Journal of Forensic Sciences
And
Criminal Investigation
ISSN: 2476-1311

Juniper
PUBLISHERS
key to the Researchers

Short Communication
Volume-5 Issue 2 - September 2017
DOI: 10.19080/JFSCI.2017.05.555663

J Forensic Sci & Criminal Inves

Does your Cyber Security make you WannaCry?

Laurie Pieters-James*

Director, Criminologist, Forensic Profiler, Africa

Submission: September 23, 2017; **Published:** September 25, 2017

***Corresponding author:** Laurie Pieters-James, Director, Criminologist, Forensic Profiler, Africa, Tel: 267 74 022 511; Email: laurie@expert-profiling.com

Short Communication

Gone are the days when you could rely on simple firewalls and basic antivirus software. Targeted attacks and socially engineered malware may enter your insufficiently secured networks through various platforms and result in many devastating outcomes - including your data being encrypted and you being held to ransom, (WannaCry being a recent example). Ransom ware is widely considered as the number one threat today, but don't kid yourself there are new, sophisticated threats being developed daily by determined cyber criminals whose sole goal is finding ingenious ways to exploit you for gain. Is your company or organization presently equipped to deal with an attack of this nature?

So what does the cyber threat landscape look like today? What are the latest trends?

a) 325 000 new malicious files are detected by Kaspersky every day.

b) There is an increase in targeted attacks and malware campaigns.

c) There is continued exploitation of the vulnerabilities of third party software. I.e. your programs like Adobe Reader.

d) There is a dramatic increase in Ransom ware.

e) There is exponential growth in mobile malware.

And for those of you who think that you are safe using Mac, there is significant increased threat to Macintosh machines. Facebook is the most widely used social media platform in Botswana today and can be a fabulous tool for socialising and for business. For this reason, it is frequently targeted by hackers. The drawback of having many Facebook friends is that you basically act as a honey pot when your friends click on malicious things.

According to Kaspersky, new malware is spreading via Facebook Messenger, and involves multi-platform malware/adware, using loads of domains to prevent tracking, and earning clicks. The code is advanced and complicated. Be careful if someone who infrequently contacts you suddenly sends you a message. The initial spreading mechanism seems to be Facebook Messenger, but how it actually spreads is still unknown. It may be from stolen credentials, hijacked browsers or click jacking. Presently, research is ongoing. The message you receive uses good old-fashioned social engineering to trick the you into clicking a link. The message contains the text "David Video" and then a bit.ly link. DON'T CLICK the link and update your antivirus frequently.

Organizations are increasingly using more advanced ICT technologies, constantly looking to improve productivity and implement cost saving technologies. Internet IT sophistication results in a visibility gap and a lack of operational information. As a result, an average major attack commonly goes undetected for 214 days before discovery. Can you imagine the damage that a hacker can inflict, or the amount of data that can be stolen during this time? Because of this cyber-attacks are becoming more frequent and sophisticated and hackers are increasingly turning to social engineering, enticing people to do their dirty work through some very clever techniques such as spear fishing. No matter how advanced your tech, in order to combat cyber threat effectively companies need to consider the human factor. Humans are always going to be the weakest link in the chain.

People are vulnerable to exploitation. They can be tricked, threatened, coerced, recruited, influenced, or paid into aiding or abetting cyber-crime. It is therefore critical for all companies to train EVERY PC user with reference to basic cyber awareness. Instilling and reinforcing cybercrime awareness through training and corporate culture is an essential tool in preventing cybercrime. African Cyber have developed an extensive range of specialist cyber related BQA accredited courses for exactly this reason. We will be addressing the issue at the 3rd Annual Cyber Crime Conference 2017, enabling attendees to glean a deeper understanding of internal threat and the "Human Hack".

Through the consulting that we do, we have learned that the risks companies think they face, are often very different from the threats that can cause them the most damage. Complex and expensive state of the art encryption and intrusion detection systems are often sought, where what is really needed is greater cyber insight at board level, stronger policy, frequent patching of software and most importantly end user education. A proactive rather than a reactive approach is always beneficial. For readers who think Botswana is exempt from cyber-attacks, you may be shocked to learn that, at the time of writing on Friday afternoon at 15h04.45, Kaspersky's real time cyber threat map was indicating that Botswana was experiencing 20129 attacks, a rather concerning statistic. As Internet speeds increase so will the frequency of successful attacks. The time has passed where the business, government and organizations in Botswana can bury their heads in the sand and pray they are not the next target.

African Cyber Security are organizing their 3rd Annual Cyber Crime Conference. The sole goal of which is to heighten awareness to the very real cyber threat faced by Botswana and to assist companies to fully understand the cyber threat and its complex nature. ACS has secured some of the best speakers in the world talking on the latest trends and solutions. The Networking opportunities at the event will afford you the opportunity to develop relationships with the world's leading cyber professionals and firms before you are targeted.-Empowering you through knowledge.

DOI: 10.19080/JFSCI.2017.05.555663