CYBER - PHYSICAL CONVERGENCE

PERIL OR OPPORTUNITY?

CROWDSTRIKE

CROWDSTRIKE

AARON AUBREY NG

INTELLIGENCE SME | SENIOR SYSTEMS ENGINEER

ARMY

GOVERNMENT

INTELLIGENCE

INDUSTRY

- **15+ years:** Innovating at the intersection of Intelligence, Security, and Strategy
- **Government**: Former Intelligence Officer/Major in the Singapore Armed Forces; Served in the Military Intelligence Organisation (MIO), the Defence Cyber Organisation (DCO), and the Digital & Intelligence Service (DIS)
- **Private Sector**: Designed and built threat intelligence programs for large Fortune 500 companies and government agencies across META and APJ
- **Education**: MSc Management Science & Engineering from Stanford University; BEng Chemical Engineering from University College London
- **Professional Accreditations**: GCTI | GPEN | GCIA | GOSI | GCIH | GSTRT | GSEC

aaron(dot)ng@crowdstrike.com

+971 55 213 6585

Aaron Aubrey Ng @ CrowdStrike

"THOSE WHO CANNOT REMEMBER THE PAST ARE CONDEMNED TO REPEAT IT."

AGENDA

1 HUMBLE **BEGINNINGS**

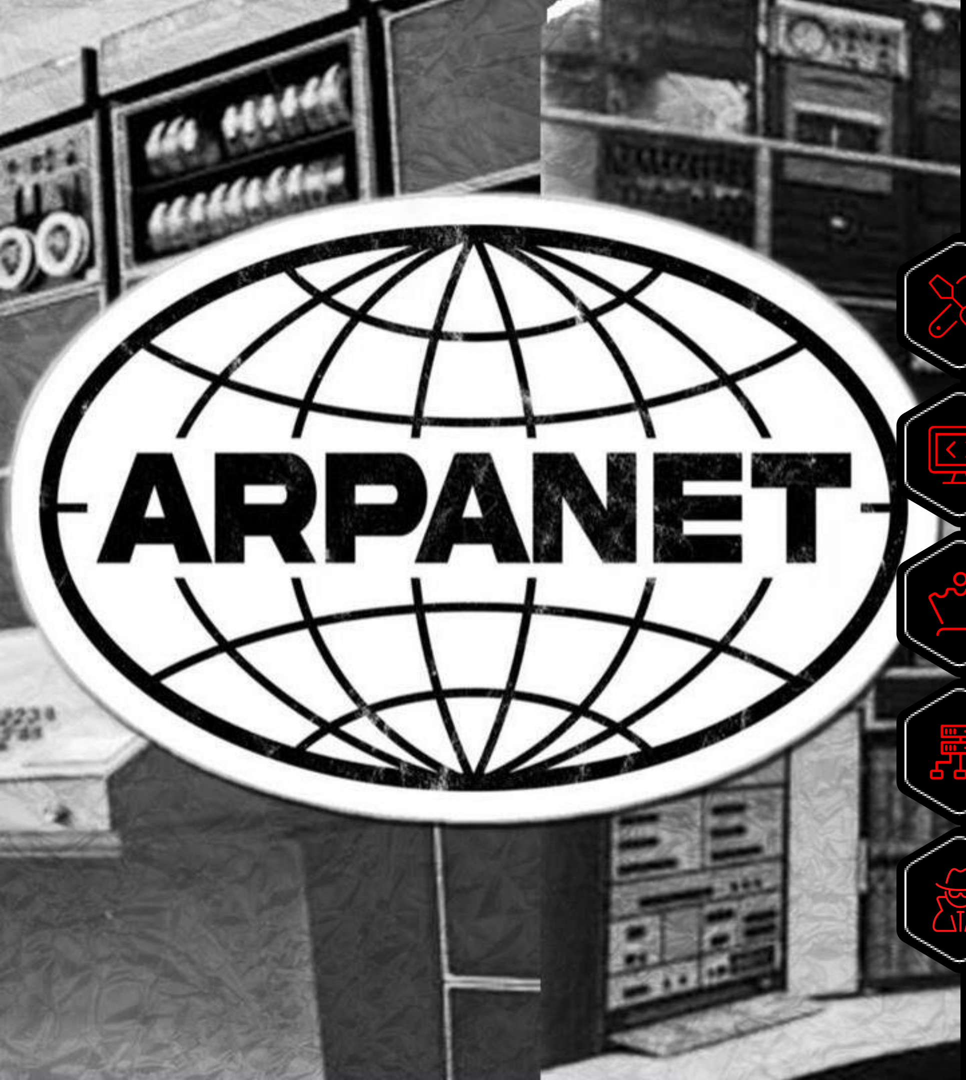
2 CYBER **ESPIONAGE**

3 PHYSICAL **DESTRUCTION**

4 **FINANCIAL** GAIN

5 THE **FUTURE** BECKONS

CROWDSTRIKE

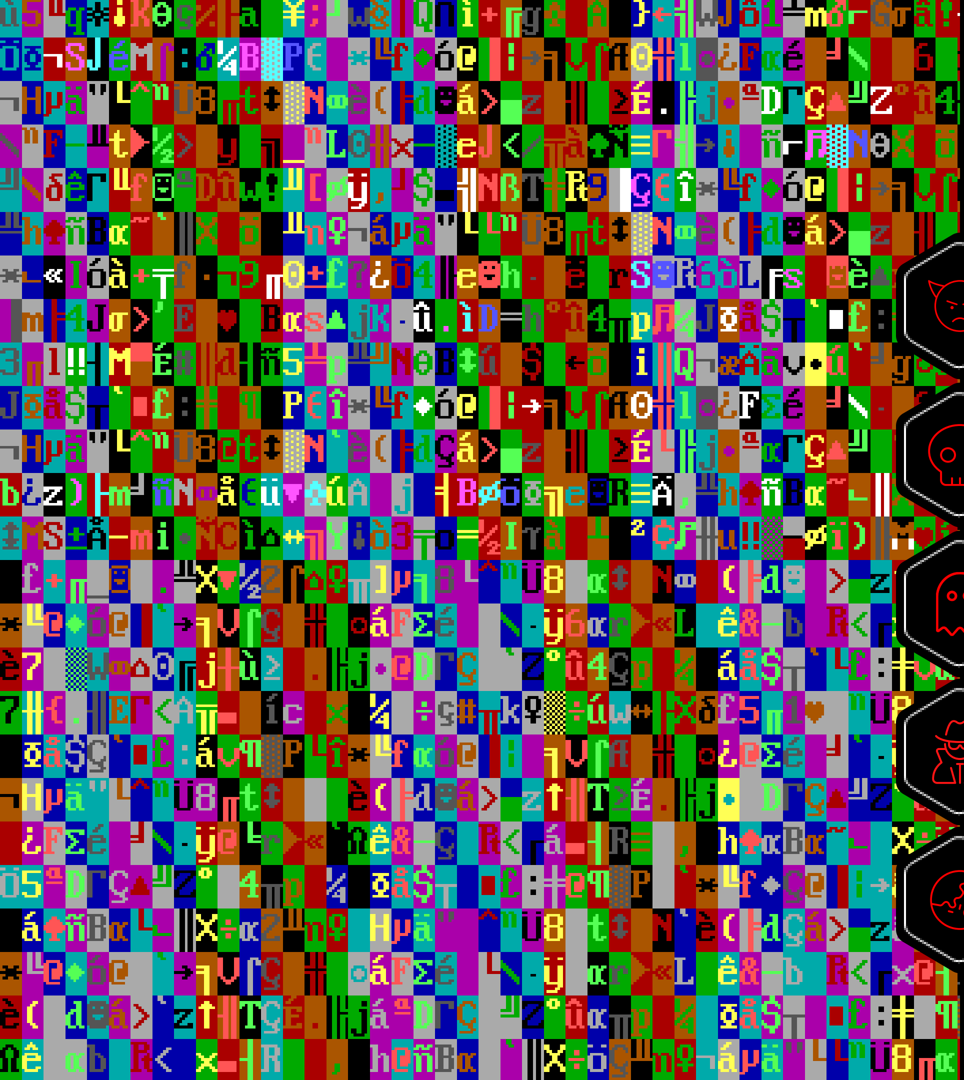


ORIGINS OF THE INTERNET

HOW IT CAME TO BE

- **ARPANET** – ADVANCED RESEARCH PROJECTS AGENCY NETWORK
- FIRST COMPUTER **NETWORK** USING **PACKET SWITCHING**
- COMMUNICATION SYSTEM FOR **MILITARY** & ACADEMIC PURPOSES
- **DECENTRALISATION** & **FAULT TOLERANT** COMMUNICATIONS
- **SECURITY** WAS NOT PART OF THE **DESIGN** CONSIDERATIONS

CROWDSTRIKE



EARLY SIGNS OF ABUSE & MISUSE

THE CAT-AND-MOUSE GAME BEGINS

- INDIVIDUALS COULDN’T RESIST TO **WAGE MISCHIEF**
- 1971 – **CREEPER WORM** WRIGGLE THROUGH ARPANET
- 1973 – **REAPER** SPREADS THROUGH ARPANET **DELETING CREEPER**
- 1979 – 16-YEAR-OLD **KEVIN MITNICK** HACKS INTO THE ARK
- 1984 – MAINSTREAM USE OF THE TERM **“VIRUS”**

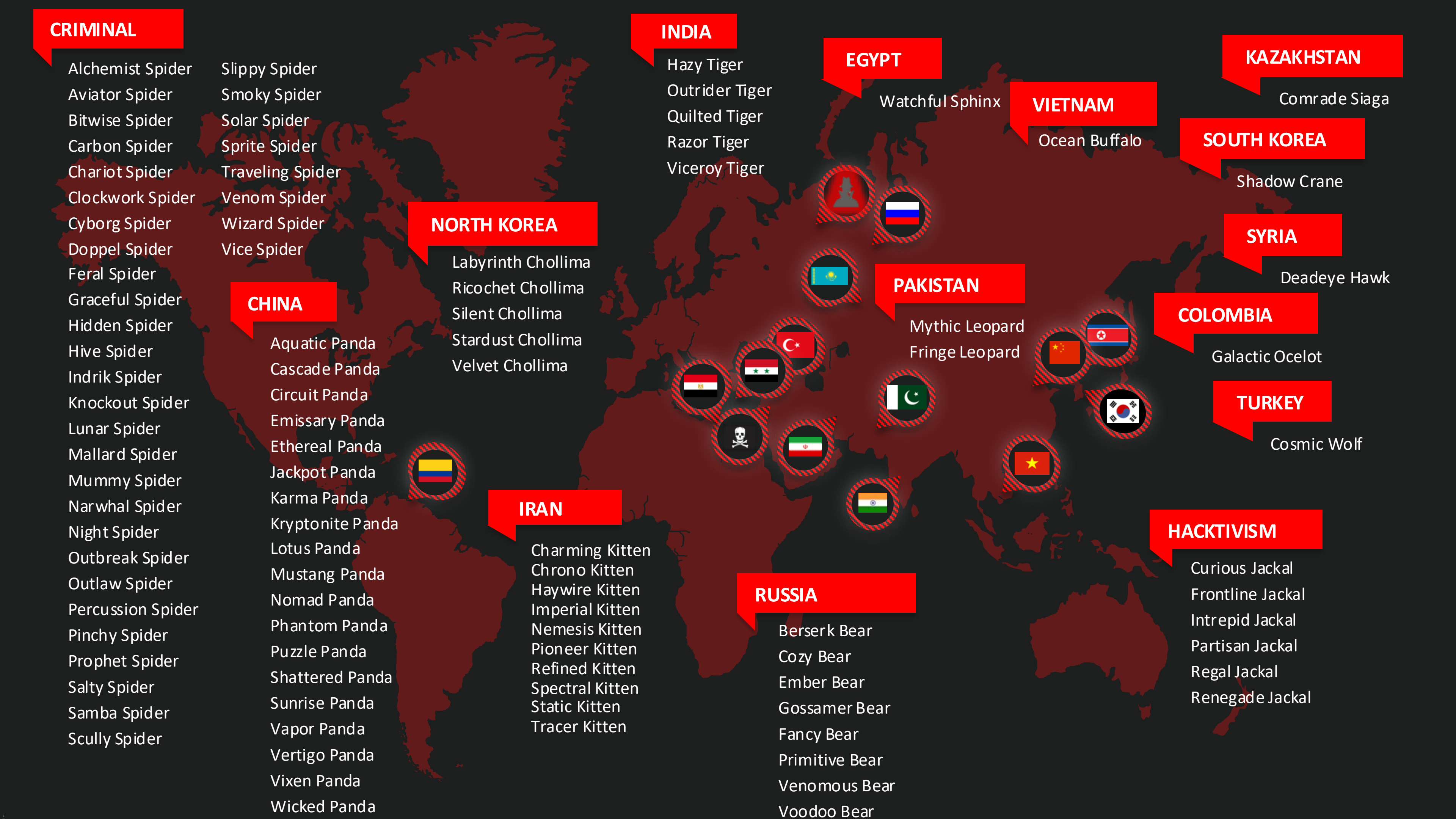
CROWDSTRIKE

PRESENT DAY ADVERSARY ATTACK MOTIVATIONS

NATION STATE

ECRIME

HACKTIVISM



CRIMINAL

- Alchemist Spider
- Aviator Spider
- Bitwise Spider
- Carbon Spider
- Chariot Spider
- Clockwork Spider
- Cyborg Spider
- Doppel Spider
- Feral Spider
- Graceful Spider
- Hidden Spider
- Hive Spider
- Indrik Spider
- Knockout Spider
- Lunar Spider
- Mallard Spider
- Mummy Spider
- Narwhal Spider
- Night Spider
- Outbreak Spider
- Outlaw Spider
- Percussion Spider
- Pinchy Spider
- Prophet Spider
- Salty Spider
- Samba Spider
- Scully Spider
- Slippy Spider
- Smoky Spider
- Solar Spider
- Sprite Spider
- Traveling Spider
- Venom Spider
- Wizard Spider
- Vice Spider

CHINA

- Aquatic Panda
- Cascade Panda
- Circuit Panda
- Emissary Panda
- Ethereal Panda
- Jackpot Panda
- Karma Panda
- Kryptonite Panda
- Lotus Panda
- Mustang Panda
- Nomad Panda
- Phantom Panda
- Puzzle Panda
- Shattered Panda
- Sunrise Panda
- Vapor Panda
- Vertigo Panda
- Vixen Panda
- Wicked Panda

NORTH KOREA

- Labyrinth Chollima
- Ricochet Chollima
- Silent Chollima
- Stardust Chollima
- Velvet Chollima

IRAN

- Charming Kitten
- Chrono Kitten
- Haywire Kitten
- Imperial Kitten
- Nemesis Kitten
- Pioneer Kitten
- Refined Kitten
- Spectral Kitten
- Static Kitten
- Tracer Kitten

INDIA

- Hazy Tiger
- Outrider Tiger
- Quilted Tiger
- Razor Tiger
- Viceroy Tiger

RUSSIA

- Berserk Bear
- Cozy Bear
- Ember Bear
- Gossamer Bear
- Fancy Bear
- Primitive Bear
- Venomous Bear
- Voodoo Bear

EGYPT

- Watchful Sphinx

PAKISTAN

- Mythic Leopard
- Fringe Leopard

VIETNAM

- Ocean Buffalo

KAZAKHSTAN

- Comrade Siaga

SOUTH KOREA

- Shadow Crane

SYRIA

- Deadeye Hawk

COLOMBIA

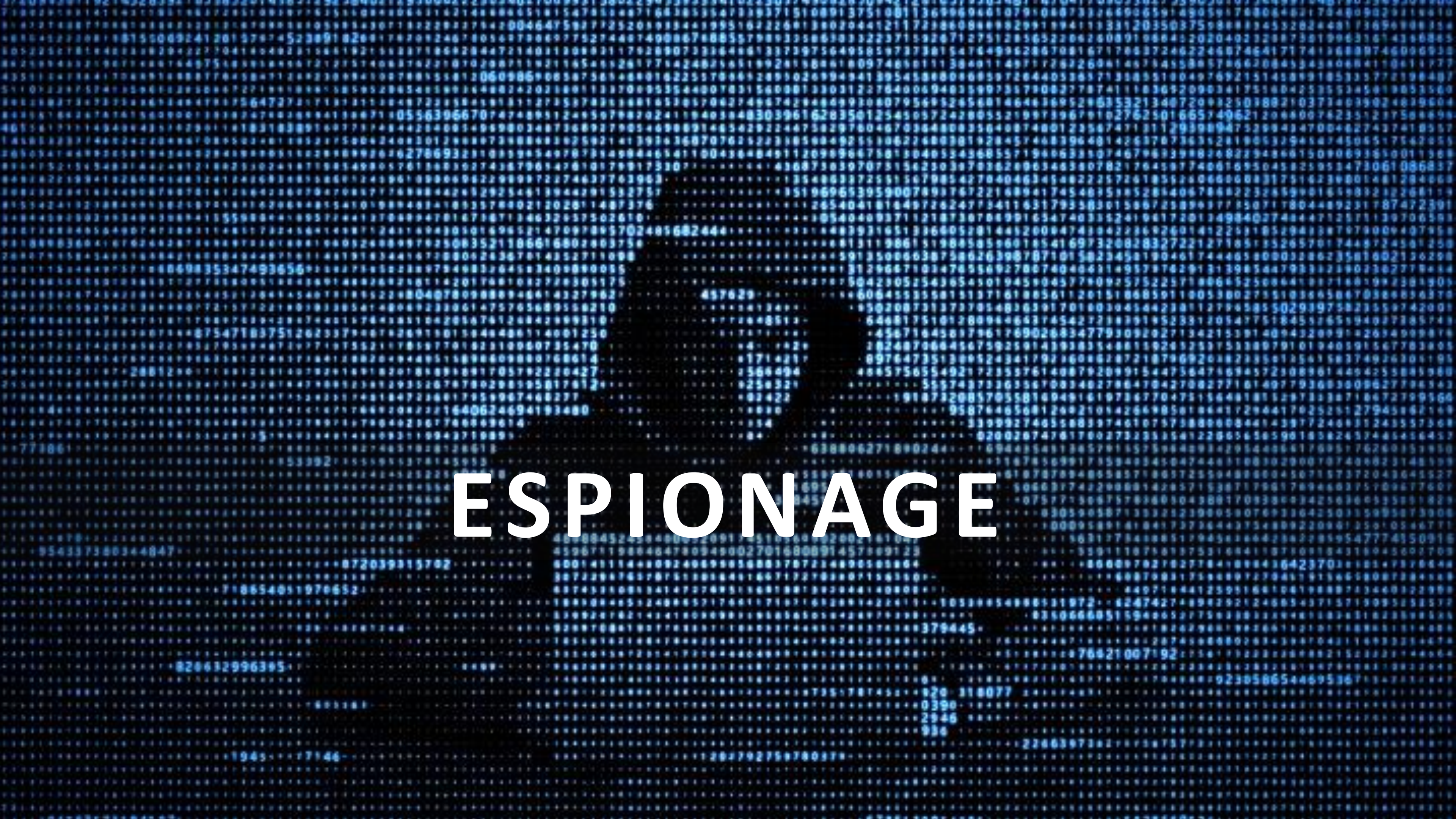
- Galactic Ocelot

TURKEY

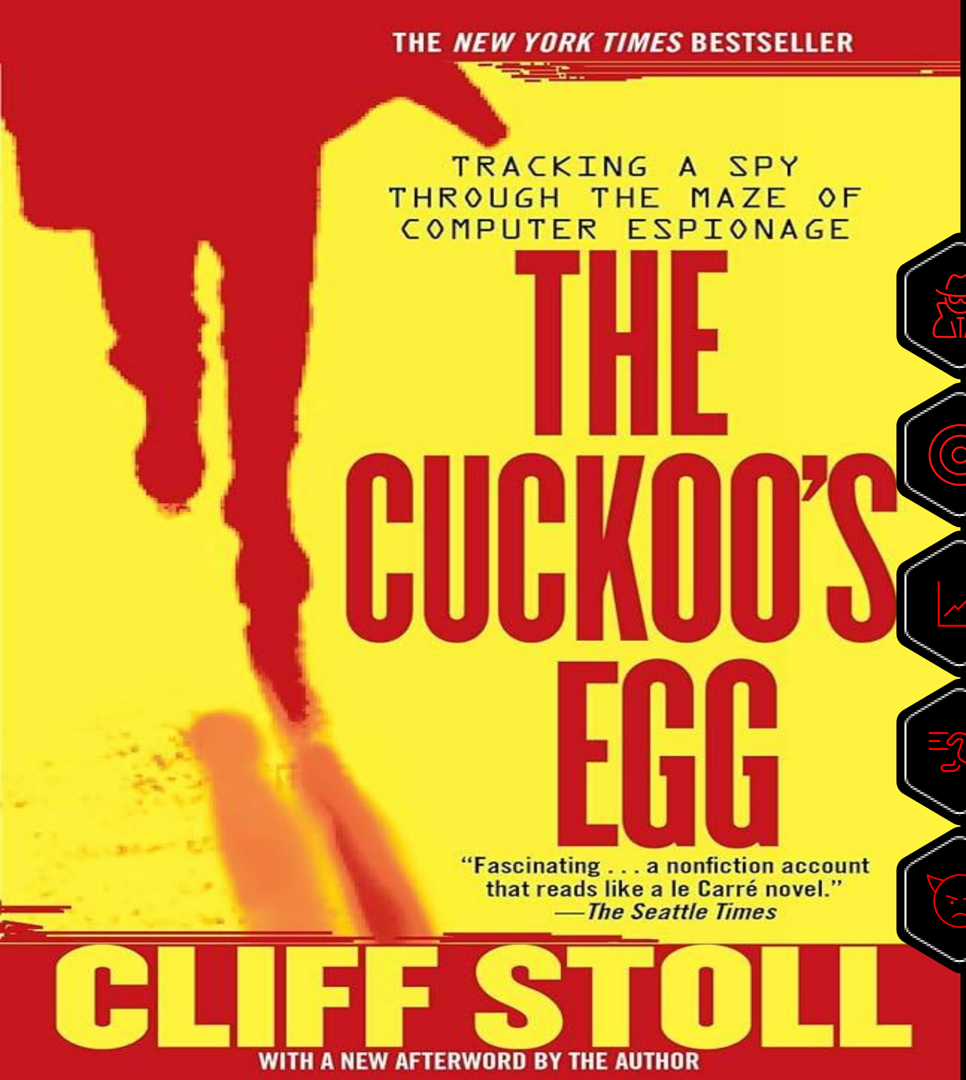
- Cosmic Wolf

HACKTIVISM

- Curious Jackal
- Frontline Jackal
- Intrepid Jackal
- Partisan Jackal
- Regal Jackal
- Renegade Jackal



ESPIONAGE


THE *NEW YORK TIMES* BESTSELLER
TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE
THE CUCKOO'S EGG
"Fascinating . . . a nonfiction account that reads like a le Carré novel."
—*The Seattle Times*
CLIFF STOLL
WITH A NEW AFTERWORD BY THE AUTHOR

EARLY DAYS OF CYBER ESPIONAGE

BEGINNING AT THE END (OF THE COLD WAR)

- **FIRST** DOCUMENTED CASE OF CYBER **ESPIONAGE** – "PRE-WEB"
- CLIFF STOLL NOTICED DISCREPANCY IN **COMPUTING TIME RECORDS**
- SYSTEMATIC TARGETING OF COMPUTERS AT **US MILITARY** BASES
- CREATED A **HONEYPOT** FOR ATTACKER, LURE WITH FAKE INFORMATION
- IDENTIFIED AS **MARKUS HESS** – WEST GERMAN SELLING INFO TO **KGB**

CROWDSTRIKE

MOONLIGHT MAZE

START OF THE ADVANCED PERSISTENT THREAT

- 1999 - CYBER ESPIONAGE BROUGHT TO **PUBLIC CONSCIOUSNESS**
- **MULTI-YEAR** CAMPAIGN – **NASA, PENTAGON, DOE, CONTRACTORS**
- **STOLEN INFO** IF PRINTED – 3X HEIGHT OF WASHINGTON MONUMENT
- ATTRIBUTED TO **RUSSIAN GOVERNMENT** BUT LACK ROBUST EVIDENCE
- 2017 – LINKED TO **TURLA** / **VENOMOUS BEAR** > **ACTIVE ADVERSARY**

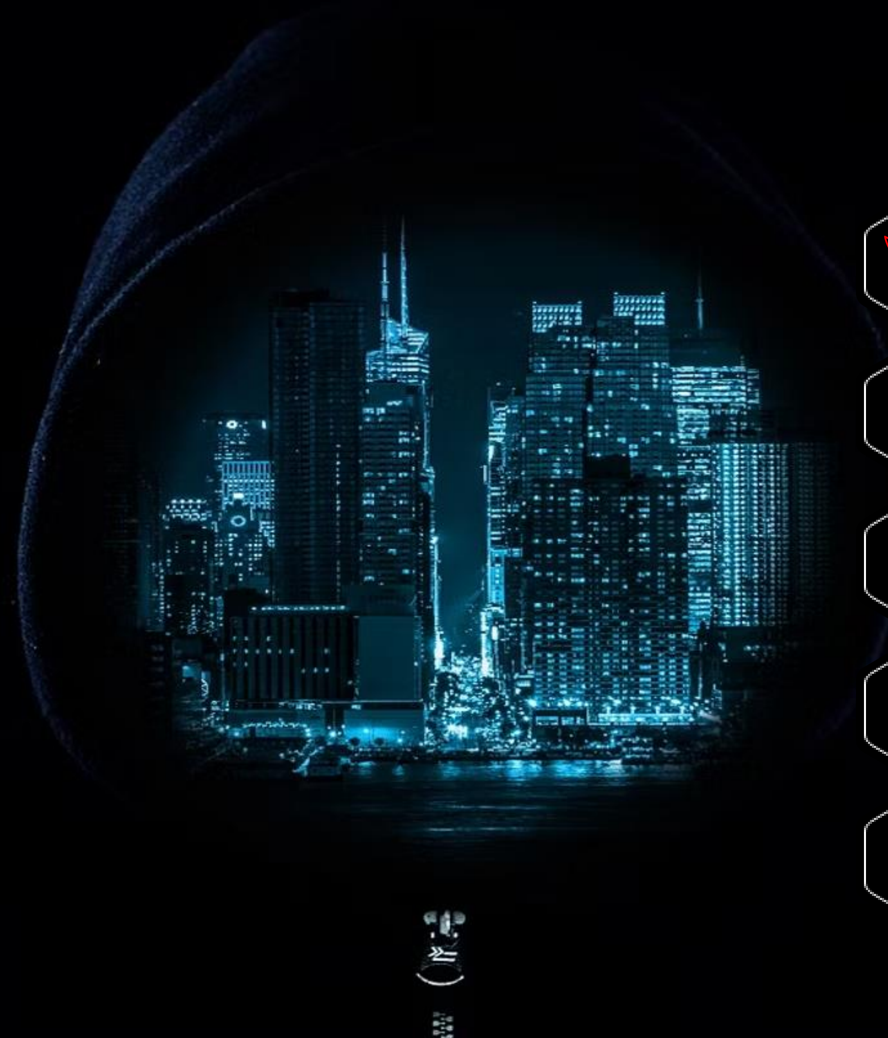
CROWDSTRIKE

TITAN RAIN

FIRST INSTANCE OF CHINESE ESPIONAGE

- **CHINESE** CYBER ESPIONAGE TARGETING **US AND UK GOV AGENCIES**
- **2003 TO 2007** – TARGET **US STATE DEPT, US DHS, UK MOD, UK FCO**
- SIGNS OF **COORDINATION**, **PERSISTENCE**, AND **SOPHISTICATION**
- ATTRIBUTED TO **PLA UNIT 61398** > **APT1** / **COMMENT PANDA**
- **DECADES-LONG** EFFORT TO **REDUCE CHINESE CYBER OPS** AGAINST US

CROWDSTRIKE



OPERATION AURORA

WIDESPREAD INDUSTRIAL ESPIONAGE

- **CHINESE** TARGETING OF **US PRIVATE SECTOR** COMPANIES
- JUN - DEC 2009 > **GOOGLE, YAHOO, ADOBE, DOW, MORGAN STANLEY**
- STEAL **TRADE SECRETS** + TARGET CHINESE **HUMAN RIGHTS** ACTIVISTS
- EVENTUALLY LED TO GOOGLE **CEASING OPERATIONS** IN CHINA
- RAISED PROFILE OF CYBER OPS AS TOOL FOR **INDUSTRIAL ESPIONAGE**

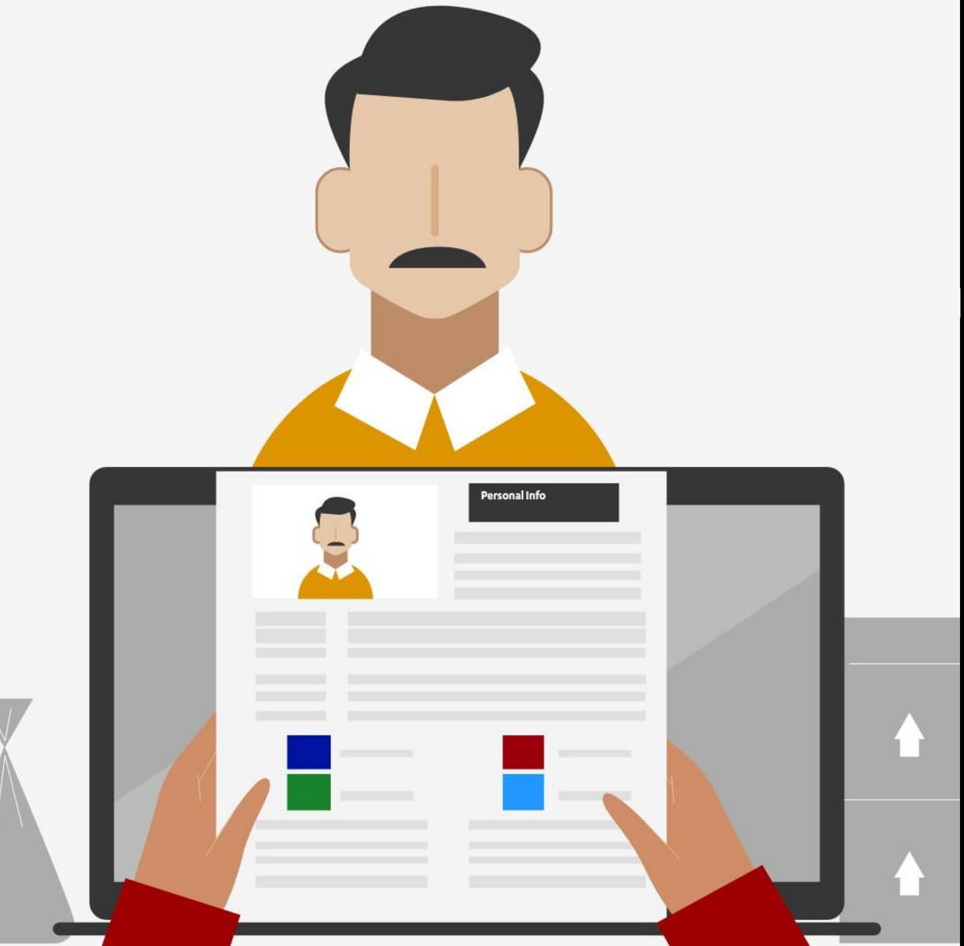
OPERATION CLOUD HOPPER

SUPPLY CHAIN COMPROMISE

- **CHINESE** TARGETING OF **MANAGED IT SERVICE PROVIDERS**
- **INTELLECTUAL PROPERTY** & **SENSITIVE DATA** OF MSP **CUSTOMERS**
- GLOBAL **VICTIMOLOGY** – US, UK, NORDICS, JAPAN, BRAZIL, INDIA, ANZ
- ATTRIBUTED TO **APT10 / STONE PANDA** – MSS TIANJIN BUREAU
- BROUGHT **SUPPLY CHAIN SECURITY** TO PUBLIC CONSCIOUSNESS

CROWDSTRIKE

BULK PERSONAL DATA THEFT



PERSISTENT BULK PII THEFT

ATTRIBUTED TO CHINESE ESPIONAGE

JAN ‘15	ANTHEM
APR ‘15	OFFICE OF PERSONNEL MANAGEMENT, USG
AY ‘15	UNITED AIRLINES
JUL ‘17	EQUIFAX
UL ‘18	SINGHEALTH
SEP '18	MARRIOTT STARWOOD GROUP
JUN '19	AUSTRALIAN NATIONAL UNIVERSITY
MAY '20	EASYJET
SEP ‘21	>10 INDONESIAN GOVERNMENT ENTITIES UNIQUE IDENTIFICATION AUTHORITY OF INDIA

RISK & IMPLICATIONS

ESPIONAGE AND YOU

- CORRELATE **BIO & CAREER DATA** WITH **BEHAVIORAL PATTERNS**
- FOREIGN **GOV PERSONNEL** DATABASES > **HUMINT RECRUITMENT**
- SENSITIVE **PERSONAL** DATA – HEALTH & PROCLIVITIES > **BLACKMAIL**
- **NOVEL** INTEL / COUNTERINTEL APPLICATIONS WITH **GENAI**
- **EVERYONE / ANYONE** CAN BECOME AN ESPIONAGE **TARGET**

PHYSICAL DESTRUCTION

OPERATION ORCHARD

CYBER IN SUPPORT OF KINETIC ATTACK

- **CYBER OP** TO FACILITATE **PHYSICAL STRIKE** AGAINST MAIN TARGET
- **RECON** – MOSSAD INSTALLS **TROJAN** ON SYRIAN OFFICIAL LAPTOP
- **HYBRID** ATTACK – **ELECTRONIC** ATTACK BEFORE PRECISION STRIKE
- BLIND SYRIAN AIR DEFENCE RADAR > IAF ENTERS SYRIA **UNDETECTED**
- EARLY DEMONSTRATION OF **"NON-KINETIC"** & KINETIC **INTEGRATION**

CROWDSTRIKE

STUXNET
THE FIRST CYBER WEAPON

- JOINT **US-ISRAEL** OP TO TARGET **NANTAZ NUCLEAR FACILITY**
- **SPECIFICALLY DESIGNED** TO CAUSE **CENTRIFUGES** TO **FAIL**
- **DEGRADE** IRAN NUCLEAR WEAPONS **IN PLACE OF** KINETIC ACTION
- FIRST INSTANCE OF **CYBER** OP CAUSING **PHYSICAL** DAMAGE
- FEARS OF **“CROSSING THE RUBICON”** WITH **DESTRUCTIVE** ATTACKS

CROWDSTRIKE

SHAMOON

LARGE-SCALE DATA DESTRUCTION

- DATA WIPED FROM **35K+** COMPUTERS – **SAUDI ARAMCO**
- MALWARE STOLE **PASSWORDS**, WIPED **DATA**, PREVENTED **REBOOT**
- “CUTTING SWORD OF JUSTICE” CLAIMED RESPONSIBILITY - FAKETIVISM
- ATTRIBUTED TO **IRAN** > LIKELY PERPETRATED BY **IRGC**
- IRAN’S **GROWING** CYBER CAPABILITY & **WILLINGNESS** TO WIELD IT

CROWDSTRIKE

FROM THE WESTERN CAPITALIST PIGS WHO BROUGHT YOU
NEIGHBORS AND THIS IS THE END
전쟁은 시작될것이다
SETH ROGEN JAMES FRANCO
이 무식한 미국놈들을 믿지 마십시오
THE INTERVIEW
인터뷰

SONY PICTURES ENTERTAINMENT

MOST DEVASTATING HACK IN CORPORATE HISTORY

- INTENDED TO PREVENT RELEASE OF **POLITICAL SATIRE**
- DATA **DESTRUCTION** – **100TB** DATA WIPED FROM HARD DRIVES
- SENSITIVE **LEAKS** – EMAILS, SALARY RECORDS, UNRELEASED FILMS
- ”GUARDIANS OF PEACE” > THINLY-VEILED DPRK **FAKETIVISM**
- **POLITICAL** CONDEMNATION, **SANCTIONS**, **CRIMINAL** CHARGES

CROWDSTRIKE

SANDS CASINO

STATE RETAILIATION AGAINST INDIVIDUAL

- DENIAL OF SERVICE & DATA DESTRUCTION ATTACK
- 75% OF VEGAS-BASED SERVERS DESTROYED > $40M IN DAMAGES
- PROVOKED BY GEOPOLITICAL STANCE OF CASINO OWNER
- DANGEROUS PRECEDENCE > STATE ATTACKS AGAINST PRIVATE SECTOR
- STATE'S RESPONSIBILITY TO PROTECT? CROSSING A REDLINE?

CROWDSTRIKE

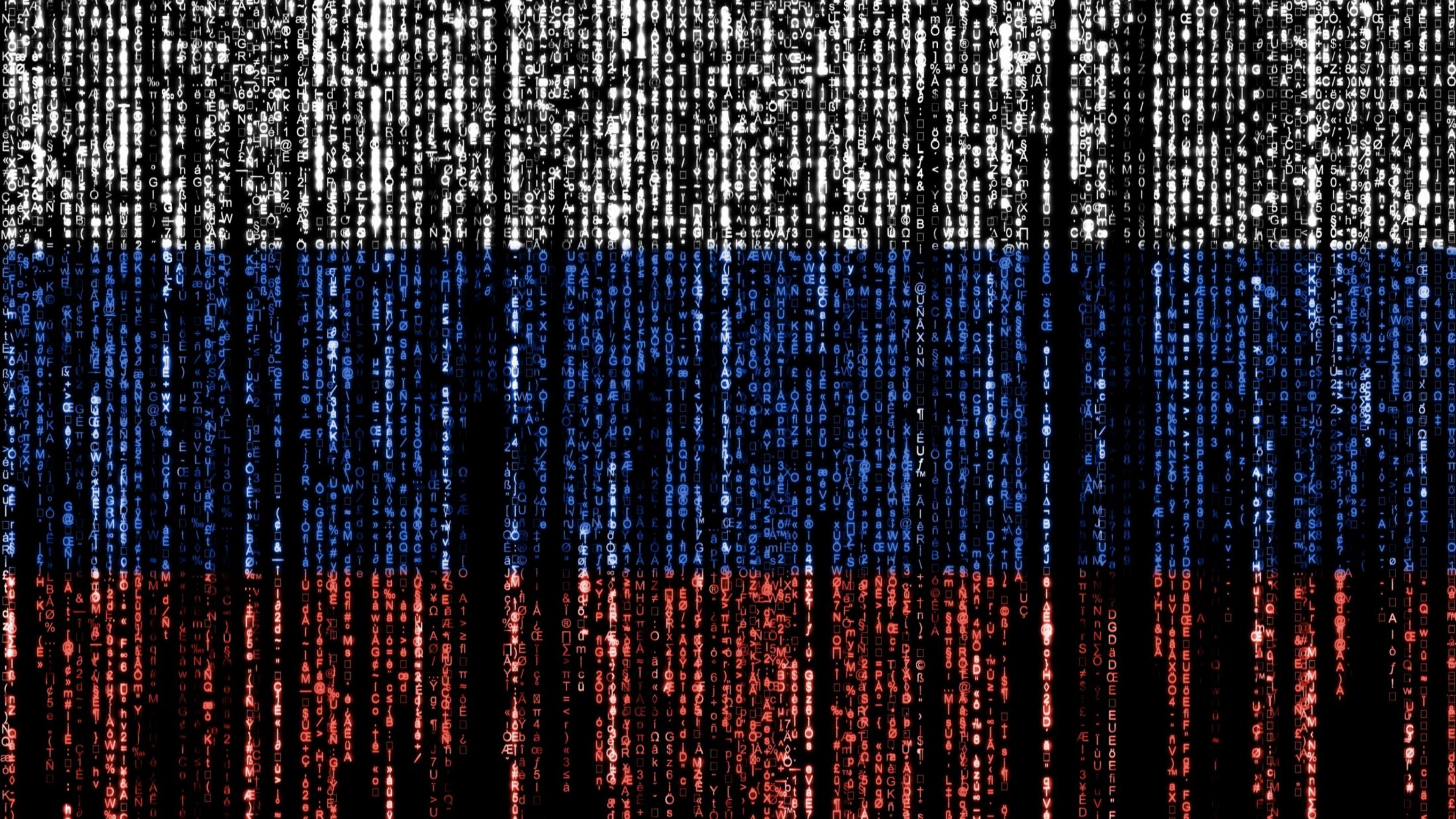
TRITON

WORLD’S MOST DANGEROUS MALWARE

- REMOTE **TAKE OVER** OF PETROL PLANT’S **SAFETY** INSTRUMENTATION
- TO **KICK IN** UPON DETECTION OF **DANGEROUS** CONDITIONS
- COULD HAVE CAUSED **RELEASE OF TOXIC GASES** OR **EXPLOSIONS**
- FLAW IN **MALWARE CODE** TRIGGERED A RESPONSE > DISCOVERY
- CODE **DESIGNED** TO PUT **LIVES AT RISK** > CROSS ANOTHER **RUBICON**?

CROWDSTRIKE

INTEGRATION INTO WARFARE



RUSSIAN INTRUSION ACTIVITY

THE ART OF (HYBRID) WAR

- KNOWN TO BE **MOST SOPHISTICATED** OF THE “BIG FOUR”
- OFFENSIVE CYBER **INTEGRATED** WITH KINETIC CAPABILITIES
- DEMONSTRATED ABILITY TO EFFECTIVELY TARGET **ICS/OT** SYSTEMS
- FULL **SPECTRUM** OF CYBER OPS – INTEL, INFO OPS, SABOTAGE, WAR
- **EXPANSIVE** VIEW OF HYBRID WARFARE + MAIN LINE OF **DEVELOPMENT**

CROWDSTRIKE

VOLT TYPHOON

PRE-POSITIONING FOR SABOTAGE

- MAY 2023 – DISCOVERY OF **CHINESE** ACTIVITY IN US **CRITICAL INFRA**
- MAINTAINED ACCESS FOR **>5 YEARS** – **PRE-POSITION** VS DATA EXFIL
- **DISRUPTIVE** / **DESTRUCTIVE** ATTACKS DURING CRISIS / CONFLICT
- CONTROL **BOTNETS** – **OPERATIONAL RELAY BOXES** FOR OPSEC
- FBI DIRECTOR > “**DEFINING THREAT** OF OUR GENERATION”

CROWDSTRIKE

FINANCIAL GAIN

RISE OF BANKING TROJAN

REVOLUTION IN ECRIME LANDSCAPE

- LEVERAGED THE CONCEPT OF A **TROJAN** MALWARE
- PURPOSE-BUILT FOR STEALING **CONFIDENTIAL BANKING INFO**
- TARGETS **BANK ACCOUNTS** AND **ONLINE PAYMENT SERVICES**
- **MAN-IN-THE-BROWSER** TECHNIQUES – WEB INJECTIONS + REDIRECTS
- THE BEGINNINGS OF **MALWARE-AS-A-SERVICE** – SCALING ECRIME

ZEUS

THE BANKING TROJAN OG

- FIRST OBSERVED IN THE WILD IN 2007 – **ANCESTOR** OF MOST TROJANS
- DISTRIBUTED THROUGH **SPAM** AND **DRIVE-BY DOWNLOADS**
- RUN **CMDS** AND **CONFIGS** FROM C2 + **WEB INJECTS** VIA API HOOKING
- OFFERED AS **MALWARE-AS-A-SERVICE**
- RETIRED IN 2010 + SOURCE CODE LEAKED IN 2011 > **NEW VARIANTS**

CROWDSTRIKE

GAME OVER ZEUS

FLOURISHING OF BANKING TROJANS

- MAJOR **ZEUS** VARIANT, DEVELOPED IN 2011
- INTRODUCED **PEER-TO-PEER** COMMUNICATIONS AS C2 METHOD
- STRUCTURE OF **HARVEST & PROXY BOTS** – C2 INTERMEDIARIES
- NO RELIANCE ON CENTRALIZED C2 – DIFFICULT TO **DETECT** & **TRACK**
- DISTRIBUTE **CRYPTOLOCKER RANSOMWARE** IN 2013

CROWDSTRIKE

CARBERP

BANKING TROJAN TO ORGANIZED ECRIME

- EMERGED IN 2010, TARGETED RUSSIAN AND UKRAINIAN **BANKS**
- SIMILAR FUNCTIONALITIES AS **ZEUS** – WEB INJECTION, INFO-STEALING
- DISTRIBUTED VIA **PHISHING** AND **SOCIAL ENGINEERING**
- MAJOR ARRESTS IN 2012 + SOURCE CODE LEAKED IN 2013 > **VARIANTS**
- FORMER MEMBERS FORM **CARBANAK** GANG – PROLIFIC ECRIME ACTOR

CROWDSTRIKE

CARBANAK GANG

RISE OF THE FINANCIALLY MOTIVATED "APT"

- EMERGED IN 2013, PIVOT TO **DIRECTLY** TARGETING BANKS
- STOLE **>$1B** FROM **>100** FINANCIAL INSTITUTIONS IN **>40** COUNTRIES
- GAIN FOOTHOLD VIA **SPEAR-PHISHING** THEN DEPLOYS CARBANAK
- CASH OUT WITH GANG CONTROLLED **ACCOUNTS** & **ATM HIJACKING**
- PRECURSOR TO **FIN7 / CARBON SPIDER** > BIG GAME HUNTING

CROWDSTRIKE

FIN7 / CARBON SPIDER

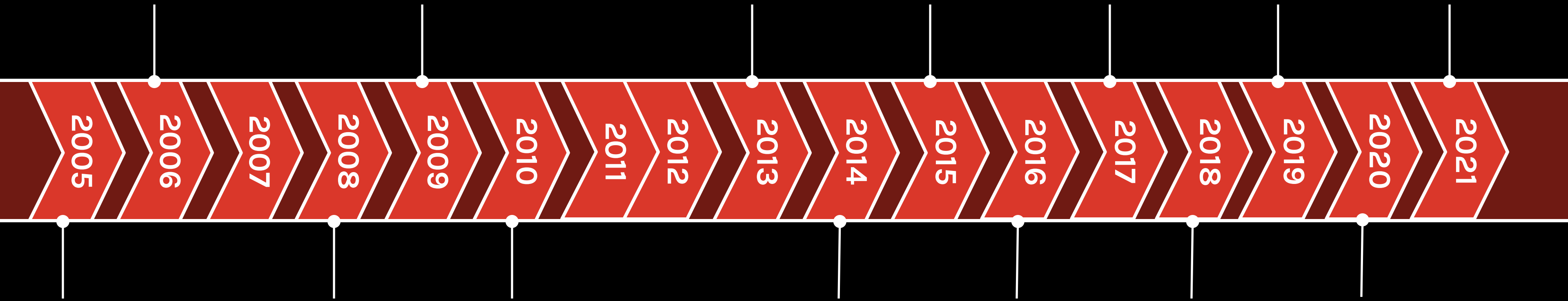
BIG GAME HUNTING RANSOMWARE

- TARGETED **RETAIL, F&B, HOSPITALITY** SECTORS IN THE US
- PIVOTED TO RANSOMWARE AS **REVIL AFFILIATE** IN 2020
- DEVELOPED THEIR **OWN** RANSOMWARE-AS-A-SERVICE - **DARKSIDE**
- RESPONSIBLE FOR THE **COLONIAL PIPELINE** ATTACK IN MAY 2021
- DECLARED “NO MORE” IN MAY 2023 BUT **RESURGENCE** IN APRIL 2024

CROWDSTRIKE

RANSOMWARE

BRIEF HISTORY OF RANSOMWARE



FIRST MODERN RANSOMWARE VARIANTS

RANSOMWARE GOES FROM 56 TO 660-BIT RSA ENCRYPTION

SCAREWARE DOMINATED BY FAKE AV & ROGUE UTILITIES

MALWARE EVOLVES TO ENCRYPTING FILES

SCAM FILEFIX PRO EXTORTS $40 TO “DECRYPT” FILES

10000 RANSOMWARE SAMPLES

BIRTH OF BTC

SCREEN-LOCKING RANSOMWARE APPEARS

OVER 100K SAMPLES

$200 RANSOMS

OVER 250K SAMPLES

CRYPTOLOCKER – $30M IN 100 DAYS

2048-BIT RSA ENRYPTION

$300 RANSOMS

OVER 4M SAMPLES

RAAS APPEARS

TESLACRYPT

JAVASCRIPT RANSOMWARE

LOCKY

HOSPITAL PAYS $17K RANSOM

$1B RANSOMWARE REVENUE

NATION STATE SPONSORED WANNACRY & NOTPETYA SPREAD WORLDWIDE

EMERGENCE OF BIG GAME HUNTING

BGH TARGETS LOCAL & STATE GOVERNMENTS

$460K LOCAL GOVT RANSOM PAYMENT

WIZARD SPIDER $100M IN REVENUE

330% INCREASE IN ECRIME DUE TO COVID-19 LURES

EXTORTION SCHEMES

RANSOMWARE ECOSYSTEM EVOLVES

RANSOMWARE CONTINUES TO RUN RAMPANT

COLONIAL PIPELINE ATTACK

ECRIME SOPHISTICATION

ZENITH OF BIG GAME HUNTING

- MAY 2021 - COLONIAL PIPELINE / DARKSIDE
- JUN 2021 – JBS / **REVIL**
- JUL 2021 – KASEYA / **REVIL**
- APR 2022 – COSTA RICA GOVERNMENT / **CONTI + HIVE**
- 2023 - RANSOMWARE PAYMENTS SURPASSED **$1B** MARK

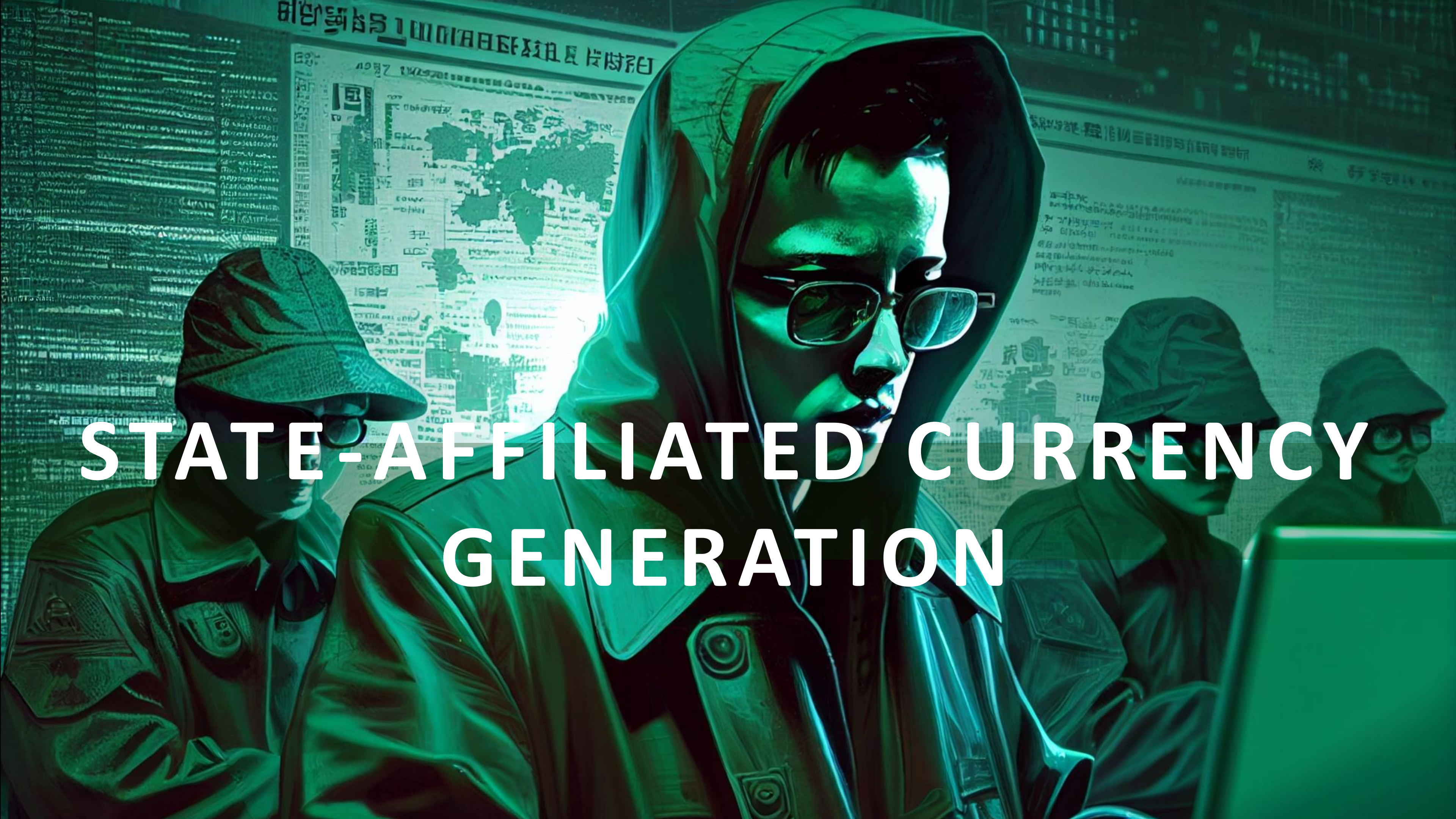
INDISCRIMINATE TARGETING

RANSOMWARE EVERYWHERE

- SCOURGE OF RANSOMWARE ATTACKS AT **SCHOOLS**, HOSPITALS, ETC
- RUSSIAN RANSOMWARE GROUPS OPERATE W/**TACIT APPROVAL**
- **LOCK-AND-LEAK** OPERATIONS BY IRAN NATION STATE ACTORS
- ECRIME GROUPS ARE GETTING **FASTER** & MORE **SOPHISTICATED**
- **INCREASINGLY TENUOUS** TO DIFFERENTIATE NATION STATE VS ECRIME

CROWDSTRIKE

STATE-AFFILIATED CURRENCY GENERATION



DPRK CURRENCY GENERATION

COMPELLED BY CIRCUMSTANCES

- CYBER-ENABLED **CURRENCY GENERATION** TO EVADE SANCTIONS
- EARLIER TARGETING OF **FINANCIAL INSTITUTIONS** – 2016 BANK HEIST
- SUSTAINED TARGETING OF **FINTECH** & **CRYPTOCURRENCY** EXCHANGES
- STOLE **$3B IN CRYPTOCURRENCY** BETWEEN 2017 TO 2023
- PROFICIENT IN **SOCIAL ENGINEERING** & CUSTOM TOOLING

CROWDSTRIKE

WHAT LIES YONDER?

GENERATIVE AI

LARGE LANGUAGE MODELS FOR CYBER

- EMERGENT TECH WITH **OFFENSIVE** & **DEFENSIVE** IMPLICATIONS
- DEMONSTRATED APPLICATION FOR **INFORMATION** OPERATIONS
- **ECRIME** ADOPTION – WORMGPT, FRAUDGPT, BLACKMAMBA
- NASCENT INDICATION OF MISUSE BY **STATE NEXUS** ADVERSARIES
- IMPLICATIONS OF **”PURPOSE-BUILT”** CYBER **LLMS** – MALWARE + TTPS

CROWDSTRIKE

QUANTUM COMPUTING

FUTURE OF ENCRYPTION & CRYPTANALYSIS

- BREAK COMMON ENCRYPTION METHODS AT ALARMING SPEEDS
- CHINESE CYBER OPERATIONS – **"COLLECT NOW, DECRYPT LATER"**
- COMMONLY PERCEIVED AS AN **"OUT OF SIGHT, OUT OF MIND"** ISSUE
- QUANTUM COMPUTING IS COMING **FASTER** THAN YOU THINK
- QUANTUM **READINESS** AND QUANTUM **SAFE CRYPTOGRAPHY**

CROWDSTRIKE

5G INFRASTRUCTURE

WORLD DOMINATION?

- 5G INFRASTRUCTURE TO FACILITATE **CYBER ESPIONAGE**
- **GEOPOLITICAL** IMPLICATIONS OF CHINA'S 5G INFRA DOMINANCE
- **SUPPLY CHAIN** THREATS – COUNTERFEIT + UNTRUSTED COMPONENTS
- **SYSTEM ARCHITECTURE** THREATS – LEGACY 4G VULNERABILITIES
- CHOOSE THE LESSER OF **"EVILS"** > "SLEEP IN THE BED **YOU MADE**"

CROWDSTRIKE

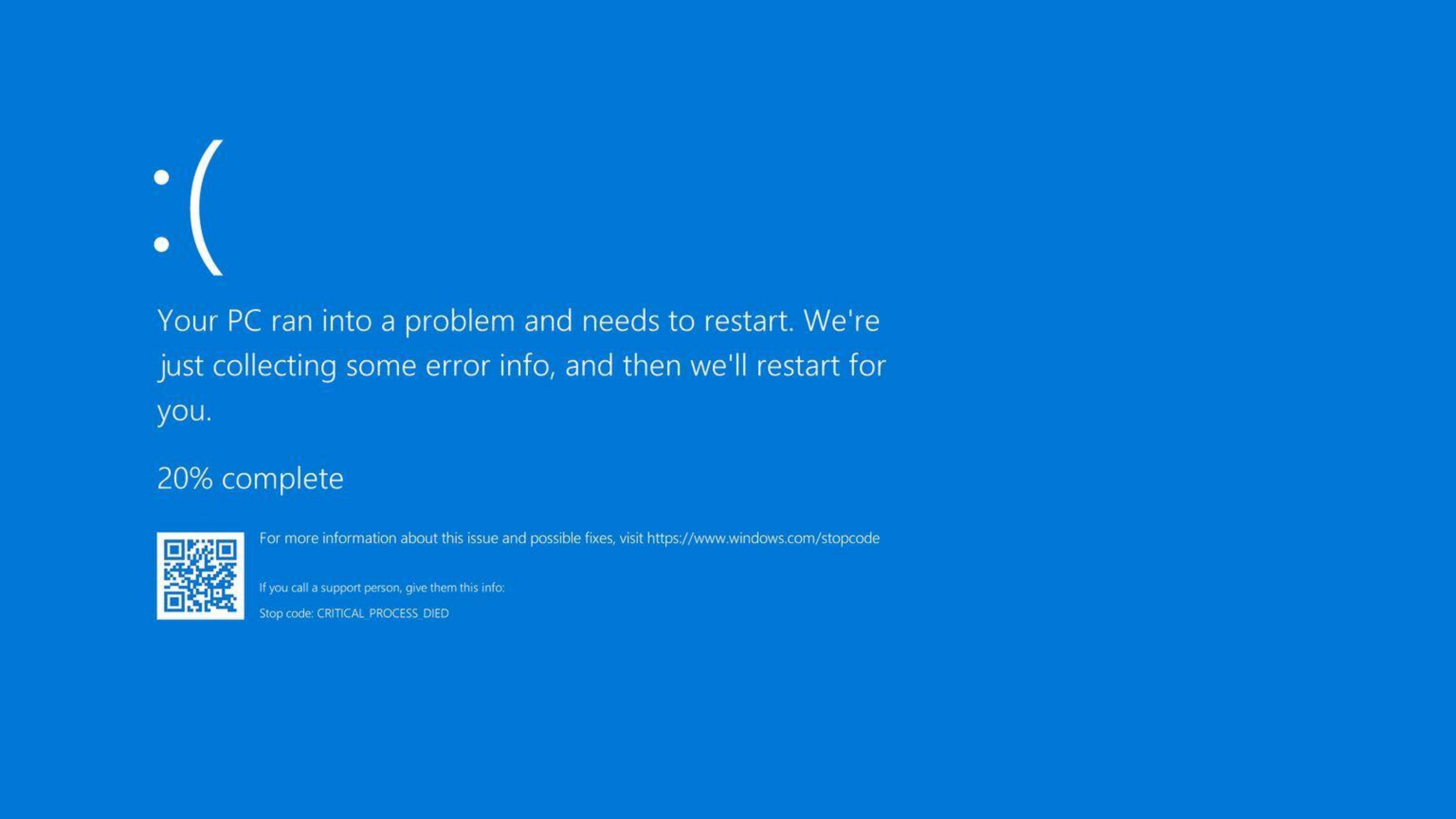
INTERNET OF THINGS

BOTNET ARMAGEDDON

- "IF IT'S **SMART**, IT'S **VULNERABLE**" – MIKKO HYPPÖNEN
- PERPETUATES THE SCOURGE OF **DDOS ATTACKS**
- OPPORTUNITIES FOR **ACCESS BROKERS** & **INFO STEALERS**
- **OPERATIONAL RELAY BOXES** FOR **SOPHISTICATED** ADVERSARIES
- FOREIGN & DOMESTIC **SURVEILLANCE** > PRIVACY & SECURITY

CROWDSTRIKE

UNINTENDED CONSEQUENCES



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED