Don’t know much about security

Martijn Grooten, Virus Bulletin

26 April 2018

Things I have done

- Mathematician
- Editor of Virus Bulletin
- Security software tester
- Conference speaker
- Lived in NL, UK, GR
- (Too) active on Twitter

Things I haven’t done

- Reverse-engineered malware
- Written a detection engine (or module)
- Found a serious vulnerability (except in my own code)
- Attended one of the Las Vegas conferences
- Finished my PhD
- Learned to speak Greek

Something I also haven’t done

Prepare a TED-like talk.

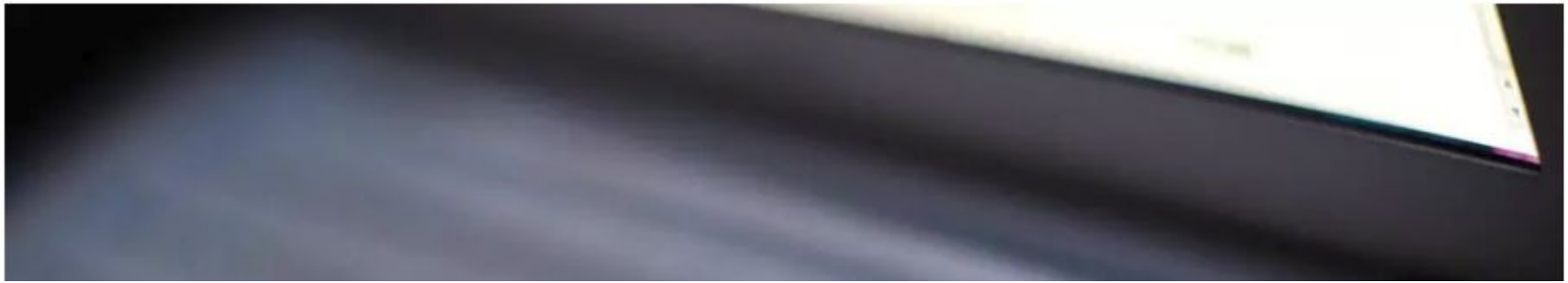
So do interrupt me if you feel like doing so.

News › Technology

Councils 'targeted by nearly 100 million cyber attacks in five years'

TOM POWELL | 1 day ago | 0 comments

Like Click to follow The Evening Standard



Evening Standard, Tuesday 20 February 2018

Durham	approx 1.3 million per month	0	0	0	
Hartlepool	2	0	1	0	
Darlington	Records not held	0	0	0	

Some things we don’t know

- How much spam is sent?
- How much malware is there?
- How many users get infected with ransomware?
- What are the largest botnets?
- How much does cybercrime cost?
- Who is really behind most nation state attacks?

What I have issues with

- Numbers that don’t mean anything other than “this is huge!”
- Irrelevant data pretending to say something
- A false sense of accuracy

(Full disclosure: I have been guilty of all of this.)

What I don’t have issues with

- The mere fact that there is a lot we don’t know
- White papers aren’t hard science
- Marketing

How much spam is sent?

- We can define well enough what spam is
- But what is “a single email”? What if it has multiple recipients? Is blocked at the SMTP level? Isn’t sent to a real user?
- The “Heisenberg uncertainty” of measuring spam

How much malware is there?

- We can define well enough what malware is
- But what is “a single piece of malware”? Same hash? Same family? Same variant within family? Does it have to be used in the wild?
- We can only measure what we know
- Did I mention the malware naming issue?

How many users get infected with ransomware?

- Every infection shows a mistake in “measuring”
- What do we count as an infection
- Do we trust the vendors or the criminals?

How much does cybercrime cost?

- ...and who is getting the money?
- How does this relate to other crimes?
- Could we get insurance to cover the “final percentage”?
- A lot of costs can’t be expressed in “euros”.

Who is really behind most nation state attacks?

- False flags!
- Fourth-party collection!
- Attackers for hire

How bad are things really?

- Not all security stories have a real-world impact
- We may make a huge deal out of relatively small events

And… what actually works?

- Security is a multi-layered approach, not just “products”
- Adversaries adapt their strategies to the defenses applied
- False positives are inevitable but hard to count the cost of

What can we do better?

- Don’t produce “large numbers”
- Look for trends
- Look for the data that we could use
- Appreciate that sometimes things are getting better

And now...

Let’s discuss!

martijn.grooten@virusbulletin.com

@martijn_grooten (DMs open)