LISA '10
Speaking Proposal Category: Practice and Experience Reports

Presentation Title: "When Anti-virus Doesn't Cut it: Catching Malware with SIEM"

Proposed by/Speaker:

Wyman Stocks
Information Security Manager
NetApp
919-476-5252
Wyman.Stocks@netapp.com

Report

Proposed Topic: "When Anti-virus Doesn't Cut it: Catching Malware with SIEM"

Malware is a problem that cuts across most every industry that uses computers today. It is also a good example of a threat that most companies assume is stopped at the perimeter. However, this presentation will discuss the danger of relying simply on desktop or perimeter security to catch an insidious threat like malware.

SIEM is short for Security Information & Event Management. Simply put, these are event correlation engines for logs. These systems help your limited security staff make sense of millions of events per day. They put many log types into one console which reduces training and analytical time.

Conficker was a wake-up call for us. I head a small team responsible for comprehensive security across over dozens of sites with over 12,000 end user devices (desktops, laptops, mobile devices, etc.) We followed standard protocol and rolled out the patch within 24 hours. Everything seemed fine. Unfortunately, like many large companies, the patch didn't hit every one of the thousands of the devices it needed to.

A few months later, we were alerted by a third party that large amounts of Conficker traffic were coming from our network. Our initial reaction was one of disbelief because we had rolled out the patches, our anti-virus software was widely deployed and updated almost daily and we had intrusion detection including the SIEM. We pressed the 3rd party for evidence. They were a little reluctant, but finally sent us some logs. Their logs matched what we saw in our SIEM.

We found many malware-infected machines that anti-virus wasn't catching. Our reaction turned from disbelief to concern because the traffic was leaving our firewalls.

To root out the problem, we used a combination of event correlation, automation and process.

1. We dedicated teammates to reviewing the logs. For example, we found generic bots and machines that were infected sending out spam. We started looking for excessive port 25 traffic. We found that by correlating certain network behaviors using session data and SIEM intelligence, we could detect malware.
2. We leveraged our SIEM to contact users immediately via email when malware was detected.
3. We set up a protocol for users to follow, giving them exact instructions on what to do to fix the problem

Our analysts worked almost daily with our anti-virus vendor collecting and submitting samples to automate the cleaning of these infected workstations. In the press we read there were only about five or six variants of Conficker. Our experience was there were many "strains" of each of those variants that anti-virus did not catch until we sent samples into our vendor.

Result: We reduced daily average from 30-50 infections to less than 10 per day in just 2-3 weeks. Today we are building more visibility into the network so that we can capture malware before it even gets to the end user.

Various indicators were used to find infected computers. These included things like traffic to known "Command and Control" (C2) servers (where malware gets instructions on what to do next), unusual network behavior on particular protocols, and other clues found during the course of investigations.

Several lessons were learned along the way that helped us understand not just the capabilities, but also the limitations of using SIEM technology. First, timestamps become extremely important when you have most of the logs from your enterprise in one console. If you are not aware of time differences, you will miss key pieces of data. Secondly, once you get past the initial wave of a certain type of crisis; the false positive rate goes up. This is mainly owing to thresholds being lowered on what actually triggers a correlation event. Thirdly, you have a learn things about your network that may not be that useful in order to get to the useful info. An example of that is in the course of investigating "spambots" you find out just how many people actually still use external SMTP servers for their personal mail. These are false positives and it is mildly useful in telling the story, but not that useful in protecting the company's network.

Going forward we have several initiatives that came out of this. One initiative is putting more emphasis on feeding our prevention measures by using data from detection and response activities. We also realized we need to build more visibility into our network. This will allow us to validate events without having to rely too much on interviewing end users and administrators. Another initiative will be to be more diligent in doing historical look-backs to see how long activity has been on our network. This will feed our detection capability as well as our response plans. It will also allow us to start thinking more in terms of attribution over the long term rather than just fixing problems one at a time.

In addition, we'll review how we use SIEM (security information and event management) and log management and discuss how to use the two together to monitor and catch other types of security threats. While not a silver bullet, SIEM has been a huge time saver for our small team, as our systems generate about 50 million events per day.

Tags: security, case study, malware, SIEM, anti-virus, managed security service, information security

Presentation Outline

Proposed Topic: “When Anti-virus Doesn’t Cut it: Catching Malware with SIEM”

- What is SIEM?
  - Security Information & Event Management
  - Simply – a correlation engine for event logs
  - Helps you make sense of 50 million events per day
- The wakeup call
  - External org informally notifies us of Conficker traffic
  - Volume is more than normal for a company of our size
- Initial Reactions
  - Disbelief
    - We rolled out the patches
    - We have AV and a SIEM
    - Asked for more info from external org
  - Concern
    - After looking at evidence
    - Traffic was leaving our firewalls
- Response
  - Use SIEM to identify network behavior indicative of a bot infection
  - Validate and engage end users manually
    - After two weeks, this was too labor intensive
    - False positive rate was very low
  - Automate notification to end users with instructions for clean up
  - Get as many unique samples as possible and pass to AV vendor
- Results
  - Drop in daily detection rate of between 30-50 to less than 10
  - <insert pretty chart>
- What did we look for?
  - Known Command and Control servers (C2)
  - Unusual volume on a particular protocol
  - Other indicators found during investigations
- SIEM automation lessons learned
  - Timestamps must be sync’d across enterprise
  - Short VPN connections cause problems in identifying the correct user
  - When volume drops, you can have a higher false positive rate
  - You have to learn things about your network that may not be that useful
- Next steps
  - Feeding prevention measures

- Building in more visibility
- Historical look-backs to determine attribution