

# International Travel Vulnerabilities

Don Vilfer, JD

Digital Evidence Ventures



### Digital Evidence Ventures



**Who we are**: Reformed lawyers, former FBI Agents, assisted by young Brainiacs.

**What we do**: Computer Forensics, Cell Phone Forensics, Research Misconduct Investigations, Fraud Investigations and yes, International Travel.



## Class Objectives

- Understand the threat landscape of international travel with data.
- Understand the limitations of some solutions.
- Create an awareness of a variety of solutions.

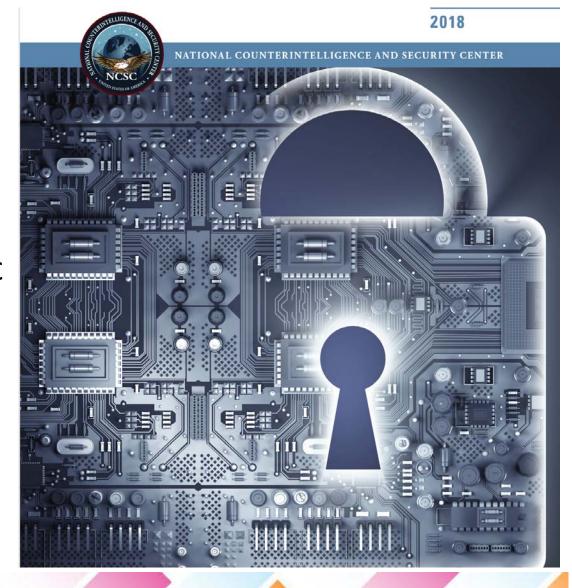
### Threats to Your Data

- Foreign Agents
- Thieves
- Hackers
- US Customs

# Foreign Agents

#### **Top Countries:**

- China (90% of all Economic Espionage)
- Russia
- Iran





202	Non-Traditional Collectors	China uses individuals for whom science or business is their primary profession to target and
	Non-maditional conectors	acquire US technology.
80	Joint Ventures (JV)	China uses JVs to acquire technology and technical know-how.
	Research partnerships	China actively seeks partnerships with government laboratories-such as the Department of Energy labs-to learn about and acquire specific technology, and the soft skills necessary to run such facilities
1	Academic Collaborations	China uses collaborations and relationships with universities to acquire specific research and gain access to high-end research equipment. Its policies state it should exploit the openness of academia to fill China's strategic gaps.
	S&T Investments	China has sustained, long-term state investments in its S&T infrastructure.
<b>₩</b>	M&A	China seeks to buy companies that have technology, facilities and people. These sometimes end up as Committee on Foreign Investment in the United States (CFIUS) cases.
凲	Front Companies	China uses front companies to obscure the hand of the Chinese government and acquire expor- controlled technology.
	Talent Recruitment Programs	China uses its talent recruitment programs to find foreign experts to return to China and work on key strategic programs.
☆	Intelligence Services	The Ministry of State Security (MSS), and military intelligence offices are used in China's technology acquisition efforts.
-0	Legal and Regulatory Environment	China uses its laws and regulations to disadvantage foreign companies and advantage its own companies.



While honored to attend...

Dear Dr. Angelica Kokkalis,

As you know we are planning to have a translational medicine conference in Hangzhou on September 19th, 2015. It is my honor to invite you as one of the speakers in the plenary session of the conference. It will be great If you can discuss the application of Han's acupoint nerve stimulator in the US.

Please let me know if you have any questions. I can be reached at (86)189699

Looking forward to hearing from you.

Sincerely yours,

Zengyu Zhang, M.D.

The organizing committee

First People's Hospital of Xiaoshan

Hangzhou, Zhejiang Province

Peoples Republic of China







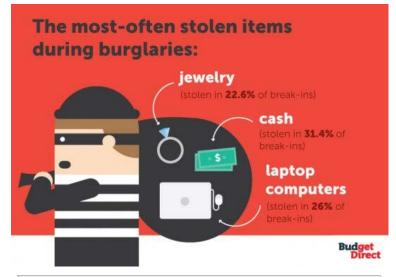


global sources

Ethics, Compliance & Audit Symposium **REACHING NEW HEIGHTS** 

# Thieves

- A laptop computer has a 1-in-10 chance of being stolen.
- A laptop is stolen every 53 seconds
- 86% of IT practitioners report that someone in their organization has had a laptop lost or stolen
  - 56% reported that this resulted in data breach
- 52% of business managers leave their laptop with a stranger when travelling
- 45% of healthcare information breaches occur on stolen laptops
- The average total cost to a business from a single laptop loss is US \$47,000





#### Hackers

#### How They Do It:

- Free Wi-Fi
- "Security Updates"
- Agent Push
- Malware
- Physical Access while away



### Hackers

	dit <u>V</u> iew <u>G</u> o	<u>C</u> apture <u>A</u> nalyze	Statistics Telephony Tools	Internals Help	lp
0 0			0、 4 4 4 7 2		૨ ੨ • • • • • • • • • • • • • • • • • •
Filter:				Expression.	n Clear Apply Save
Vo.	Time	Source	Destination	Protocol	Length Info
	62 13.6322330	8.26.65.101	192.168.1.106	HTTP	455 HTTP/1.1 200 OK (application/json)
	53 13.8317800	192.168.1.106	8.26.65.101	TCP	54 51136-80 [ACK] Seq=1089 Ack=402 Win=255356 Len=0
	64 14.1190520	192.168.1.100	255.255.255.255	UDP	82 Source port: 49157 Destination port: 1947
		192.168.1.158		NBNS	92 Name query NB STUDY<20>
			rver-3Broadcast	ARP	60 Who has 192.168.1.18? Tell 192.168.1.10
		192.168.1.135		UDP	82 Source port: 64429 Destination port: 1947
		192.168.1.158		NBNS	92 Name query NB STUDY<20>
		192.168.1.106		TCP	55 [TCP Keep-Alive] 50977-80 [ACK] Seg=1 Ack=1 Win=16271 Len=1
		74.121.136.13		TCP	66 [TCP Keep-Alive ACK] 80+50977 [ACK] Seq=1 Ack=2 win=33 Len=0 SLE=1 SRE=2
		Apple_9e:61:e		ARP	60 Who has 192.168.1.115? Tell 192.168.1.158
		Apple_9e:61:e		ARP	60 Who has 192.168.1.28? Tell 192.168.1.158
		Apple_9e:61:e		ARP	60 Who has 192.168.1.137? Tell 192.168.1.158
		192.168.1.106 74.121.136.13		TCP	55 [TCP Keep-Alive] 50976+80 [ACK] Seg=1 Ack=1 Win=16114 Len=1 66 [TCP Keep-Alive ACK] 80+50976 [ACK] Seg=1 Ack=2 Win=36 Len=0 SLE=1 SRE=2
				TCP	
		ces on wire (f	his hits) 87 hytes ca	ntured (656	
⊕ Fra					66 bits) on interface 0
⊕ Fra	mernet II, Sr	c: Pegatron_5f	f:d8:d7 (e8:40:f2:5f:d	18:d7), Dst:	: Broadcast (ff:ff:ff:ff:ff)
⊕ Fra ⊕ Eth ⊕ Int	ernet II, Sre	c: Pegatron_5f ol Version 4,	f:d8:d7 (e8:40:f2:5f:d Src: 192.168.1.135 (1	8:d7), Dst:	: Broadcast (ff:ff:ff:ff:ff) 35), Dst: 192.168.1.255 (192.168.1.255)
Fra Eth Int	ernet II, Sr ernet Protoco er Datagram Pr	c: Pegatron_5f ol Version 4,	f:d8:d7 (e8:40:f2:5f:d	8:d7), Dst:	: Broadcast (ff:ff:ff:ff:ff) 35), Dst: 192.168.1.255 (192.168.1.255)
⊕ Fra ⊕ Eth ⊕ Int ⊕ Use ⊕ Dat	ernet II, Sro ernet Protoco er Datagram Pr a (40 bytes)	c: Pegatron_5f ol Version 4, rotocol, Src F	f:d8:d7 (e8:40:f2:5f:d Src: 192.168.1.135 (1 Port: 64429 (64429), D	8:d7), Dst: 92.168.1.1 st Port: 19	: Broadcast (ff:ff:ff:ff:ff) 35), Dst: 192.168.1.255 (192.168.1.255)
⊕ Fra ⊕ Eth ⊕ Int ⊕ Use □ Dat	ernet II, Sro ernet Protoco er Datagram Pr a (40 bytes)	c: Pegatron_5f ol Version 4, rotocol, Src F	f:d8:d7 (e8:40:f2:5f:d Src: 192.168.1.135 (1	8:d7), Dst: 92.168.1.1 st Port: 19	: Broadcast (ff:ff:ff:ff:ff) 35), Dst: 192.168.1.255 (192.168.1.255)
Fra Eth Int Use Dat	ernet II, Sreernet Protoce er Datagram Pr a (40 bytes) Data: 69506d4	c: Pegatron_5f ol Version 4, rotocol, Src F	f:d8:d7 (e8:40:f2:5f:d Src: 192.168.1.135 (1 Port: 64429 (64429), D	8:d7), Dst: 92.168.1.1 st Port: 19	: Broadcast (ff:ff:ff:ff:ff) 35), Dst: 192.168.1.255 (192.168.1.255)

0020

0060

UNIVERSITY Ethics, Compliance & Audit

Symposium
REACHING NEW HEIGHTS

26 49 20 19 6d 61 77 61 79 61 74 61 63 6f 6e 66 65 72 65 6e 63 65 6f 6e 63 79 62 65 72 73 65 63 75 72 69 74 79 2e 46 6f 75 6e 64 61 77 69 72 65 6c 65 73 73 63 6f 6e 65 63 74 69 6f 6e 69 6e 62 65 74 77 65 65 6e 63 6c 61 73 73 65 73 2c 73

erence on cyber s urity. Found a wi less connection i between classes,

#### **US Customs**

- Border searches not subject to Fourth Amendment protection.
- 2018 US Customs policy allows agents to continue to inspect information that's stored on a device. But they can't copy that information or connect to an external device to analyze the contents, unless they have *reasonable suspicion* of criminal behavior.
- Contraband and how they search for it.
- Controlled information or scientific equipment subject to Export Administration Regulations or Intl Traffic in Arms Regulations.
- A word about other borders...

#### Limitations of Solutions

- Encryption
- Using the Cloud
- USB drives

#### More Effective Solutions

- Take a Clean Laptop/Phone
- Do Not Work
- Contact your export control officer before going
- Auditors can raise awareness and ask about a "Clean Laptop Program"

### **Campus Contacts**

- ANR Kathleen Nolan knolan@ucanr.edu
- LBNL Shilpani Perera <u>sperera@lbl.gov</u>
- UCB Alaisha M. Hellman <u>amhellman@berkeley.edu</u>
- UCD Craig Allison <a href="mailto:ccallison@ucdavis.edu">ccallison@ucdavis.edu</a>
- UCI Amy Green <u>acgreen1@uci.edu</u>
- UCLA Ann Pham ann.pham@research.ucla.edu
- UCM Deb Motton <u>dmotton@ucmerced.edu</u>
- UCR Charles Greer, Jr <u>charles.greer@ucr.edu</u>
- UCSB Brian McCurdy <u>exportcontrol@research.ucsb.edu</u>
- UCSC Lisa Coscarelli <u>lcoscare@ucsc.edu</u>
- UCSD Brittany Whiting <u>brwhiting@ucsd.edu</u>
- UCSF Joan Doherty <u>Joan.Doherty@ucsf.edu</u>
- UCOP Marci Copeland <u>marci.copeland@ucop.edu</u>

#### Resources

#### **Export Control Officers**

https://www.ucop.edu/ethics-compliance-audit-services/compliance/international-compliance/campus-contacts.html

#### CISO's

https://www.ucop.edu/information-technology-services/initiatives/uc-ciso-committee/members-and-staff.html



#### Questions?

Don Vilfer, JD

Digital Evidence Ventures

1013 Galleria Blvd., suite 280
Roseville, CA 95678

916-883-2020



don@DigitalEvidenceVentures.com

