

THREAT INTELLIGENCE PLAYBOOK:

MAKING SENSE OF INDICATORS

THE RISE OF RANSOMWARE

In 2017, organizations around the world realized that a new era of cyber threats had dawned. Ransomware has advanced significantly and is now capable of taking out infrastructure and operations across the globe, weaponizing known vulnerabilities such as EternalBlue and crippling businesses for months or more. WannaCry marked the start of these techniques and was one of the most damaging ransomware attacks in history. It was followed by NotPetya, and most recently, Bad Rabbit, the third major attack to cause widespread disruption this year.

Organizations struggle to quickly respond to or remediate these intrusions for many reasons—first and foremost to contain an attack. Other reasons for quick action include managing the high volume of security alerts they receive each day, and gaining knowledge about an attacker's infrastructure. Many organizations are bogged down in reactive work and often overlook the value of crucial information. This leads to organizations missing some of the most critical insights their alerts and indicators can provide to shift to a more proactive posture.

A critical part of arming against increasingly aggressive malware, ransomware and threat actors is to develop and use threat intelligence in a strategic way during investigations. Doing this requires in-depth analysis of threat data, including indicators, to gain deeper knowledge about the types of threats attempting to penetrate an organization. Indicators are made up of both threat data and threat intelligence, and investigators use these types of information to identify malicious actors and their activities. While threat data includes single pieces of isolated information with no context applied (such as IP address or suspicious URLs), threat intelligence is the contextualization of that information. Analysis is done on the threat data to determine if it is important to the security needs of a specific organization, and then used to support investigation or threat hunting activities.

494 IT professionals were surveyed about Threat Intelligence in an April 2016 SANS Institute Report.

86%

Said their organizations engage in some type of threat intelligence gathering or hunting activity.

75%

Said they had reduced their attack surface as a result.

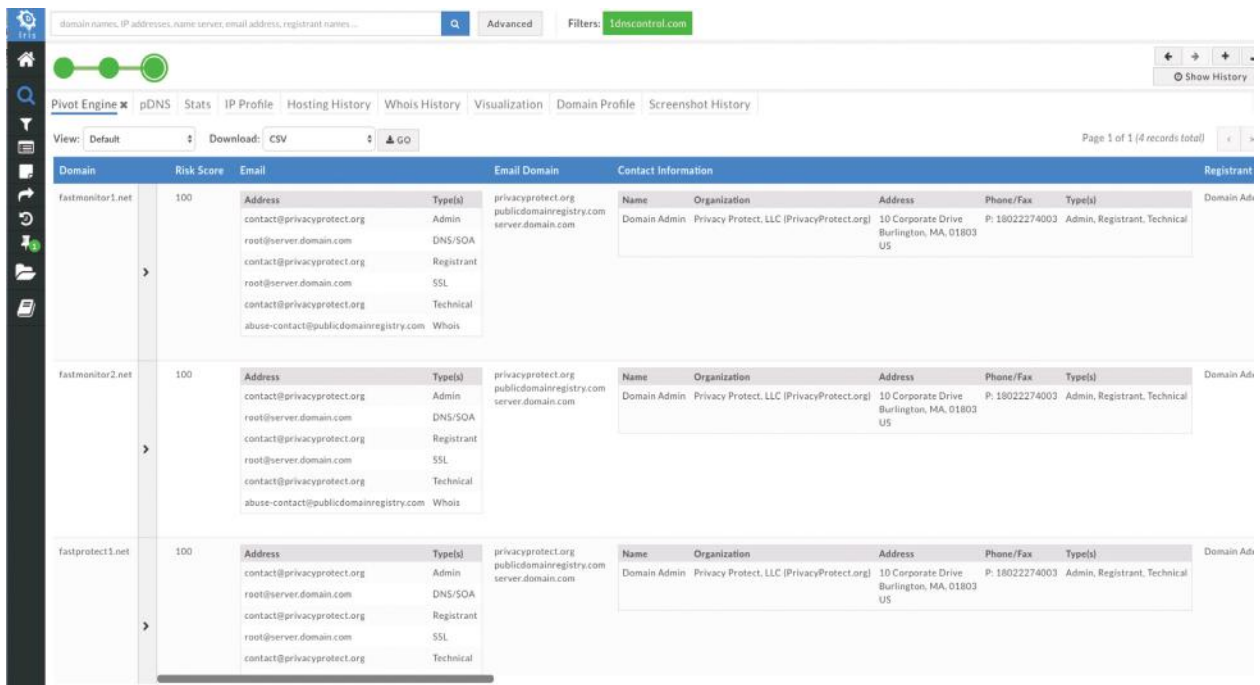
+50%

Said they had not implemented a formal program or repeatable process for investigating threat, illustrating the need for more industry education on how organizations can improve threat intelligence and act on their indicators.

This paper will outline the distinctions between Indicators of Compromise (IOCs) and Indicators of Attack (IOAs), their uses and attributes and how they can be uniquely leveraged to enrich cybersecurity investigations.

Following the Bad Rabbit outbreak, DomainTools researchers explored the attacker’s command and control infrastructure that had been made public by security analysts to investigate the attack further. Pivoting on the IOCs in DomainTools Iris and correlating them with other historical data, the analysts identified four additional domains related to the Bad Rabbit infrastructure.

In this specific example, using DomainTools Iris platform, the BadRabbit distribution domain of 1dnscontrol[.]com can be used as an initial pivot point. Looking at the historical name server of 1dnscontrol[.]com gives the analyst four additional domains related to BadRabbit infections and distribution. During a known or suspected outbreak, these would be important domains to block or flag for alerting.



Domain	Risk Score	Email	Email Domain	Contact Information	Registrant										
fastmonitor1.net	100	<ul style="list-style-type: none"> Address: contact@privacyprotect.org Type(s): Admin Address: root@server.domain.com Type(s): DNS/SOA Address: contact@privacyprotect.org Type(s): Registrant Address: root@server.domain.com Type(s): SSL Address: contact@privacyprotect.org Type(s): Technical Address: abuse-contact@publicdomainregistry.com Type(s): Whois 	<ul style="list-style-type: none"> privacyprotect.org publicdomainregistry.com server.domain.com 	<table border="1"> <thead> <tr> <th>Name</th> <th>Organization</th> <th>Address</th> <th>Phone/Fax</th> <th>Type(s)</th> </tr> </thead> <tbody> <tr> <td>Domain Admin</td> <td>Privacy Protect, LLC (PrivacyProtect.org)</td> <td>10 Corporate Drive Burlington, MA, 01803 US</td> <td>P: 18022274003</td> <td>Admin, Registrant, Technical</td> </tr> </tbody> </table>	Name	Organization	Address	Phone/Fax	Type(s)	Domain Admin	Privacy Protect, LLC (PrivacyProtect.org)	10 Corporate Drive Burlington, MA, 01803 US	P: 18022274003	Admin, Registrant, Technical	Domain Ad
Name	Organization	Address	Phone/Fax	Type(s)											
Domain Admin	Privacy Protect, LLC (PrivacyProtect.org)	10 Corporate Drive Burlington, MA, 01803 US	P: 18022274003	Admin, Registrant, Technical											
fastmonitor2.net	100	<ul style="list-style-type: none"> Address: contact@privacyprotect.org Type(s): Admin Address: root@server.domain.com Type(s): DNS/SOA Address: contact@privacyprotect.org Type(s): Registrant Address: root@server.domain.com Type(s): SSL Address: contact@privacyprotect.org Type(s): Technical Address: abuse-contact@publicdomainregistry.com Type(s): Whois 	<ul style="list-style-type: none"> privacyprotect.org publicdomainregistry.com server.domain.com 	<table border="1"> <thead> <tr> <th>Name</th> <th>Organization</th> <th>Address</th> <th>Phone/Fax</th> <th>Type(s)</th> </tr> </thead> <tbody> <tr> <td>Domain Admin</td> <td>Privacy Protect, LLC (PrivacyProtect.org)</td> <td>10 Corporate Drive Burlington, MA, 01803 US</td> <td>P: 18022274003</td> <td>Admin, Registrant, Technical</td> </tr> </tbody> </table>	Name	Organization	Address	Phone/Fax	Type(s)	Domain Admin	Privacy Protect, LLC (PrivacyProtect.org)	10 Corporate Drive Burlington, MA, 01803 US	P: 18022274003	Admin, Registrant, Technical	Domain Ad
Name	Organization	Address	Phone/Fax	Type(s)											
Domain Admin	Privacy Protect, LLC (PrivacyProtect.org)	10 Corporate Drive Burlington, MA, 01803 US	P: 18022274003	Admin, Registrant, Technical											
fastprotect1.net	100	<ul style="list-style-type: none"> Address: contact@privacyprotect.org Type(s): Admin Address: root@server.domain.com Type(s): DNS/SOA Address: contact@privacyprotect.org Type(s): Registrant Address: root@server.domain.com Type(s): SSL Address: contact@privacyprotect.org Type(s): Technical 	<ul style="list-style-type: none"> privacyprotect.org publicdomainregistry.com server.domain.com 	<table border="1"> <thead> <tr> <th>Name</th> <th>Organization</th> <th>Address</th> <th>Phone/Fax</th> <th>Type(s)</th> </tr> </thead> <tbody> <tr> <td>Domain Admin</td> <td>Privacy Protect, LLC (PrivacyProtect.org)</td> <td>10 Corporate Drive Burlington, MA, 01803 US</td> <td>P: 18022274003</td> <td>Admin, Registrant, Technical</td> </tr> </tbody> </table>	Name	Organization	Address	Phone/Fax	Type(s)	Domain Admin	Privacy Protect, LLC (PrivacyProtect.org)	10 Corporate Drive Burlington, MA, 01803 US	P: 18022274003	Admin, Registrant, Technical	Domain Ad
Name	Organization	Address	Phone/Fax	Type(s)											
Domain Admin	Privacy Protect, LLC (PrivacyProtect.org)	10 Corporate Drive Burlington, MA, 01803 US	P: 18022274003	Admin, Registrant, Technical											

This provides a clear example for how indicators can be utilized proactively to block and monitor dangerous domains.

“Threat data is traditionally from internal incident response or external sources, and organizations must do the analysis necessary to turn that data into intelligence that can be used to improve their overall security posture.”

- Senior Security Researcher at DomainTools

UNDERSTANDING IOCS

Several data elements can make up an IOC, which is typically observed after an initial attack or compromise. IOCs often fall into one of four categories:



Command and control domains and DNS requests, which provide pivot points to look for additional attacker infrastructure.



File attributes, such as filenames, file languages and vulnerable file types that raise red flags.



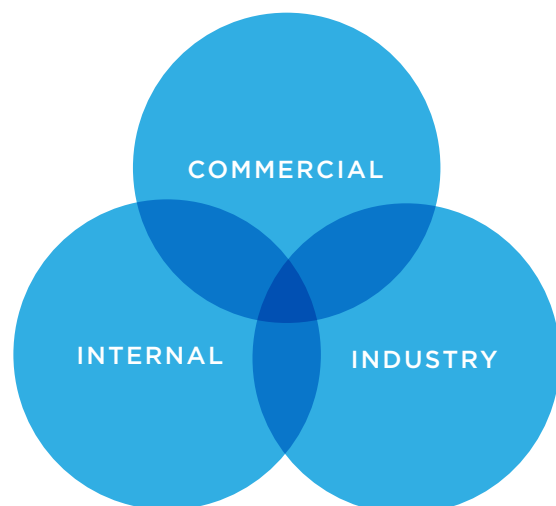
IP addresses, similar to domains, can be explored in Passive DNS to uncover more about an attacker.



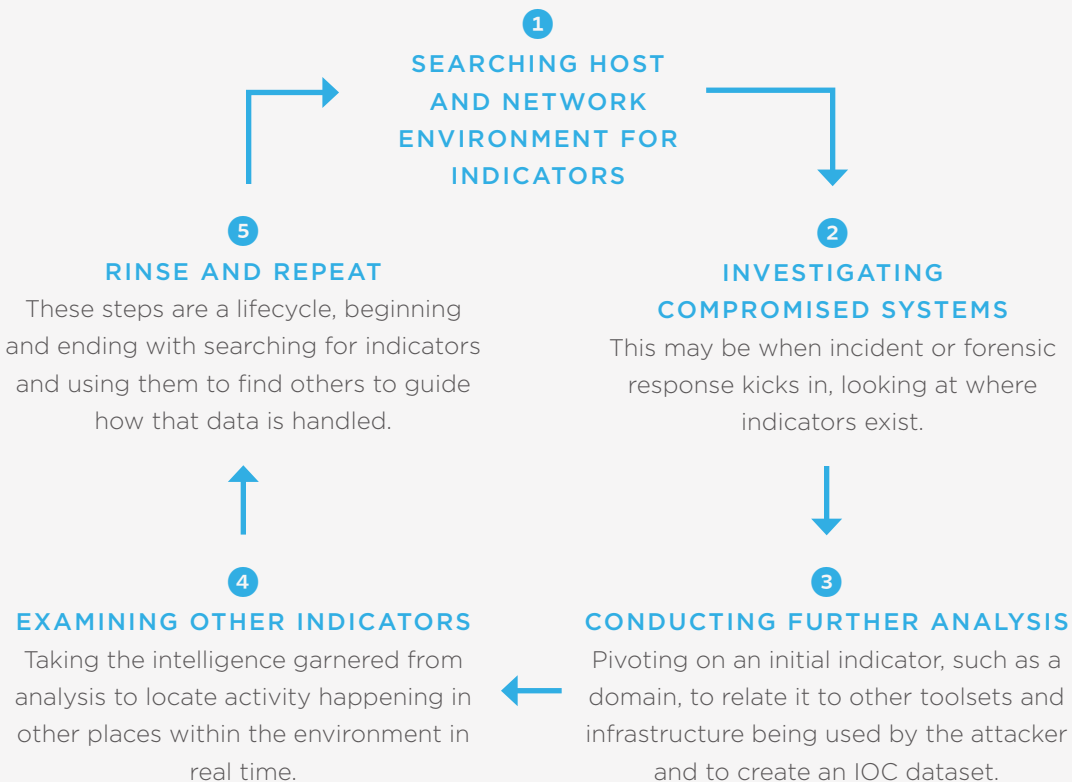
Hashes, when on a host or network can be analyzed for maliciousness – and because they are unique, they can quickly reveal additional important information.

IOCS CAN ORIGINATE FROM SEVERAL SOURCES:

- >> **Internal:** Activity and incident response engagements on the host or network, such as suspicious communications or changes in schedule rotation found in log files. This may also include URI strings on the network, which can give detailed information about an attack.
- >> **Commercial:** API feeds, which are not contextualized, but provide IOC data that can be further analyzed. Many of these are available as part of paid subscriptions.
- >> **Industry:** Blogs, APT reports, white papers, ISACs lists, free blacklists and other industry sources aimed at threat data sharing.



Properly processing an IOC, and converting that data into threat intelligence that identifies malicious behavior, requires a roadmap of steps to take. By taking these steps, security analysts can utilize IOCs to proactively develop rules that monitor and block identified threats and infrastructure, retroactively perform forensics to detect and stop lateral movement, potentially stop data exfiltration and strengthen incident response to triage and remediate. Steps include:



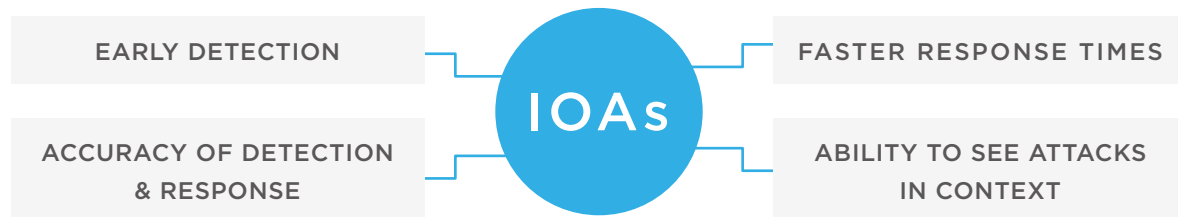
There are a handful of tools to help generate, analyze and pivot on IOCs. As mentioned in the Bad Rabbit example, DomainTools Iris can be used to cluster IOCs in a way that unveils additional related indicators. This allows the security team to proactively or retroactively build out intelligence on the attacker infrastructure and block or monitor as needed.

SHARING IOCS

Sharing this IOCs across an organization and with partners, customers and law enforcement is also important, and there are several formats to do so. STIX, a structured and standardized language for presenting threat information, is a favorite format among many investigators and supports data elements including incidents, exploits and other observables. The companion technology TAXII, serves as a 'roadway' for transferring STIX or other threat intelligence securely. CybOX is also useful, and can classify domains, email attachments and patterns as observables, enabling the trade of in-depth information across many defined objects.

UNDERSTANDING IOAS

Although IOCs do provide significant value, they have their limitations. IOCs must be a known artifact, and not always timely. IOCs may not detect malware in volatile memory or malware-free intrusions and threats from 0-days. This is where Indicators of attack (IOAs) become incredibly important, as they overcome these limitations.



IOAs are events that may reveal an active attack before IOCs become visible. These indicators focus on detecting the intent of a particular attacker or threat group. IOAs are comprised of three broad classifications:



Unknown attributes such as a zero-day, or malware that is in memory.



IOC analysis that enables threat hunting on specific domains or other attributes.



Contextual information about whether an attack is valid, where it is coming from or how severe it may be.

IOAs typically originate from the following internal data sources:

- >> Firewall rule logs
- >> SIEM logs
- >> Proxy rule logs
- >> IDS/IPS rule logs
- >> AV logs
- >> Endpoint security logs
- >> Network infrastructure logs
- >> Application/Database/Webserver logs

As with IOCs, human analysis is where the real value of this data is realized. Doing this will provide context around a specific threat actor and perspective on how to proactively block their campaigns or attacks. IOA analysis enables early detection, faster response times, the ability to predict lateral movements and more accurate network rules for defensive security, ultimately reducing dwell-time. When analyzing IOAs, investigators are looking for red flags and performing analysis on them to find suspicious behavior, early attack stages, signs the environment is being profiled and open services being prodded. Analysts can find this data by evaluating some of the following:

- >> User activity
- >> Vulnerability info
- >> Server/host activity
- >> Application activity
- >> Network activity /registry changes
- >> Database activity
- >> Security device activity

It is also important to define the many attributes IOAs may include, such as system attributes, network attributes, malware attributes and email attributes. This allows a security team to make a baseline of the environment so analysts can easily detect IOAs when standard attributes change. For example, email data in the From, Received and Message-ID fields can include potential IOAs. Further analysis of unusual email headers may reveal dangerous phishing attempts or provide insight into an actual attacker. Pivoting on known malware attributes can lead to the identification of other malware that might be used by the same attackers.

Searching user accounts can also uncover IOAs. User accounts that have the most access to distinct hosts, such as a single user that can access many hosts across the globe, may indicate a threat actor trying to laterally move across the network or exfiltrate data. Similarly, identical file blocking across the enterprise can signal a potential attack being attempted simultaneously on multiple hosts.

MAKING THE MOST OF INDICATORS

In the context of an investigation, we can note IOCs as historical, and known bad, and IOAs as proactive, only considered “bad” based on the context of the environment and additional data. IOCs are typically pulled from actual compromises and used to reactively identify malicious behavior and pivot on historical context to improve future security. Because IOAs provide investigators with insights into an attacker’s behaviors, persistence and stealth mechanisms in real time, they can help stop threat actors in their tracks.

The end objective of leveraging indicators is to automate much of the analysis so that it can lead to intelligent alerts that signal the security team to take action. When we understand the difference between IOCs, which are mainly seen after the fact, and IOAs, which are more proactive, we can begin to realize what the indicators are, how they can help us and how to use them across our environments.

“Leveraging IOAs helps us cut down on the dwell time for an attacker, ideally preventing them from moving forward into the environment and doing major damage. The key is finding these indicators before they compromise systems.”