It's not who's first…it's who puts the industry first

The healthcare industry has been hit with two significant and subsequent cyber challenges in recent weeks, (WannaCry and Petya) which caused business impact for several organizations and in both cases the damage was largely mitigated across the industry. This information is widely known; what is *not* widely known is what the role of information sharing was between private industry and the public sector specifically between the NH-ISAC Threat Intelligence Committee members (TIC) and the HHS Healthcare Cybersecurity Communications and Integration Center (HCCIC). In times of cyber crisis it is imperative for all enterprises to understand what the indicators of compromise (IOCs) are, how the malware works and spreads, and ultimately what controls are effective. These three steps appear to be simple but can be illusive without the right access to cyber communities that share resources and analysis. The HCCIC supported the emergency response team in the HHS Secretary's Operations Center (SOC) throughout both the WannaCry and Petya incidents. The HCCIC is how HHS carries out its cybersecurity responsibilities as directed in Presidential Policy Directive 41 and the National Cyber Incident Response Plan from the US Computer Emergency Readiness Team or US-CERT. The NH-ISAC is the primary interface from the private sector for the HCCIC to share information and respond in times of business resiliency crisis.

In both recent events (Wannacry and Petya) a number of supposedly industry subject matter experts (SMEs) shared misinformation (inaccurate information) that actually hurt the efforts of enterprises more than helped, which was problematic. There are several drivers for this phenomenon:

1. Being the first to understand how the malware works and how to potentially stop the spread of malware and then sharing this information provides name recognition and commercial benefit that appears to be the primary motivation in many cases
2. Malware analysis of sophisticated exploit code is technically challenging and takes time along with multiple samples
3. Both events included components of malware weaponized by some of the best technical minds and then modified by others that raised the degree of difficulty considerably

These are examples of early public announcements related to the two incidents that were inaccurate and therefore somewhat misleading for enterprises attempting to minimize the potential business impact for their respective enterprises:

- Endpoint News by Arsalan Arif (June 30th 2017 10:45 AM EDT) (endptscom) Claiming one firm neglected to patch their Windows devices [not accurate information and misleading]

- *"NotPetya malware was spread via drive-by exploit kits, e-mails with malicious attachments, embedded URI links"* [None of this is true]
- Many other intelligence briefings from specific security product companies followed this formula for information…
    - *We've studied the malware variants and understand the threat vectors…we recommend that you use all of our products to help mitigate this incident*

In each of the early samples of supposedly security intelligence, the threat vector was misunderstood and whatever malware analysis that these conclusions were based on were either incomplete or came from other sources. Therefore there was no real benefit for enterprises seeking to understand the most effective remediation approaches to consider since the threat vector was not clear. As a result enterprises relying on these early sources may allocate scarce technical resources to focus on protecting against the wrong threat vector. Each potential authoritative source that rushes to publish results or opinion shares information that does more damage to the industry than good. It's a simple case of trying to be first instead of trying to put the industry first. **In the case of Petya, having a privileged user with access to MeDoc *was* the threat vector used to impact the healthcare entities.**

Healthcare enterprises need to recognize that public sources of security intelligence is really helpful and easy to access but they can't be the only source in the event that the source is more interested in being first. Paying for security intelligence services is helpful but also not enough for a healthcare enterprise. Healthcare enterprises should do what banks do and join Information Sharing and Analysis Centers (ISACs) where relationships are established that help improve information sharing that pay big dividends in times of crisis.

Early information about WannaCry from multiple sources indicated the primary method of spreading the malware was through phishing emails (a reasonable assumption based on the majority of exploits in recent years) which was inaccurate. The NH-ISAC Threat Intelligence Committee members pooled engineering resources and obtained access to several different variants, reverse engineered the malware samples and shared information in real time with members using a chat feature. The conclusion that was verified was the method for spreading was Server Message Block (SMB) a commonly used MS Windows protocol for recognizing connected devices and printers on a network. The NH-ISAC TIC then confirmed the four controls necessary for preventing any business impact from a WannaCry infection and shared this information with all members, the HHS Healthcare Cybersecurity Communications and Integration Center (HCCIC), the Department of Homelands Security (DHS) and ultimately the healthcare sector. The NH- ISAC TIC members benefited from the opportunity to share really talented engineering resources, obtain accurate information on how the malware worked and spread in real time with the engineers with the ability to validate their understanding of the appropriate corrective actions with peers committed to putting the industry first. The latter is what makes the ISACs unique since commercial interests take a back seat to the industry needs. It also enables opportunities for health sector enterprises that don't have large cyber teams to benefit from learning from front line engineering resources which threat vectors to focus on resulting in a more thorough understanding of the actual event and the appropriate corrective actions.

The Petya attack impacted four healthcare organizations in the US as a result of the requirement by the Ukrainian government to use the MeDoc financial and tax accounting software and a software update process was used to spread the malware. Early reports from security intelligence firms, also covered in the press, suggested the threat vector was phishing email and exploitation of the SMB protocol. The malware analysis performed by the NH-ISAC TIC confirmed that the primary threat vector was access to MeDoc and had nothing to do with how well each of them performed their patch management process. The NH-ISAC TIC had direct access to malware samples from multiple firms impacted and the actual malware samples were immediately reverse engineered to confirm the threat vector. Cyber professionals from the impacted firms worked together with engineers from many firms to complete the malware analysis and compare results with actual experience with remediation and mitigation from those impacted organizations.

So patching systems is always good advice, in this case, it would have not prevented the infection. **Preventing infection of a privileged user using MeDoc represents the key control that applies in this specific case of Petya.** The NH-ISAC TIC was established to handle these types of security incidents working collaboratively with the HCCIC.

The two cyber security events have enabled the healthcare industry to learn techniques and methods for improving business resiliency. One of the most important learnings is the importance of being part of a community where security professionals can share information and engineering resources to put the industry first with no interest in being the first to report vulnerabilities for commercial or other purposes.

The table below contains a few examples of IOCs mistakenly attributed to NotPetya and widely shared by researchers and security vendors.

IOC	ACTUAL MALWARE
hxxp://185.165.29[.]78/~alex/svchost.exe	Karo Ransomware
415FE69BF32634CA98FA07633F4118E1	Andromeda/Gamarue phishing campaign (delivered Karo)
Order-20062017.doc	Andromeda/Gamarue phishing campaign (delivered Karo)
coffeinoffice[.]xyz	LokiBot C2
84.200.16[.]242/myguy.xls	Karo Dropper
french-cooking[.]com/myguy.exe	Karo Payload Dropper