IBM Security

# Perspective on the Recent "Petya" Cyberattacks

**What is the Petya Ransomware campaign?** A calculated ransomware campaign with a heavy footprint in Ukraine was detected on June 27, 2017. The source of the attack is currently unknown. To date, the attack has affected global organizations in the banking, pharmaceutical and transportation industries.

Most reports, and the ransom demand itself, refer to the activity as Petya, a well-known malware that has existed for quite some time, but at least one security company believes it is not a true Petya variant. IBM can confirm the ransomware tool is spreading via the National Security Agency (NSA) exploit ETERNALBLUE, similar to the WannaCry events last month.

While this attack is not identical to WannaCry, it is operating in a similar fashion—mainly an existing ransomware tool has been updated with a new infection capability, allowing it to propagate very quickly, with potentially significant impact. IBM believes the response and remediation steps that led to effectively responding to WannaCry are highly applicable to today's attack. IBM X-Force Command Center is fully activated to determine true cause, provide recommendations, and work responses with our clients.

**Broad implications:** Organizations around the world need to understand the elements of these attacks and be prepared for copycat attacks with new twists. While ransomware – the criminal practice of stealing data and not returning it to its owner until a ransom payment is made – was the profit-gaining tactic of choice, criminals could shift to new tactics and schemes in the future. For example, they could use the one-to-many attack scheme through the Microsoft vulnerability to steal personally identifiable information or embed Remote Access Trojans.

**Actions for all enterprises:** Take steps to prevent such attacks, or to get help

- **Patch systems immediately to help prevent attacks.** For example, IBM's BigFix solution automatically deployed the patch for WannaCry2 in May 2017.
- **Deploy Security Intelligence systems to detect attacks,** such as Watson for Cyber Security.
- **Develop a response playbook with your team**, in case you are infected.
- **Refer to X-Force Ransomware Response Guide** to evaluate organizational readiness

- **Ensure your employees, suppliers and others who work with your company receive regular security training,** such as how to spot suspicious emails.
- Follow the updates on **X-Force Exchange** and SecurityIntelligence.com
- If you have been impacted by the Petya attacks, call IBM X-Force Incident Response Hotline: 1-888-241-9812 US, (001) 312-212-8034 Outside the US