Internet Economics and Financial Technology

Computer Science COMSM0019

Malware & Cybercrime

Dave Cliff

Department of Computer Science
University of Bristol

csdtc@bristol.ac.uk

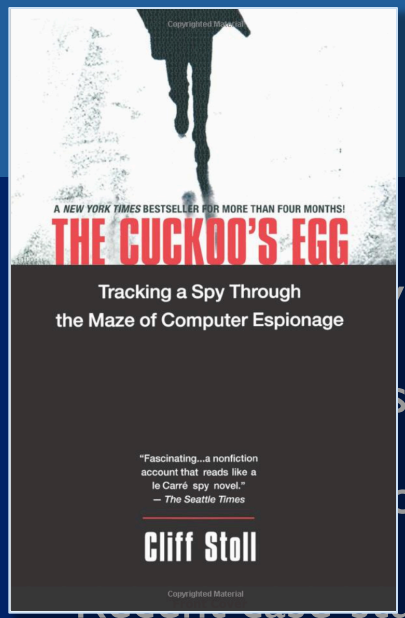
University of BRISTOL

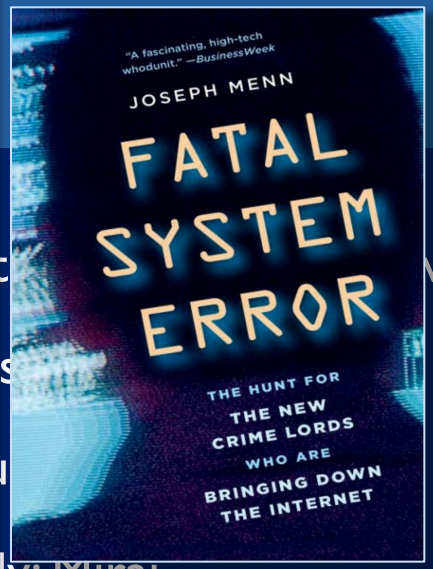
Why here?

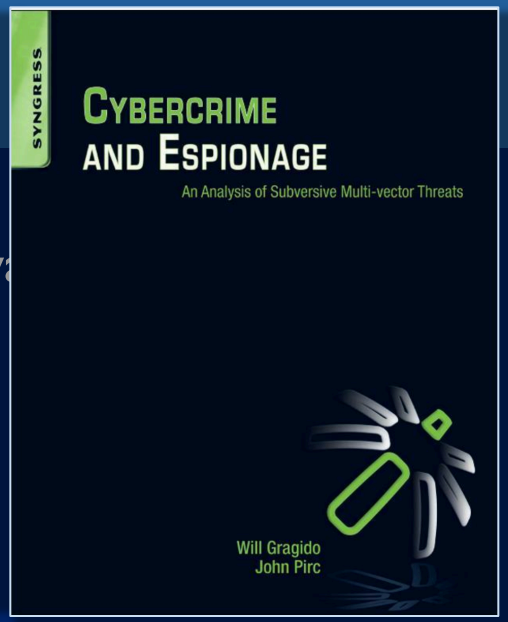
- Criminals target/fake fintech: does that make their work fintech too?
- Cybercrime/cybersecurity are forms of economic activity
- The internet facilitates many new forms of criminal activity, much of it financial
- This has major economic aspects:
  - Cybersecurity is a very big business
  - Cybersecurity failures can be very costly to clean up
  - Criminals can make a lot of money from malware-enabled scams and attacks
- Nation-states now major players too: cybercrime enabling cyberwarfare
  - No Geneva Convention on cyberwar, so anything goes: cyberwarcrime is undefined

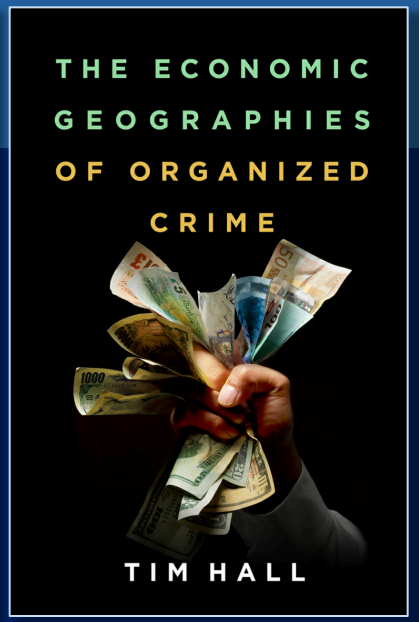
Le Menu

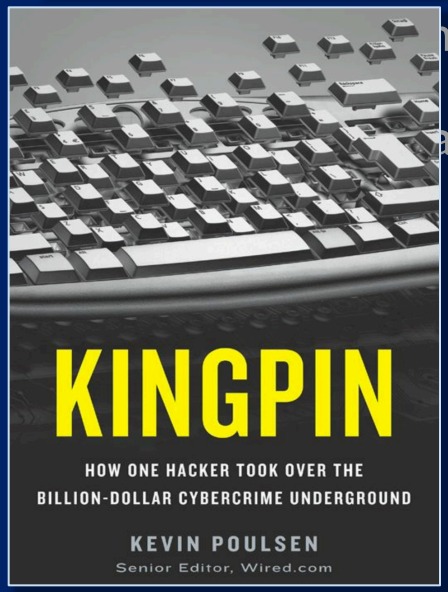
- A bit of history: the rise of viral malware
- Throttling viruses
- Going underground
- Security Economics

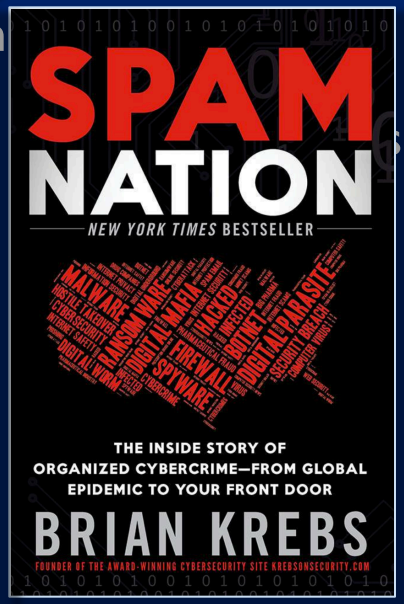

A NEW YORK TIMES BESTSELLER FOR MORE THAN FOUR MONTHS!
THE CUCKOO'S EGG
Tracking a Spy Through the Maze of Computer Espionage
"Fascinating...a nonfiction account that reads like a le Carré spy novel." — The Seattle Times
Cliff Stoll
Copyrighted Material

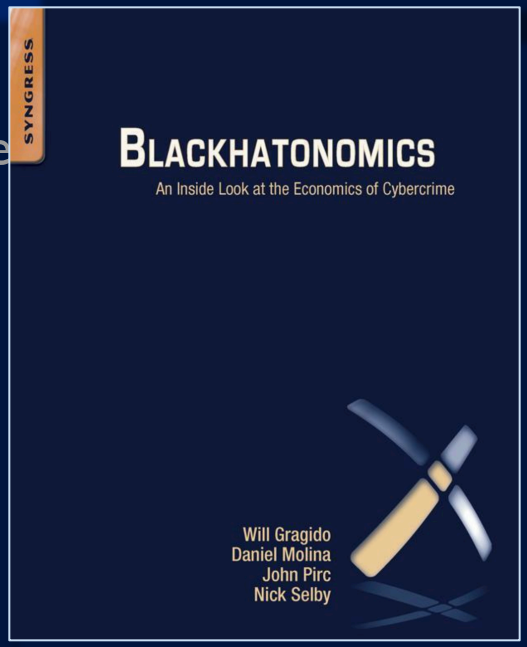

"A fascinating, high-tech whodunit." —BusinessWeek
JOSEPH MENN
FATAL SYSTEM ERROR
THE HUNT FOR THE NEW CRIME LORDS WHO ARE BRINGING DOWN THE INTERNET

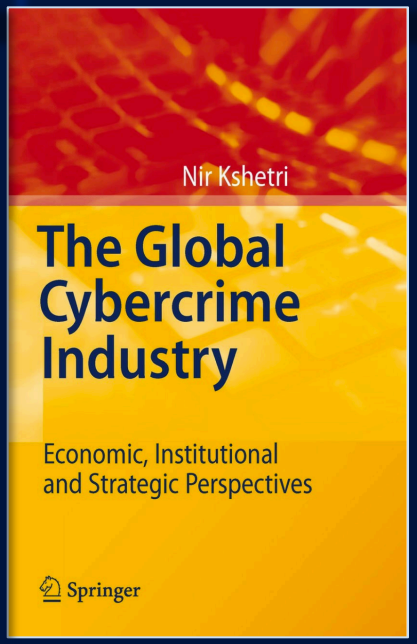

SYNGRESS
CYBERCRIME AND ESPIONAGE
An Analysis of Subversive Multi-vector Threats
Will Gragido
John Pirc


THE ECONOMIC GEOGRAPHIES OF ORGANIZED CRIME
TIM HALL


KINGPIN
HOW ONE HACKER TOOK OVER THE BILLION-DOLLAR CYBERCRIME UNDERGROUND
KEVIN POULSEN
Senior Editor, Wired.com


SPAM NATION
NEW YORK TIMES BESTSELLER
THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR
BRIAN KREBS
FOUNDER OF THE AWARD-WINNING CYBERSECURITY SITE KREBSONSECURITY.COM


SYNGRESS
BLACKHATONOMICS
An Inside Look at the Economics of Cybercrime
Will Gragido
Daniel Molina
John Pirc
Nick Selby


Nir Kshetri
The Global Cybercrime Industry
Economic, Institutional and Strategic Perspectives
Springer

SWIFT INSTITUTE

SWIFT INSTITUTE WORKING PAPER NO. 2016-004

FORCES SHAPING THE CYBER THREAT LANDSCAPE FOR FINANCIAL INSTITUTIONS

WILLIAM A. CARTER

PUBLICATION DATE: OCTOBER 2, 2017

The views and opinions expressed in this paper are those of the authors. SWIFT and the SWIFT Institute have not made any editorial review of this paper, therefore the views and opinions do not necessarily reflect those of either SWIFT or the SWIFT Institute.

CYBERCRIME AND ESPIONAGE

An Analysis of Subversive Multi-vector Threats

Will Gragido
John Pirc

THE ECONOMIC GEOGRAPHIES OF ORGANIZED CRIME

TIM HALL

BILLION-DOLLAR CYBERCRIME UNDERGROUND

KEVIN POULSEN

Senior Editor, Wired.com

BRIAN KREBS

FOUNDER OF THE AWARD-WINNING CYBERSECURITY SITE KREBSONSECURITY.COM

SYNGRESS

BLACKHATONOMICS

An Inside Look at the Economics of Cybercrime

Will Gragido
Daniel Molina
John Pirc
Nick Selby

Nir Kshetri

The Global Cybercrime Industry

Economic, Institutional and Strategic Perspectives

Springer


Cybercrime and Espionage
An Analysis of Subversive Multi-vector Threats
Will Gragido
John Pirc
THE ECONOMIC GEOGRAPHIES OF ORGANIZED CRIME
TIM HALL
Computer Viruses and Other Malicious Software
A THREAT TO THE INTERNET ECONOMY
OECD
CKHATONOMICS
Look at the Economics of Cybercrime
Will Gragido
Daniel Molina
John Pirc
Nick Selby
Nir Kshetri
The Global Cybercrime Industry
Economic, Institutional and Strategic Perspectives
Springer

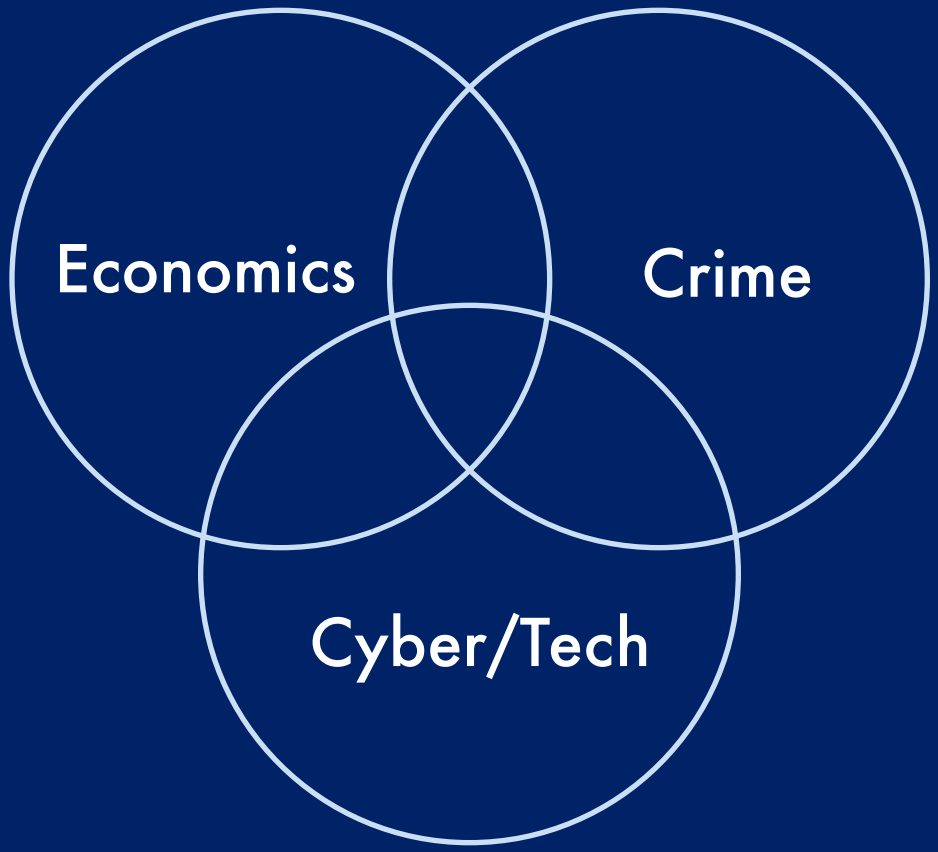

OECDpublishing
Please cite this paper as:
van Eeten, M. J. and J. M. Bauer (2008), "Economics of Malware: Security Decisions, Incentives and Externalities", OECD Science, Technology and Industry Working Papers, 2008/1, OECD Publishing.
doi: 10.1787/241440230621
OECD Science, Technology and Industry Working Papers 2008/1
Economics of Malware
SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES
Michel J. van Eeten, Johannes M. Bauer
OECD
THE ECONOMIC GEOGRAPHIES OF ORGANIZED CRIME
TIM HALL
Nir Kshetri
The Global Cybercrime Industry
Economic, Institutional and Strategic Perspectives
Springer


THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE
Center for Strategic and International Studies
July 2013
Report
McAfee
An Intel Company
OECDpublishing
OECD
THE ECONOMIC GEOGRAPHIES OF ORGANIZED CRIME
TIM HALL
Nir Kshetri
Springer
John Pirc
Nick Selby
KEVIN POU
Senior Editor, W


Report
Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity
Center for Strategic and International Studies
intel Security
OECDpublishing
THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE
Center for Strategic and International Studies
July 2013
Report
OECD
OECD
BILLION-DOLLAR CYBERCRI
KEVIN POU
Senior Editor, W
John Pirc
Nick Selby
Springer


Report
Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity
Center for Strategic and International Studies
OECDpublishing
THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESP
July 2013
OECD
REPORT
McAfee
Together is power.
Economic Impact of Cybercrime— No Slowing Down
February 2018
CSIS

Le Menu



But first… some terminology

- Virus: a program that copies itself via attachment to "host" code
  - When the host code is moved by a user, the virus moves with it
- Worm: self-replicating program that needs no host, no user intervention
- Trojan: malware that masquerades as something else, invites the user to run it
- Rootkit: malware that runs concealed from normal user-process monitoring
  - As if it had "root" administrator privileges
- Backdoor: a route into a system that bypasses security measures
- Zombie: a machine controlled via backdoor/rootkit techniques
- Botnet: a network of several zombies, controlled as one distributed facility
- Ransomware: malware that encrypts files and demands a ransom to decrypt it
- Phishing: fake emails that appear to come from trusted sources, asking for details
- Whitehat: malware/attack developed for benign purposes (cf Blackhat)

Economics

- Standard PC/server security market is significant
- 2012: Symantec ranked 6th biggest software company in the world by revenue
  - Software revenues in 2012: c. $6.4Bn;
  - 2018 c.$4.5Bn (Kaspersky $0.7Bn; McAfee HOWMUCH?)
- These companies make *legitimate* profits/gains from combating computer crime
- If X attacks Y with denial of service, Y loses revenue (=cost to Y)
- If X attacks Y with a virus/worm, Y pays for cleanup (=cost to Y)
- If X phishes passwords from Y, X can steal money/data from Y (Y loss; X gain)
- If X zombies Y's PC into a botnet, Y's PC works for X (Y cost, X gain)
  - X can charge users of the service now provided by Y (e.g. spam, phishing, porn sites)

Baby-steps…

Financial Impact of Malware Attacks 1997–2006

	Worldwide Impact (U.S. $)
2006	$13.3 Billion
2005	14.2 Billion
2004	17.5 Billion
2003	13.0 Billion
2002	11.1 Billion
2001	13.2 Billion
2000	17.1 Billion
1999	13.0 Billion
1998	6.1 Billion
1997	3.3 Billion

Source: Computer Economics, 2007

Figure 1

Source: http://www.computereconomics.com/article.cfm?id=1225

2014 Estimate: $491 Bn - SC Magazine: IDC / Uni of Singapore

CSO Online: Oct 2018 Summary

No 2019 Summary yet

https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html

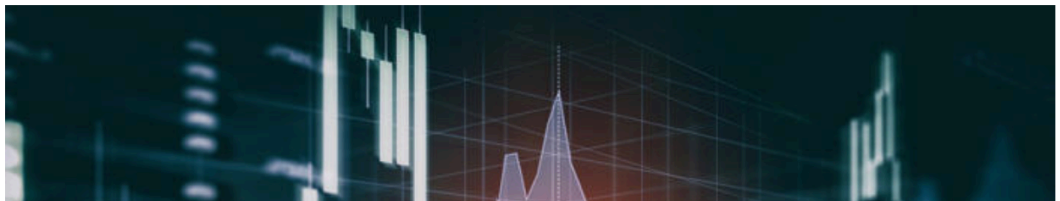
TODAY'S TOP STORIES

Top cybersecurity facts, figures and statistics for 2018

Some hard numbers from studies and surveys give you a sense of the state of cybersecurity.

By Josh Fruhlinger

CSO | OCT 10, 2018 9:52 AM PT



MORE LIKE THIS

What is cryptojacking? How to prevent, detect, and recover from it

CSO Online: Oct 2018 Summary

https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html

Ransomware is down, cryptomining is up

"With last year's outbreak of NotPetya [and Wannacry?] ransomware … became one of the most talked about forms of malware of 2017. Yet at the same time, the actual rates of malware infection began to plummet around the middle of the year, until by December 2017 it represented only about 10 percent of infections. "

"What happened? Well, it seems attackers have figured out that you catch more flies with honey than with vinegar, and rather than demanding your victims send you bitcoins, you can just infect their computers with bitcoin-mining software without their noticing instead. By early 2018, 90 percent of all remote code execution attacks were associated with cryptomining."

CSO Online: Oct 2018 Summary

https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html

Email is still the problem

- According to Verizon's 2018 Breach Investigations report, 92 percent of malware is still delivered by email.

- One of the most common methods of email malware infection is through phishing attacks, which are becoming increasingly targeted. And security pros are taking notice. Out of the 1,300 IT security decision makers surveyed for CyberArk Global Advanced Threat Landscape Report 2018, 56 percent said that targeted phishing attacks were the top security threat they faced.

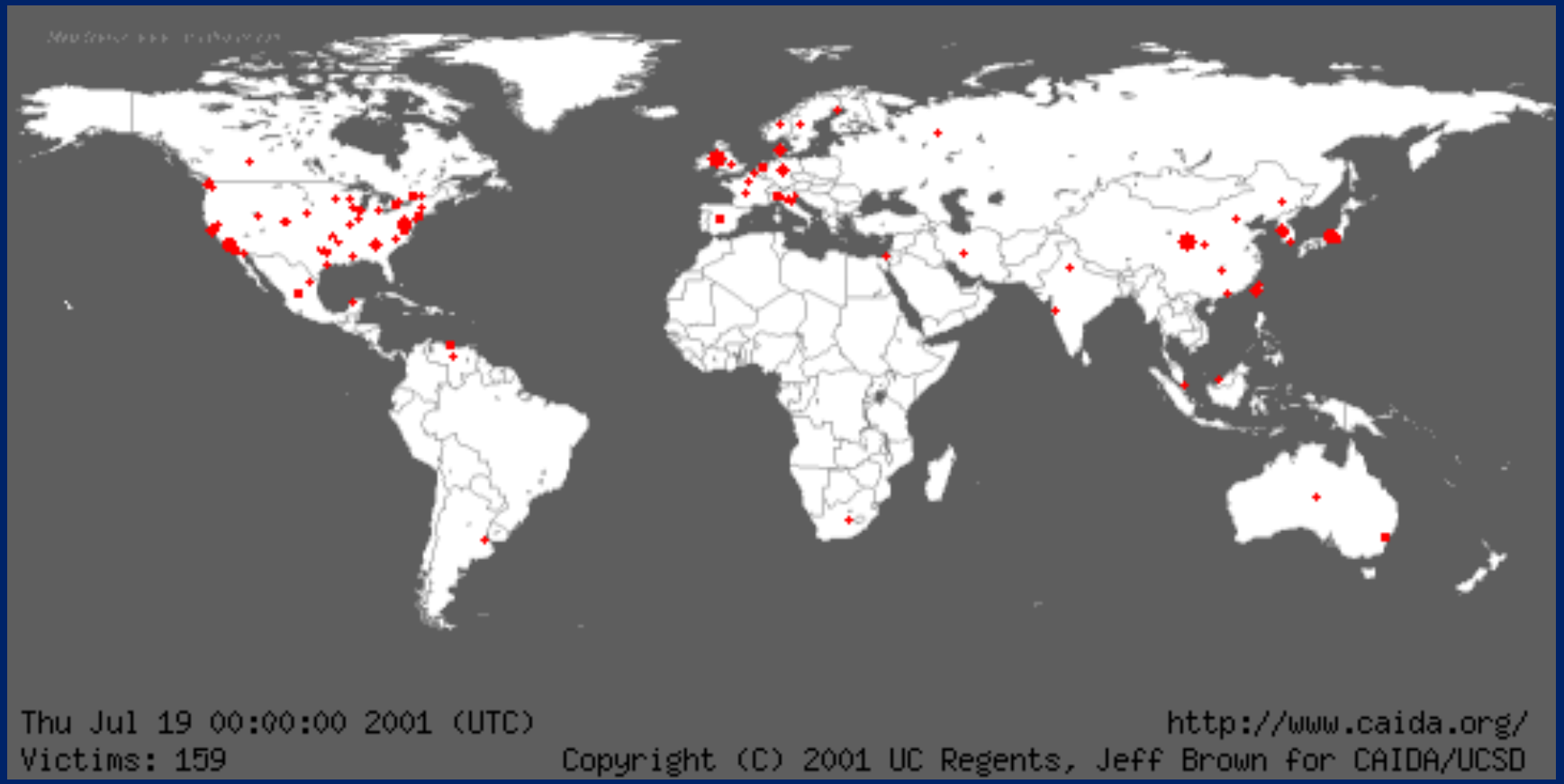
Malware: the early days

- 1970s: a few isolated, harmless, non-malicious "hack" viruses
- 1982: Apple II operating system floppies infected by *Elk Cloner*
  - First large-scale infection by replicating code
- 1983/84: "Computer Virus" phrase coined by Fred Cohen
- 1986: *Brain Boot Sector* virus is first to infect IBM PCs
- 1987: IBM release first antivirus software product to customers
- 1987: *Christmas Tree* is first to spread via email address book, paralyses several major networks e.g. EARN, BITNET, VNET
- 1989: Morris Worm: first widespread internet release (via Unix, buffer overrun)
- 1989: *Ghostball* is first multipartite virus (>1 vector: boot sector and .exe)
- 1990: *1260* introduces polymorphic malware to evade pattern-detector antivirals

Post-1990

- 1995: *Concept Virus* first to attack via MSWord macros
- 1998: *CIH* family of "spacefillers"
  - code sliced into "cavities" so that infected files don't alter in size
- 1999: *Melissa* mass-mailing macro virus causes widespread shutdown of email
- 2000: *ILoveYou* worm infected approx 10% of all machines on the internet.
  - Spread via email address books: opening the email auto-executed a visual basic script to send the message on to all the host's contacts (plus trashing important files on the host). Many mail servers collapsed under the sudden spike in activity. Estimated $5.5bn clean-up costs. Pentagon, CIA, and UK Parliament all had to shutdown email systems, as did many large corporations (cf Christmas Tree?)
- 2001: *CodeRed* buffer-overrun in MSFT InternetInfoService (IIS)
  - Copied itself to multiple hosts, then sat dormant for DoS attack on a number of fixed IP addresses, including www.whitehouse.gov. 359,000 hosts with peak infection rate of 2,000/min. IIS patch had been available for months
- *CodeRed2* followed a few months later

CodeRed world tour



And then it gets really nasty

- 2001: *Nimda* uses multiple vectors (email, network file sharing, web browsing, MSFT IIS vulnerabilities [again], and backdoors left by *CodeRed2)* allowed very rapid spread: 22mins to do what Code Red did in three days: a "Zero Hour" attack. Damage=$635m
- 2003: *SQL Slammer* exploited buffer overflow in MSFT SQL Server caused major DoS and slowed entire internet: 150,000-200,000 victims. SQL Patch had been available for months (just like *Code Red*)
- 2003: *MSBlaster* launched a distributed DoS attack on Microsoft IP domain, from thousands of host-victims including BMW and Federal Reserve Bank of Atlanta
- 2004: *MyDoom* infected 1M machines before launching a distributed DoS attack on Microsoft and SCO Group.
- 2004: *Sasser* exploits buffer overflow in WinXP/2k and forces cancellation of 40 Delta Airlines transatlantic flights, Australian trains, Australian Banks, etc.
- 2004: *Witty* specifically attacks security/antivirus software (but for a single vendor: IBM) – cf HIV.
- What if someone develops a multi-vendor *Witty,* with *Nimda* multiple vectors?

HP Virus Throttle

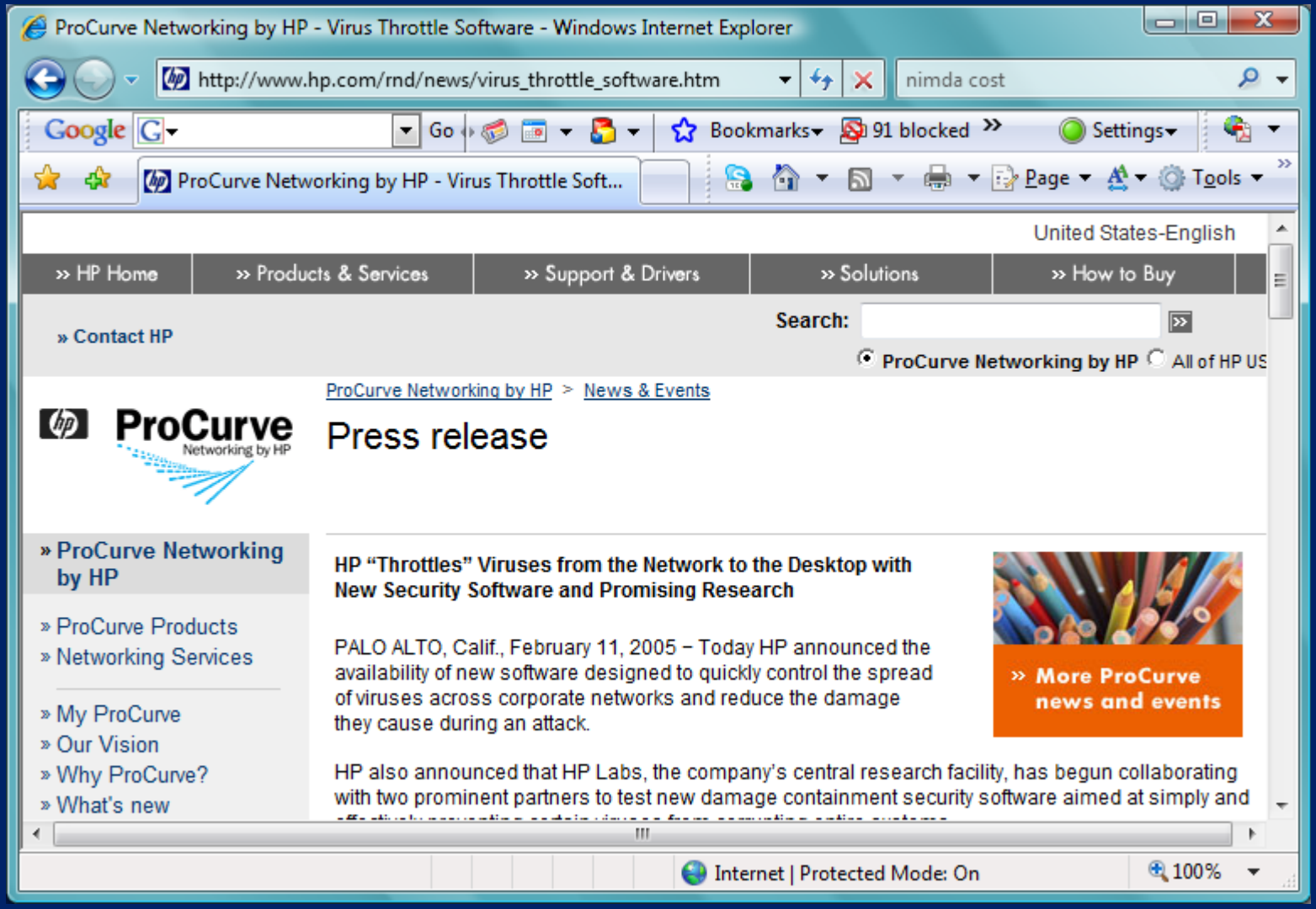
- J. Twycross and M. Williamson (2003) *Implementing and Testing a Virus Throttle*.
  - HP Labs Technical Report HPL-2003-103
- Traditional signature-based approaches are case-by-case and increasingly defeated by polymorphism, cavity-filling (e.g. CIH), and memory-residency
- Three key innovations:
  - Focus on *network behavior* of the virus (lots of connections per second)
  - Doesn't stop mobile code from entering the system: instead, stops it from leaving
  - Outgoing connections are delayed, not dropped, so is robust to false positives
- Make network nodes "socially responsible" so that they "withdraw from society" if/when they believe they have an infection – like when we get sick with flu
- Monitor self activity; if suddenly making many more connections than normal, *throttle back* and alert operator – this *throttles* the virus

HP Virus Throttle: results from live test-bed

connections per second	stopping time	allowed connections
Nimda		
120	0.25s	1
Test Worm		
20	5.44s	5
40	2.34s	2
60	1.37s	1
80	1.04s	1
100	0.91s	1
150	0.21s	0
200	0.02s	0
SQLSlammer		
850	0.02s	0

Figure 3: Average time taken by the throttle to stop real and test worms

HP Virus Throttle: released as a product (Feb 2005)



HP Virus Throttle: in ProCurve routers (Dec 2006)

How might the throttle be defeated?

- Like most/all security measures, the throttle is not a universal panacea
- It limits the rate of fast-spreading viruses, which is great
- Signature-based approaches for immunization are still very valuable

- With a bit of cunning, it may be possible to come up with a way around throttling

- The clue:

How you boil a frog without worrying it….

And more…

- 2006 – Oompa-A - First MacOS-X virus (trojan)
- 2007 – Storm Worm -> Storm Botnet: 1.7M infected machines, used to send Spam for payment in the 'Black Hat' economy.
- 2008 – Stormf**ker – Takes over parts of the Storm botnet.
- Competition between Storm and another botnet – Nugache – allegedly resulted in a price-war for the distribution of spam in the black hat economy.

- 2008-09 –*Conficker* – largest infection since SQLSlammer;
  - 9-15M machines in 3 months following No'v08 release; (hits French Navy, UK MoD, UK Houses of Parliament; Manchester City Council; Greater Manchester Police; etc.)
  - **Sits and waits,** then uploads revised versions of itself; with different properties and vectors. The owners also actively modify the virus: finally downloads & installs *Waledec* botnet payload in Apr09.
- 2007-09: *Zeus* massive banking/finance-specific keylogger botnet: 3.6M machines in USA alone (still active)

…and on and on….

- PGPCoder 2010, then Cryptolocker 2013
- "Ransomware": trojan infects machine, encrypts it, then you have to pay money (BitCoin) to get the decryption key
- …if the criminals actually decide to give it you ☺
- Attackers say that they will delete the key if payment not made via a set deadline; seems that actually they often just set a new deadline but increase the ransom.
- Symantec estimate that 3% of victims pay up.

- Oct 2016: Mirai botnet causes major disruption: Twitter, Spotify, Paypal all adversely affected.

- May 2017: Wannacry ransomware hits NHS, costs £100M+.

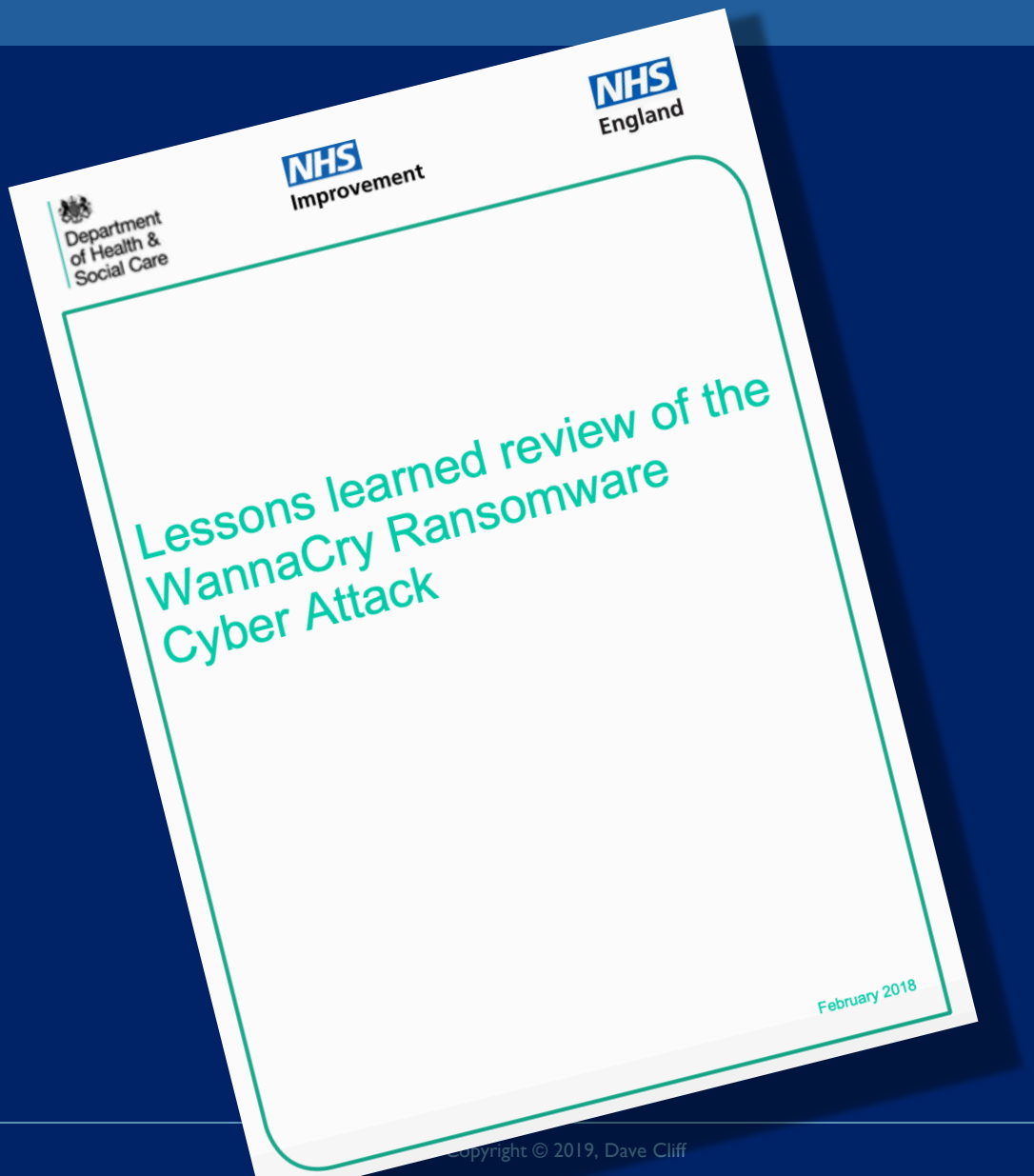
- April 2018: Russian state-sponsored attack on domestic internet routers

Mirai: 500Knode DDoS battle for Minecraft hosts

USER:	PASS:	USER:	PASS:
root	xc3511	admin1	password
root	vizxv	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdipc	root	klv1234
root	default	root	Zte521
root	juantech	root	hi3518
root	123456	root	jvbzd
root	54321	root	anko
support	support	root	zlxx.
root	(none)	root	7ujMko0vizxv
admin	password	root	7ujMko0admin
root	root	root	system
root	12345	root	ikwb
user	user	root	dreambox
admin	(none)	root	user
root	pass	root	realtek
admin	admin1234	root	00000000
root	1111	admin	1111111
admin	smcadmin	admin	1234
admin	1111	admin	12345
root	666666	admin	54321
root	password	admin	123456
root	1234	admin	7ujMko0admin
root	klv123	admin	1234
Administrator	admin	admin	pass
service	service	admin	meinsm
supervisor	supervisor	tech	tech
guest	guest	mother	fucker
guest	12345		

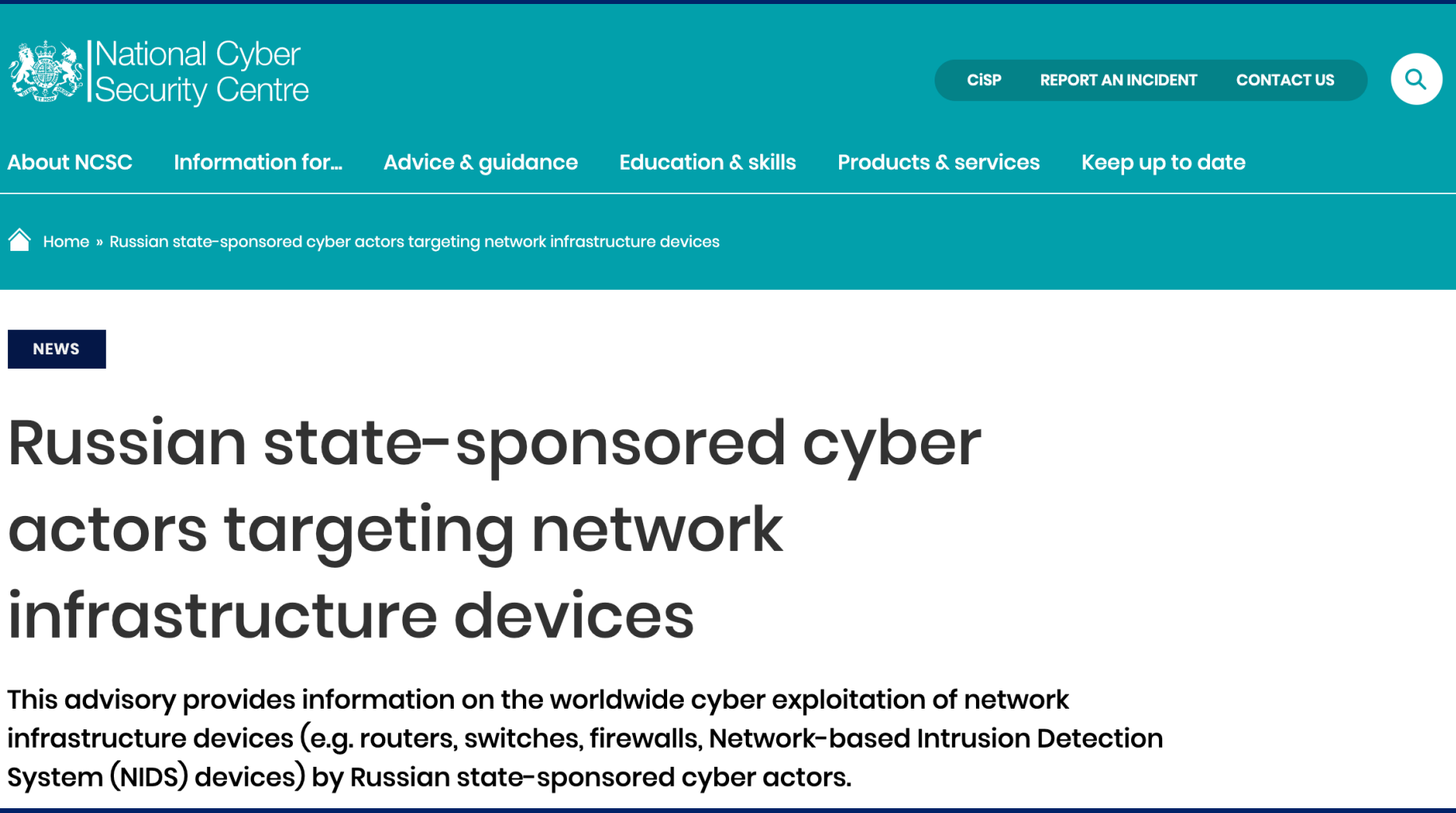
Wannacry postmortem report (Feb 2018)

https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf



UK NCSC (Apr 2018) Report on Russian attack

https://www.ncsc.gov.uk/news/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices



Russia is not the only state that engages in cyberwar…

Operation Olympic Games: Stuxnet & descendants

- US/Israeli program of cyber-sabotage, in development since ?2005?
- Believed to be USA's (or any nation's) first sustained use of cyber-weapons
- Targeting Iran's nuclear enrichment facilities
- 'Stuxnet' accidentally escaped due to a programming error; discovered in 2010
  - Error led Stuxnet to infect an engineer's laptop; took it home and it spread onwards
- Very precise targeting: only attacks Siemens control software controlling two specific brands of motor, when they spin at a specific speeds
  - Disrupts the spinning, prevents desired operation of centrifuge

- Sep 2011: Duqu identified as a close relative/descendant of Stuxnet, but targeted at keylogging and similar forms of data-capture & exfiltration
- May 2012: Flame, another relative of Stuxnet "the most sophisticated malware ever" spreads via USB and LAN; can record audio, keylogs, screenshots, network traffic, and Skype. Acts as beacon for nearby Bluetooth devices
- Dec 2017: Triton, another Stuxnet relative, attacks safety systems of a nuclear power station, suspected of being in Saudi Arabia.

Flame

ars TECHNICA

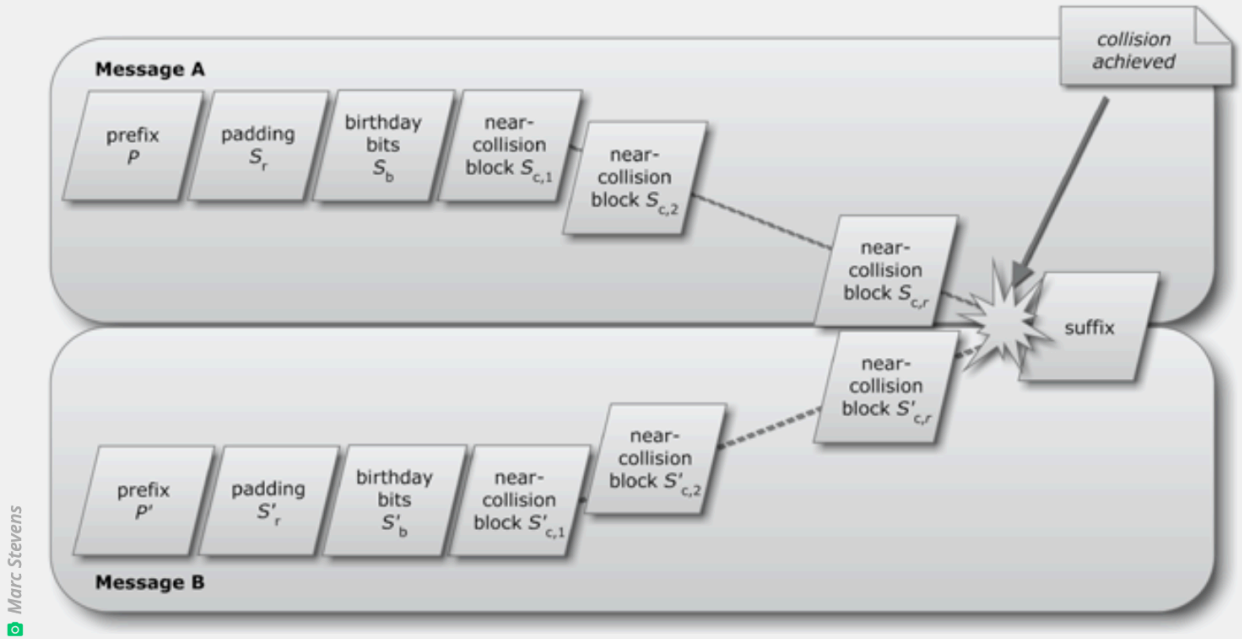
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STO

BIZ & IT —

Crypto breakthrough shows Flame was designed by world-class scientists

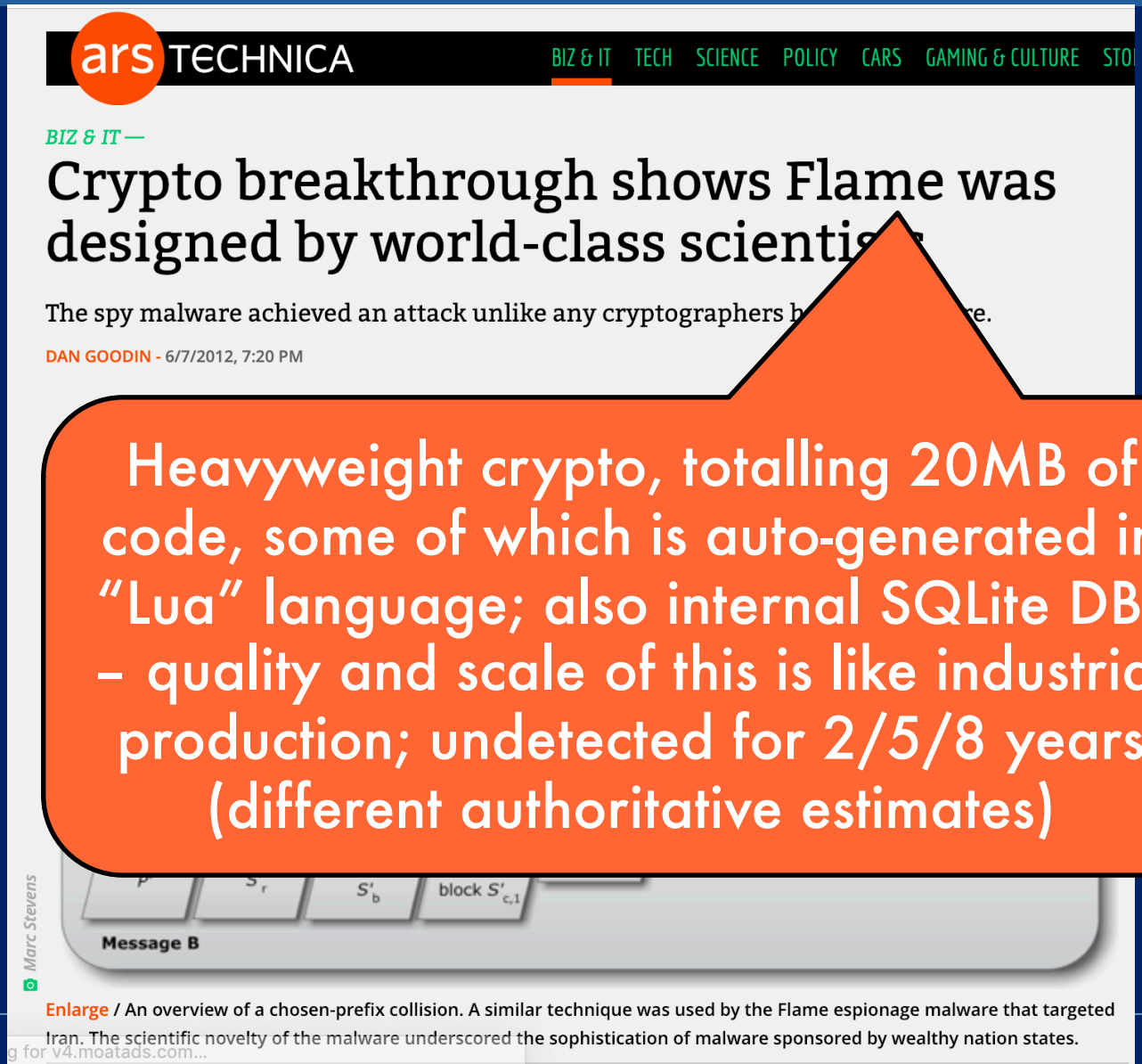
The spy malware achieved an attack unlike any cryptographers have seen before.

DAN GOODIN - 6/7/2012, 7:20 PM



Enlarge / An overview of a chosen-prefix collision. A similar technique was used by the Flame espionage malware that targeted Iran. The scientific novelty of the malware underscored the sophistication of malware sponsored by wealthy nation states.

Flame


ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLICY
CARS
GAMING & CULTURE
BIZ & IT —
Crypto breakthrough shows Flame was designed by world-class scientis
The spy malware achieved an attack unlike any cryptographers h re.
DAN GOODIN - 6/7/2012, 7:20 PM
Heavyweight crypto, totalling 20MB of code, some of which is auto-generated in "Lua" language; also internal SQLite DBs – quality and scale of this is like industrial production; undetected for 2/5/8 years (different authoritative estimates)
block $S'_{c,1}$
Message B
Marc Stevens
Enlarge / An overview of a chosen-prefix collision. A similar technique was used by the Flame espionage malware that targeted Iran. The scientific novelty of the malware underscored the sophistication of malware sponsored by wealthy nation states.

Characterizing the current situation (Gragido & Pirc, Ch.7)

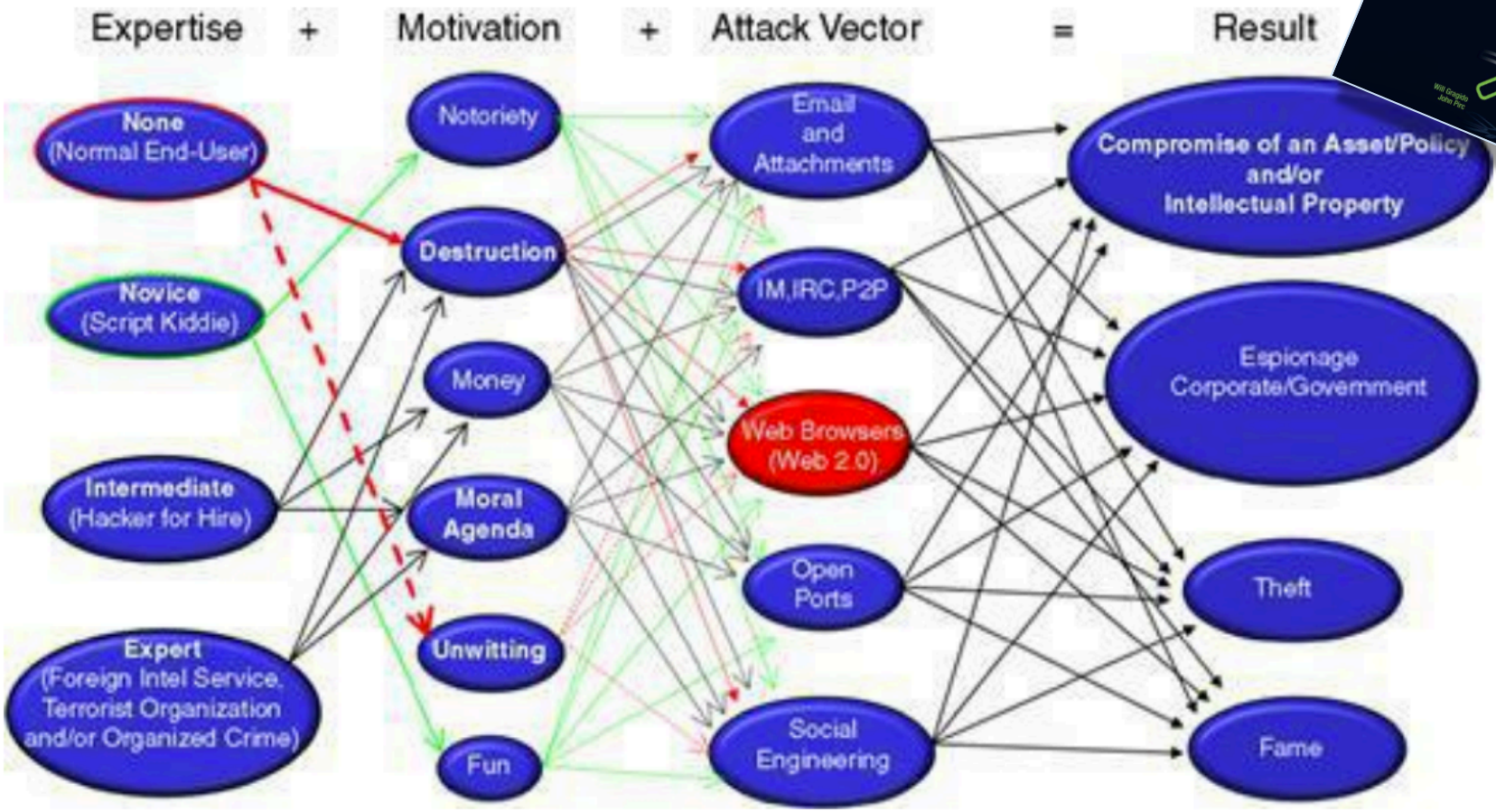


Figure 7.1 Classification at a glance.

Characterizing the current situation (Gragido & Pirc, Ch.7)

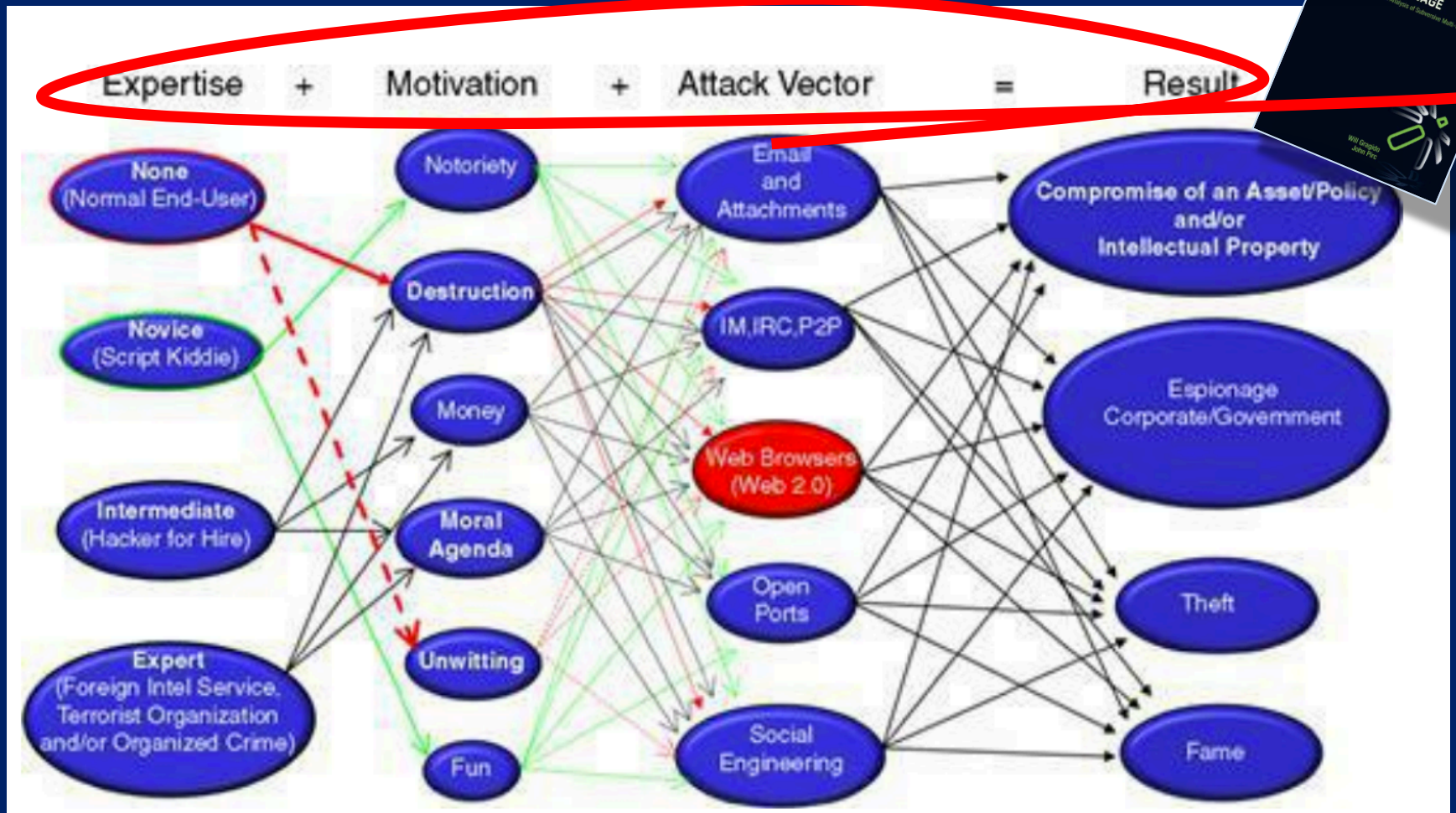


Figure 7.1 Classification at a glance.

Characterizing the current situation (Gragido & Pirc, Ch.7)

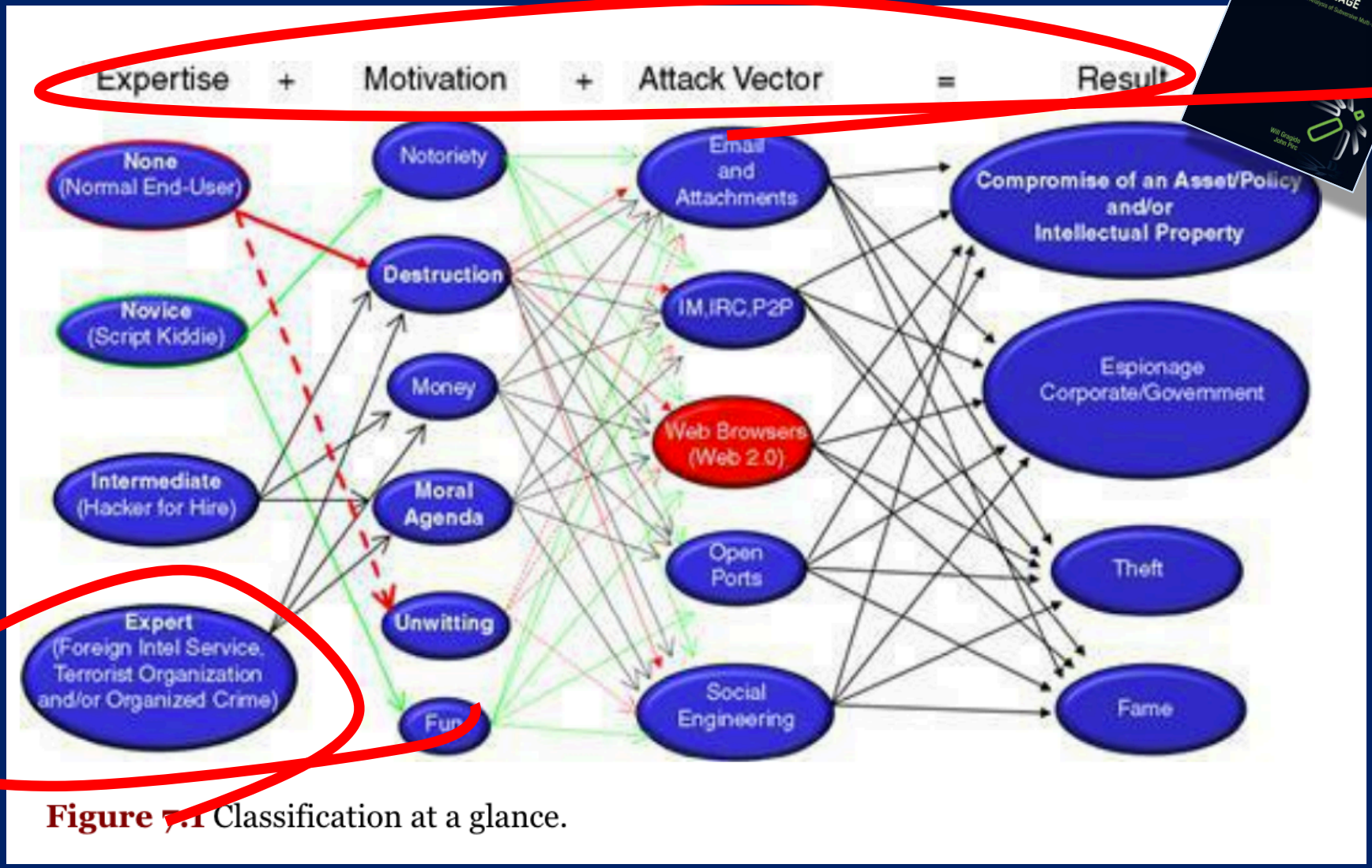
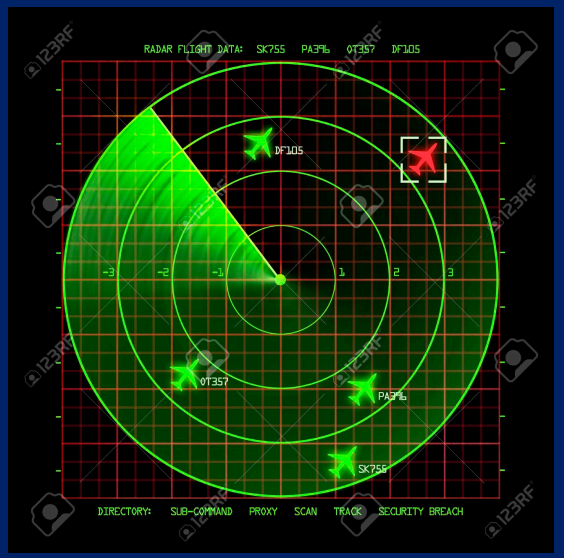


Figure 7.1 Classification at a glance.

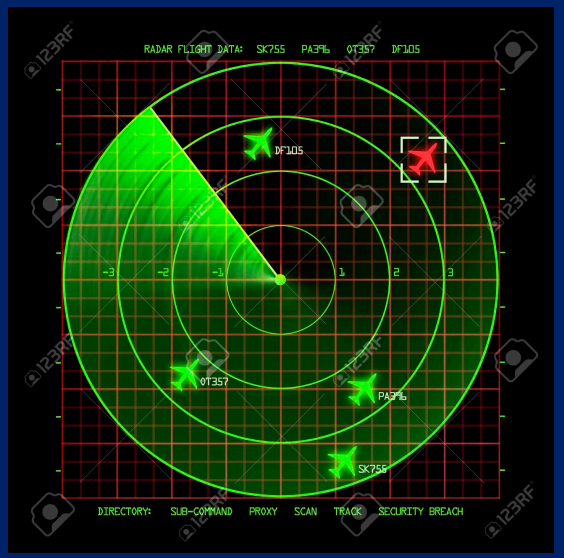
Cyber WAR! WHAT IS IT GOOD FOR?

Cyber WAR! WHAT IS IT GOOD FOR?



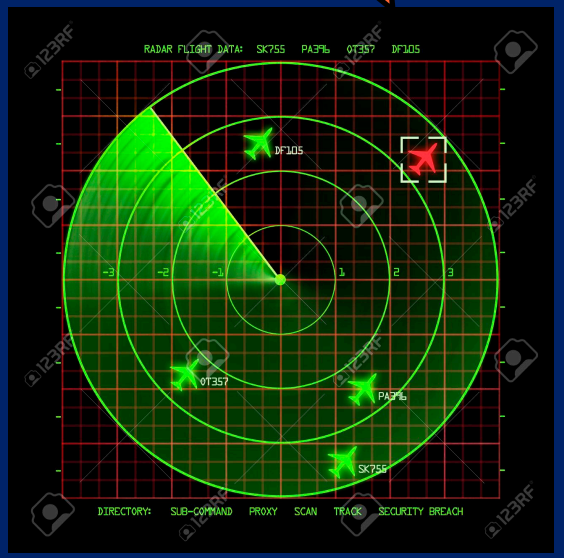
Cyber WAR! WHAT IS IT GOOD FOR?

Military hardware commissioning costs are hugely expensive (wrt attack-by-software)



Cyber WAR! WHAT IS IT GOOD FOR?

Anti-detection countermeasures difficult/expensive for military hardware; stealthy software cheaper



Vulnerability Disclosure

- Security companies and consultants would spot vulnerabilities and disclose them publically ('Full Disclosure')
- They argued that this would force software companies to improve security and release patches.
- It also generated publicity for the security companies, and possibly lucrative consultancy contracts….
- Did it improve security…? Or give hackers information…?
- Move to 'Responsible Disclosure': Tell the software company in advance to give them a head start in developing a patch, then go public a while later

The Vulnerabilities Market

- Software vulnerabilities have costs to find: time, expertise.
- Software vulnerabilities have a value.
  - 'Black Hat' hackers can gain direct economic benefit.
  - SW companies can make their SW more secure.
  - Security agencies can conduct surveillance and cyber-warfare.

- So an informal 'marketplace' has developed…
  - Companies identify vulnerabilities, and sell them to the highest bidder…
  - Small specialist companies, and large defense contractors

‘Security for the 1%....’

- ‘Ethical’ sellers sell only to ‘NATO-approved governments’.
- These pay more than the original SW company
- The SW therefore remains vulnerable: Security researchers that would formerly have disclosed information do not.
- Hence it leads to less secure SW, with government agencies holding the levers….
- Furthermore, even ‘ethical’ sellers may be fooled into selling to a black hat organisation, due to the use of ‘middlemen’.

Economics of Information Security

- Ross Anderson at Cambridge pioneered this approach, and has a great webpage
  - http://www.cl.cam.ac.uk/~rja14/econsec.html
- Many security systems/measures fail because the economic incentives in the system don't match the security needs/requirements
  - Failures might be because of bad incentives rather than bad design
  - E.g. if the person who guards a system is not the person who suffers when the system falls to an attacker, guarding is likely to be ineffective
    - Would you pay £30 p.a. to prevent malware DoS attacks on www.nestle.com?
    - Would you pay £30 p.a. to prevent malware from phishing your bank details?
- For a 4-page article in *Science* see: www.cl.cam.ac.uk/~rja14/Papers/econ_science.pdf
- For an extended (26pp) version, see: http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf

Economics of I

- Ross Anderson at … great webpage
  - http://www.cl.car…
- Many security sys… entives in the system don't ma…
  - Failures might b…
  - E.g. if the perso… ers when the system falls to an atta…
    - Would you … ww.nestle.com?
    - Would you … r bank details?
- For a 4-page … s/econ_science.pdf
- For an exten… a14/Papers/econ_czech.pdf

Four Open Problems in Security-Economics

- 1) Algorithmic Mechanism Design
  - Design the network protocols and interfaces to be strategy-proof
  - "Designing bad behavior out of systems may be cheaper than policing it afterwards"
  - Using auction theory, e.g. combinatorial auctions for distributed strategy-proof routing
- 2) Psychology and Security
  - Inappropriate obedience (cf Milgram 1961 experiments) – eg. phone PIN phishing
  - Security usability, and studies of deception
  - Behavioral Economics (aka economic psychology)
    - Humans are not always perfectly rational and/or perfectly self-interested
    - Decision-making under risk and uncertainty shows several cognitive biases
    - Recent research (Simon Baron-Cohen) indicates systematic gender biases too
      - Most (but not all) men are "Systematizers"; most (but not all) women are "Empathizers"

Four Open Problems in Security-Economics

- 3) Network Topology and Information Security
  - Network topology can affect conflict dynamics
  - Different topologies have different robustness properties
    - (eg Scale-free networks good at resisting random attacks; less good at resisting targeted attacks.)
  - Need to better understand functional topology of technology networks

- 4) Large Project Management
  - Large IT System Project failures can cost billions and threaten whole organisations
  - Seems that approx 30% of all large projects fail, regardless of advances in technology

Summary

- ‘Evolutionary arms race’ between malware and malware detection providers.
- Significant economic impact in both damages and software revenue.
- Virus throttling prevents rapid spread of ‘epidemics’ before malware signature is identified.
- Criminals moved to other forms of malware: ransomware; cryptomining rootkits.
- Portection against, and detection of, state-sponsored cyberattacks are now a commonplace factor in national defence planning.
- Security economics looks at issues beyond the traditional technical focus.