KNOW THE UNKNOWN®

Success Story:
WannaCry Ransomware

WHITE PAPER

Challenge

Worms like WannaCry and Petya operate as essentially zero-day attacks: they can lie dormant on our networks and then rapidly spread between devices upon waking up. The consequences of being hit by one is dramatic: precious data is either ransom-locked or wiped and thus often irrecoverable. This means millions in lost data, restoration fees, public relations, and stock-holder confidence.

When FedEx was hit by Petya, for example, their subsidiary TNT Express experienced "widespread service delays" and were unable to "fully restore all of the affected systems and recover all of the critical business data that was encrypted by the virus."[1] Shares in the company dropped 3.4% in the wake of the attack.[2]

Consumer goods giant Reckitt Benckiser downgraded their full-year revenue growth target by 1% due to the same attack. The company's CEO said around 500 systems, 2,000 servers, and 15,000 laptops were affected by the virus, which took a mere 45 minutes to 1 hour to propagate. Company shares dropped 3% following this announcement.[3]

A similar attack on ECMC, a hospital based in Buffalo, NY, took down 6,000 computers and forced staff to rely on paper charts and face-to-face messaging. According to their own admission, remediation costs totaled nearly $10 million.[4]

Losses to companies have hit hundreds of millions of dollars. Networks infected by such worms cause widespread service and business disruption, staff inefficiencies when calendaring systems go offline, and large-scale data loss when work, emails, and notes are wiped out. Such costs will only continue to mount as new cyber threats and vulnerabilities are always found. Not long after the WannaCry and Petya attacks, for example, Microsoft announced a newly discovered exploit in all SMB protocols which threatens nearly every enterprise across the world. [5]

The most difficult challenge with these worms is finding them and halting their spread before such massive damage is done. They leave very little trace of their entry before they wake-up, making spotting the WannaCry attack before it takes place incredibly problematic. And when the attack begins, their spread is extremely fast and can take down huge portions of a network within a single day.

Stopping a Worm & Saving Millions

Even the most recent of these attacks like WannaCry and Petya still echo the basic principles of past-worms, and as such, they are both preventable and stoppable. During the Code Red, Nimda, and ILOVEYOU attacks of the early-2000s, businesses that had invested in a NIKSUN-like solution were able to run a rapid report to get a list of all infected devices and cut them off from their network. Instead of thousands of machines being affected, they were able to resolve the incident with minor losses of hundreds or less. This process takes a mere few minutes and thus could have saved Reckitt Benckiser from their hour-long attack.

Total, 100% visibility is simply the only way to stop these worms from becoming too damaging. It not only makes the worm trackable and stoppable as it spreads, it can even allow you to discover it while it is sitting dormant. By having a holistic view of your network, you can find out exactly where a worm is and where it is spreading to so that it can be removed from your network.

There is no other way to get this information. Just as the CDC needs to know who has a virus and where they are located so that it can quarantine them to stop its spread, administrators need a full view of your network to find and resolve malware incidents. Similarly, this 100% visibility is needed to conduct a thorough investigation ex-post to understand who let malware onto your network, when and where it happened, and how it took place to better protect your assets in the future.

While many businesses are not proactive in protecting themselves from such threats, those that are save themselves from massive losses. Cyber attacks are a real, known problem with widespread consequences. Taking the steps necessary to detect and resolve incidents is absolutely critical to ensuring your company stays afloat.

Why Do Cyber Threats Persist Despite Significant Investment to Counteract Them?

The fundamental reason that many cyber attacks still get through is because all traditional security sensors still rely upon known vectors. While many solutions claim to supply us with "all the data," it is important to inquire whether it is really "all of it" or just "all of that which they are aggregating."

For example, log aggregation solutions may suggest "we have all the data" and, indeed, they can supply us with every log that has been made. However, let us think about how the logs are generated in the first place. In the example of a computer, the logs that are generated are a result of someone determining what is important to log in the first place. It is fundamentally restricted by some input that dictates what to log and what not to log.

The same problematic input is required in event data collection. Someone, or some configuration, has determined the conditions under which an event is generated. SIEM tools then collect all these events and present them to the user for analysis. So yes, they do have "all the data," only if the definition of the data is "all events."

Similarly with flow data, it is determined what flows to log and how much metadata to include in the flow record.

Inevitably, when we implement a solution where we believe we have "all the data," we need to fundamentally understand if it is "all" or some subset category of the greater "all."

It should now be clear how zero day attacks succeed. We may think we have "all the data" but we actually are only given "all the logs or events" that we are collecting. Hackers, or to be precise crackers, know that this is what we are doing. They design their attacks to go around the visibility that we have into logs and events. In other words, they find a way around these known methods by operating in the "dark" parts of our networks.

So how can we succeed here? In order to understand what solutions might actually work, we can turn to the physical world to gain some insights. In this realm, for example, buildings have access logs. Collecting all access logs may lead us to conclude that we have "all the data," but in reality, it is not sufficient to prove who did what, when, where, and how. While access logs may help us look for a correlation between when someone entered and what occurred, such a task often requires a supremely time consuming investigation and yet can never be 100% definite if there are multiple personnel that may match our search criteria.

If a robbery takes place, how can we know that, without a doubt, it was a particular individual who is responsible? How can we prove what they did, when, where, and how they did it? The answer to this is to place security cameras that monitor and record the entire building, 24/7. Not only can we then immediately rewind back in time to see any incident that has taken place, we can also watch video feeds in real-time and stop security breaches as they occur. In fact, we can also set up image processing software that can look for patterns and behaviors and send out alerts, lock doors to trap the intruder, and more.

So the obvious answer to our problem of stopping and investigating cyber threats, including even zero day attacks, is to create something like a security camera that watches over every transaction. This is exactly what NIKSUN has been doing and perfecting over two decades. NIKSUN integrates full (or partial if required for privacy, etc.) packet capture with complete analytics at the packet, session, and all the way to the application layer. With NIKSUN, zero day attacks cannot be hidden from surveillance because it has already captured all actual activity of the malware. The malware has no way to circumvent being captured if it is deposited via the network or if it conducts any activity on the network.

Metadata, flow-data, malware, and APT analysis, as well as anti-virus programs and system patches, are proven now to be insufficient to combat such attacks. While such tools are useful in their own right (and all of these types of analysis are also included in NIKSUN's solution suite), they cannot provide answers to unknown threats that operate in the "dark" part of your network – the part that we aren't collecting logs and events about. Analysis can only be done with pre-known knowledge, so zero-day attacks and worms which hide under the typical radar are not easily detected and resolved. Anti-virus programs also rely on having the signature of an attack prior to it occurring, while system patches are only a retroactive fix and cannot find malware that was deposited while doors were open.

Given that NIKSUN has the ability to record a vast amount of information, the question becomes if we can find the information that we are looking for quickly. If we were to take continuous, 24/7 footage of a vault, for example, it would be useless without being able to easily search through it to find notable events. This fundamental difficulty is exactly what NIKSUN has solved and why it is the pioneer and industry leader in this space. NIKSUN's singular mission is to record all data at the highest rates without dropping a single packet and at the same time also index all the data in real-time to allow for extremely fast searching.

But can anyone, not just heavily specialized cybersecurity experts, use such a tool? Over the course of its existence, NIKSUN has made this possible as well. NIKSUN operates with a plain-English (as well as advanced expression for the experts) search and provides an extremely user friendly

GUI, expert tools, and point and click analysis that is a game changer in the industry. It boils investigation down to just one or two clicks and visualizes everything that we need to know for easy and rapid forensics even if the user is not a forensics expert.

In the case of WannaCry, for example, it shows us exactly what devices are infected and where the worm is trying to spread with a simple diagram and list of IPs. While many tools also allow for good visualization, the NIKSUN GUI is highly pivotable from any information to any other, giving the user a very quick way to find the needle in the haystack. Thus, even a non-technical person can find the information they seek. This is critical because of the limited cyber security resources available today. In this industry, we often have to leverage tools to handle complex tasks, and as we shall see in the example below, NIKSUN has engineered a solution addressing this concern.

Stopping WannaCry With Just a Few Clicks

Let us take an example in which a WannaCry worm has entered a network and begun spreading to see how NIKSUN can help us detect and resolve this incident. In doing so, we can save millions of dollars associated with losing thousands of machines and their critical data.

We enter the NIKSUN GUI, which is a robust web-based platform that can be accessed from any smart device. To determine where the WannaCry worm is and is spreading to, we can use a simple plain-English search to determine what anomalous traffic is moving through Microsoft's SMB protocols (colloquially known as EternalBlue). Practically speaking, this intuitive feature of NIKSUN's solution means that all network activity here could have been easily monitored as soon as Microsoft announced the SMBv1 vulnerability. This means that WannaCry and Petya could have been found even before their signatures were publicized. Even though these attacks were "unknown" threats at the time, they are still discovered by NIKSUN.

Let us say we are a non-expert and don't know much about what to look for. So we will simply enter the terms "port SMB and not apptype SMB," to say "give me all information about devices communicating through the SMB service but was not really SMB," i.e. faking to be legitimate SMB traffic. We could also have easily used "port 445 and not apptype SMB," if we were so inclined. The NIKSUN application will sort all the synonyms out on its own. Figure 1 below is a screen shot of the GUI where we are now presented with all traffic moving through this open door that is not a standard communication on the SMB protocol.

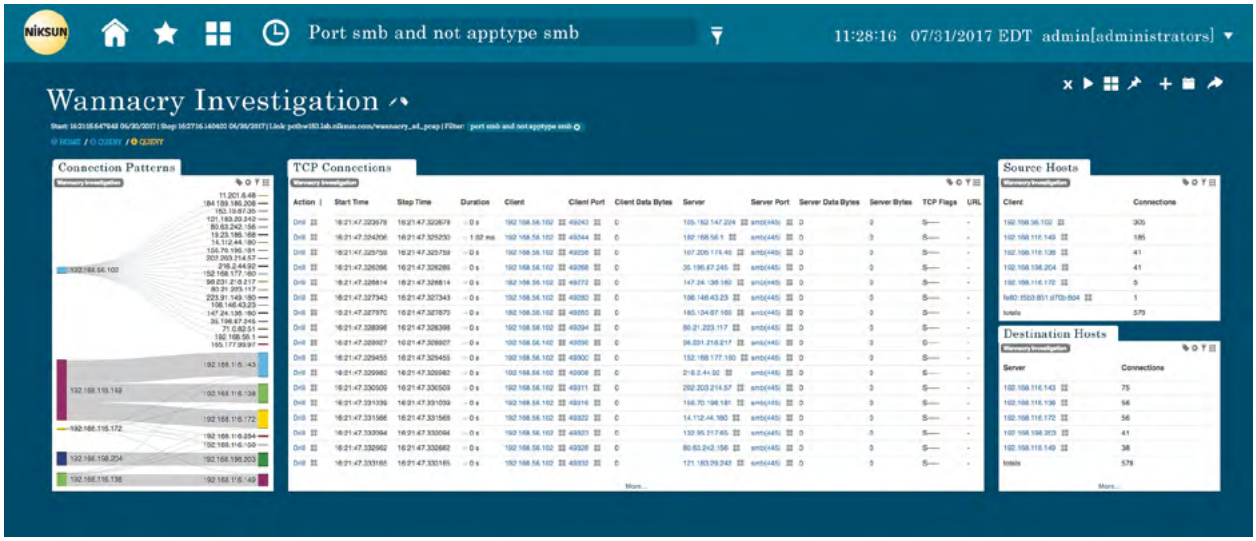


***Figure 1**: Overview of Anomalous Behavior on SMB*

We immediately notice the primary infected hosts in the "Connection Patterns" tile (far left). Let us zoom in on it by clicking the tile or with either a standard browser zoom or a pinch zoom on a touch device. As shown in Figure 2, we can see that the IPs 192.168.56.102 (in blue), 192.168.116.149 (in red), 192.168.116.172 (in yellow), 192.168.198.204 (in purple), and 192.168.116.138 (in green) are clearly acting anomalously by scanning multiple devices on the SMB protocol. So with just one plain-text search, NikOS Everest has brought up and displayed all infected devices on this network. It has also visualized WannaCry's attempted spread for further monitoring.

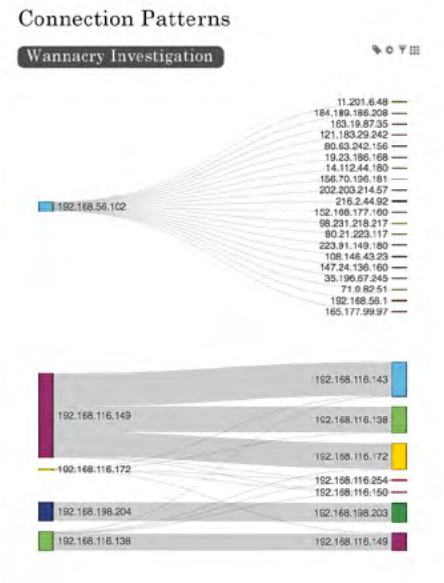
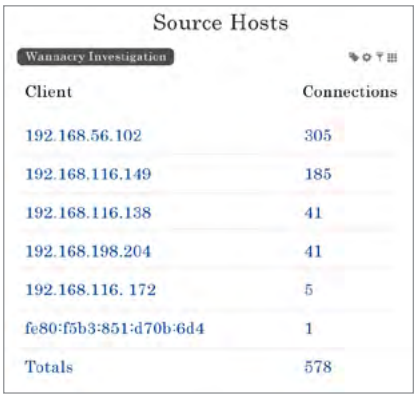


Figure 2:
Mapping All Infected Hosts and Their Attempted Spread

Looking back at the Overview screen in Figure 1, we also see a tabular list of all infected hosts for rapid remediation. We zoom in on this tile (Figure 3). With NIKSUN, all the information related to WannaCry and its attempts to spread are brought up immediately with just one click. The key to winning against such worms is to be able to fetch such lists (and many more obviously within more complex examples) quickly, even if they occurred in the past. By doing so, we can rapidly prune off these devices from the network and hence stop the WannaCry worm from spreading further. If we do not take this action, the worm could spread to thousands of hosts, making our remediation task impossible.


Source Hosts

Wannacry Investigation

Client	Connections
192.168.56.102	305
192.168.116.149	185
192.168.116.138	41
192.168.198.204	41
192.168.116. 172	5
fe80:f5b3:851:d70b:6d4	1
Totals	578

Figure 3
A Tabular List of All Infected Hosts

We can repeat this process iteratively until we ensure that no remaining malware is still on the system. After pruning the IPs listed off, we simply run the same search again to verify that no other devices with WannaCry still exist on this network. We can then work to block the ransomware completely from entering and then attempt to inoculate various hosts against this worm.

Next, let us look further to find out more specifics. We will now select the report "Application Forensics" in the NIKSUN list of prebuilt reports. Figure 4 shows this report; let us discuss how it allows us to further investigate the worm's behavior. In the tile titled "Application Sessions" (top left of Figure 4), we can see that the ransomware has attempted to reach out to a specific web address that NIKSUN analytics has pre-analyzed and reports to us that it does not exist (the words "Server Failure" at the end of the URL in green report this fact).

The WannaCry worm has the behavior that if this domain is registered, the worm will stop spreading, and if the domain is not registered, then it will continue to propagate. This allows anyone, including law enforcement, to register these websites in order to stop WannaCry from spreading. The point to note is that this discovery reported by NIKSUN's "breadcrumbs technology" allows a user to both know what WannaCry is trying to do and provides for further forensics on its behavior. We have effectively gone "back-in-time" to understand how this ransomware is programmed and how it is behaving at the time when the data traversed the network. Using this extra information, we can now protect our, and possibly other, networks from future attacks.

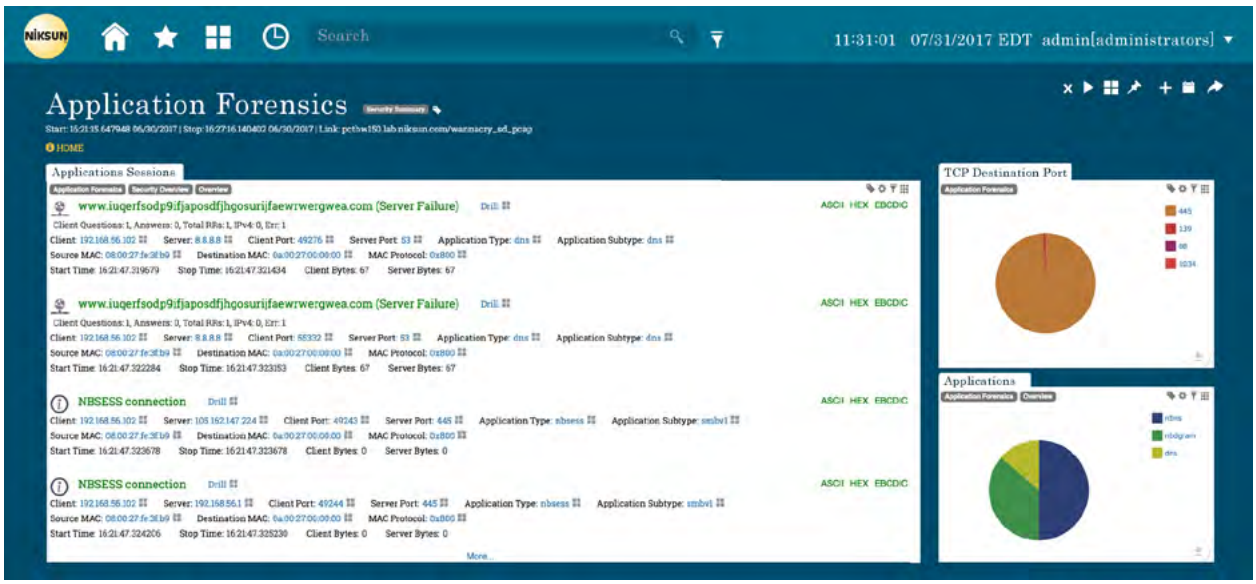


Figure 4
Finding WannaCry's Kill-Switch with NIKSUN Forensics

Investigating agencies can also be given a secure, audited and complete body of evidence that is necessary to identify and take action against the attacker. Just as it helped the U.S. Secret Service litigate against an international identity theft ring in the "largest investigation of its type," (niksun.com/basham/) NIKSUN analytics can be used to prosecute the perpetrators of worms like WannaCry and Petya in a court of law.

Proactive Alerting on WannaCry and Petya

Next, we would like to set up some proactive alerts so that we do not have to run a report retroactively if a similar attack occurs in the future. These alerts can be immediately messaged if any further activity takes place, rendering Petya nearly useless on this network. Further, automation can be leveraged to take action when such alerts are received. This automation, which NIKSUN has helped its customers configure, can be used to automatically prune such infected devices from the network, inoculate them (if possible) and then bring them back online, or archive them for further human analysis. A proactive enterprise could have actually set up this alert months before their network was attacked by WannaCry and Petya.

Figure 5 displays how this alarm would show up in this instance: every time an infected host tries to reach out, a critical alert would be displayed right at the NIKSUN Security screen (one click away from the NIKSUN GUI's main menu) for fast remediation.

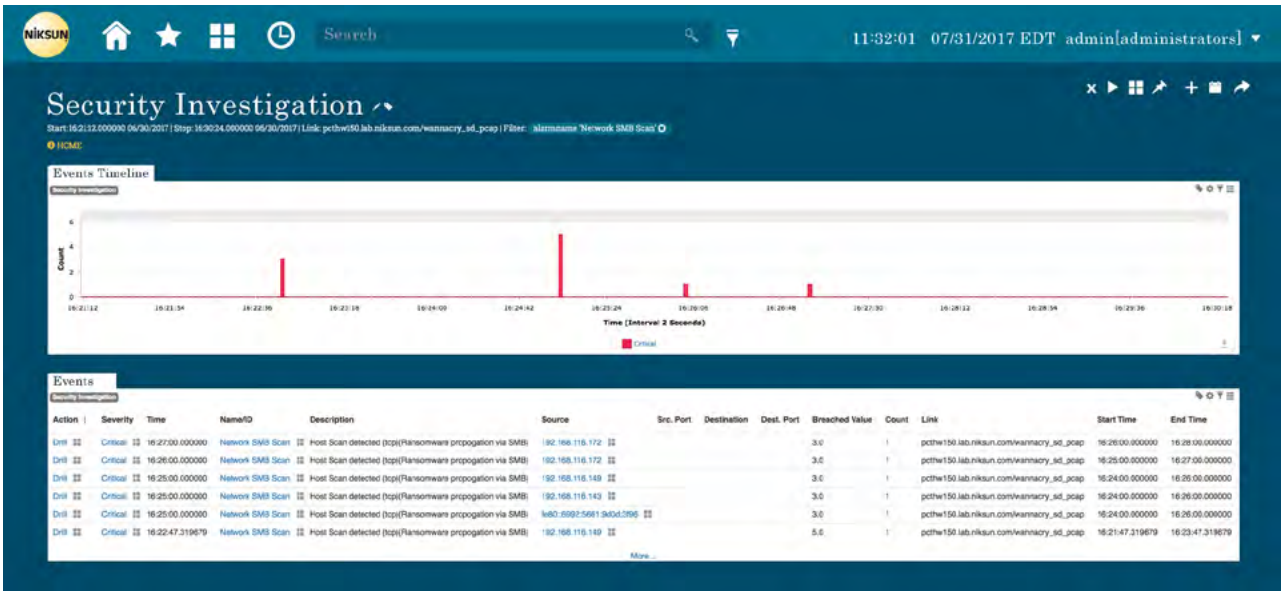


Figure 5
Real-Time Alerting on Worms like WannaCry and Petya

Alarms From Across the World

With NIKSUN's STIX and TAXII support, feeds from around the world can be pulled into NIKSUN's full-visibility detection software in order to rapidly report on all security incidents that are relevant to your network. This robust information-sharing feature keeps you up-to-date on the latest cyber threats and utilizes NIKSUN's zero-loss paradigm to make prevention possible.

Because of NIKSUN's highly robust framework, STIX and TAXII feeds within a NIKSUN device can immediately deliver a report of infected devices and allows for fast surface level analytics and granular deep-dive investigation of every known-exploit.

At the same time, NIKSUN's Full Packet Capture (FPC) solution means even unknown-exploits can be found and thus resolved. Just as a virus constantly evolves to render a medicine useless, cyber threats always develop to find a way around security perimeters. To break this cycle, you cannot solely rely upon targeted defenses but instead must be able to act in real-time on your network. Where targeted defenses can only stop threats we know, a holistic view of every potential entry point lets you stop even those threats that we don't know.

Total Visibility Into Both Physical and Virtual Networks

NIKSUN's solutions can be deployed across multiple physical and virtual servers and within a private or public cloud for complete monitoring across your infrastructure. It provides a total view of the both the physical and virtual world, including both north-south and east-west traffic. When it comes to worms, this is an absolutely critical feature that helps network administrators secure the entirety of one's network, not just a subset of it.

NIKSUN NetOmni provides a top-down holistic view of business service disruptions, performance issues, and security incidents. It offers a central location from which global network events can be responded to in real-time, making a worm like WannaCry stoppable as soon as it enters your network, from anywhere in the world, whether it be in your data center or in your machine instances in the cloud.

The entire suite of NIKSUN applications with NikOS Everest are now available on any smart device. Hence, busy security and network administrators, even if they are away from their desks or computers, can access the full NIKSUN solution suite from any smart device and can still find and resolve incidents in real-time.

Always Available, Even in Face of the Most Difficult Threats

By offering both local and external authorization and authentication, NIKSUN offers the convenience of integration while ensuring availability. That is, even if connectivity to the external server is lost during a network outage or ransomware attack, the users can still access the NIKSUN appliance. Just as a backup power generator is critical in ensuring that a business is able to run smoothly in extreme weather, this feature of NIKSUN's solution is necessary in keeping a network safe, and crucial data secure, under extreme cyber-threats. Had the network gone down during this WannaCry attack, for example, NIKSUN's appliance would still be recording everything just like an independent security camera on your network.

One-Click Audit Reports

NIKSUN's one-click audit report also allows an easy way for auditors to look at all the necessary information required to complete their security checks, drastically cutting down on time spent. The audit report can be setup with passwords and can be made available only to specific people with appropriate access rights, such as only key network administrators. The report contains information about system configuration settings, security policies, user and group permissions, external authentication settings, and more, giving you the information that makes protection from worms like WannaCry and Petya possible.

Robust Scalability

NIKSUN's solutions have been tested at an industry-leading traffic flow of 10 Tbps and working with 50 PB of data warehousing in one of the world's largest networks (the scaling limit of the technology is much larger though). It has passed the highly stringent testing of the U.S. Department of Defense (DoD) and is the chosen provider of full packet capture for the Defense Information Systems Agency (DISA). At the same time, the solution is highly scalable, allowing you to meet your network needs no matter what size it is without overpaying for bandwidth and storage you don't need. NIKSUN's suite is a "plug-and-play" solution that allows you to scale as your network does, ensuring that you are always fully protected. Such proven scalability is critical for you to ensure security even if the networks you are protecting grow significantly larger or more complex than you may have originally planned.

Summary of an Effective Solution

It should be clear from this discussion that any solution that can combat zero day attacks and worms like WannaCry and Petya must have the following key features:

- 100% visibility into physical and virtual networks through zero-loss Full Packet Capture technology that can keep up with your network speeds
- Real-time and simultaneous capture, inspection, indexing, correlation, storage, and search of all data for fast querying and mean-time-to-resolution
- Comprehensive, real-time threat detection that alerts on abnormal network behavior, immediately
- A top down holistic view of all network activity across multiple physical and virtual locations
- A deliverable, rapid report that finds all devices that were infected or may be scanned for hijacking tomorrow
- A complete record of any breach that tells the who, what, where, when and how, with the ability to see how ransomware or wipers got in - both retroactively and in real-time
- Event and actual transaction reconstruction up to the application layer to view applications, attachments, and downloads that let ransomware and wipers in
- Complete evidence of the ransomware or wiper that utilizes a "breadcrumbs" approach that could be used for prosecution in a court of law

[1] http://www.washingtontimes.com/news/2017/jul/19/fedex-warns-material-losses-cause-petya-computer-v/

[2] http://www.businessinsider.com/fedex-cyberattack-will-have-material-impact-on-full-year-results-2017-7

[3] http://www.telegraph.co.uk/business/2017/07/24/reckitt-benckiser-sales-take-knock-crippling-cyber-attack/

[4] http://buffalonews.com/2017/07/26/cost-ecmc-ransomware-incident-near-10-million/

[5] https://threatpost.com/windows-smb-zero-day-to-be-disclosed-during-def-con/126927/

NIKSUN
Corporate Headquarters
457 North Harrison Street
Princeton, NJ 08540
t: +1.609.936.9999
toll free: +1.888.504.3336
f: +1.609.419.4260
info@niksun.com

Massachusetts
8 Faneuil Hall Marketplace
3rd Floor
Boston, Massachusetts 02109

India
Vatika Business Centre
Vatika Business Park
Block Two, 1st Floor
Sector 49, Sohna Road
Gurgaon 122018, Haryana
t: +91.124.441.6999

Japan
Level 7, Wakamatsu Building 3-3-6
Nihonbashi Honcho, Chuo-ku
Tokyo 103-0023 Japan
sales_japan@niksun.com

Europe
sales_europe@niksun.com

Canada
sales_canada@niksun.com

Caribbean & Latin America
sales_cala@niksun.com

Middle East
sales_middle_east@niksun.com

APAC
sales_apac@niksun.com

About NIKSUN: *NIKSUN is the recognized worldwide leader in making the Unknown Known. The company develops a highly scalable array of real time and forensics-based cybersecurity and network performance management solutions for government & intelligence agencies, service providers, financial services companies, and large enterprises such as retailers and manufacturers. NIKSUN's award-winning appliances deliver unprecedented flexibility and packet capture power. The company's patented real-time analysis and recording technology is the industry's most comprehensive solution for secure and reliable network infrastructure and services. NIKSUN, headquartered in Princeton, New Jersey, has sales offices and distributors throughout the US, Europe, the Mid East and Asia-Pacific.*