SYNESIS For Cyber Security Markets

WHITE PAPER

By Steve Wong
steve.wong@toyotechus.com
https://www.linkedin.com/in/stephencwong/

INTRODUCTION

In May of 2017, the "WannaCry" network cryptoworm was set loose onto the world, causing chaos in data centers across the globe. According to some estimates, this cryptoworm impacted more than 200,000 organizations in 150 countries[1].

WannaCry belongs to a class of cryotoworms known as ransomware and the way they work is especially treacherous. This cryptoworm attacks Windows operating systems (OS) by going after a known exploit in the OS. It would encrypt files and demand a ransom payment in exchange for decrypting these same files. If your files were affected by this worm, and you do not pay the ransom, the net effect is as if your files had been deleted. Furthermore, this worm has a transport mechanism which allows itself to propagate over networks, potentially creating havoc on networks near and far.

A month after this worm was unleashed, a total of over 130,000 (USD) was paid by victims to have their files decrypted. Both Microsoft and the British government believe a certain Asian rogue country was the launching point for WannaCry.

Then in late March of 2018, officials in Atlanta, Georgia reported that the city's computer systems were still not yet fully operational after the city was hit with a wide scale ransomware attack the previous week. It left the capital city crippled with many city employees unable to access the Internet or e-mail. In many city offices, it was reported that many were operating on pen and paper instead of computers.

Meanwhile, Wi-Fi access at Hartsfield-Jackson Atlanta International Airport, the world's busiest airport, was turned off as a precaution. Hackers ultimately demanded a $51,000 ransom payment. The cost in lost productivity, however, was far greater.

These two recent incidents highlight how much our digital infrastructure is at risk due to cyber attacks.

LIMITATIONS OF NETWORK SECURITY APPLIANCES

The field of Network Forensics is a sub-branch of digital forensics relating to the monitoring of networks and also capturing network traffic for further analysis. Organizations can only benefit from network forensics by having complete records of past network events for their protection as well as their customers.

As organizations grow so also does the amount of network traffic they generated and received. IT groups may keep long-term records of network traffic in metadata form but the most comprehensive form of network record keeping are packets. But recording all network packets is typically not possible. Packets will be lost due to oversubscription due to high traffic rates and limited storage.

Modern network security appliances from many cyber security companies are designed to protect organizations from security breaches including malware, viruses, trojan horses and cryptoworms like WannaCry. They are often an enterprise's first line of defense. Furthermore, these appliances are often updated to insure that they have the latest signature profiles of malware, viruses, trojan horses and cryptoworms to aid with detection.

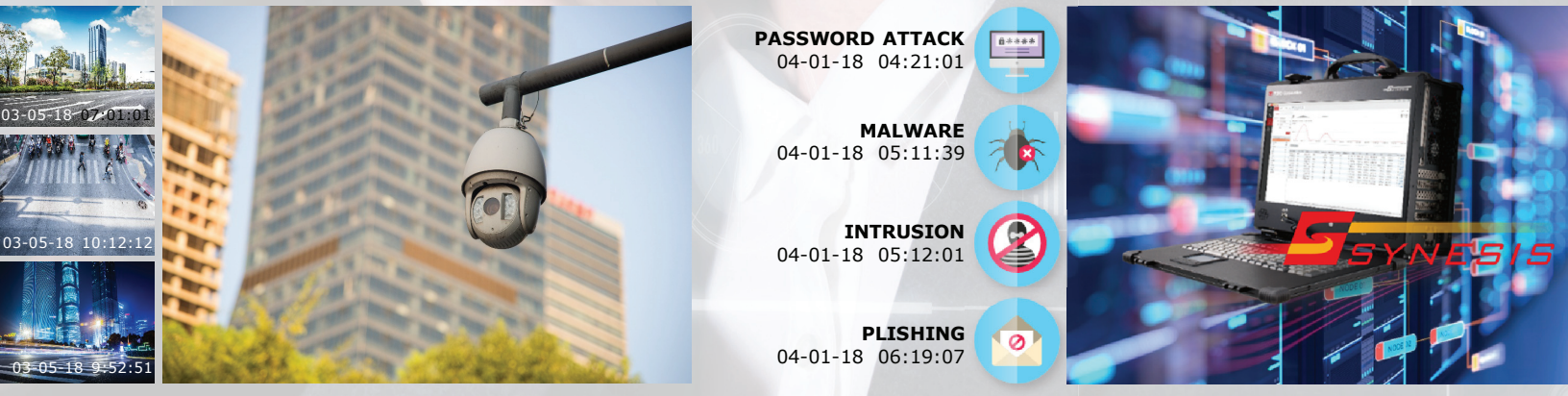

Figure 1: Works just like a Video Surveillance System but Designed for Networks

[1] source: Wikipedia

These appliances are designed and optimized for packet-level, real-time analysis; as such, they lack a number of proven capabilities that would make them more adept at and capable of identifying and combating cyber attacks.

For example, these appliances typically have limited storage capabilities and cannot store any large amounts of data or network packets, particularly in high-speed networks. This limits any ability to perform any meaningful network forensics once an attack has taken place. Without such information, there is no way to examine the network packets and flows that have contributed to this breach.

COMBATTING THREATS WITH SYNESIS

With its deep packet store technology supporting up to several hundred terabytes of high-speed packet capture storage, SYNESIS offers the only solution in the market able to capture network packets at 1, 10, 40 and even 100 Gb/s Ethernet line rates. Every network packet and event is captured without exception. The way SYNESIS works is analogous to a surveillance camera that continuously captures and records all video. The difference is that SYNESIS works on network data. See figure 1.

In figure 2, we show how SYNESIS can be used in conjunction with a cyber security appliance to provide a tried, reliable and repeatable method of capturing network data for the purpose of providing data availability for such appliances. The idea here is that network data is "mirrored" to the cyber security appliance as well as the SYNESIS. When a security event does occur, the network frames and flows associated with that event can be analyzed and/or passed on to law enforcement agencies and cyber security experts. See figure 3.

PACKET REPLAYER

The SYNESIS product also offers a packet replayer feature that is especially useful for companies that are developing security products. With this capability, real-world wire-rate traffic can be captured and replayed with micro-second level packet gap granularity. Once a cyber security vendor has written code to detect and address a particular threat, it becomes important to test it in an environment to demonstrate that it truly does function as intended. The packet replayer feature of SYNESIS provides exactly this functionality.

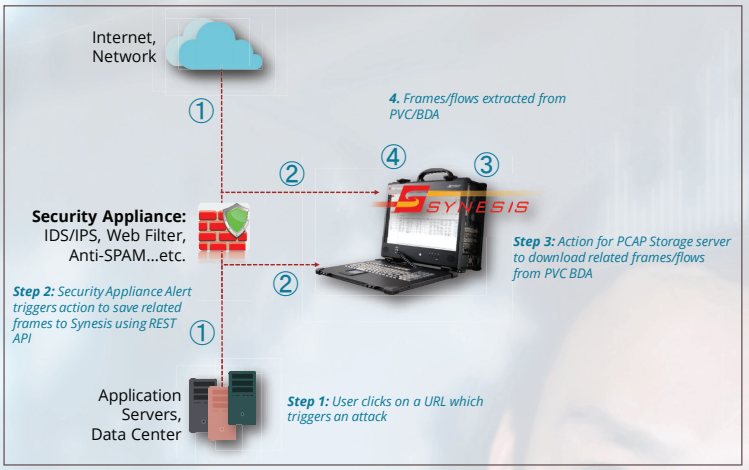

Figure 2: SYNESIS Used In Conjunction with Other Cyber Security Appliances

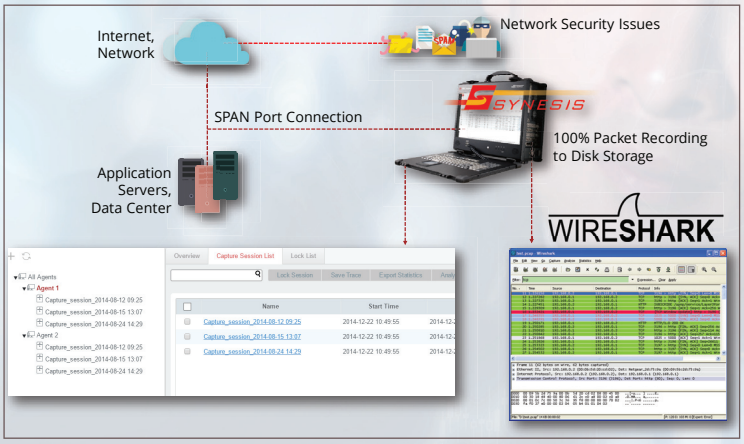

Figure 3: 100% of Network Traffic Is Captured Allowing for Forensics

CONCLUSION

Whether you are an enterprise company trying to combat cyber security threats or a vendor developing cyber security products, you will find that SYNESIS is an invaluable solution to complement your existing toolset.

TOYO Corporation
Quest for Precision
TOYOTech
42840 Christy Street, Suite 110, Fremont, CA 94538
Phone 510-438-9548
http://www.toyotechus.com

06/17/2018 (SCW)