Prepared Testimony of Salim Neino, Chief Executive Officer, Kryptos Logic

U.S. House of Representatives Committee on Science, Space & Technology, Joint Subcommittee on Oversight and Subcommittee on Research and Technology Hearing

15 June 2017

Chairman LaHood, Chairwoman Comstock, Ranking Member Beyer and Ranking Member Lipinski, thank you for the opportunity to appear before you today at this joint Subcommittee hearing. We greatly appreciate your interest in cybersecurity and look forward to sharing our thoughts and perspectives with you and your Members.

WannaCry Involvement and Response

On May 12th, 2017, Kryptos Logic identified a high-velocity, high-impact global security threat with the immediate potential to cause an immeasurable amount of damage. While the intent of this threat was unclear and its motives and origins ambiguous, it was immediately evident that its approach was unusually reckless. This threat has now popularly become known as ``WannaCry." It was at this time that Marcus Hutchins, Director of Threat Intelligence for Kryptos Logic's Vantage (our breach monitoring platform and feed) notified me of our team's active monitoring of the developing situation.

On this date at approximately 10:00 a.m. Eastern time, while investigating the code of WannaCry, we identified what looked like an anti-detection mechanism, which tested for the existence of a certain random-looking domain name. Our team proceeded to register the domain associated to this mechanism and directed it to one of the "sinkholes" controlled by and hosted on the Kryptos Logic network infrastructure. We then noticed and confirmed that the propagation of the WannaCry attack had come to a standstill because of what we refer to as its ``kill-switch" having been activated by our domain registration.

While our efforts effectively stopped the attack, and prevented WannaCry from continuing to deploy its ransom component (which irreversibly destroys important files) we knew that by then the attack had already propagated freely for hours, at minimum. Based on the velocity of the attack, estimated by sampling data we collected from our infrastructure currently blocking the attack, we believe had that anywhere between 1-2 million systems may have been affected in the hours prior to activating the kill-switch, contrary to the widely reported – and more conservative – estimate of 200,000 systems.

One month after registering the kill-switch domain, we have mitigated over 60 million infection attempts – approximately 7 million in the United States – and we estimate that these could have impacted a minimum 10-15 million unique systems. I will note that the largest attack we thwarted and measured to date from WannaCry was not on May 12 or 13th when the attack started, but began suddenly on June 8th and 9th on a well-funded hospital in the east coast of the United States. It is very likely the health system is still unaware of the event. We measured approximately 275,000 thwarted infection attempts within a 2-day period. Another hospital was hit on May 30th, in another part of the country. A high-school in the Midwest was just hit beginning on June 9th.

Presumably every system at this location would have had its data held hostage if not for Kryptos Logic's kill-switch.

Moreover, Kryptos Logic has been under constant attack by unidentified attackers attempting to knock our systems offline, thus disabling the kill-switch and further propagating the attack. The earlier of these attacks came by the well-known Mirai botnet which took down large portions of the United Kingdom, Germany and part of the east coast of the United States earlier this year. Despite these attempts, our systems remained resilient and we increased counter-intelligence measures to mitigate the amplitude of the attacks against us.

Observations and Thoughts Regarding Cybersecurity Response and Policy

We believe the success of WannaCry illustrates two key facts about our nation's systems:

- Vulnerabilities exist at virtually every level of our computer infrastructure, ranging from operating systems to browsers, from media players to Internet routers;
- Exploiting and weaponizing such vulnerabilities has a surprisingly low entry barrier: anyone can join in, including rogue teenagers, nation states, and everyone in-between.

So, how do we adapt and overcome/mitigate these weaknesses? While many cybersecurity experts who have come before me offer the usual gloomy “there are no silver bullets,” I have had the opportunity to play on both fronts; on offense, via penetration testing and competitive hacking (including winning Defcon CTF, a kinetic and defense based hacking tournament) and on defense, providing protection to Global 100 organizations with very high enterprise risks.

Our attack responses must be more agile and with higher velocity and intensity. While the nation has considerable literature on risk, maturity models and various frameworks, the actual resources for cyberdefense (execution) are scarce as there simply is not presently an adequate level of highly skilled, highly experienced, and highly available operators in the cybersecurity field. While there is no shortage of “ideas” which claim to be able to solve an infinite amount of problems, each and every subsequent idea needs development, support, testing, maintenance, etc. – all of which we characterize as “developer debt.” Unfortunately, many of these solutions take too long to procure and end up being outdated - and essentially useless - before the ink dries on the paper it is written on.

I am optimistic, however, that there is a successful path and strategy forward. Application and software level mitigations which protect against the exploitation techniques used by hackers have moved the needle to protect against exploitation of the very fabric on which we build our defense assumptions. Mitigations, albeit incomplete, are nonetheless effective, and have increased the cost of identifying vulnerabilities in systems and developing programs to exploit them. Other mitigations include various design approaches like compartmentalization of data, systems, and transmissions. Such mitigations have measurably raised the bar required for mass exploitation in critical communications software like Internet browsers, web servers, and other protocols which are fundamental to business continuity.

As assessing risk is the bane of security, what actually is effective?

Investing in technology doesn't necessarily guarantee any actual improvement; in fact, one could argue that introducing more technology stack exacerbates maintenance debt and creates immediate monetary loss because there are few metrics or analytics to actually measure the effectiveness of any particular technology. This is because we are typically years behind attackers in terms of the "sword/shield battle." As these resources ebb and flow, "knowledge gaps" are created, e.g., the loss of a domain knowledge specialist who cannot be immediately replaced.

We also must be less risk averse in terms of the defensive operations we undertake, more open to failure and ready to adapt and learn from these failures. We need a stronger focus on threat modeling and "fire drill" simulations that will be focused on the events of a magnitude which could cause significant damage. A significant response failure with the WannaCry incident was that there was no real guidance or course of action that was well communicated; the media focused on the points contrary to defense (who did it?), and this incident could have resulted in a complete breakdown of processes had this been an unpatched "zero-day" vulnerability and there was no luxury of a "kill-switch".

The largest success, though incomplete, was the ability for the FBI and NCSC of the United Kingdom to aggregate and disseminate the information Kryptos Logic provided so that affected organizations could respond. Information sharing can be valuable but our framework can be vastly improved by triaging cybersecurity threats and events of magnitude in a clear and repeatable scale, not dissimilar to the Richter scale, which measures the energy released in an earthquake. Likewise, a scale that takes the technical and social elements of a threat into account to evaluate its destructive power enables first responders – us – to better organize and mobilize focus on the most important areas of risk.

While there do exist various scoring systems for evaluating the purely technical element of a threat, they fall short in terms of clear and actionable information outside of information technology. We focus too much on application specific vulnerabilities with abstruse names like MS17-010, and none of these values are effective in quantifying the overall impact potential on a wider global environment. We need an easier to grasp method of prioritizing threats that have a large scale destructive potential in context, like WannaCry. To this end, once we have determined a method to evaluate attacks with respect to the aforementioned technical and contextual specifics, we may then place efforts on the simulation of these high-risk cases against our networks and further develop better communication methods, courses of action, and of course preempt these attacks with improved resiliency given the new awareness of these risks and their appropriate mitigations.

In conclusion, one of the largest issues is the transitory nature of a crisis. The message still has not resonated of the destructive potential of these attacks and the importance of its awareness. We think this can be explained simply by the fact their organizations are too slow to adapt to such a volatile landscape, there is a vast human resource shortage, and little by way of metrics to demonstrate return on investment in defensive technologies.

Again, I thank the Subcommittee for inviting me to appear before you today to discuss Kryptos Logic's involvement in lessons learned for WannaCry, and I welcome the opportunity to answer any questions you may have.