



***THE HAND THAT STRIKES,  
ALSO BLOCKS***

***HITB2023AMS***

***SAUMIL SHAH***

ringzero.training

# SAUMIL SHAH

founder

ringzerø

hacker,  
trainer,  
speaker,  
entrepreneur,  
rebel

educating,  
entertaining,  
and exasperating  
audiences since 1999





2006  
4 items



2008  
7 items



2009  
27 items



2010  
8 items



2011  
1 item



2012  
13 items



2015  
3 items



2017  
28 items



2018  
5 items



2019  
3 items



2021  
5 items



2023  
1 item



gsec  
27 items



misc  
3 items





**A TALE OF TWO KEYNOTES**

  
**black**  
ASIA




A man with glasses and an orange shirt is speaking at a podium. The podium has a laptop on it and a logo for 'black hat ASIA 2017'. The background is a green wall with light patterns.

**ATTACKS SUCCEED  
BECAUSE DEFENSE IS  
REACTIVE.**

SAUMIL SHAH  
"The Seven Axioms Of Security"  
BH ASIA 2017

  
**black hat**  
ASIA 2017

A man with short blonde hair and glasses, wearing a dark blue button-down shirt, stands behind a dark podium. He is speaking into a microphone. The podium features the Black Hat Asia 2017 logo, which includes a silhouette of a person wearing a hat inside a circle, above the text "black hat" and "ASIA 2017". The background is dark with a green light projection on the left side.

**ATTACKS ARE A  
TECHNICAL PROBLEM,  
DEFENSE IS A  
POLITICAL PROBLEM**

THOMAS DULLIEN,  
"Why we are not building a  
defendable Internet" BH ASIA 2017

  
**black hat**  
ASIA 2017



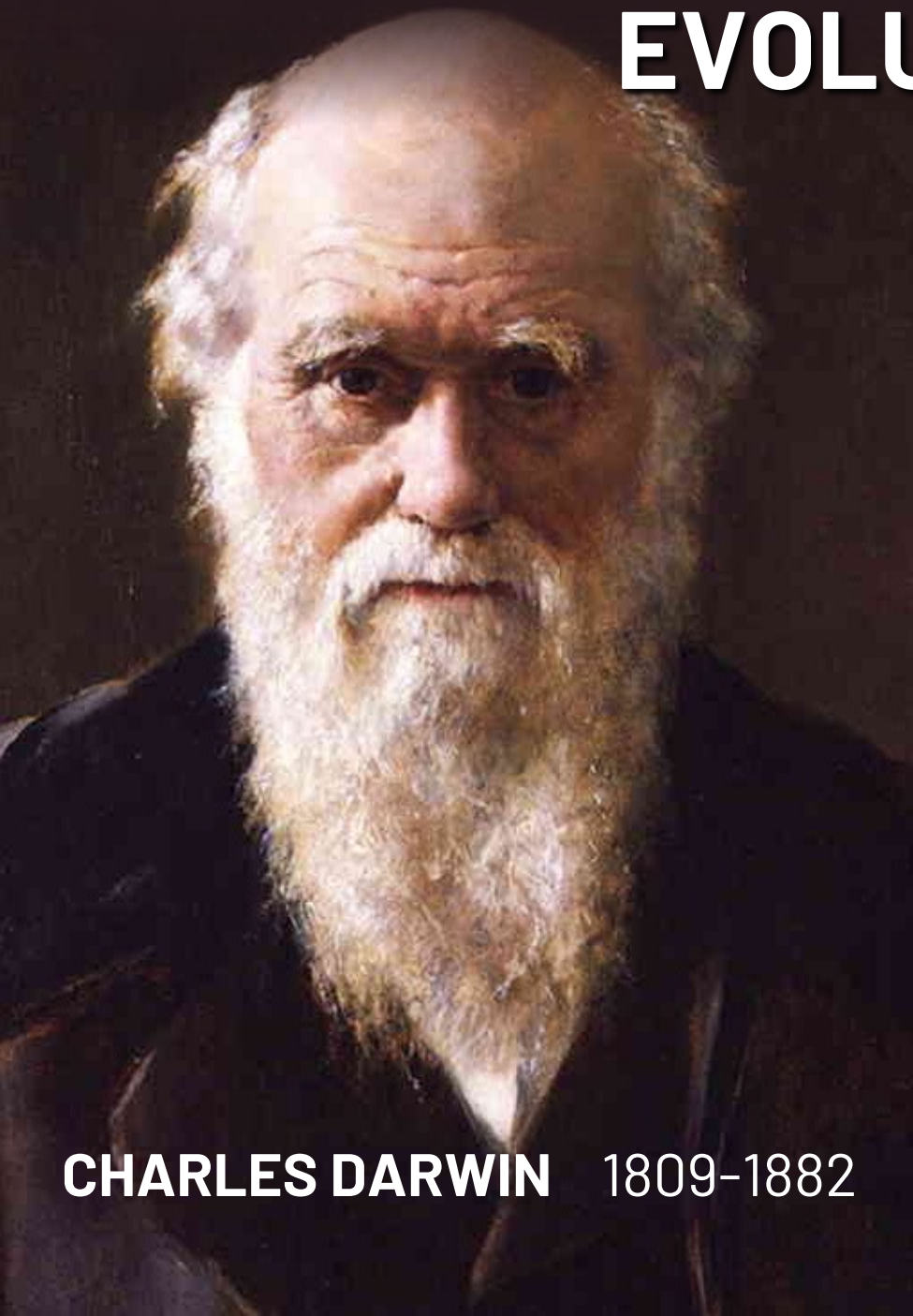


**THIS IS A TALK ABOUT**

**EVOLUTION  
ATTACKS  
DEFENSE  
PEBKAC**



# EVOLUTION



**CHARLES DARWIN** 1809-1882



**GORDON MOORE** 1929-2023



# EVOLUTION & MOORE'S LAW

"The number of  
components per  
Integrated Circuit  
shall double every  
couple of years"

- Gordon Moore, 1965





# Virginia Tech System X: Nov 2003

A photograph of a man in a grey blazer and glasses standing in a server room. He is looking at a laptop computer that is open on a server rack. The room is filled with rows of server racks, each containing numerous circuit boards and components. The lighting is dim, with some blue light emanating from the server racks.

12  
1100 PowerMac G5's  
12 TFLOPS  
#3 Supercomputer in  
the world, Nov 2003  
> 10 TFLOPS, < \$10M

Dr. Srinidhi Varadarajan



# NVIDIA AGX Xavier: Nov 2019

## Jetson AGX Xavier

512-Core Volta GPU with 64 Tensor cores

11 TFLOPS (FP16)  
22 TOPS (INT8)

(2x) NVDLA Engines

5 TFLOPS (FP16)  
10 TOPS (INT8)

### Nvidia Jetson AGX Xavier Developer Kit

by nVidia

★★★★★  8 ratings

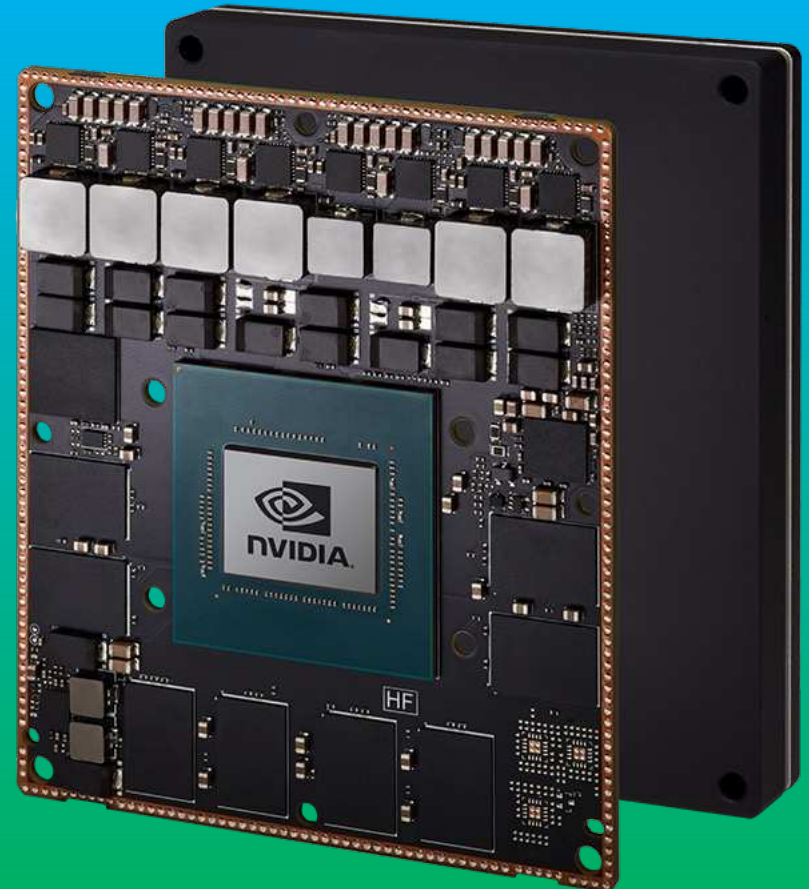
M.R.P.: ₹ 2,43,599.00

**\$1715**

Price: ₹ 1,23,990.00 **FREE Delivery.**

You Save: ₹ 1,19,609.00 (49%)

Inclusive of all taxes



# 2007 - Evolutionary Milestone



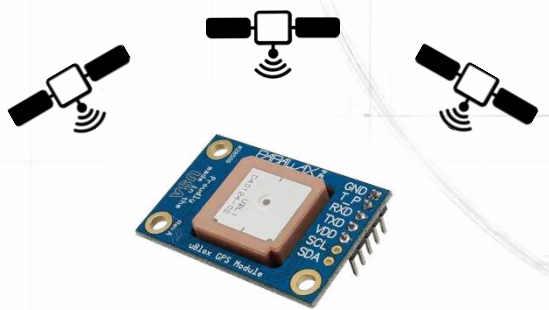
=



**The Microprocessor is the new Transistor**

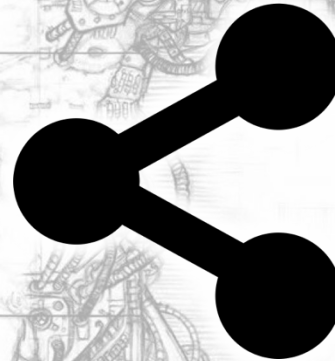
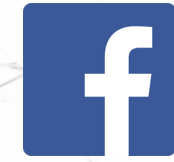
# 2007

# 3G



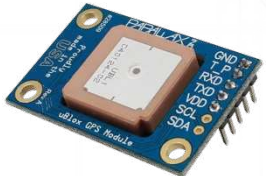


# 2007 - Social Virtualization



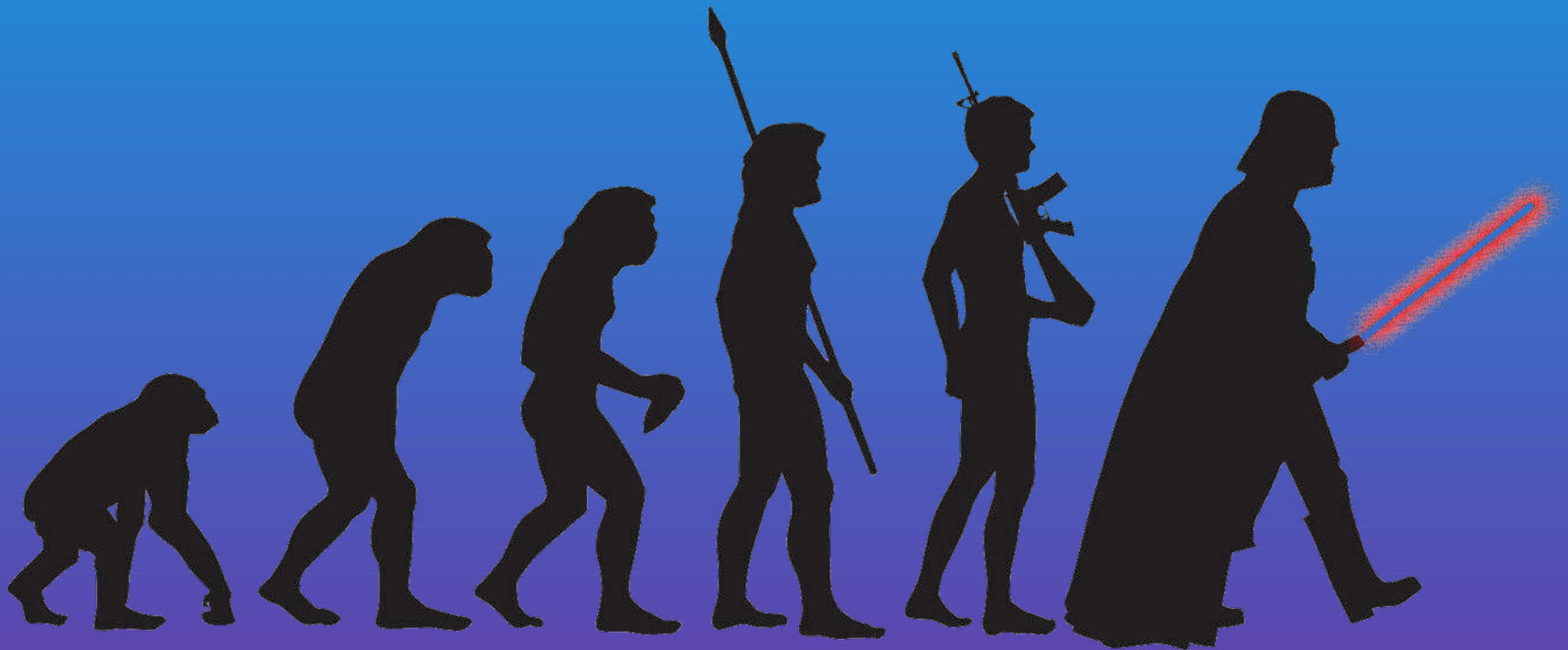
# 2007 - Autonomy

3G 





# The Evolution of Attacks: 2001-20



# Exploit Development - 2002

Individual effort.  
1 week dev time.  
3-6 months shelf life.  
Hundreds of public domain exploits.

"We did it  
for the LOLs."





# Evolution of Targets



Servers

Applications

Desktops

Browsers

Pockets

Minds

# Attacks Follow The Money

A man in a dark suit and sunglasses is seated in the foreground, looking towards the right. In the background, a desert landscape features a green military truck with a canvas cover, and several soldiers in olive drab uniforms. One soldier in the mid-ground is holding a yellow helmet. Another soldier in the foreground is wearing a maroon beret. The scene is set in a dry, hilly desert environment under a clear sky.

Defacement  
and DDoS

ID Theft and  
Phishing

Financial  
Fraud

Targeted  
APT

Ransomware

Nation State



# Evolution Quiz:





Wana Decrypt0r 2.0

## Ooops, your files have been encrypted!

English



### What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

### Payment will be raised on

5/22/2017 12:06:15

Time Left

02: 23: 59: 47

### Your files will be lost on

5/26/2017 12:06:15

Time Left

06: 23: 59: 47

[About bitcoin](#)

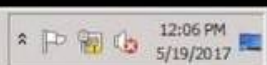
[How to buy bitcoins?](#)

[Contact Us](#)

**Send \$300 worth of bitcoin to this address:**

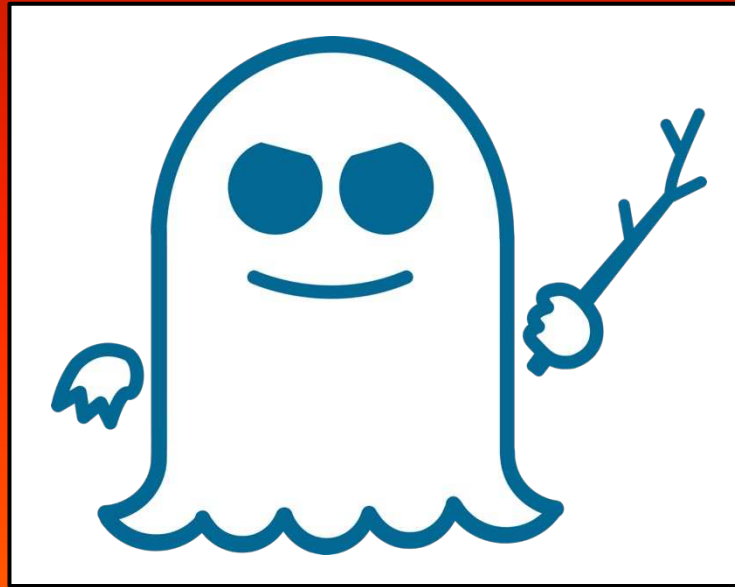
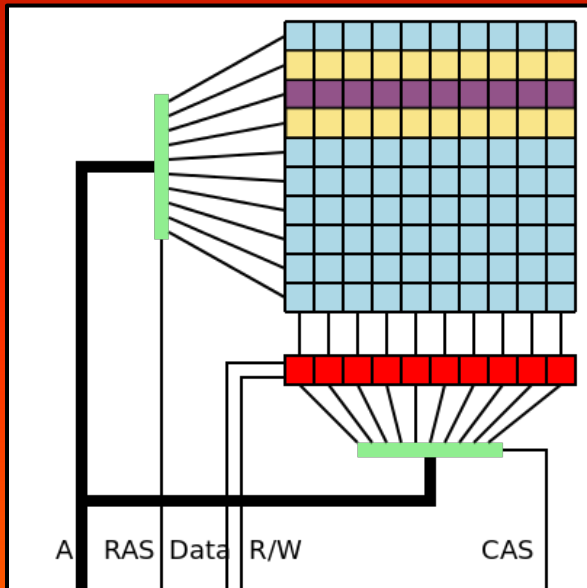
 **115p7UMMngo1pMvkcHijcRdfJNXj6LrLn**

your important files  
xt, but don't see the  
s removed the decrypt  
ter.  
files you have to run  
lication file named "  
ore from the antiviru  
instructions!





# ROWHAMMER, SPECTRE, MELTDOWN



Do Attackers and Defenders even fully understand them?

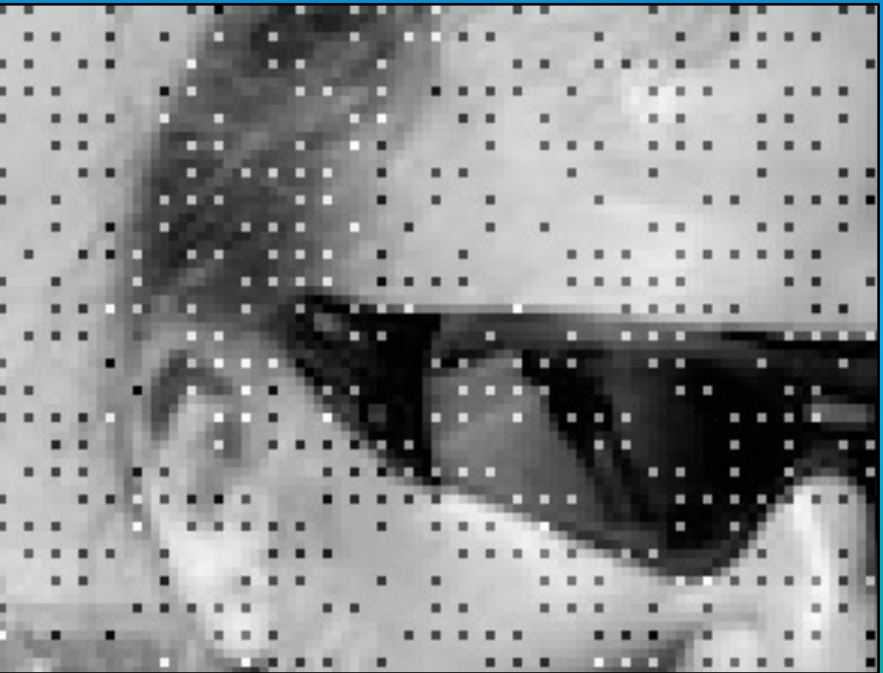
# STEGOSPLOIT

EXPLOIT  
CODE

PIXEL  
ENCODER

ENCODED  
IMAGE

IMAJ  
S



STEGO-  
DECODER  
JAVASCRIPT

POLYGL  
OT



TARGET BROWSER

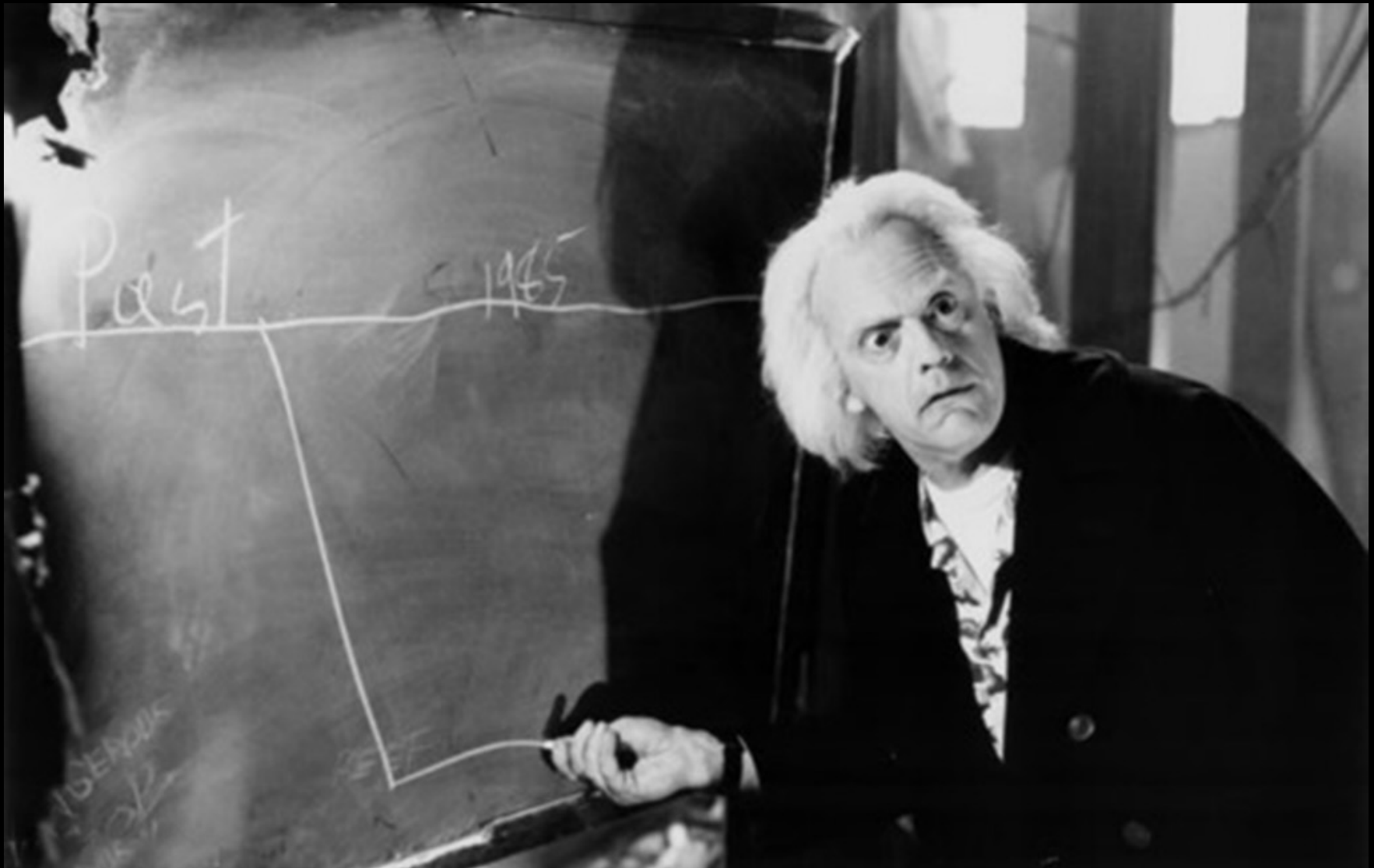


# NAKATOMI SPACE



wherein buildings reveal near-infinite interiors, capable of being traversed through all manner of non-architectural means.

# TWO TIMELINES





# Timeline 1: A new species evolves

ReIRO /GS **CFG** NOZZLE  
**DEP** Isolated  
Heap SEHOP  
**ASLR** SafeSEH



MitiGator



halvarflake @halvarflake

28/02/17

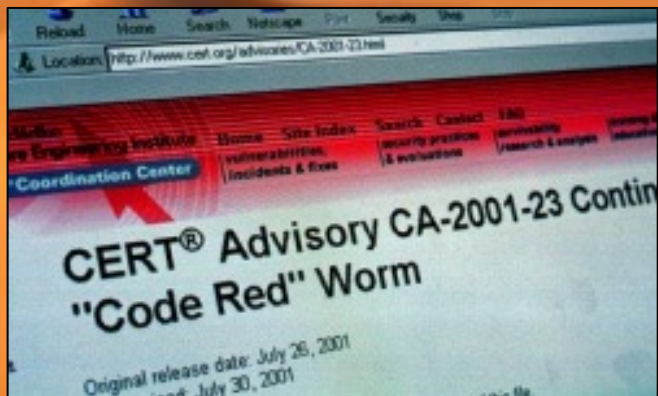
MitiGator. The well-intentioned, but short-sighted and not terribly effective alligator, always working to make exploitation harder. [pic.twitter.com/iUdaeur8P](https://pic.twitter.com/iUdaeur8P)



↻ 113

♥ 174

# Timeline 2: Microsoft 2001



```
6E 63 nterfaces Conc
56 2E ept Virus(CV) V.
29 32 6, Copyright(C)2
56 2C 001, (This's CV,
4D 45 No Nimda.) MIME
```

## It's Time to End Information Anarchy

By Scott Culp  
October 2001

*Code Red. Lion. Sadmind. Ramen. Nimda.* In the past year, computer worms with these names have attacked computer networks around the world, causing billions of dollars of damage. They paralyzed computer networks, destroyed data, and in some cases left infected computers vulnerable to future attacks. The people who wrote them have been rightly condemned as criminals. But they needed help to devastate our networks. And we in the security community gave it to them.

It's high time the security community stopped providing blueprints for building these weapons. And it's high time computer users insisted that the security community live up to its obligation to protect them. We can and should discuss security vulnerabilities, but we should be smart, prudent, and responsible in the way we do it.



From: Bill Gates

Sent: Tuesday, January 15, 2002 5:22 PM

Subject: **Trustworthy computing**

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people.

Over the last year it has become clear that ensuring .NET is a platform for **Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing -- or able -- to take advantage of all the other great work we do.**

Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.



# MICROSOFT STRIKES BACK



**Organization for Internet Safety**

## **Security and IT Industry Leaders Form Organization for Internet Safety**

*New Alliance Will Propose Best Practices for Handling Security Vulnerabilities*

**Sept. 26, 2002** — The Organization for Internet Safety (OIS), a unique alliance of leading technology vendors, security researchers and consultancies, today announced its formation. The OIS was formed to propose and institutionalize industry best practices for handling security vulnerabilities to ensure that security and technology vendors, and security researchers, can more effectively protect Internet users. Founding members of the OIS include @stake, BindView Corp., Caldera International, Inc. (The SCO Group), Foundstone, Guardent, Internet Security Systems, Inc., Microsoft Corp., Network Associates, Oracle Corporation, SGI and Symantec.



# 2005: CiscoGate – Michael Lynn

[Blog](#) >

## Cisco Harasses Security Researcher

I've [written about full disclosure](#), and how disclosing security vulnerabilities is our best mechanism for improving security -- especially in a free-market system. (That essay is also worth reading for a general discussion of the security trade-offs.) I've also written about how security companies treat vulnerabilities as public-relations problems first and technical problems second. This week at [BlackHat](#), security researcher Michael Lynn and Cisco demonstrated both points.

Lynn was going to present security flaws in Cisco's IOS, and Cisco went to [inordinate lengths](#) to make sure that information never got into the hands of the their consumers, the press, or the public.

Cisco threatened legal action to stop the conference's organizers from allowing a 24-year-old researcher for a rival tech firm to discuss how he says hackers could seize control of Cisco's Internet routers, which dominate the market. Cisco also instructed workers to tear 20 pages outlining the presentation from the conference program and ordered 2,000 CDs containing the presentation destroyed.

In the end, the researcher, Michael Lynn, went ahead with a presentation, describing flaws in Cisco's software that he said could allow hackers to take over corporate and government networks and the Internet, intercepting and misdirecting data communications. Mr. Lynn, wearing a white hat emblazoned with the word "Good," spoke after quitting his job at Internet Security Systems Inc. Wednesday. Mr. Lynn said he resigned because ISS executives had insisted he strike key portions of his presentation.

### Search

Powered by [DuckDuckGo](#)

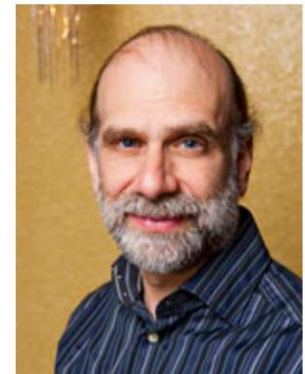
 

blog  essays  whole site

### Subscribe



### About Bruce Schneier



I've been writing about security issues on my [blog](#) since 2004, and in my monthly [newsletter](#) since 1998. I write [books](#),





CAN  
SEC  
WEST

2009

Photo credit: Garrett Gee

# Google P0: Raising the Stakes

The screenshot shows the Pwnium website interface. At the top left is the 'Pwnium' logo. At the top right, it displays 'Cash Remaining: \$1,940,000'. Below this are four summary cards: 'Successful Ex...' with a money bag icon and the number '1', 'Chrome Explo...' with a bug icon and the number '1', 'Non-Chrome ...' with a bug icon and the number '0', and 'Patched' with a bug icon and the number '0'. A section titled 'Pwnium Exploits' contains a table with the following data:

| Name       | Type of Pwn         | Cash Award | Status      | Patched |
|------------|---------------------|------------|-------------|---------|
| Pinkie Pie | Full Chrome Exploit | \$60,000   | Unconfirmed |         |

Below the table is a section titled 'Pwnium Status Updates' with the text: 'Pwnium 2 is now open for submissions!'.



# Exploit Development - 2012



photobomb

2-12 month dev time.  
24h to 10d shelf life.  
Public domain  
exploits = zero.  
Cost,value of  
exploits has  
significantly risen.

- COMMERCIALIZED
- WEAPONIZED
- POLITICIZED



# 2012

## Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits

4 comments, 2 called-out + Comment now

*This story accompanies a profile of the French exploit-selling firm Vupen in the April 9th issue of Forbes magazine.*

A clever hacker today has to make tough choices. Find a previously unknown method for dismantling the defenses of a device like an iPhone or iPad, for instance, and you can report it to Apple and present it at a security conference to win fame and lucrative consulting gigs. Share it with HP's Zero Day Initiative instead and earn as much as \$10,000 for helping the firm shore up its security gear. Both options also allow Apple to fix its bugs and make the hundreds of millions of iPhone and iPad users more secure.



Meet The Hackers Who Sell Spies The Tools To


But any hacker who happens to know one Bangkok-based security researcher who goes by the handle "the Grugq"—or someone like him—has a third option: arrange a deal through the pseudonymous exploit broker to hand the exploit information over to a government agency, don't ask too many questions, and get paid a quarter of a million dollars—minus the Grugq's 15% commission.

| Vulnerability         | \$        | Source  |
|-----------------------|-----------|---|
| Some exploits"        | 250,000   | Govt. official referring to what "some people" pay. |
| A "real good" exploit | > 100,000 | SNOsoft Research Team                               |
| Chrome                | 60,000    | Google  |
| Vista                 | 50,000    | Raimund Genes, Trend Micro                          |
| Weaponized exploit    | 30,000    | David Maynor, Secureworks                           |
| iDefense purchases    | 10,000    | David Maynor, Secureworks                           |
| WMF                   | 4,000     | Alexander Gostev, Kaspersky                         |
| Google                | 3,133.7   | Google  |
| Mozilla               | 3,000     | Mozilla   |
| Excel                 | 1,200     | Ebay auction site                                   |


credit: Forbes 23.3.2012 Shopping for Zero Days  
Charlie Miller, the 0-day market


# Bug Bounties or Bug Bazaars?



 **Zeroodium** @Zeroodium · 2h  
Breaking News: We offer one million US dollars (\$1,000,000) for iOS9 exploits/jailbreak: [zerodium.com/ios9.html](http://zerodium.com/ios9.html)  
#bugbounty #Jailbreak #0day  
↳ 207 ★ 72

 **Zeroodium** @Zeroodium · Sep 16  
Our price range for 0days we acquired so far: Mobile \$100K, Browsers \$50K-30K+Sandbx/Krnl \$50K-30K, Flash \$45K-25K, Office \$40K-25K, Java \$0  
↳ 80 ★ 49

 **Chaouki Bekrar** @cBekrar · Sep 14  
Life is short, sell your 0days  
↳ 153 ★ 113


 **Zeroodium** @Zeroodium · Sep 4  
Our friends of ZDI canceled Pwn2Own mobile (re Wassenaar). You wanted to participate & you're upset? We buy your exploit for up to \$100,000

 **Alex Stamos**  
@alexstamos

Bug Bounty researchers are incredibly short-sighted and keep acting in a way that discourages new programs.

**Dan Guido** @dguido  
The researcher responses to this bug bounty are awful. They're not there to pay your salary, it's a thank you.  
[forbes.com/sites/thomasbr...](http://forbes.com/sites/thomasbr...)

13/07/16, 21:59

 **Chaouki Bekrar** ✓  
@cBekrar

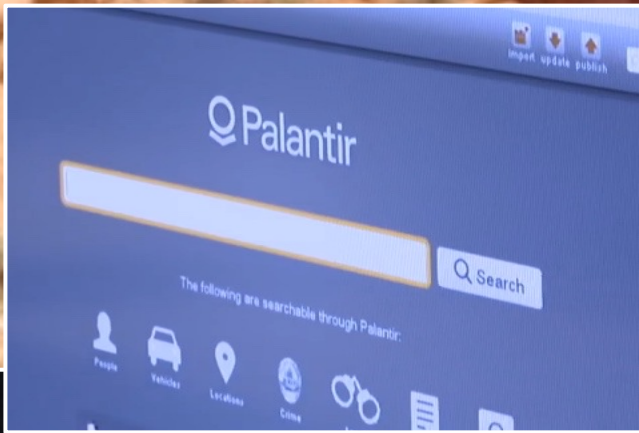
Poll: If you had an expensive 0day, would you sell it & feed your family, or give it for free to software vendors to feed their shareholders

|                           |     |
|---------------------------|-----|
| I fully support my family | 80% |
| I suck shareholders dicks | 20% |

422 votes • Final results  
01/10/16, 13:38



# LØRD OF CYB3RW4R



Lorenzo Franceschi-Bicchierai  
@lorenzoFB

Here's an up-to-date price list for exploits, according to sources who work in the zero-day industry:

- iOS remote jailbreak: \$2 million
- Chrome remote exploit with sandbox escape: \$500,000-\$1 million
- Firefox remote: \$200,000
- Tor \$150,000-\$250,000



## How a Tiny Startup Became the Most Important Hacking Shop You've...

Inside the secretive industry that helps government hackers get around encryption.

[motherboard.vice.co](https://motherboard.vice.com)

11:18 AM - 7 Feb 2018



## How To Win The Media War Against Grassroots Activists: Stratfor's Strategies

The playbook: isolate the radicals, "cultivate" the idealists and "educate" them into becoming realists. Then co-opt the realists.

by *Steve Horn*





2010

**"For a few hundred K,  
could you put together  
a team that would  
break-in just about  
anywhere?"**



Haroon Meer

CCDCOE Conference on  
Cyber Conflict - 2010

## (4) Some Ugly Facts

***“For a few hundred K (USD), could you put together a team that would break-in just about anywhere?”***

|                    |     |
|--------------------|-----|
| haroon meer        | YES |
| Saumil Shah        | YES |
| Ivan Arce          | YES |
| Felix (fx) Lindner | YES |

\$100k – 500k





**Once you're in...**

**...what are you going to do?**

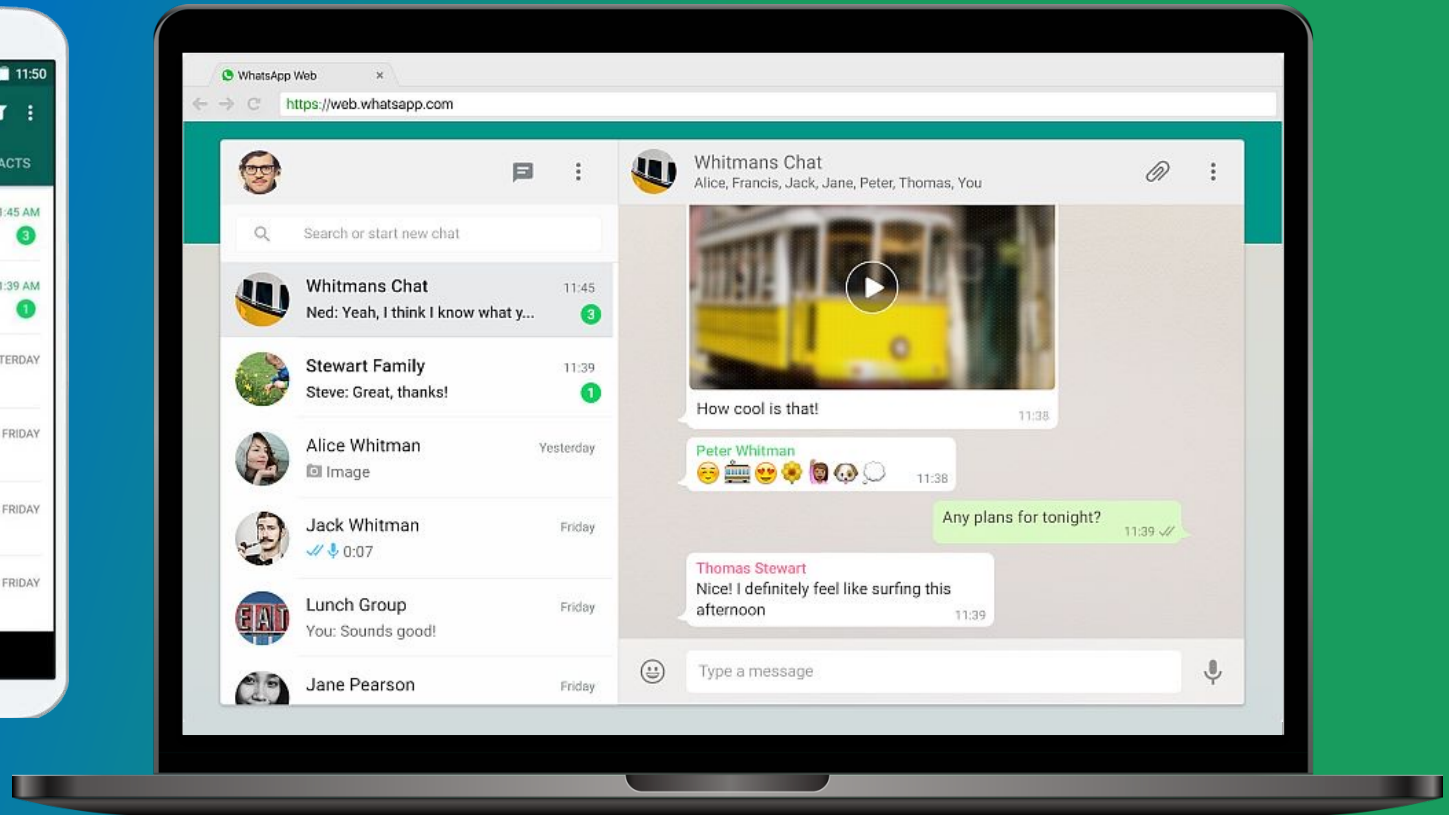
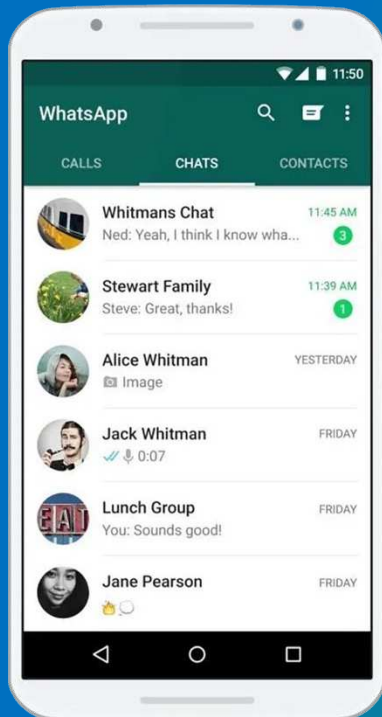


**While Attack is cheaper  
than Defense...**

...attacker toolchains  
are far more complex  
than the public  
demonstrations  
we have seen so far.

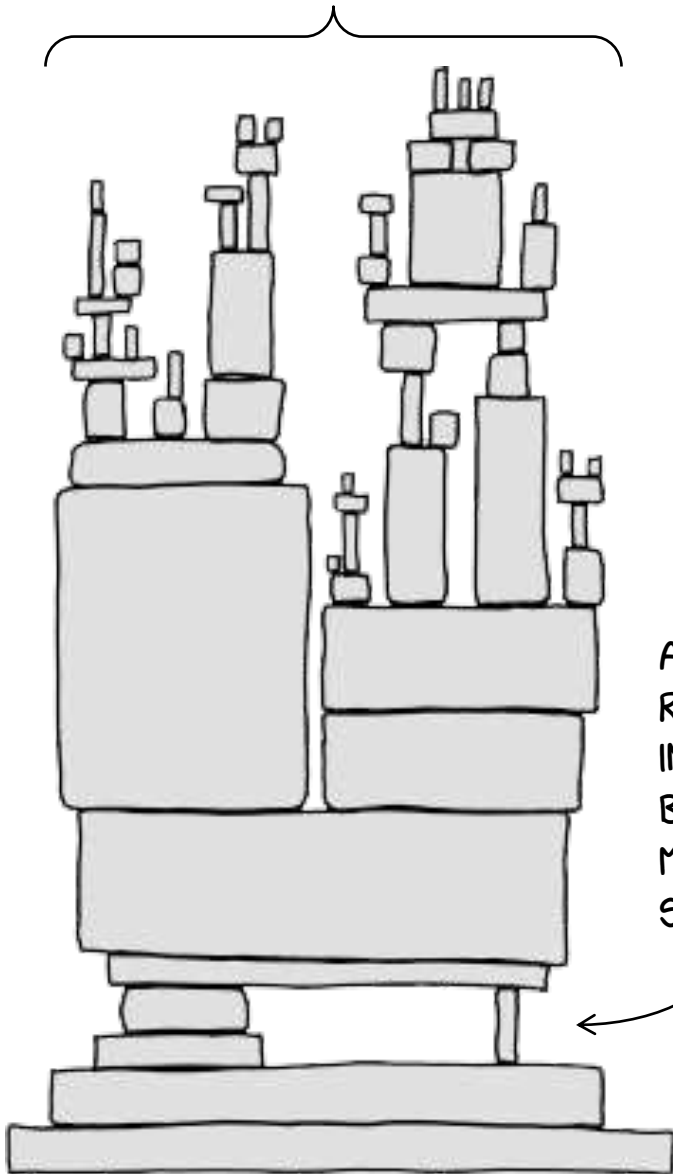


# ECONOMICS OF ATTACK



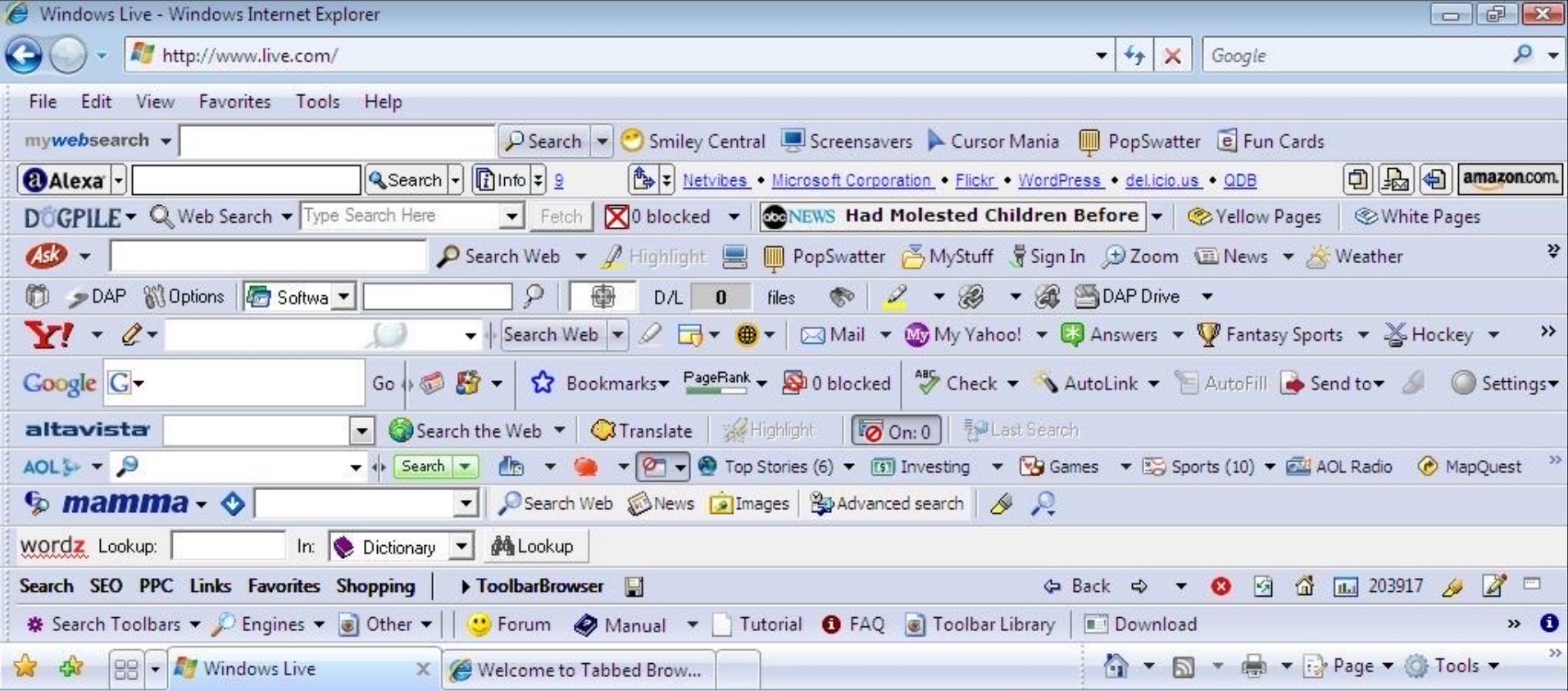


ALL MODERN DIGITAL  
INFRASTRUCTURE



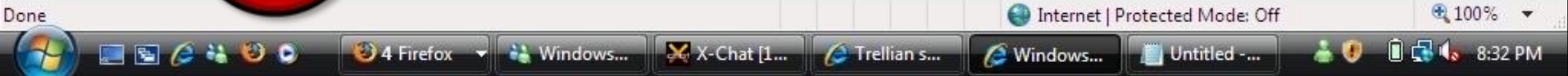
# One Weakness...

A PROJECT SOME  
RANDOM PERSON  
IN NEBRASKA HAS  
BEEN THANKLESSLY  
MAINTAINING  
SINCE 2003



**...fits all.**

**SUPPLY CHAIN ATTACKS. Since 2010**





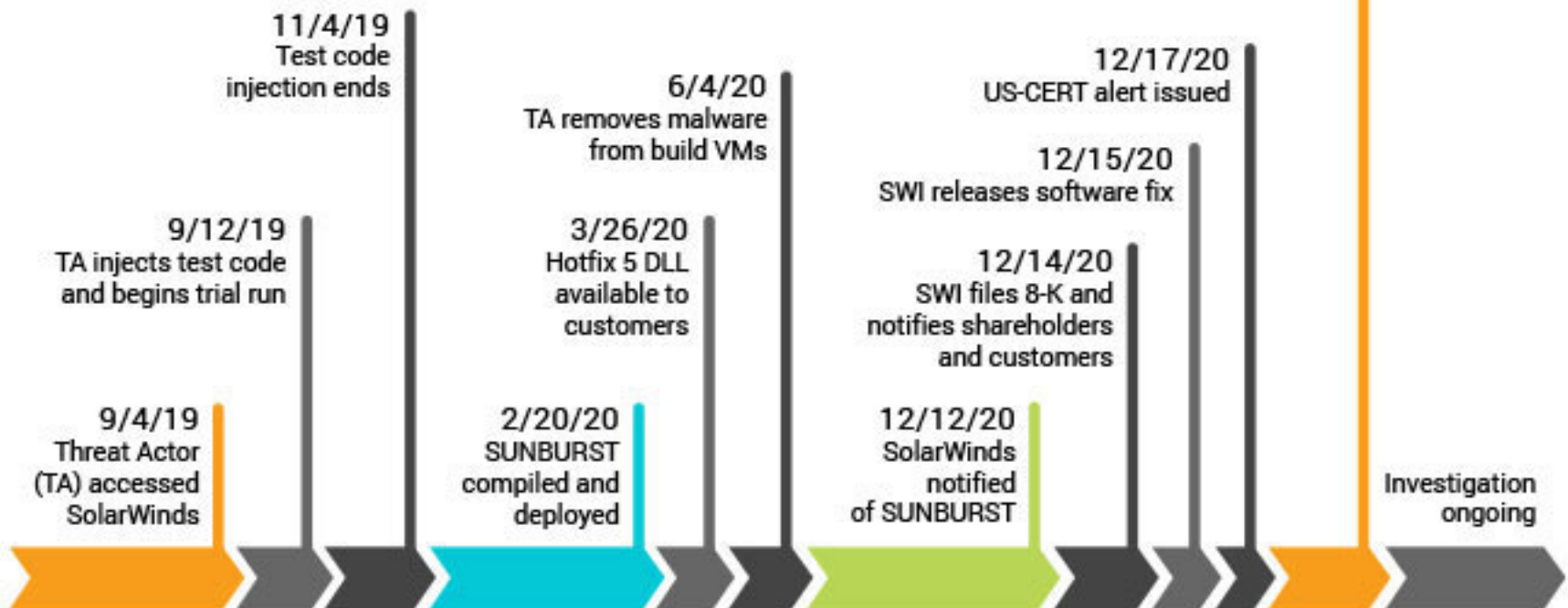
# solarwinds

*The Power to Manage IT*

**September  
2019**

**December  
2020**

**1/11/21**  
New findings  
related to  
SUNSPOT  
released



## DEFENDERS

- ☀ Did <GARTNER MAGIC QUADRANT PRODUCT> see it coming?
- ☀ Win 10's Exploit Mitigations?
- ☀ Was Solarwinds software even part of the THREAT MODEL?



## ATTACKERS

- ✦ Any sophisticated 0-day used?
- ✦ Any Stuxnet style cyberweapon used?
- ✦ Don't you wish YOU would have thought of this? 😊



# The more sophisticated the technology, the more vulnerable it is to primitive attack.

Doctor Who, "Pirate Planet"



# DEFENSE 2001-20

**FIREWALLS**

**IDS/IPS**

**ANTIVIRUS**

**WAF**

**DLP, EPS**

**DEP, ASLR**

**SANDBOX**

**THREAT INTEL**

Reactive Approach

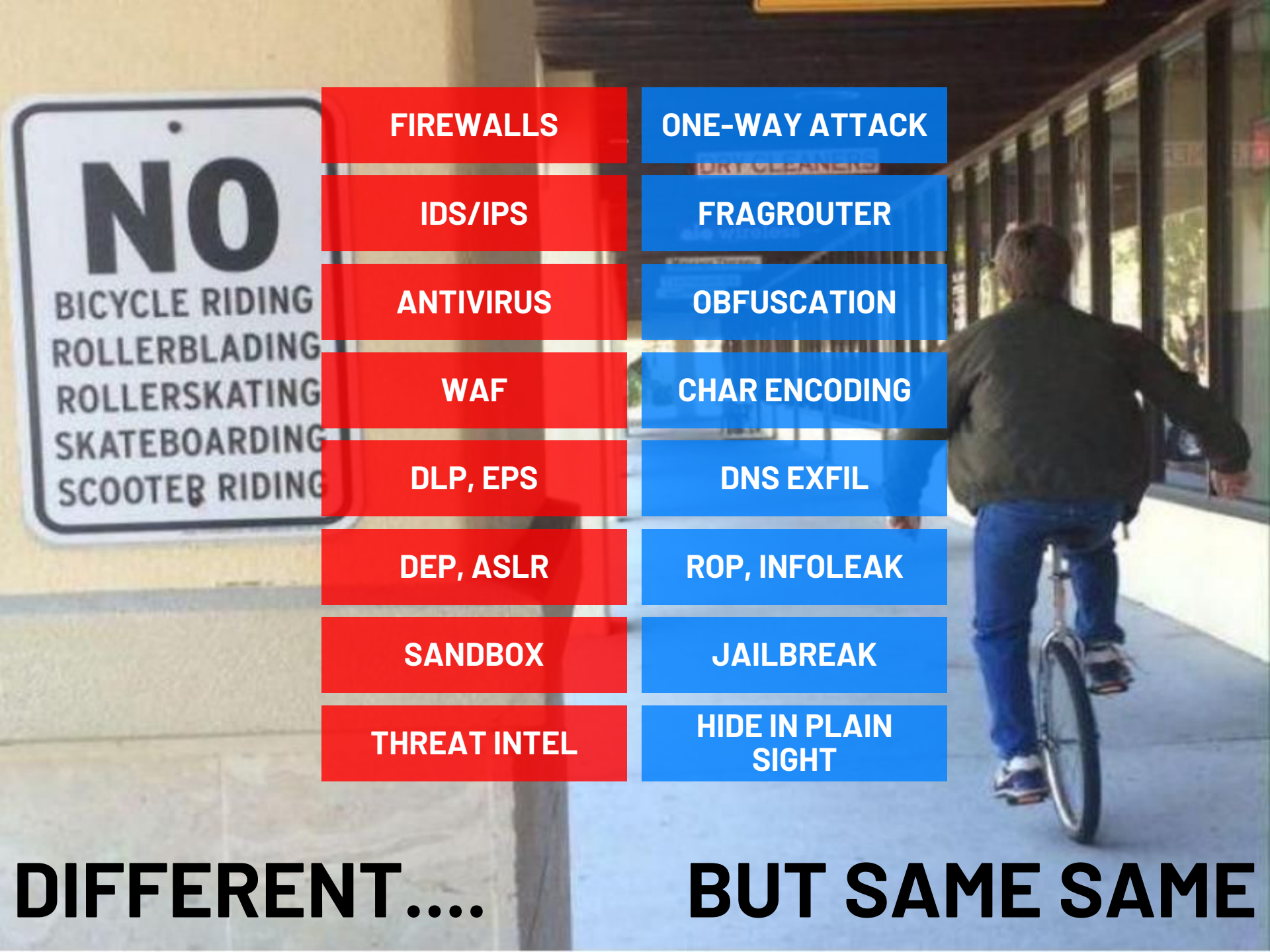
Block the Bad Things  
and be Secure again



**NO**  
BICYCLE RIDING  
ROLLERBLADING  
ROLLERSKATING  
SKATEBOARDING  
SCOOTER RIDING

**DIFFERENT....**





**FIREWALLS**

**ONE-WAY ATTACK**

**IDS/IPS**

**FRAGROUTER**

**ANTIVIRUS**

**OBFUSCATION**

**WAF**

**CHAR ENCODING**

**DLP, EPS**

**DNS EXFIL**

**DEP, ASLR**

**ROP, INFOLEAK**

**SANDBOX**

**JAILBREAK**

**THREAT INTEL**

**HIDE IN PLAIN  
SIGHT**

**DIFFERENT....**

**BUT SAME SAME**





"WE SELL SECURITY"

Rules

Signatures

Updates

Machine Learning





  
**black hat**  
ASIA 2017

## Security products

Why is there a market for this?

- CISO needs to make purchasing decisions in a market full of poor products.
- Biggest risk to CISO is being seen as “having forgotten” a risk
- Solution is often *portfolio purchase*: “Buy one of each product category”



# Products To The Rescue?



Jim Schwar  
@jimiDFIR



Replying to [@MalwareJake](#)

CISO: How many windows hosts  
do we have?

AV Guy: 7864

Desktop Management: 6321

EDR Team: 6722

CMDB Team: 4848

SIEM TEAM: 9342

08/02/18, 19:25



**THERE WILL BE  
VULNERABILITIES**



# SCHRÖDINGER'S HACK



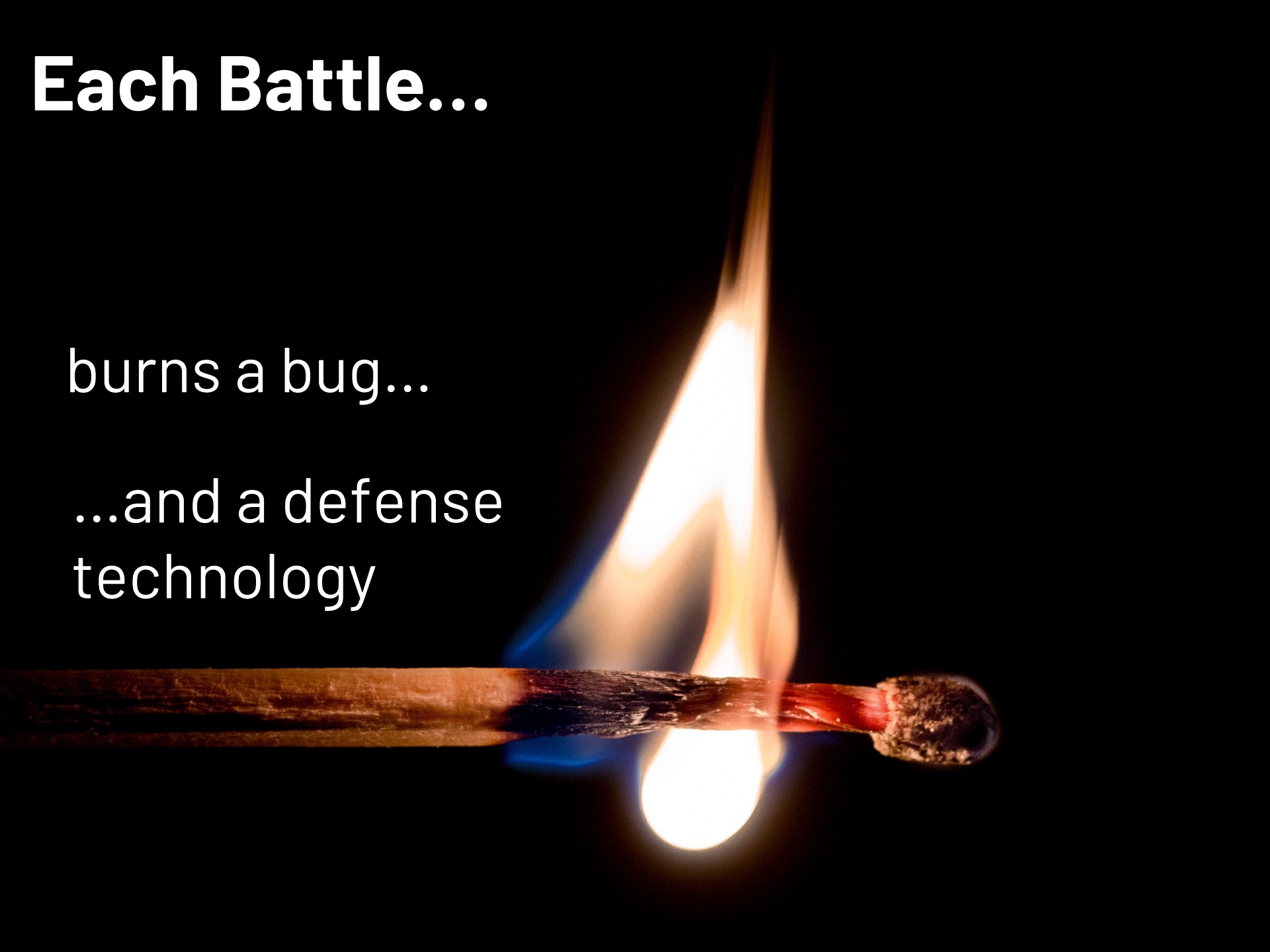


**WHEN ATTACKS  
MEET DEFENSE**

# Each Battle...

burns a bug...

...and a defense  
technology



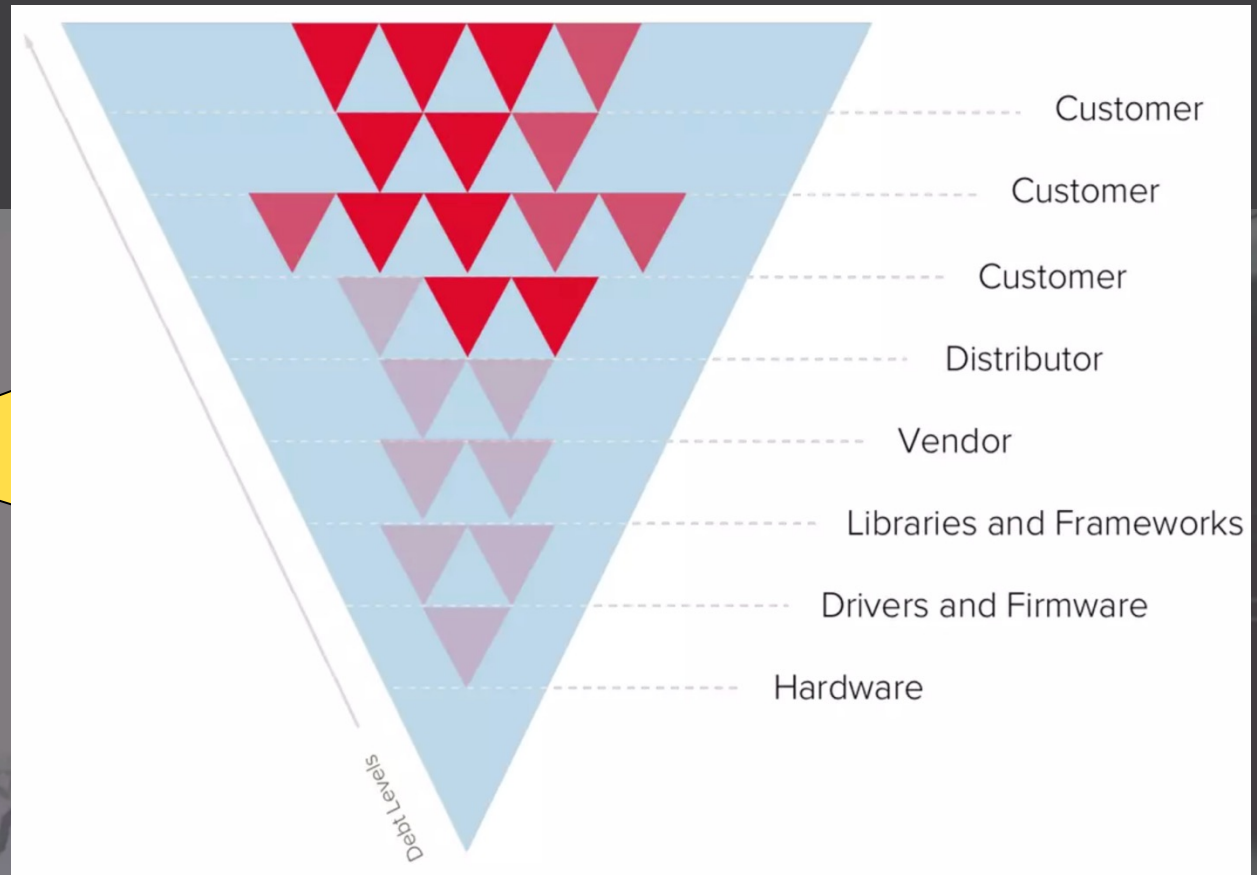


**CYBERWEAPONS**



**USE THEM OR LOSE THEM**

# DEFENSE TECH



| Reference | Date       | BU  | Project            | Category             | Description  | Grading (1-10) | Prime | Interest Rate | 2017               | 2018               | 2019               | 2020               |
|-----------|------------|-----|--------------------|----------------------|--|----------------|-------|---------------|--------------------|--------------------|--------------------|--------------------|
| DR-17-057 | 08/11/2017 | RPS | Web Refresh        | Third Party          | Pentesting finding ref SP-EXT-RPS-181017 deferred to v 1.2 | 4              | 0.055 | 0.044         | £ 2,600.00         | £ 2,714.40         | £ 2,833.83         | £ 2,958.52         |
| DR-17-058 | 23/12/2017 | INF | AWS Migration      | Instructure Shortcut | Propose 2FA solution for remote admin access rejected      | 6              | 0.055 | 0.066         | £160,000.00        | £170,560.00        | £181,816.96        | £193,816.88        |
| DR-18-001 | 02/02/2018 | FIN | Autotask Migration | Feature              | Proposal to migrate PPI to alternate platform rejected     | 5              | 0.048 | 0.048         |                    | £ 13,500.00        | £ 14,148.00        | £ 14,827.10        |
| DR-18-113 | 19/04/2018 | BCL | Project Epsilon    | Process              | Proposal to perform comprehensive Threat Model rejected    | 3              | 0.048 | 0.0288        |                    | £ 2,650.00         | £ 2,726.32         | £ 2,804.84         |
|           |            |     |                    |                      |  |                |       |               | <b>£164,617.00</b> | <b>£191,442.40</b> | <b>£203,544.11</b> | <b>£216,427.34</b> |



DEAR CISO

**SAY** @roqueciso

**TO ANOTHER P.O.**

**NO**

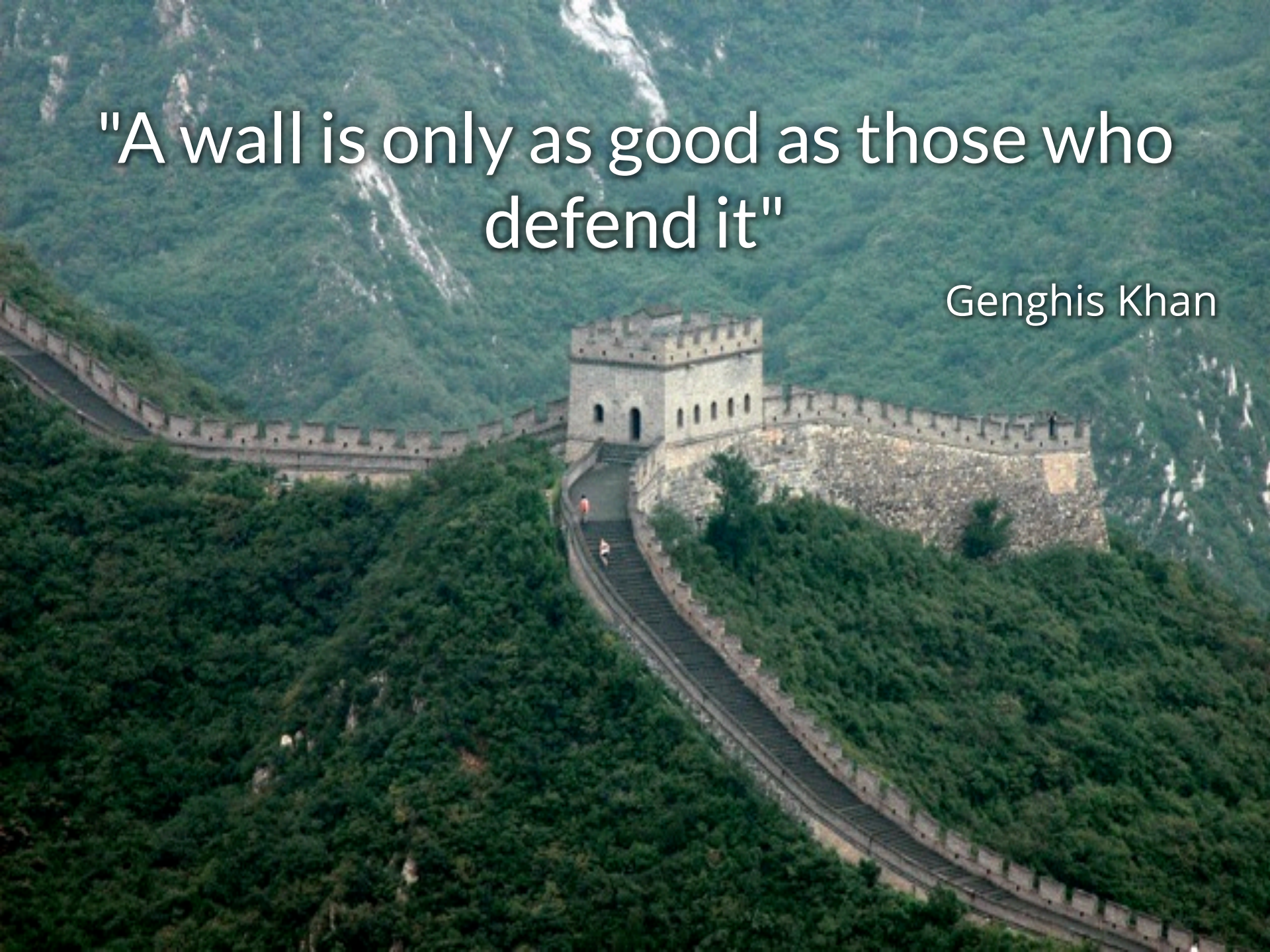
THE CAMPAIGN TO STOP CISOS  
BUYING RANDOM VENDOR CRAP





"A wall is only as good as those who  
defend it"

Genghis Khan



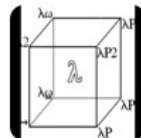
# PEBKAC



**the grugq** @thegrugq

7m

It's surprising how critical good phishing technique is with these APT attacks. Effective phishing is more important than 0day.



**sp** @LambdaCube

42s

@thegrugq User-hardening efforts have made barely any progress compared to software-hardening efforts over the last years.





# HAVE NOTS

Not capable

"Cyber Security" is not my business

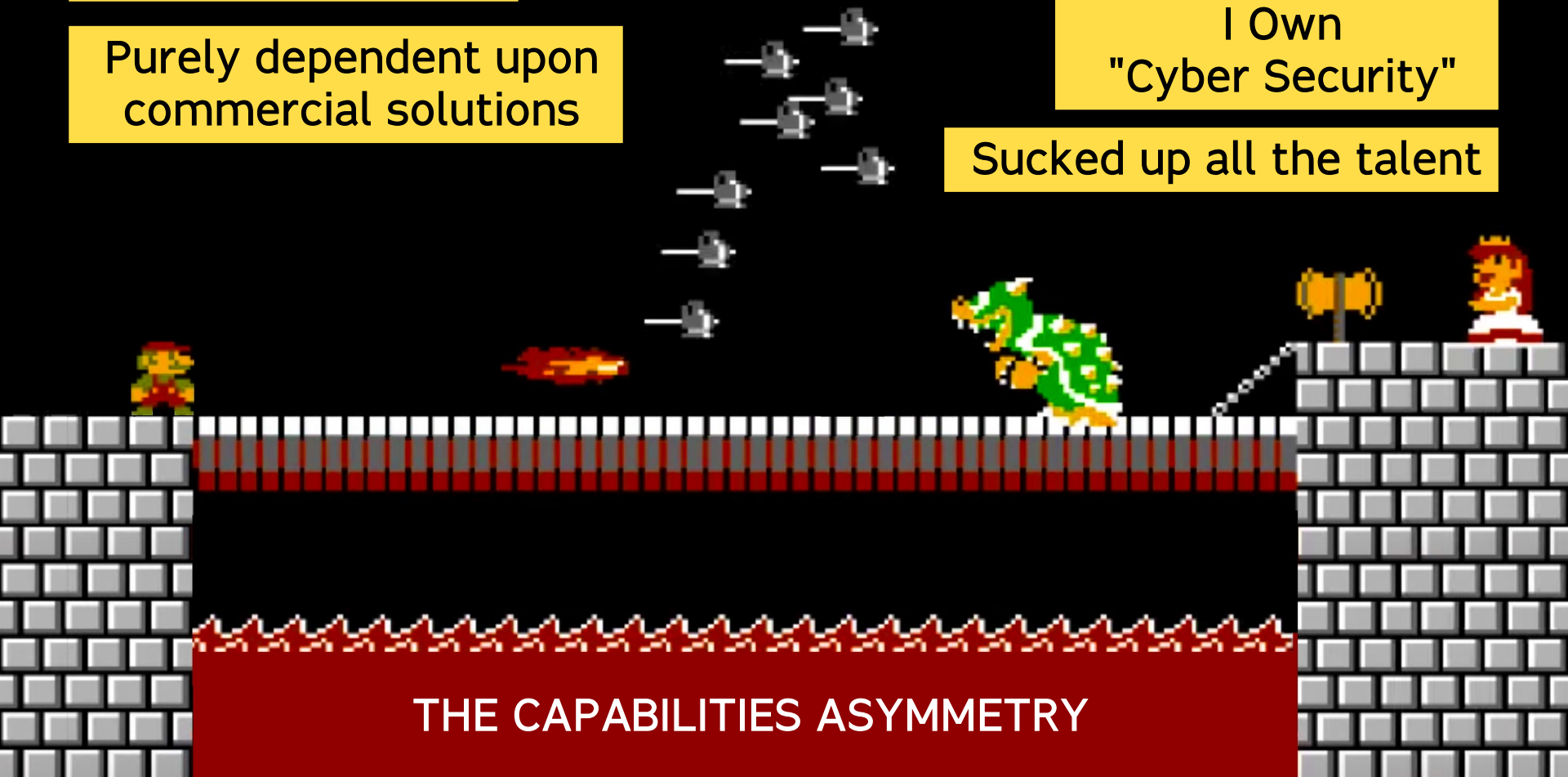
Purely dependent upon commercial solutions

# HAVES

Capable of custom tooling and operations

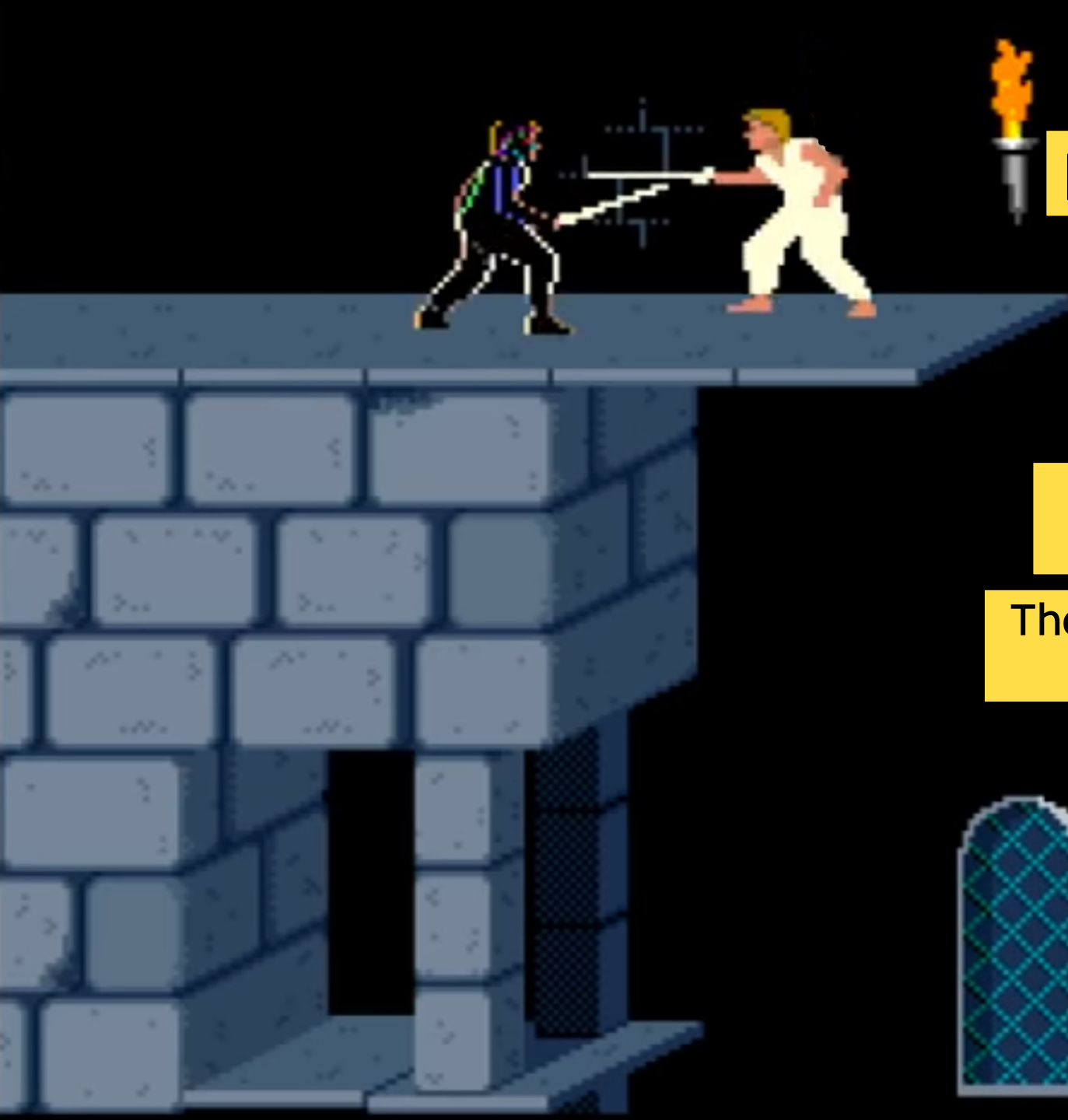
I Own "Cyber Security"

Sucked up all the talent



THE CAPABILITIES ASYMMETRY





# RESISTANCE

Pass The Parcel

Rules, Signatures,  
Updates, Patches

The Next Short-Lived  
Security Product

Encumber  
Users

INFOSEC:  
The business of  
selling FEAR





# RESONANCE

Take Ownership

Build Defendable Systems

Security and Trustworthiness as a core feature

EMPOWER Users

INFOSEC:  
The business of enabling TRUST



# Takeaway Elements

**NAKATOMI SPACE:  
THERE WILL BE  
BUGS**

**PRODUCTS ARE  
SHORT LIVED**

**THE MORE  
THINGS  
CHANGE, THE  
MORE THEY  
REMAIN THE  
SAME**

**BUGS: USE THEM  
OR LOSE THEM**

**DON'T OVERLOOK  
TECH DEBT**

**INVEST IN  
CAPABILITIES**

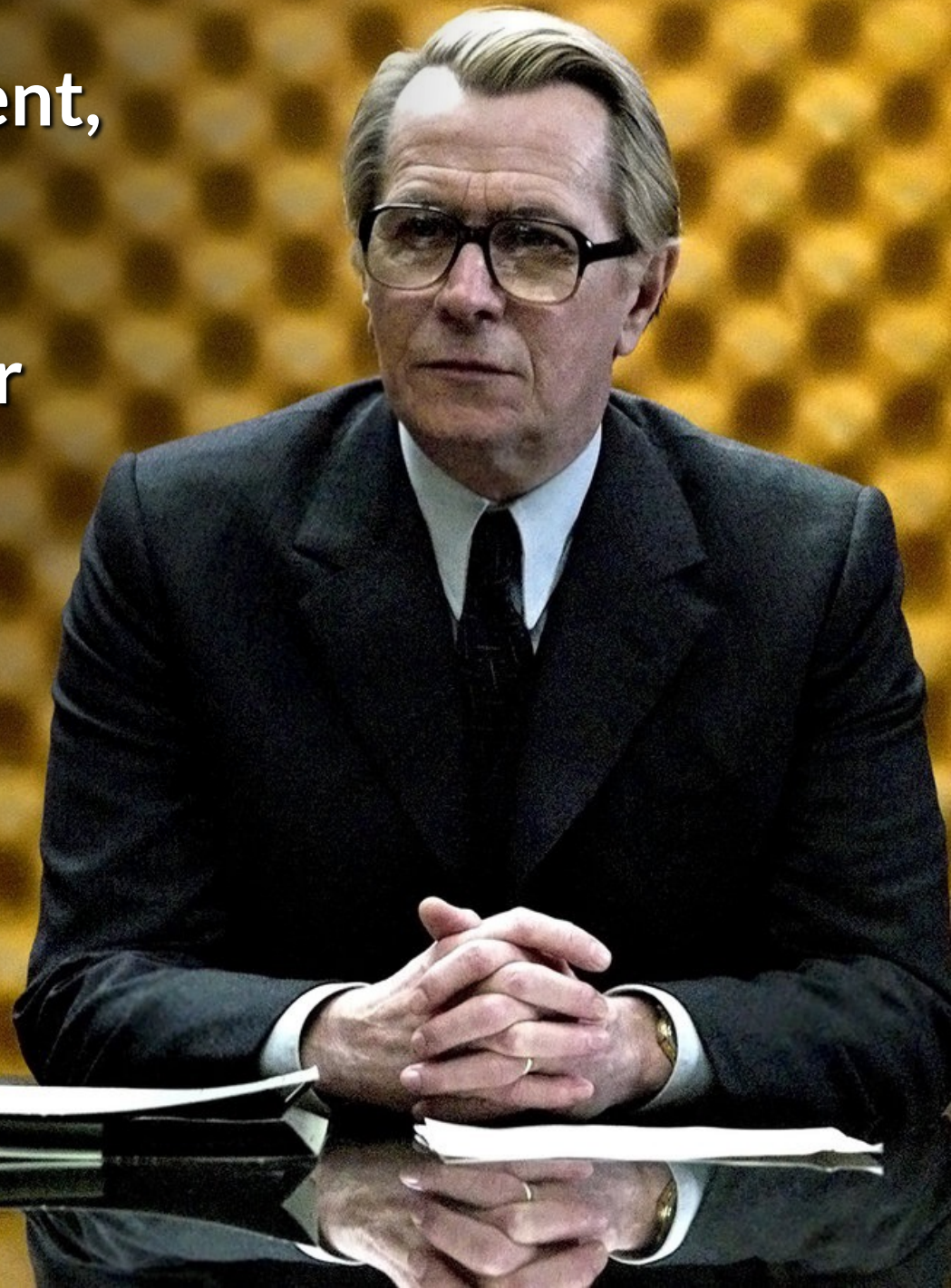
**PEOPLE >  
PRODUCTS**



**We are not so different,  
you and I.**

**We've both spent our  
lives looking for the  
weaknesses in  
one anothers'  
systems.**

George Smiley,  
Tinker, Tailor, Soldier, Spy





2006  
4 items



2008  
7 items



2009  
27 items



2010  
8 items



2011  
1 item



2012  
13 items



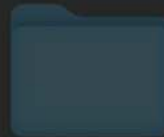
2015  
3 items



2017  
28 items



2018  
5 items



2019  
3 items



2021  
5 items



2023  
1 item



gsec  
27 items



misc  
3 items



untitled folder



ringzerø

ZERØ  
**GRAVITY**  
2023  
AUG 5-8  
LAS VEGAS

**THANK YOU**

**SAUMIL SHAH**  
**@therealsaumil**

**HITB2023AMS**