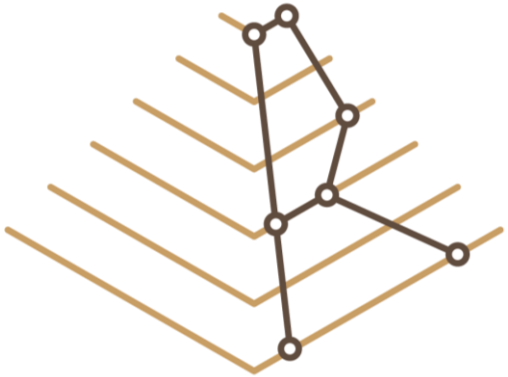
INTERNET FORENSIC PLATFORM FOR TRACKING THE MONEY FLOW OF FINANCIALLY-MOTIVATED MALWARE



RAMSES

9th Community of Users on Safe, Secure and Resilient Societies - Workshop on Cybercrime
6th December 2017

Darren Hurley-Smith

University of Kent | Computing

European Commission

Index

- Introduction to RAMSES project:
  - General presentation of the project: main objectives and consortium
- WP 4: Economic Modelling of Ransomware as a Business:
  - The current state of ransomware from an economic perspective
  - Expectations of near future developments
- Questions

Consortium

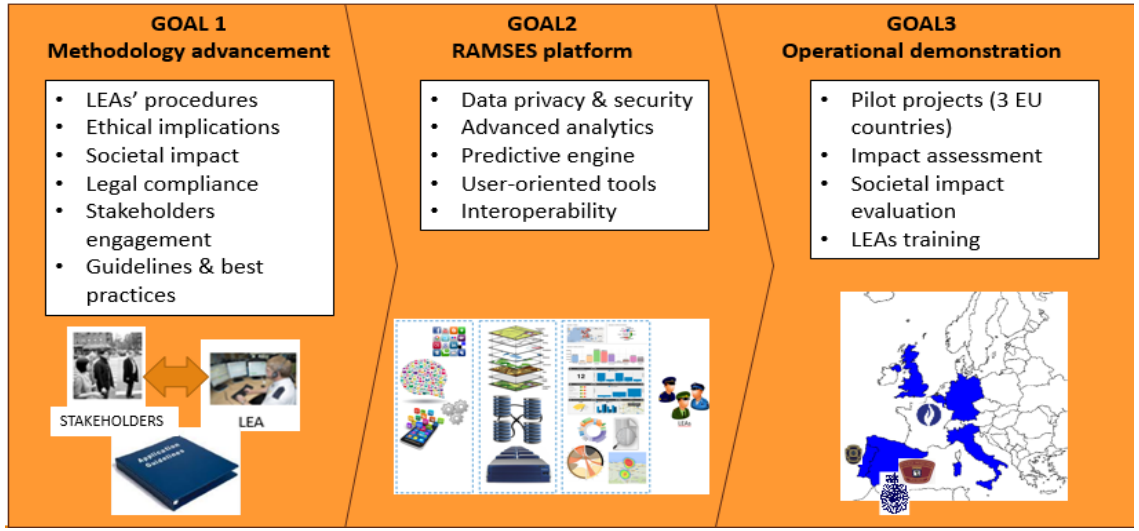
1. Treelogic (TREE) - coordinator
2. Polícia Judiciária – Ministério da Justiça (MJ)
3. University of Kent (UNIKENT)
4. Research Centre on Security and Crime (RISSC)
5. Universidad Complutense Madrid (UCM)
6. College of the Bavarian Police (BayFHVR)
7. Trilateral Research (TRI)
8. Politecnico di Milano (POLIMI)
9. Belgian Federal Police (BFP)
10. Saarland University (USAAR)
11. Spanish National Police (MI)

Project Fiche

- Topic: **FCT-04-2015 - Forensics topic 4: Internet Forensics to combat organized crime**
- Duration: **36 Months** (**September 2016 – August 2019**)
- Budget:
  - Total: € 3,803,087
  - Requested: € 3,532, 000
- Consortium:
  - 2 SME's: TREE and TRI 3 public authorities: MJ, BFP, MI
  - 1 research centre: RISSC
  - 5 universities: UNIKENT, UCM, POLIMI, ByFHVR, USAAR

Project AIMS

- **OBJ.1** - Developing effective guidelines and collaborative methodologies for LEAs investigations
- **OBJ. 2** - Developing a set of tools for Internet Forensics
- **OBJ.3** - Demonstrating the impact of the RAMSES platform, through several pilot exercises in different countries, training and awareness campaigns.

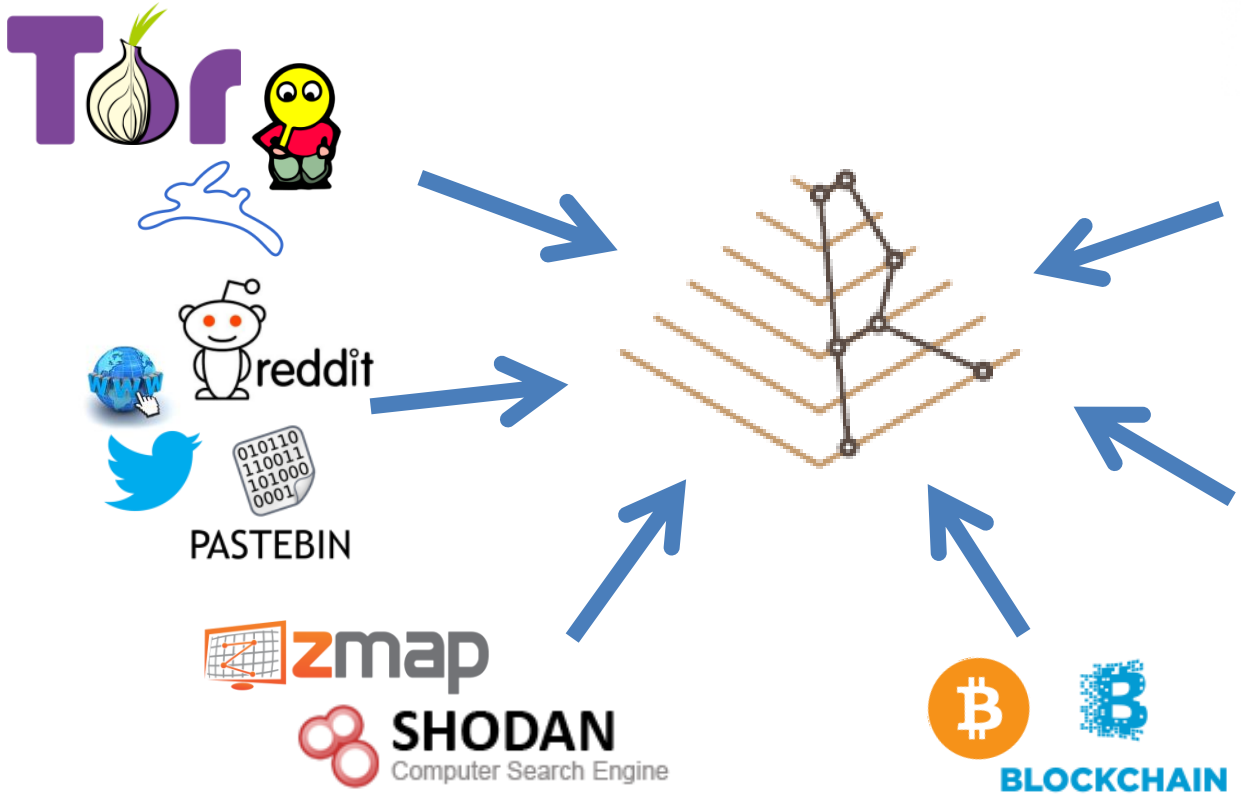


List of Work Packages (WPs)

WP No	WP Title	Partner No (L)	Short Name	Person-Months	Start	End
WP1	Project Management & Coordination	1	TREE	44,5	M1	M36
WP2	Policing Requirements. Scenarios definition	2	RISSC	45	M1	M9
WP3	Privacy, ethical and social impact assessment	7	TRI	26,5	M1	M36
WP4	Modelling ransomware for the point of view of Economic Theory and Applications	3	UNIKENT	32	M1	M18
WP5	Big Data infrastructure for data extraction, storage, analysis and exploitation	1	TREE	93	M3	M34
WP6	Forensic analysis of malware monetization techniques	8	POLIMI	48	M3	M24
WP7	Forensics Tools and techniques for discovering hidden information in malware samples	5	UCM	102,75	M3	M24
WP8	Validation pilot exercises	4	RISSC	92,25	M17	M36
WP9	Dissemination, Communication and Exploitation	6	BayFHVR	63	1	36
WP10	Ethics requirements	1	TREE	N/A	1	36
				547,5		

PLATFORM FIRST APPROACH

RAMSES Concept:



Malware Analysis, Steganography and Multimedia Forensics.

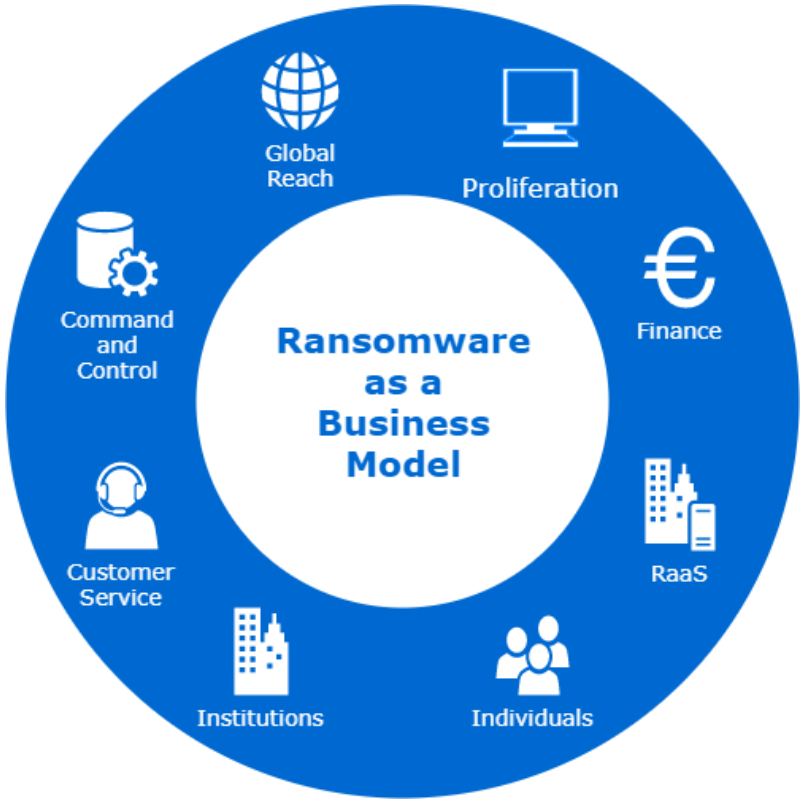
RAMSES tools

Politie Police

Fachhochschule für öffentliche Verwaltung und Rechtspflege in Bayern

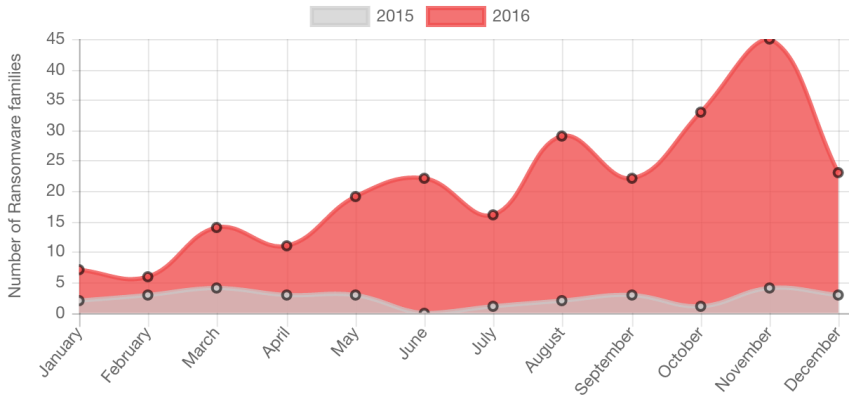
Economic Aspects of Ransomware

- Identify how Ransomware makes money
  - Revenue streams
  - Costs
- Predicting how this is likely to evolve
  - Response to competition from other criminals
  - Response to opposition LEAs
  - Response to defensive measures (e.g. backups)
- LEAs want to increase the cost to the criminal
  - A better informed/protected public increases likelihood that they will not pay ransoms
  - LEAs can reduce the perception of ransomware as a profitable enterprise before criminals realise their current ransom demands are sub-optimal!

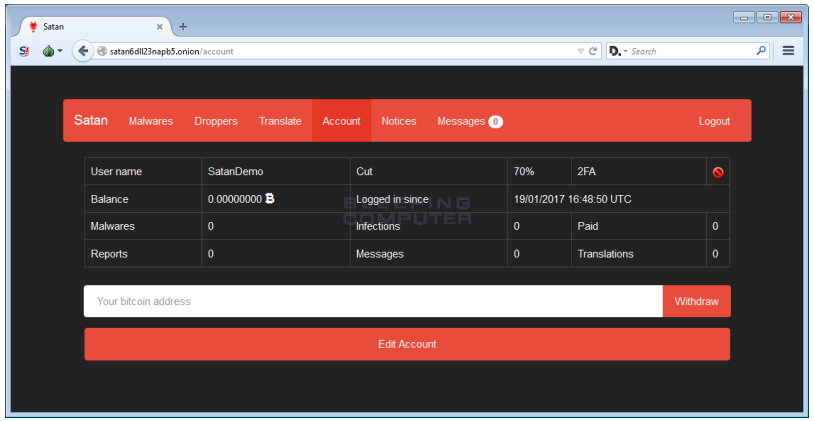


The Attacker's Costs

- Distribution networks may be purchased
- Ransomware as a Service (RaaS) is an upfront cost
- Staff and localisation are ongoing costs
- Sophistication increases cost
- Profit motives encourage efficiency



Graph showing a 725% spike in Ransomware Families (Trend Micro, Dec 2016)



Satan Ransomware Service Front-end (Bleeping Computer, Feb 2017)

Determining the Price of Ransom

- Uniform Pricing is most common
  - Simple, but must be set at an appropriate price
- Price discrimination requires additional information
  - Cooperative malware, and/or specific demographic
- Bargaining was found to diminish the attacker's position
  - Being known to negotiate invalidates your initial offering

FAMILY	STARTING DEMAND	LOWEST DEMAND	%DISCOUNT
CERBER	530	530	0%
CRYPTOMIX	1900	635	67%
JIGSAW	150	125	17%
SHADE	400	280	30%
			AVERAGE: 29%

Examples of Ransomware that allow negotiation (F-Secure, 2017)

Game Theory applied to Ransomware

- Consider a Game of Ransomware
  - A criminal wants to extract the maximum ransom for release of encrypted files
  - Their victim wants their files returned, but may not wish to pay
- R. Selten (1988) proposes a simple game of kidnapping
  - We consider the encrypted files to be the equivalent of a hostage
  - The criminal may choose to infect a machine, be caught, fail to extract ransom, destroy files, and/or receive their ransom
  - The victim can choose whether or not they pay
- Lapan and Sadler (1988) propose an extended game, accounting for deterrence
  - The victim may spend resources on prevention and mitigation measures
  - The criminal must succeed in infecting machines that they choose to target

Simple Game of Ransoming

1. The criminal decides if they will infect the victim's machine
2. Criminal sets ransom demand D > 0
3. Victim receives demand and may propose counter offer C
4. The criminal may irrationally destroy files, resulting in a payoff of –Y < 0 for the criminal, and –W < 0 for the victim
   i. Y represents the cost of time spent by criminal
   ii. W represents the victim's valuation of their files
5. Criminal may release files for C. If C < M (a minimum acceptable offer held secretly by the criminal), the files will be destroyed
6. The criminal may be caught with probability *q*. It is less costly to be caught having not destroyed files.
   i. -X is a reduction of cost –Z for the criminal for potential cooperation with authorities or perceived 'good' behaviour

Outcome	Payoffs	
	Criminal	Victim
Criminal doesn't infect computer	0	0
Release of files for C	C	-C
Files destroyed	-Y	-W
Criminal caught after release of files	-X	0
Criminal caught after destruction of files	-Z	-W

Table 1: Payoffs to different outcomes
Simple games of kidnapping
(Hernandez-Castro, Cartwright, & Stepanova 2017)

Opposed Game of Ransoming

1. Victim chooses how much to spend E on defensive measures
2. Criminal chooses whether to attack
   i. This incurs additional cost A on the victim, representing active countermeasures
3. The attack fails with probability $\theta(E)$
   i. θ is a continuous monotonically increasing function of E
   ii. With probability 1- θ(E) the attack succeeds
   iii. A failed attack costs the criminal –F (effort/resources expended)
   iv. A failed attack costs the victim –A-E (combined cost of defense)
4. If successful, criminal demands C as ransom
   i. Victim can choose whether or not they pay
   ii. If they pay, they regain their files. Criminal gets C and victim pays costs –C and -E
   iii. If they don't pay, their files are destroyed, and they incur costs –W (victim's valuation of files) and -E

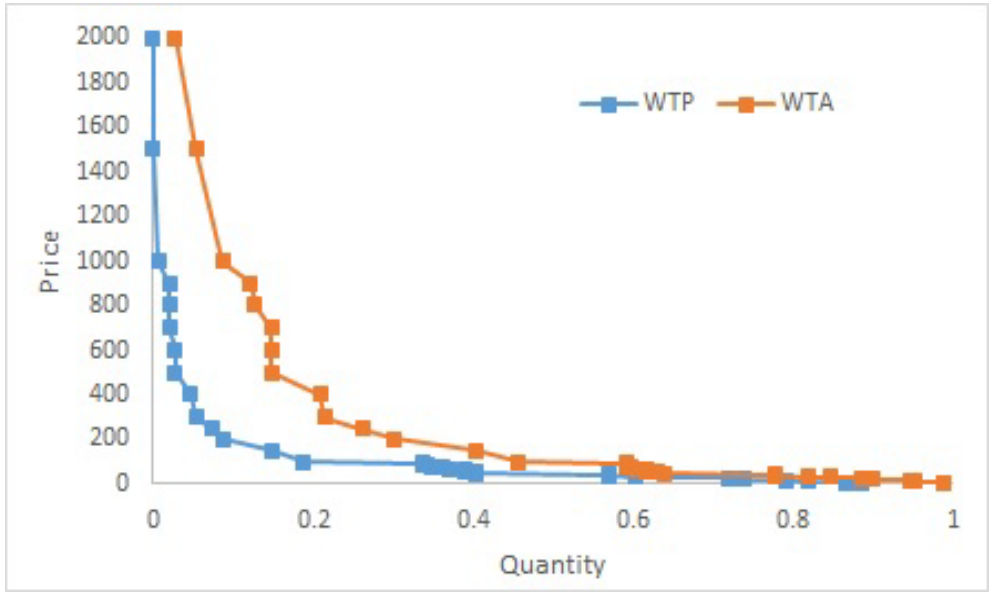
Outcome	Payoffs	
	Criminal	Victim
No attack	0	-E
Failed attack	-F	-A-E
Release of files for ransom C	C	-C-E
Ransom not paid	-L	-W-E

Table 2: Payoffs to different outcomes
Kidnapping with possible deterrence
(Hernandez-Castro, Cartwright, & Stepanova 2017)

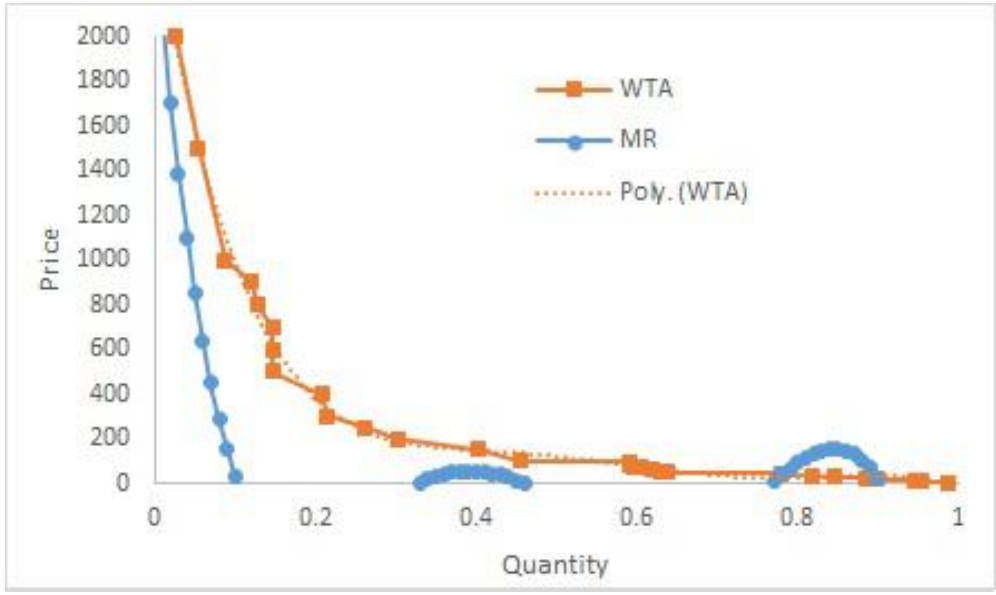
A Survey of Willingness to Pay

- A face-to-face survey was conducted
  - 149 respondents (54% male, avg. age 24)
- Two factors were tested: Willingness to Pay (WTP) and Willingness to Accept (WTA)
  - Horowitz & McConnell (2002) state that one typically observes a higher WTA than WTP
  - Bateman et al. (2005) argue that true valuation will be closer to WTA than WTP
  - Hernandez-Castro, Cartwright, and Stepanova (2017) identify that optimal ransom demands are found where marginal revenue equals marginal cost.

Survey Results



Demand curve elicited using Willingness to Accept and Willingness to Pay (Hernandez-Castro, Cartwright & Stepanova 2017)



Demand curve elicited using Willingness to Accept and Marginal Revenue (Hernandez-Castro, Cartwright & Stepanova 2017)

Current State of Ransomware as a Business

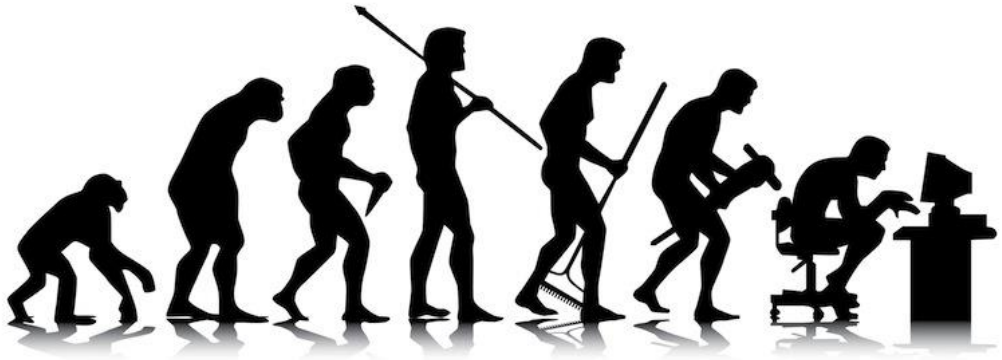
- Ransoms are currently too low
  - Too much focus on **quantity over quality**
- Price discrimination is primitive
  - Fantom had some basic price banding ability
  - Not generally seen in current ransomware
- Bargaining is seen as desirable
  - Lowering ransoms to increase number of payers
  - Suboptimal for the same reasons as low ransoms
- Some evidence of **marketization**
  - Ransomware as a Service
  - Botnet as a Service
  - Bitcoin tumbling
- **Customer Service is generally good though!**

	SUPPORT CHANNELS			NEGOTIATING		TOTAL
CRITERIA	Do they have a support form? Do they give an email address?	Responsiveness - Do they respond quickly, always within the day?	Helpfulness - Are they helpful when asked for assistance with making Bitcoin payment?	Did they lower the price?	Did they extend the deadline?	
POINTS POSSIBLE	2	3	3	2	1	11
CERBER	Good support form but no email.	Yes, very responsive.	Not helpful. However their site has pretty good Bitcoin instructions.	No	Yes	6
	1	3	1	0	1	
CRYPTOMIX	Email addresses	Yes, very responsive.	Not helpful.	Yes, two times.	Yes	7
	1	3	0	2	1	
JIGSAW	Messaging form was never online. Sent email message.	Yes, very responsive.	Very helpful. Offered a lot of assistance.	Yes	Yes	9
	1	3	3	1	1	
SHADE	Email, plus support form to use if no email response	Yes, very responsive.	Not helpful.	Yes	Yes	7
	2	3	0	1	1	
TORRENT LOCKER	Support form.	No response.	No response.	No	No	1
	1	0	0	0	0	

Customer service scores for 5 Ransomware strains (F-Secure, 2016)

Our Prediction: A Likely Path of Evolution

- Propagation will become increasingly random
  - Infect as much as possible, then differentiate
  - Requires pre-infection and/or real-time **intel**
- An understanding of economic strategy will emerge
  - Compartmentalization of tasks leads to specialization
  - **Review of data** from previous attacks fuels this change
- Ransom values will increase
  - The **quantity > quality fallacy** will likely be recognized soon
- **Price discrimination** will become more common
  - Optimal pricing is optimal within bands
  - Identifying strata of WTP/WTA allows **quantity** to increase **without compromising value**
- Cost-benefit analyses by businesses will be exploited
  - **Ease of payment** and knowledge of insurance costs will allow ransomware operators to exploit **convenience and reputation**



Conclusion

- Current ransomware strains show little economic sophistication
  - They show signs of experimentation with new concepts
  - Increased media attention and **awareness of profitability** will draw talent to this domain
- Ransomware will increase in economic sophistication
  - Marketization is very likely – **specialization is inevitable**
  - Ransom prices will **increase**
  - Price discrimination is very likely – the intelligence and techniques to gather more are already available
  - Cyber-criminals are likely to capitalize on **reputation and convenience** to increase the appeal of paying
  - A focus on total profit instead of the number of paying victims will emerge
- Next output of WP4: A software implemented predictive model
  - Focuses on profit maximization
  - Will allow LEAs and Researchers to identify likely developments
  - Countermeasures can be derived ahead of these developments appearing in the wild

Questions? Comments?

- Thank you!
  - Darren Hurley-Smith D.Hurley-Smith@kent.ac.uk