Cyber Security Community Update

May 2017

Greetings! There has been a significant increase in cyber attacks. The recent spate of ransomware incidents have left organisations and individuals across the globe feeling **targeted and vulnerable.**

The cybersecurity team at Wolfpack have compiled a **list of great articles** and a **short opinion piece** to equip the community to be better prepared for the next round of attacks - which may take on different attack vectors to what we expect.

Yours securely
The Wolfpack Team

In This Edition:

Ransomware News Updates

1. Start here **- A simple "layman" article and video** on WannaCry & ransomware **- Link to CNNTech**

2. A detailed semi-technical & incident response explanation **on WannaCry & ransomware - Link to troyhunt.com**

3. Related Attacks:

a. AdylKuzz **- A similiar type of malware** but instead of encrypting your device it **"parasites" your resources for cryptocurrency mining - Link to gigamon.com**

b. EternalRocks **- Dubbed "WannaCry 2.0" with 5 additional NSA exploits** the worm installs **Tor,** lays low for **24 hours** & then begins comms with the **command & control server - Link to cnet.com**

4. WHAT'S NEXT?

a. Critical infrastructure sectors *such as* ***banks, airports, telecom networks and stock markets*** *have been asked to take precautions to shield themselves against crippling global ransomware attacks* ***- Link to publicintelligence.net***

b. Implantable medical devices are largely vulnerable to attack. *One study solely on* ***pacemakers*** *found more than* ***8,000 known vulnerabilities*** *in code inside cardiac devices* ***- Link to bbc.co.uk***

c. Your home could be held ransom. Avast has sent out a warning of cyber criminals who may target home appliances such as Smart TVs or home automation systems **- Link to fin24.com**

Wolfpack Opinion Piece

Following the Wannacry incident, we felt it necessary to provide guidance to manage ransomware attacks in future. Edwin our IT Security Operations Officer elaborates below.


Edwin Mpofu
IT Security Operations Officer

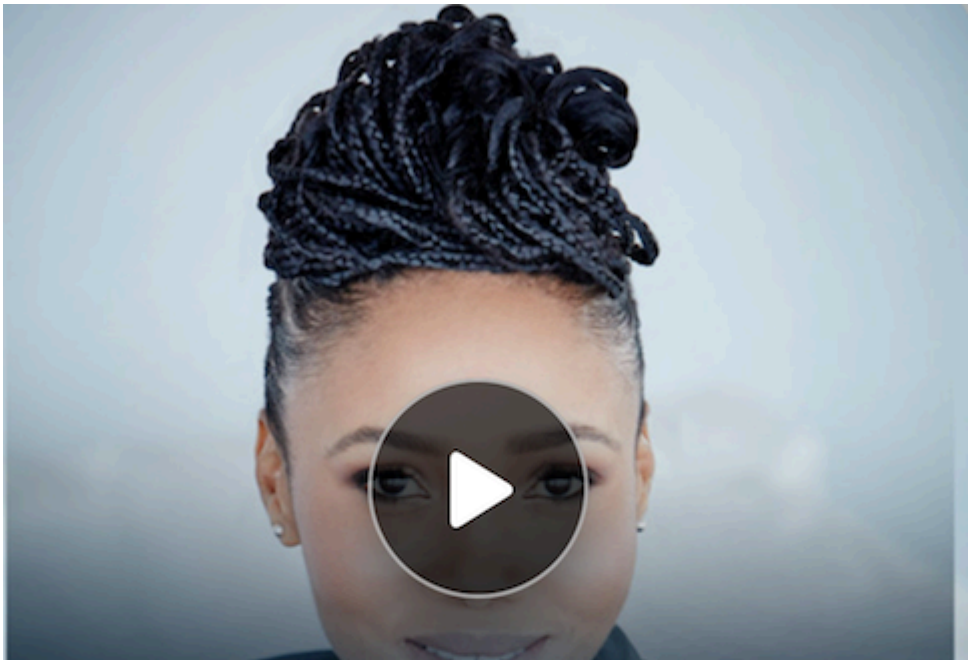
Most ransomware attacks follow a typical mode of operation:

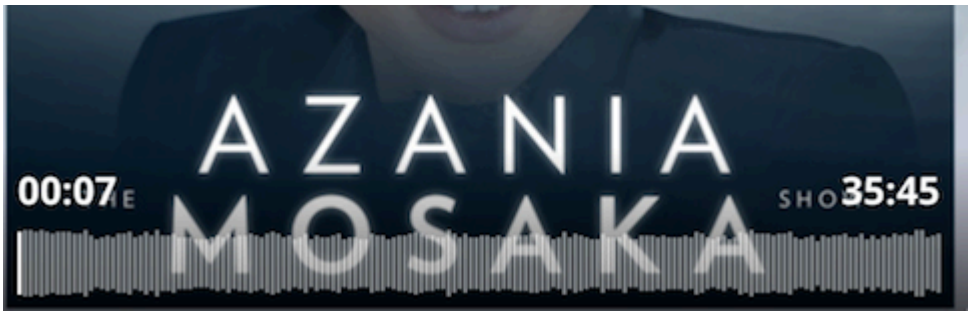
1. Researching and identification of targets
2. Delivery of the initial exploit file through the appropriate infection vector
3. Once the initial exploit file establishes persistence, a call is made to the command and control server to download the actual ransomware
4. Cryptographic parameters are set up and then the encryption of files begin
5. Once encryption is complete, a ransom demand is made

To download a short guide (**without the vendor pitch**) that explains the steps to prevent and recover from a ransomware attack **click here**

Wolfpack In the News

Craig Rosewarne recently ran a 35 minute **masterclass on hacking and cyber security** with Azania Mosaka on **702 talk radio** station. The talk covered a range of topics on cybercrime and scams aimed at both companies and individuals - with a **live demo** on how perpetrators are now **using telephone number spoofing** techniques to trick their victims into paying money over.





Wolfpack Training

1. ISO27001 Foundation (12 – 13 June)

- This course enables the participants to learn about the basics of best practices for implementing and managing an Information Security Management System (ISMS) as specified in ISO/IEC 27001, as well as the best practices for implementing the information security controls based on ISO/IEC 27002.

3. ISO27001 Lead Implementer (10 – 14 July)

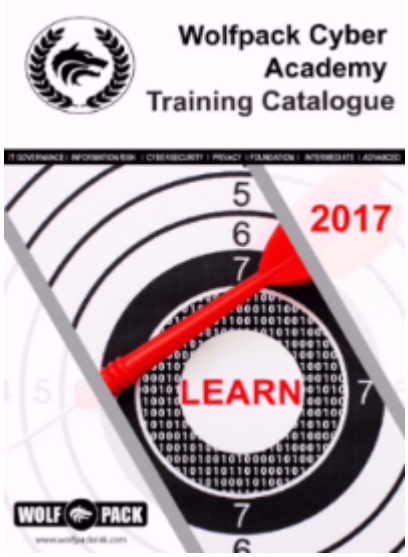
- This five-day intensive course enables participants to develop the expertise necessary to support an organisation in implementing and managing an Information Security Management System (ISMS) based on ISO/IEC 27001. Participants will also be given a thorough grounding in best practices used to implement information security controls from all areas of ISO/IEC 27002.

2. ISO27005 IT Risk Foundation (26 – 27 June)

- This course enables participants to learn about the best practices in risk management based on ISO/IEC 27005, as well as understanding how different parts of a risk management programme and the implementation stages of an optimal risk assessment are conducted.

For more information please email: **academy@wolfpackrisk.com**

PS - Enquire about our tailored Incident management training programme.



Click here to download our training catalogue

Event of Interest

SecureJohannesburg 2017 Conference

Wolfpack are a proud media partner of the (ISC)² SecureJohannesburg 2017 conference.

This one day conference will address the most significant technical trends which influence companies today. Leaders and professionals will be present and the conference will end with an interactive panel discussion. You will have the opportunity to meet likeminded professionals, discuss and exchange ideas, and better your understanding of how to identify, approach, and address security challenges which threaten present business progress.

Date: 05 October 2017

Venue: KPMG Wanooka Place, Johannesburg

For more information **click here**

Please use the following code for **15% discount - ISC2WolfpackSJ2017**

Job Vacancies

CSIR
our future through science

Senior Information Security Specialist

Job purpose: The incumbent will be responsible for coordinating, implementing and maintaining information security technologies, standards, procedures and processes required to ensure that the CSIR has adequate information security operations controls. In addition, the specialist will ensure that the controls are regularly measured and monitored for effectiveness. This position is based in Pretoria.

Experience: 8 years IT & 5 years IS experience

Qualifications: A Bachelor's degree in Information technology / systems, computer science, computer / electronic engineering or related field

To download a detailed job spec visit - Senior IS Specialist

Information Security Specialist

Job purpose: The CSIR has a vacancy for an Information Security Specialist who will support the operations of the information security management system within the Information Security Office. The incumbent will also be responsible for developing and driving information security training and awareness initiatives as well as managing all communication avenues. This position is based at Pretoria.

Experience: 7 years IT & 4 years IS experience

Qualifications: A Bachelor's degree in Information technology / systems, computer science, computer/ electronic engineering or related field

To download a detailed job spec visit - IS Specialist

Information Security Governance, Risk and Compliance Specialist

Job purpose: The incumbent will direct, develop, implement and maintain a comprehensive CSIR-wide information security governance, risk and compliance (GRC) strategy. This position is based in Pretoria.

Experience: 10 years information technology experience, of which 6 years must be in information security & 3 years in information security governance, risk and compliance

Qualifications: A Bachelor's degree in information technology / systems, computer science, computer / electronic engineering or related field

To download a detailed job spec visit - IS GRC Specialist