ARBOR NETWORKS

securitycurrent Whitepaper

The Hunted Becomes the Hunter

securitycurrent

The ground has shifted under most enterprise IT security staff. Breaches are now capturing prime-time air across mainstream media outlets. As the world becomes more connected, it is no longer enough for enterprises to react once an alert indicates an attacker is inside the network. Instead, with continuous packet capture and threat feeds followed by analysis, it is now possible to hunt the attackers and locate them versus waiting for an alert. Breaches may be viewed as a security problem, but they're a bigger issue. This is a business problem; similar to lost customers, inventory, or market share, but it just happens to be through technology. Experienced security leaders and executives have already recognized this challenge and are working towards assembling the perfect blend of people, process, and technology. What is it that they are forming? Internal teams directed to stop waiting for alerts to indicate there's a problem and to go hunt for the attacker.

Why Waiting for Alerts Is No Longer a Good Option

Motivated attackers understand their target and how to avoid being detected. Alerting the security operations center (SOC) is the way many teams react to an attack. But what if the attacker has a foothold into the network and there is no alert? On the flipside, organizations are enduring critical alert overload. If everything is a priority, nothing is a priority. Investigation of these events is time-consuming and leads to false positives and alert fatigue, potentially causing security teams to dismiss some events and look left when they should be looking right. Many reputable breach reports show discovery of compromise is through external parties as opposed to the internal security team. For example, Verizon's 2014 Data Breach Investigations Report (DBIR) continued to illustrate external entities are discovering breaches more so than internal teams.

In fact, a 2012 U.S. congressional testimony[1] indicated that 94% of breach victims learn of the compromise through third parties, with only 6% independently discovering breaches. The simple fact of the matter is that attackers are penetrating networks and advanced security teams have begun to recognize the need to move from sitting and waiting to going on the hunt for the attacker.

When teams do this, the hunted becomes the hunter.

What Is the Concept of Hunting?

What if security teams seek out the attacker as opposed to waiting for them to slip up and trip an alert? With motivated attackers penetrating successfully, security leaders are creating internal teams of hunters to locate the attacker and to eradicate them as quickly as possible. This is a change in mindset from the way teams have long been accustomed to identifying incidents. Even in the early days of antivirus software, the system alerted when something went wrong based on what it knew. Shortly thereafter, intrusion detection systems (IDS) and intrusion prevention systems (IPS) continued to alert the same way. As a result, teams have grown accustomed to waiting for events and assume if there's no noise, everything must be fine.

So what's the better alternative? Be reactive and wait for the attacker to make a mistake and trigger an alert, or be proactive and use security analytics to locate the attacker? Preventing the exfiltration of data is futile without the ability to detect before it's too late. Pravail Security Analytics enables security teams to focus their attention where it matters most.

Hunting For Signs of Compromise

The statement "persistence pays off" is embedded in the mindset of an advanced attacker. As such, organizations hunting for signs of an intrusion have the opportunity to use the data available to eradicate an attacker and to reduce their dwell time. Lockheed Martin's Cyber Kill Chain®[2] demonstrates why it is critical to disrupt the attacker as early into their mission as possible. The Cyber Kill Chain outlines attacker tactics whereby an end-to-end process fails their mission if the chain is disrupted. Lockheed Martin outlines the kill chain through seven phases:

Arbor Networks' Pravail® Security Analytics empowers security teams to have a fighting chance defending the enterprise. To be successful at hunting for an attacker, security teams need visibility, speed, accuracy and analysis across historical and real-time data.

Arbor Networks understands this requirement and uses big data technology to enable security teams to make faster, and more importantly, accurate decisions across complex networks.

Pravail Security Analytics delivers real-time and historical deep inspection to simplify analysts' workload hunting for the attacker. The ability to replay captured traffic using the latest security intelligence is important because it provides retroactive forensics to uncover possible pre-existing compromise and to eradicate the attacker before data exfiltration occurs.

[1]Testimony before the U.S.-China Economic and Security Review Commission. Additional information at:
http://www.uscc.gov/sites/default/files/3.26.12bejtlich.pdf
[2] Lockheed Martin's Cyber Kill Chain
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

1. **Reconnaissance** – Research and profiling the target
2. **Weaponization** – Creation of remote access Trojan with an exploit to deliver
3. **Delivery** – Channels such as email and websites
4. **Exploitation** – Victim OS or application is exploited
5. **Installation** – Payload enables attacker persistence through malicious program
6. **Command and Control (C2)** – Infected host(s) beacon outbound to C2 network
7. **Actions on Objectives** – Data exfiltration or pivot point to another target

Going on the offensive, which is not about hacking back in the context of this paper, provides the opportunity to uncover the attacker's activity and to disrupt their mission. It's about taking an active role in finding the attacker. The U.S. military defines several steps in its discovery process that can carry over to security teams' ability to detect an intruder. The steps[3] include: find, fix, track, target, engage and assess. It's the find and fix steps that speak to hunting the attacker as opposed to waiting for an alert. Identifying what's normal versus abnormal takes a combination of security analytics and human intelligence. With refined data, security teams can then take what's meaningful and turn it into actionable intelligence to disrupt the mission. Without this intelligence security teams will miss the opportunity to disrupt the attackers' mission. However, with this intelligence, security teams can identify both system vulnerabilities and locations to begin the hunt. They can also identify the tactics an attacker is likely to use and the steps the attacker took to laterally move through the network.

Adopting the National Intelligence Cycle

As defined in part one of this series, (Security Analytics: A Required Escalation in Cyber Defense)[4], security intelligence is any information that indicates an attack is in progress or has succeeded. Intelligence can also be the byproduct of security analytics—the application of security intelligence to large data sets, usually of full packet captures.

Together, analytics and intelligence provide teams with the resources they need to hunt for problems.

The security industry can learn from how national intelligence works[5] to protect the country using the cycle defined below. Security teams can use this cycle to step through the process in search of an attacker through the data collected.

- Planning and Direction – this is the beginning (outlining specific requirements) and end of the cycle because finished intelligence drives new requirements.
- Collection – gathering of raw information (OSINT, HUMINT) to derive mission intelligence.
- Processing – a usable collection of data to be used by analysts in its original form.
- Source Analysis and Production – data is converted into intelligence through the work conducted by analysts.
- Dissemination – the timely output of intelligence information is delivered to stakeholders to support decisions.

Arbor Networks Pravail Security Analytics interacts with data. Pravail speeds through years of data and moves forward and backward in time to follow threats and the source of the attack.

Furthermore, Pravail can identify previously undetected zero-day attacks. Whenever the detection capability is updated, all stored packet captures are automatically captured through the Pravail Security Analytics solution to identify previously undetected zero-day attacks.

What Are Some Key Indicators of Compromise (IOC)?

Armed with data feeds, teams can dig deeper into activity to uncover potential compromise. There are breadcrumbs that teams on the hunt will be able to follow through the analytic data available.

Similar to studying film of an opponent, the ability to play, pause and rewind provides insight into what happened. Perhaps more importantly, it shows how it happened so that the same incident doesn't repeat. It's common for compromised hosts to get reimaged in order to get the

[3] Lockheed Martin's Intel Driven Defense Paper
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
[4] Security Analytics: A Required Escalation in Cyber Defense
http://pages.arbornetworks.com/website_ITHarvest_SecurityAnalytics.html?utm_source=securitucurrent
[5] How National Intelligence Works: http://www.intelligence.gov/mission/how-intelligence-works.html

machine back up and operational. But how did the compromise occur in the first place and can it happen again? Or has it already? Those who have not learned from the incident are likely to repeat it.

Indicators of compromise are a never-ending list, but there are many that are considered the path of least resistance in attacker discovery. Examples include:

- Unusual egress network traffic
- Failed logins
- System file or registry changes
- Communication among unrelated or unauthorized hosts
- Geolocation abnormalities
- Internal lateral movement
- Unauthorized database activity
- Abnormal DNS traffic
- Unauthorized applications using HTTP/S to blend in

XML-based sources of IOCs include the OpenIOC Framework[6] as well as availability from Mitre's CybOX[7] to name a few. The list of IOCs is constantly updated and seemingly endless, which is why combining security analytics with human intelligence needs to remain a priority.

Historically, teams have focused their efforts on critical vulnerabilities as a means of defending against the greatest risk. It's easy to understand this mindset, especially with teams strapped for resources. However, the initial compromise can exploit more than just critical vulnerabilities, which means leaving exposure by glossing over medium and low vulnerabilities.

What's more, there's no insight into possible compromise through a zero-day attack. Internal lateral movement won't be discovered through a vulnerability scan, which requires teams to go on the offensive. This further reinforces the need for proactive discovery to reduce the amount of time an attacker is able to maneuver within the network and work towards achieving its mission.

Heartbleed and Shellshock use cases:

1. Determine vulnerable hosts to prioritize countermeasures
2. Assess real-time and historical hostile activity
3. Know when and where hosts were attacked to hunt and eradicate the attacker

Pravail Security Analytics Use Cases

If there's data, collect it.

Full packet captures allow analysts to make intelligent decisions as to what to do next. There's also postmortem value from using large captured data sets to better understand the vulnerable state through root-cause analysis.

Without this level of detail, security teams can miss critical pieces of information in understanding how an incident occurred. This can lead to the wrong action being taken, which interrupts the business rather than the attacker. Security analytics enable businesses that go on the offensive to recognize what data is meaningful, what action to take, and what can be understood about the attack to be better prepared for the next event.

Consider how security analytics can help detect and prevent major attacks such as Heartbleed and Shellshock, two of 2014's biggest bugs. Pravail Security Analytics provides insight when hosts are vulnerable on a global scale so that organizations can:

1. Confirm risk against a specific attack based on endpoint vulnerability data.
    - Which hosts are vulnerable so that teams can narrow their focus? Knowledge about a target's vulnerable state is step one in remediating risk, followed up by attack intel and attempts to deliver a payload to exploit systems.

[6] OpenIOC Framework: http://www.openioc.org/
[7] Mitre's CybOX: https://cybox.mitre.org/

2. Understand malicious activity such as a highly targeted attack against important assets across specific network segments.
    - In-the-moment data analysis provides complete host and network visibility to determine hostile activity. Furthermore, in the case of Heartbleed and Shellshock, the capability to replay previous exploit activity pinpoints which systems have been attacked.
3. Gain insight into the attack and its timeline.
    - Answering which hosts were attacked, when, where, and the source, is then used to provide countermeasures. Security teams are able to answer key questions the business wants to know and make adjustments based on the past and present events.

Explore, Understand, Identify

Traditionally, teams have been focused around *prepare, detect, analyze and respond*. Now as an attacker evolves, security teams must proactively hunt and explore in order to understand each threat, take actionable intelligence, and defend the enterprise.

The added complexity doesn't solve problems, but rather provides a source of intelligence. What the enterprise needs is data to make decisions. Security analytics is the glue that binds together a wide variety of technology feeds along with people to take the following action.

1. Identify key assets and the business' competitive advantage (intellectual property)
2. Create a baseline through the collection of data from logs and packet captures
3. Determine defensive goals around key assets
4. Outline sources of information that provide intelligence
5. Escalate to incident handling based on data analysis

These steps form the basis of exploring the network, understanding data value, and identifying attacker tactics. The difference is an active versus passive defense; the waiting game approach is no longer an option.

The value is that enterprise IT security teams are forced to be more engaged with the business to discover and understand where the high-value targets exist and which activities are normal versus abnormal. The process then leads to using security analytics to replay activity and help to determine what events could be signs of an attacker.

People, Process, and Technology

It's no secret that security professionals are in high demand. The Bureau of Labor Statistics[8] indicates the job outlook for security analysts is projected to grow 37% from 2012-2022, which is faster than average.

Talk to a security manager and s/he will tell you hiring and retaining security talent is a significant challenge. Technology can only do so much. Without the team to get the job done, it can be futile.

It is one thing to talk about going on the hunt, but it's another to put together the right people and process. This is an important component to staffing a team that must overhaul and transform the traditional "wait and see" approach.

It's also a mind shift for business leaders who don't comprehend a lot of the security risks and what they mean to the business. Addressing the following requirements will better position security leaders and their teams to be more successful.

1. Determine the Need – While this may sound obvious, it's still crucial. In order to start off on the right foot, security leaders must be able to:
    - Determine what is at risk. This includes performing asset inventory on systems and data as well as third parties and trusted suppliers. This should already be part of an existing incident response plan and team. Generally, a seasoned team of incident responders who are already in an established role are fulfilling this duty. If not, going on the offensive is counterintuitive if assets aren't managed and a Computer Security Incident Response Team (CSIRT) isn't well established.
2. Building a Business Case – Management needs to understand the reasoning behind this endeavor in order to support the initiative. To meet this need, security leaders must:
    - Draw a clear relationship between the business and benefits of security. The justification for security budgets should not come

[8] Occupational Outlook Handbook: Bureau of Labor Statistics: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

from data such as the number of attacks generated, but rather the business and where it is at risk for security incidents. This approach helps managers to understand their line of business and how security is protecting them so they can meet their goals. In its list of top skills for CSIRT members, CERT[9] includes personal skills (written, verbal, and presentation). Obviously technical skill is required, but in order to gain traction with management, there must be a business case, which starts with effective communication.

3. Establishing or Revising the Team – As previously stated, a CSIRT team should already be in place in order to advance to the next level. The team should be made up of professionals with well-rounded skills, such as:
    - Incident response, programming, data analysis, business acumen, systems administration and leadership (management or team leads). There is value in ensuring not everyone is like-minded. When teams are on the hunt, thinking differently as a collaborative team is a competitive advantage to avoid a narrow approach and not thinking outside the box.
4. Systems and Data Feeds – Updated data feeds from industry sources and sharing services provide insight into attacker tactics and trends.
    - Receiving actionable data from subscription services as well as industry sharing is needed to stay abreast of activity. iSIGHT Partners, Looking Glass, FS-ISAC, US-CERT and OSINT sources are available. Once received, systems can then reanalyze the data to determine if there are any IOCs based on refreshed information.
5. Act on Intelligence (Hunt) – Teams need continuous assessments with correlated data to narrow their search.
    - In addition to hunting, it is important to relate back to the initial steps focused around the business. Similar to Lockheed Martin's Cyber Kill Chain, these steps are also important for the success and support of this initiative. Security's objective to support and secure business strategy should be brought full circle as a mechanism to showcase the value of the security program and, in particular, the need for incident response and active research.
6. Postmortem – Lessons learned are invaluable.
    - Reflecting on lessons learned should involve management as well as the security team. The ability to communicate what was at risk, and how it happened, and sharing this information with external entities makes the entire process stronger. For a variety of reasons, often legal ones, sharing is kept close to the vest. Unfortunately, this is one of the more frustrating issues in the industry where businesses don't share, yet criminals do.

Conclusion

Relentless adversaries require businesses to approach incident response differently. The industry has fallen behind and while our goal of prevention is always the top priority, the fact remains: persistent attackers will find a way in. It's just a matter of time.

The technology is here to provide teams with the data they need to make proactive and intelligent decisions. Full packet captures provide for rich security analytics data and enable teams to go on the hunt. The end result is a smarter team with a fighting chance.

Security leaders moving in this direction are reflecting on key assets and creating the foundation with the right people, process, and technology. Adversaries are a business problem, but security can respond to this challenge by being proactive and by making the necessary structural changes to eradicate the attacker more quickly.

[9] What Skills are Needed When Staffing Your CSIRT? http://www.cert.org/incident-management/csirt-development/csirt-staffing.cfm?