RSA SOLUTION OVERVIEW

Advanced Threat Detection and Response with RSA® NetWitness® Logs and Packets

SPOTTING ADVANCED THREATS WITH BEHAVIOR ANALYTICS AND DATA SCIENCE MODELING

Using Behavior Analytics and Data Science to Identify Covert Channels and C2 Threats

Security professionals increasingly suffer a "needle-in-the-haystack" problem. Security tools – especially rule-based ones – along with systems, applications, and infrastructure, create so much data that it has become extremely difficult to uncover the signal of a real attack. The use of automated data analytics has become a central component of modern security architectures. Behavior analytics tools, in particular, help make sense of this vast amount of data, and speed threat detection and response without the need for signatures or analyst tuning. This approach makes it easier for security organizations of any maturity to gain visibility into behavior patterns, detect high risk anomalies, lateral movement and ultimately find malicious actors before they can impact the business.

While many vendors claim to use behavioral techniques, their effectiveness is constrained because they fail to utilize true data science models, and they rely on log data alone. Log data, which is often driven by alerts from preventative controls, does not provide the needed visibility to find today's attacks. The data ingested into the system is as important as the analytical models themselves. Augmenting logs with packet, netflow and endpoint data, along with business context and threat intelligence prior to performing multiple types of analytics is necessary. Without this visibility, security analysts can miss the full scope of a compromise, where signals from diverse systems reveal attacks that are virtually impossible to isolate with any single data set.

Combining disparate data, enriching it with business context and threat intelligence, and utilizing automated behavior analytics provides the fastest path to mitigate threats prior to business impact. This is what we refer to as a business-driven security strategy: linking business context with security incidents to detect and respond faster in a prioritized way to ultimately protect what matters most.

Today's threats hide their activity among all the other things that are happening in complex IT environments. These threats rely on the assumption that security teams have neither the tools nor the time to investigate deeply enough to distinguish between their activity and those of employees, customers or partners. Today's sophisticated attackers use ways to get information in and out of the organization that evade detection, leveraging what are known as "covert channels" that enable "command and control" (C2) of resources. Many successful recent public attacks have covert channels communicating with C2 servers that can fully compromise systems. For example:

- Phishing scams typically use covert channels to deliver malware to victims, making it difficult to spot that initial "click" on the offending link.

- After compromise, today's threats often use covert channels to effect command and control of victim endpoints, hiding communication traffic amongst normal web traffic.

In addition to behavior analytics to detect C2 activity, using data science techniques to reveal the use of covert channels means that security teams can spot these sophisticated threats quicker, and reduce the likelihood that an attack harms the organization.

Beaconing Hosts Communicating with Command and Control Sites

When an internal host gets compromised, attackers typically open a "backdoor" to allow communication between a C2 site and the compromised system. Since most organizations have a restrictive policy around the inbound connections they will accept, the attackers get around this by equipping the compromised host to regularly "phone home" to pick up instructions for launching the next stage of the attack.

Internal hosts "beaconing" to a C2 host at a high level looks very much like any other http traffic, say for example regularly polling a news site, but there are often clues to distinguish it from communications activity with normal hosts if one looks more carefully. Among others, these indicators include:

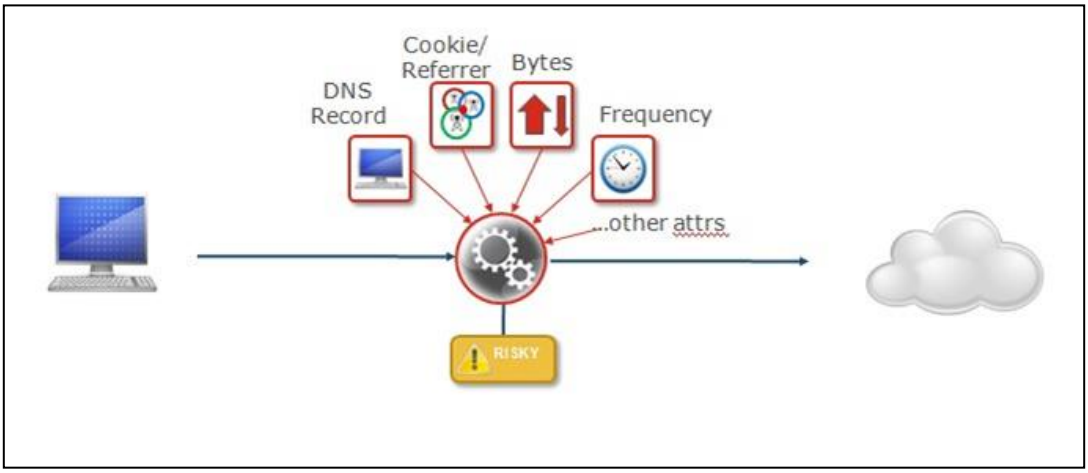
• **Frequency of communications.** Typical beaconing happens at a regular but relatively infrequent cadence, for short periods of time – this is in contrast to standard web traffic, which is usually either "one-time" or more frequent.

• **Bytes uploaded vs downloaded.** Typical web sessions initiated by humans download far more than they upload – web servers serve up pictures and other content as a result of a URL request. However, malicious sessions often upload far more than just a short request for a URL.

• **Use of cookies.** Typical web sessions place multiple cookies within the user's browser to track user activity across that website and others. Malicious sessions seldom use cookies.

• **Use of referrer strings.** The vast majority of web sessions come from the user clicking on a hyperlink, resulting in a "referrer string" in the URL request. Malicious sessions generated from local malware generally don't.

• **URL lengths.** Because people are supposed to remember high-level URLs (such google.com, cnn.com etc.), they are usually short in length. However malicious services often embed themselves deep down in web servers, resulting in unusually long destination URL generated from within the organization.



Specifying hard and fast alert thresholds for any of these individual metrics is inherently difficult, and therefore error prone. Thus, applying data science analytics is essential to identifying "outliers" from normal traffic, while taking into consideration many of these factors at the same time.

Why Spotting the Use of Covert Channels is a Challenge

Spotting covert channel activity falls into two areas – looking at both inbound and outbound connections, detecting internal hosts with anomalous outbound communication patterns, and spotting those external hosts that are most likely to be compromised. Two common symptoms of covert channel activity are:

• **Beaconing** – where an internal host periodically connects to a C2 host controlled by the attacker, an activity that is designed to look like normal web browsing traffic.

• **Suspicious domains** – where an attacker obfuscates the source of attacks by hiding itself among the millions of domains that users in the organization talk to.

The problem is, neither of these symptoms are easy to spot using signatures or any hard and fast detective rules. However, most covert channel activity leave behind clues that, if detected, can help to distinguish malicious from normal traffic. Making a determination as to whether an internal or external host is suspicious involves collecting and examining multiple pieces of data over extended time periods, detecting deviations for regular behaviors and creating a probability-weighted risk score based upon the results.

Suspicious Internet Domains Hide Among Normal Traffic

Perpetrators of scams often compromise existing hosts on the Internet, and redirect victims toward these sites to either collect private information, or to deliver malware. Many conventional security defenses maintain "watch lists" of known IP addresses and domain names that host these attacker services. However, to thwart these static defenses, attackers often use "fast flux" techniques, compromising many hosts, registering many domains and redirecting different victims to different domain through different servers, making effective static watch lists almost impossible to compile and maintain.

Suspicious domains can be tricky to spot, and identification generally relies upon inspecting raw traffic going to and from those domains. For example:

• **Number of IP addresses associated with a domain**. Most conventional domains only have a few IP addresses associated with them. Malicious domains often have dozens of IP addresses associated with them to evade static IP watch lists.

• **Number of domain name owners associated with a DNS address**. Most conventional IP addresses are only associated with a few domain owners. Malicious servers and domains often a have complex many-to-many system of IP addresses, to domain hosts, and to domain owners, so a high number of domain owners associated with a system is suspicious.

• **Number of users hitting those domains relative to its complexity**. A popular domain like Google or Yahoo, or a popular hosting service (Amazon EC) will have lots of domain names and IP addresses associated with it. But then again, since it is popular, many users will likely be accessing it. On the other hand, a domain that few people are accessing, but with dozens of IP addresses and owners is more likely to be malicious.

• **Traffic content types**. Most conventional servers have one or two roles; they are either web servers, mail servers, DNS servers, etc. Suspicious domains often host many services on the same server.

• **GETS vs PUT/POSTs**. Most web servers serve up far more content than people upload to it. Domains where the ratio of POSTs to GETs is high are more likely malicious. Similar to the beaconing host example above relating static and fixed ratios for these values can be highly error prone, requiring more advanced data science techniques to essentially identify those outliers from normal, taking into consideration many indicative factors at once.

RSA Integrates Real-time Behavior Analytics to Rapidly Identify "Command and Control" Activity

At a high level, internal hosts "beaconing" to a C2 host look very much like any other http traffic -- for example, regularly polling a news site. But there are often clues to distinguish C2 traffic from communications activity with normal hosts. Among others, these indicators include: frequency of communications, how long ago the domain was registered, strange user agents, lack of referrer, or domains not connected to very often. By gathering and analyzing this data – over long time horizons and in real time – defenders can identify a beaconing host's "tell."

RSA NetWitness Logs and Packets Behavior Analytics C2 module evaluates web traffic and alerts analysts if a domain exhibits behaviors consistent with a malware command and control server. The alerts contain visibility into the indicators and contextual data useful when responding to an alert.

RSA NetWitness Logs and Packets' Cutting Edge Techniques Keep Security Teams Ahead of Advanced Threats

None of the analysis described above can alone identify with certainty a covert channel in an organization. What makes this analysis difficult is the statistical analysis required across ALL sessions and across all of these measures to identify these suspicious sessions. Few systems have the underlying data, speed, or smarts to do this. Past approaches have been highly error prone and inefficient as systems have depended on:

• Rules and threshold-based alerts that may work in one environment but not another, or need constant modification as web behavior evolves

• Highly manual approaches that rely on creating reports of search-based results and manually spotting patterns within the results

• "Vanilla" Big Data systems and countless hours of customization getting them to collect the right data and spot the types of behaviors described above

RSA NetWitness Logs and Packets employs advanced statistical methods to spot these types of attacks, plus provides an infrastructure upon which to build other detection and reporting use cases. Automated enrichment of data with business context about users and systems, and the ability to detect lateral movement inside the organization, gives RSA NetWitness Logs and Packets customers the tools needed to hunt and defeat today's advanced threats. It's designed to:

• Provide complete visibility to identify and investigate attacks

- Eliminate blind spots with visibility across logs, networks, and endpoints
- Inspect every network, packet session and log event for threat indicators at time of collection with capture time data enrichment
- Augment visibility with additional compliance and business context, to create a business-driven security posture

• Detect and analyze even the most advanced of attacks before they can impact the business

  - Discover attacks missed by traditional SIEM and signature-based tools by correlating network packets, NetFlow, endpoints and logs
  - Identify endpoint malware missed by conventional AV in real-time
  - Start finding incidents immediately with out–of-the-box reporting, intelligence, and rules
  - Identify high risk indicators of compromise by harnessing the power of big data and data science techniques

• Take targeted action on the most important incidents

  - Instantly pivot from incidents into deep endpoint and network packet detail to perform network forensics and understand the true nature and scope of the issue
  - Prioritize investigations and streamline multiple analyst workflows in one tool
  - Maximize your team's potential by implementing RSA's best practice-based security operations management tools and training

Conclusions

To detect advanced attacks, multiple data types need to be combined. Data sources such as network packet, log, endpoint, and cloud data provide the ability for RSA NetWitness Logs and Packets to discover attacks missed by log-centric SIEM and signature-based tools. It's the only solution that can correlate all of the needed data sources, applying advanced behavioral techniques and data science models. These advanced security techniques provide security teams with speedier detection, raising the effectiveness of threat detection and response activities, and providing organizations with a complete platform for business-driven security.