WhatWorks in Detecting and Blocking Advanced Threats:

A Real Case Study at a Large Research Organization

with

WhatWorks is a user-to-user program in which security managers who have implemented effective internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know more about? Let us know. www.sans.org/whatworks

About the User
The user interviewed for this case study has requested anonymity to maintain confidentiality, but has allowed us to refer to him as a Cyber Security Analyst at a Large Research Organization. The SANS WhatWorks program can help our security community at large make more informed decisions by encouraging seasoned professionals from major user organizations to share their stories without revealing the name of the organization.

Summary
A large research organization must allow users to collaborate, manage their own IT environments and aggressively use the Internet – all high risk activities. The desire to take a more aggressive approach to detecting security incidents prompted them to look at new toolsets to detect intrusions. In their evaluation, the team found that FireEye performed as a proactive sensor that actively inspected traffic on their high speed networks and detected malicious events that were going unseen by other installed network security systems. The FireEye products installed easily, are monitored and maintained with very little personnel overhead, and generate a very low rate of false positives.

~~~~~~

Interview

Q: Can you describe your IT environment?
A: We're an open laboratory and people need to collaborate. Our users take responsibility for maintaining and managing their systems. So they're able to download and install software code that is required to complete their day to day business. We're primarily a Windows 7 user base but we also have Macs, Linux and fewer than a thousand Windows XP boxes amongst a total of 15,000 systems on our network.

Q: What problems or threats prompted you to look for a product like FireEye?
A: We're constantly looking at new technologies. Our former CIO was approached by FireEye directly with the technology paradigm. Three to five years ago we were offered the opportunity to take a look at and evaluate this new malware protection system that sits on the perimeter of our network.

"Taking security defenses to the next level is what our researchers like to do – that's why FireEye is so compelling."

Q: In that time frame had you seen targeted malware or threats that caused you to be looking for that type of capability beyond the standard IDS antiviral tools you were probably already using?
A: Yes. We were using the traditional signature-based mechanisms, like Cisco IDSes, Snort IDSes and other signature-based anomaly detection. We weren't doing anything that was actively interrogating our traffic and detonating real-time binaries to determine their cause or purpose on our network.

Q: Was there an incident that you investigated and found things that got in? Was it general awareness of a threat? What got things moving?
A: The paradigm switch from a signature-based anomaly detection to a real proactive capability is what got things moving.
~~~~~~

Q: How do you acquire technology like FireEye and others? How did you convince management to fund it?
A: Our primary business is research. Our cyber guys are constantly challenging us with new problems and we're co-located and integrated within our research organization. I'm in an operational role, and we work together with researchers on projects and real-world problems. We're delivering and evaluating products – not reinventing commercial off-the-shelf tools. Taking security defenses to the next level is what our researchers like to do – that's why FireEye is so compelling. What can we do with the FireEye data? How can we integrate that into cyber intelligent systems or how can we pull it into indicators of compromise? Those types of next-generation capabilities are important to our customers and are driving our research here. We don't have to justify it; it's part of our process.

Q: Did you compare FireEye against any alternatives?
A: We always try to do that. For example, if you're looking at Cisco you're looking at Juniper and also probably looking at Palo Alto. But for FireEye there isn't really any competitor. From a commercial off-the-shelf capability perspective, we didn't have anybody really to compare it to – it didn't exist at the time.

Q: What did you procure and how did you initially get going?
A: We brought in the FireEye appliance. It's one of the few appliances that does exactly what it advertises: bring it in, put it in a rack, configure the interfaces and just wait for things to happen. It was just so fast and easy – so simple to use that you didn't have to bring in a team of offsite developers. It didn't require a bunch of professional services for four weeks to tune it and then tune it every year. You can operate it with very little personnel overhead and it feeds almost any SIEM or case management system. We were able to plug it in and immediately see effects on monitoring for malicious behavior. The other big bang for us was we didn't see 2,000 events a day; the events that we saw were meaningful. FireEye reporting results are very intuitive – a technician or an initial triage operator can review and evaluate the results.

"We were able to plug it in and immediately see effects on monitoring for malicious behavior."

Q: Where did you place the sensor topologically on your network? Just on an Internet feed and then inside a firewall?
A: If you're coming from the cloud into our environment the first thing you meet is our Blue Coat proxy and then the FireEye appliance. We initially had it out-of-band because we weren't comfortable blocking at that time, but we have since moved it into an inline blocking mode.

Q: Who manages and operates it?
A: From a cyber security perspective, we are managing and operating it. We have the full line of FireEye Malware Protection System (MPS) products here now (web, email and file). Based upon the success that we saw with the Web MPS with regard to the active threats against our environment, we've gone full in with FireEye to defend against advanced malware. Our security organization maintains and manages all appliances using FireEye Central Management System (CMS), which is very effective. Some of the other appliances, like Blue Coat, are managed by our network team.

Q: And you have the Web, Email and File MPS products?
A: We do. We're in a beta program with the File MPS product. We have the CMS, the Malware Analysis System (MAS), two email MPS and the web MPS. We're trying to get more redundancy out of our web network so we're looking at adding additional web MPS appliances soon.

Q: Where do FireEye appliance alerts go?
A: All of these alerts are forwarded into a case management system that we developed here. It's essentially an event triage type of environment that pulls the information in and classifies it as one of three categories: Runners, Repeaters and Strangers. For Runner events, as an example, the FireEye Web MPS will report on a callback activity. So if a system is detected that matches a pattern of behavior indicative of transmitting data out to the command and control server, then we will burn and rebuild that system. The system is compromised and we don't have to question it, given the fact that FireEye alerted on it. We gain no further intelligence so we have the system imaged and the recommendation is sent directly to the service desk without having a cyber operator triage it. Stranger events are new and emerging. What we traditionally found with the FireEye Web MPS was when it detected a malicious binary, a few days later the anti-virus companies would provide signatures and we would find other compromised systems in our environment. Stranger events require some level of human investigation. Repeaters are systems that are coming through our environment more than one time; it could be a false positive issue, but it could also be that we're missing something in the analytics.

Q: How did you detect things prior to deploying FireEye? Were you simply using AV and the existing IDS?
A: Right. AV, existing IDS, and our SIEM. Think of it as a pyramid with this case management system sitting over the top of it, so the rest of our appliances, our events, are essentially feeding up to that case management system.

Q: Once you deployed FireEye did it give you visibility into things you weren't seeing before or reduce the amount of human time it was taking to deal with alerts that were bubbling up through these other sources?
A: FireEye is catching zero-day events and it's catching them much faster than our AV or other traditional signature-based detection systems. There's also the FireEye Dynamic Threat Intelligence Cloud that shares threat intelligence globally. If a FireEye customer on the East Coast receives a malicious binary, I know of it before my end-users even show up for work – it really reduces the threshold between when you potentially have an event and when you have knowledge and intelligence about the event.

"FireEye is catching zero-day events, and it's catching them much faster than our AV or other traditional signature-based detection systems."

Q: The 2011 event was something that FireEye alerted you to. Can you walk me through that event?
A: FireEye detected some initial indicators that there was a threat from an adjoining network with whom we had a trusted relationship, but we did not manage their network. Several months later after the incident, we were informed of the compromise that happened in the other adjoining network. We were able to detect, monitor and then

remediate within a few days versus having to wait three to four months for the other network to realize their problem and then inform us about it.

Q: What sort of indication was it? Was it an inbound executable that triggered FireEye?
A: The indicator was a malicious executable downloaded onto the victim system as a result of casual browsing by the user. In "The Anatomy of a Hack" they start off with goal setting and then reconnaissance and then the third step is to develop access. FireEye is detecting these threats at the develop access phase. Before they're ever in your system and able to act on the target, you're detecting them with the FireEye appliance.

Q: Have you kept any statistics before and after using the FireEye approach?
A: I do have data for the period of time. A great number of our events are detected by the FireEye Web MPS; drive-by downloads are a huge problem here. Prior to FireEye, we were processing around 232 events and 47 incidents per month. Now, with FireEye we actually double that. We're now seeing 400 to 600 events, and about 80 incidents a month.

Q: Any lessons you learned as you went through deploying and as a user that you think would be helpful to other people following in your path?
A: Put the FireEye appliance in inline mode of deployment. Don't mess around with evaluating it in an out of band condition. My biggest piece of advice is just to architect it the way that they tell you to architect it from the get-go. The CMS is invaluable if you're going to try to manage a global grid; it really makes it a lot easier on the overhead and a lot easier for the analyst or the system administrator to manage from one central location. The email appliance we found is equally as valuable as the Web MPS.

Q: On the email side, are you using something else to look at inbound attachments, using FireEye in addition to it, or did it replace what you had been using?
A: We had an IronPort appliance sitting on the border and its spam filter eliminates about 90 percent of the incoming email, but we're still catching a significant number of zero-day binaries and attachments. I can recall one apparent APT threat that spoofed the identity of one of our managers and then sent inbound emails to that person's staff. They misspelled several of the staffers' names so those emails got dropped. The ones that made it through had malicious URLs. We had to have at least one person click on the link; the FireEye appliance evaluated it and then blocked subsequent clicks on the link. Only that one system was compromised and we rebuilt it.

Q: What about any lessons learned in any tuning you have to do or false positives or that type of thing?

"FireEye is one of the few systems that I've seen that does what it's advertised to do."

A: If you're going to be managing more than one appliance, definitely evaluate the CMS and deploy it in your architecture. In terms of false positives and tuning, it's a very low rate and you can manage a lot of the false positives and tuning from the client itself. You can also work with FireEye tech support and within an hour or two they usually give you the information you need to tune your appliance or they'll issue a new security update. FireEye is one of the few systems that I've seen that does what it's advertised to do.

Q: How is tech support; any problems on that side of things?
A: I have not had any issues with regard to tech support. They were slow for a while, but they're definitely making changes and growing as an organization and a company. We've seen huge changes in their user interface. FireEye has also implemented some of our requests; for example, integration with some of my other appliances; the ability to send an alert out to my host-based analysis system; and to pull the data off of the host to compare the sandbox. We have full packet capture by clicking on a link. The output from FireEye's appliances and the way they integrate and intelligently communicate with the other systems is phenomenal. We have a capability to collect forensic data on the victim, or host, and compare it to the data that FireEye generates when it reports an event. I just don't see that in other offerings.

"The output from FireEye's appliances, and the way they integrate and intelligently communicate with other systems is phenomenal."

Q: Are there any new features you are looking for FireEye to add in the future?
A: Yes. Improving some of the analysis capabilities; for example, being able to query into the cyber intelligence that is specific to us here. I want to be able to customize the images that run in the FireEye virtual machines; right now the standard image that comes with the appliance is not representative of our environment. It should include Mac and Linux and other operating systems and the ability to customize those that are interesting to us. We'd like mobile capability. We need to be able to secure our cloud offerings and extend it out to our mobile hosts. Currently, I only know when they're behind my cloud or when they're behind my sensor grid. We're looking for FireEye to be the innovator there and provide us with some solutions.

Q: How much care and feeding does it take to manage and monitor the FireEye appliances?
A: I have a total of five FireEye appliances, including the file MPS, which we're evaluating as a beta product. We probably spend a tenth of one head maintaining all five of them.

SANS Bottom Line on FireEye products at a Large Research Organization:

1. Simple to install without professional services;
2. Requires little manpower to monitor and maintain;
3. Works with many SIEM products and is simple to integrate into case management systems;
4. Accurately detects targeted malicious executables and compromised machines with a very low percentage of false positives;
5. Good tech support and overall high marks for innovation and responsiveness.

For more information, visit www.fireeye.com, email Info@fireye.com or call FireEye at (877) FIREEYE.