INTRODUCTION

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

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

A month after this worm was unleashed, a total of over $130,000 were paid by victims to have their files de-encrypted and recovered. Both Microsoft and the English government believe a certain Asian rogue country was the launching point for WannaCry.

Then in late March of 2018, officials in Atlanta, Georgia said 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 email. 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 shutdown as a precaution. Hackers ultimately demanded a $51,000 ransom payment from the city. The cost in lost productivity is far greater.

These two recent incidents highlight how much our digital infrastructure is put at risk to cyber attacks in our connected world.

LIMITATIONS OF NETWORK SECURITY APPLIANCES

As organizations grow so also does the amount of network traffic. Corporations may keep records of traffic using data records but the most comprehensive form of record keeping are packets. However, recording packets is not possible at high rates. Packets will be lost due to oversubscription due to high traffic rates and limited storage.

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

Modern network security appliances from many cyber security companies are designed to protect organizations from numerous 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 detections.

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 very limited packet storage capabilities and thus cannot capture and store any large amounts of data or packets, particularly in modern high speed networks. This limits any ability to performing any sort of meaningful network forensics once

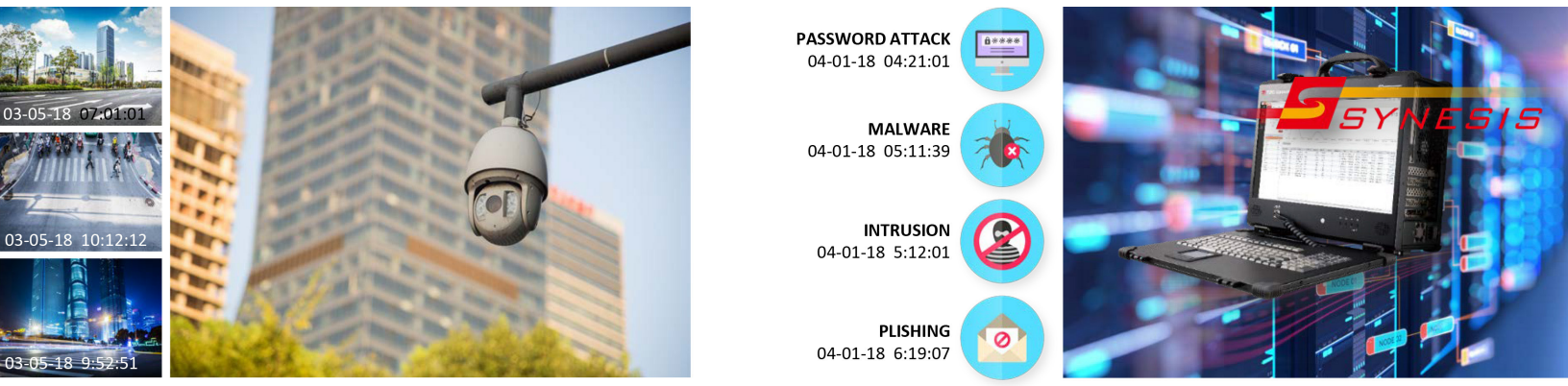

Figure 1: Works just like a Video Surveillance System but for Designed for Networks

[1] source: Wikipedia

an attack has taken place as possessing large volume of continuous past network events is required. Furthermore, without such information, there is no way to examine the network packets and flows that have contributed to this breach.

COMBATTING CYBER SECURITY 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 place able to capture network packet at 1, 10, 40 and even 100 Gb/s Ethernet line rates without packet loss. Every network packet and thus event is captured without exceptions. The way Synesis works is analogous to a surveillance camera that continuously captures and records all video. The difference is that it works on network data. See figure 1.

In figure 2, we show 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 insuring 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 stored away and/or passed on to law enforcement agencies and cyber security experts. See figure 3.

PACKET REPLAYER

The Synesis product 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 one of these cyber security vendors have written code to detect and address these threats, it becomes important in a test environment to demonstrate that it truly does work. The packet replayer feature of Synesis provides exactly that functionality.

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 an invaluable solution to compliment your existing toolset.

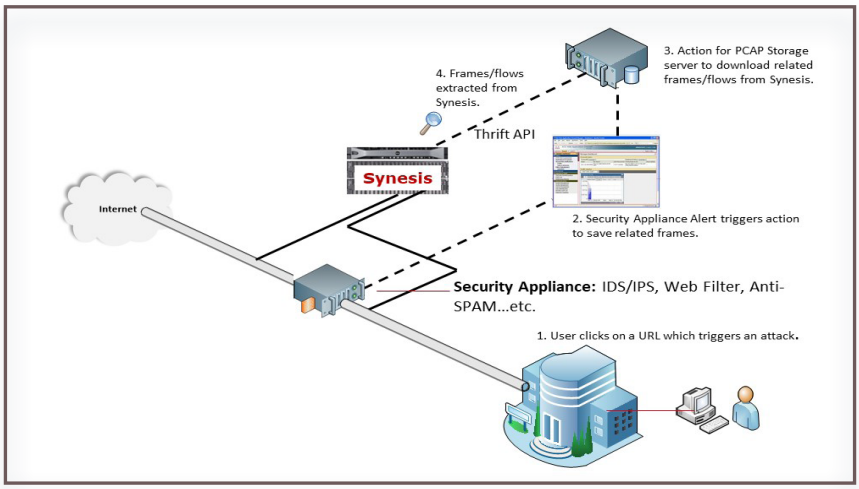

Figure 2: Synesis Used In Conjunction with Other Cybersecurity Appliances

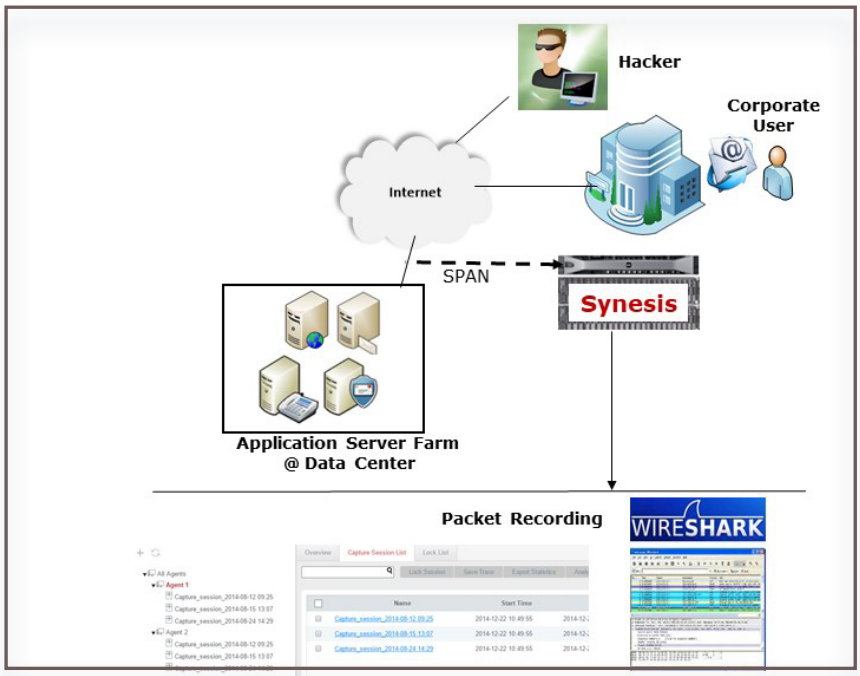

Figure 3: 100% of Network Traffic Is Captured Allowing for Forensics

TOYOTech LLC
42840 Christy Street, Ste. 110, Fremont, CA 94538
Phone 510-438-9548
http://www.toyotechus.com