCICwatchlist	AISCOMM	MEDIUM
3/18/19	4/8/19	Source: Infoblox Property: Scanner_Bruteforcing	Scanner	Scanner_Bruteforcing	Infoblox	MEDIUM
3/8/19	3/15/19	Source: EmergingThreats Property: Scanner_Generic	Scanner	Scanner_Generic	EmergingThreats	NONE
3/8/19	3/15/19	Source: EmergingThreats Property: Scanner_SSH	Scanner	Scanner_SSH	EmergingThreats	NONE

Figure 2: The long history of malicious activity is revealed around the source of detected threat activity

Current DNS Records

A quick glance to see common DNS record types tells you a lot about the services on a remote host. Mail Exchanger (MX) and no website (A), extended DNS fields all tell a story about the purpose of the remote host/domain.

Related Domains

These domains have been tied to the indicator being researched based on many possible associations, such as malware that uses multiple domains.

Related URLs

These websites have been tied to the indicator being researched based on many possible associations, including malware or spam.

Related IPs

These are IP addresses that have been tied to this domain.

Related File Samples

These samples are based on possibly malicious files directly associated with the domain/IP. The most common source would be malware (virus) engines that report on files originating from or communicating to the domain.

MITRE ATT&CK™

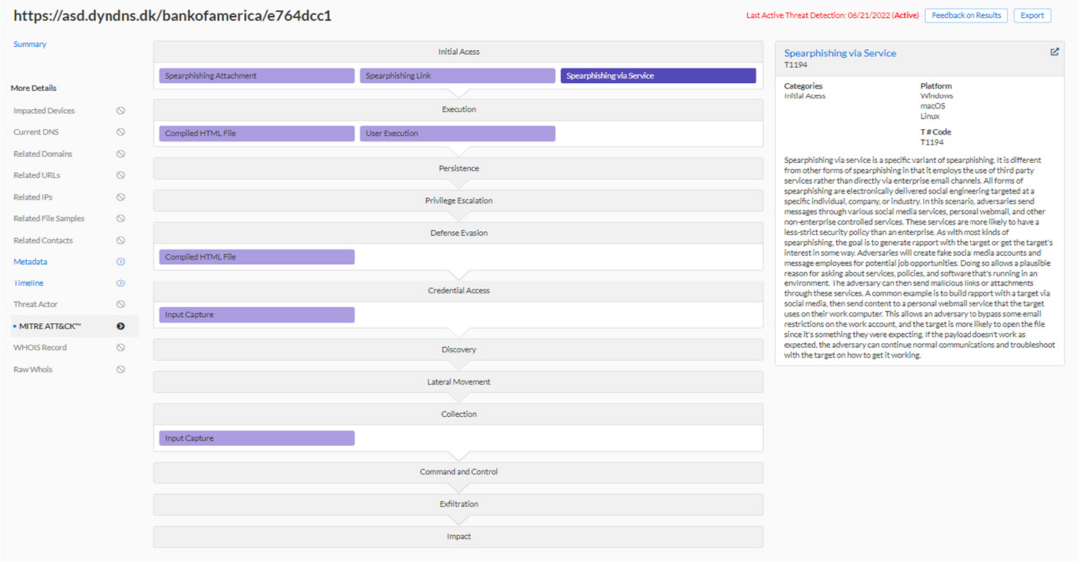
MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. Only MITRE ATT&CK tools relevant to the current search are displayed so you can use MITRE ATT&CK to enhance, analyze, and test your threat hunting and detection efforts.

Threat Actor

If data on a threat actor is available related to the indicator, then it will be shown and highlighted. This helps you to learn about them, their tools, methods and possible motivations for attack.

WHOIS Record

WHOIS Record is based on public records obtained from multiple domain registrations and Internet IP authorities. Different authorities provide more or less data, and in some cases allow nearly anonymous recording. When using WHOIS record for researching domains or IPs, pay close attention to data such as the "abuse" contact email and domain servers, as this information might point you to the actual owner.



https://asd.dyndns.dk/bankofamerica/e764dcc1

Last Active Threat Detection: 06/21/2022 (Active)

Spearphishing via Service
T1194

Categories
Initial Acess

Platform
Windows
macOS
Linux

T # Code
T1194

Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries send messages through various social media services, personal webmail, and other non-enterprise controlled services. These services are more likely to have a less-strict security policy than an enterprise. As with most kinds of spearphishing, the goal is to generate rapport with the target or get the target's interest in some way. Adversaries will create fake social media accounts and message employees for potential job opportunities. Doing so allows a plausible reason for asking about services, policies, and software that's running in an environment. The adversary can then send malicious links or attachments through these services. A common example is to build rapport with a target via social media, then send content to a personal webmail service that the target uses on their work computer. This allows an adversary to bypass some email restrictions on the work account, and the target is more likely to open the file since it's something they were expecting. If the payload doesn't work as expected, the adversary can continue normal communications and troubleshoot with the target on how to get it working.

Figure 3: Based on the threat under investigation, this report provides guidance from the MITRE ATT&CK framework.

DOSSIER SOURCE DESCRIPTIONS

The Dossier threat indicator research tool uses multiple sources. Using the Dossier toolset, users can make accurate decisions more quickly and with greater confidence based on the contextual information obtained from a dozen sources simultaneously. Dossier source descriptions include:

Infoblox Cyber Intelligence Unit (CIU)

The CIU is the Infoblox threat research team, responsible for threat research (hunting, investigation, etc.), detection technologies (AI, Machine Learning, etc.), and the aggregation and curation of threat intelligence from dozens of sources to provide Infoblox customer. This work powers Dossier investigation capabilities as well as the defensive capabilities of BloxOne Threat Defense.

Current DNS

Search results from Current DNS furnish all the available information about a given hostname from DNS nameservers.

Metadata

This tool supplies a single view into related articles from the web that mention or link to the searched indicator. Analysts are provided a safe environment to access this information without the risk of following potentially malicious links.

Geolocation

The geolocation tool plots the identified coordinates on a map, providing city-level accuracy. Other information includes ISP, city, region, latitude/longitude and country.

Google Safe Browsing

Google Safe Browsing, or GSB, enables applications to check URLs against Google’s constantly updated lists of suspected phishing, malware and unwanted software pages.

Infoblox InfoRanks

The InfoRanks list provides the most popular second-level domains (SLDs) updated each day from an aggregated dataset based on DNS records from various data sources. The process to determine the rank for each domain uses count information in combination with statistical inference techniques to accurately estimate the SLDs’ true ranks over time, making it a powerful replacement for the now defunct Alexa rank. You can filter the results by Domain or Rank by clicking the column header.

Passive DNS

Passive DNS is the historical DNS record for hostnames. When searching a hostname, Passive DNS will return all IPs that the hostname has resolved to and those caught by the Passive DNS sensors in the previous 12 months. When searching an IP, Passive DNS will return all hostnames that have pointed to that IP. Note that not every DNS change is caught, so there will be missing information.

Reverse DNS

The Reverse DNS tool performs a reverse DNS lookup of an IP address by searching domain name registry and registrar tables.

Reverse Whois

This tool provides you with data on domains such as name, address, telephone number, email address or physical address of the registrant listed in current or historical Whois records.

Malware Analysis

Data collection of malicious content is detected by aggregation of antivirus engines and website scanners.

Whois

Whois is an Internet record listing that identifies who owns a domain and their contact information. Whois records are an essential resource for maintaining the integrity of the domain name registration and website ownership process; they can reveal information to help determine any risk associated with a domain.

DOSSIER APIS

Dossier provides APIs to make connecting between related solutions—like security information and event management (SIEM) and security orchestration, automation and response (SOAR)—automatic, enhancing the overall experience and improving investigation and response efficiency.

PRIORITY ACCESS TO INFOBLOX THREAT RESEARCH

Dossier provides quick access to the most recent research and news from the Infoblox Cyber Intelligence Unit (CIU) on emerging threats including threat advisories, research notes and follow-up analyst reports. And, as a cloud-native portal, your analysts and researchers can access this information anywhere, anytime for quick reference on-line or to download as PDFs for easier sharing.

TIDE (THREAT INTELLIGENCE DATA EXCHANGE)

TIDE is another feature of BloxOne Threat Defense that can further enhance the threat intelligence behind Dossier, and uplift the effectiveness of the entire security stack.

Take control of your threat intelligence and have TIDE automatically ingest and normalize threat intelligence from the sources you choose. Dossier will have instant access to your optimal blend of threat intelligence for threat hunting and investigation. But TIDE can also auto-distribute your chose of threat feeds to other solutions in the security stack, uplifting their detection and other capabilities, and helping you to get more out of your overall security investment.

infoblox

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20230915v1