WannaCry – USM Gives Full Visibility

At this point everybody has likely heard about WannaCry, a new ransomware variant that is exploding in the news. It's epidemic—in a very short period of time, hundreds of thousands of systems in over 99 countries have been compromised, including high-profile victims like the British National Health Service (NHS). The attack is reminiscent of the OpenSSL vulnerability last year and Heartbleed the year before. Given USM's ability to detect this threat, this presents a tremendous opportunity for you to sell the awesomeness that is USM to your prospects.

Here is what you need to know...

What is WannaCry?

WannaCry is a ransomware variant that takes advantage of an exploit in the Windows operating system (MS17-010) that was released by a hacking organization called Shadow Brokers in March. The exploit and tools were allegedly part of a collection of spy tools used by the National Security Agency (NSA). Microsoft patched the vulnerability pretty quickly after the release, but there are likely millions of computers that have not been updated even today with that latest patch. Thus, they are vulnerable and actively being attacked. WannaCry exploits that known vulnerability to get a foothold into an environment and spreads, potentially without the need for authentication or any other user action. It's pretty bad and will likely get worse before it gets better.

Can AlienVault be used to detect systems vulnerable to MS17-010?

***Absolutely*.** Both USM Anywhere and USM Appliance have a built-in signature to detect this vulnerability on our customer's systems. Customers can run a scan of their systems to assess and identify the ones that are potentially vulnerable. We highly recommend that our customers run a scan immediately to identify vulnerable systems and apply the patch. Failing to do that can quickly and easily result in a compromise should WannaCry get into their environment.

Can AlienVault be used to detect attacks using the MS17-010 Vulnerability?

Absolutely. The AlienVault Labs Security Research Team published updated threat intelligence for both USM Anywhere and USM Appliance to detect exploitation of the vulnerability. If a system is discovered to be exploited, an alarm will be generated so that the AlienVault security analyst can immediately go remove the system from the network and resolve it.

For customers who are using USM Anywhere, they also have the added benefit of the built-in response orchestration capability offered by the Forensics and Response AlienApp. Via this app, if a system is determined to be infected, the user can immediately take a response action that quarantines or otherwise shuts down the infected system to prevent the system from further attacking and infecting other systems on the network. This is **not** something a traditional SIEM can do. It's the power of unified security and orchestration action response!!

What do USM users need to do?

USM Anywhere users are automatically updated and protected. There is nothing they need to do other than perhaps run a vulnerability scan on their systems. USM Appliance customers just need to update the threat intelligence on their system to get the latest signatures so that their USM Appliance solution can detect the vulnerability and threats. (This function will be automated in the next update v5.4)

What do you need to do?

You have at your disposal one of the best threat detection and incident response solutions on the market. It combines the essential security capabilities with the threat intelligence

(such as this) needed to stay on top of new and/or emerging threats in the wild.

If you have a customer who is concerned the impact on their business of an undetected threat, Alienvault has the solution for existing threats and future peace of mind.

Register your customer today and we can show them how Alienvault USM can help protect their business.