Cybersecurity

Abel Sanchez

MIT Campus | Cambridge, MA


THE NEW NORMAL

Hacking Tradition

At MIT, a "hacker" is someone who does some sort of interesting and creative work at a high intensity level.


DANGER

Morris Worm
1988

By

Robert
Tappan
Morris

Cyber Security Attacks Price List

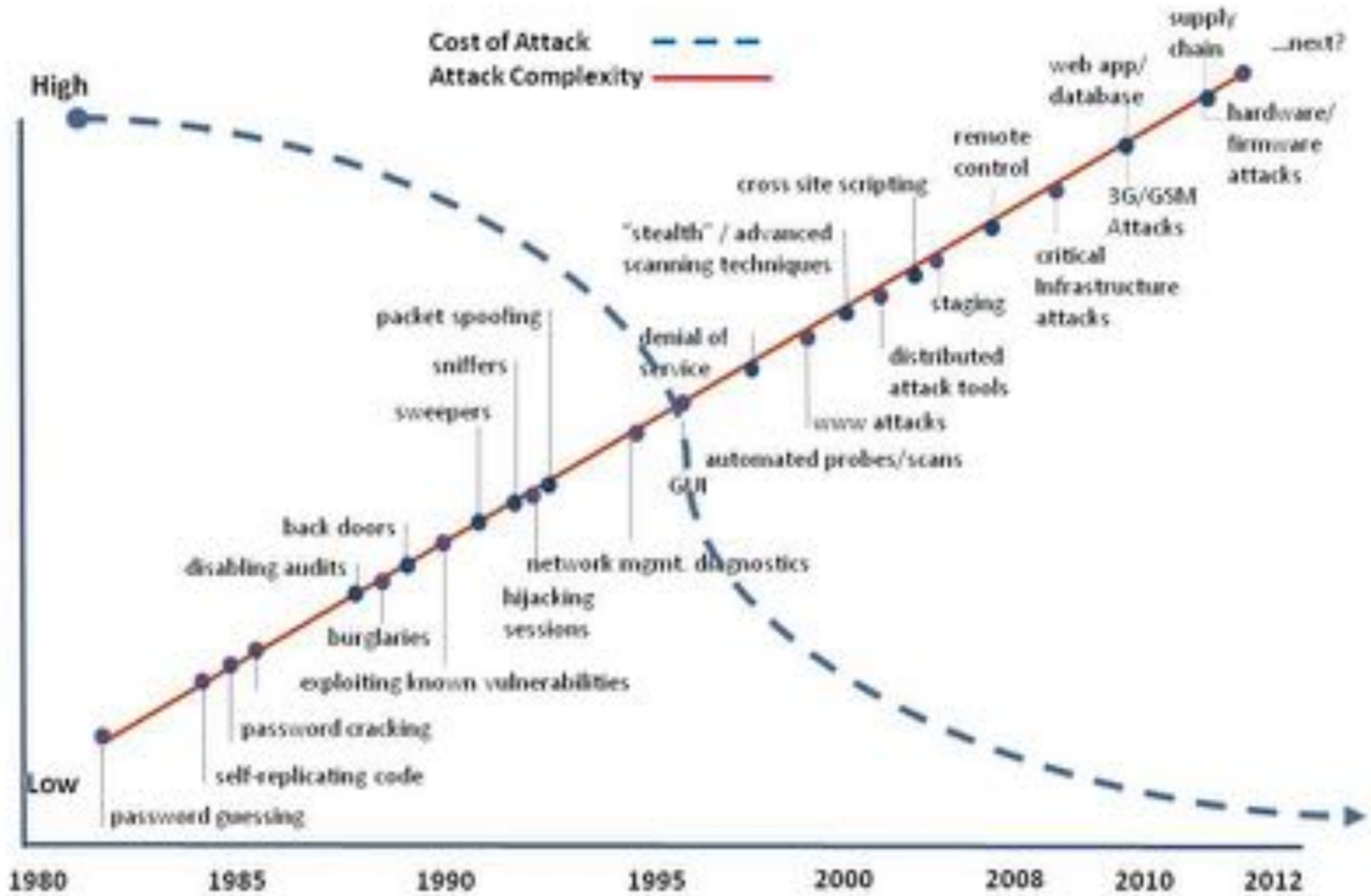
- Basic crypter (for inserting rogue code into a benign file): $10-30
- SOCKS bot (to get around firewalls): $100
- Hiring a DDoS attack: $30-70 for a day, $1,200 for a month
- Email spam: $10 per one million e-mails
- Expensive email spam (using a customer database): $50-500 per one million e-mails
- SMS spam: $3-150 per 100-100,000 messages
- Bots for a botnet: $200 for 2,000 bots
- DDoS botnet: $700
- ZeuS source code: $200-$500
- Windows rootkit (for installing malicious drivers): $292
- Hacking a Facebook or Twitter account: $130
- Hacking a Gmail account: $162
- Hacking a corporate mailbox: $500
- Scans of legitimate passports: $5 each
- Winlocker ransomware: $10-20
- Unintelligent exploit bundle: $25
- Intelligent exploit bundle: $10-3,000
- Traffic: $7-15 per 1,000 visitors for the most valuable traffic (from the US and EU)

** Ars Technica, Wired, Russian Underground 101, Trend Micro, Max Goncharov*


Applications
Places
Sun Jan 26, 11:32 AM
Accessories
Electronics
Graphics
Hamradio
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Universal Access
Other
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
DNS Analysis
IDS/IPS Identification
Live Host Identification
Network Scanners
OS Fingerprinting
OSINT Analysis
Route Analysis
Service Fingerprinting
SMB Analysis
SMTP Analysis
SNMP Analysis
SSL Analysis
Telephony Analysis
Traffic Analysis
VoIP Analysis
VPN Analysis
braa
cisco-auditing-tool
cisco-torch
copy-router-config
merge-router-config
nmap
onesixtyone
snmpcheck
zenmap

Diminishing Attack Costs & Increasing Complexity

Increased network complexity & dependence means more attacks succeed with high payoffs
Technology advances mean lower cost for a successful attack



Defense Cost

Attack Cost

Why?

- Explosive Growth of Information Technology!
- Not slowing down, accelerating
- Digitalization, automation, intelligence
- *Software Is Eating the World* By Marc Andreessen
- Every business is a technology business

HOW FAST CAN YOU BECOME A PASSWORD HACKER?

Password Explosion

- 25+ accounts per user
- Reuse spreads vulnerabilities
- I have over 100 passwords
- How many do you have?

Most Common Passwords

- Top 10 most common passwords:
  - 123456
  - 123456789
  - 1234
  - password
  - 12345
  - 12345678
  - admin
  - 123
  - qwerty
  - 1234567

Password Character Set

95 Character Set

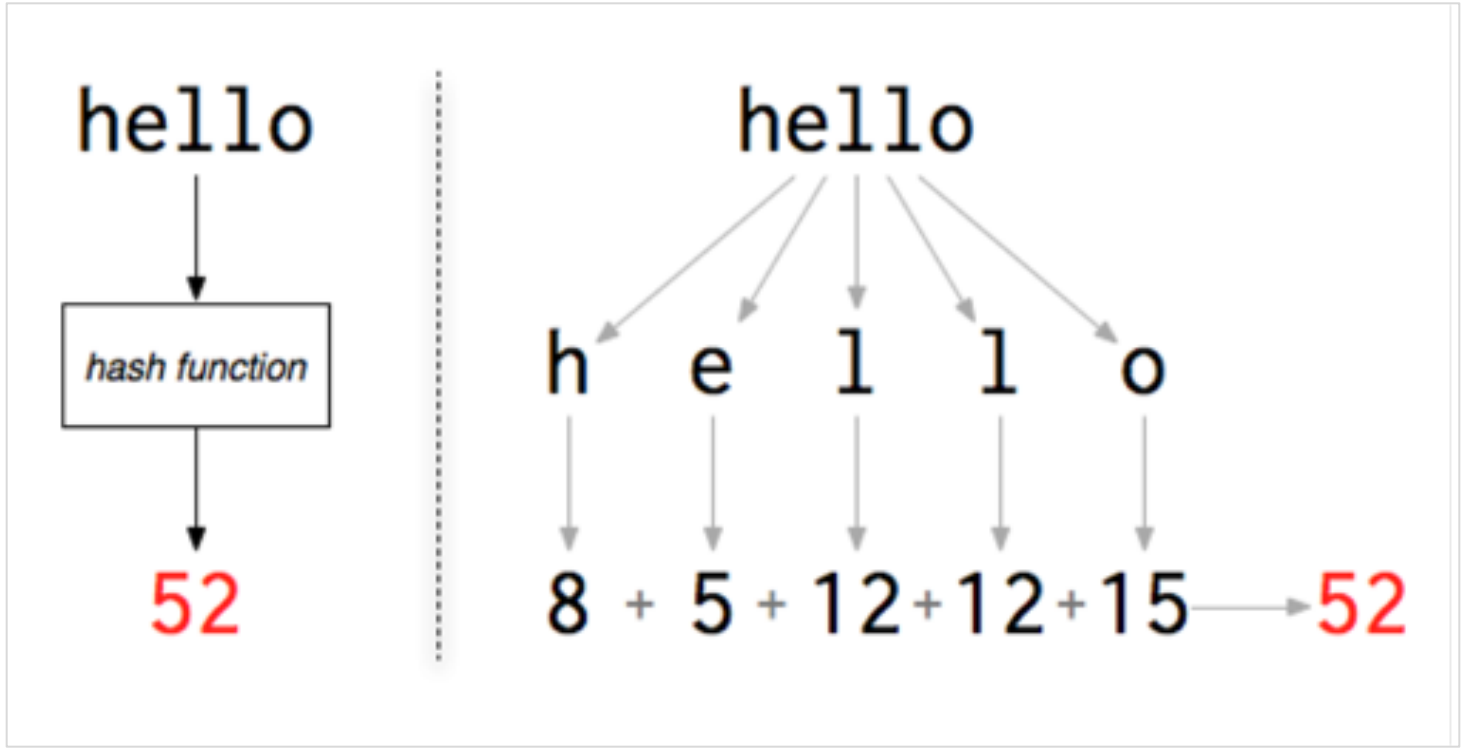
- The "95" comes from the standard 95 characters on a US keyboard. 26 upper, 26 lower, 10 digit, 33 special chars.

```
var charSet =  ['a','b','c','d','e',
                'f','g','h','i','j',
                'k','l','m','n','o',
                'p','q','r','s','t',
                'u','v','w','x','y','z',
                'A','B','C','D','E',
                'F','G','H','I','J',
                'K','L','M','N','O',
                'P','Q','R','S','T',
                'U','V','W','X','Y','Z',
                '0','1','2','3','4',
                '5','6','7','8','9',
                '`','~','!','@','#',
                '$','%','^','&','*',
                '(',')','_','+','-',
                '=','{','}','|','[',
                ']','\\',':','\"',';',
                '\'','<','>','?',',',
                '.','/',' '
                ];
```

Possible Passwords

- 95^1 = 95
- 95^2 = 9025
- 95^3 = 857375
- 95^4 = 81450625
- 95^5 = 7737809375
- 95^6 = 735091890625
- 95^7 = 69833729609375
- 95^8 = 6634204312890625

Hashing



http://www.filosophy.org/post/8/what_is_a_password_anyway/

MD5 Hash

pi  72ab8af56bddab33b269c5964b26620a

Goal

- Find a list of passwords to crack
- Find a good password cracker
- Crack over 5% of passwords

Find Passwords to Crack

- Lots of lists online
- Dedicated forums to cracking passwords
- Choose a friendly forum
- Choose MD5-hashed passwords
- Choose a list with 7,000 passwords

With 25 GPUs

- 350 billion guess/sec NTLM
- 95^8 combinations in just 5.5 hours
- You can brute force every possible eight-character password containing upper- and lower-case letters, digits, and symbols

95^8 = 6634204312890625

= 6,634,204,312,890,625/350,000,000,000

= 18,955 secs = 316 mins = 5.27 hours

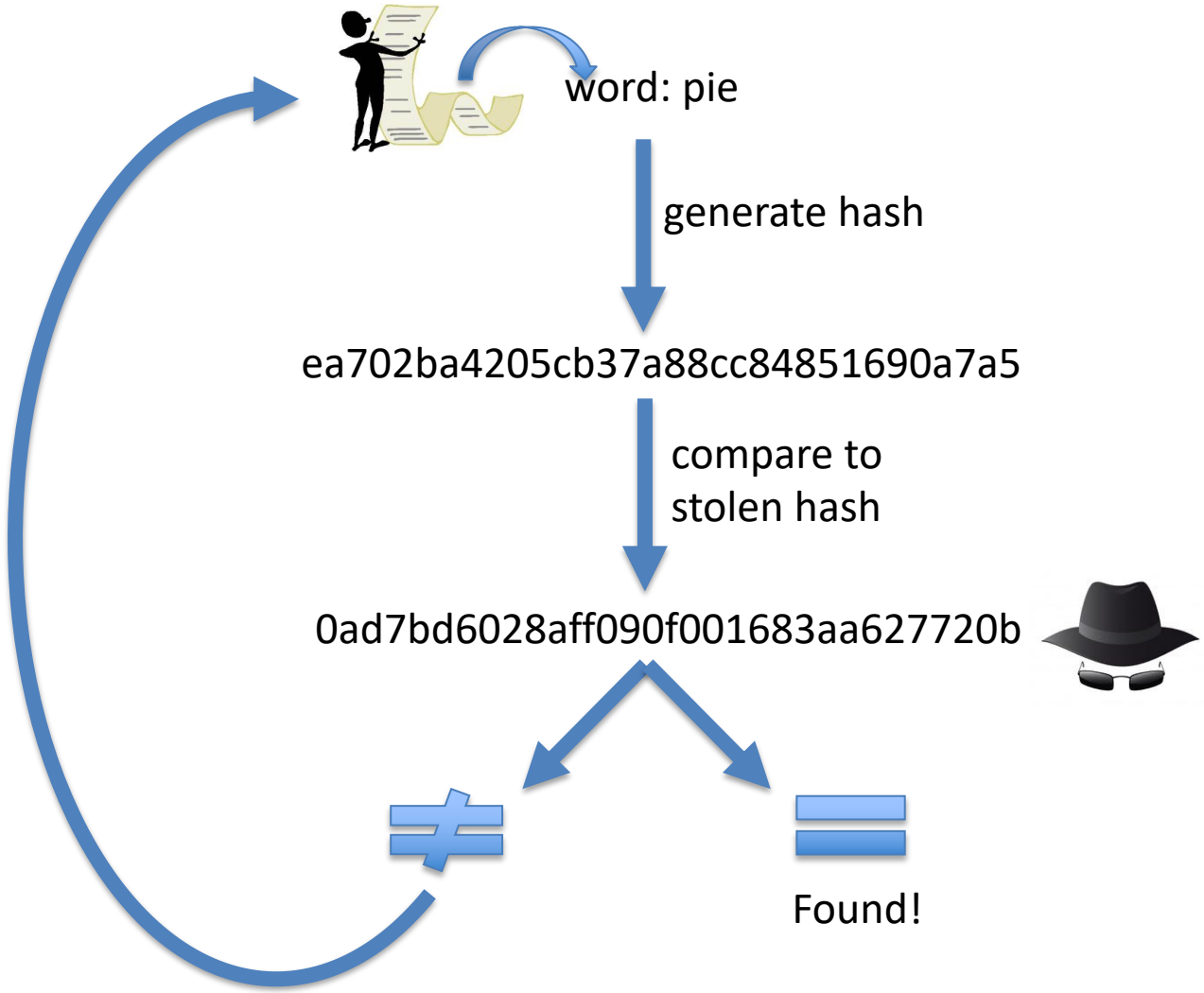
Jeremi Gosney unveiled the machine last week at the Passwords^12 conference in Oslo, Norway, http://passwords12.at.ifi.uio.no/Jeremi_Gosney_Password_Cracking_HPC_Passwords12.pdf

Brute Force is the Last Resort

Wordlists: 2009 Change in Technique

- In 2009, RockYou.com exposed 32 million plaintext passwords which came to 14.3 million once duplicates were removed.
- Marked marked a shift in approach

Wordlist Attack



Wordlists: LinkedIn Example Crack

- LinkedIn:
  - 6.5 million LinkedIn password SHA1 hashes
  - 20% cracked in 30 seconds
  - 30% cracked in 2 hours
  - 64% in one day
  - 90% cracked in 6 days
- Tools
  - 500-million-strong word list
  - 4 AMD Radeon HD6990 graphics cards (3072x4)
  - 15.5 billion guesses/sec
  - ≈$5K

Bank of Wordlists is Growing

- Each year:
  - millions passwords published online
- Billions real-world passwords in the wild
- Growing community community sharing & cracking
- http://pastebin.com/
- https://haveibeenpwned.com/Passwords

357	7,839,042,160	92,712	113,252,553
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
161,749,950	Dubsmash accounts

Recently added breaches

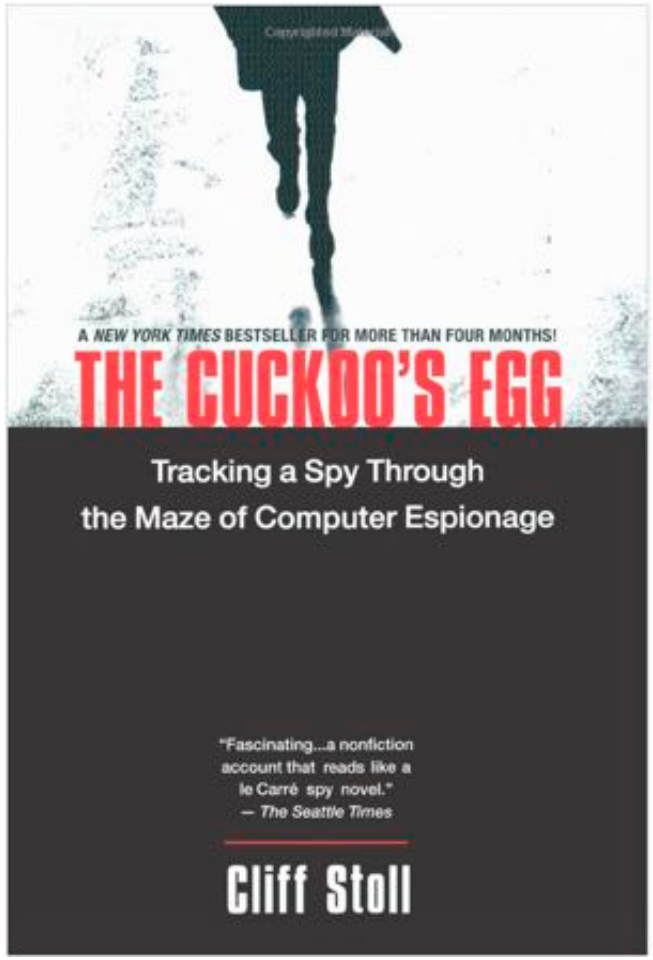
52,623	Demon Forums accounts
871,190	Everybody Edits accounts
3,073,409	Intelimost accounts
11,657,763	Whitepages accounts
14,867,999	500px accounts
3,830,916	Bookmate accounts
28,510,459	HauteLook accounts
15,025,407	8fit accounts
17,204,697	ixigo accounts
48,881,308	Houzz accounts

https://haveibeenpwned.com

Big Data: Wordlists Patterns

- Patterns:
  - Majority of capital letters at the beginning of a password
  - Most numbers and punctuation show up at the end
  - First names followed by years, such as John1980 or Peter1965
  - Special characters at end or beginning
  - Special characters taking place of similar looking letters, "princess" become "prince$$"
  - Mirroring words, so "book" becomes "bookkoob" and "password" becomes "passworddrowssap."
  - Capital followed by 5 letter word, followed by 1-3 numbers

History

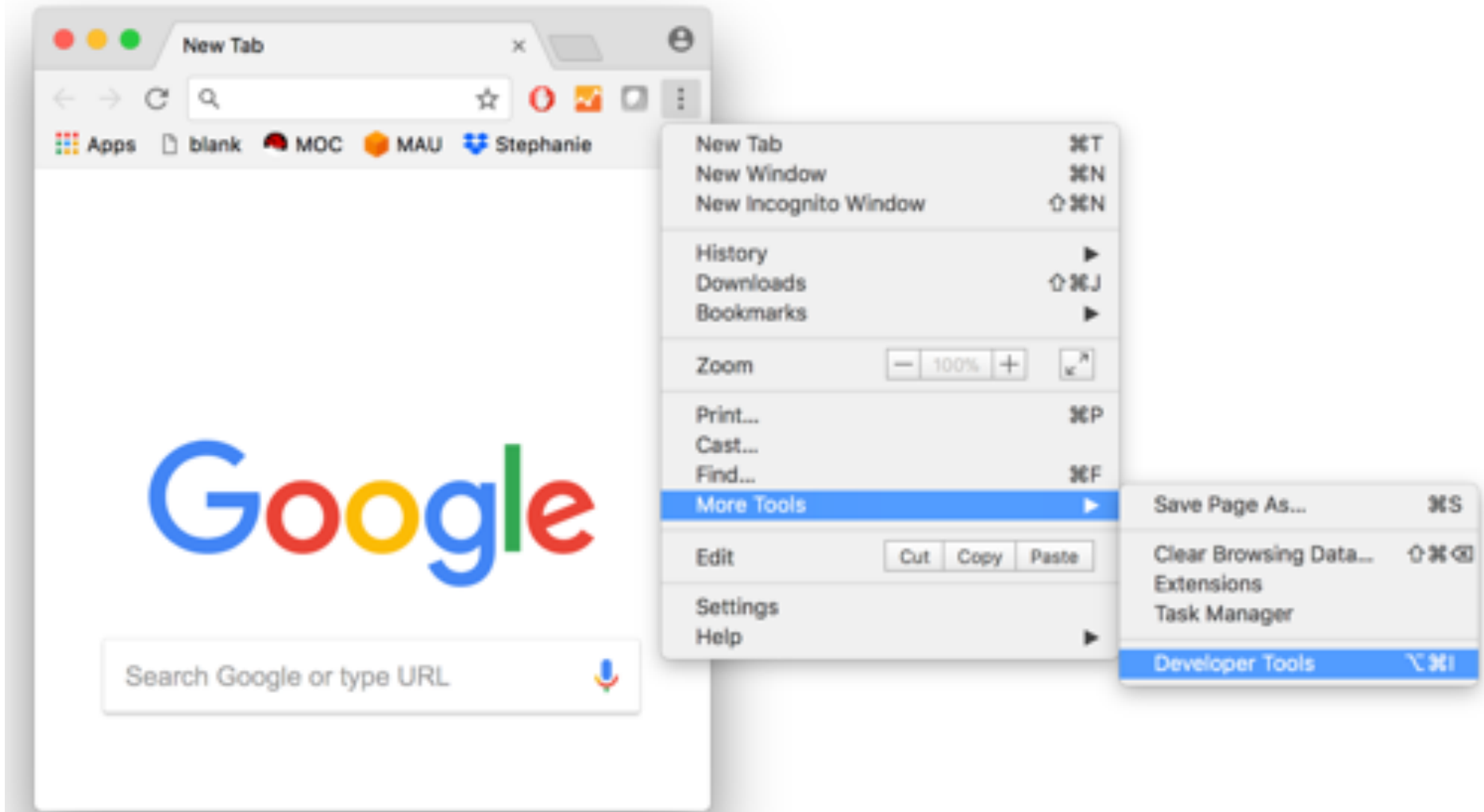


Book: The Cuckoo's Egg, Cliff Stoll
Documentary: The KGB, the Computer, and Me, NOVA

Password Advice

- Password Managers
- Don’t reuse passwords
- Multiple factors
- Biometrics on the way

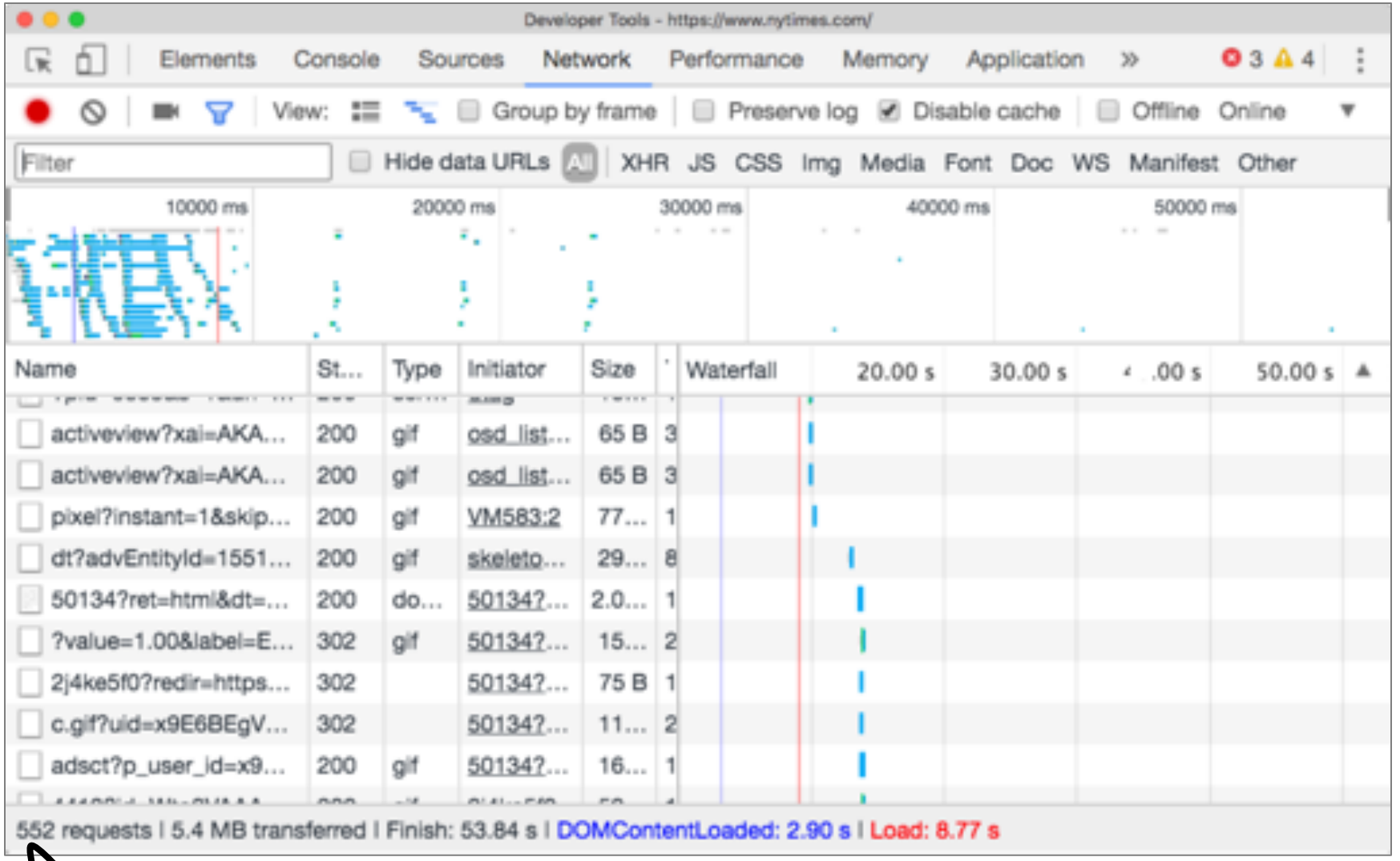
BROWSER PRIVACY


New Tab
Apps
blank
MOC
MAU
Stephanie
Google
Search Google or type URL
New Tab ⌘T
New Window ⌘N
New Incognito Window ⇧⌘N
History
Downloads ⇧⌘J
Bookmarks
Zoom
100%
Print... ⌘P
Cast...
Find... ⌘F
More Tools
Edit
Cut
Copy
Paste
Settings
Help
Save Page As... ⌘S
Clear Browsing Data... ⇧⌘⌫
Extensions
Task Manager
Developer Tools ⌥⌘I

Implications of Navigating to a URL

- Sample
  - http://www.nyt.com

Navigating to the New York Times



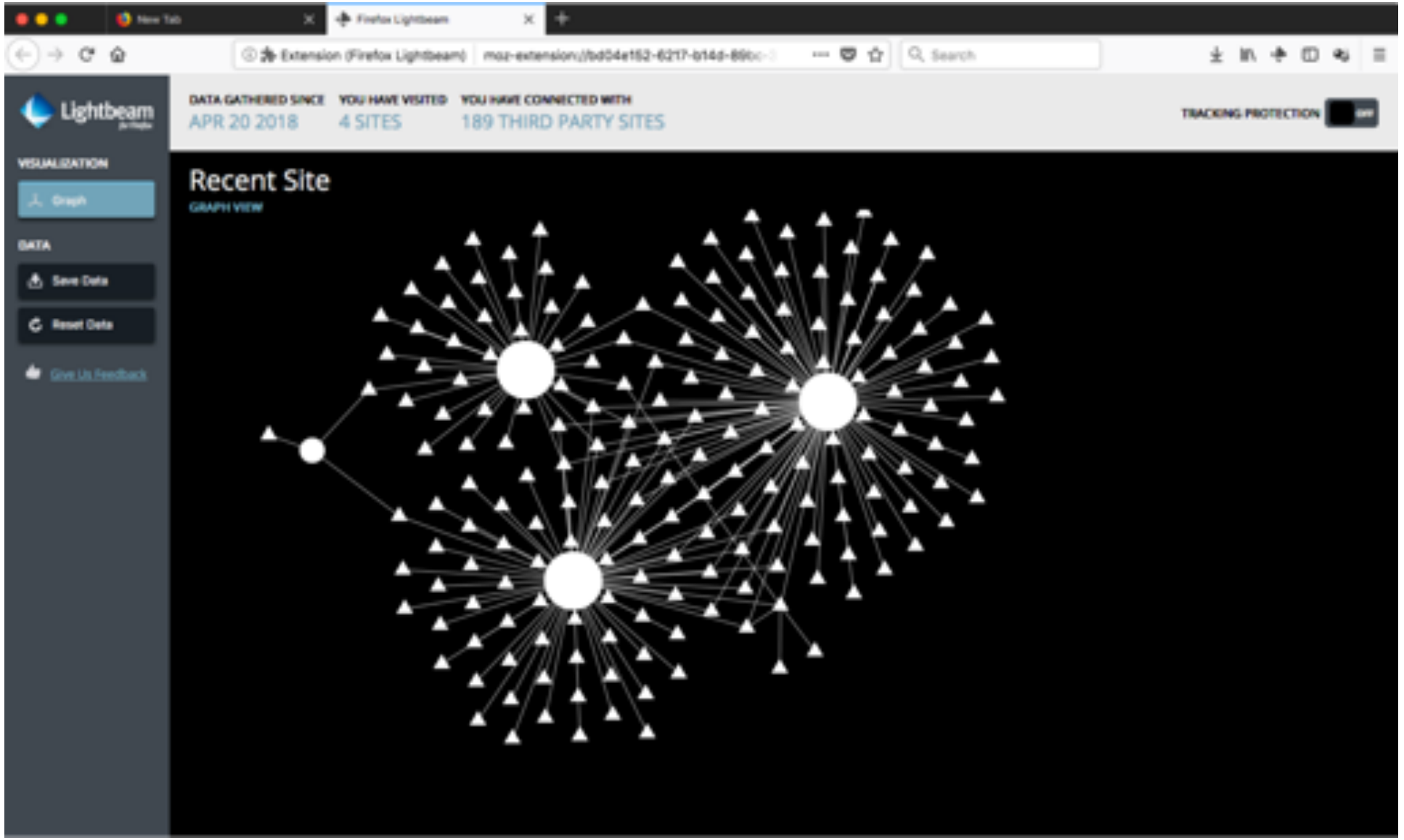
552 requests to other addresses by navigating to single page!

Let’s navigate to three sites

Lightbeam

for Firefox

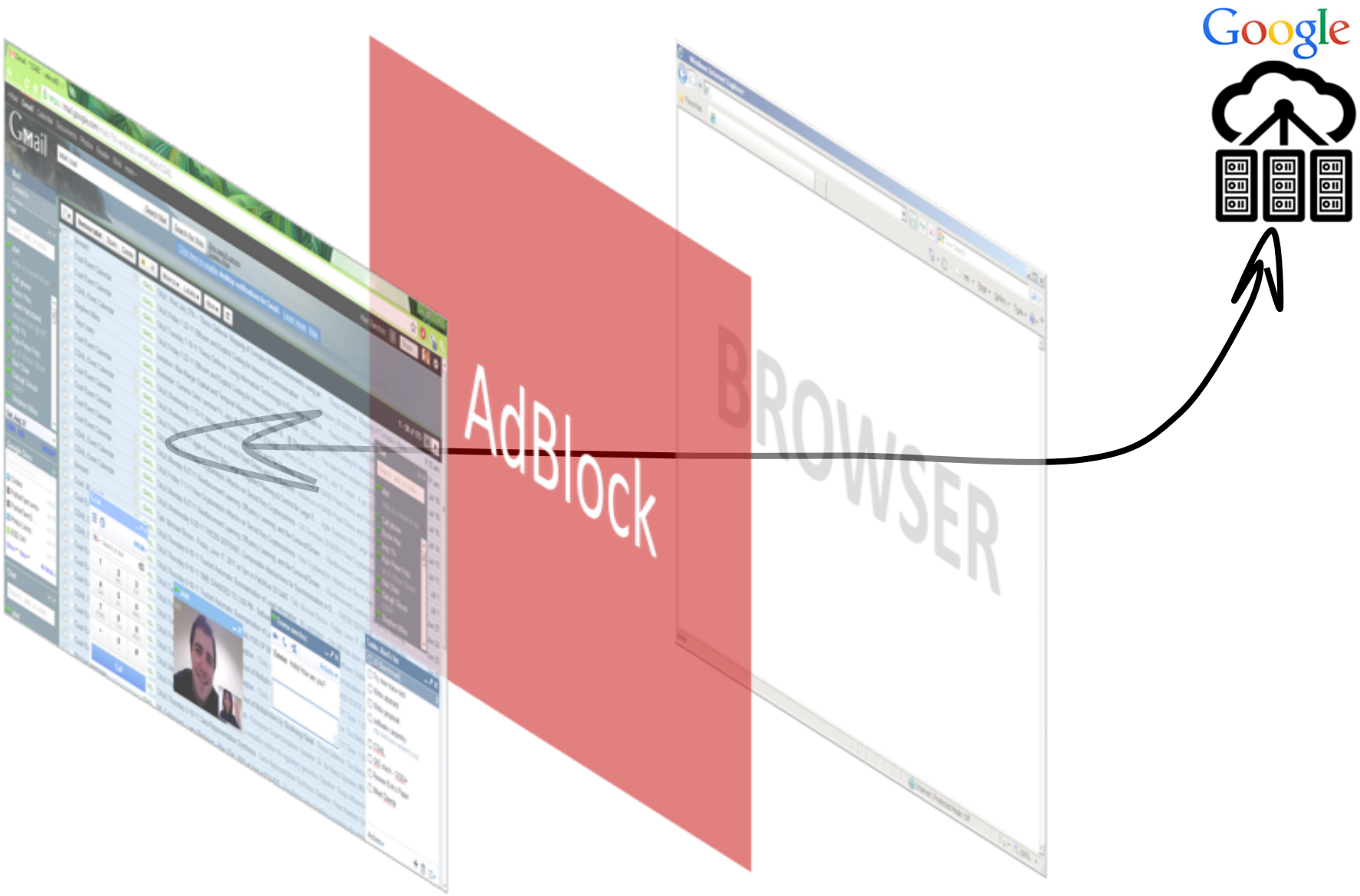
Information Sharing



Browser

- Largest attack platform
- Over 20M LOCs
- Zero-days like OS
- You could teach a CS curriculum on the browser

Plugins



AdBlock

- *The Wall Street Journal* reported that paying customers include Google, Microsoft, and Taboola.

Avoid

- Free Wi-Fi in:
  - Hotels
  - Airports
  - Cafes
  - Airplanes
- If you use it, avoid
  - Entering passwords
  - Entering PII, PHI

VPNs

- Is the VPN using up-to-date protocols?
- Reputation/history of company, people behind it?
- Terms of service?
- Protection, what is not covered?
- Privacy policy?

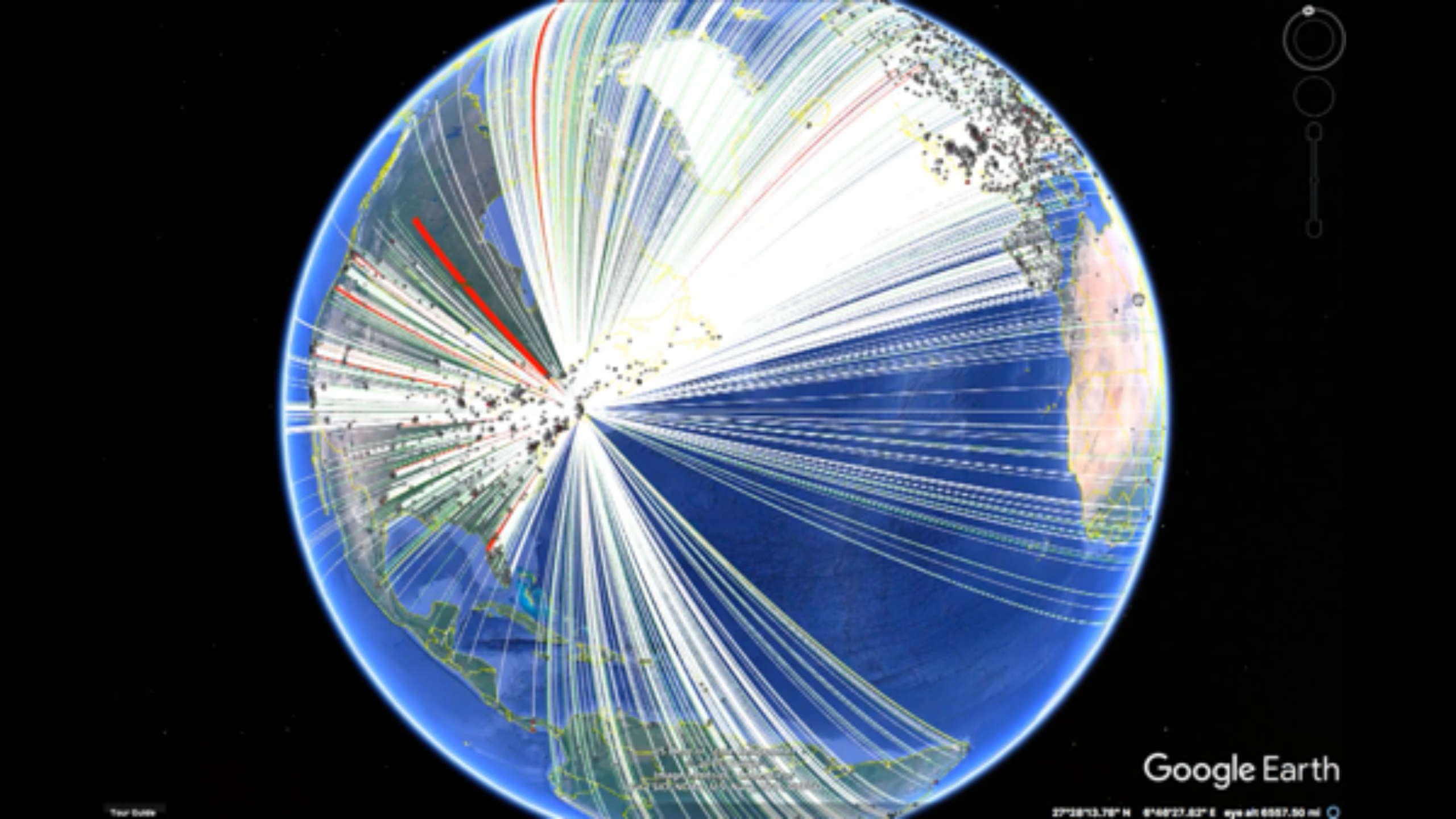
MIT EXPERIMENT


Connected
12 Hours
No users
Collected Attack Data

Demo …

- →←↑↓, r


Google Earth Pro
Search
Places
My Places
Sightseeing Tour
Temporary Places
Layers
Primary Database
Borders and Labels
Places
Photos
Roads
3D Buildings
Ocean
Weather
Gallery
Global Awareness
More
Terrain
Sign In
Google Earth


Google Earth


FAKE NEWS


Protecting Election Integrity
Fighting Fake News
Data Privacy

A Facebook War: Libyans Battle on the Streets and on Screens


Facebook

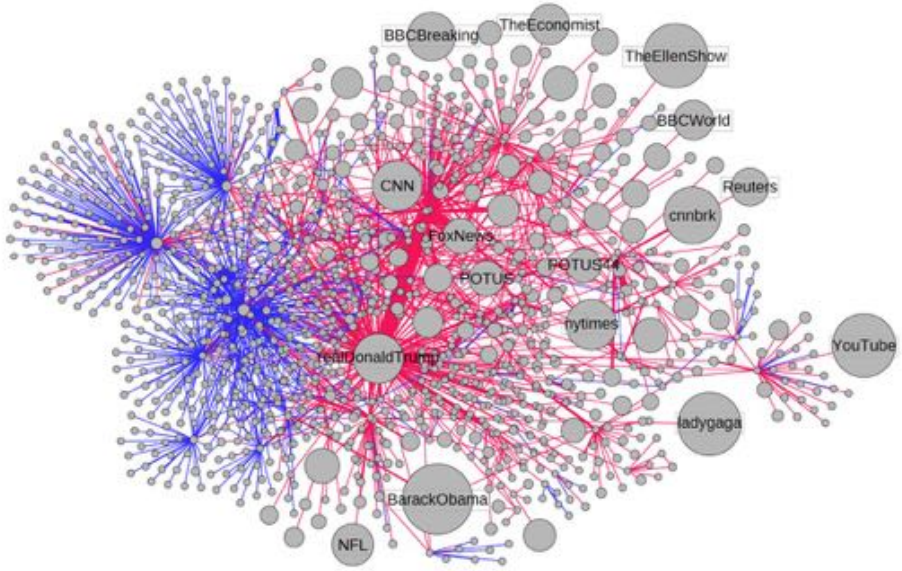

Cambridge
Analytica
facebook

The New York Times

Russian Hacking and Influence in the U.S. Election

Complete coverage of Russia's campaign to disrupt the 2016 presidential election.

Study: It only takes a few seconds for bots to spread misinformation



false stories travel "farther, faster, deeper, and more broadly than the truth in all categories of information ... a false story only needs roughly 10 hours to reach 1,500 users on Twitter, compared to 60 hours for a true story.

"No matter how you slice it, falsity wins out,"

They examined 14 million messages shared on Twitter between May 2016 and May 2017, spanning the presidential primaries and Trump's inauguration. And they found it took just six percent of Twitter accounts identified as bots to spread 31 percent of what they term "low-credibility" information on the social network. The bots managed this feat in just two to 10 seconds

https://arstechnica.com/science/2018/11/study-it-only-takes-a-few-seconds-for-bots-to-spread-misinformation/

Real-time Facial Reenactment

Live capture using a commodity webcam


FINDING TALENT

Too Few Professionals

2 MILLION:
GLOBAL SHORTAGE OF CYBERSECURITY **PROFESSIONALS BY 2019**[7]

3X
RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14[8]

84%
ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR **OPEN SECURITY JOBS ARE QUALIFIED**[9]

53%
OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS **6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES**[10]

77% **OF WOMEN**
SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER.
FOR MEN, IT IS 67%.[11]

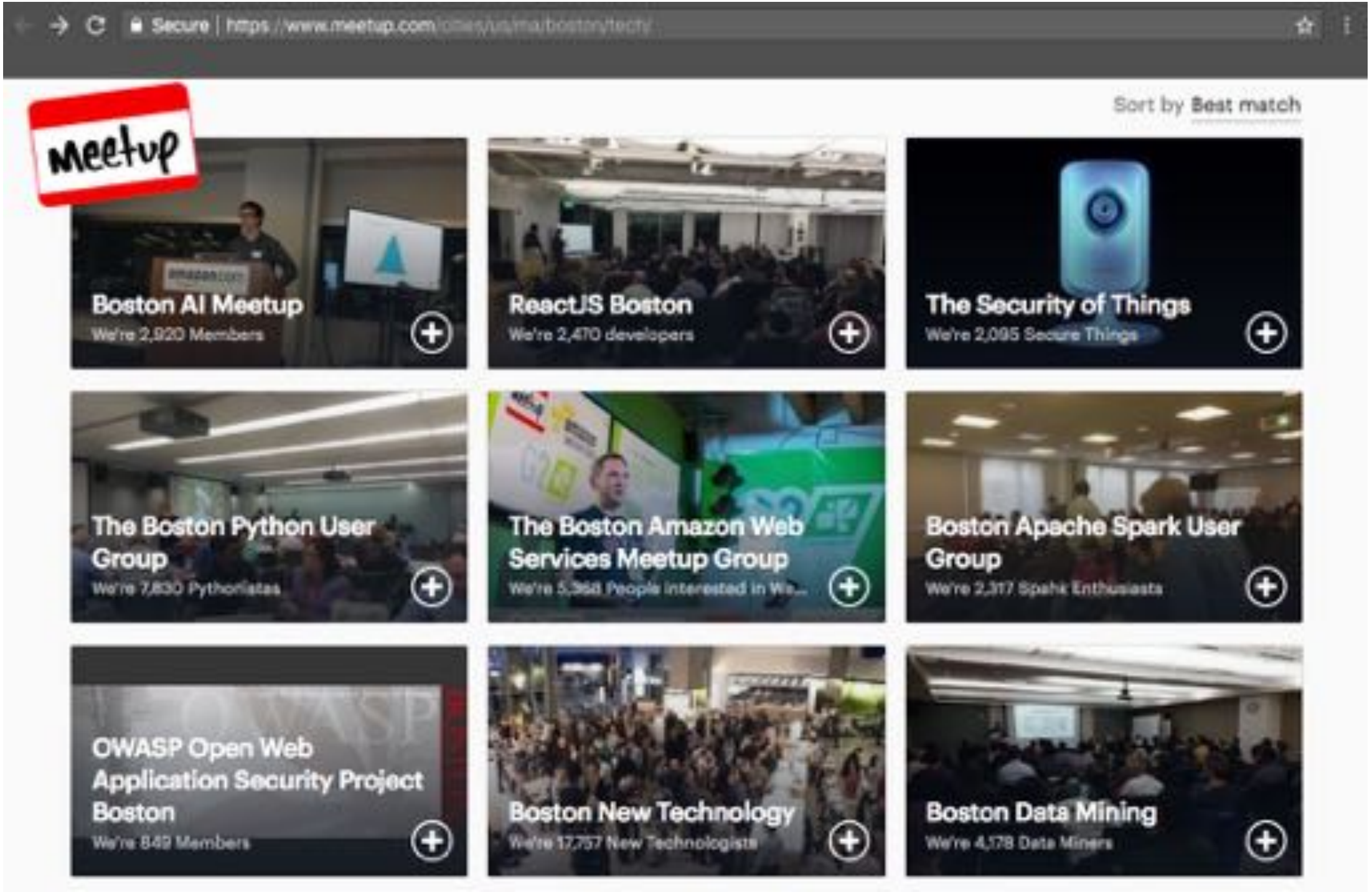
89% **OF U.S.**
CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO **HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.**[12**]

Build A Pipeline

- Strong ties with top talent sources
  - MIT and Peers
- Start small
  - Build from there

Non-traditional Sources

- Open source community – Github
- Hackathons
  - Last MIT hackathon had 500 people
  - Great majority not from MIT
- Meetups
- Bootcamps
  - 16 weeks, 2017 output approached 50% of all accredited colleges in Computer Science
- Nanodegrees


Secure | https://www.meetup.com/cities/us/ma/boston/tech/
Meetup
Sort by Best match
Boston AI Meetup
We're 2,920 Members
ReactJS Boston
We're 2,470 developers
The Security of Things
We're 2,095 Secure Things
The Boston Python User Group
We're 7,830 Pythonistas
The Boston Amazon Web Services Meetup Group
Boston Apache Spark User Group
We're 2,317 Spark Enthusiasts
OWASP Open Web Application Security Project Boston
We're 849 Members
Boston New Technology
We're 17,757 New Technologists
Boston Data Mining
We're 4,178 Data Miners

Lead the Community

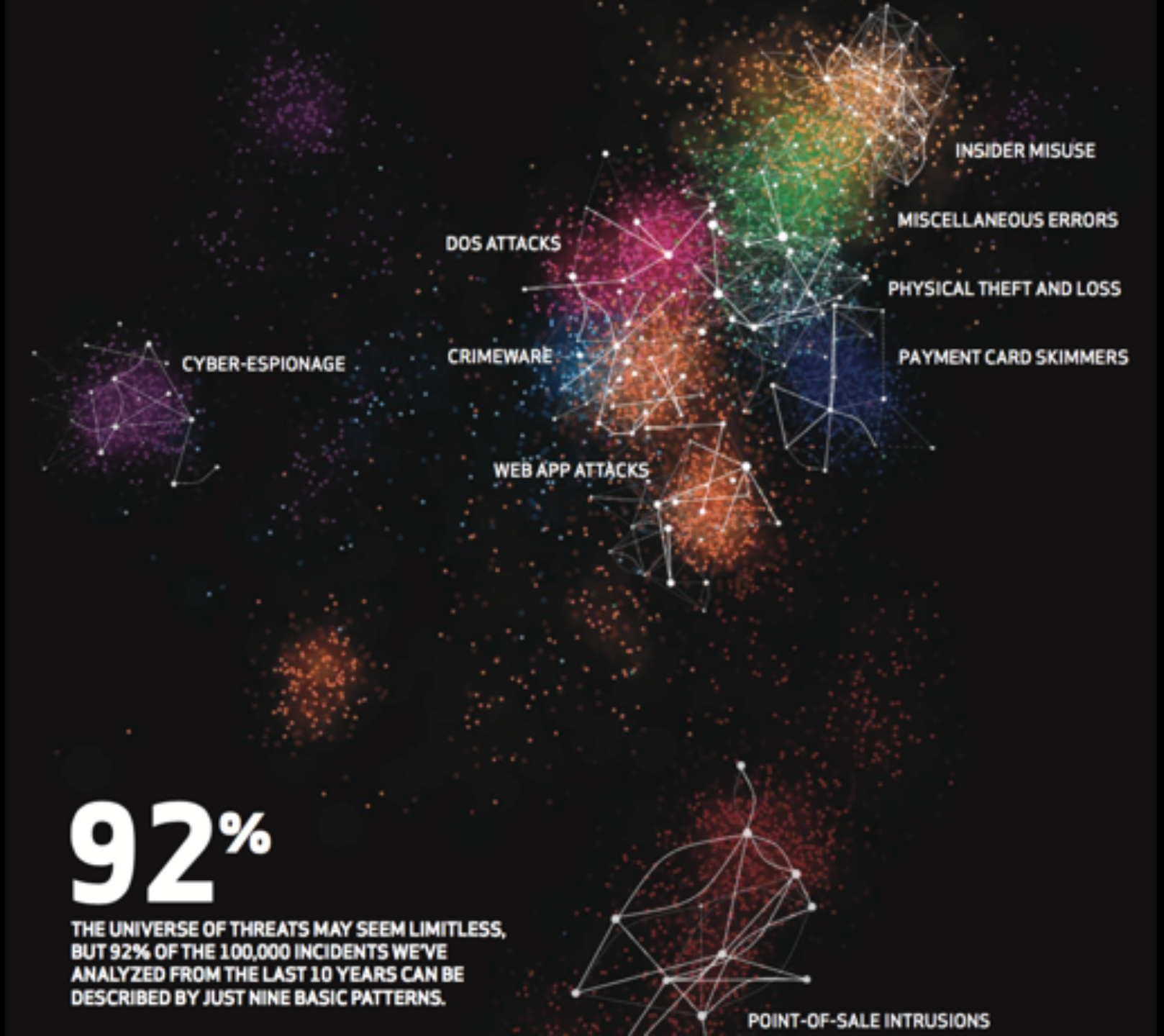
- Contribute to community code bases
- Speak at community events
- Engage, participate
- Be recognized as a thought leader
- Run/sponsor hackathons

Gamulation: gamification + simulation

- Puts learner right in the middle of a fun
- Engaging story-line and environment
- Compete with other learners
- Perform the skills and actions you would in real life
- Red/Blue team training


$50,000
1
01:48
00
ACQUIRING TARGET
26
01:39
00
$30,000
6
01:29
00

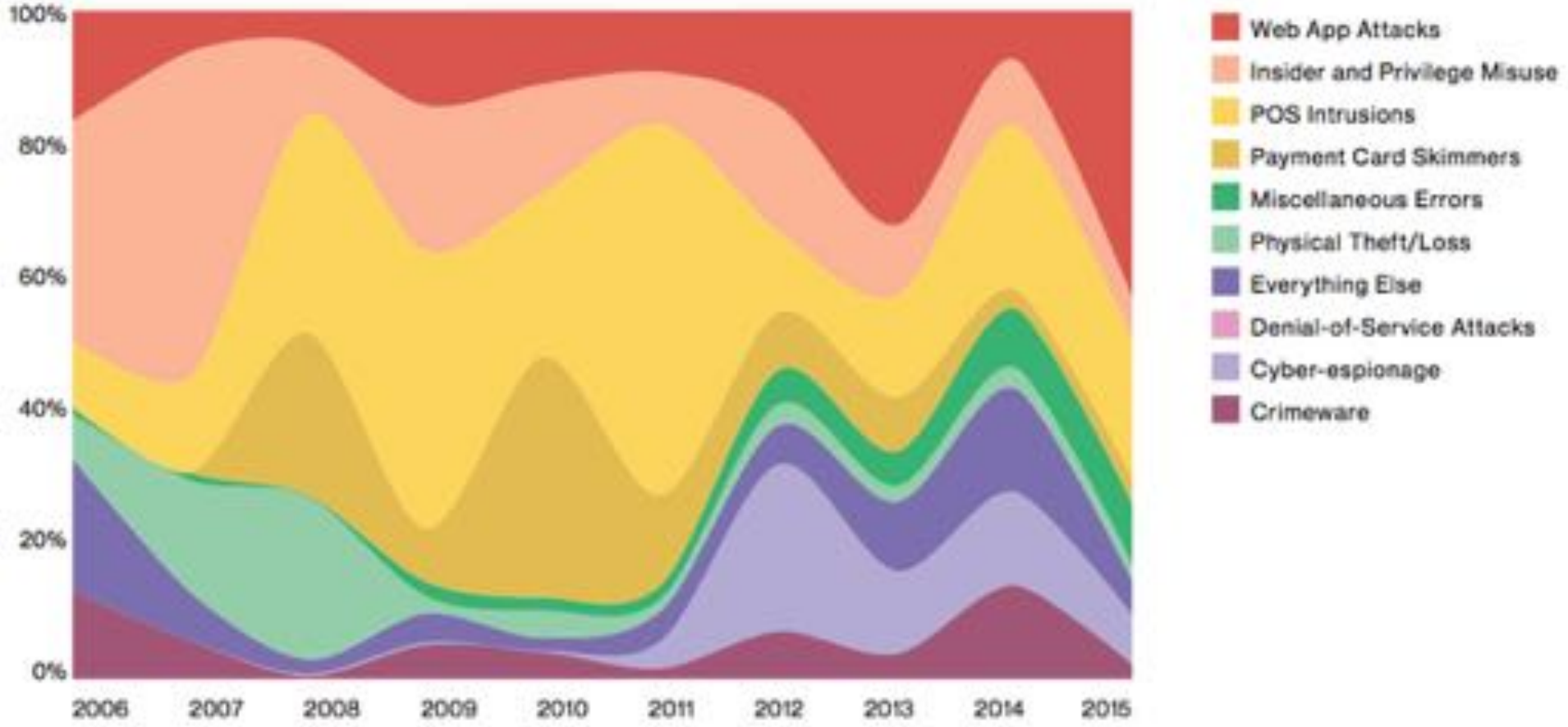

PATTERNS



92%

THE UNIVERSE OF THREATS MAY SEEM LIMITLESS, BUT 92% OF THE 100,000 INCIDENTS WE'VE ANALYZED FROM THE LAST 10 YEARS CAN BE DESCRIBED BY JUST NINE BASIC PATTERNS.

Breaches over time



Patterns by industry

Crimeware	Cyber-espionage	Denial of Service	Everything Else	Stolen Assets	Misc. Errors	Card Skimmers	Point of Sale	Privilege Misuse	Web Apps	Incident patterns by industry minimum 25 incidents (only confirmed data breaches)
			1%	<1%	1%	<1%	95%	1%	1%	Accommodation (72), n=282
	7%		17%	17%	27%			3%	30%	Educational (61), n=29
				3%			47%		50%	Entertainment (71), n=38
1%	<1%	<1%	2%	<1%	2%	9%		4%	82%	Finance (52), n=795
3%	3%		11%	19%	22%		7%	32%	3%	Healthcare (62), n=115
1%	3%		4%		25%		1%	11%	57%	Information (51), n=194
3%	47%		3%				3%	24%	21%	Manufacturing (31-33), n=37
4%	19%		25%	4%	15%			21%	13%	Professional (54), n=53
12%	16%		4%	9%	37%			13%	9%	Public (92), n=193
1%	1%		4%		1%	3%	64%	2%	26%	Retail (44-45), n=182

Phishing

2015	
Clicked	23%
Opened	11%

2016	
Clicked	30%
Opened	12%

US-CERT

Patching is a problem

99.9%
OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.

About half of the CVEs exploited in 2014 went from publish to pwn in less than a month.

Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

CLOSING THOUGHTS

Stop blaming users

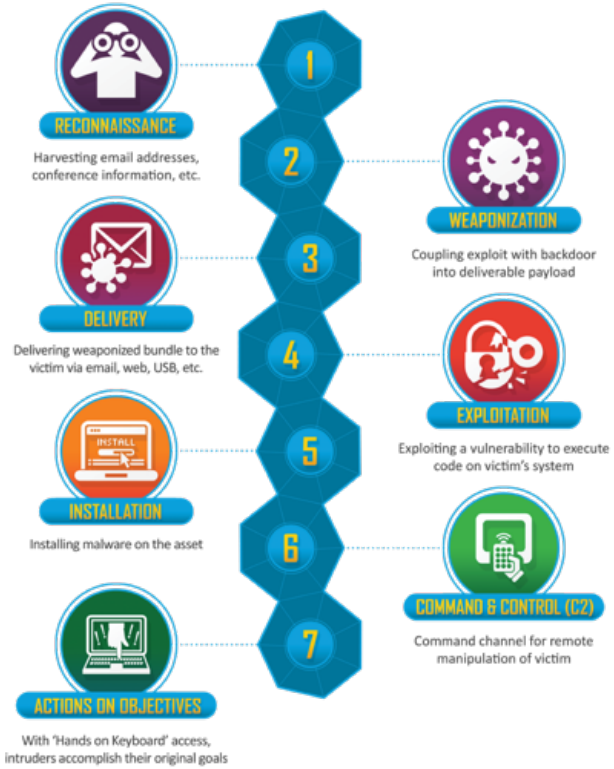
- Security warnings have become meaningless
- Passwords
  - Stop the complexity rules
  - Stop password expiration
  - Let people use password managers
- Phishing works because linking works

Security needs to change

- If users do not change, security needs to change
- Successful examples
  - Automatic updates
  - Cloud docs vs desktop docs
  - Sandboxing for browsing

Frameworks

LM Kill Chain



NIST

Function Unique Identifier	Category
ID	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
PR	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
DE	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RS	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
RC	Recovery Planning
	Improvements
	Communications

Functions

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Crowd Strike

SECURITY FOUNDATIONS

Asset management and maintenance
Data classification
Testing and exercises
Operational baselines
Backups

PREVENTION

Access controls
Security architecture and segmentation
Hardening
Patching and vulnerability management
Account / Authentication management
Preventive technologies
Secure development

DETECTION

Log management and analysis
Detection technologies
Monitoring process
Proactive hunting

RESPONSE

Triage
Plans and playbooks
Communications and escalation protocols
Roles and responsibilities
Forensic analysis
Containment and eradication
Root cause and lessons learned

GOVERNANCE

Plans, policies, and procedures
Security culture
Awareness and training
Risk management
Executive management

THREAT INTELLIGENCE

Risk identification
Strategic intelligence
Operational intelligence
Intelligence sources

Guidance

- Look at your peers
- Use industry best practices
- Hire external council, assessments
- Practice major incident response plan
  - Including media
  - At least once a year
- Revisit incident response plan after each major event
- Buy insurance


IBM Security

Guidance

- Invest in Machine Learning (ML) for security
- Consultants role
- Build the team internally

State of the practice?

We have the technology, the brains, the funding, yet …

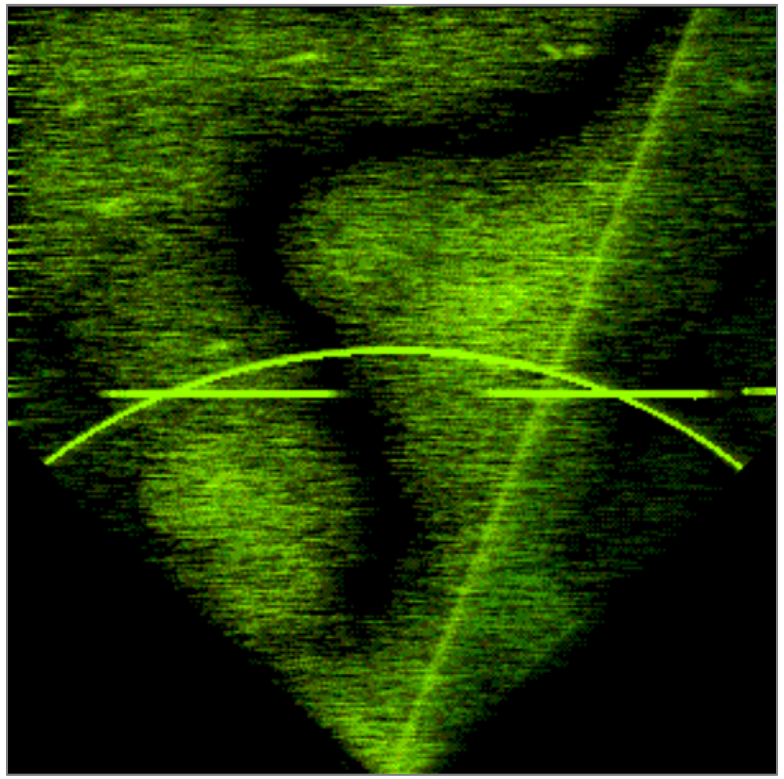
- Our operations are slow … reactive …
- We are running into a skill gap/fatigue
- We don’t make their life hard enough

Security Teams Today

- Spend most of their time
  - Tuning
  - Mastering
  - Configuring
  - A lot of effort to make tools work

Technology transforming human operations

1965 Aviation Radar

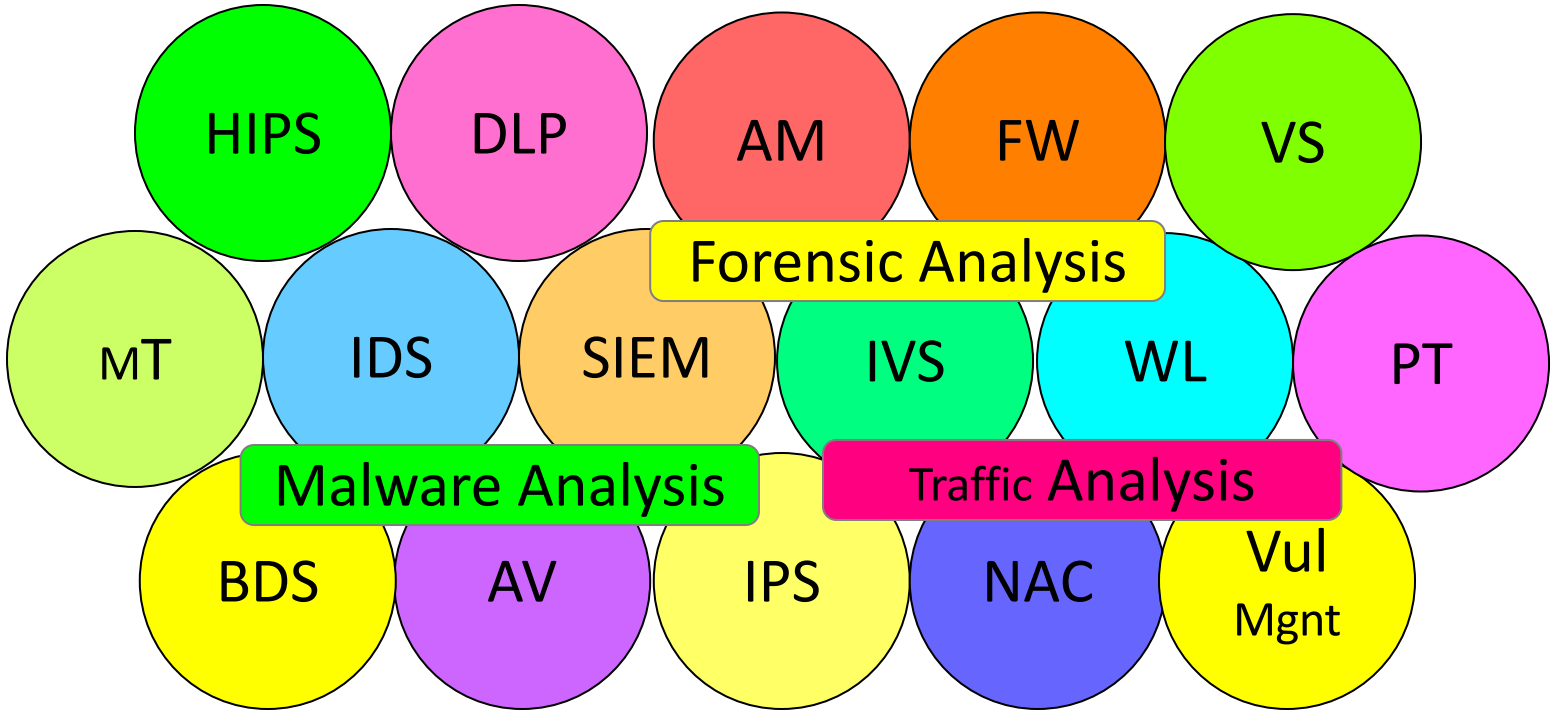


2015 Tactical Situation Display

Operator Transformation

	Fly	Fighter	System Op	Think/Decide	
HUMAN					**Policy**
PLATFORM	Stick Throttle Gun	Jet Engines Missiles	Radar BVR Missiles RWR	Detect Threat Identify Threat Select Weapon Human Decision	

Tool explosion



Conclusion

- Build talent pipelines
- Best practices – top controls
- Cybersecurity Patterns
- Invest in ML security

Q & A