SHE BLINDED ME WITH SCIENCE

Understanding Misleading, Manipulative, and Deceptive Cybersecurity

Josiah Dykstra, PhD
@JosiahDykstra
dykstra@EssentialCybersecurityScience.com

The views expressed in this presentation are mine alone. Reference to any specific products, process, or service do not necessarily constitute or imply endorsement, recommendation, or favoring by the United States Government or the Department of Defense.

The content of this presentation is not intended to malign any religion, ethnic group, club, organization, company, individual, vendor, product, or service. Any such material presented in any format, without limitation, is for informational purposes only. Any potential customer of any vendor is expected to conduct their own due diligence and assessment of the vendor, product, or services as appropriate for their needs.

HELLO

I'm Josiah. I'm a Scientist.

WHY THIS?

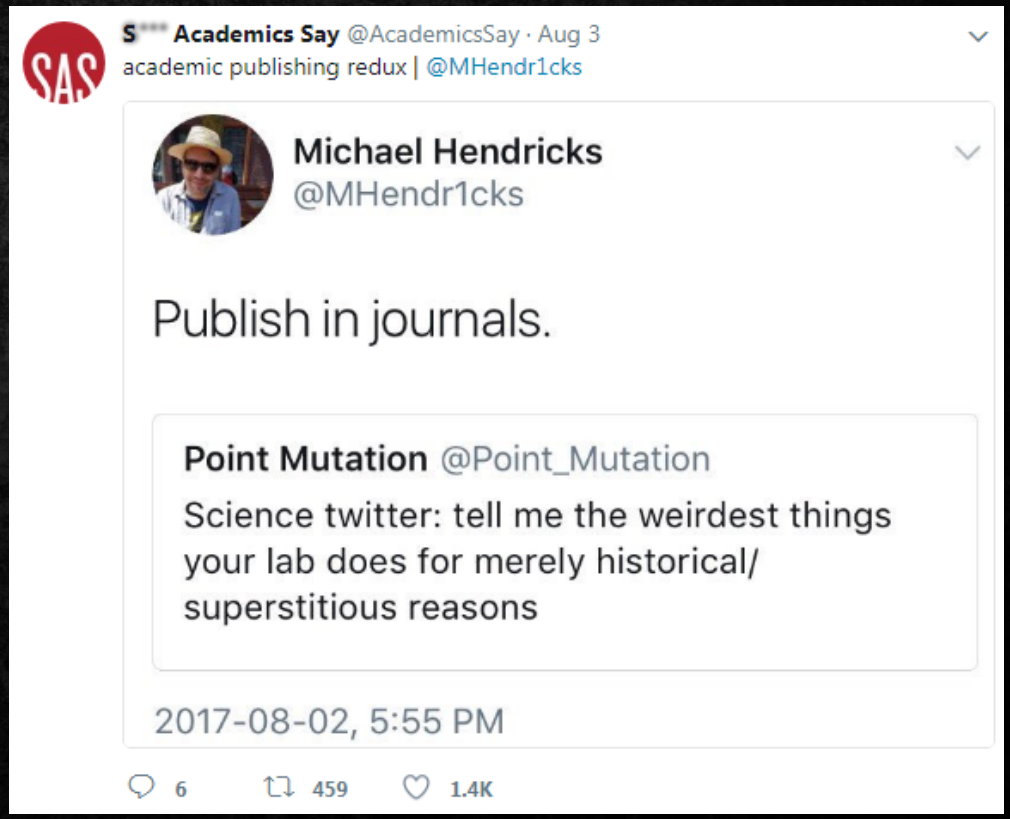
Bureau of Labor Statistics

Quick Facts: Information Security Analysts	
2016 Median Pay	$92,600 per year
Typical Entry-Level Education	Bachelor's degree
Work Experience in a Related Occupation	Less than 5 years
On-the-job Training	None
Number of Jobs, 2014	82,900
Job Outlook, 2014-2024	18% (Much faster than average)

Average Age	42.2
Gender Composition, 2015	77% male
Race, 2015	74% white

https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1
https://datausa.io/profile/soc/151122/#demographics

Few cybersecurity practitioners read academic research papers



Few cybersecurity practitioners read academic research papers

> The present study aimed to extend Bashir et al.'s (2015) research into cybersecurity competition participants by using more comprehensive measures of self-efficacy and similar personality variables to elucidate the role of self-efficacy in broader cybersecurity outcomes.

https://www.usenix.org/system/files/conference/ase16/ase16-paper-wee.pdf

Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

Mathy Vanhoef
imec-DistriNet, KU Leuven
Mathy.Vanhoef@cs.kuleuven.be

ABSTRACT

We introduce the key reinstallation attack. This attack abuses design or implementation flaws in cryptographic protocols to reinstall an already-in-use key. This resets the key's associated parameters such as transmit nonces and receive replay counters. Several types of cryptographic Wi-Fi handshakes are affected by the attack.

All protected Wi-Fi networks use the 4-way handshake to generate a fresh session key. So far, this 14-year-old handshake has remained free from attacks, and is even proven secure. However, we sho
tion att
already
handsh
eters su
receive
value. C
key, an
on the
tocol in
and dec
TCP st
TKIP ar

NBC 7 SAN DIEGO | Home | News | Weather | SportsWrap | Entertainment | ••• | 69° | Connect

'Krack' Security Flaw Puts Every Wi-Fi Connection at Risk

But the gaping hole in the Wi-Fi protocol is fixable

sign in | become a supporter | subscribe | search | jobs | US edition

theguardian

US | politics | world | opinion | sports | soccer | tech | arts | lifestyle | fashion | business | travel | environment | browse all sections

home › tech

Wifi

'All wifi networks' are vulnerable to hacking, security expert discovers

WPA2 protocol used by vast majority of wifi connections has been broken by Belgian researchers, highlighting potential for internet traffic to be exposed

< 7,341

Alex Hern

@alexhern

Monday 16 October 2017 04.33 EDT

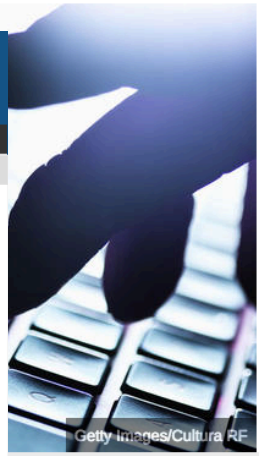


The researchers have given the weakness the codename Krack, short for Key Reinstallation AttaCK. Photograph: Vladislav Kochelaevskiy / Alamy/Alamy

Advertisement

GENERAL DYNAMICS
Information Technology

CLOUD SOLUTIONS
Complete Choice.
Complete Solutions.
Complete Confidence.



heir smartphone and laptop,

ome network is
te chats to baby

Click For Sound

Tri-City Medical Center
ADVANCED HEALTH CARE...FOR YOU

TRENDING STORIES

1 VIDEO Chula Vista to Offer Amazon $400M in Incentives for HQ2

2 3.6 Magnitude Earthquake Hits Near Santa Ysabel

MARKETING SCIENCE
HACKING ARTICLE TITLES

- Title Type
- Title Length
- Readability
- Humor

http://eprints.rclis.org/19669/1/Jamali_title.pdf
http://rsos.royalsocietypublishing.org/content/2/8/150266
https://ai2-s2-pdfs.s3.amazonaws.com/21c0/7eb72853a4012af90a5b316af0d481519563.pdf

10

43

48

32

129

61

108

58

14

14

Accepted papers

1. **An Historical Examination of Open Source Releases and Their Vulnerabilities.**

   Nigel Edwards (Hewlett-Packard Laboratories), Liqun Chen (Hewlett-Packard Laboratories).

2. **Non-tracking Web Analytics.**

   Istemi Ekin Akkus (Max Planck Institute for Software Systems (MPI-SWS)), Ruichuan Chen (Max Planck Institute for Software Systems (MPI-SWS)), Michaela Hardt (Twitter Inc.), Paul Francis (Max Planck Institute for Software Systems (MPI-SWS)), Johannes Gehrke (Cornell University).

3. **A Cross-Protocol Attack on the TLS Protocol.**

   Nikos Mavrogiannopoulos (KU Leuven - IBBT), Frederik Vercauteren (KU Leuven - IBBT), Vesselin Velichkov (University of Luxembourg), Bart Preneel (KU Leuven - IBBT).

4. **Mobile Data Charging: New Attacks and Countermeasures.**

   Chunyi Peng (University of California, Los Angeles), Chi-yu Li (University of California, Los Angeles), Guan-Hua Tu (University of California, Los Angeles), Songwu Lu (University of California, Los Angeles), Lixia Zhang (University of California, Los Angeles).

5. **The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems.**

   San-Tsai Sun (University of British Columbia), Konstantin Beznosov (University of British Columbia).

6. **CensorSpoofer: Asymmetric Communication using IP Spoofing for Censorship-Resistant Web Browsing.**

   Qiyan Wang (University of Illinois at Urbana-Champaign), Xun Gong (University of Illinois at Urbana-Champaign), Giang T. K. Nguyen (University of Illinois at Urbana-Champaign), Amir Houmansadr (University of Illinois at Urbana-Champaign), Nikita Borisov (University of Illinois at Urbana-Champaign).

7. **Self-service Cloud Computing.**

   Shakeel Butt (Rutgers University), H. Andres Lagar-Cavilla (GridCentric Inc.), Abhinav Srivastava (AT&T Labs-Research), Vinod Ganapathy (Rutgers University).

8. **Aligot: Cryptographic Function Identification in Obfuscated Binary Programs.**

   Joan Calvet (Universite de Lorraine, LORIA), Jose M Fernandez (Ecole Polytechnique de Montreal), Jean-Yves Marion (Universite de Lorraine, LORIA).

9. **Populated IP Addresses -- Classification and Applications.**

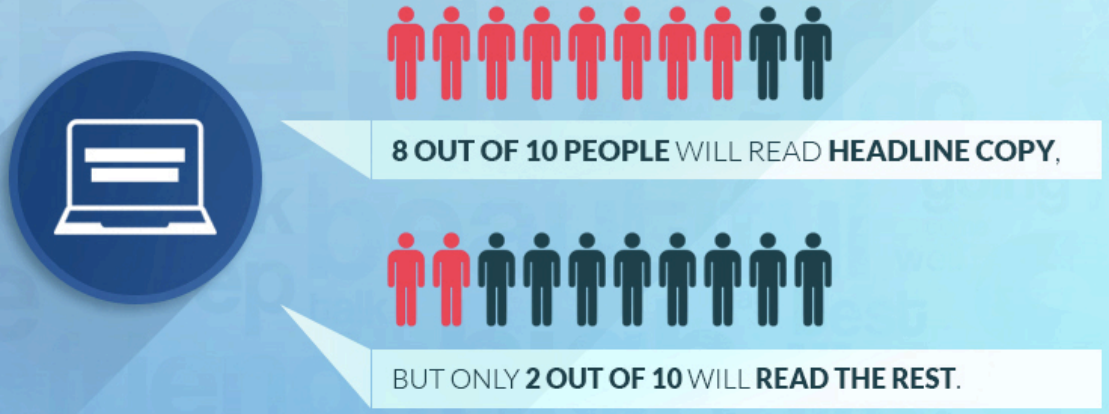
   Chi-Yao Hong (UIUC), Fang Yu (MSR Silicon Valley), Yinglian Xie (MSR Silicon Valley).

10. **On the Parameterized Complexity of the Workflow Satisfiability Problem.**

    Jason Crampton (Royal Holloway, University of London), Gregory Gutin (Royal Holloway, University of London), Anders Yeo (University of Johannesburg).

Google Scholar Citations for First 10 2012 CCS Papers

What Makes A GOOD HEADLINE



https://blog.kissmetrics.com/creating-headlines-for-clicks/





https://blog.kissmetrics.com/creating-headlines-for-clicks/

CYBERSECURITY "MAGIC"


SNAKE OIL LINIMENT
THE STRONGEST AND BEST LINIMENT KNOWN FOR THE CURE OF ALL PAIN AND LAMENESS.
USED EXTERNAL — ONLY. — FOR
RHEUMATISM
NEURALGIA
SCIATICA
LAME BACK
LUMBAGO
CONTRACTED MUSCLES
TOOTHACHE
SPRAINS
SWELLINGS
ETC.
CLARK STANLEY'S
TRADE MARK
SNAKE OIL LINIMENT.
CURES
FROST BITES
CHILL BLAINS
BRUISES
SORE THROAT
BITES OF ANIMALS INSECTS AND REPTILES.
IT GIVES IMMEDIATE RELIEF
IS GOOD FOR EVERYTHING A LINIMENT OUGHT TO BE GOOD FOR
Manufactured by
CLARK STANLEY
Snake Oil Liniment
Company
Providence, R. I.


PANTENE
scientifically proven healthier hair
from inside out with
PRO-VITAMIN


TRESemmé
NEW SYSTEM
KERATIN
SMOOTH
WITH
MARULA OIL

SCIENCE
AND "SCIENCE"



OUR METHOD

In 2014, 26% of Americans reported a clear understanding of scientific study.



OUR KNOWLEDGE

Nearly half of Americans cited the Internet as their primary source of science and technology information in 2014.



OUR BELIEFS

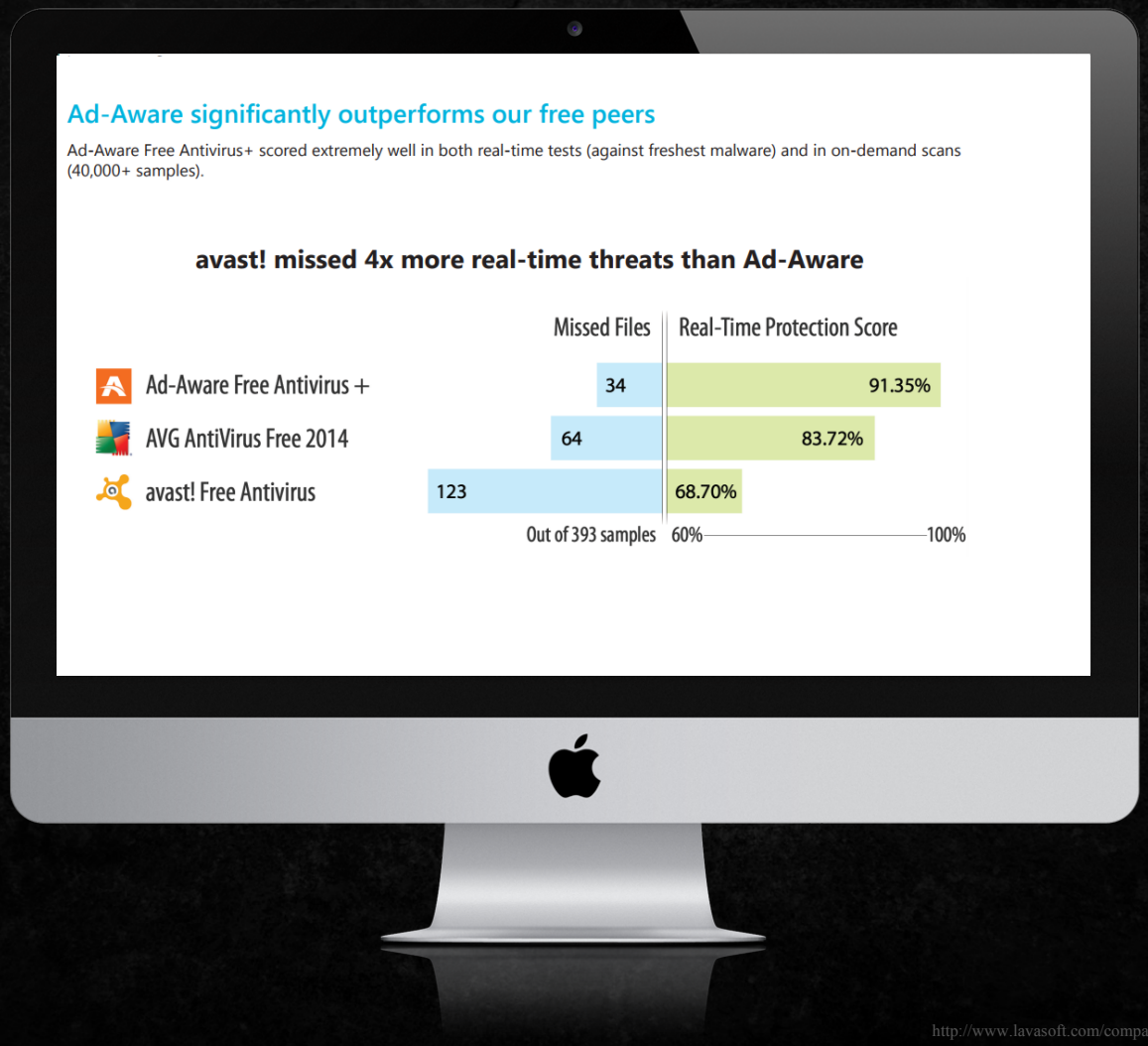
About 4 in 10 Americans say they have "a great deal of confidence" in the scientific community.

National Science Board, "Science and Engineering Indicators," 2016
https://www.nsf.gov/statistics/2016/nsb20161/uploads/1/nsb20161.pdf

FAILURE TO NOTICE?



http://www.lavasoft.com/company/press/adaware11/files/ad-aware_free_product_sheet.pdf



http://www.lavasoft.com/company/press/adaware11/files/ad-aware_free_product_sheet.pdf

ZoneAlarm By Check Point

My Account | Cart | EN

PC Security | NEW Anti-Ransomware | Mobile Security | Free | Support | Renew



Windows 10/8/7, Vista and XP

The 100% virus-free guarantee is based on AV-Test's 6/6 Protection score, with 100% protection from zero-day attacks and 100% detection of widespread and prevalent malware.

ZoneAlarm®

EXTREME SECURITY 2017

Virus Free. 100% Guaranteed. [Terms]

- Protects you from WANNACRY and all other zero-day attacks
- Prevents identity theft with advanced Anti-Phishing protection
- Defends your entire family with best antivirus and Parental Controls
- Find My Laptop, PC Tune-Up, Online Backup, Identity Protection and more are included.

3 months | 1 year | 2 years

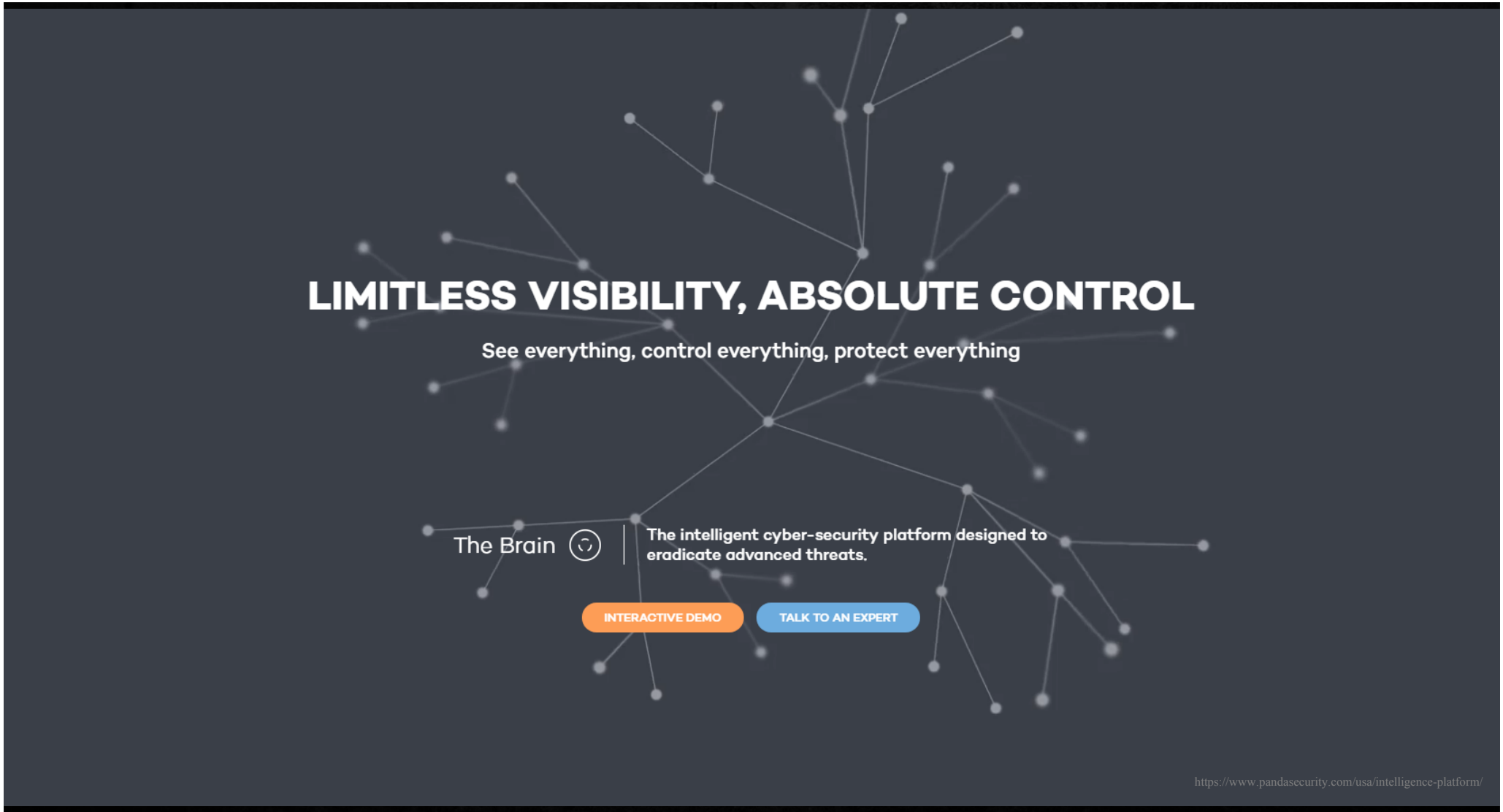
~~$89.95~~ $59.95

5 PCs

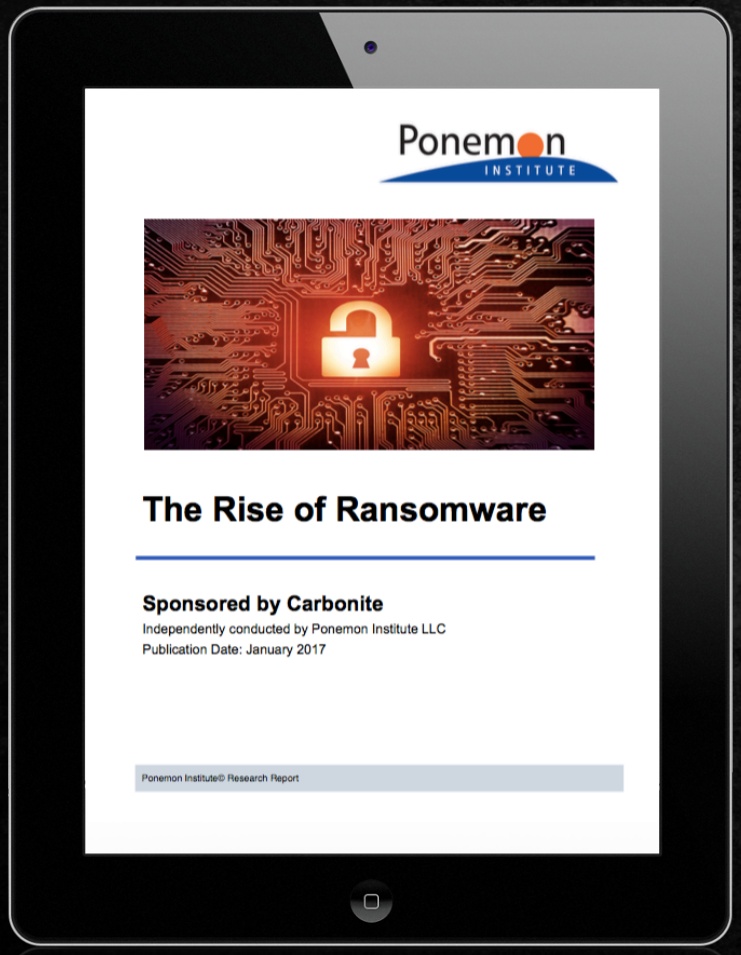
Buy Now

Free Trial

https://www.zonealarm.com/software/extreme-security/



https://www.pandasecurity.com/usa/intelligence-platform/



Reports and Surveys

- The Global State of Information Security® Survey 2017 (PwC)
- M-Trends® 2017
- Verizon's 2017 Data Breach Investigations Report
- Cisco 2017 Annual Cybersecurity Report
- Tenable Global Cybersecurity 2017 Assurance Report Card

https://www.ponemon.org/library/the-rise-of-ransomware

https://projects.fivethirtyeight.com/p-hacking/

HACKING SCIENCE



https://projects.fivethirtyeight.com/p-hacking/

HACKING SCIENCE

1 CHOOSE A POLITICAL PARTY

Republicans | Democrats

2 DEFINE TERMS

Which politicians do you want to include?

- [ ] Presidents
- [x] Governors
- [ ] Senators
- [ ] Representatives

How do you want to measure economic performance?

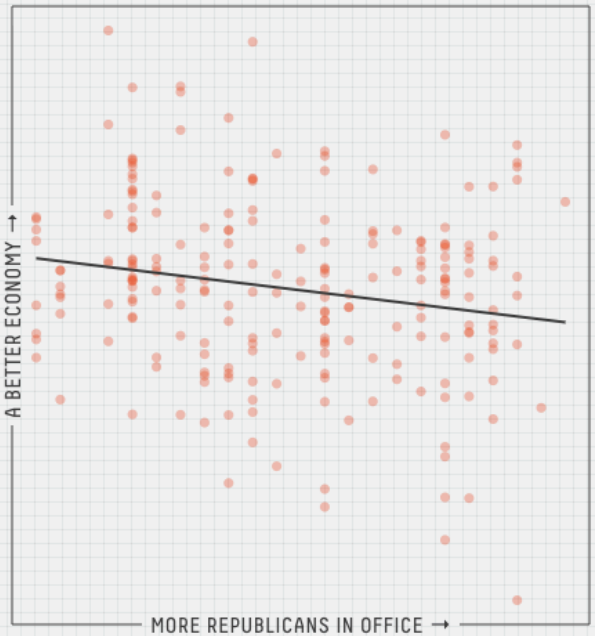
- [ ] Employment
- [x] Inflation
- [x] GDP
- [x] Stock prices

Other options

- [ ] **Factor in power**
  Weight more powerful positions more heavily
- [x] **Exclude recessions**
  Don't include economic recessions

3 IS THERE A RELATIONSHIP?

Given how you've defined your terms, does the economy do better, worse or about the same when more Republicans are in office? Each dot below represents one month of data.



4 IS YOUR RESULT SIGNIFICANT?

If there were no connection between the economy and politics, what is the probability that you'd get results at least as strong as yours? That probability is your p-value, and by convention, you need a **p-value of 0.05 or less** to get published.



Result: Publishable

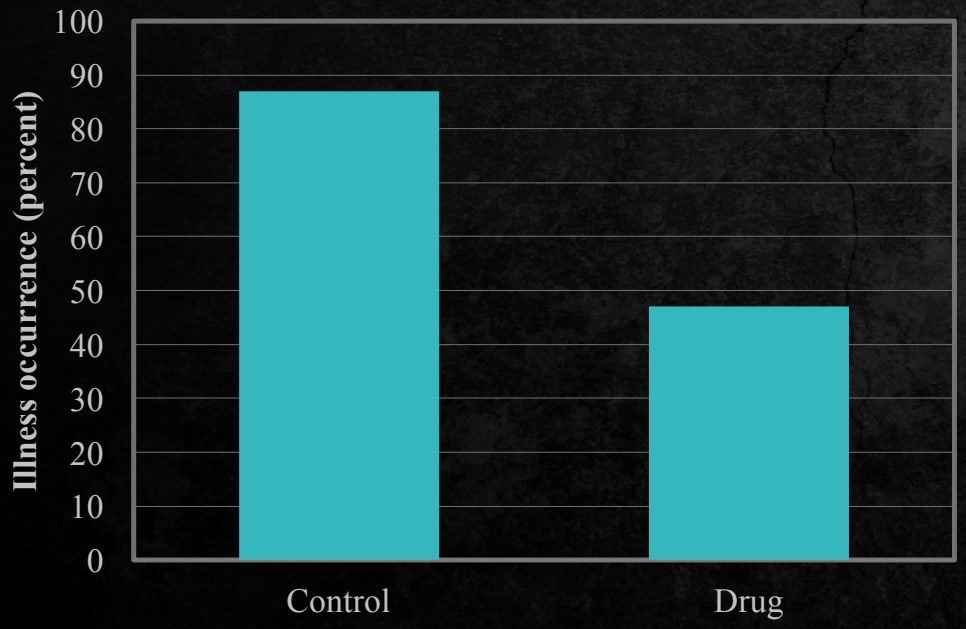
You achieved a p-value of **less than 0.01** and showed that **Republicans** have a **negative** effect on the economy. Get ready to be published!

If you're interested in reading real (and more rigorous) studies on the connection between politics and the economy, see the work of Larry Bartels and Alan Blinder and Mark Watson.

Data from The @unitedstates Project, National Governors Association, Bureau of Labor Statistics, Federal Reserve Bank of St. Louis and Yahoo Finance.


HUMAN FACTORS
Opportunities for Research
Who: Users, designers, administrators, adversaries
What: Beliefs, perceptions, motivations, biases, …
How: International, ecological validity, external validity

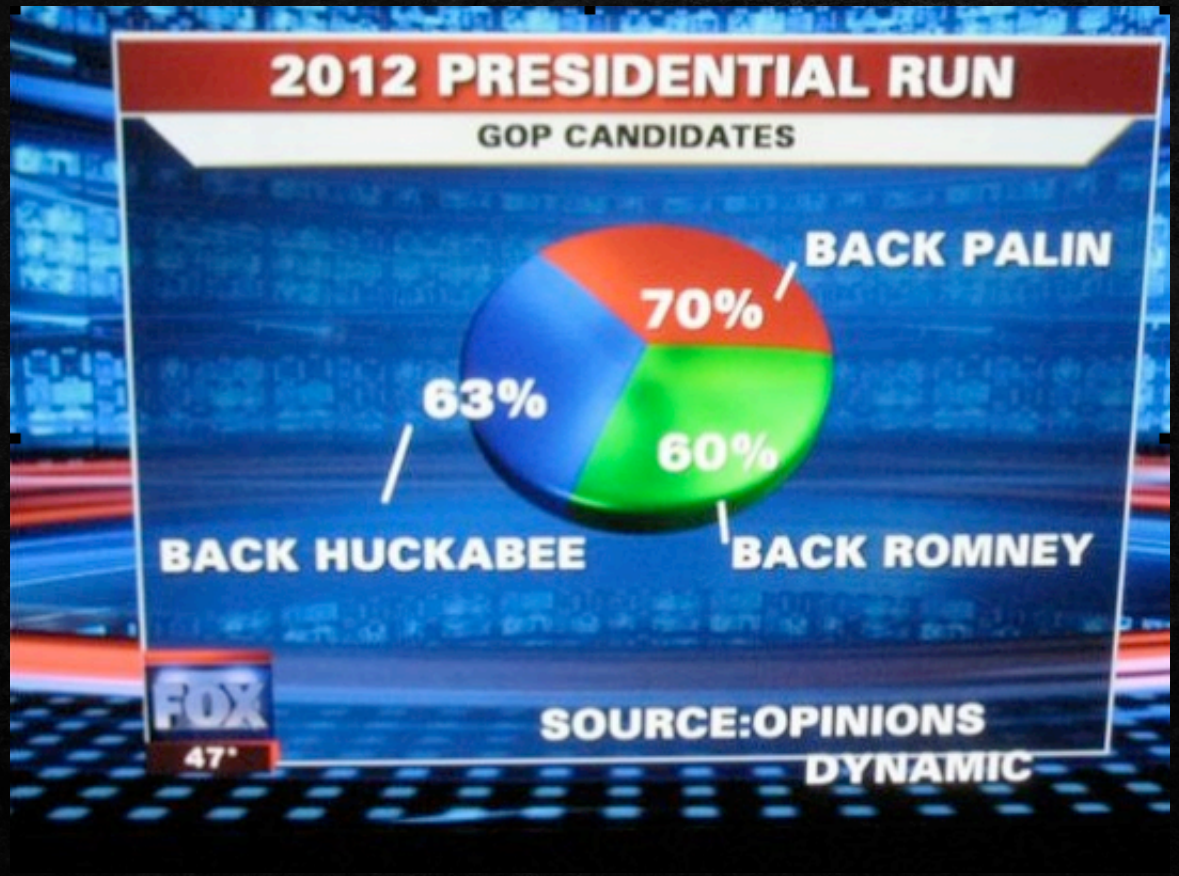
GRAPHS
INCREASE PERSUASION



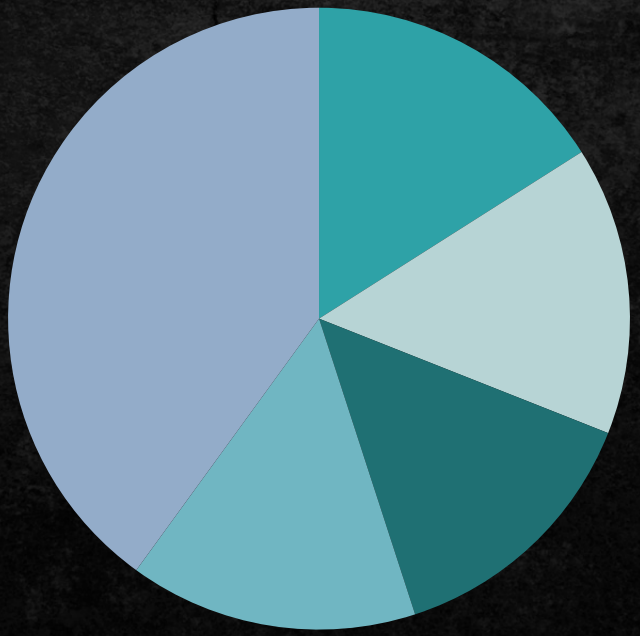
97% VS 68%

Participants given graphs expressed greater belief in the claims, rating the medication as more effective (6.83 of 9) than did participants given verbal description only (6.12 of 9). A chi-square test indicated that a higher percentage believed the medication would truly reduce illness for the graphs group (96.55%) than for the control group (67.74%).

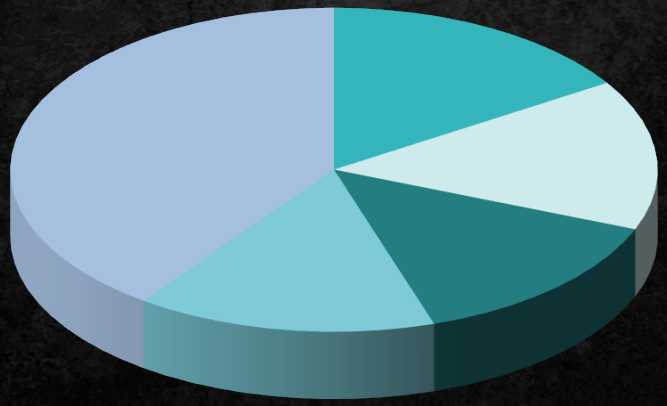
Aner Tal and Brian Wansink. "Blinded with science: Trivial graphs and formulas increase ad persuasiveness and belief in product efficacy." Public Understanding of Science, 2016, Vol. 25(1), 117-125.


2012 PRESIDENTIAL RUN
GOP CANDIDATES
BACK PALIN
70%
63%
60%
BACK HUCKABEE
BACK ROMNEY
FOX
47'
SOURCE:OPINIONS DYNAMIC

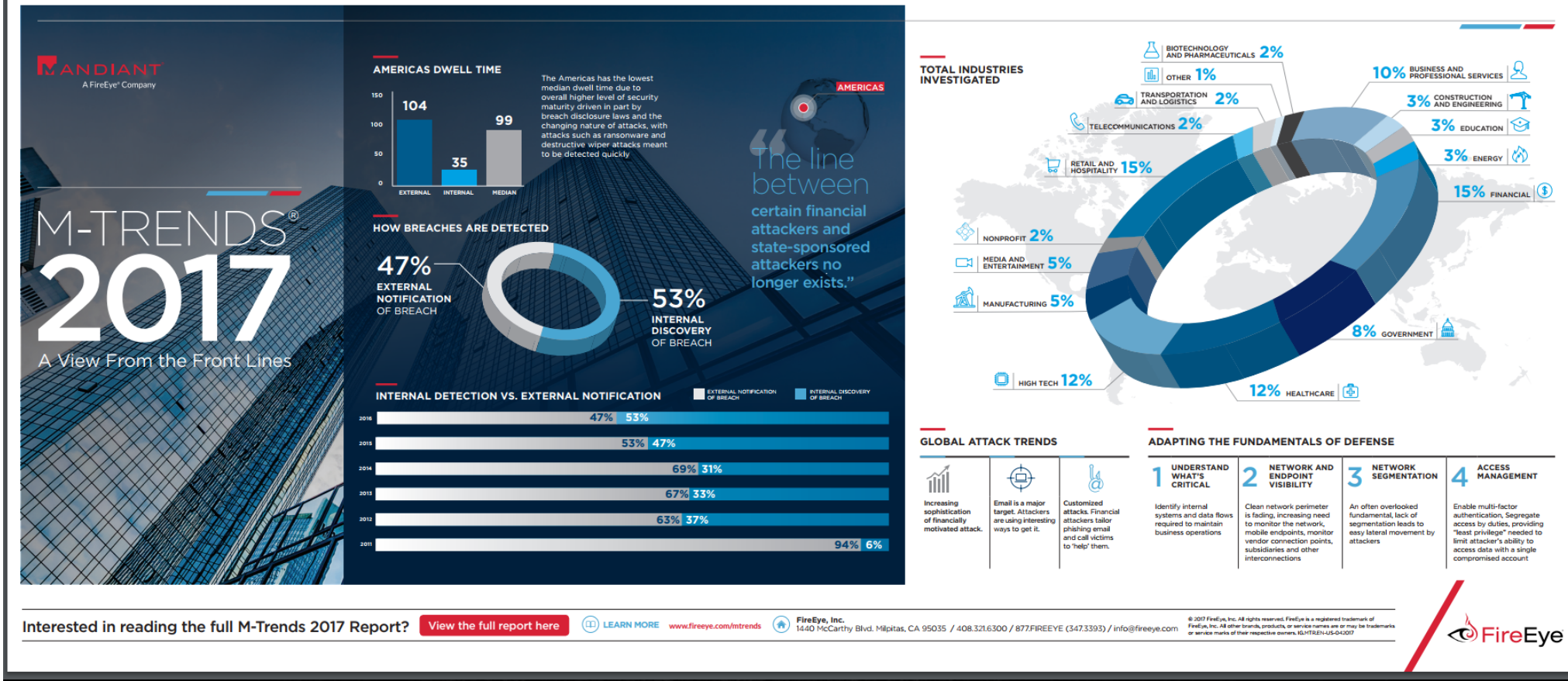
PIE CHARTS



PIE CHARTS




Logstash Search
2 days ago to 3 minutes ago
QUERY
bytes:[0 TO 4000000] AND @tags:success
FILTERING
EVENTS OVER TIME
MAP
REVENUE
22%
VOLUME
9%
TOP DESTINATIONS
TOP SOURCES
GEO PAIRS
ALL EVENTS
0 to 100 of 500 available for paging
Fields



https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/ig-mtrends-2017.pdf

WHAT CAN YOU DO?

Federal Trade Commission

Protecting America's Consumers

According to the FTC's complaint, D-Link promoted the security of its routers on the company's website, which included materials headlined "EASY TO SECURE" and "ADVANCED NETWORK SECURITY." But despite the claims made by D-Link, the FTC alleged, the company failed to take steps to address well-known and easily preventable security flaws, such as:

- "hard-coded" login credentials integrated into D-Link camera software -- such as the username "guest" and the password "guest" -- that could allow unauthorized access to the cameras' live feed;
- a software flaw known as "command injection" that could enable remote attackers to take control of consumers' routers by sending them unauthorized commands over the Internet;
- the mishandling of a private key code used to sign into D-Link software, such that it was openly available on a public website for six months; and
- leaving users' login credentials for D-Link's mobile app unsecured in clear, readable text on their mobile devices, even though there is free software available to secure the information.

https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate

ADVICE FOR RESEARCHERS

- Continually practice communication of science.
- Be truthful and accurate. Substantiate claims.
- Keep marketing and technical staff in sync.
- Watch out for deceptive claims.
- Report deception.



WHO PAID?

Who conducted and/or paid for the work? Compared with evaluations or results that came from the vendor, independent analysis and results are less prone to seeking evidence that simply confirms a desired result.



WHAT WORDS?

What do the adverbs and adjectives mean? Statements that use subjective, imprecise words such as “significantly” or “substantially” might carry a different meaning or judgement than my own.



WHAT SAMPLE?

What was the size and composition of the data sample? I have low trust and confidence in results and claims based on representatively small sample sizes or selectively-chosen data points – both of which may over (or under) inflate the true claim.

DISAPPEARING SECURITY

- Continued state of poor security adoption and practice (devs and users)
- Ideally, build less vulnerable systems
- Despite active and valiant work at adoption and usability, many users cannot or will not avail themselves of many cyber security options
- Hands-off, behind-the-scenes cyber defense the new norm?
- Users seem to be accepting auto-updates


Q&A