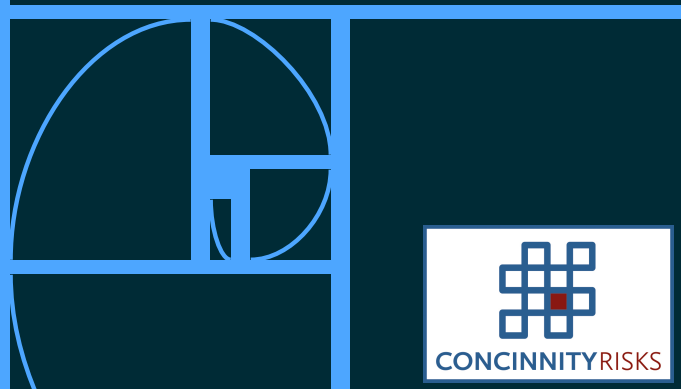
An ethical hacker's view of our world

IMCC 2018



Éireann Leverett:Founder
eireann <dot> leverett (at)
cantab <dot> net

Concinnity Risks

What is a day like for ethical hacker?
Long red team days.

Get a coffee, and check to see who clicked links yesterday.

- ✓ Yep, got the CEO
- X Didn't get the CFO
- Send them a fake text
- Analyse some computer programs for flaws
- Login into CEO's accounts that are in scope over lunch
- Use the flaws to compromise a safety critical system
- Yep got the CFO
- Have dinner
- Write exploits till midnight

If you think phishing rates will save you...
I can send more than one email, and I do A|B testing and stats.

9%

For three and a half years we simulated hacks on:
Power|Water|Sewage|OG|Marine|Aviation|Telecoms

I participated or ran over 70 assessments (avg 2 weeks) all over the world. To summarise that experience for you in a non technical manner:

1. Everything is a file.
2. Change that file and you change the world.
3. Understanding a system is the hardest part, but once you do, you can change the world.

Would you like a little demonstration?
Remember when I said everything is a file?

Can I get a volunteer? Well, the internet of today relies on phones.

So....

I understand the constraints of technological disasters
Accidental OR Malicious

For eample, many Internet of Things devices use SMS to accomplish various tasks. The ability to spoof text messages might:

- irrigate a field
- disable a firewall setting
- Give false sensor readings from bridge traffic detectors

The ability to spoof a text message in these environments can lead to very dangerous situations in malicious hands. While my "prank" here today is conducted in a safe environment, the real world runs on mobile phones, and doesn't ask kindly for volunteers.

A brief moment of philosophical advice...

Too much emphasis is made on *how* technology works or can be

I devote my life to exploring and understanding technical systems.
I can assure you it is not possible to master all **the hacks** or **the technologies**.
It is often the least important part.
What is less studied and more relevant is *why* people abuse technology.
You should also focus more on restoration, than on prevention!

Motivation: Insider Threat Sector: Offshore Oil & Gas
United States v. Azar (2:09-cr-00240)

After being turned down for a permanent position with a company, he logged back in a week later with his credentials and disabled crucial H2S gas alarms. If anything had gone wrong, people could have been injured or died on the platforms because of his actions. We're lucky he wasn't an actual hacker, or things might have been much much worse.

This is a lesson organisations need to learn quickly: how to quickly revoke credentials, and be confident of a lockout.

He was sentenced in 2009, but this simple illustration makes it clear, that even if systems are very secure, you will have insider threats, and some of those may lead to expensive, dangerous, or deadly consequences.

CONCINNITYRISKS

Motivation: Drug Smuggling Sector: Marine
Europol Intelligence Notification 004-2013

Phishing. Trojans. Keyloggers.

Figure: This allowed the criminals to pick up containers early, bypassing some customs checks.

Motivation: Ransom Sector: Marine
Maersk

- Heroicaly, reimaged 45k desktops and 4K servers in 0 days.
- This cost them 2-300 million.
- Will have an even wider impact on their downstream partners.
- This is probably affirmative, but what about the silent CBI?

CONCINNITYRISKS

Obligatory NotPetya Reference
CBI and Silent are a much bigger problem.

risk capital news & intelligence
reinsurance

REGISTER | SIGN IN
Search our site
NEWS ANALYSIS OPINION ADVERTISE ABOUT US CONTACT US

NEWS

PCS: NotPetya insured losses now $3bn+

4 September 2018

The industry's ultimate insured losses from the June 2017 NotPetya virus will now exceed $3bn with the majority emanating from silent - or non-affirmative - coverage, according to the independent loss adjudicator, Property Claims Services (PCS).

The update is an increase on a Q2 loss estimate which calculated the total insured loss at $2.7bn from the cyber virus.

The loss upgrade coincides with the launch of a new cat cyber loss index from PCS that may eventually lead to greater reinsurance and retro capacity being devoted to the fast expanding class.

Most popular


Marine insurers facing EUR590mn bill for Lürssen shipyard loss


China Re realises ambition with Chaucer acquisition

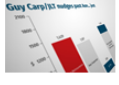

Guy Carp-JLT Re set to become largest reinsurance broker...just

Figure: Mostly silent, and roughly half of affirmative!

CONCINNITYRISKS

Compare that what ransomware made globally.
This is a pretty hefty externality.

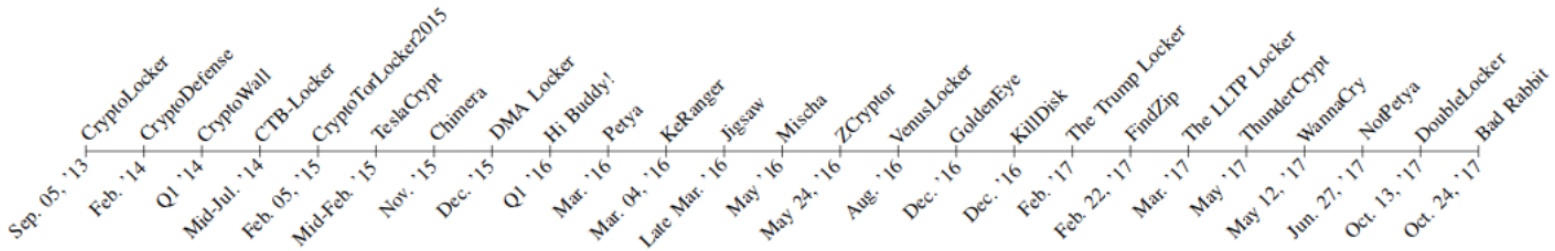


Figure 3: Occurrence of Bitcoin ransomware

Ransomware	Overall			Ransom		
	Payments	BTC	USD Value	Payments	BTC	USD value
CryptoLocker	51,766	133,045.9961	42,292,191.17	804	1403.7548	449,274.97
CryptoDefense	128	138.3223	70,113.41	108	126.6960	63,859.49
CryptoWall	51,278	87,897.8510	45,370,589.00	3,730	5,351.2329	2,220,909.12
DMA Locker	298	1,433.3463	580,763.95	117	339.4591	178,162.77
NotPetya	70	4.1787	10,284.42	33	4.0576	9,835.86
KeRanger	13	10.0044	4,175.35	10	9.9990	4,173.12
WannaCry	341	53.2906	99,549.05	238	47.1743	86,076.76

Table I: Summary of overall payments and ransom payments to the ransomware for which the observed payments align with their period of activity and ransom demands

Figure: Approximately 88.4M USD[1] across all families of ransomware.

[1] https://arxiv.org/pdf/1804.01341.pdf

Estimated losses from Ransomware
You're writing affirmative cyber, aren't you?

So payouts are 34 x the ransoms earned by by the malware authors.

CONCINNITYRISKS

What is the most popular cipher in Ransomware?

You know weird things, Eireann.

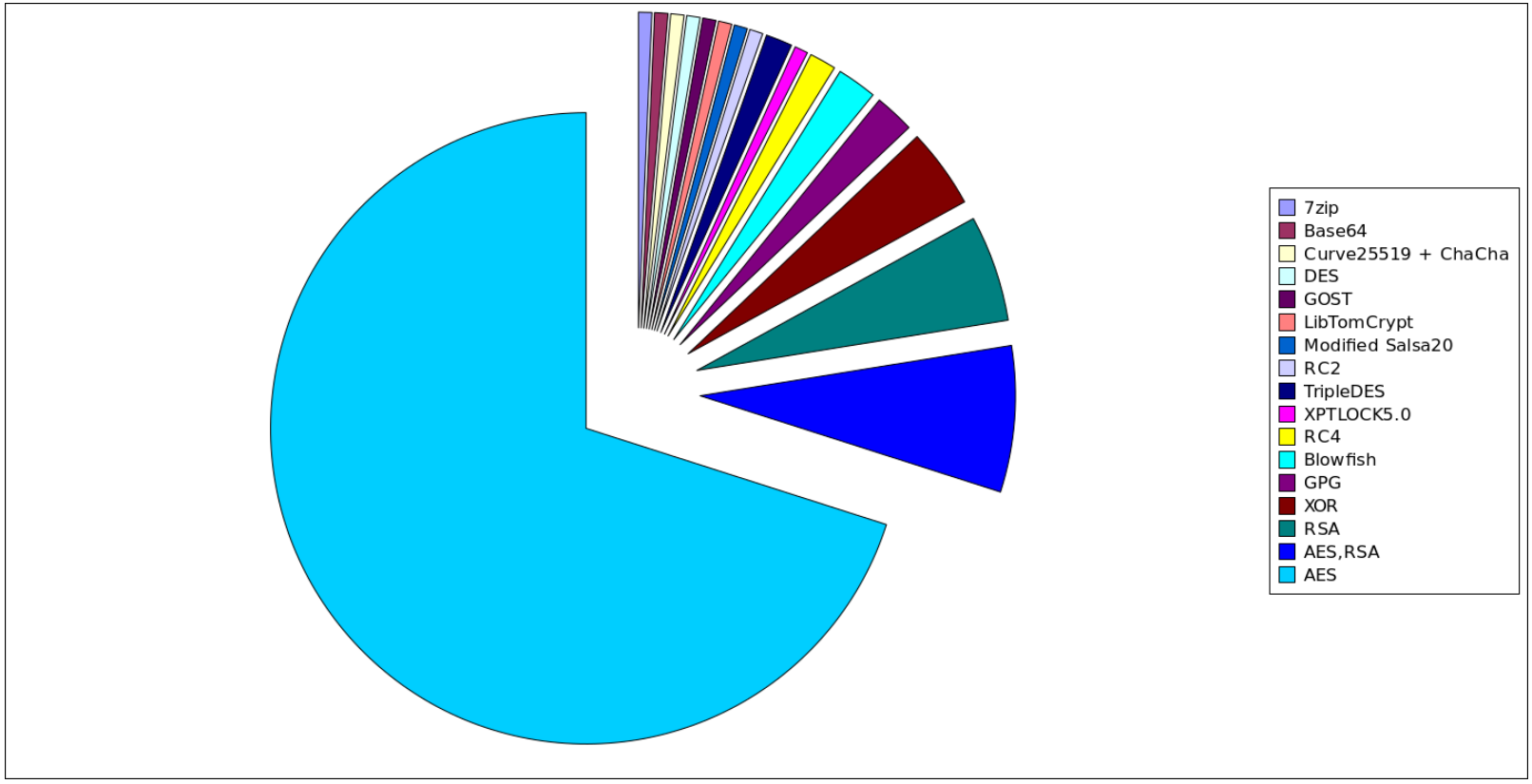


Figure: We have a clear winner!

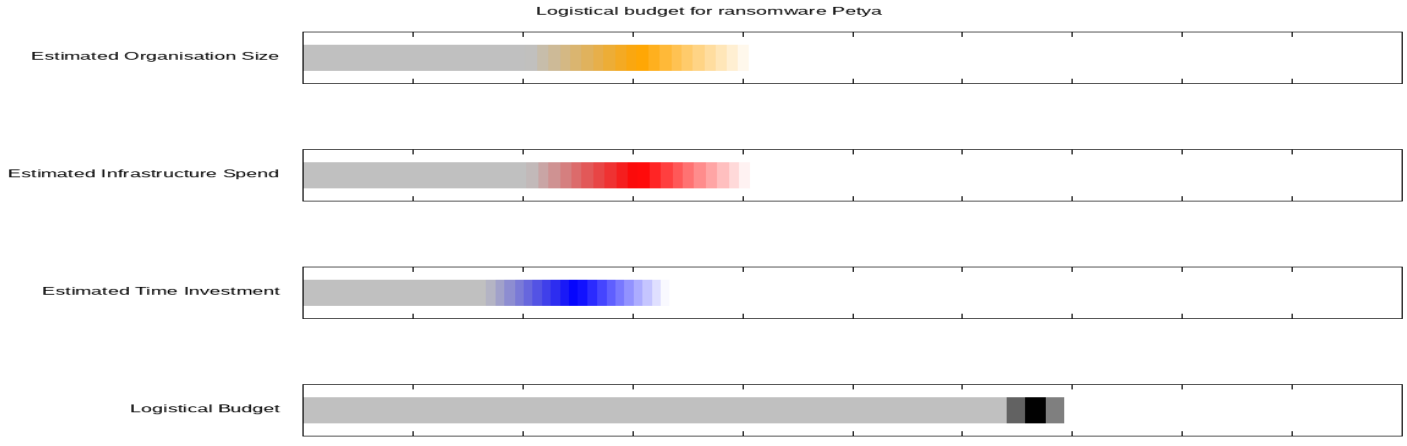
Just for laughs, cost benefit of AES
Did I mention I like maths?

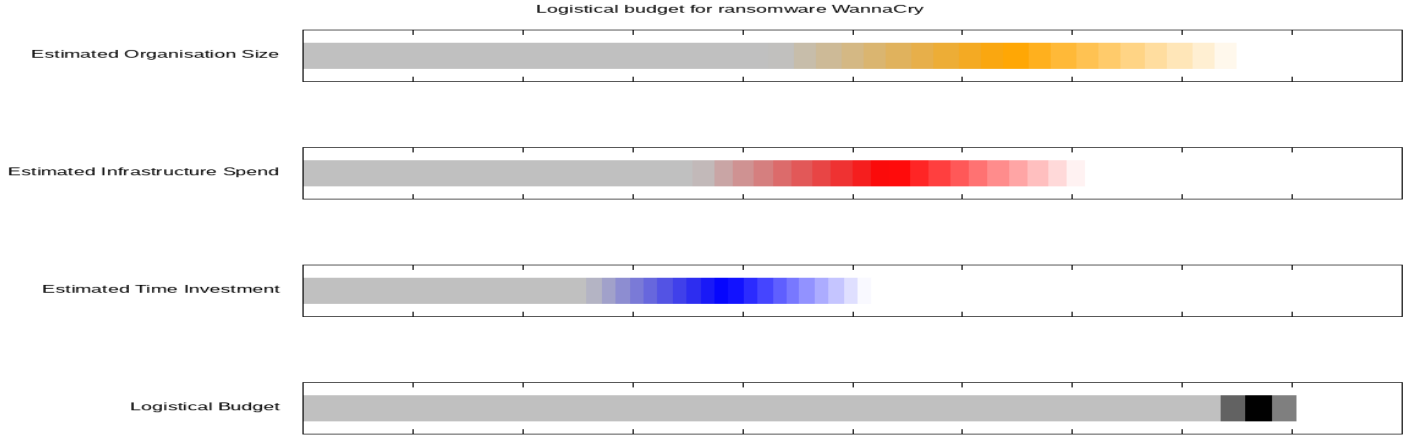
250B[2] VS 1.98B (0.66 cipher share of 3B+)

[2] https://nvlpubs.nist.gov/nistpubs/gcr/2018/NIST.GCR.18-017.pdf

CONCINNITYRISKS

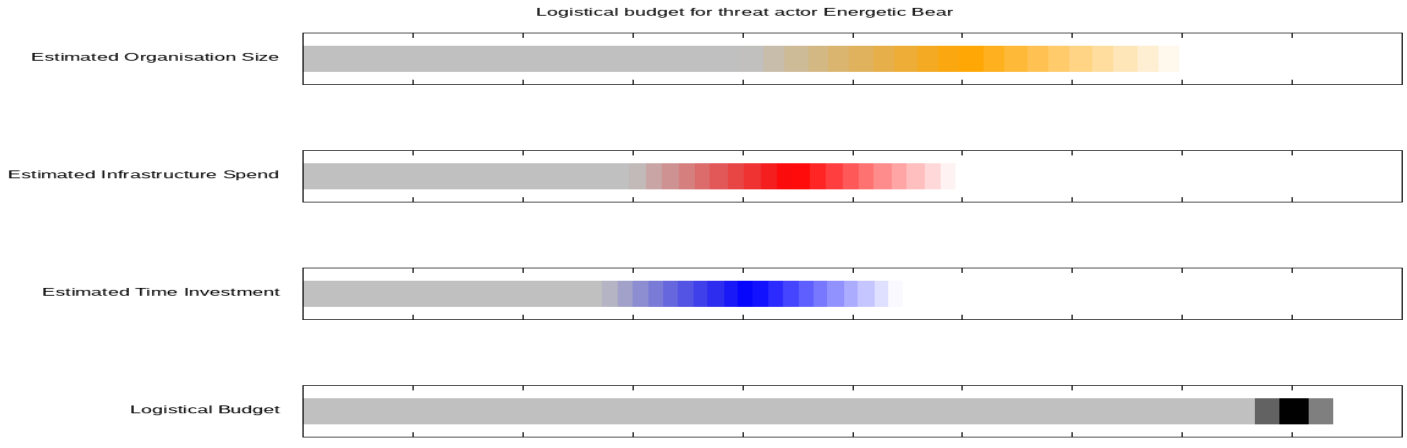
Can we compare ransomware strains quantitatively?
Towards risk quantification

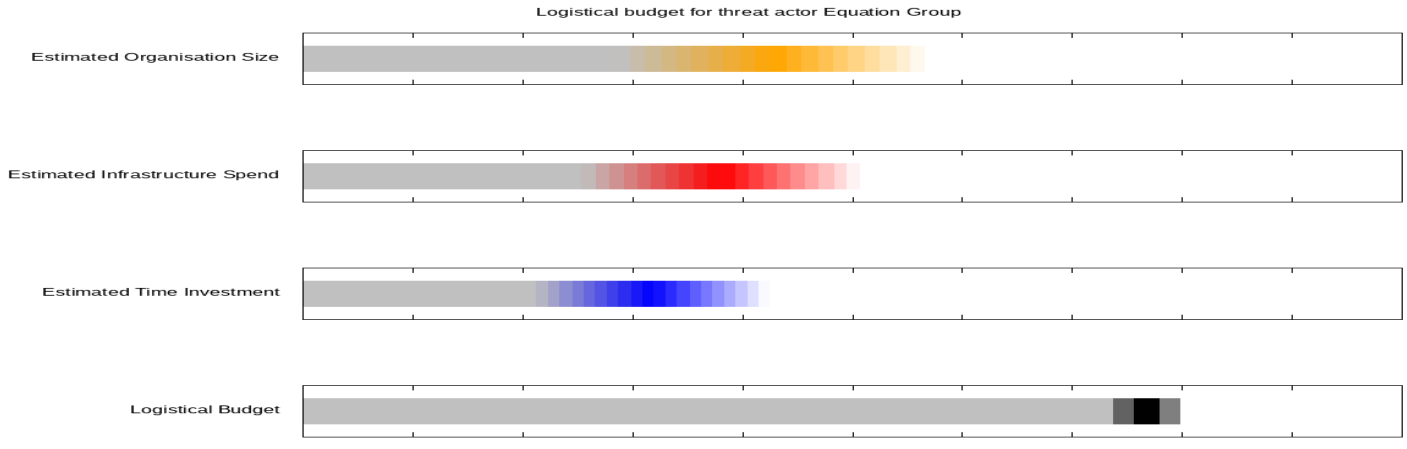




CONCINNITYRISKS

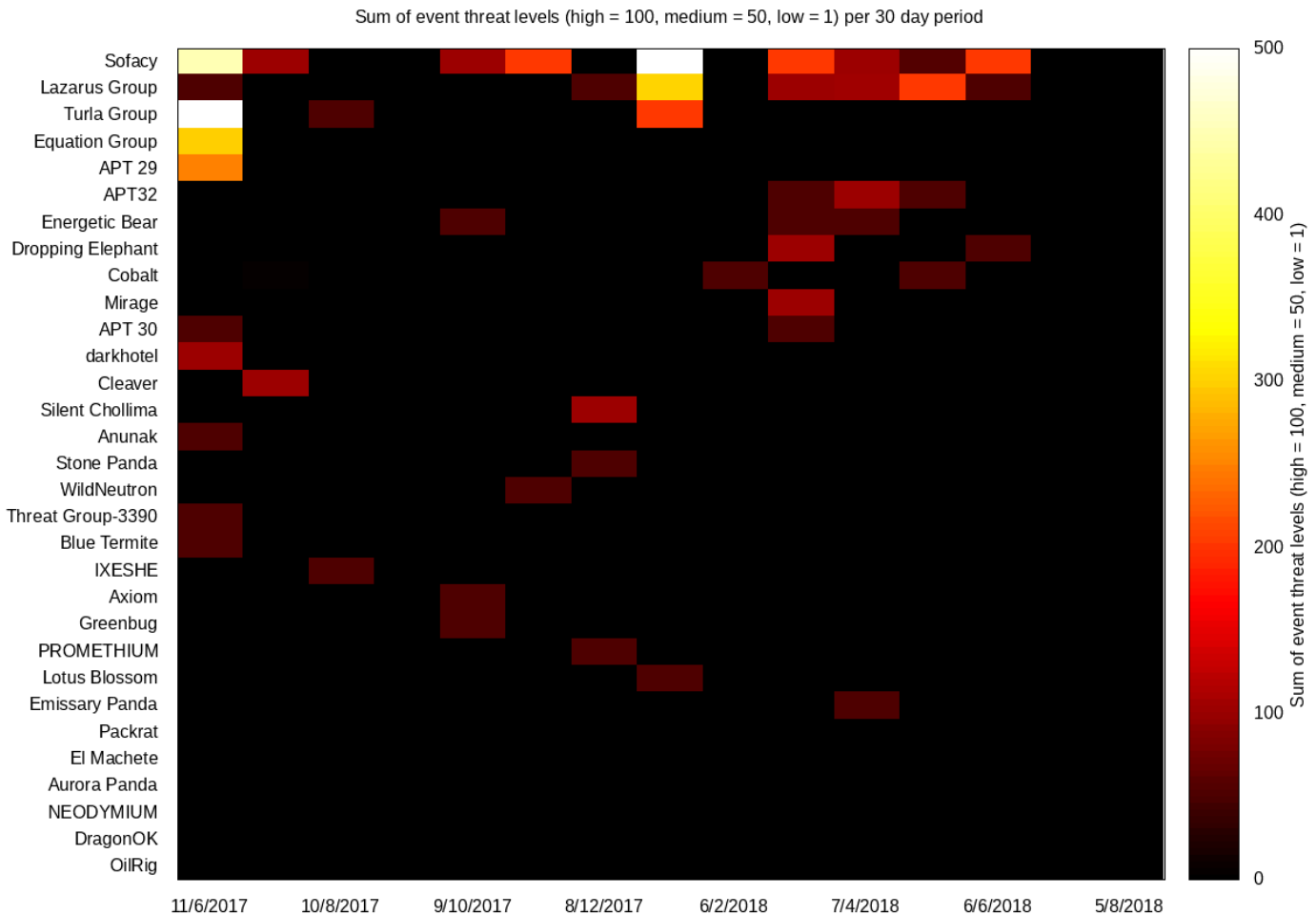
Not only can we do this for ransomware...
But also threat actors generally!





CONCINNITYRISKS

What happens when we put all this together?
Over time?



Booters and Stressors
A tour of the criminal underground

A collection of illegal[3] websites offer services to *boot* computers and/or *stress* networks

- 7-17k attacks of this type witnessed daily.
- 90% of attacks $<$ 1 hour
- DDoS coverage for insurance policies is AFTER 8 hours
- 75% of victims are only targeted once
- 5 bucks was the cheapest booter/stressor cost
- In Q3 2014, some researchers found and talked to over 43 of these "services"[4]

[3] Depending on jurisdiction and usage

[4] https://www.tandfonline.com/doi/abs/10.1080/01639625.2016.1169829

Distributed Denial of Service is a growth industry

CONCINNITYRISKS

DDoS is not just virtual harm...
It is starting to have real world impacts

DDoS Attack Takes Down Central Heating System Amidst Winter In Finland

November 09, 2016 Mohit Kumar

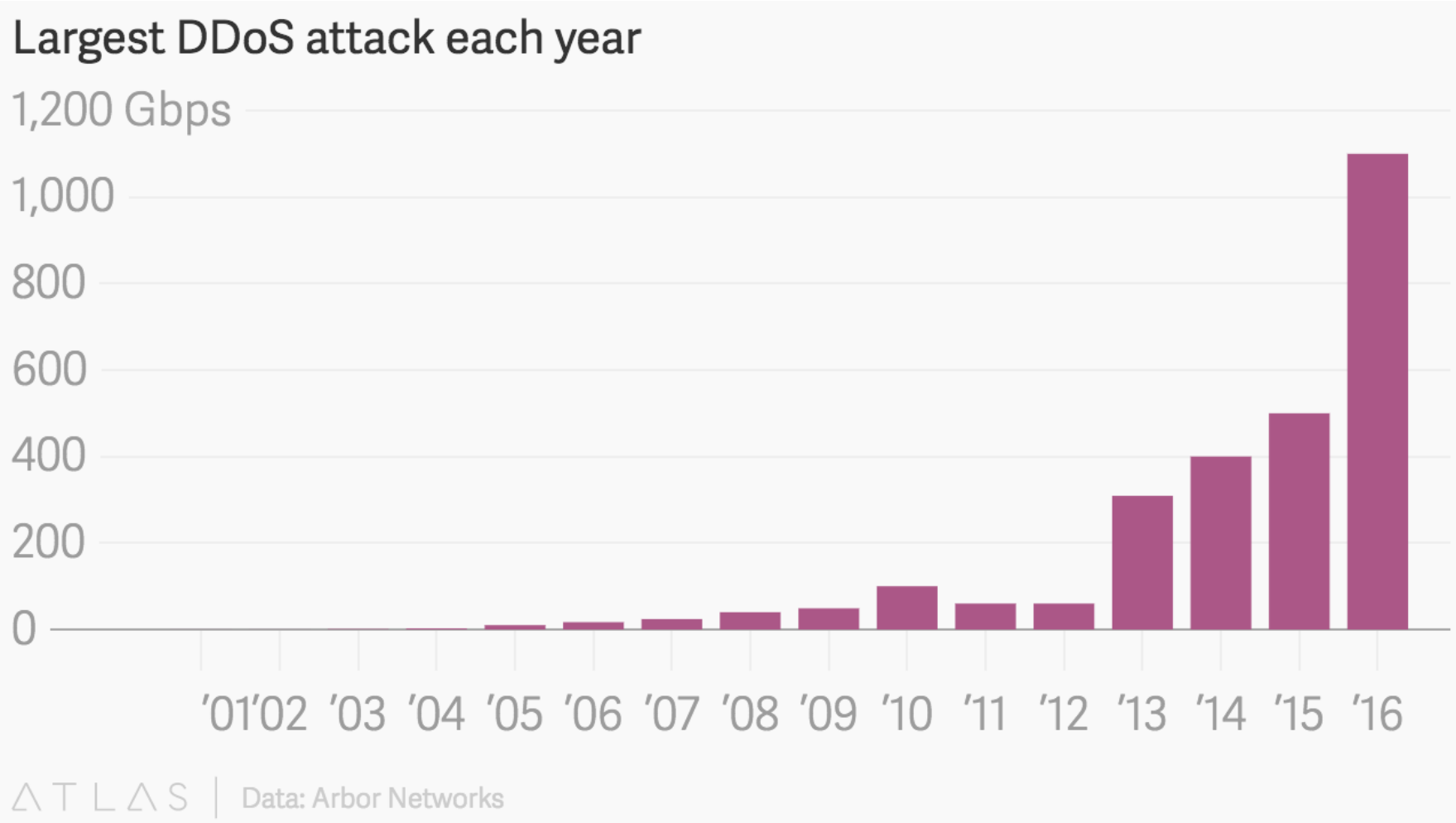
SPONSORED
Patch Management
Software Deployment

Figure: It's only a matter of time before DDoS causes loss of life.

Distributed Denial of Service is a growth industry

CONCINNITYRISKS

Estimating a DDoS Catastrophe
Historical sizes



Distributed Denial of Service is a growth industry

We can (and did!) do better.
Estimate Potential Cat from potential.

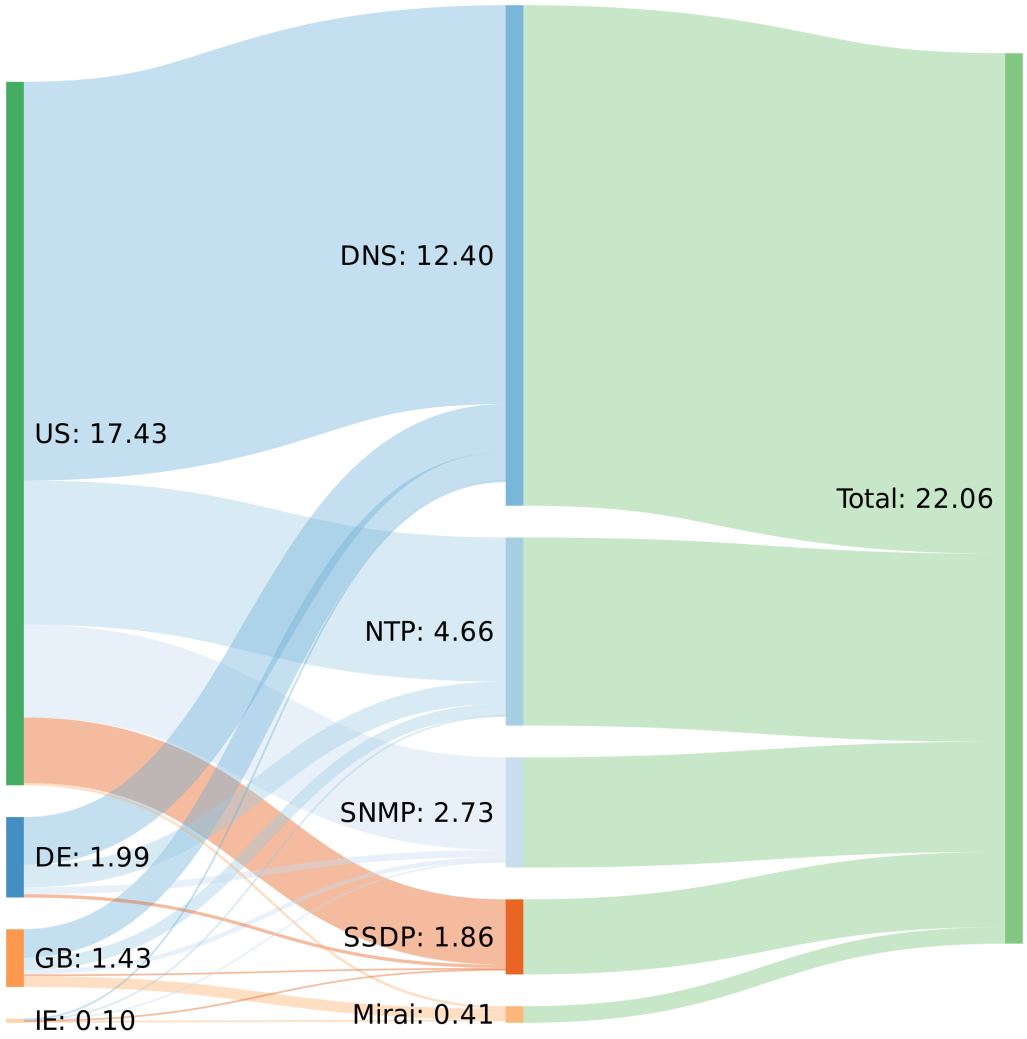
$$113.76 \text{ Tb/s}^5 > 4.8 \text{ Tb/s}$$

[5] https://www.measurementlab.net/publications/Leverett-Kaplan-2017.pdf

Distributed Denial of Service is a growth industry

CONCINNITYRISKS

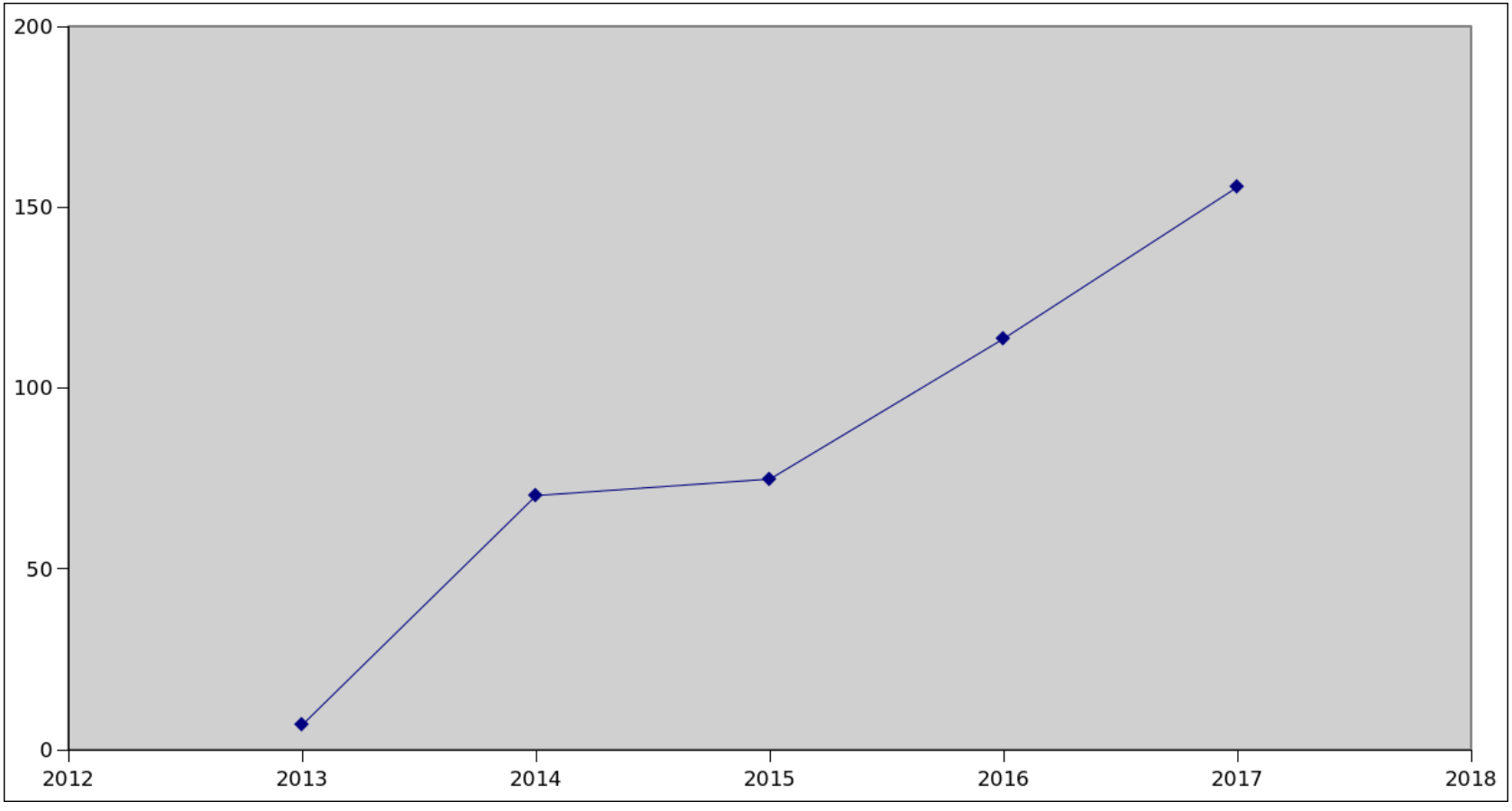
We can also break down by country...
Or protocol.



Distributed Denial of Service is a growth industry

CONCINNITYRISKS

The severity potential is growing...
which is why it is so cheap to make booter/stressor sites!



Conclusions
Don't trust text messages!

- Hacks are growing in severity, frequency, and losses
- It helps to have someone who knows how to break things
- Ransomware is quantifiable and insurable
- DDoS is quantifiable and insurable
- Exclude and affirmative!
- Do not stay silent!

CONCINNITYRISKS

A plug for our upcoming book
Shameless!

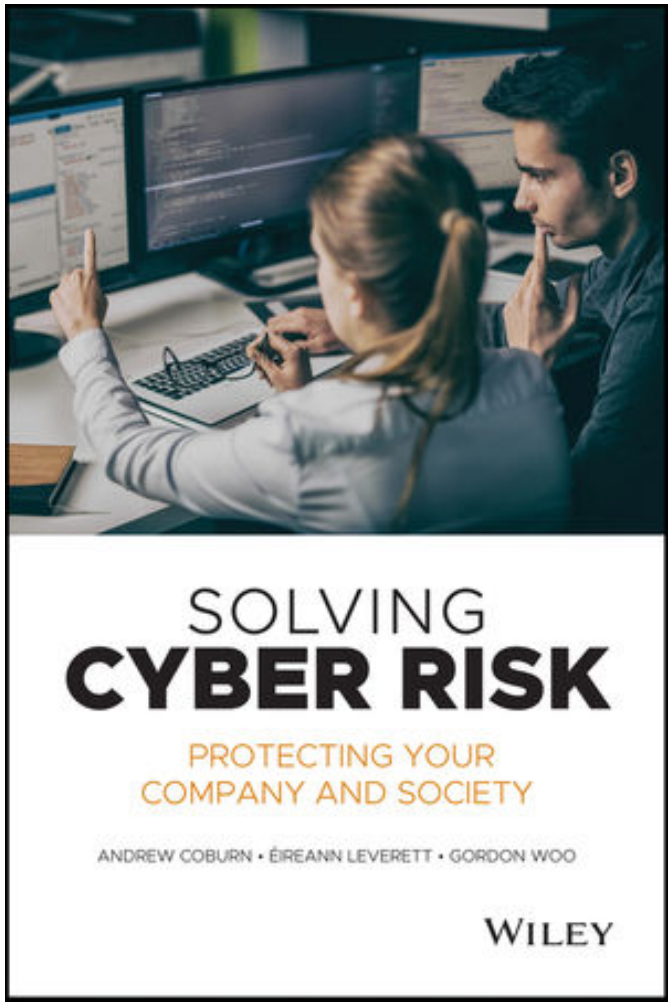


Figure: Out in January, 2019