SimulationDeck®
PATENT PENDING

CASE STUDY

ANALYZING THE INFORMATION ENVIRONMENT DURING A CYBER-ATTACK: LESSONS LEARNED FROM #PETYA/NOTPETYA

CHALLENGE

Nusura wanted to better understand the role played by social media, traditional news media and other open source information during the global Petya/NotPetya cyber-attack. According to a Reuters article published by Fortune Tech., the Petya/NotPetya cyber-attack that began on June 27, 2017 infected thousands of computers in dozens of countries with file erasing malware. Initially mistaken for Petya ransomware, the virus first infected computer systems in Ukraine where it locked computer files in infected systems and displayed a ransom message demanding $300 in Bitcoin.

Four hours into the attack, Kapersky Labs tweeted that the virus was actually a destructive wiperware that permanently deleted files with no options for restoration. Over the course of nearly three days the attack affected major corporations across industries including shipping giant Maersk and WPP, the world's largest advertising agency. The global economic impact was immense, costing $850 million worldwide according to Reuters.

During the attack and in the days that followed, Nusura noticed that social media played a key role in providing information about the progression of the virus and corporate response actions. For example, Kapersky Labs, an internet security giant, broke the news of Petya/NotPetya on Twitter, providing initial updates about countries affected and alleging that the ransomware was an enhanced strain of Petya.

According to an article by The Register, an online UK publication, Janus Cybercrime Solutions, the hacking group responsible for creating the original Petya Virus later also used Twitter to confirm that this new ransomware was not a version Petya.

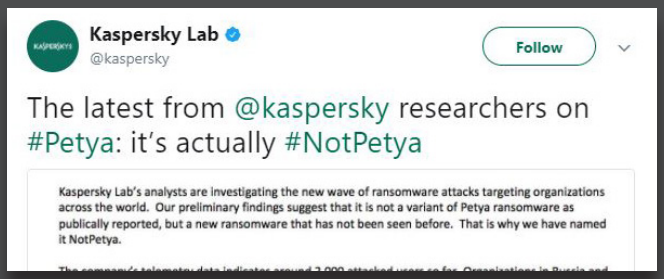
Nusura social media analysts and cyber security experts needed a way to capture, re-create and replay the event in order to better study the relevant social media posts and other open source data.

IN BRIEF

CHALLENGE: Nusura wanted to learn more about the role of Social media during the Petya/NotPetya cyber-attack.

APPROACH: Nusura's team of cyber and social media subject matter experts used SimulationDeck to build a time-lapsed simulation of the information environment.

RESULTS: The information environment provides a lense through which government agencies and corporations can monitor the progression and effects of a cyber-attack. Organizations need to integrate cyber-attack preparedness into emergency response and communications plans, and training and exercise programs.



Kapersky Labs broke the news of Petya/NotPetya on Twitter, providing initial updates about countries affected and alleging that the ransomware was an enhanced strain of Petya.

Janus Cybercrime Solutions also used Twitter to confirm that this new ransomware was not a version Petya.

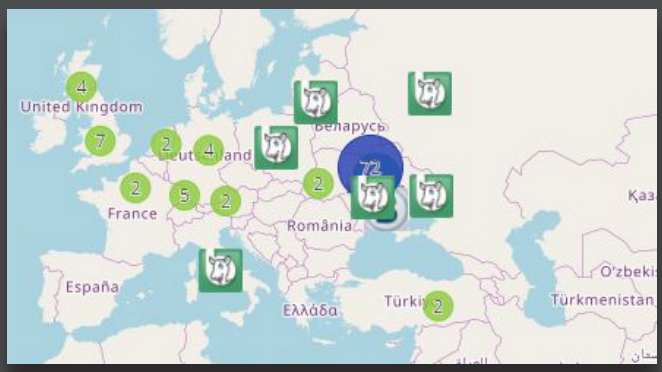
POWERED BY nusura Experience Innovation

SimulationDeck is a training and exercise delivery platform that simulates the information environment, helping teams validate plans and practice responding to crises in a realistic setting.

APPROACH

The team used Nusura's proprietary training and exercise delivery tool, SimulationDeck, to create a microcosm of the information environment related to the Petya/ NotPetya cyber-attack. First, Nusura captured hundreds of key social media posts, news stories, website articles, text and video blogs, and TV news broadcasts related to the attack.

The team then uploaded these real-world sources from the information environment into SimulationDeck's social media and website simulators, turning a three-day cyber-attack into a four-hour simulation.[1] The team also used metadata from real-world social media posts to geo-locate representative posts on SimulationDeck's social media mapping tool, GeoDeck.



GeoDeck is a geo-location tool on SimulationDeck that allows users to emulate geo-tagging social media posts and analyze where social media activity occurs during an incident.

Using this time-lapsed simulation, Nusura subject matter experts studied the progression of the attack by monitoring the geo-locations where social media posts first begin to appear and analyzing where and how they spread. The team also evaluated the impact of corporate and government messaging, journalist coverage and public conversations as they unfolded over social media, corporate websites, news stations and other internet sites.

RESULTS

The information environment provides a lens through which to evaluate the progression and effects of a cyber-attack. In the same way that social media provides emergency responders with information about the progression and effects of a hurricane or other natural disaster, social media can also provide situational awareness for organizations monitoring the progression and effects of a cyber-attack. For example, many affected organizations like Maersk and Posteo used social media to update

[1] Personally identifiable information (PII) was removed from social media posts from members of the public.

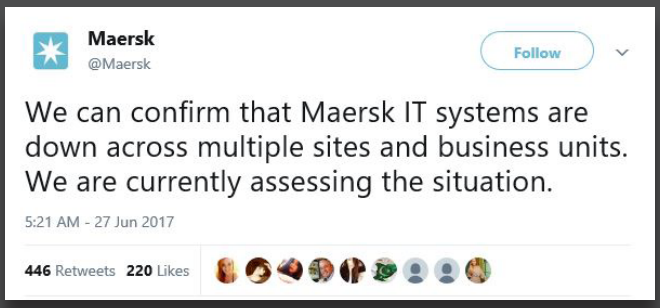
employees, customers and other stakeholders about the impacts of the attack and protective actions the organizations were taking. In another example, social media was used by the press to share a photo from an anonymous source after DLA Piper was impacted.

While the information environment can provide tremendous situational awareness and help inform better decision-making, without a plan and operating procedures for effectively gathering and leveraging the hundreds of thousands of data points, it can be impossible to navigate effectively.

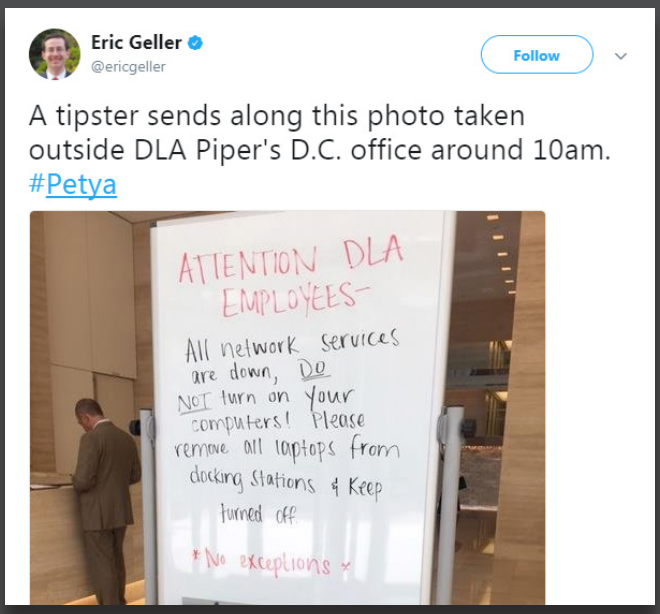
The information environment during and after reports of the Petya/NotPetya cyber-attack surfaced was overwhelming and convoluted. Volumes of social media posts covered a wide range of themes including concerns from affected companies, proposed fixes for the corrupted files, and speculation about whether or not the virus was actually ransomware. There were also multiple groupings of information and followers. On Twitter, for example, posts including the #Petya/NotPetya hashtag contained one set information, while the @Petya_Payments account had its own set of followers and posts that at times conflicted with information being shared by #Petya/NotPetya hashtag users.

Cyberspace is the new theater of war. Preparedness and practice is critical. Organizations need cyber-attack response plans that include protocols for leveraging the information environment both as an intelligence gathering and decision making tool, and as a communications platform. Plans must be validated and teams trained to execute the plans proficiently in order to promote organizational resiliency.

Social media and the increasingly important role played by the information environment is changing the way organizations understand and respond to emergencies and crises of all kinds. As the information environment continues to evolve, teams must be well prepared and practiced at engaging with this dynamic digital ecosystem in order to successfully confront and manage future crises.



Maersk used social media to update employees, customers and other stakeholders about the impacts of the attack and protective actions the organizations were taking.



Social media was used by the press to share a photo from an anonymous source after DLA Piper was impacted.

@Petya_Payments was a Twitter handle created to report payments made to the hackers' bitcoin wallet. As cyber security experts revealed that NotPetya was malware, social media users used the @Petya_Payments handle to help warn affected organizations to avoid paying the ransom.