THE RISE OF THREAT HUNTING AND WHY IT MATTERS

One day in early 2017, DomainTools' senior security researcher Kyle Wilhoit noticed a domain flagged by a research tool during his routine daily trawl of suspect indicators. Discovering the domain was hidden behind Whois privacy protection, he decided to try and uncover the underlying IP address, an important investigative moment threat hunters call the 'pivot'.

Leveraging DomainTools' Iris, Wilhoit quickly unmasked the IP, from which he pivoted using passive DNS to reveal a number of associated domains. Moving down the kill chain, the domains' command & control (C2) eventually led to a Word document posing as a survey from The Israeli Ministry of Communications. Clearly, the document was a lure for an email phishing campaign, but which one among the thousands launched every day? More hunting yielded a web page hosting a convincing replica of the VPN login page for the Israeli Prime Minister's office in a campaign bearing the hallmarks of the shadowy CopyKittens espionage group.

The success of individual phishing campaigns isn't always clear to researchers but in this case the time spent unraveling the malicious infrastructure from a single suspect domain was not wasted.

More hunting yielded a web page hosting a convincing replica of the VPN login page for the Israeli Prime Minister's office...

This example illustrates what threat hunters do and how they do it. Starting with the unpromising dead end of a single obscured domain, Wilhoit was able to reveal the underlying infrastructure of a phishing campaign aimed at a nation state. At every point, the hunt could have hit a dead end but he was able to use specialized tools to pivot and bypass obstacles in search of his ultimate target - one that potentially nobody else had yet discovered.

Compare and contrast this mode of researching threats with established 'reactive' security practices, which would have waited for the attack to trigger from inside an email inbox. By this late stage, it would be up to endpoint security to intercept or block executables or embedded URLs, assuming it had any way of identifying these as malicious in the first place.

Successful or not, components used in the attack might in theory have eventually triggered an alert or red flag, prompting forensic investigation by the security team. It's easy to see from even this simple example how heavily weighted cybersecurity's timeline is in favor of attackers over defenders.

This white paper describes how Wilhoit's mindset, skills and approach to threat hunting research are starting to find their way into mainstream Security Operations Centers (SOCs), while assessing the long-term significance of this development for enterprise security and beyond.

© Copyright DomainTools, 2017. All Rights Reserved.

THREAT HUNTERS UP CLOSE

Threat hunters can be divided broadly into two groups.

Research Threat Hunters

The first are professional researchers like Wilhoit who work for cybersecurity vendors and Internet companies, or operate alone. Once seen as technical outsiders, a surge in attacks and breaches has seen this group move to center stage and they are now employed by every company with any involvement in understanding and countering security threats. Their job is to look for 'badness' on behalf of their company's clients, often sharing the results of their investigations with the wider security community through blogs, white papers and in conference presentations.

Organizational Threat Hunters

A second group is the growing ranks of organizational threat hunters who work for large enterprises alarmed to find themselves on the receiving end of organized cyberattacks on a scale few anticipated even a handful of years ago. While research hunters are embedded inside companies focused on research and mitigation, organizational hunters typically work from within the SOCs that have become important threat-fighting hubs for the commercial world, sometimes in the form of managed services provision.

Organizational hunters typically work as part of larger SOC teams, dovetailing with incident response (IR) teams who act as first responders to security threats. Although these hunters are sometimes deployed after a compromise to find traces of persistent malware and C2 connected to known incidents, the majority of them work proactively to analyze threats that have not yet been identified, leaving 'after-the-event' forensic analysis to dedicated specialists. SOCs always include a range of skillsets, but the threat hunter's role is a proactive rather than defensive part of that team.

The two groups serve different but equally important roles. Research threat hunters have become an important source for intelligence on new attacks, disseminated publicly. Organizational hunters, by contrast, are the leading-edge of emerging organizational defense systems who utilize their skills to get ahead of attacks targeted at their organization or industry. The evolution of organizational threat hunting holds major implications for corporate cyber-defense inside SOCs, suggests Wilhoit: "Hunting is a fundamental mind-shift in the paradigm of corporate security."

© Copyright DomainTools, 2017. All Rights Reserved.

THREAT-HUNTING AWARENESS

A 2017 survey carried out by LinkedIn's Information Security Community uncovered rapidly growing knowledge of the field among cybersecurity professionals:

Almost **two thirds** expressing a high level of familiarity with threat hunting.

Three quarters said they believed threat hunting held major significance for their organizations.

When respondents were asked how confident they were about the ability of their own SOCs to detect advanced threats:

Three quarters said they were either 'not confident or only moderately confident' the ability of their own SOCs to detect advanced threats.

Around **half** believed they were hindered by slow response times, too many false positives, a lack of confidence in automation and reporting tools, and not enough skilled staff.

When questioned about 'cutting edge' or advanced capabilities, more uncertainty emerged:

64%
of respondents are pessimistic about their SOC's ability to cope with hard-to-detect emerging threats.

30%
believed their SOC was 'advanced' but not necessarily innovative enough.

6%
Rated their SOC as cutting-edge, ahead of the curve.

The obvious question is what it is that professionals define as cutting edge. Interestingly, only **14%** of SOC employees questioned engaged in activities with a clear threat hunting element to their makeup, with **80%** stating that they were not spending enough time looking for emerging threats. Only **a fifth** proactively looked for threats with the rest dedicated to old-style response. SOCs ended up missing **four out of ten** threats, taking an average of **40** days to uncover their existence.

The whole survey underlines how advanced threat hunting – looking for hidden problems on a proactive basis – has a ways to go. Most SOCs lack advanced threat-hunting capabilities, either in terms of the personnel, budgets or the platforms used to support them.

75%
Of professionals would like to see more investment in threat-hunting support systems.

50%
Believe that threat hunting system would pay for themselves in a year.

95%
of respondents expressed a preference to work in SOCs based around a more sophisticated threat hunting approach to security, a statistic that predicts future growth.

Source: 2017 Threat Hunting Report, Crowd Research Partners

© Copyright DomainTools, 2017. All Rights Reserved.

So, what does organizational threat hunting entail? Within SOCs, it's a role that must display a range of skills coupled to an unusual mindset.

OBJECTIVES

The point of threat hunting is to intercept threats of every caliber at the earliest opportunity. This allows security teams to reduce or even eliminate 'dwell time,' the period that elapses before a threat is discovered. As the 2017 Threat Hunting Report indicates, in many cases dwell time can be weeks, by which time most cyberattacks will have had ample time to do a serious damage.

MENTALITY

The first assumption of an organizational threat hunter is that all defenses will be permeated at one point or another, no matter how often they are upgraded and maintained. It follows that the second assumption is that the attacker is already inside the network even if no alerts have been generated. This approach isn't a replacement for conventional defenses, which remain necessary, so much as a way of enhancing them. But threat hunting is always a way of looking for threats that won't be picked up by conventional perimeter defenses.

Says Wilhoit: "It's important for mature organizations to hunt not just advanced adversaries, but also the mundane attackers using ransomware, for instance. And keep in mind that just because an attacker isn't using advanced techniques doesn't mean they can't and don't cause the most damage."

THINK LIKE A HACKER

A methodical approach to threat hunting can be defined as the sort of thoroughness in which no trail of evidence is overlooked or left unexamined. Various approaches can be deployed in the hunting process but it can, broadly speaking, be targeted (appraising a known actor, campaign or technique) or generic (looking for and following one type of indicator).

The threat hunter must go beyond the static idea of an attacker identified through a single malware signature or intrusion technique and start from a hypothesis about an attack, often in response to a recent compromise in which an attacker has gained a foothold in the network. This offers a way to understand how an attacker got behind the organization's defenses in the first place, and can be broken down into a number of stages.

STEALTH

Threat hunters must keep a low profile so as not to alert an attacker that they have been detected or are being monitored. It's cat and mouse with the difference that the two arch rivals never meet. Threat hunters must use stealth when hunting on a network or host, and there are several ways that can assist hunters in becoming silent. For example, they will typically prefer to view logs view passive sources- such as a SIEM device. This prevents an attacker from becoming aware that an analyst is looking more closely at a possibly compromised device. Additionally, in some cases, hunters may choose to take an image of the compromised host and analyze the data on a carbon copy. In any event, the trick is never to let the attacker know they might be monitored.

TOOLS AND DATA

The key to effective threat hunting is always primarily the manual skills and approach of the analyst but tools and data are a close second. Data comes from security infrastructure - SIEM, intrusion detection alerts, endpoint security or privilege management – which generates the raw material for a hunt. In some cases, tools like Yara are used to sift and research individual indicators, speeding up the process of moving down the kill chain. Additionally, information is often obtained from public research from like blogs and whitepapers. Many organizations also utilize outside threat feeds, often delivered via APIs or web portals.

Threat artifacts and Indicators of Compromise (IOCs) come in many shapes and sizes, including command & control (C2) infrastructure, IP addresses, domains, file hashes, mutexes, host, file, and system indicators. Because this can appear to be legitimate activity, the skill – the "art "as Wilhoit calls it – is always knowing what to pay attention to without becoming bogged down in noise.

© Copyright DomainTools, 2017. All Rights Reserved.

"Hunters typically need an immense amount of data to understand threats. This data could come from IPS/IDS, proxies, firewalls, volatile memory, file or OS artifacts, binaries, C2s, web server logs, web app logs, and any other data source," says Wilhoit.

"Hunting can also help identify low-level vulnerabilities and high-level architectural issues, since hunters are finding ways attackers attempt to and successfully compromise the organization."

MEASURING THREAT HUNTING MATURITY

How can organizations assess how well they are implementing threat hunting? Different models exist for describing organizational maturity but DomainTools' uses the following categorizations:

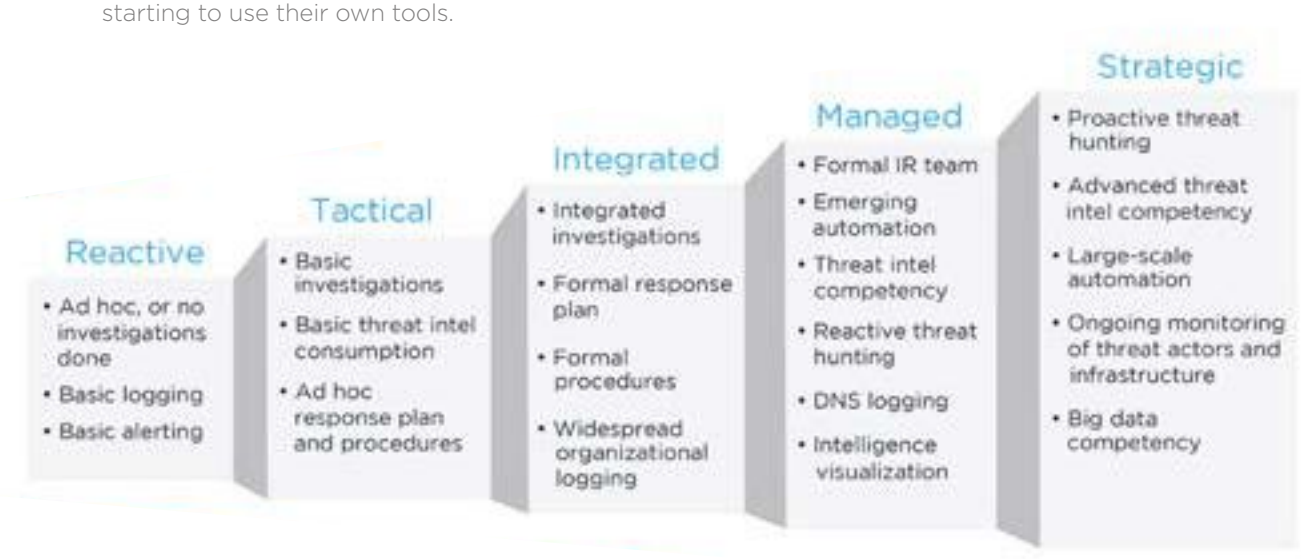
The reactive security team: Where SOCs started – investigations are ad hoc, unstructured, logging and alerting is basic. Organizations rely on endpoint AV, intrusion prevention and Intrusion detection layers to spot threats.

The tactical security team: Still basic but response plans exist in an ad hoc state to cope with mitigation. Staff have access to basic threat intelligence sources and carry out some log analysis.

The integrated security team: Developed procedures in place to cope with mitigation backed by an integrated use of tools and staff expertise. Mature use of SIEM and more extensive analysis of logs.

The managed security team: Incident response team is clearly defined with greater use of automation and intelligence to aid proactive hunting and response. DNS logging and diagnostics become critical at this level so that IPs connecting to suspect domains can be traced. Threat hunters tasked with performing extensive log analysis.

The strategic security team: Advanced threat hunting – a fully-integrated threat-hunting team using advanced intelligence sources, tools with extensive log analysis automation to speed investigation. At this level, teams profile threat actors and have embraced big data analytics and are starting to use their own tools.



HUNT TEAM SKILLS

We can see from this that a mature hunt team is a demanding environment built from diverse technical skills. These can be overlapping but should include roles covering incident response, forensics, both of which imply real-world experience. Ideally, static malware analysis (someone skilled at disassembling and piecing together new and novel malware) is important as are network specialists (spotting traffic anomalies) and threat intelligence experts.

"It's important to note that a hunt analyst doesn't need to be an expert in each of these," says Wilhoit. "For instance, if a hunter doesn't know how to statically reverse engineer malware, they can pass that sample to the malware team, which will pass the results back to the hunt team member."

© Copyright DomainTools, 2017. All Rights Reserved.

MEASURING SUCCESS

A fundamental issue with threat hunting remains validation – how do organizations know they are doing it right? This is a particular concern for the large number of organizations that have recently overhauled their SOC to introduce threat hunting into the mix. According to Wilhoit, data from the period immediately before threat hunting was introduced is key.

"You have to do metrics year-over-year with the baseline being the year prior to implementing threat hunting. That will be your foundation – how many threats did you catch retrospectively through a SIEM environment versus did you proactively catch a threat and contain to one host?"

This can be boiled down to the simple takeaway that once a hunt team is in place, the response team should have less to do. "You have to look at how wide an infection was because once you implement a hunt team incidents should be far less widely distributed."

CONCLUSION: THE NEW AGE OF THREAT HUNTING

We have now seen how threat hunting is becoming an important way for organizations to change the way they conceive of and design their cybersecurity operations. Fundamental to this is the idea that security compromise is no longer a worst-case scenario as an inevitability. Simply detecting threats is not enough – they must be understood and intercepted far more rapidly than in the recent past.

Ultimately, threat hunting's successful integration into today's SOCs will depend on the men and women doing the job. According to Wilhoit, they will have to marry technical skill with communication and organizational smarts. "Threat hunters need to be renaissance men and women, capable of understanding and speaking with not just all of the IT security function, but also other IT functions like system administration."

Looking for badness' rather than waiting for it to happen will require long-term investment in people, skills and tools; a paradigm shift for those organizations still inclined to view cybersecurity as an engineering rather than business issue. The rise in the importance of threat hunting will present cultural and technical challenges, but containing and preventing attacks will be well worth the effort.

© Copyright DomainTools, 2017. All Rights Reserved.