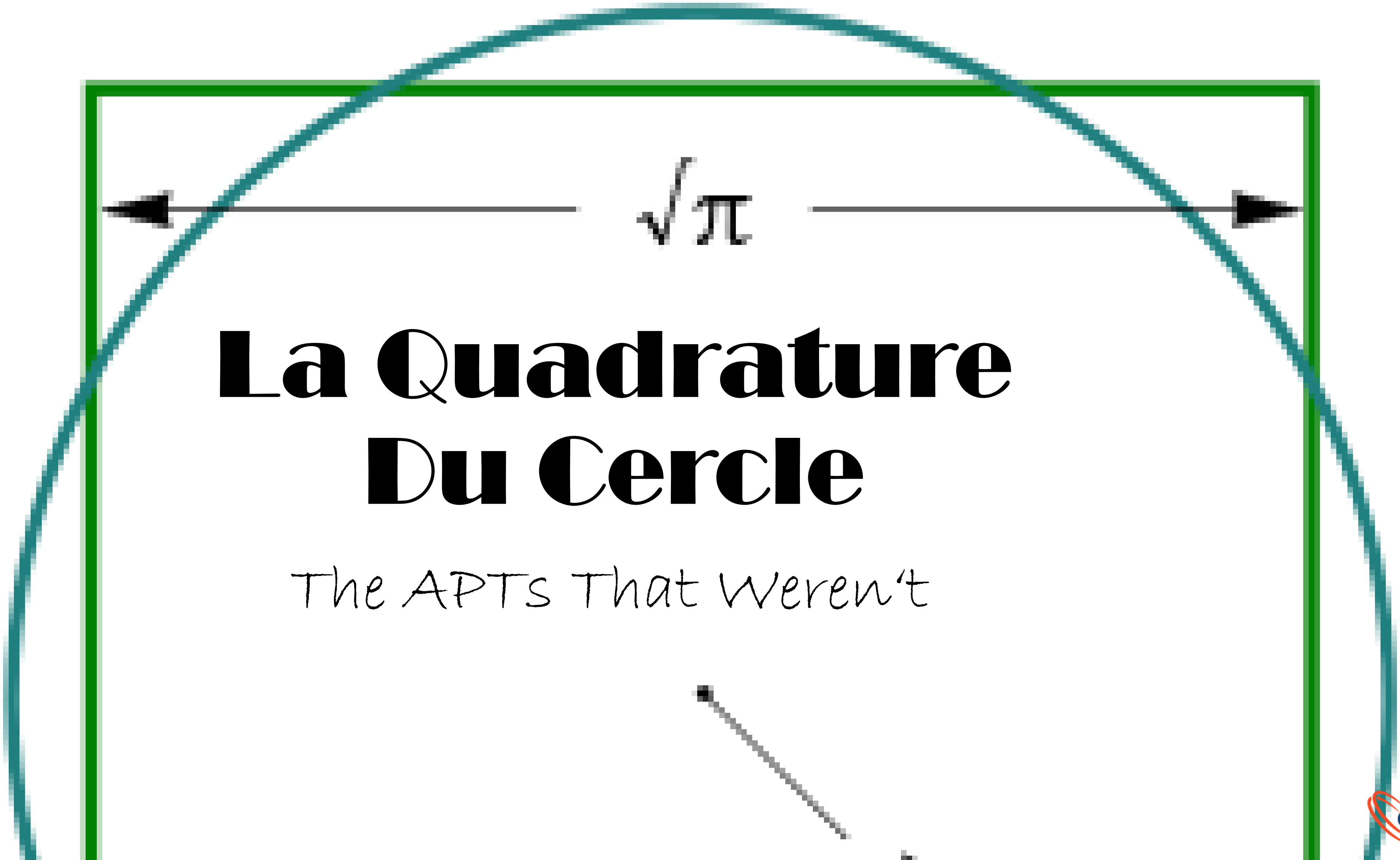
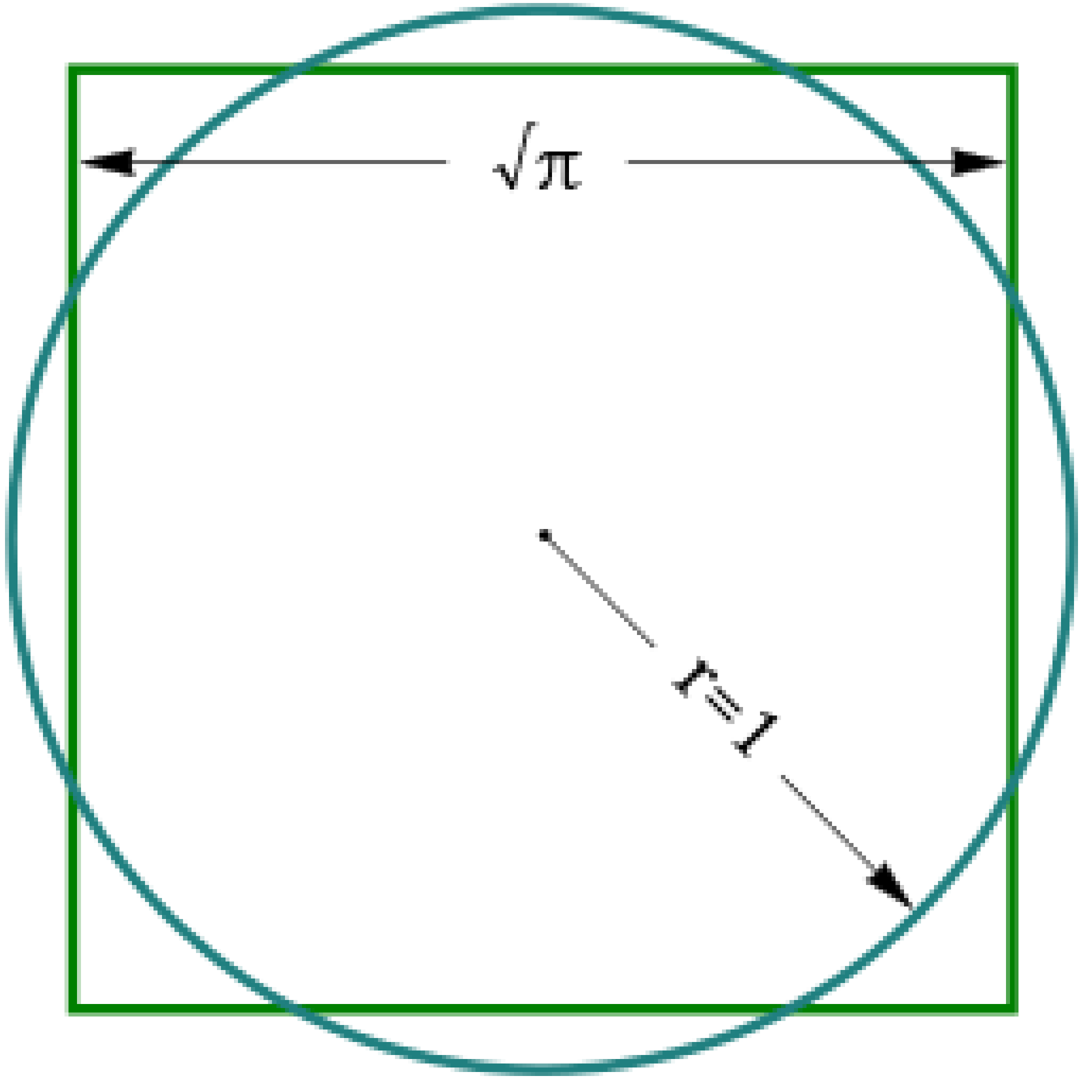


La Quadrature Du Cercle

The APTs That Weren't

CYPHORT



La cuadrature du cercle

la cuadratura del circulo

Die Quadratur des Kreises

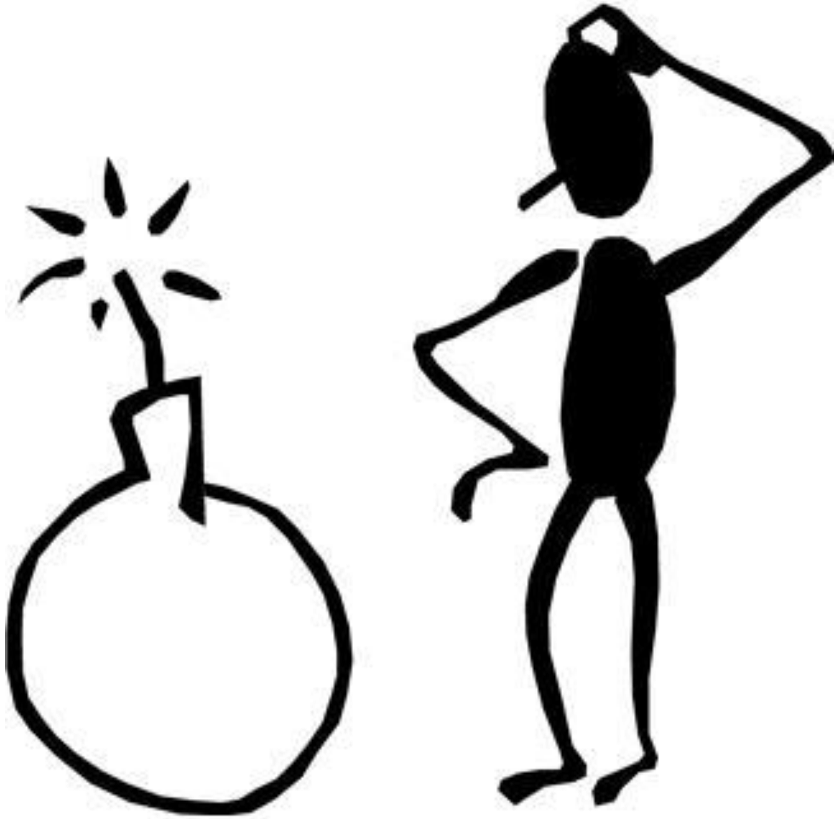
Squaring the circle

квадрату́ра кру́га

Marion Marschalek

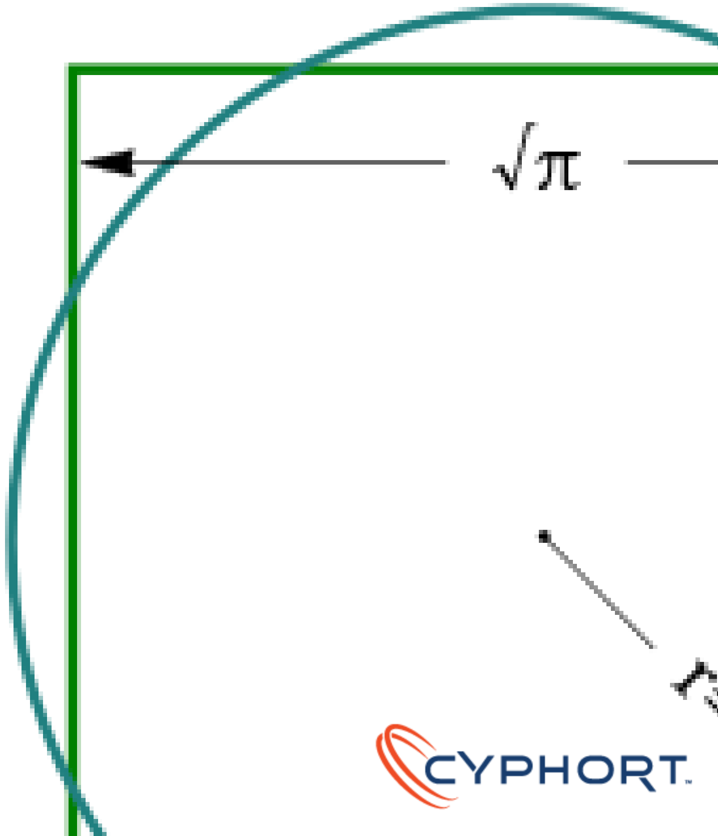
marion@cyphort.com
@pinkflawd

CYPHORT™



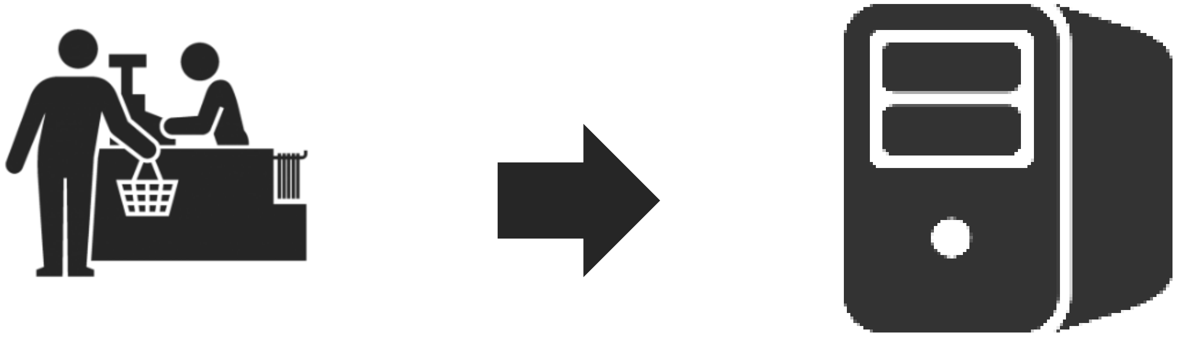
What makes an APT

- Reconnaissance – gather information
- Incursion – break in
- Discovery – look around
- Capture – collect goods
- Exfiltration – get goods out



The single most beautiful APT

November 2013 Target Corporation suffered one of the most severe large-scale retail hacks in US history



Memory scraping on running processes, fetching card data

Dumping data to a file on a share, regularly pushing out to C&C

ADVANCED

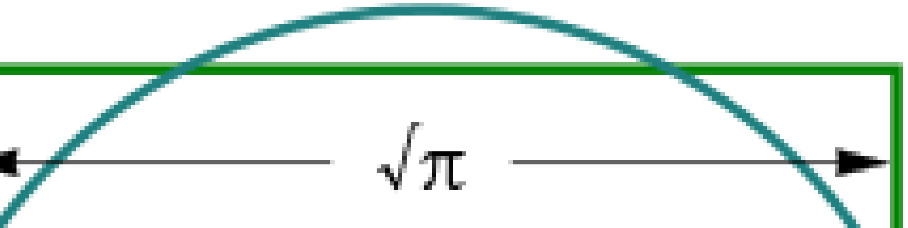
[ədˈvaːn(t)st]

we don't understand it

we detected it too late

PERSISTENT

[pəˈsɪstənt]



CYPHORT

Threat detection always relies on patterns.

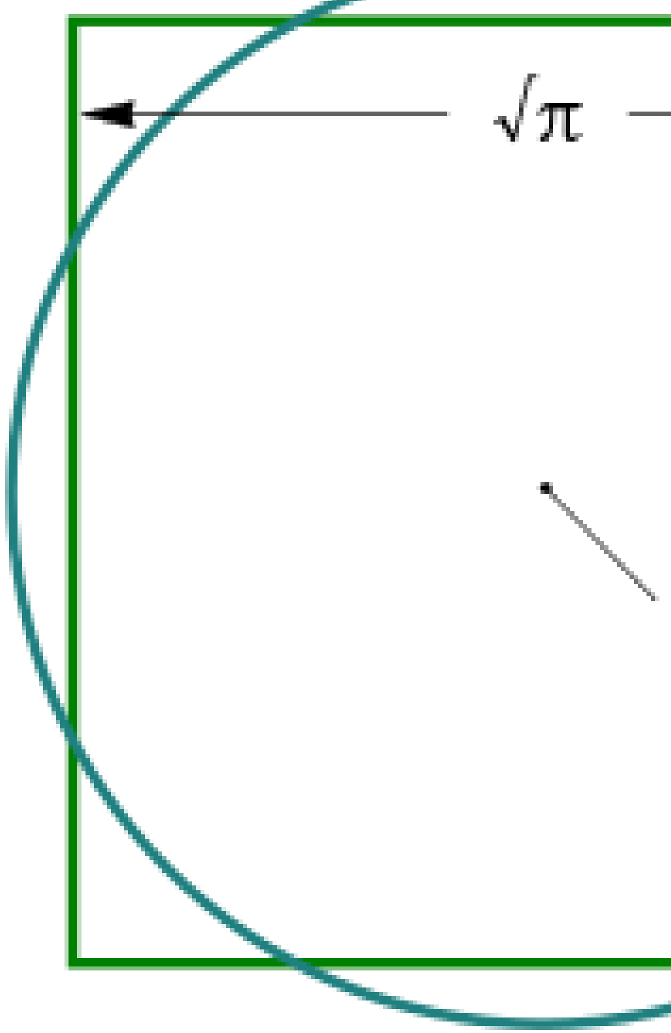
Hashes

Signatures

Behavior

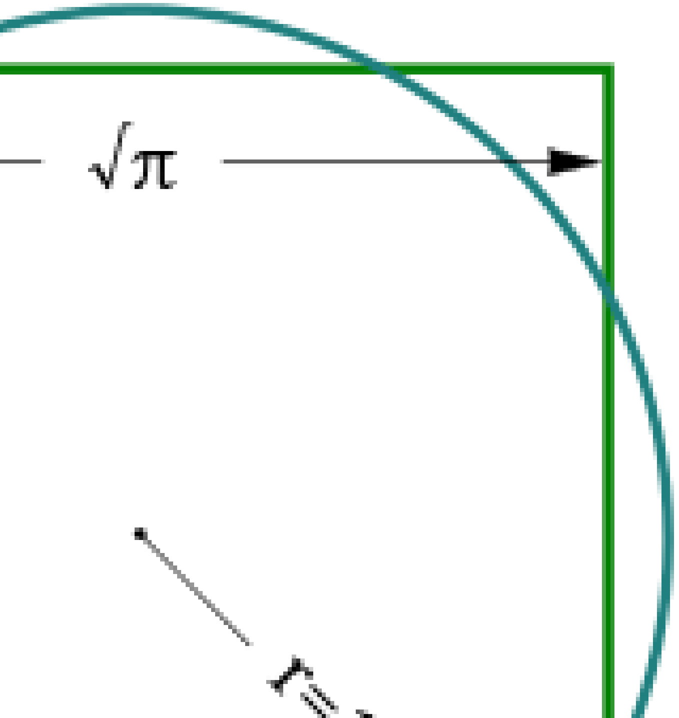
IOCs

Anomalies



Why oh why can't we find it?

I CAN SEE DEAD PATTERNS …



Curiouser and Curiouser!

- cried Alice

Cheshire Cat

Checking for running security processes

Orchestrator component executing binaries from disk

2002

Prepared to run on _old_ Windows versions

Using APIs deprecated after Win95/98/ME

Function to check for the MZ value,
the PE value and the NE value

2002

Implementation traits and user agent string indicate Win NT 4.0 as target platform

Persists as shell extension for the icon handler

Wants to run in the context of the 'Progman' window

Implant to monitor network activity

2007-2009

Evasive when network sniffer products are running

Super stealthy network communication:

Versatile communication method

9+ C&C servers, infrequent intervals

Communication done through injected standard browser instance

2007-2009

Fine tuned
to paddle around
Kaspersky security
products

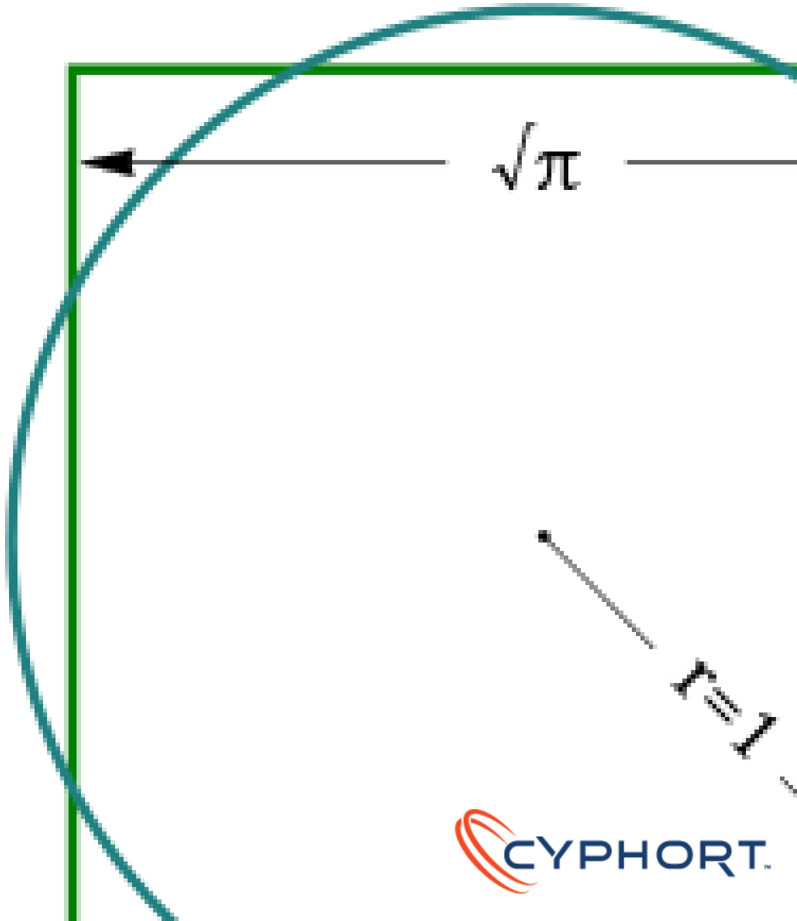
2011

CYPHORT

~DF

AP

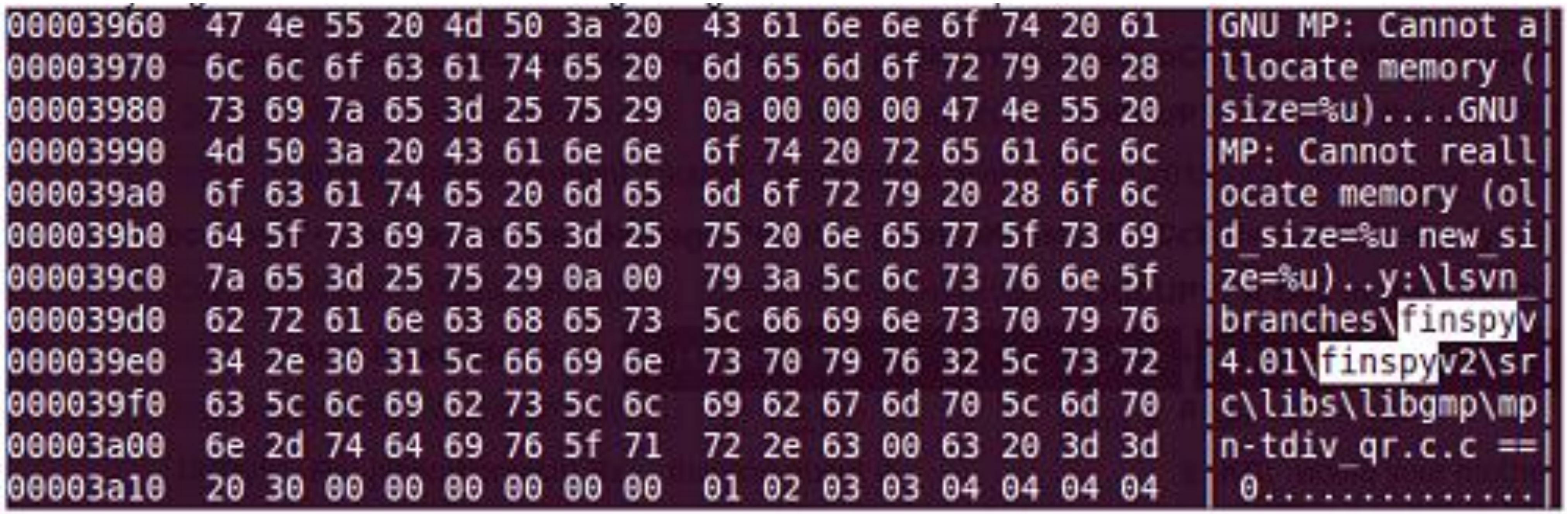
Nation State Cyber Espionage ?



From Bahrain With Love

FinFisher Suite from Gamma International UK Ltd.

Sent to Bahraini pro-democracy activists



```
00003960  47 4e 55 20 4d 50 3a 20  43 61 6e 6e 6f 74 20 61  |GNU MP: Cannot a|
00003970  6c 6c 6f 63 61 74 65 20  6d 65 6d 6f 72 79 20 28  |llocate memory (|
00003980  73 69 7a 65 3d 25 75 29  0a 00 00 00 47 4e 55 20  |size=%u)....GNU |
00003990  4d 50 3a 20 43 61 6e 6e  6f 74 20 72 65 61 6c 6c  |MP: Cannot reall|
000039a0  6f 63 61 74 65 20 6d 65  6d 6f 72 79 20 28 6f 6c  |ocate memory (ol|
000039b0  64 5f 73 69 7a 65 3d 25  75 20 6e 65 77 5f 73 69  |d_size=%u new_si|
000039c0  7a 65 3d 25 75 29 0a 00  79 3a 5c 6c 73 76 6e 5f  |ze=%u)..y:\lsvn_|
000039d0  62 72 61 6e 63 68 65 73  5c 66 69 6e 73 70 79 76  |branches\finspyv|
000039e0  34 2e 30 31 5c 66 69 6e  73 70 79 76 32 5c 73 72  |4.01\finspyv2\sr|
000039f0  63 5c 6c 69 62 73 5c 6c  69 62 67 6d 70 5c 6d 70  |c\libs\libgmp\mp|
00003a00  6e 2d 74 64 69 76 5f 71  72 2e 63 00 63 20 3d 3d  |n-tdiv_qr.c.c ==|
00003a10  20 30 00 00 00 00 00 00  01 02 03 03 04 04 04 04  | 0..............|
```

http://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

MALWARE

/ˈmalwɛːɐ̯/

Software that doesn't come with an EULA

- Morgan Marquis-Boire

Offense Going Commercial

TeleStrategies

ISS World

Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering

Washington, DC
10-12 October, 2012

Brasilia, BR
23-25 July, 2013

Prague, CZ
4-6 June, 2013

Dubai, UAE
4-6 March, 2013

Kuala Lumpur, MY
11-13 December, 2012

More Info
More Info
More Info
More Info
More Info

Nation States Going Criminal

CYPHORT

State Sponsored

Industrial Espionage

Canada spying on Brazil‘s M

NSA spying on Brazil‘s Petr

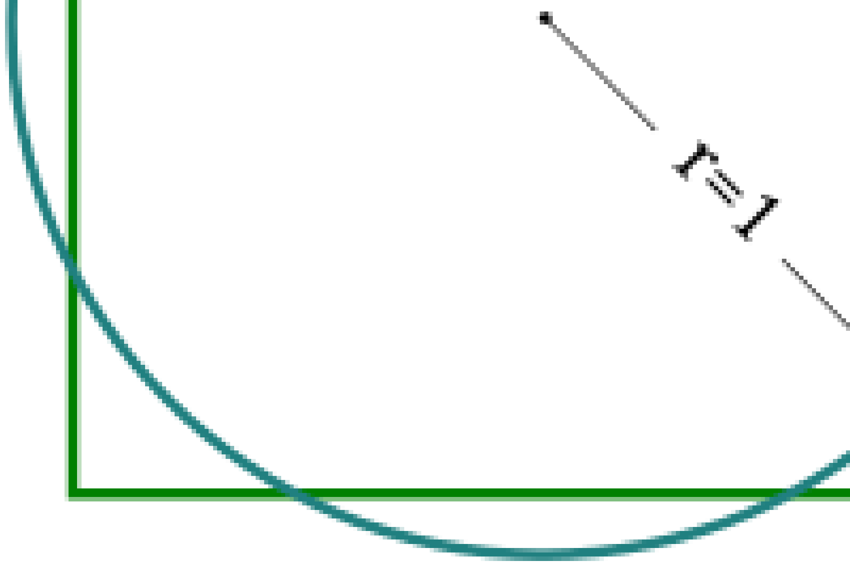
France spying on IBM/Texa

China spying on about ever

THREAT DETECTION INDUSTRY

http://www.cbc.ca/news/canada/brazil-canada-espionage-which-countries-are-we-spying-on-1.1930522
http://www.bloomberg.com/news/articles/2013-09-08/u-s-government-spied-on-brazil-s-petrobras-globo-tv-reports
http://www.nytimes.com/1990/11/18/world/french-said-to-spy-on-us-computer-companies.html

How Threat-Detection went Threat-Intel



Malware.. ‘watching’

Actor tracking

Publicity

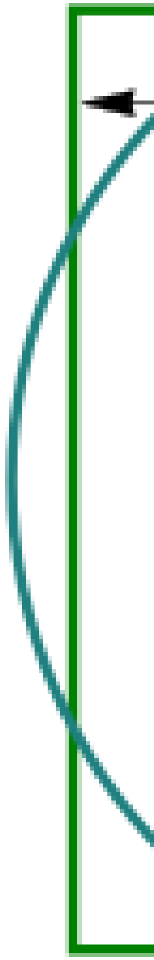
APT numbering, logos & names

FRENEMIES & THE FUNGUS AMONGUS

Or: When Malware Became Intellectual Property

Intelli.. wot?

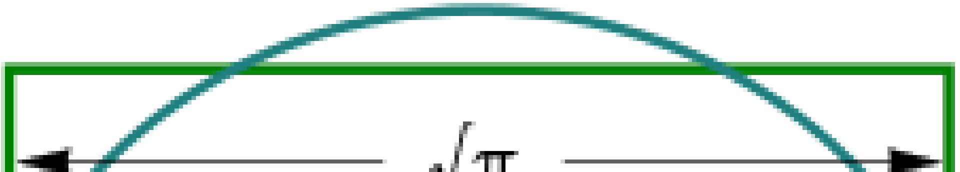
- Reverse engineering turns political when you take apart the wrong binaries
  - mass malware => targeted malware => nation state malware
  - mass malware <= targeted malware <= nation state malware
- Marketing and publicity?
  - Bad for business in the long run
    - Blowing up e.g. Spanish government ops might not help contracting with them in the future
- Providing offenders with free audits



Ethical Questions In APT Research

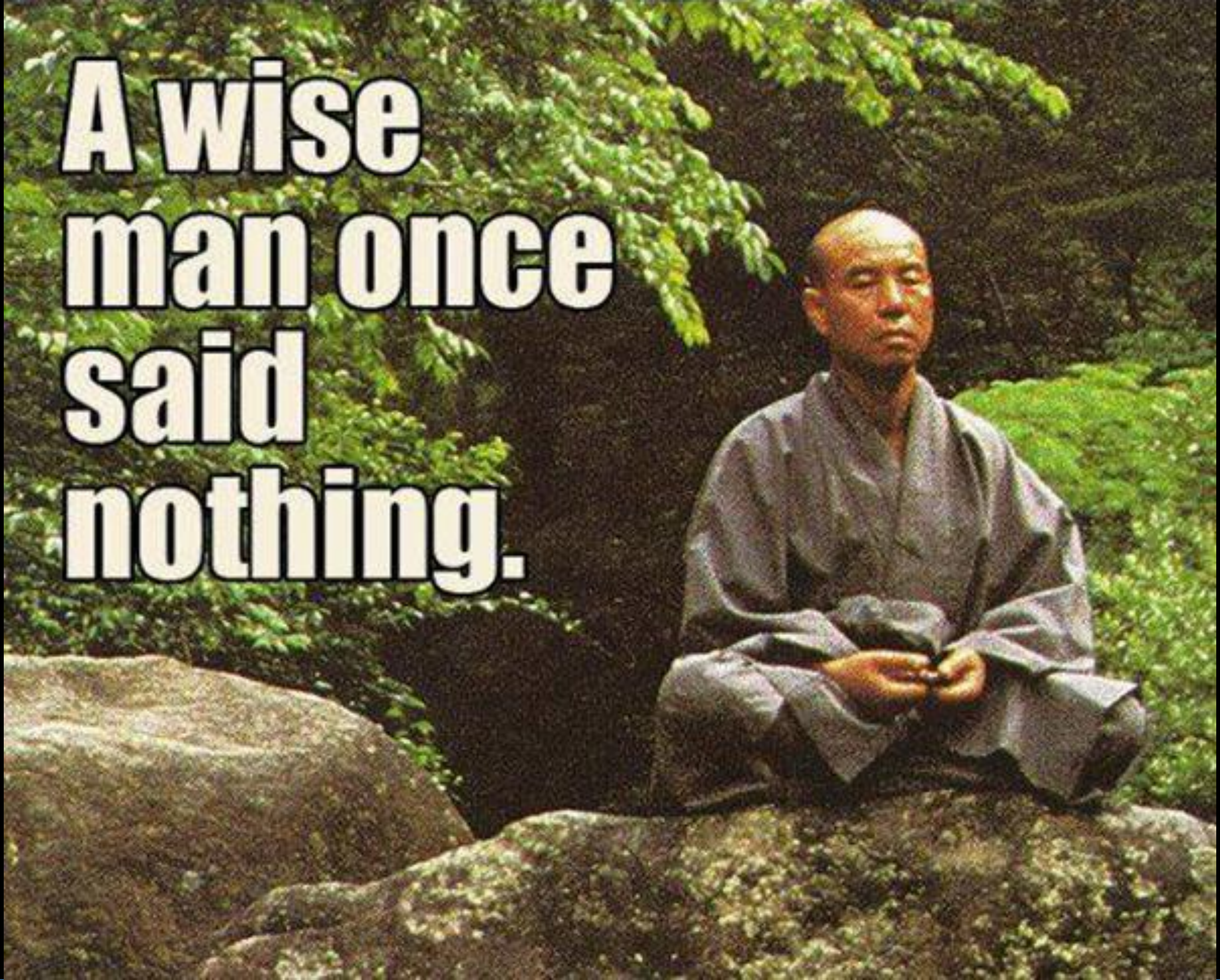
"… if the malware is detected, it will also make it **easier for extremists to protect themselves** against cyber spying attempts."

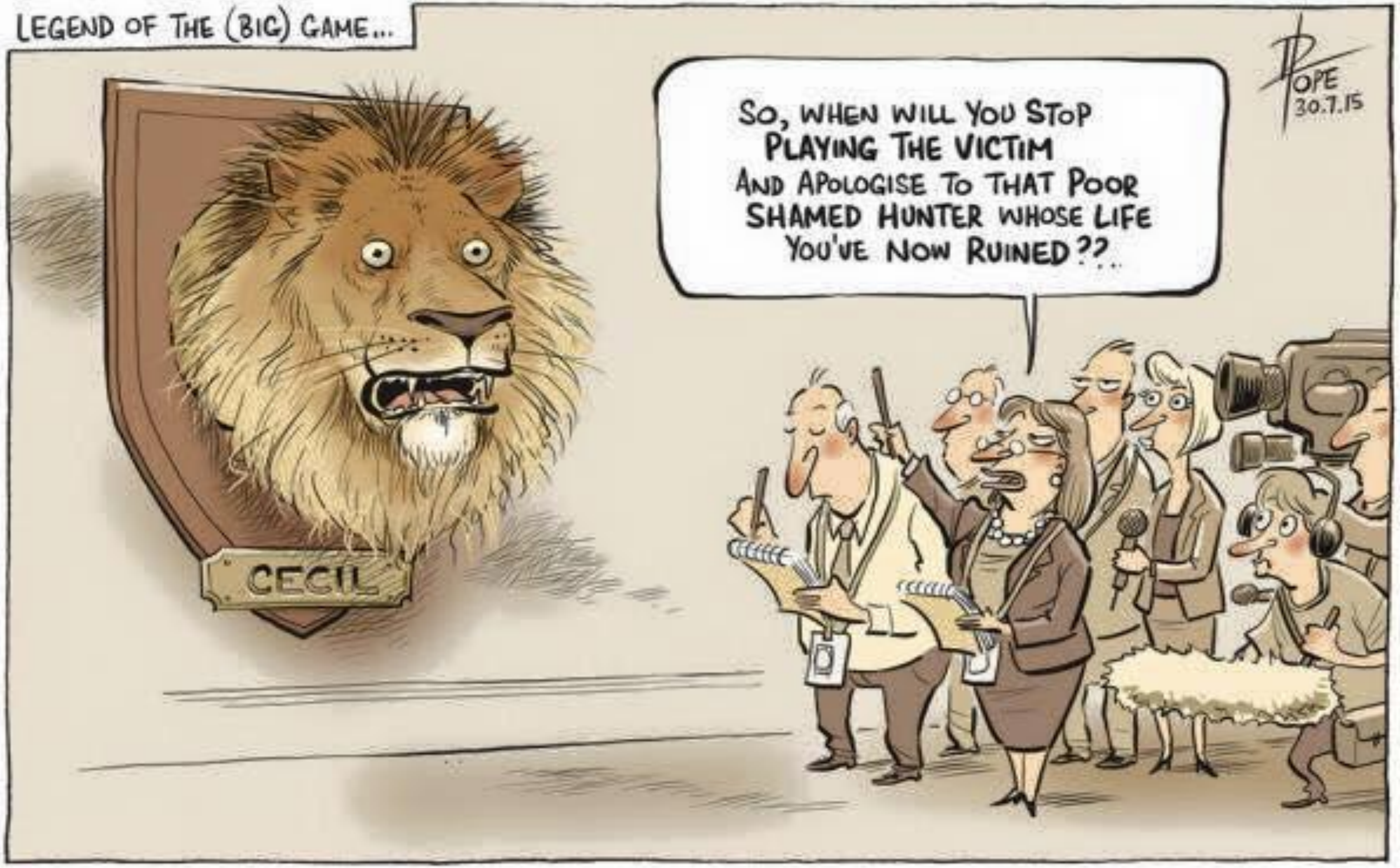
" … the researcher's insight into the operation […] is always superficial. At first glance, it might appear that the **targeted entity is "innocent",** such as an academic or a journalist, but in reality they **could be a radical academic or a terrorism-facilitating journalist.**"

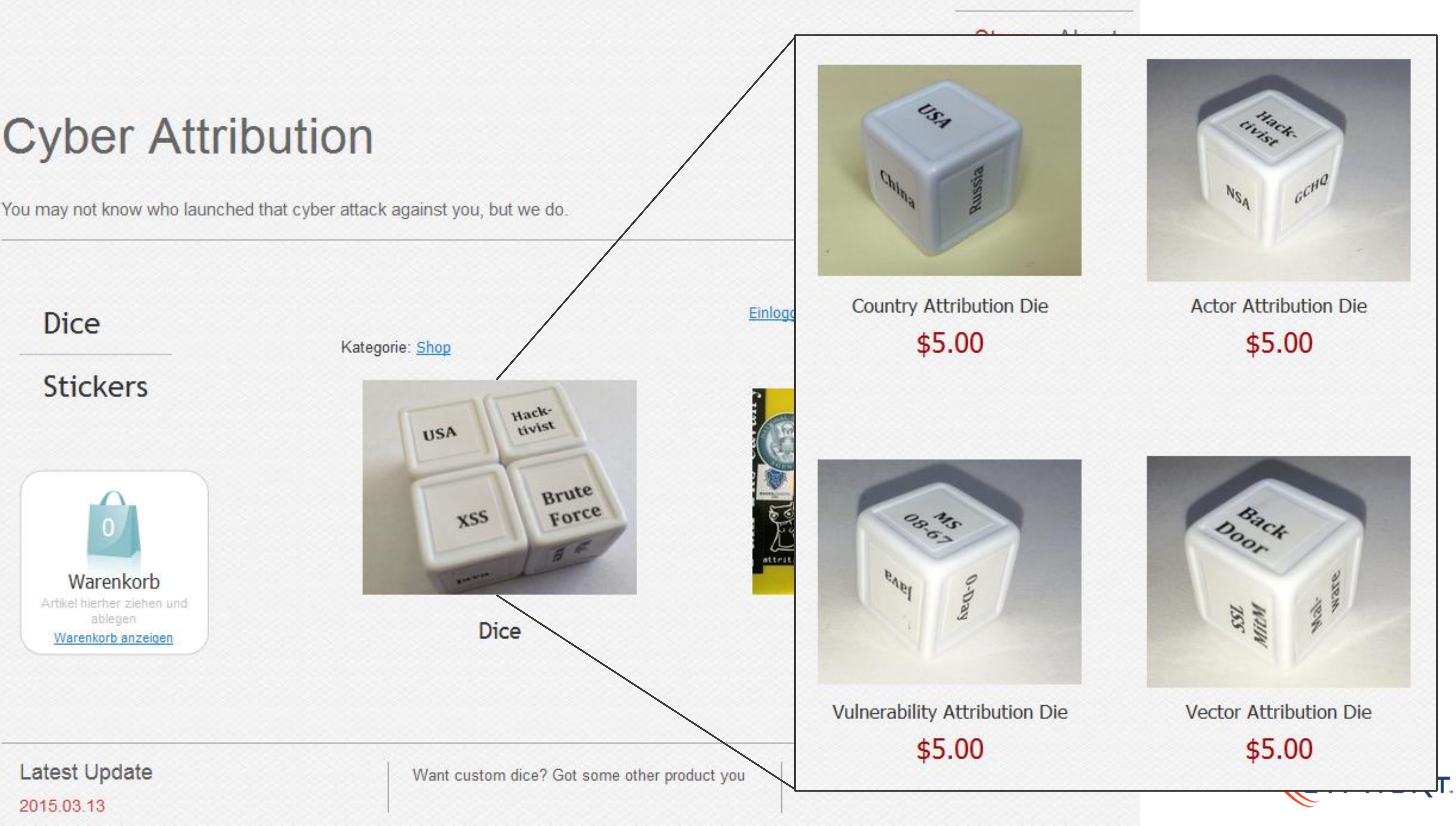


http://www.securityweek.com/long-term-strategy-needed-when-analyzing-apts-researcher

OPwot?


A wise man once said nothing.


LEGEND OF THE (BIG) GAME...
POPE 30.7.15
SO, WHEN WILL YOU STOP PLAYING THE VICTIM AND APOLOGISE TO THAT POOR SHAMED HUNTER WHOSE LIFE YOU'VE NOW RUINED??...
CECIL



Cyber Attribution

You may not know who launched that cyber attack against you, but we do.

Dice

Stickers

Warenkorb

Artikel hierher ziehen und ablegen

Warenkorb anzeigen

Kategorie: Shop

Einlogg

Dice

Country Attribution Die

$5.00

Actor Attribution Die

$5.00

Vulnerability Attribution Die

$5.00

Vector Attribution Die

$5.00

Latest Update

2015.03.13

Want custom dice? Got some other product you

Ahmed Mansoor

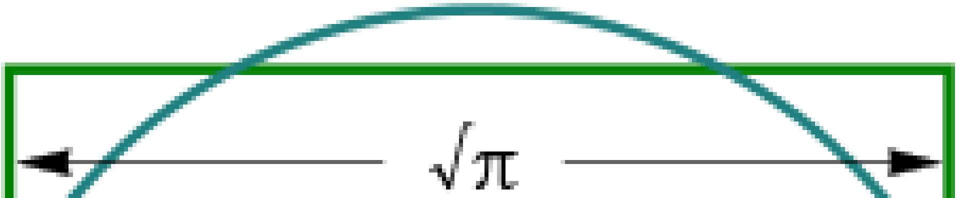
and the
UAE Five

]HackingTeam[
Rely on us.

Sometimes Attribution isn't Tricky

83.111.56.188

```
inetnum: 83.111.56.184 – 83.111.56.191
netname: minaoffice-EMIRNET
descr: Office Of Sh. Tahnoon Bin Zayed Al Nahyan
descr: P.O. Box 5151 ,Abu Dhabi, UAE
country: AE
```

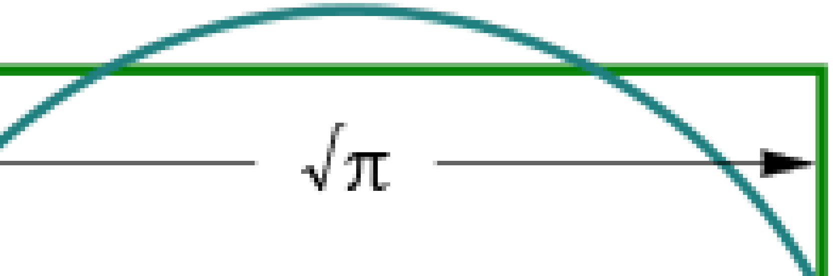


APT Attribution Cheatsheet

Any need for actor **attribution**? – Most likely **no.**

Any need for actor **tracking**? – In certain cases, **maybe.**

Any need for actor(-tool) **recognition**? – Probably, **yes.**



Sony breach linked to Armenian organized criminal group

Executive Summary

On November 24, 2014, personally identifiable information about Sony Pictures Entertainment (SPE) employees and their dependents, e-mails between employees, information about executive salaries at the company, copies of unreleased Sony films, and other information, was obtained and released by a hacker group going under the moniker "Guardians of Peace" or "GOP".

Although the motives for the hack have yet to be revealed, the hack has been tied to the planned release of the film The Interview, which depicts an assassination attempt on North Korean leader Kim Jong-un, with the hackers threatening acts of terrorism if the film were to be released.

Recently, a team of 5 researchers from Mandiant/FireEye examined the evidence left behind by the attackers. This research has provided insight into the likely source of these attacks. Though not definitive, our analysis provides a much clearer picture and suggests an organized criminal group operating out of the Republic of Armenia is responsible for the data breach impacting Sony Pictures Entertainment. This diclosure casts further doubt on the FBI's assertion that the attack was carried out by state-sponsored actors under the control of North Korea, a theory that has been all but discredited by a host of security professionals since the attack became public, including DeVry graduate Luciano Lariviere.

> I don't think North Korea did it.
>
> — Luciano Lariviere, DeVry graduate

The research team is quite certain, however, that the Guardians of Peace hacker group played no role in this attack. The clues left behind confirm that the group claiming responsiblity were a fabrication to throw investigators off the trail and to mask the true source.

Links to Armenia

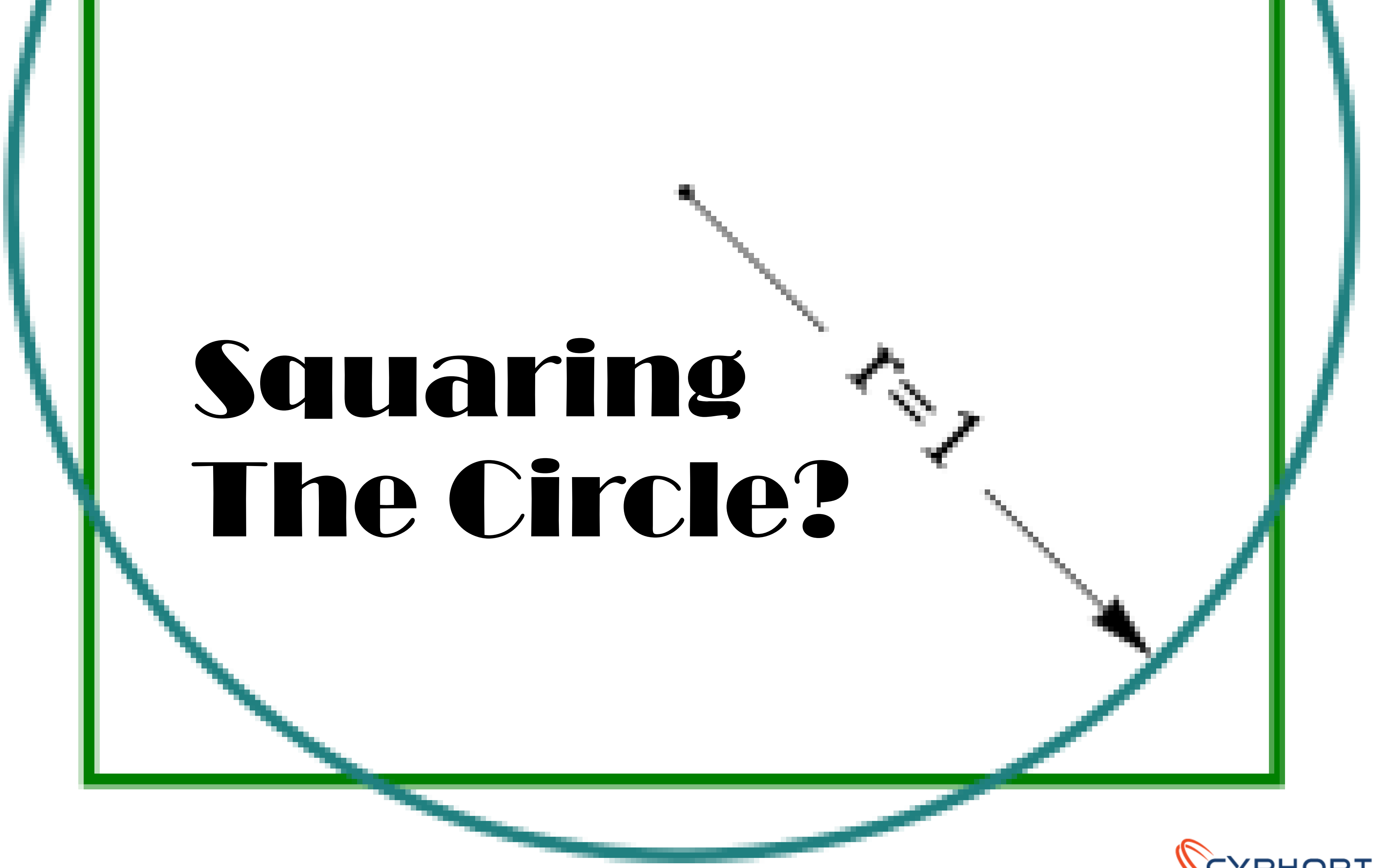
The research team was able to reconstruct the attack from the ground up and discovered a number of IP addresses that are linked to other attacks that have been attributed to actors in Armenia as well as the presence of Armenian text in the comment strings of the malware that was recovered during the forensic investigation. Some of these malware samples have also been used in Armenian attacks.

Additional signals intelligence acquired by the research team has also implicated an actor based in Armenia. This intelligence is highly classified and cannot be released in a public document, but the research team has briefed investigators with the U.S. Federal Bureau of Investigation on the findings.

Timeline of Events

Date	Description
October 19, 2014	Initial introduction of malware to the SPE computing environment. Malware is delivered using a "spear phishing" message targeted at a high level executive with subject line "Special request from James Franco"
November 7,	Malware begins communicating with C2 server at 217.96.33.165. Malware begins to spread using SMB shares and credentials obtained from the C2.

Squaring The Circle?



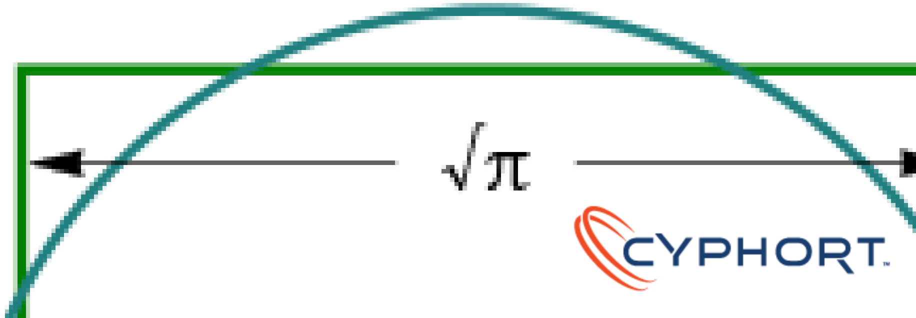
"An attacker only needs to find one weakness while the defender needs to find every one."

"Defender Economics", Andreas Lindh, Troopers15

Risk = Vulnerability * **Threat** * Impact

Threat = Intent * Capability * Opportunity

„When Threat Intel met DFIR" Chopitea & Mouchoux, hack.lu 2015



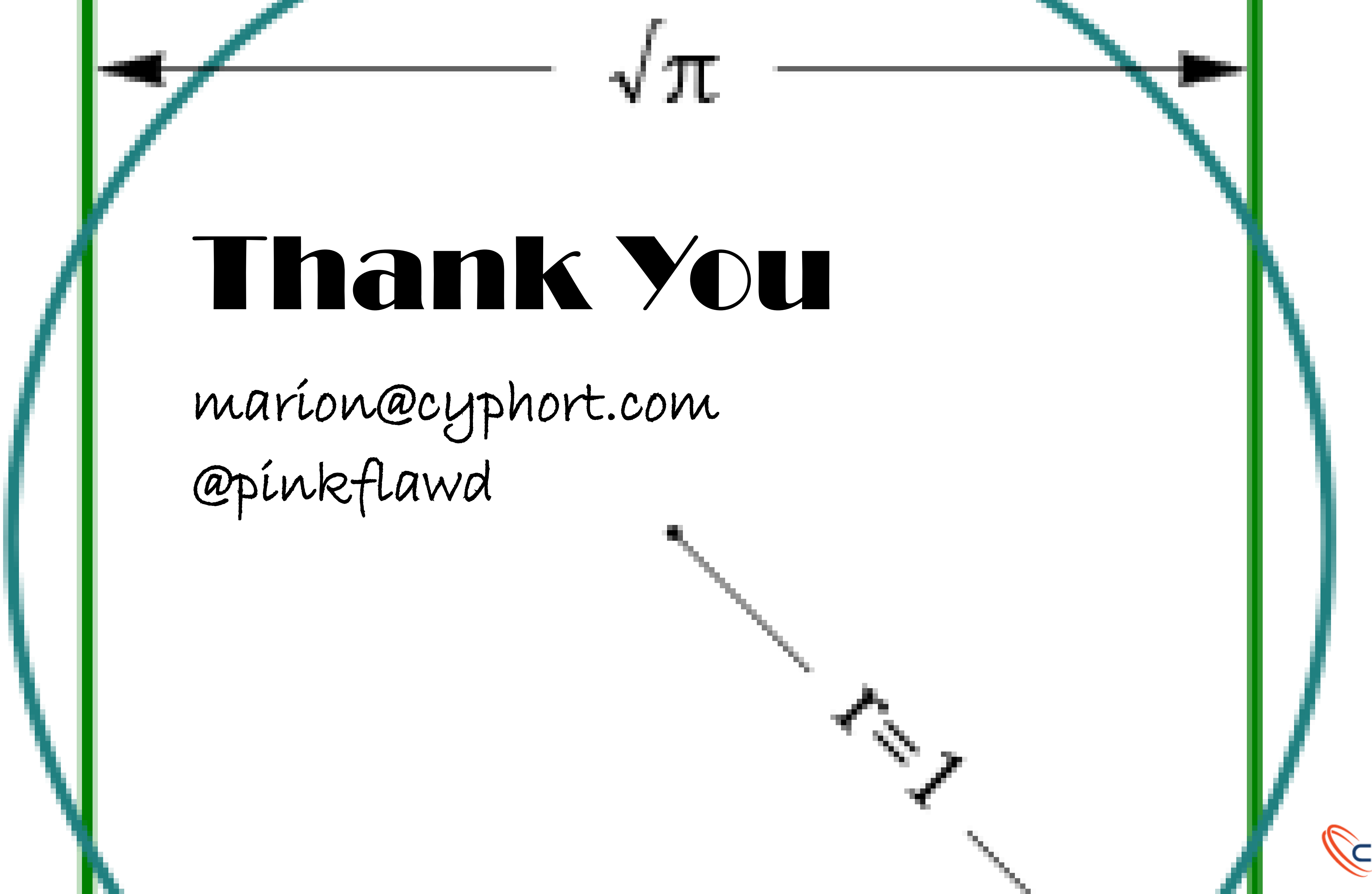
Threat modeling

Compartmentalization

2-factor Authentication

Encryption

Secrecy



Thank You

marion@cyphort.com
@pinkflawd

CYPHORT

Resources

http://www.cbc.ca/news/canada/brazil-canada-espionage-which-countries-are-we-spying-on-1.1930522

http://www.bloomberg.com/news/articles/2013-09-08/u-s-government-spied-on-brazil-s-petrobras-globo-tv-reports

http://www.nytimes.com/1990/11/18/world/french-said-to-spy-on-us-computer-companies.html

http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/

http://media.kaspersky.com/pdf/Guerrero-Saade-VB2015.pdf

http://www.securityweek.com/long-term-strategy-needed-when-analyzing-apts-researcher

https://cryptome.org/2013/03/call-to-cyber-arms.pdf

http://archive.hack.lu/2015/When%20threat%20intel%20met%20DFIR.pdf

http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1305571.shtml

http://www.bbc.com/news/world-asia-china-34360934