



CONFRONTING THE CYBER THREAT

David J. Hickton
Founding Director
University of Pittsburgh Institute for Cyber
Law, Policy, and Security

SAC-PA Workshop
Pittsburgh, Pennsylvania
June 22, 2017

Chinese Economic Espionage



First time the United States has leveled cyber espionage charges against the military of a foreign country

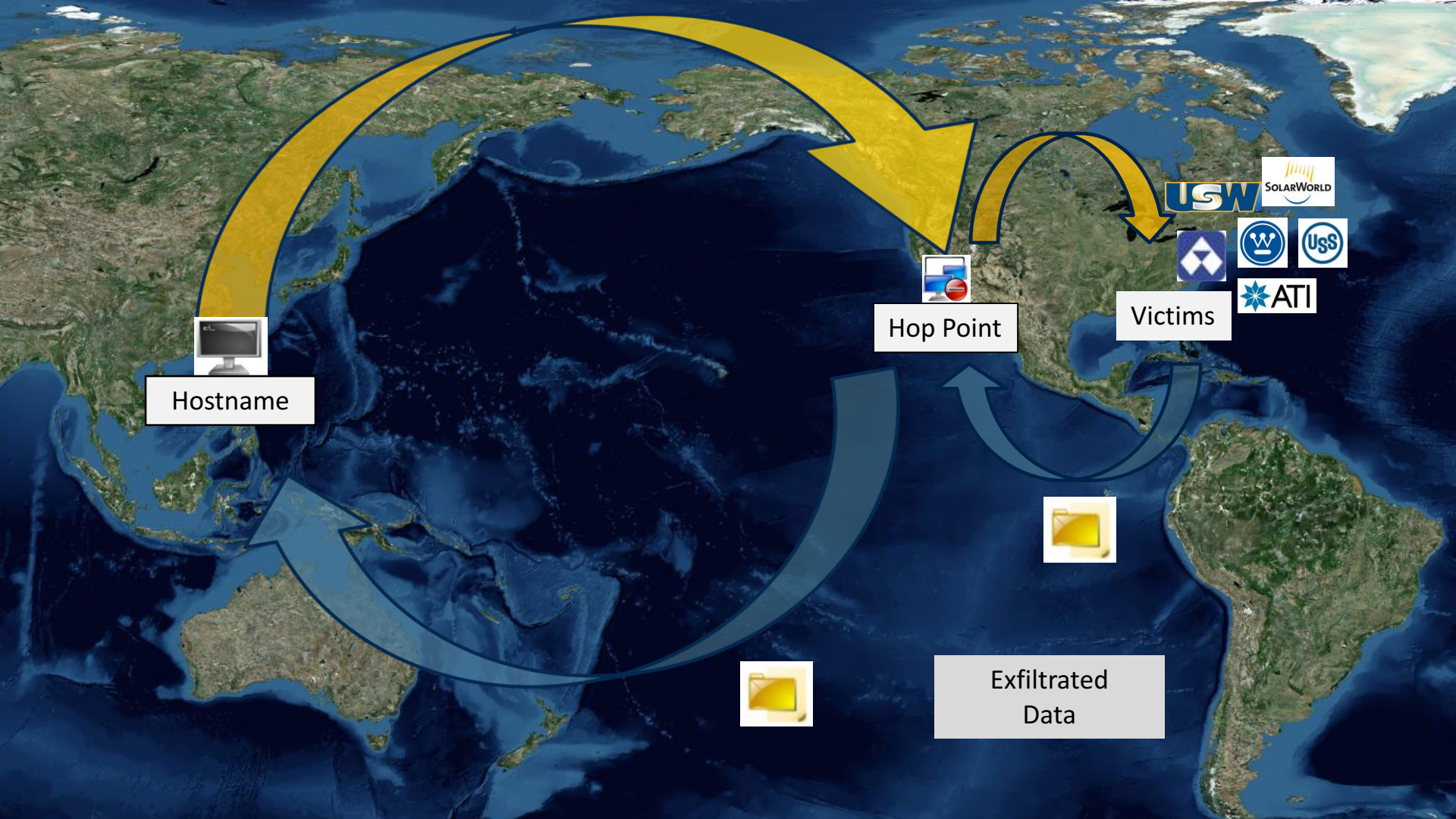


31-count indictment charges five members of Chinese military with theft of technological secrets and communications

Wang Dong **Gu Chunhui** **Huang Zhenyu**



Sun Kailiang **Wen Xinyu**



Chinese Economic Espionage



PLA Unit 61398

Employs hundreds, perhaps thousands of personnel

Requires personnel trained in computer security and computer network operations

Requires personnel proficient in the English language

Has large-scale infrastructure and facilities in the “Pudong New Area” of Shanghai

Chinese Economic Espionage

What Did They Steal?



Credentials

Intellectual property

Strategic plans

Cost and price data

Trade case

GameOver Zeus/Cryptolocker

GameOver Zeus Malware

One million infected computers worldwide;
25% in the United States

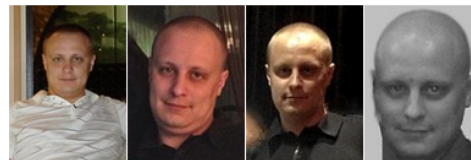
\$100M+ wire transferred from compromised
computers to cyber criminals overseas

Haysite Reinforced Plastics in Erie, Penn. bilked
of \$375K in October 2011

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

**EVGENIY MIKHAILOVICH
BOGACHEV**



Darkode

Global Cybercrime Marketplace

Largest, most sophisticated English-language forum

Buy, sell, trade, share cybercrime products

Malware, botnets, passwords, Facebook Spreader, Dendroid

WELCOME TO DARKODE
"International marketplace for selling machines and other legal stuff"

Profile • Private Messages • Search • FAQ • Memberlist • Usergroups • Log out

You last visited: [redacted]
The time now is: [redacted]
[review/darkode Forum Index](#)

View posts since last visit
View your profile
View unanswered posts

UNVERIFIED (LEVEL -3)

Forum	Topics	Posts	Last Post
Introductions Introduce yourself!	131	1025	Fri Feb 20, 2015 9:48 pm
Suspended Suspended people Moderator	54	562	Thu Jan 22, 2015 5:14 pm
Approved People that have been approved will have their threads moved here	169	1793	Wed Jan 14, 2015 9:18 am

HALL OF SHAME / FAME

Forum	Topics	Posts	Last Post
Verified Report successful business here. Moderator	210	1206	Sun Jan 18, 2015 1:15 pm
Reviews - HIDDEN SECTION - Moderator	38	363	Sun Oct 12, 2014 8:38 am
Scammers List of known scammers. Report scammers here. Moderator	199	3071	Sat Feb 14, 2015 3:45 pm
Seller reports Sellers report if they will be inactive, to avoid confused customers Moderator	54	201	Wed Jan 07, 2015 5:24 pm

MARKETPLACE (LEVEL 0)

Forum	Topics	Posts	Last Post
Services Hosting, crypting, traffic, ...	33	248	Fri Feb 20, 2015 8:44 am
BUY / SELL / TRADE - HIDDEN SECTION - Moderator	1261	4751	Tue Nov 18, 2014 7:14 pm
Buy Sources, binaries, installs, ...	56	140	Sun Feb 22, 2015 12:48 am
Sell Sources, binaries, installs, ...	86	251	Sat Feb 21, 2015 6:45 pm
Trade Sources, binaries, installs, ...	10	16	Sat Feb 21, 2015 6:57 pm

Darkode



Operation SHROUDED HORIZON



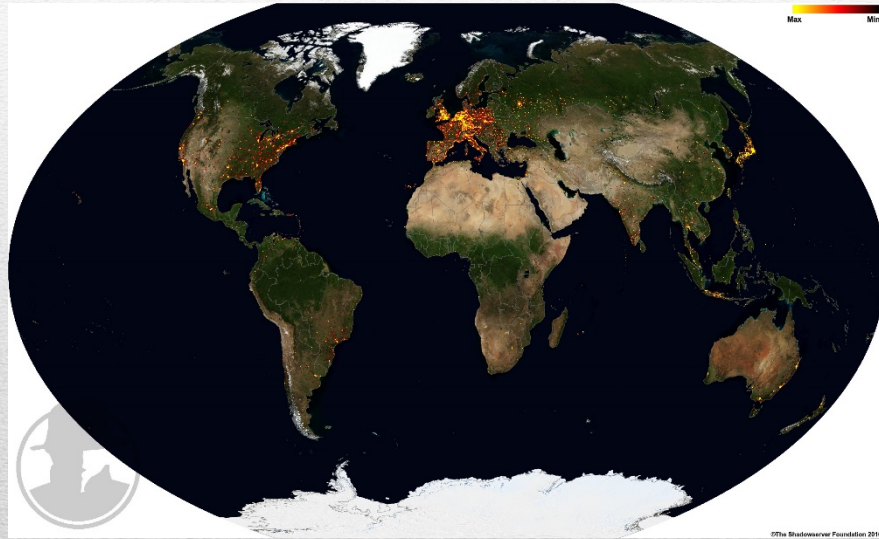
Multi-year investigation, infiltrated forum at high level

Seized domain

70 members and associates searched or arrested globally

U.S. charges 12 criminally in U.S., Sweden, Pakistan, Spain and Slovenia

Avalanche Network



Delivery platform to launch and manage mass global attacks and money mule recruiting campaigns

Infected computers in 189 countries


Monetary losses: hundreds of millions

Five individuals arrested; 37 premises searched; 39 servers seized worldwide

Challenges of Cybercrime Fighting



Opportunities of Cybercrime Fighting



Forge relationships with the private sector that are appropriate, lawful and effective

Improve reporting of cyber intrusions

Centralize intelligence and sharing regarding cyber intrusions

Opportunities of Cybercrime Fighting



Enhance development and distribution of cyber intelligence products to private sector and across government

Increase and expedite international cooperation

Improve victim outreach and cooperation



Discussion and Questions
