RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: TV-T01

THE NEW GEOPOLITICS OF CYBERSECURITY RESEARCH

John Bambenek

Vice-President, Security Research and Intelligence
ThreatSTOP
@Bambenek / @ThreatSTOP

Where we have come from…

- RSA Attendance: 17,000 (2008) - ~45,000 (2018)
- Gmail/Facebook Created: 2004
- Twitter Created: 2006
- There were no APTs (until 2013 Mandiant APT1 report)
- Cybersecurity spending: $27.4B (2010) - $66B (2018)
- What's IoT?
- BOTTOM LINE: Just a few short years ago, we were a niche concern both for business and for government.

Where we have come from…

Ted Stevens' Tubes Statement

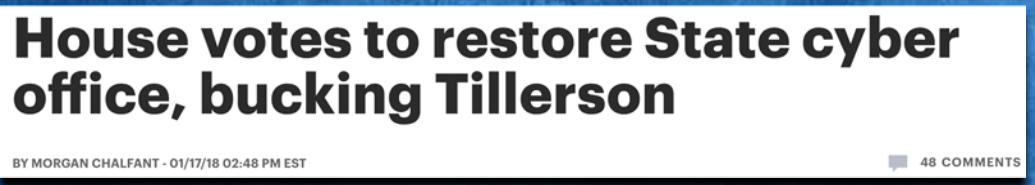
- "And again, the Internet is not something you just dump something on. It's not a big truck. It's a **series of tubes**. And if you don't understand those tubes can be filled and if they are filled, when you put your message in, it gets in line and it's going to be delayed by anyone that puts into that tube enormous amounts of material, enormous amounts of material. "

June 28, 2006

Series of Tubes Remix

From "Politics of Net Neutrality" - https://www.slideshare.net/hartjeff12/net-neutrality-28022490

Where we are today…


House votes to restore State cyber office, bucking Tillerson

BY MORGAN CHALFANT - 01/17/18 02:48 PM EST

48 COMMENTS


SUBSCRIBE | ABOUT | RSS

cyberscoop

SNG

VERNMENT | TRANSPORTATION | HEALTHCARE | TECHNOLOGY | FINANCIAL | WATCH | LISTEN | ATTEND | COMMUN

GOVERNMENT

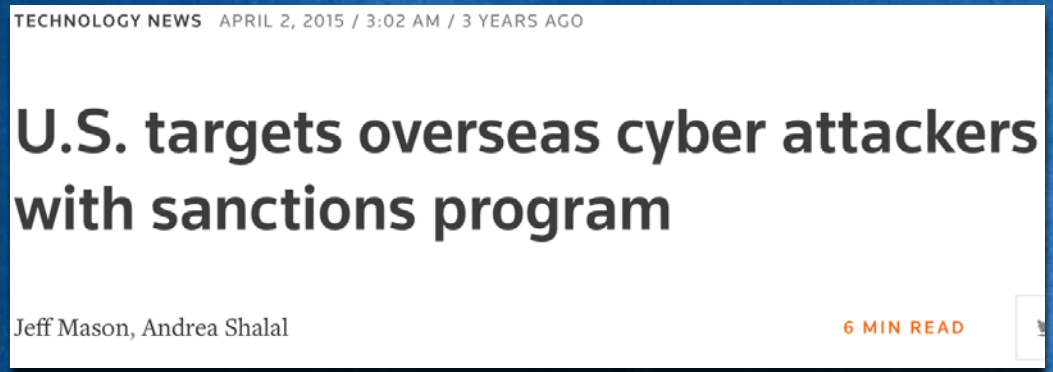
The Wassenaar Arrangement's latest language is making security researchers very happy


SECURITY

Trump: Cybersecurity is a national defense priority

In a strategy document, the White House calls for stronger defenses against hackers from criminal enterprises and places like Russia, China and Iran.

BY LAURA HAUTALA, ALFRED NG / DECEMBER 18, 2017 2:35 PM PST


TECHNOLOGY NEWS APRIL 2, 2015 / 3:02 AM / 3 YEARS AGO

U.S. targets overseas cyber attackers with sanctions program

Jeff Mason, Andrea Shalal

6 MIN READ


How to attract a board-level cybersecurity expert

By Stacy Collett

Contributing Writer, CSO | JUL 28, 2016 3:42 AM PT

Threat STOP

RSAConference2018

The “Big” Cases of the Last 24 Months

- 2016 Elections (and subsequent elections)
- WannaCry & NotPetya
- Olympic Destroyer

But it's come with costs…

- We are more visible than we have ever been (with more scrutiny).
  - CSOs are getting fired over breaches.
- In the political realm "politics is perception", we're in a fact free world.
- Much of what used to go on in private intel sharing lists now get leaked to press.

The SEC says companies must disclose more information about cybersecurity risks

Posted Feb 21, 2018 by Catherine Shu (@catherineshu)

Our mistakes are now more costly…

- A quick “not-well-thought-out” e-mail, could have outsized consequences for an organization…
  - And the individual…

FUTURE TENSE | THE CITIZEN'S GUIDE TO THE FUTURE. | DEC. 14 2016 4:54 PM

FROM SLATE, NEW AMERICA, AND ASU

“Is This Something That’s Going to Haunt Me the Rest of My Life?”

What it’s like to be the IT guy who accidentally helped Russia (maybe) hack the election.

By Will Oremus

The Many Flavors of Spies…

Official Cover

- Has a diplomatic posting, protecting by immunity.
- Can get PNG'd… with several days notice.
- Generally know who they are.

Non-Official Cover

- Could be anyone, operating in secret.
- Can be arrested, prosecuted, shot.
- Governments will still try to protect them (i.e. prisoner swaps).

The Many Flavors of Spies

Official Cover

Image source: ABC News

Non-Official Cover

Image source: bio.com

The Kaspersky Dilemma

POLITICS | NATIONAL SECURITY

Russia Has Turned Kaspersky Software Into Tool for Spying

Searches exploited popular Russian-made antivirus software to seek classified material, officials say

By *Shane Harris* and *Gordon Lubold*

Oct. 11, 2017 1:44 p.m. ET

- Like any AV, collects telemetry from install base.
- Accused of opportunistically searching for US classified materials.
- Various ties to RU government among employees, etc.
- Set off chain-reaction in industry to look at vendor telemetry.

Russia's Response

- We're still waiting to see what Russia is going to do about all this…

Russia Threatens Retaliation If Pentagon Bans Kaspersky Software

By **Stepan Kravchenko**

June 30, 2017, 11:23 AM CDT

But no US firm would do the same, right?

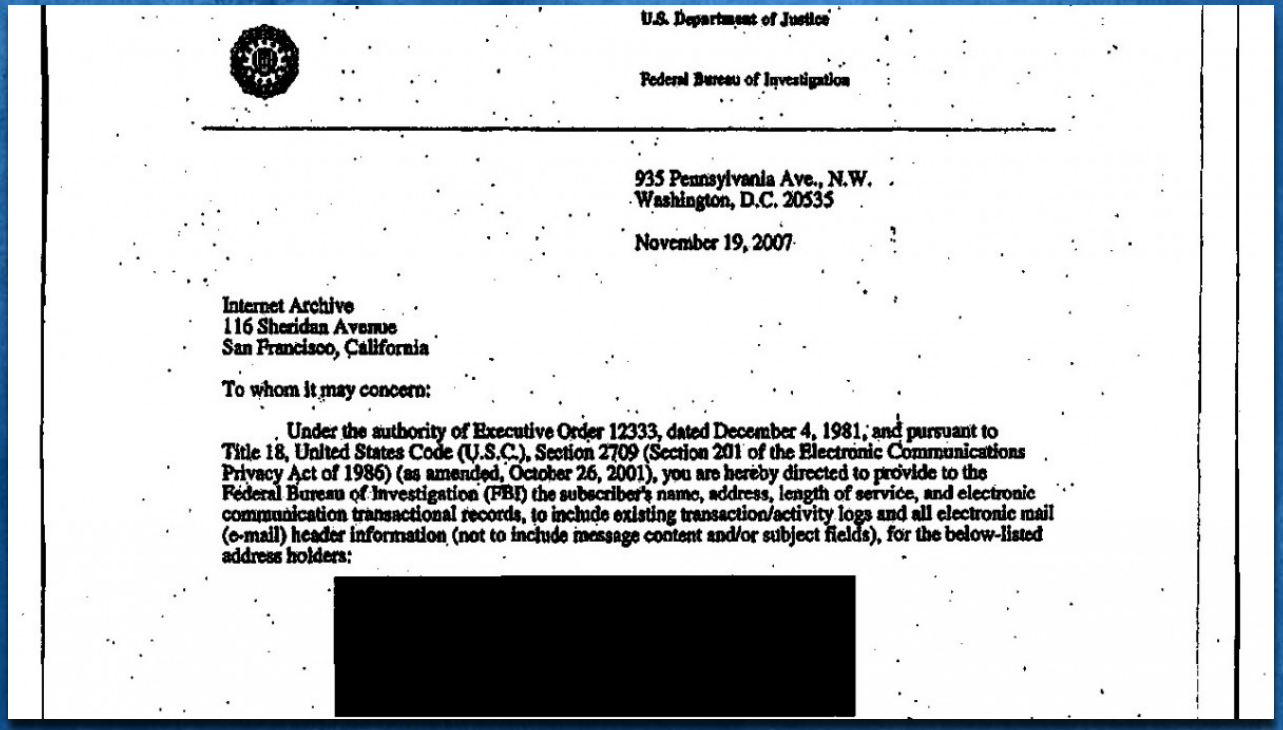
Things Kaspersky Does

- Collect telemetry from clients
- Share data with law enforcement
- Protect against APT threats
- Research new threats

Things US Cybersecurity Firms Do

- Collect telemetry from clients
- Share data with law enforcement
- Protect against APT threats
- Research new threats

But we don't necessarily give information to spy agencies… do we?



U.S. Department of Justice

Federal Bureau of Investigation

935 Pennsylvania Ave., N.W.
Washington, D.C. 20535

November 19, 2007

Internet Archive
116 Sheridan Avenue
San Francisco, California

To whom it may concern:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act of 1986) (as amended, October 26, 2001), you are hereby directed to provide to the Federal Bureau of Investigation (FBI) the subscriber's name, address, length of service, and electronic communication transactional records, to include existing transaction/activity logs and all electronic mail (e-mail) header information (not to include message content and/or subject fields), for the below-listed address holders:

[redacted]

Are honeypots the new SIGINT?

- We've come up with threat intelligence to apply traditional intelligence techniques to cybersecurity…
- We haven't considered what else bringing this has cost us.
  - Wassenaar for awhile contemplated making vulnerability info "weapons" and those researchers into "arms dealers".

CYBERSECURITY

John Bolton, cyber warrior

Trump's incoming adviser has said the U.S. should launch a 'retaliatory cyber campaign against Russia' and 'use WikiLeaks for target practice.'

By **CORY BENNETT** | 04/01/2018 07:00 AM EDT

A New Class of Spy…

- A new third class of spy: “no cover”
- What do our governments owe us if we get picked up because someone says we are spying?
  - A consular official will give you a list of lawyers and let your family know you may be a little late* coming home.
  - * (read as “a lot late”)
- What’s legal to one country may be a crime to another…

Aren’t you a little paranoid?

- It is doubtful the majority of people doing security research are going to be treated as spies by a foreign government.
  - But they certainly CAN (and have been) treated as valid intelligence targets.
- NSA’s TAO has all but said they target administrators and security professionals because they have “the keys to the kingdom”.

INSIDE THE NSA’S SECRET EFFORTS TO HUNT AND HACK SYSTEM ADMINISTRATORS

Ryan Gallagher, Peter Maass

March 20 2014, 4:07 p.m.

What to do about it?

- The more cybersecurity is a political issue, the more the rules of politics apply.
  - That means perception management.
- The more cybersecurity is a geopolitical issue, the more those rules apply.
  - We are subject to laws of almost every government on earth.
- What is your own personal risk appetite? (i.e. Are you willing to modify and limit travel?)
  - Sometimes, research may need to be left on table ifthe stakes are too high.

What to do about it?

- Most important… the job is getting more stressful
  - Take care of yourself.

From giphy:

THANK YOU!

jbambenek@threatstop.com / @bambenek