Network-based Threat Intelligence: Searching for the Smoking Gun

Version 1.3

Released: February 22, 2013

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051

info@securosis.com www.securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

Licensed by Damballa

Damballa automates the discovery of an organization's highest risk devices under criminal control. As the experts in advanced threat protection, Damballa discovers and analyzes evidence of malicious network traffic in real time, profiling the criminal actors and rapidly identifying the compromised devices that represent the biggest risk. Our patent-pending solutions automatically detect and terminate criminal activity, stopping data theft and providing the forensics needed to expedite incident response and remediation. Damballa protects any type of server or endpoint device including PCs, Macs, Unix, iOS, Android and embedded systems across corporate, ISP and telco networks. Damballa protects more than 300 million endpoints globally at mid-size and large enterprises in every major market and for some of the largest ISP and telecommunications providers in the world.

Copyright

Table of Contents

Understanding the Kill Chain

Our recently published Early Warning paper described using external threat intelligence to better leverage internal data collection, shortening the window between an attack and the ability to defend against it. But of course the devil is in the details, and taking this concept to reality requires actually putting these ideas into practice. There are number of different types of "threat intelligence" that can and should be utilized in an Early Warning context. We have already documented a detailed process map and metric model for malware analysis (check out our Malware Analysis Quant research). Being able to identify and search for specific indicators of compromise on your devices can be invaluable for determining the extent of an outbreak.

But what can be done to identify malicious activity if you *don't* have the specific IoCs for the malware in question? That's when we look at the network to yield information about what might be a problem, even if controls on the specific device fail. Why look at the network? Because it's very hard to stage attacks, move laterally within an organization, and accomplish data exfiltration without using the network.

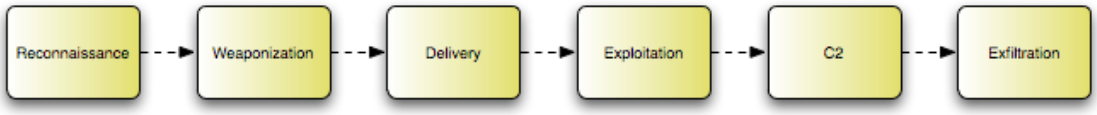
Why look at the network? Because it's very hard to stage attacks, move laterally within an organization, and accomplish data exfiltration without using the network.

This means attackers leave a trail of bits on the network, which can provide a powerful indication of the kinds of attacks you are seeing, and which devices on your network are already compromised. This paper will dig into these network-based indicators, and share tactics to leverage them to quickly identify compromised devices. Hopefully shortening this detection window will help to contain the damage and prevent data loss.

In order to understand how to detect signs of malware on your network, you need to understand how malware gains a presence in a network, spreads within that network, and finally moves the data out of the network. This has become known as the Kill Chain.

Describing the Attack

There has been plenty of research over the years about how malware performs its nefarious business. The best description of the Kill Chain we have seen was back in 2009, by Mike Cloppert, and we recommend you check it out yourself. To illustrate Mike's terminology, let's describe how malware works at a high level.



Source: Security Intelligence: Attacking the Kill Chain

- **Reconnaissance**: The attackers first profile their targets. Understanding how the target organization is structured, gleaning information about the control set, and assembling information that can be used in social engineering attacks.
- **Weaponization**: Next comes preparing malware to exploit a vulnerability on the device. This involves R&D efforts to find exploits, which allow the attacker to gain control of the victim's device, and development of a delivery system to get the exploit onto the target device.
- **Delivery**: Once the exploit is weaponized it needs to be delivered to the target. This usually means some kind of effort to get the target to take an action (typically clicking a link or using an application attack) to visit a web page to deliver the malware.
- **Exploitation**: This is the actual execution of exploit code on the target device to provide the attacker with control of the device. This can be a complicated process, which may take advantage of known or unknown vulnerabilities in operating system or application code. Nowadays this tends to be a multi-stage process where a downloader gains control of the machine and then downloads additional exploit code. Another focus in this step is obfuscation of the attack to hide the trail of attackers and stay below the radar.
- **C2**: Known nowadays as Command and Control, this is the newly compromised device establishing contact with its control network to receive further instructions.
- **Exfiltration**: Once the attackers reach their goal, they must package up their spoils and move the stolen data to a place where they can pick it up. Again, this may be a sophisticated endeavor as evading detection as the stolen data leaves the organization can be difficult.

There has been significant innovation in a number of the aspects of the kill chain, but the overall process remains largely the same.

There has been significant innovation in a number of the aspects of the kill chain, but the overall process remains largely the same. Let's talk a bit about how each step has evolved over the past 3 years. Let's start with reconnaissance, which has become far easier now that many targets seem to publish their life stories and sordid details on public social networks. There are tools today (such as Maltego) which can automatically

assemble a fairly detailed profile of a person by mining social networks. Despite the warnings of security professionals, folks are not about to stop sharing their information on social networks, and that makes attacker recon efforts much easier.

In terms of weaponization, we have seen increasing sophistication and maturity in how exploits are developed and updated. Aside from a third-party market for good exploits creating a significant economic opportunity for those willing to sell exploits, we see attackers using modern software development techniques such as Agile programming to improve the quality of their attack code. Additionally the attackers undertake detailed and sophisticated quality testing against not only target devices but also against security software to ensure the attacks are not detected by commercial anti-malware technologies. Finally, attackers now package up their code into 'kits' for use by anyone with a checkbook (or a BitCoin account). So sophisticated malware is now within easy reach of unsophisticated attackers. Awesome.

Attackers now package up their code into 'kits' for use by anyone with a checkbook (or a BitCoin account). So sophisticated malware is now within easy reach of unsophisticated attackers. Awesome.

In terms of delivery, in light of malware's rapid rate of change, many attackers opt to deliver a very small downloader onto the compromised device. Once C&C contact is established, the downloader receives a particular package for whichever role the attacker has selected for it. For exploitation, the continuing advance of operating system security (kudos to Microsoft in making Windows 7 and 8 much harder to exploit) has shifted attackers to the new low-hanging fruit: application software. First they targeted browsers, but as browser security advanced attackers shifted focus to popular applications such as Java and Adobe Reader. *We can count on attackers to continue finding the weakest software link on target devices.*

The area of most rapid advancement is command and control, which makes sense because ongoing communication with devices is the lifeblood of the malware enterprise. Current C&C networks feature resilient, multi-tiered structures with high survivability. When the first tier of distribution points is taken down, there always seems to be another set ready take its place, and isolating the real command and control nodes is hard. Additionally, C&C nodes frequently hide in plain site by compromising and then leveraging legitimate web sites and domains, making them even more difficult to identify. Finally, attackers have also evolved their exfiltration tactics, recently moving away from proprietary encrypted protocols to encrypting only specific files, in order to make detection harder.

But all these advances represent a point in time. By the time you read this attackers will be changing tactics and evolving the efficiency of their exploits, command and control, and exfiltration.

But all these advances represent a point in time. By the time you read this attackers will be changing tactics and evolving the efficiency of their exploits, command and control, and exfiltration. Malware is truly an arms race, and for the past few years attackers have had the upper hand.

Building an Army

For many attackers there is safety in numbers. They work to develop armies of compromised devices that can number in the hundreds of thousands, to ensure they have ready access to tremendous offensive firepower when needed. The advantage of multi-stage attacks and constant communication with compromised devices via command and control is that devices can lie dormant and may be repurposed at any time by sending new exploit code and instructions.

Detection of these compromised devices typically involves waiting until they do something bad and then reacting to contain the threat. The bad news is that many of these compromised devices don't act compromised in any obvious way, in an attempt to evade efforts to catch anomalous or bad behavior. The good news is that in light of the on-demand nature of malware networks, devices need to communicate frequently with the C&C hierarchy to get updated direction. Even if the instructions from C&C are to do nothing. That gives you an opportunity to detect C&C traffic and remediate the device before it gets does something bad. It's not exactly proactive, because the device is already compromised, but it's much better than cleaning up the mess after the compromised device launches an attack, right?

The good news is that in light of the on-demand nature of malware networks, devices need to communicate frequently with the C&C hierarchy to get updated direction.

Thus the focus on network-based threat intelligence, to follow the proverbial trail of bits on the network, in order to isolate compromised devices before they do something bad. Think *Minority Report* but without the cool visualizations.

Following the Trail of Bits

Attackers are very good at their jobs, so it's best to assume any endpoint is compromised. But with recent advances in obscuring attacks (through tactics such as VM awareness) and the sad fact that many compromised devices lie in wait for instructions from their C&C network, you need to start thinking a bit differently about finding compromised devices – even if they don't act compromised.

Network-based threat intelligence is all about using information gleaned from network traffic to determine which devices are compromised. Modern malware's dynamic nature makes extensive use of the network for updates, to communicate with command and control systems, for automated beaconing, etc. Fortunately we can follow that trail of bits to pinpoint the malware and find compromised systems. Attackers try to hide in plain sight and obscure their communications within the tens of billions of legitimate packets traversing enterprise networks. But they always leave a trail or evidence if you know what to look for.

Attackers try to hide in plain sight and obscure their communications within the tens of billions of legitimate packets traversing enterprise networks. But they always leave a trail or evidence if you know what to look for.

It turns out we learned most of what we need in kindergarten. It's about asking the right questions. The five key questions are Who?, What?, Where?, When?, and How?, and they can help us determine whether a device may be compromised. So let's dig into our questions to see how this would work.

Where?

The first key set of indicators to look for is *where* devices are sending requests. This is important because modern command and control requires frequent communication with each compromised device. So the malware downloader must first establish contact with the C&C network; then it can get new malware or other instructions.

The old reliable network indicator is reputation. First established in the battle against spam, security researchers tag each IP address as either 'good' or 'bad'. Yes, this looks an awful lot like the traditional blacklist/negative security approach of "blocking bad". History has shown the difficulty of keeping a blacklist current, accurate, and comprehensive over time. And attackers are continually

advancing the state of their art, so we always have blind spots in our ability to identify questionable traffic by reputation.

One of these blind spots results from attackers using legitimate sites as C&C nodes or for other nefarious uses. In this scenario a binary reputation (good or bad) is inadequate – the site itself is legitimate but not behaving correctly. For instance, if an integrated ad network or other third party web site is compromised, a simplistic reputation system could flag an entire site as malicious, even though its only a small third party component causing the problem. A recent example of that was the Netseer hack, where browser-based web filters flagged traffic to legitimate sites as malicious due to integration with a compromised ad network. They threw the proverbial baby out with the bathwater, which may be the right approach from a defensive standpoint, but won't make you any friends with end users not able to use frequently visited sites.

Another issue with IP reputation is the fact that IP addresses change constantly based on what command and control nodes are operational at any given time. Much of the sophistication in today's C&C infrastructures has to do with how attackers associate domains with IP addresses on a dynamic basis. With the increasing use of domain generating algorithms (DGA), malware doesn't need to be hard-coded with specific IP addresses – instead it cycles through a set of domains (based on its DGA) searching for a C&C controller. This provides tremendous flexibility, enabling attackers to protect the ability of newly compromised devices to establish contact, despite domain takedowns and C&C interruptions.

This makes the case for DNS traffic analysis in the identification of C&C traffic, along with monitoring the packet stream. Ultimately domain requests (to find active C&C nodes) will be translated into IP addresses, which involves a DNS request. By monitoring these DNS requests for large amounts of predictable (typically automated) traffic, patterns associated with C&C traffic and domain generation algorithms can be identified.

When?

If we look to the basics of network anomaly detection, by tracking and trending all ingress and egress traffic, flow patterns can be used to map network topology, track egress points, etc. By identifying a baseline of normal communication patterns we can pinpoint new destinations, communications outside 'normal' activity, and perhaps spikes in traffic volume. For example, if you see traffic originating from the marketing group during off hours, without a known reason (such as a major product launch or ad campaign), that might warrant investigation.

By analyzing and profiling how each piece of malware uses the network, you can monitor for those traffic patterns on your own network.

What?

The next question involves what kinds of requests and/or files are coming in and going out. We wrote a paper on Network-based Malware Detection, so we won't revisit it in much detail here. But we need to point out that by analyzing and profiling how each piece of malware uses the network, you can monitor for those traffic patterns on your own network.

This also enables you to work around VM-aware malware. The malware escapes detection as it enters the network, because it doesn't do anything when it detects it's running in a sandbox VM. But on an bare-metal device it executes malicious code to compromise the device. To take the analysis to the next level, you can track the destination of the suspicious file, and then monitor specifically for evidence that the malware has executed and done damage. Again, it's not always possible to block malware on the way in, but you can shorten the window between compromise and detection by searching for identifying communication pattern that indicate a successful attack.

How?

You can also look for types of connection requests which might indicate command and control or other malicious traffic. This might include strange or unusual protocols, untrusted SSL, spoofed headers, etc. You can also attempt to identify requests from automated actors, which have predictable patterns even when randomized to simulate a human being.

But this puts all egress and ingress traffic in play — it all needs to be monitored and analyzed to isolate patterns and answer where, when, what, and how. Of course that still leaves one key final question.

Who?

Now we get to the issue of analyzing the specific device for atypical behavior. Clearly the device in question should behave in a certain way, depending on the role of the user in the enterprise, so behavioral anomalies may indicate compromise. For example, you probably don't want an engineer's device to be hosting a website serving up private content. Or you don't want someone from the finance team to be mining the R&D networks in the middle of the night. These are obvious examples, but show the kind of behavior that can and should be profiled. With that profile, you can monitor the network traffic to ensure it's consistent with expected behavior and if not, alert on potentially bad behavior.

Turning Data into Dynamic Intelligence

Any organization can ask the key questions. But any single organization will only see small subset of attacks under way. So without factoring in external information – the intelligence part of network-based threat intelligence – gleaned by leveraging some type of information sharing network, you can only look for stuff already happening to you. That defeats the purpose of Early Warning.

So without factoring in external information – the intelligence part of network-based threat intelligence – gleaned by leveraging some type of information sharing network, you can only look for stuff already happening to you.

To make network-based threat intelligence work you need access to a significant amount of traffic, in order to find and recognize useful patterns. Failing that you need to partner with a provider with this kind of data, and the ability to deliver it to you in a useful fashion.

Network-based threat intelligence must be dynamic because the targets, algorithms, domains, and pretty much everything else, are constantly changing. Attackers change their approaches constantly to improve efficiency, obscurity, and resilience. So you need to continually adapt the patterns you search for.

One other essential point is defining a compromise. A single indicator does not necessarily mean a device is compromised. And we all know the hazards of false positives in security practice. So the success or failure of any security control will hinge on your ability to make efficient and accurate determinations of compromise.

Quick Wins with NBTI

Now that we have established that you can look for (and possibly find) indicators of an advanced malware attack by monitoring network traffic, it's time to deploy some sensors and get to work finding compromised devices in your environment. These pwned devices can provide a Quick Win to prove the value of network-based threat intelligence. Oh yeah, you also may be able to interrupt attacks before real damage and exfiltration occur. That's the concept behind the Early Warning System.

Deployment

As we have described, network-based threat intelligence requires monitoring key network segments for indicators of attack traffic (typically command and control). Many organizations have extensive and sprawling network infrastructures, so you probably cannot monitor everything initially. Start by prioritizing networks for the best chance to get a Quick Win and hopefully break the Data Breach Triangle. So where do you start?

Today's malware systematically uses downloaders to get the latest and greatest attack code, which means the compromised device needs to communicate with the outside world at some point.

The first and easiest place to start monitoring the network is your egress pipes to the Internet. Today's malware systematically uses downloaders to get the latest and greatest attack code, which means the compromised device needs to communicate with the outside world at some point. This Internet communication offers your best opportunity to identify devices as compromised, if you monitor your egress networks and can isolate these communications. Besides providing an obvious choke point for identification of command and control traffic, egress connections tend to be lower bandwidth than internal network segments, making egress monitoring more feasible than full internal monitoring.

We have long advocated full network packet capture, in order to enable advanced analytics and forensics on network traffic. In our React Faster and Better research we named the Full Packet Capture Sandwich: deploying network capture devices on the perimeter and in front of particularly critical data stores. This approach is totally synergistic with network-based threat intelligence — once you capture the network traffic you can can look for command and control indicators. Of course if full packet capture isn't deployed, you can just monitor the networks using purpose-built sensors looking specifically for these indicators. Obviously real-time network-based threat intelligence feeds integrated into the system are critical in this scenario — you only get one chance to identify C&C traffic because you aren't capturing it.

Another place for network traffic monitoring is internal DNS infrastructure. As described earlier, DNS request patterns can indicate domain generation algorithms and/or automated (rather than human) connection requests to the C&C network. Unless your organization is a telecom carrier you won't have access to massive amounts of DNS traffic, but large enterprises running their own DNS can certainly identify trends and patterns within their infrastructure by monitoring DNS.

Finally, in terms of deployment, you will always have the push/pull of inline vs. out-of-band approaches to network security. Remember that network-based threat intelligence is a largely reactive approach for identifying and finding command and control traffic which indicates a compromised device. The entire Early Warning System concept is based on shortening the window between compromise and detection, rather than attempting to prevent compromise. Of course it would be even better to identify C&C traffic on the egress pipe and block it, preventing compromised devices from communicating with attackers.

It would be even better to identify C&C traffic on the egress pipe and block it, preventing compromised devices from communicating with attackers.

But we need to be cautious with the bane of every security practitioner: the false positive. So before you block traffic or kill an IP session you need to be sure you are right. Of course most organizations want the ability to disrupt attack traffic, but very few actually use it. Most "active network controls", including network-based malware detection devices, are implemented in monitoring/alerting mode, because most practitioners consider impacting a legitimate connection far worse than missing an attack.

A Jury of (Network) Peers

So you have deployed network monitors – what now? How can we get that elusive Quick Win to show immediate value from network-based threat intelligence? You want to identify compromised devices based on communication patterns. But you don't want to wrongly convict or disrupt innocent devices, so let's dust off an analogy dating back to the anti-spam battles: the jury. During

the early spam battles, analyzing email to identify unsolicited messages (spam) involved using a number of analysis techniques (think 30-40) to determine intent. None of those techniques was 100% reliable alone, but in combination, using a reasonable algorithm to properly weigh their effectiveness, spam could be detected with high reliability. That "spam cocktail" still underlies many of the email security products in use today.

You will use the same approach to weigh all network-based malware indicators to determine whether a device is compromised or not, based on what you see from the network. It's another cocktail approach, where each jury member looks at a different indicator to determine guilt or innocence. The jury foreman – your analysis algorithm – makes the final determination of compromise. By analyzing all the traffic from key devices you should be able to identify the clearly compromised ones. This type of detection provides the initial Quick Win. You had a compromised device you didn't know was compromised, until you monitored the traffic it generated, and identified that traffic as possibly malicious. That's a win for monitoring & analysis!

> Nothing personal, folks, but we have yet to come across an environment of a few thousand machines without any compromised devices. It's just statistics. Employees click on stuff, and that's all she wrote.

You shouldn't worry about whether you will find anything with this approach. In just about any reasonably-sized enterprise, the network will show a handful to a few dozen compromised devices. Nothing personal, folks, but we have yet to come across an environment of a few thousand machines without any compromised devices. It's just statistics. Employees click on stuff, and that's all she wrote. The real question is how well you know which devices are compromised and how severe the issues are – how quickly do you need to take action?

Intelligence-driven focus

Once you have identified which devices you believe have been compromised, your incident response process kicks in. As we described in the Malware Analysis Quant research, the effort involved in fully investigating every device, analyzing and verifying each attack, isolating the malware in use, and searching for those indicators elsewhere in your environment is significant. Given the reality of limited resources, you'll need to make tough choices about where to focus first. The good news is that you will be able to leverage your network-based threat intelligence, along with other internal data, to generate a fairly clear picture of what to focus on. Let's roughly prioritize which compromised devices to deal with first:

1. **Critical devices:** Devices with access to protected information and/or particularly valuable intellectual property should bubble to the top. Fast. If a device on a protected and segmented network shows indications of compromise, that's **bad** and needs to be dealt with immediately.

Even if the device is dormant, traffic on a protected network that looks like command and control is smoke, and you need to act quickly to ensure the fire doesn't spread. Or enjoy your disclosure activities…

2. **Active malicious devices:** If you see device behavior which indicates an active attack (perhaps reconnaissance, moving laterally within the environment, blasting bits at internal resources, or exfiltrating data), that's your next order of business. Even if the device isn't considered critical, if you don't deal with it promptly it might find an exploitable hole to compromise a higher-value device. So investigate and remediate these devices next.

3. **Dormant devices:** These devices show behavior consistent with command and control (typically staying in communication with a C&C network), but aren't really doing anything yet. Given the number of other fires raging in your environment, you may not want to remediate devices immediately. But that decision is somewhat controversial, so we will handle it separately.

These priorities are fairly coarse but should be sufficient. You don't want a complicated multi-tier rating system which is too involved to use on a daily basis. And keep in mind that intelligence can provide a decent idea of the specific adversary behind an attack, as well as an indication of motive. Depending on what you know of the attacker (hacktivist vs. organized crime syndicate, for example), this may be another criteria to determine urgency and best path for remediation.

To Remediate or Not

It may be hard to believe, but there are real scenarios where you may not want to immediately remediate a compromised device. The first – and easiest to justify – is when the device is part of an ongoing investigation and HR, legal, senior management, law enforcement or anyone else has mandated that the device be observed and otherwise left alone. At that point the decision is no longer in your hands, and the ramifications of an actively compromised device on your network don't fall in your lap. Well, ultimately they will, but you will at least be able to point the finger at someone else as you get thrown under the bus.

Another scenario where remediation may not be the best course of action is when you need to study and profile the malware, and its command and control traffic, through direct observation.

Another scenario where remediation may not be the best course of action is when you need to study and profile the malware, and its command and control traffic, through direct observation. Obviously you need a sophisticated security program to undertake a detailed malware analysis process (as described in Malware Analysis Quant), but clearly understanding and identifying indicators of

compromise can help identify other compromised devices, and enable you to deploy workarounds and other infrastructure protections, such as IPS rules and HIPS signatures.

That said, in most cases you will just want to pull the device off the network as quickly as possible, pull a forensic image, and then reimage it. That's usually the only way to ensure the device is clean before letting it back into the general population. If you are going to follow any of the observational scenarios, however, they and your decision tree need to be documented and agreed on as part of your incident response plan.

Every security investment is scrutinized for value, but the good news is that network-based threat intelligence can provide immediate and measurable benefit in terms of identifying compromised devices. It is incumbent on you to tell the stories and show how the intelligence was instrumental in improving security.

Communicating the Win

As we discussed in Building the Early Warning System, your success stories won't tell themselves, so when the process succeeds – likely early on – you will need to publicize it and identify how network-based threat intelligence helped to identify compromised devices well before traditional means of finding successful attacks. Let's excerpt a bit from that research to illuminate what we're talking about:

> *There are two key areas to focus on. The first is finding proof of an attack in progress, which you successfully remediate thanks to threat intelligence and the EWS. This illustrates that you will be compromised, so success is a matter of containing the damage and preventing data loss. The value of the EWS is in shortening the window between exploit and detection. If you can definitively say that you get threat intel on emerging attacks (particularly on competitors or partners) and then evaluate whether action needs to be taken, that allays the fear of senior management that Security has no idea what's happening until it is already over – too late. Even better if you can discuss how preemptive workarounds and remediations, implemented in response to threat intelligence, blocked an actual attack. Finally, to whatever degree you quantify the time you spend remediating issues and cleaning up compromises, you can show how much you saved by using external feeds to refine your efforts and prioritize your activities.*

Every security investment is scrutinized for value, but the good news is that network-based threat intelligence can provide immediate and measurable benefit in terms of identifying compromised devices. It is incumbent on you to tell the stories and show how the intelligence was instrumental in improving security.

Go Operational: Integrating with Enterprise Security Systems

As compelling as network-based threat intelligence is, before you can provide value and increase your security program's effectiveness you need to integrate with other enterprise security systems. For instance, you will want to be able to send alerts about indicators of compromise to your SIEM or other alerting system to kick off the investigation process. Likewise, the ability to configure workarounds such as IPS blocking rules based on network indicators provides the ability not merely to identify compromised devices, but also to block C&C or exfiltration traffic. Obviously false positives are a concern – as with any blocking rule – but the ability to disrupt attackers can be extremely valuable. Likewise, integration with Network Access Control could shift a device flagged as potentially compromised onto a quarantine network until it can be investigated and remediated. All these integrations take the data from concept to action, and contribute directly to containing the damage from compromised devices.

In terms of forensics, network-based threat intelligence could integrate with a full packet capture/network forensics platform. In this use case, when a device shows potential compromise its traffic can be captured for forensic analysis. *The captured command and control traffic is the proverbial smoking gun.* You also get an opportunity to investigate the malware with the actual packets. This enables you to be more precise and efficient about what traffic to capture, and ultimately what to investigate.

By integrating network-based threat intelligence with more active security controls, it is possible to contain damage more effectively than waiting for the FBI, Secret Service, or your local law enforcement organization to let you know you have a problem.

Remember that the objective of an Early Warning System is to shorten the windows between compromise, detection, and remediation. By integrating network-based threat intelligence with more active security controls, it is possible to contain damage more effectively than waiting for the FBI, Secret Service, or your local law enforcement organization to let you know you have a problem.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com or ask via the Securosis Nexus (http://nexus.securosis.com/).

About the Analyst

Mike Rothman, Analyst/President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **The Securosis Nexus**: The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible. Access it at <https://nexus.securosis.com/>.

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and/or speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <http://securosis.com/>.