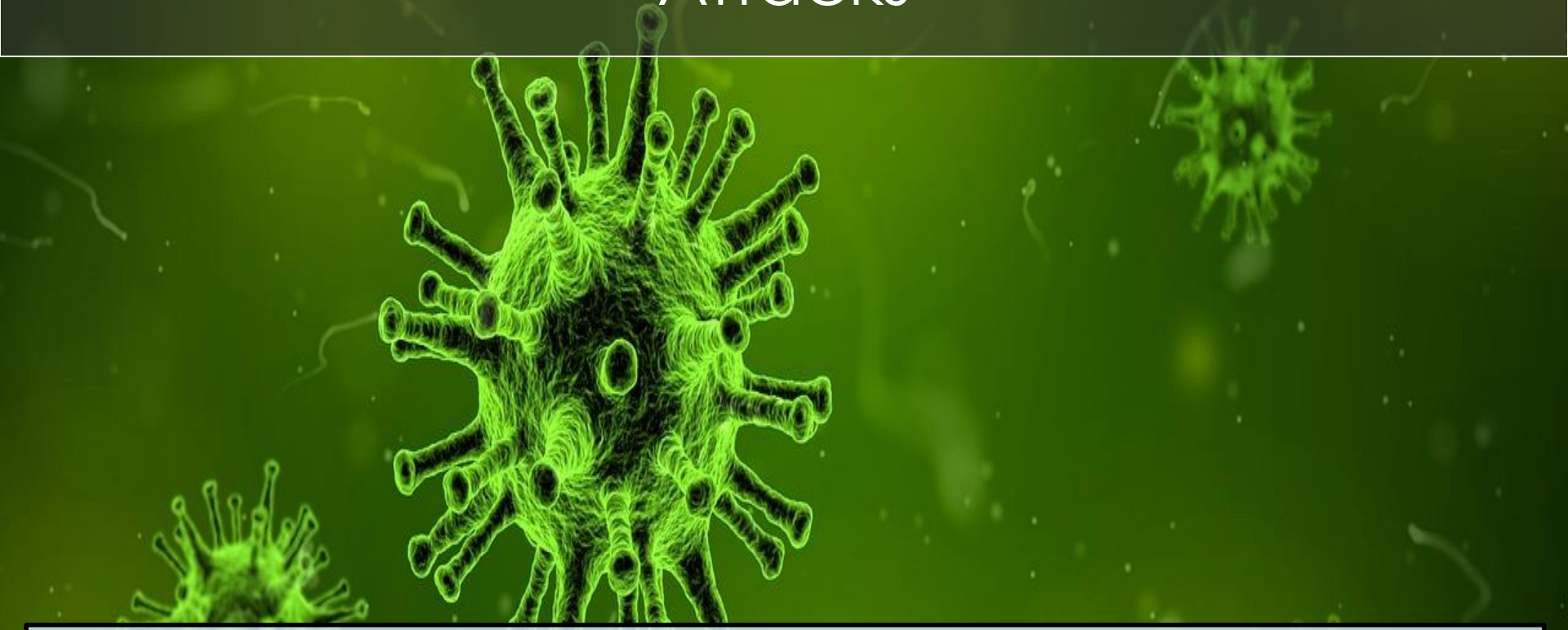
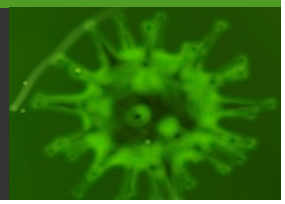
Conceptualizing Human Resilience in the Face of the Global Epidemiology of Cyber Attacks



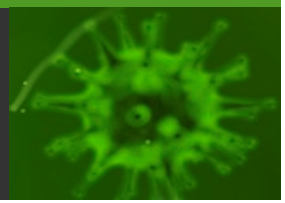
L Jean Camp, Marthie Grobler,
Julian Jang-Jaccard, Christian Probst,
Karen Renaud, Paul Watters

Cyber is Global



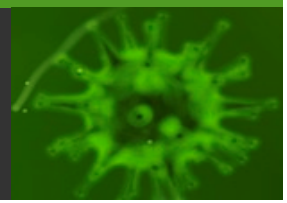
- It is unrealistic to study cyber at a local level
- Cyber "infections" do not stop at country borders
- We are all connected to the global internet
- Hackers operate globally

Cyber Epidemiology



- Individuals are **highly distinct**, **independent**, and **important** agents within a socio-technical system.
- Benefit from understandings of disease
- Understanding how cybercrime thrives

Need …

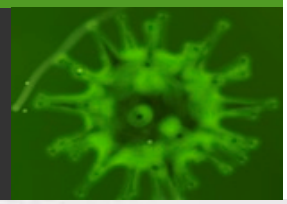


- a holistic, ecologically valid approach
- to engender **resilience** and understanding **of location-specific vulnerability** to social engineering attacks.

Focus

- **Individuals**, not organizations or teams
- Understanding **individual** behavior
- Identify the challenges of investigating the ***human dimension*** of cyber epidemics

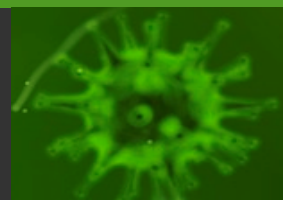
Humans



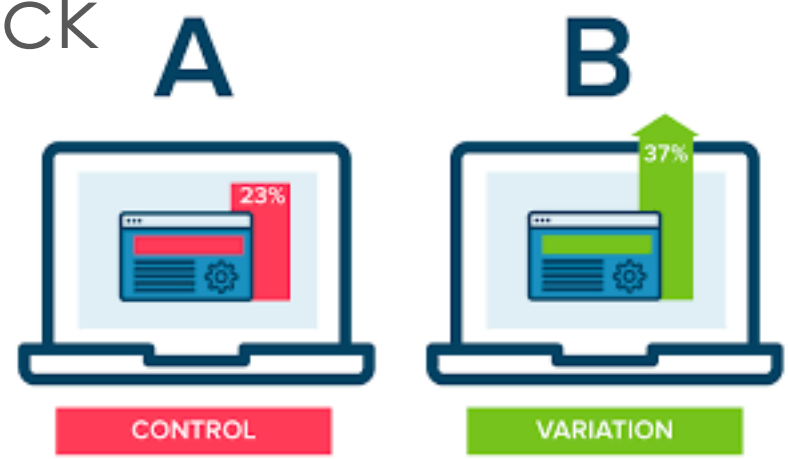
- Are often treated as homogenous
- Identically indistinguishable nodes
- With some notable exceptions this is how the human in the socio-technical system is seen

Bashir et al, 2017.

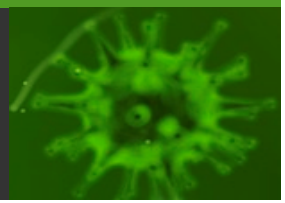
Consequence



- Most human subject studies, carry out explorations with using controlled A/B tests
- implemented once,
- with limited feedback



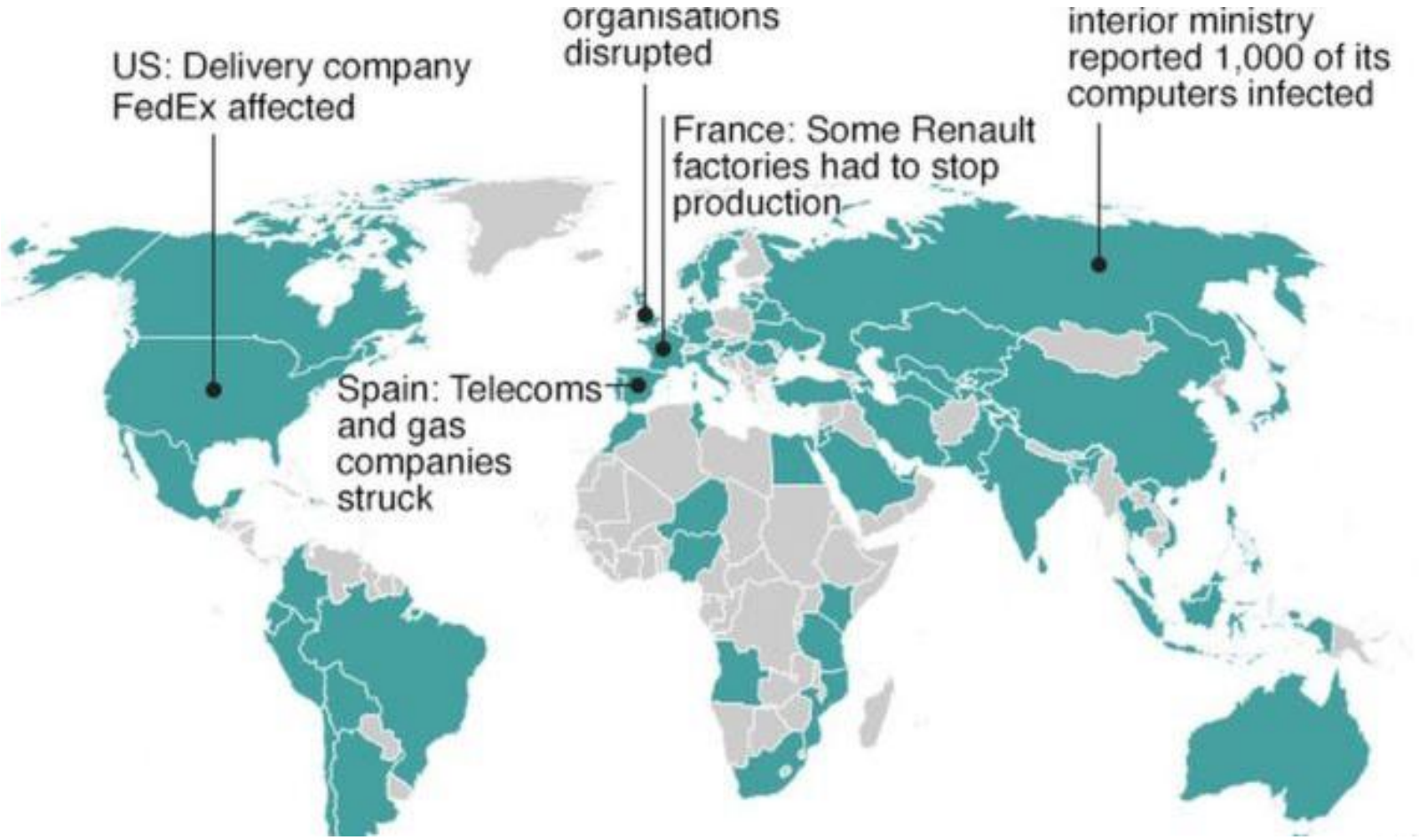
Cybercriminals are smarter

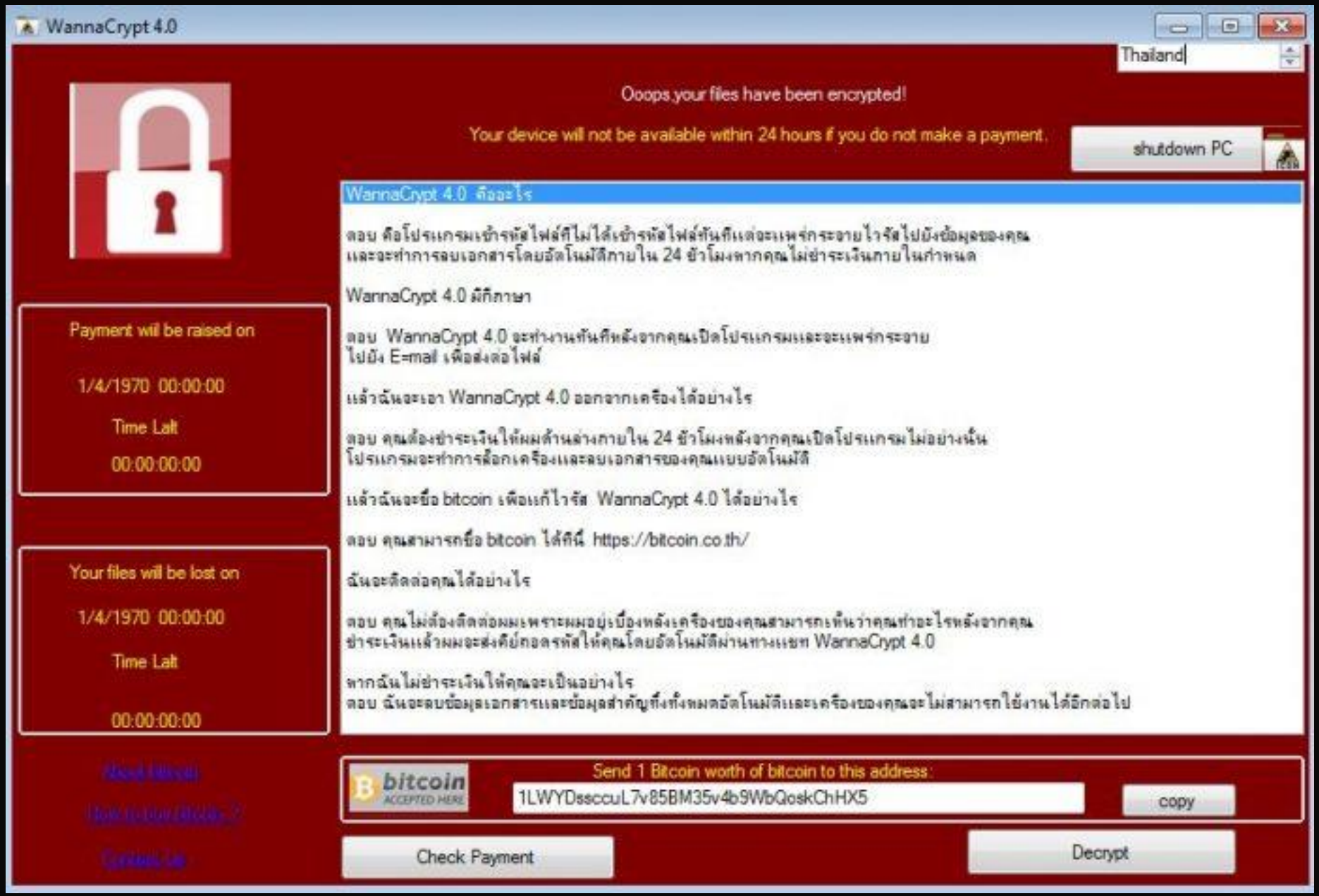


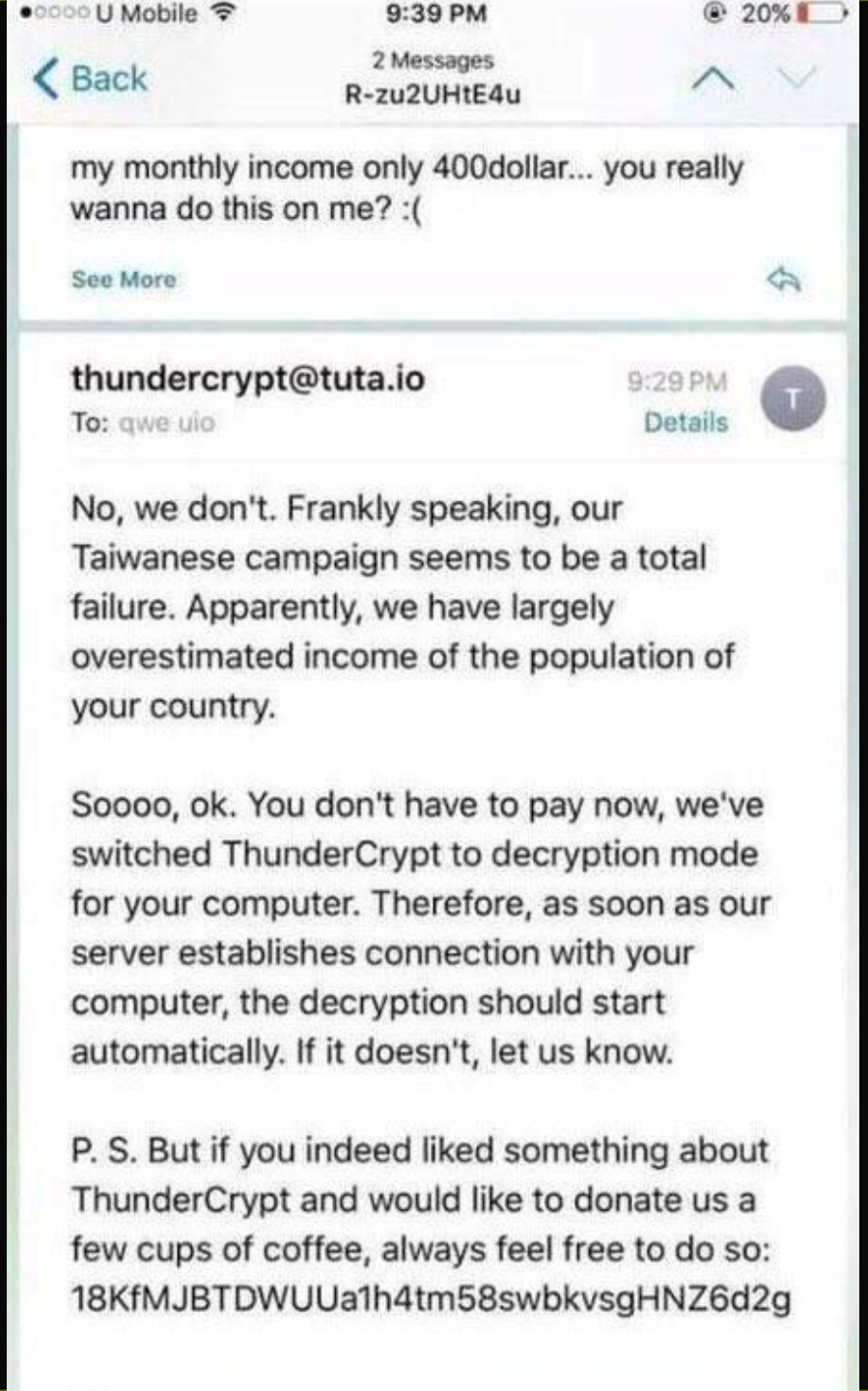
- one malware model distinguished between "***careful***" and "***careless***" populations, matching the dynamics of an *epidemic* that matches observed behavior
- WannaCry primarily targeted countries perceived to be wealthy


Country
Botnet
China
wcrypt
Russian Federation
wcrypt
Peru
wcrypt
France
wcrypt
Canada
wcrypt

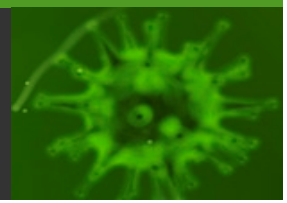
Who was hit?


US: Delivery company FedEx affected
organisations disrupted
France: Some Renault factories had to stop production
interior ministry reported 1,000 of its computers infected
Spain: Telecoms and gas companies struck


WannaCrypt 4.0
Thailand
Ooops,your files have been encrypted!
Your device will not be available within 24 hours if you do not make a payment.
shutdown PC
WannaCrypt 4.0 คืออะไร
ตอบ คือโปรแกรมเข้ารหัสไฟล์ที่ไม่ได้เข้ารหัสไฟล์ทันทีแต่จะแพร่กระจายไวรัสไปยังข้อมูลของคุณ
และจะทำการลบเอกสารโดยอัตโนมัติภายใน 24 ชั่วโมงหากคุณไม่ชำระเงินภายในกำหนด
WannaCrypt 4.0 มีกี่ภาษา
ตอบ WannaCrypt 4.0 จะทำงานทันทีหลังจากคุณเปิดโปรแกรมและจะแพร่กระจาย
ไปยัง E=mail เพื่อส่งต่อไฟล์
แล้วฉันจะเอา WannaCrypt 4.0 ออกจากเครื่องได้อย่างไร
ตอบ คุณต้องชำระเงินให้ผมด้านล่างภายใน 24 ชั่วโมงหลังจากคุณเปิดโปรแกรมไม่อย่างนั้น
โปรแกรมจะทำการล็อกเครื่องและลบเอกสารของคุณแบบอัตโนมัติ
แล้วฉันจะซื้อ bitcoin เพื่อแก้ไวรัส WannaCrypt 4.0 ได้อย่างไร
ตอบ คุณสามารถซื้อ bitcoin ได้ที่นี่ https://bitcoin.co.th/
ฉันจะติดต่อคุณได้อย่างไร
ตอบ คุณไม่ต้องติดต่อผมเพราะผมอยู่เบื้องหลังเครื่องของคุณสามารถเห็นว่าคุณทำอะไรหลังจากคุณ
ชำระเงินแล้วผมจะส่งคีย์ถอดรหัสให้คุณโดยอัตโนมัติผ่านทางแชท WannaCrypt 4.0
หากฉันไม่ชำระเงินให้คุณจะเป็นอย่างไร
ตอบ ฉันจะลบข้อมูลเอกสารและข้อมูลสำคัญทั้งทั้งหมดอัตโนมัติและเครื่องของคุณจะไม่สามารถใช้งานได้อีกต่อไป
Payment will be raised on
1/4/1970 00:00:00
Time Lalt
00:00:00:00
Your files will be lost on
1/4/1970 00:00:00
Time Lalt
00:00:00:00
About bitcoin
How to buy bitcoins ?
Contact Us
bitcoin
ACCEPTED HERE
Send 1 Bitcoin worth of bitcoin to this address :
1LWYDssccuL7v85BM35v4b9WbQoskChHX5
copy
Check Payment
Decrypt

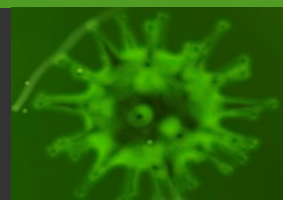

U Mobile
9:39 PM
20%
Back
2 Messages
R-zu2UHtE4u
my monthly income only 400dollar... you really wanna do this on me? :(
See More
thundercrypt@tuta.io
To: qwe uio
9:29 PM
Details
No, we don't. Frankly speaking, our Taiwanese campaign seems to be a total failure. Apparently, we have largely overestimated income of the population of your country.
Soooo, ok. You don't have to pay now, we've switched ThunderCrypt to decryption mode for your computer. Therefore, as soon as our server establishes connection with your computer, the decryption should start automatically. If it doesn't, let us know.
P. S. But if you indeed liked something about ThunderCrypt and would like to donate us a few cups of coffee, always feel free to do so:
18KfMJBTDWUUa1h4tm58swbkvsgHNZ6d2g

Attackers vs Defenders



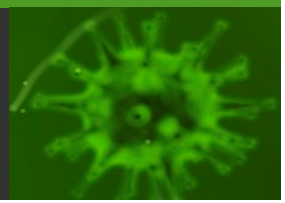
- social engineering attacks are highly optimized and targeted by attackers
- Defenders still use rough categorizations
- Cyber-social system concept now emerging

Proposal



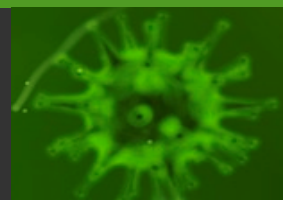
- systematic use of
  - consistent tested mechanisms
  - reported in a consistent manner
- Enable complementary, systematic investigations that
  - Reflect extant understanding of resilience to social engineering
  - can be improved with the inclusion of new data over time.

Proposal



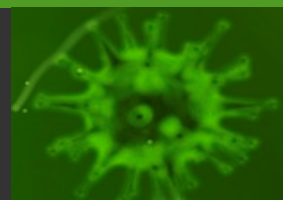
- Archive data produced from consistent, validated tests in scales that speak to generalized human responses to common cybercrimes
- Drive those data into as many disciplines that can comment on
  - experiencea of a cybercrime victim
  - decision-making failures (and the cybercrime's success) at moment of contact

Ultimate goal



to be able to identify the most vulnerable populations, and use that to craft interventions that can limit the spread of malware via the human agent.

Ultimate goal

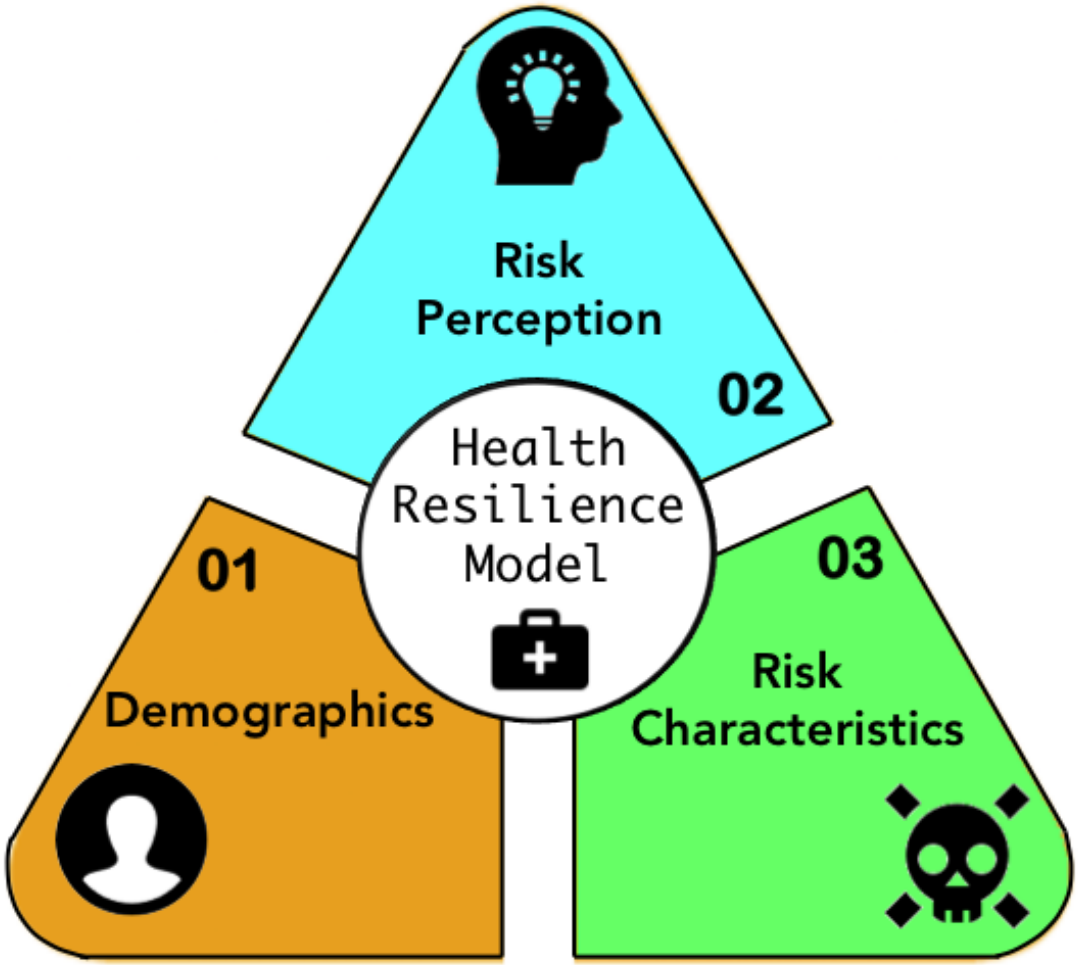


the collection of data that will allow analyses of human responses to the malicious operations *and* the contribution of the built computing environment to their failed, destructive responses to those attacks

We need

- consistent methodological "security health" measurement tools
- used and refined across regions and cultures.
- Experimental methods can eliminate social desirability and other biases

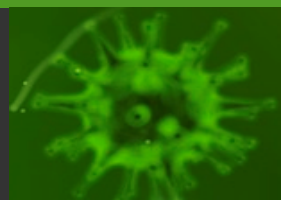
Health Resistance Model



Demographics

- Age (e.g. adolescents, elderly)
- Gender and risk resilience
- Language mastery
- These factors can lead to increased risk of infection

Risk Perception



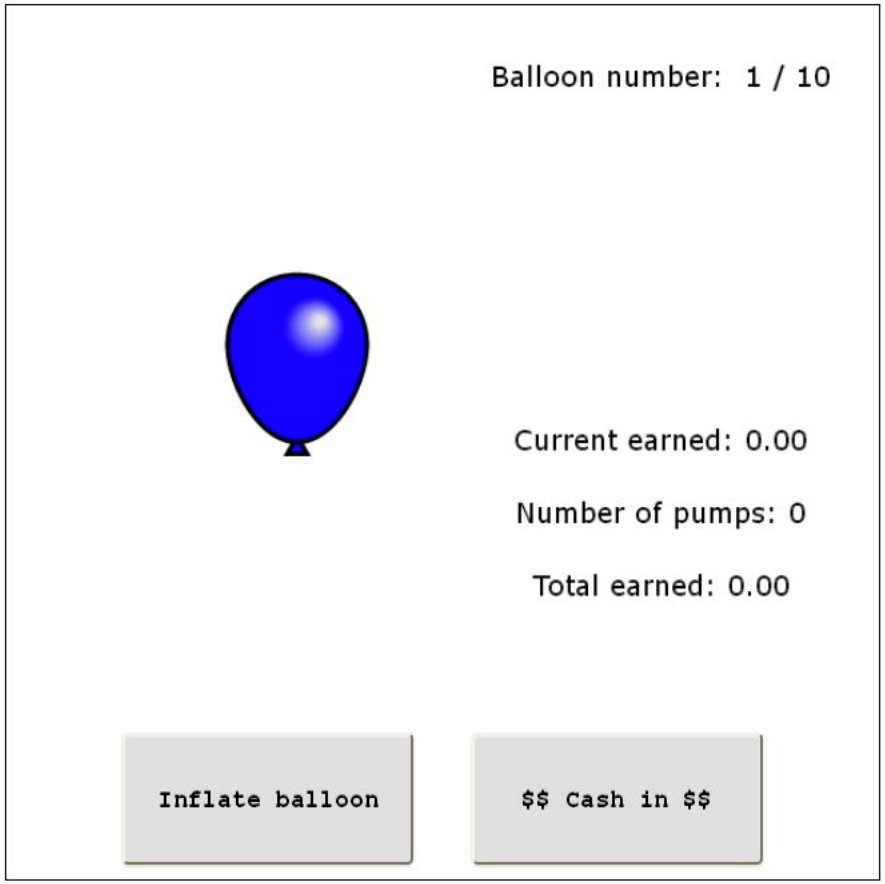
- Characteristics of Hazard
- Availability of risk information
- Frequency of Internet use
- Financial transactions online

Risk Characteristics

- Measure of control over risk
- Voluntariness of activity
- Resilience
- depth of security signalling
- costs/availability of user defection from the event/transaction that is presenting risk.

Tools

- Balloon Analogue Risk Test (BART)



Tools

- Internet Users Privacy Information Concerns (IUPIC)

Information Systems Research
Vol. 15, No. 4, December 2004, pp. 336–355
ISSN 1047-7047 | EISSN 1526-5536 | 04 | 1504 | 0336

informs

DOI 10.1287/isre.1040.0032

Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model

Naresh K. Malhotra
College of Management, Georgia Tech, 800 West Peachtree Street, Atlanta, Georgia 30332,
naresh.malhotra@mgt.gatech.edu

Sung S. Kim
School of Business, University of Wisconsin–Madison, 975 University Avenue, Madison, Wisconsin 53706,
skim@bus.wisc.edu

James Agarwal
Haskayne School of Business, University of Calgary, 2500 University Drive NW, Calgary, Alberta, T2N 1N4, Canada,
james.agarwal@haskayne.ucalgary.ca

Tools

- Simple Usability Scale (SUS)

SUS - A quick and dirty usability scale

John Brooke

Redhatch Consulting Ltd.,
12 Beaconsfield Way,
Earley, READING RG6 2UX
United Kingdom

email: *john.brooke@redhatch.co.uk*

Tools

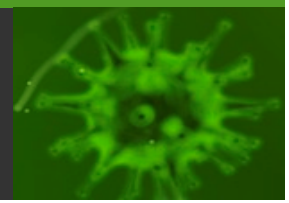
- Task Load Index (TLX)

Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research

Sandra G. Hart
Aerospace Human Factors Research Division
NASA-Ames Research Center
Moffett Field, California

Lowell E. Staveland
San Jose State University
San Jose, California

Tools



- Security Behavior Intention Scale (SEBIS)

Scaling the Security Wall

Developing a Security Behavior Intentions Scale (SeBIS)

Serge Egelman
International Computer Science Institute
Berkeley, CA, USA
egelman@cs.berkeley.edu

Eyal Peer
Bar-Ilan University
Ramat Gan, Israel
eyal.peer@biu.ac.il

Tools

- End-User Expertise Instrument

Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)

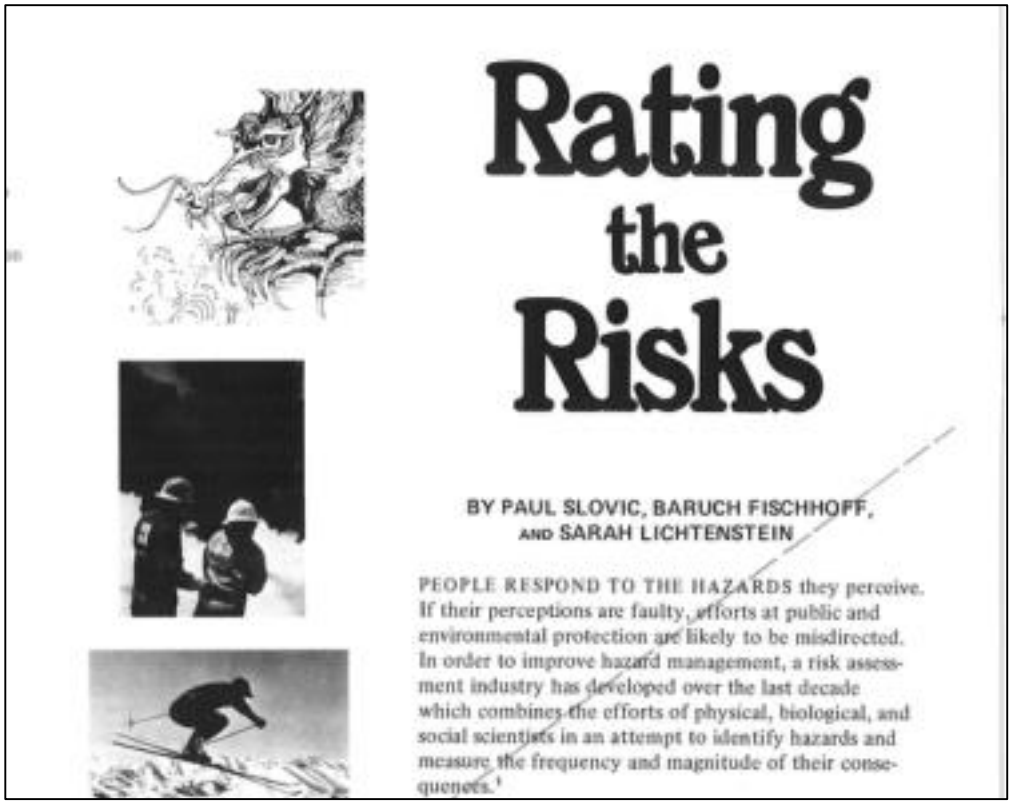
What Can Johnny Do?–Factors in an End-User Expertise Instrument

P. Rajivan, P. Moriano, T. Kelley and L.J. Camp

School of Informatics and Computing, Indiana University, Bloomington, USA
e-mail: {prajivan; pmoriano; kelleyt; ljcamp}@indiana.edu

Tools

- Nine-Dimensional Canonical Risk Dimensions



Rating the Risks

BY PAUL SLOVIC, BARUCH FISCHHOFF, AND SARAH LICHTENSTEIN

PEOPLE RESPOND TO THE HAZARDS they perceive. If their perceptions are faulty, efforts at public and environmental protection are likely to be misdirected. In order to improve hazard management, a risk assessment industry has developed over the last decade which combines the efforts of physical, biological, and social scientists in an attempt to identify hazards and measure the frequency and magnitude of their consequences.[1]

Cultural Differences

- ‘Western, Educated, Industrialized, Rich and Democratic’ (WEIRD) societies
- Security and privacy concerns of internet users vary across different cultural and political settings,

eCrime Differences

Pharmaceutical SPAM

- Caribbean payment service
- Indians filled orders
- Chinese provided DNS
- Russia coordinated affiliates

Cultural Challenges

- Different privacy requirements in different countries
- GDPR applies in Europe but different legislation elsewhere
  - Need to enable opt-out
- Language differences

Logistic Challenges

- Aligning payment to minimum wage requirements
- Motivation levels
- Research ethics in different countries/institutions are different

Conclusion

- Need a commitment by the involved research communities to share aggregate data and experimental platforms
- to facilitate a more accurate global comparison on online risk resilience

Conclusion cont'd

- provide more valuable insight in terms of global resilience and where interventions are required
- a set of well-understood, well-documented, and systematically used methods to explore phishing resilience

Thank You. Any questions?