Understanding A Cyber Attack

Goals for Today's Discussion

- Demonstration of how being globally interconnected poses risks
- High-level engineering analysis of the Petya attack
- Possible prevention
  - System infection
  - Propagation of Petya

Background and Pre-Attack Timeline of Events

Approximately 3 to 4 months before the attack

- An update to MeDoc* was used to deploy Petya.

March 14, 2017

- Microsoft releases security bulletin MS17-010 notifying the public of a patch for a vulnerability found in the Server Message Block (SMB) Protocol. SMB allows files to be shared across networks.

April, 2017

- The Shadow Brokers publish EternalBlue. EternalBlue is the name given to the malware that “exploits” the SMB Protocol vulnerability.

May 12, 2017

- WannaCry ransomware cyber attack impacts 230,000 computers in 150 countries. WannaCry encrypted a computer’s files and demanded ransom payments using Bitcoin Currency.

MeDoc is a financial and accounting software application used by the Ukrainian government and companies doing business with the Ukrainian government.

Petya Cyber Attack Analysis

June 27

- National Bank of Ukraine
- Ukraine utility companies
- Government ministries
- Chernobyl radiation monitoring system
- Other businesses in Ukraine

- Initial attack disguised itself as ransomware requiring a US $300 Bitcoin payment
- Cybersecurity analyst noted similarity to May 2017 WannaCry attack
- Discovered to be much more lethal and designed to destroy files

Petya Cyber Attack Analysis

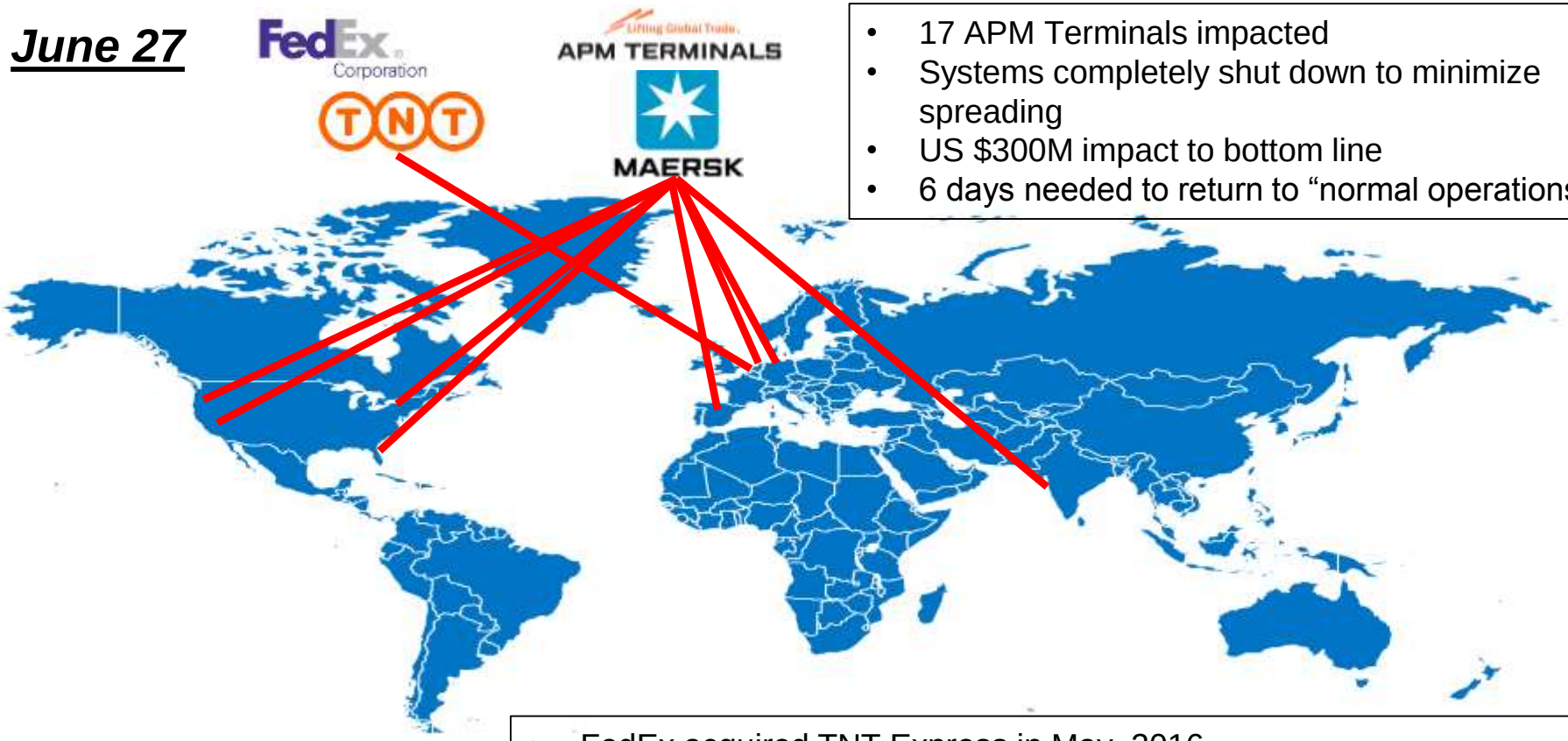
June 27 5:45pm

- Merck's office in Ukraine impacted by the attack
- Spread to Headquarters in New Jersey
- Impacted Heritage Health System in Pennsylvania

- Russia was the second most impacted country
- Rosneft reported no stop in oil production
- Evraz reported no impact to steel output
- Home Credit consumer lender closed

Petya Cyber Attack Analysis

June 27



- 17 APM Terminals impacted
- Systems completely shut down to minimize spreading
- US $300M impact to bottom line
- 6 days needed to return to “normal operations”

- FedEx acquired TNT Express in May, 2016
- 4% to 7% reduction in FedEx earnings directly related to Petya attack
- FedEx/TNT Express did not have cyber insurance
- Wide spread delays; orders were handwritten
- FedEx was also attacked during the WannaCry attack

Engineering and Technical Lessons

- Patching ALL your computers, servers, and network appliances is critical to protecting your organizational network.
- Not all attacks can prevent your systems from being attacked or breached, but keeping your systems patched increases your security posture.
- Limit user access to system administrator tools.
- Develop an incident response plan if you are attacked and breached by malware.
- Create plans to ensure your computers and other systems meet strict engineering configuration management compliance requirements.
- Supply Chain Risk Management (SCRM) and interconnectivity to your IT infrastructure are critical risk management components.

Engineering and Technical Lessons

90% of maritime companies spent less than 10% of their IT budget on cybersecurity and resilience, 70% spent under 10% of their budget, and 10% spent nothing at all

- Futurenautics

Only 37% of organizations have a cybersecurity response plan

- DVN GL

43% of seafarers have reported sailing on a vessel that became infected with a virus or malware

- Futurenautics

Human errors account for 52% of the root cause of security breaches

- CompTIA

37% of Microsoft servers on ships are vulnerable to hacking due to not applying available software patches

- Network World

About 99% of all cybersecurity breaches are from known vulnerabilities and 90% of these breaches have available patches

- ESC Global Security

Organizations should use automated patch management tools to expedite the distribution of patches to systems

- NIST

Nearly 80% of stakeholders do not consider the shipping industry safe and secure from cyber risk

- Safety4Sea

Up to 70% of cyber attacks go undetected

- GovTech

Questions?

Contact Information

Points of Contact

James Espino, President
james.espino@gnostech.com

Sarah Carter, Vice President
sarah.carter@gnostech.com

Theresa DeSantis, Corporate Development
theresa.desantis@gnostech.com

Headquarters

650 Louis Drive, Suite 190
Warminster, PA 18974
215-443-8660

2468 Historic Decatur Road, Suite 230
San Diego, CA 92106
619-220-0896

Stay Connected with Gnostech


www.gnostech.com


www.twitter.com/gnostechinc


www.linkedin.com/company/gnostech-inc