314 DAY BATTLE PLAN

THE MODERN CYBER-CRIMINAL'S ATTEMPT TO STAY UNDETECTED

The average data breach goes unnoticed for 314 days.
What can happen in the days, weeks and months after an initial breach?

DAYS 0-10

Cyber-criminal's battle plan:
Spread out across an organisation

Adversary Process:
Steal credentials to get additional access points and more privileges connected to the domain controller.

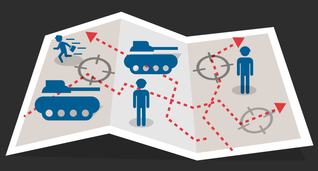
Defence strategy:
Ensure all accounts are audited or maintained to monitor abnormal access.

DAYS 10-20

Cyber-criminal's battle plan:
Create a plan B and a plan C for access

Adversary Process:
Determine alternative routes back in if they're discovered.

Defence strategy:
Evolve your defensive posture in response to adversarial changes with a Prevent – Detect – Respond strategy across the entire IT ecosystem.



DAYS 20-40

Cyber-criminal's battle plan:
Set up camp where the data is

Adversary Process:
Identify and locate the 'crown jewels' of a company's data, before running commands to determine how they can use different networks to see the targeted data.

Defence strategy:
Segment your networks and ring fence the high value data, putting additional security layers around the company crown jewels.

DAYS 40-60

Cyber-criminal's battle plan:
Discover relevant and valuable data and create a 'shopping list'

Adversary Process:
Create a recursive file listing of valuable information to get more detail on specific information sets.

Defence strategy:
Apply the principle of least privilege as not all users need access to all data and create audit logs to see who is accessing and moderating high value data.

DAYS 60-80

Cyber-criminal's battle plan:
Getting data out of an organisation

Adversary Process:
Use one of a number of ways to retrieve data such as compress it or gain remote access to copy and paste data onto a remote machine.

Defence strategy:
Constantly monitor, respond to and defend against data exfiltration as criminal evolve their tactics.

DAYS 80-314

Cyber-criminal's battle plan:
Maintain a surveillance operation and avoid detection

Adversary Process:
Learn fast and change tactics, move around in a network and create new and cunning ways to remain undetected.

Defence strategy:
Examine perimeter security and set up layers of network and endpoint trip wires internally.

visit our website for more information on how SecureWorks can help protect your network from cyber-criminals: **www.secureworks.co.uk**

SecureWorks