Infocyte®

The Threat of Malware in Africa

Hunt Threats with Infocyte

In the News:

- Dexter malware strikes POS systems in South Africa, resulting in tens of millions of Rand lost
- Malware attacks account for 80% of cybercrime in Kenya 2015/16
- Fileless malware infects 8 Kenyan and 6 Ugandan banks and institutions

IT Infrastructure Infection Rates:

Libya (98%), Zimbabwe (92%), Algeria (84%), Cameroon (83%), Nigeria (82%), Ivory Coast (81%), Kenya (78%), Senegal (78%), Tunisia (74%), Morocco (66%) and Mauritius (57%)

African Countries Lost Over $2 Billion

- Nigeria – $550 million (2016)
- South Africa - $443.5 million (2016)
- Kenya – $175 million (2016)
- Tanzania - $85 million (2016)
- Ghana – $50 million (2016)
- Uganada – $35 million (2016)
- Senegal – $24 million (2016)

Spotlight on South Africa:

- 32% of organizations have experienced cybercrime
- Only 35% of organizations have a cyber incident response plan implemented
- 57% believe they will be affected in the next two years

Africa, Technology and the Threat of Malware

The rapid expansion of IT connectivity and businesses in Africa has led to the continent becoming a high value target for cyber-attacks of all kinds. Although Africa still has the lowest global Internet penetration rate at 28.6%, this accounts for 10% of all global users. Compare this to a penetration rate of 74% in Europe accounting 17% of global users.

Africa is currently experiencing exponential growth, fed by the rise in the prices of raw materials and the boom in the technological sector. The digital economy is developing at lightning speed. As in many things for Africa – the potential for the technology is virtually boundless, and so are the financial stakes.

But, Africa is not immune to IT security threats – countries like Botswana, Nigeria and South Africa have been featured in the news due to their prominence on global security threat indexes. Estimates vary, but together African nations such as Kenya, Angola, Nigeria, Rwanda, Botswana, Uganda, Tanzania, and South Africa lose billions of dollars per year.

Generally speaking, Africa now has one of the highest global mobile malware infection rates. This is arguably a consequence of timing for some industries. The relatively recent and rapid growth of Financial Services for example: some African nations were able to entirely skip the stages of bricks and mortar bank branches and landline telephones, and move directly into online banking and mobile telephone apps. Such rapid growth does not allow the time necessary to progressively establish proper security procedures.

The more complex and interconnected an industry is, the more rapidly new technologies are integrated and reliance grows. As technologies evolve at such a rapid pace however, so do adversaries and the threats they pose.

Realities and Future Trends

A highly significant proportion of IT infrastructure in Africa is running off of pirated software, which is never patched with security updates. This leaves the endpoints virtually naked when it comes to protecting systems and data. Combine the systemic weaknesses in national and corporate IT security infrastructures, the large and growing target base and the release of malware toolkits onto the dark web's global marketplace, and there is no question that Africa will continue to be targeted by malware on a significant and growing basis.

As African businesses develop and mature there will be increasing amounts of Intellectual Property and other proprietary information. The financial risks of neglecting security will grow accordingly.

Malware is becoming increasingly sophisticated, attacks are more frequent and the costs keep rising. Old malware rarely dies: it just lies dormant for a time. Exploit kits are rising in popularity once again, after approximately a year of decreasing usage. The Rig Exploit kit and the Terror Exploit kit have both experienced a drastic resurgence in the early months of 2017.

Typical responses to threats are to increase security. However when it comes to malware – the fact is that it doesn't matter what defenses are in place... malware still breaches. A recent Crowd Research Partners report found that 44% of security threats go undetected by automated security tools.

We know that enterprises are attacked hundreds, sometimes thousands of times per day. And despite significant investment in defensive technologies, malware continues to breach these defenses. To make matters worse, the average security breach goes undetected for over 6 months. Six months is a long time for an organization to live with malware unknowingly. Six months is a long time for malware to extract data and wreak havoc.

Fileless Malware and APTs

The recent "Fileless" malware that targeted over a hundred banks and financial institutions along with other organizations worldwide is a prime example of why threat hunting is of critical importance.

Fileless malware is a piece of nasty software that does not copy any files or folder to the hard drive in order to get executed. Instead, payloads are directly injected into the memory of running processes, and the malware executes in the system's RAM. These features make fileless malware incredibly difficult to detect using standard solutions.

There are other examples of advanced persistent threats that plague the security industry include: botnets, rootkits, RATs, macro enabled documents and scripts.

Undoubtedly there will be new threats emerging, and they will be available to hackers and criminals. It is not enough to merely defend and try to keep up with specific threats as they appear.

While it is important to keep AV, whitelisting and EDR technologies incorporated into a robust security posture – what is required to properly respond and react to malware is a threat-hunting platform.

The Infocyte Difference

- Infocyte's HUNT solution uses volatile memory analysis to reconstruct what is happening on an endpoint at a given point in time.
- Infocyte HUNT is not reliant on a host OS, which may be itself compromised.
- Our solution is not an EDR nor an SI (Security Intelligence) tool - it is a post-compromise detection tool.
- Infocyte HUNT does the work it would take a highly skilled forensic examiner months to complete, in minutes.
- Infocyte HUNT is the only true malware hunting platform currently on the market.

The Infocyte Methodology

Infocyte's methodology combines agentless scans with our File Intelligence and Digital Forensic Analytics Services into statistical models that determine the risk profile of endpoints.

Infocyte HUNT scans:

- Validate everything currently running or scheduled to run on endpoints
- Analyzes each system's volatile memory to discover signs of manipulation or hidden processes
- Are agentless
- Typically take just minutes to complete
- Do not rely on a potentially compromised host operating system to deliver results

Infocyte HUNT Benefits

- Definitively answers if you have been breached
- Advanced detection combines forensic automation and patent-pending memory analysis
- Fast. Infocyte HUNT can scan upwards of 25,000 endpoints per day
- No training required to effectively use Infocyte HUNT
- Final report provides collected intelligence and enables you to take action with swift remediation and incident response.

Start Hunting.
Contact us to learn how.

Infocyte®

CORPORATE HEADQUARTERS
110 E. Houston St. Floor 6
San Antonio, TX 78205
+ 1.844.INFOCYTE (844.463.6298)
sales@infocyte.com

www.infocyte.com
@InfocyteInc