IBM Security

Perspective on the Global "WannaCry2" Cyberattacks Hitting Critical Infrastructure

What is WannaCry2? A rapidly spreading cyberattack that was first detected in March and has impacted businesses in nearly 100 countries. Currently, the source of the attack is unknown. The WannaCry2 attacks have crippled critical infrastructure, including hospitals, telecommunications and distribution/supply chain services.

The scale of this attack was possible because of a vulnerability in the Microsoft Windows Operating System. Although it began like any routine phishing scheme – in which a user clicks on a bad link and malware takes over – WannaCry2's exploitation of the Windows vulnerability enabled it to spread with great speed from one workstation to a network of users. As a result, it was an attack of one-to-many versus standard phishing attacks, which typically infect one user at a time. While the attack appears disabled now, we expect hackers to reanimate it rapidly, and organizations need to prepare fast.

Broad implications: The implications of the design of this one-to-many attack are profound. 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.

Impact on IBM Security clients: When the Windows vulnerability was detected in March, IBM X-Force security researchers helped to ensure that IBM Security clients were protected. Those using IBM's BigFix security patching or QRadar Network protection technologies were better protected. At the same time, Watson for Cyber Security analyzed alerts on the attack and fed data to our customers and our Managed Security Operations Centers.

Protective actions for all enterprises: Take steps to prevent such attacks, or to get help now:

- **Patch systems immediately to prevent attacks.** For example, IBM's BigFix solution automatically deployed the patch for WannaCry2 several weeks ago.
- **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.
- **Ensure your employees, suppliers and others who work with your company receive regular security training,** such as how to spot suspicious emails.
- **Refer to X-Force Ransomware Response Guide** to evaluate organizational readiness
- **Follow the updates on X-Force Exchange and SecurityIntelligence.com**
- **If you have been impacted by the WannaCry2 attacks, call IBM X-Force Incident Response Hotline:** 1-888-241-9812 US, (001) 312-212-8034 Outside the US