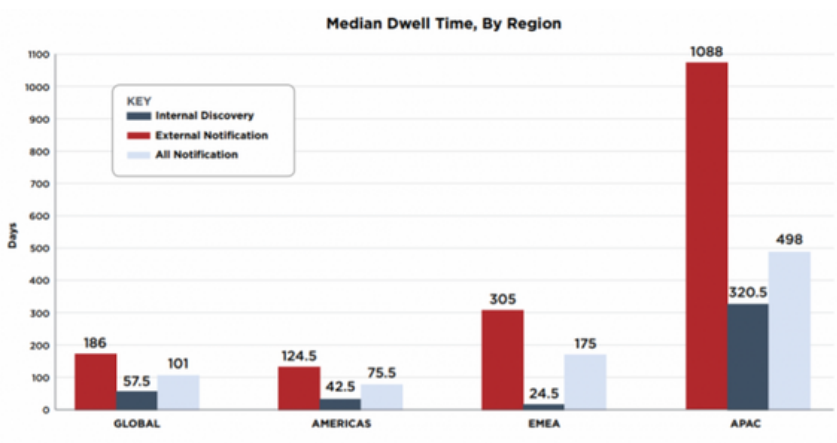
activereach

HAVE YOU BEEN BREACHED?

Network protection attracts much of today's security budget, but increasing protection will offer diminishing returns. Meanwhile data breaches are still happening, the dwell time is increasing.

A small investment in detection capabilities can deliver a greater reduction of risk than adding more protection.

AVERAGE DWELL TIME



In EMEA the median dwell time of a breach not discovered internally was 305 days - a staggering 10 months!

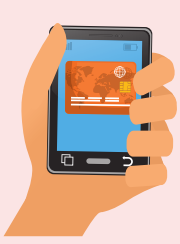
Source: Mandiant M-Trends 2018

LATERAL SPREAD

After criminals have taken up virtual residence without detection they are free to move laterally throughout the network and deploy all manner of attacks.

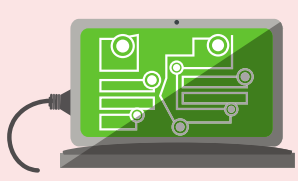
CRYPTO-JACKING

BOTNET RECRUITMENT



PAYMENT CARD SCRAPING

CREDENTIAL THEFT



SUBVERTING SOFTWARE DEVELOPMENT

TRENDS IN CRIMINAL ACTIVITY

Criminals want to convert breaches into money as efficiently as possible, and at as little risk of capture, as possible.

New techniques which prove to have poor risk-reward ratios for criminals tend to drop quickly from the charts.

Source: ENISA Threat Landscape Report 2018

Top Threats 2018

1. Malware
2. Web Based Attacks
3. Web Application Attacks
4. Phishing
5. Denial of Service
6. Spam
7. Botnets
8. Data Breaches
9. Insider Threats
10. Physical Manipulation/damage/theft/loss
11. Information Leakage
12. Identity Theft
13. Crypto--jacking
14. Ransomware
15. Cyber Espionage

INDICATORS OF ATTACK

- Unusual phone calls and questions
- Unusual account login activity
- Requests from unusual places, or at unusual times of day
- Unusually large request volume for one file
- Changes to clean registry or system files
- Mobile device profile changes
- Executable files in temp directories
- Local network scans and probes
- Log files being deleted

Find out more at www.activereach.net/breach-detection