The changing
y Threat
ape

Vic

ee India

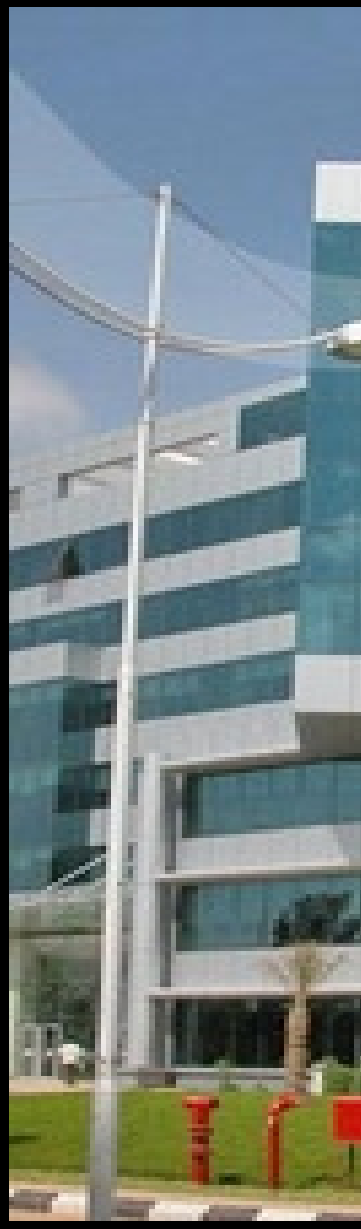
largest R&D site

largest threat-
ce team

uct development, but
echnical support, PM,

ent applications

very McAfee product
bution from India



ING FOR ESPIONAGE

HACKING FOR PROFIT

HACKING FOR FUN

2003

2005

Nation-State Coordin
Kinetic/Cyber Operat

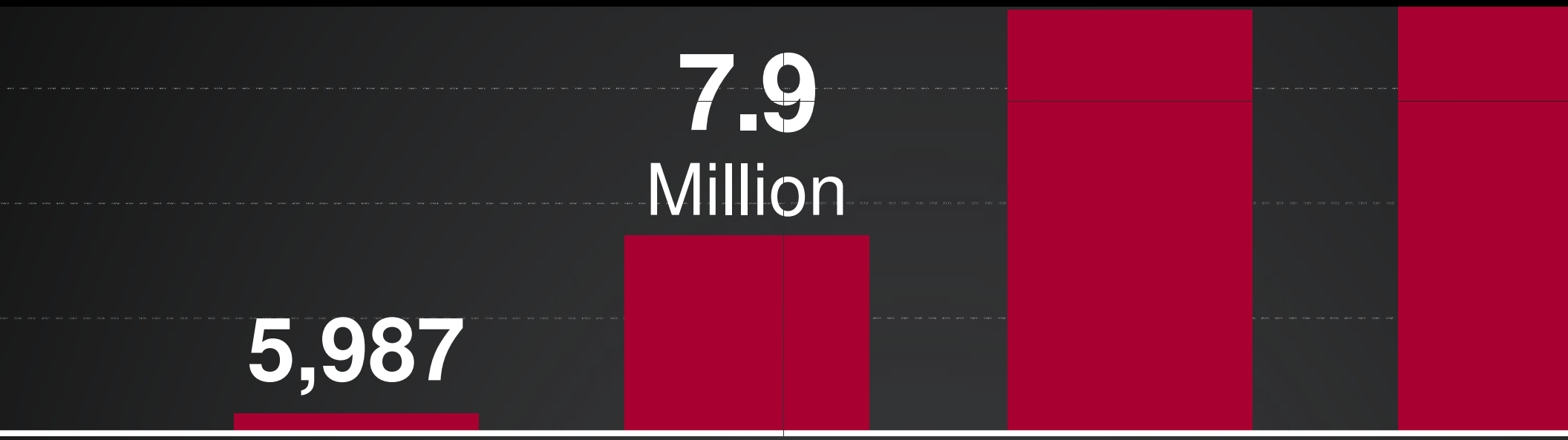
Cyberespionage

Cybercriminals

Threat Sophistication

ALWARE Tsunami
rives CYBERCRIME

34.
Millio



Afee reviews about

100,000

potential malware samples per

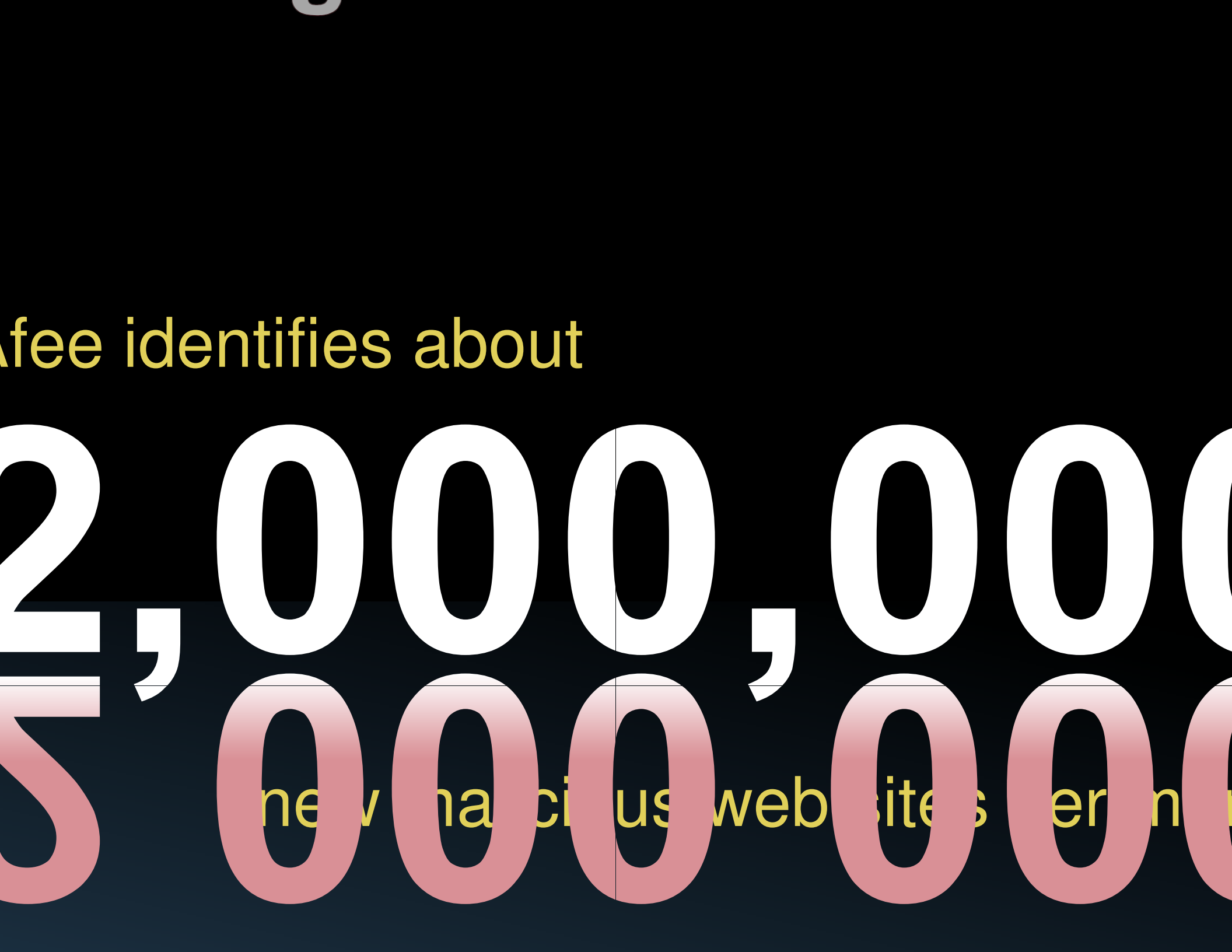
McAfee identifies over

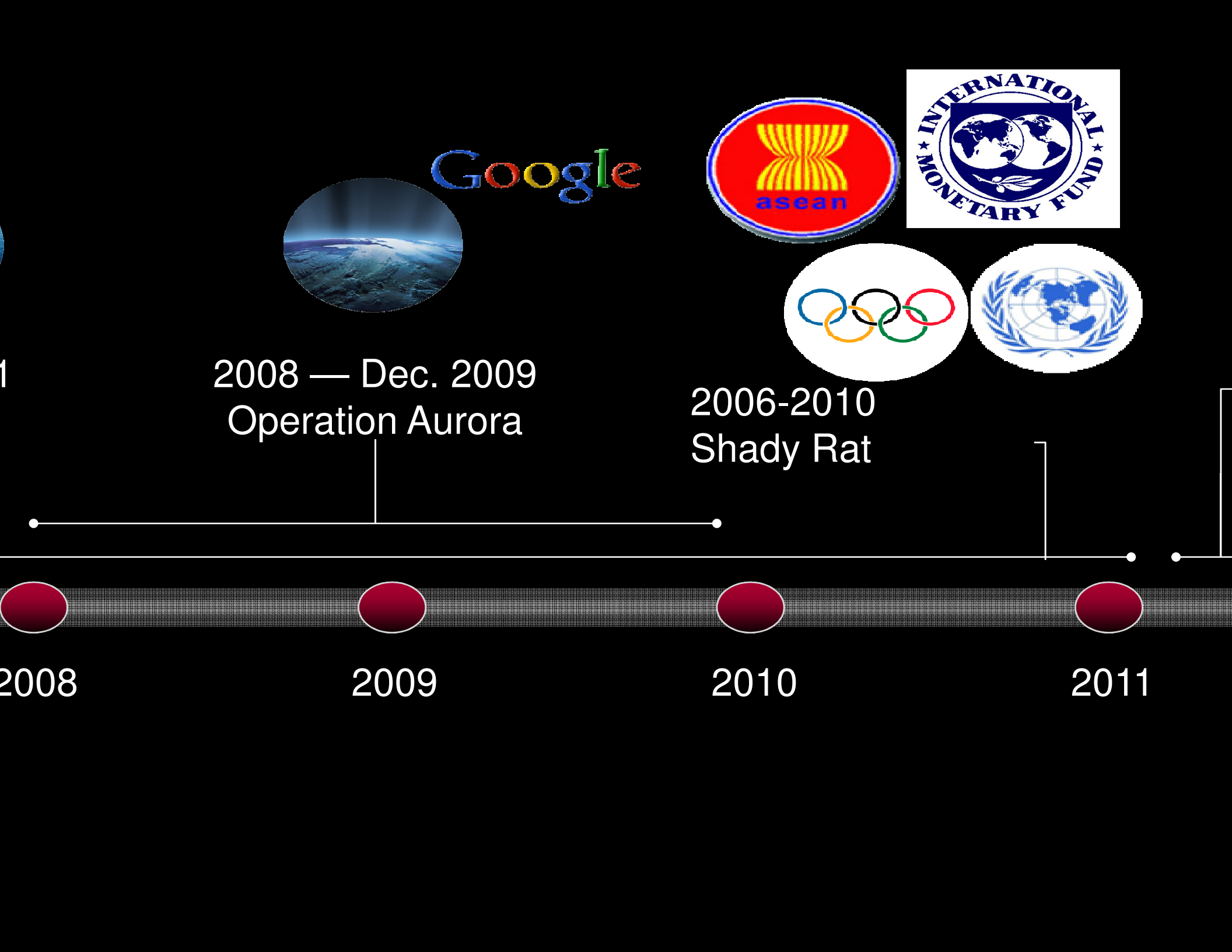
55,000

22,000

new unique pieces of malware per da

Afee identifies about




Google
asean
INTERNATIONAL MONETARY FUND
2008 — Dec. 2009
Operation Aurora
2006-2010
Shady Rat
2008
2009
2010
2011

the Business of Security

- Reactive Security (plain AV)
- Proactive Security

evention

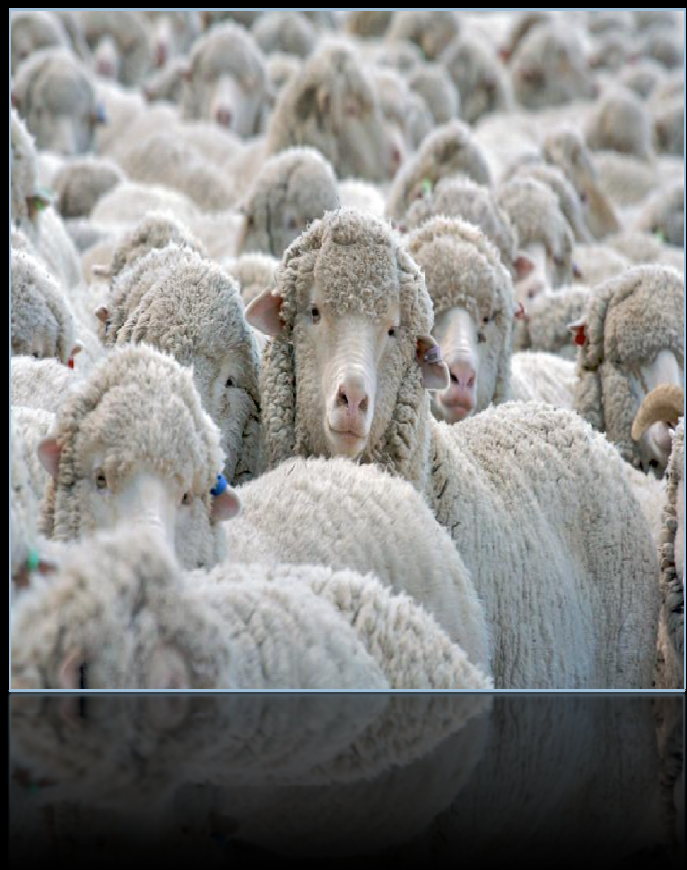
white-listing

ctive Protection

the situation

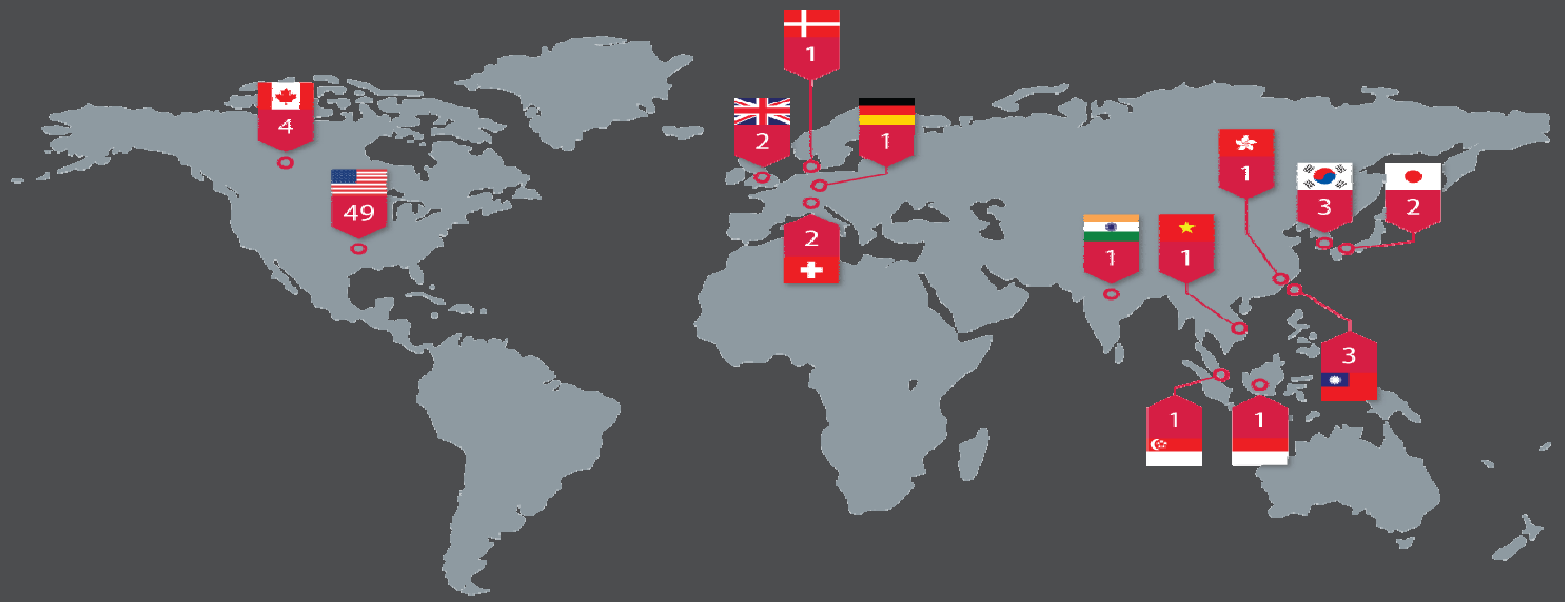
zation of IT

on



Operation Shady RAT

usions into **70+**
anies, governments and
ganizations during the



6

- ...truction/ ...y Industry 3
- ... Industry 1
- ...gy 1
- ... Power 1

13

- Electronics Industry 3
- Computer Security 2
- Information Technology 2
- Satellite Communications 2
- News Media 2
- Information Services 1
- Communications Technology 1

13

- Defense Contractor 13

4

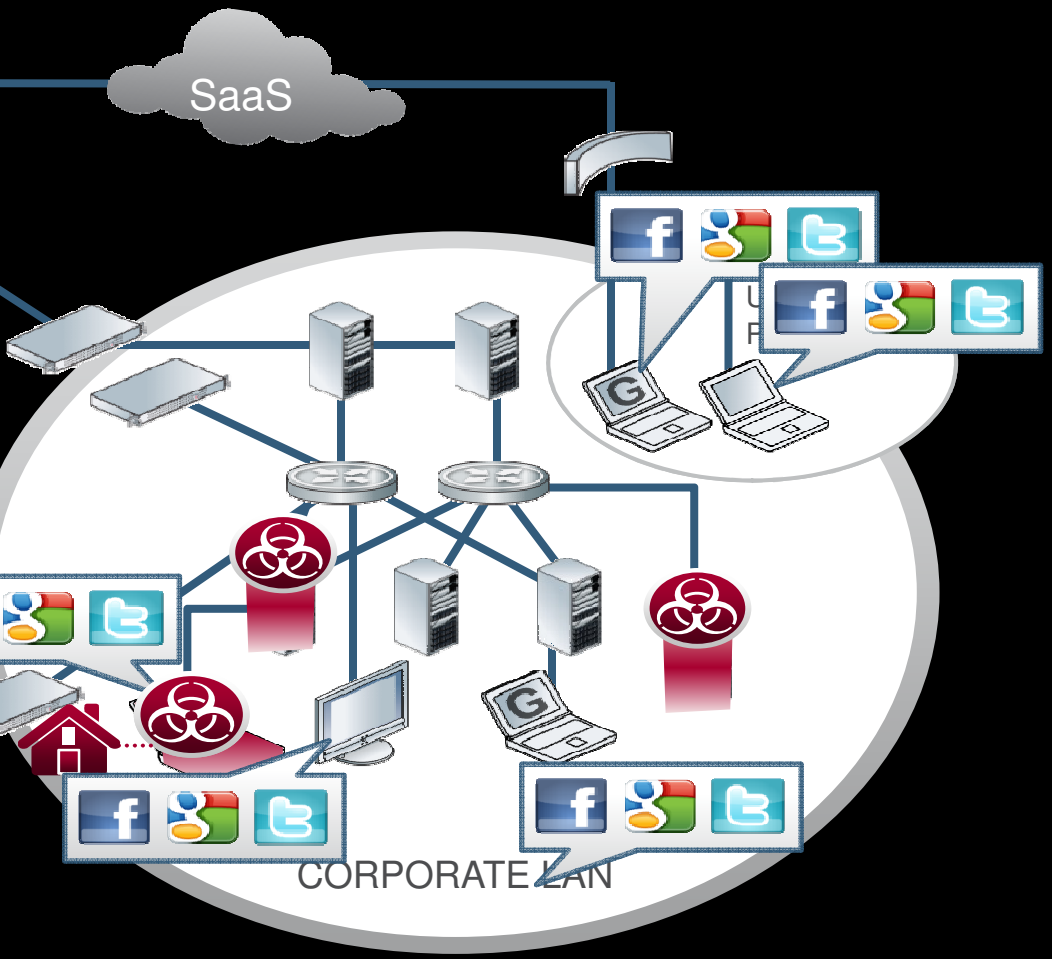
- Real Estate 2
- Accounting Industry 2
- Agriculture 1
- Insurance 1

tics of an APT

ck. Usually focused on a type of goal – not opportu
ltiple methods – social engineering, sql injection, r
adar" – Hard to detect using conventional methods

in this attack was 28 months
e of 72 companies identified was 8.75 months

phy is affected
business is affected – public, private, government



Reconnaissance

- Map org chart (Identify attack targets)
- Social reconnaissance (acquire email,
- Scan for vulnerabilities (web server/OS

Social Engineering Targete

- Phishing email (malicious PDF, DOC, e
- Gain physical access (impersonate clea
- Candy drops around building(Thumb dr

Establish Covert Backdoor

- Command execution on target
- Gain elevated user privileges, Inject ad
- Laterally move within network & establi

Establish Command & Cont

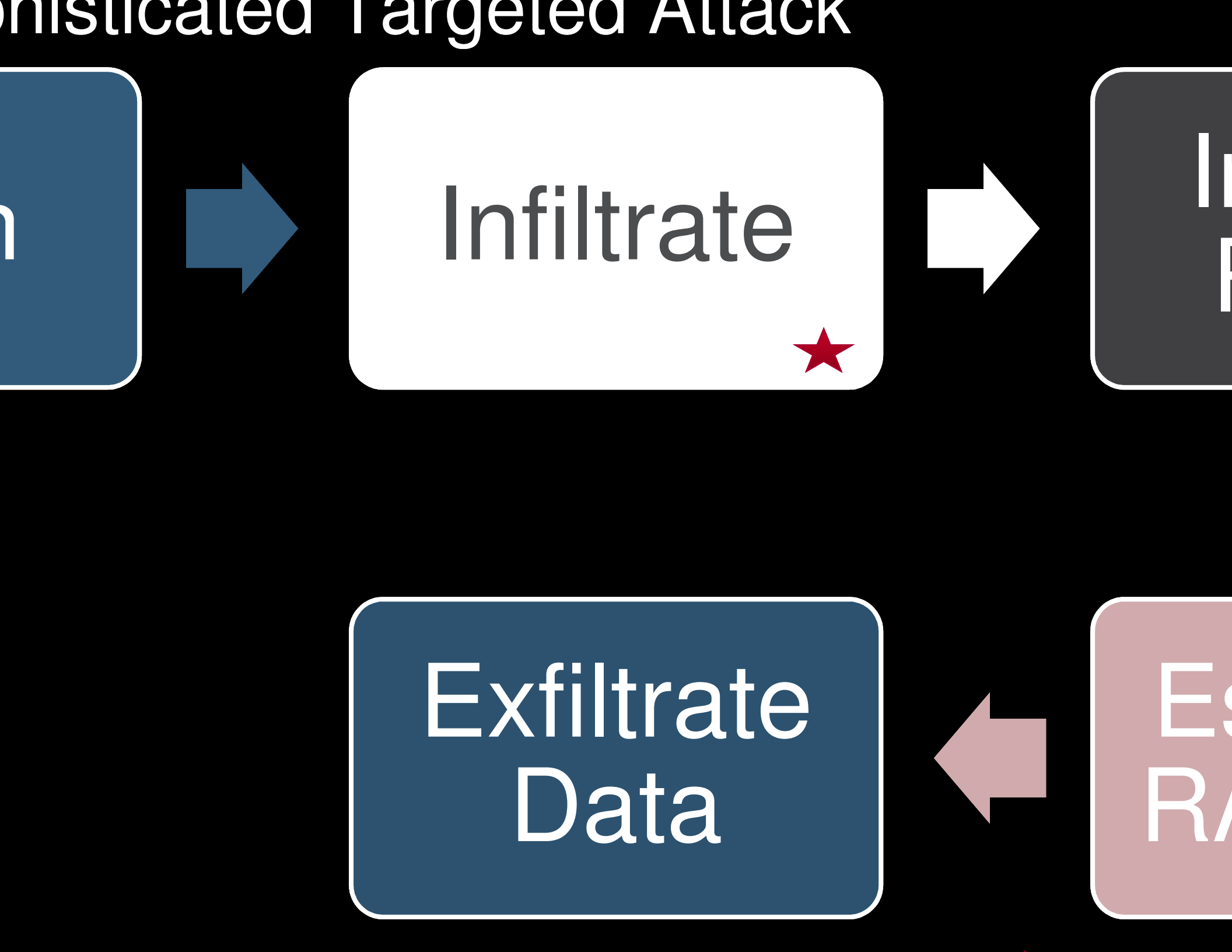
- Install system admin tools (Keyloggers,
- Establish encrypted SSL tunnel
- Utilize a remote administration tool (RAT

Complete Objectives

- Ex-filitrate Intellectual Property, Trade S
- Control critical systems

Maintain Persistence

- Revamp Malware to avoid detection
- Utilize other attack methods to maintain
- Continue monitoring networks, users, d


Infiltrate
Exfiltrate Data

ultimate goal

ata is coveted
crets
e
ses
ves
plans
details for new
auctions
stores
acts
nfigurations

STOLEN D
NOW
REACH
PETABY
OF
CONTEN

er the Radar

file size

mmon AP file names

e, explore.exe, lprinp.dll, wiinzf21.dll

detection avoidance

HTTP connections

ection and Service persistence

ication

t of backdoors connect outbound-only

use TCP port 80 or 443; 17 percent are mixed

S

s

has

yie

e Global 2000 are divided into two cat

e who've

been

promised

l know it

Those wh

been

comprom

and don't

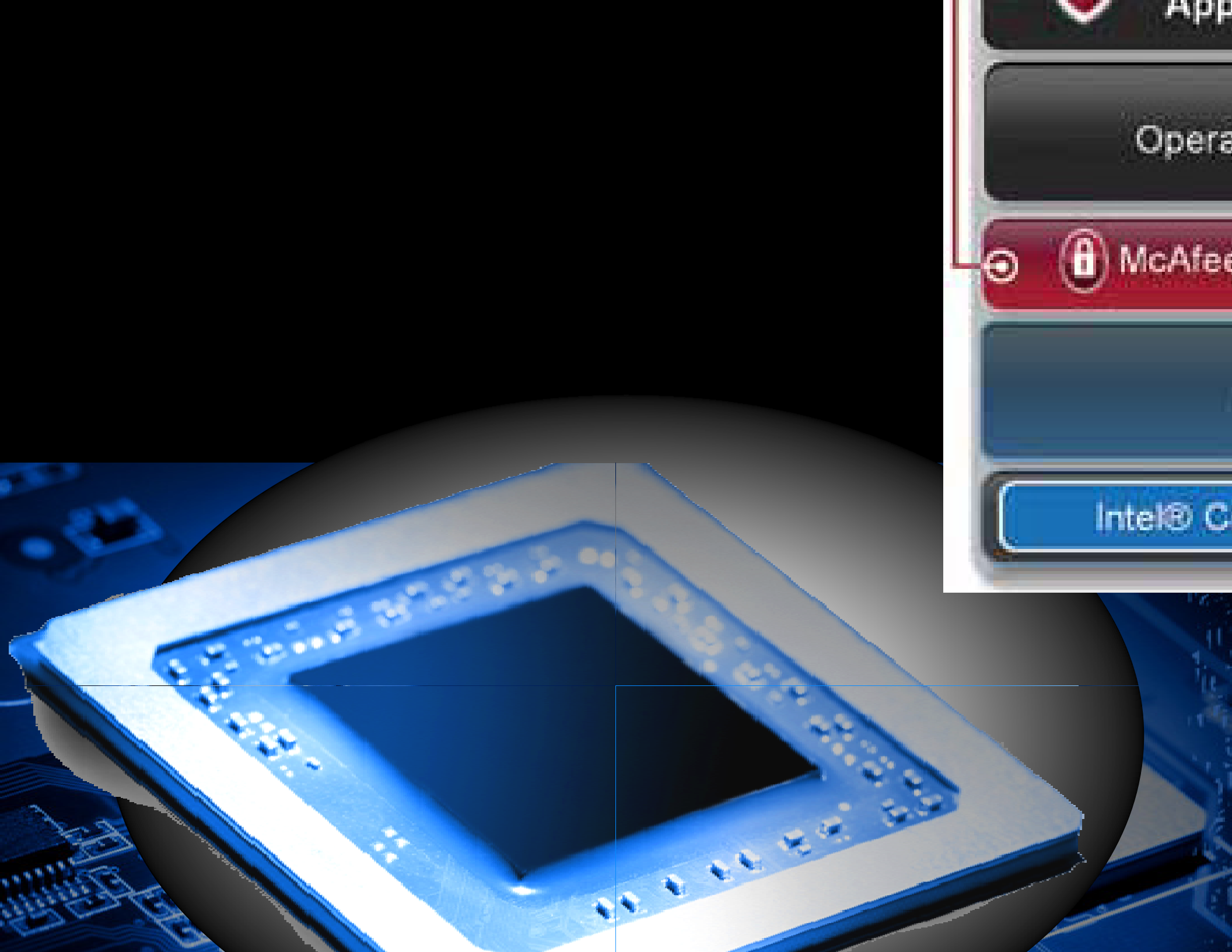
it yet!

ep 1: Basics: Email security, Firewall, IPS, Web
putation

ep 2: Application whitelisting

ep 3: Database activity monitoring

ep 4: DLP for exfiltration prevention and monitorin


Opera
McAfee
Intel®

ght Vs Light Weight

ft

Security

Experts

telligence

Security

kage Prevention

e Security

gies

Vs

On My

An I

Sin

olicy is Not Sufficient

- out Security Technologies
- ies/Procedures as well
- aining & Communication
- st “the innocent single click”
  - was from a co-worker”
- vord practices
- physical and IT
- aining & more Training

Greatest Battle
ies Within”

Thank You!