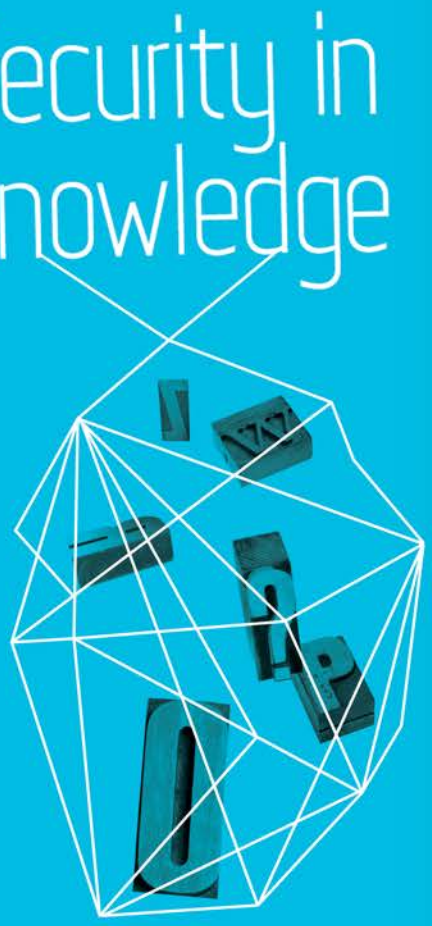
Trojan Horse: The Widespread Use of International Cyber-Espionage as a Weapon



Mark Russinovich
Author of Zero Day and Trojan Horse

Session ID: EXP-R35
Session Classification: Intermediate

- "Today, U.S. officials indicate that more than 20 countries have various kinds of information operations (IO) directed against the United States."
- "Computer systems at the Pentagon and other military sites get "attacked" thousands of times each year."

Order Code RL30735

CRS Report for Congress

Received through the CRS Web

Cyberwarfare

Updated June 19, 2001

Steven A. Hildreth
Specialist in National Defense
Foreign Affairs, Defense, & Trade Division

Agenda

- Defining terms
- A brief history
- Anatomy of cyberespionage
- Implications and nation-state policy
- What should you do?

Defining Terms

	Only State Actors	Information gathering or theft of intellectual property	Undermines function of computer network	Political or national security purpose	Equivalent of armed attack or in context of armed conflict
Cyberespionage		X			
Cyberattack			X	X	
Cyberwarfare	X		X	X	X

Computer Network Attack (CNA)
Computer Network Exploitation (CNE)

Offensive Cyber Operations (OCO)
Defensive Cyber Operations (DCO)

The Why

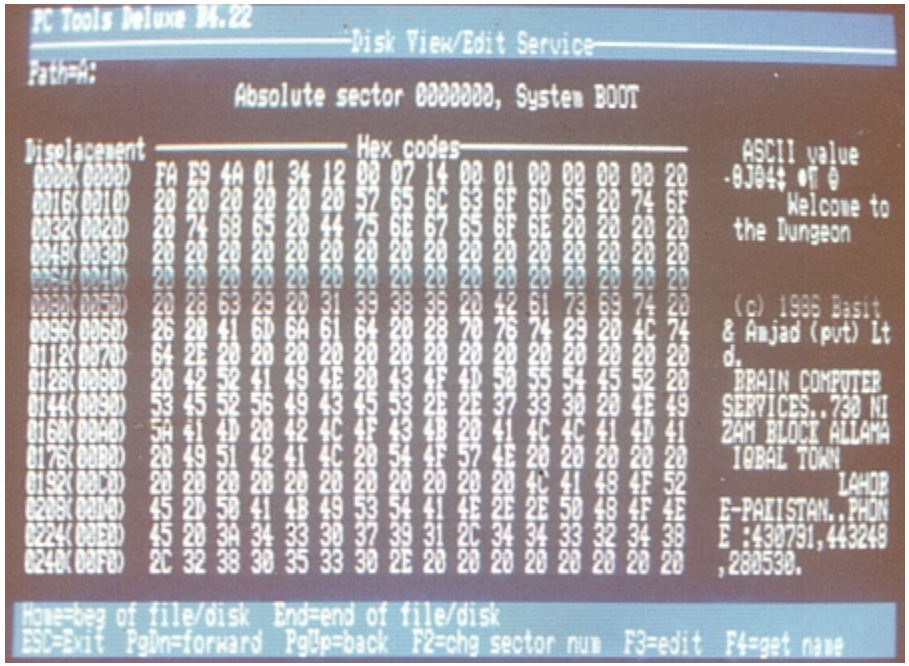
Reasons for states to maintain and utilize an aggressive cyber capability:

1. To deter other states by infiltrating their critical infrastructure
2. To gain increased knowledge through espionage in cyberspace, which makes it possible for states to advance more quickly in their military development
3. To make economic gains where technological progress has been achieved—for example, through industrial espionage
4. To be able to attack and paralyze an adversary's military capacity or the adversary's ability to control its own forces in a conflict

A Brief History

A Brief History: The 1980's

- The potential for cyberespionage and cyberattacks was demonstrated by malware and accidental attacks as early as the 1980's

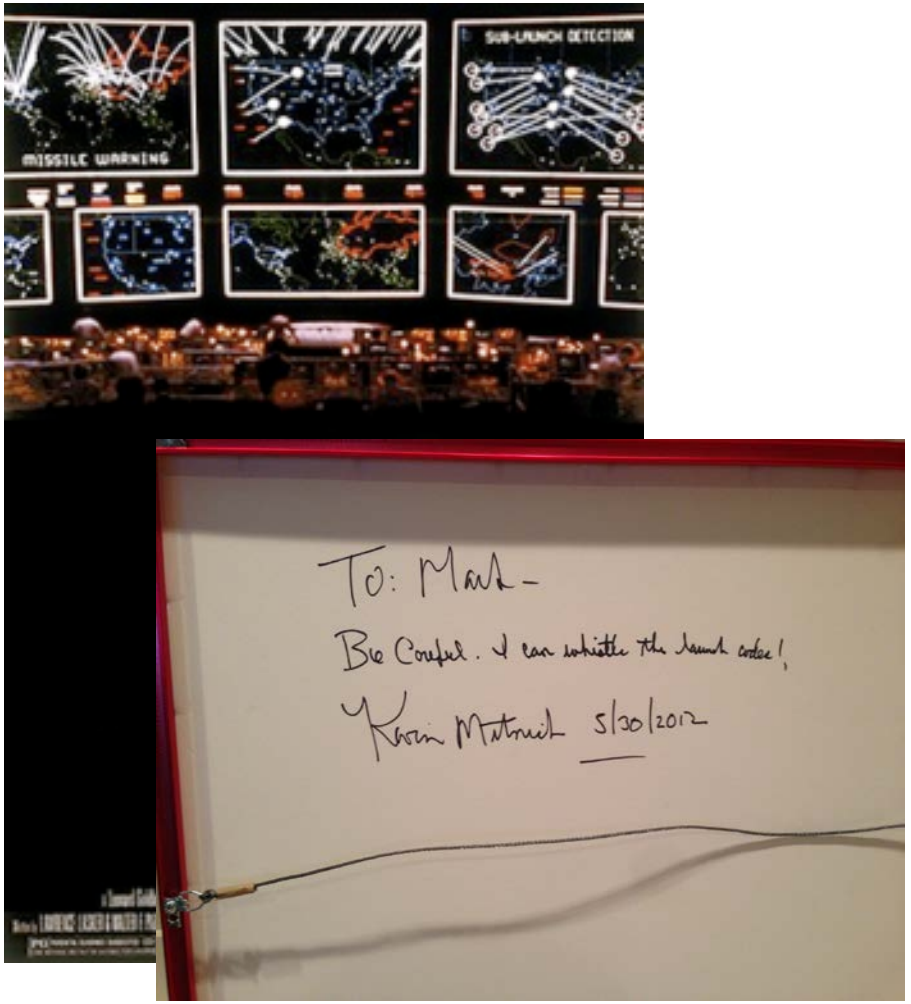


1984: Brain, the 1st PC virus

1988: Robert Morris, author of the Morris Worm

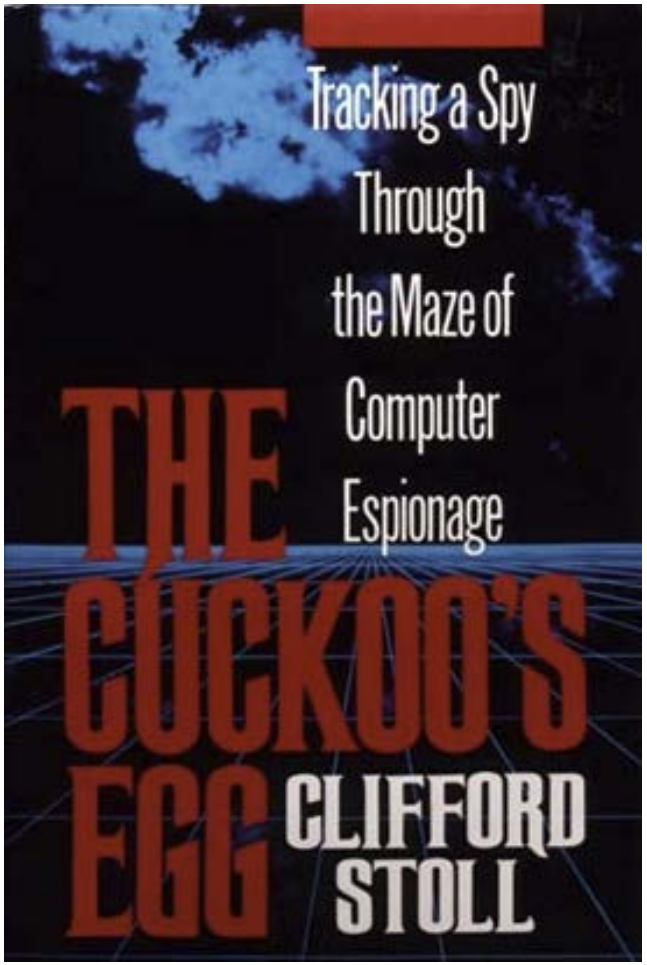
1983: War Games

- Actually, War Games introduced the public to cyberwarfare even earlier
- Showed most extreme scenario



1986: The Cuckoo's Egg

- Cliff Stoll's account of hunting a cyberspy: first documented case of cyberespionage
- Reads like a thriller
- Results in capture of German citizen selling US intelligence to the KGB



1997: Eligible Receiver

- Nation-state recognition of Cyberspace: first US cyberwarfare exercise
- 90-day operation, 35-person Red Team representing rogue state attacked US power and communication infrastructure systems
- Result: classified

> *"[Eligible Receiver] clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure."*
>
> -- Kenneth Bacon, Pentagon spokesman

- Led to formation of Joint Task Force Computer Defense

1998: Moonlight Maze

- US discovers cyber penetration of Pentagon, NASA, and US Department of Energy
- Thousands of documents exfiltrated:
  - Troop movements
  - Military hardware
  - Base maps
- DOD traces connections to Russian mainframes

2003-2005: Titan Rain

- Shawn Carpenter, analyst at Lockheed Martin and later Sandia National Labs, discovered breach and data exfiltration
- FBI and Army cyber-intelligence investigated
- Traced to servers in China
- Result: Classified
  (but Carpenter fired)

2007: Estonia

2008: South Ossetia War

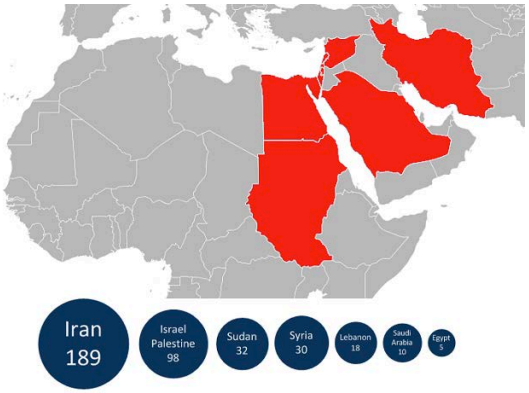
- Estonia decides to move Bronze Soldier of Tallinn
  - The Nashi, Pro-Kremlin youth group, launch DDOS attack on Estonian government servers
- Three days before Georgia invaded South Ossetia, Alania TV hacked
  - Followed by DDOS of Georgian and Azerbaijani web sites
  - Russian GRU and FSB implicated

2006-Now: Recent China

- 2006-2011 Shady Rat
  - Penetration of 72 corporations and government organizations
- 2009-2011 Night Dragon
  - Exfiltration of energy company information
- 2009-2010 Operation Aurora
  - Penetration to modify source code of Google, Adobe, Juniper Systems, Rackspace and others
- 200?-2009 GhostNet
  - Penetration of political, economic and media targets in 103 countries
- 2012 NY Times, Wall Street Journal, Washington Post
  - Penetration of media covering corrupt communist party leader

2005-2012: Operation Olympic Games

- 2005-2010: Stuxnet
  - First known cyber-kinetic attack
  - US cyberattack on Iranian nuclear enrichment
- 2009-2012: Flame
  - Complex, multi-component cyberespionage malware aimed at Iran
- 2009-2012: Gauss
  - Similar to Stuxnet, cyber espionage focused



2012: Shamoon

- First known "mass wipe" cyberattack
- Flattened 30,000 Saudi Aramco desktops
- Believed to be Iran

BBC News Sport Weather Travel Future

NEWS TECHNOLOGY

Home | US & Canada | Latin America | UK | Africa | Asia | Europe | Mid-East | Business | Health | Sci/Environment

27 August 2012 Last updated at 07:47 ET

Share

Saudi Aramco oil giant recovers from virus attack

About 30,000 workstation computers are back online at Saudi Aramco after a virus hit the world's largest oil producer.

Remote access was still restricted "as a precaution" the group said.

Oil production was not affected by the virus which struck on 15 August, Saudi Aramco added.

The company took its website offline after the attack and now carries a message on its front page apologising for any inconvenience.

Saudi Aramco says oil production was not disrupted by the virus attack

Related Stories

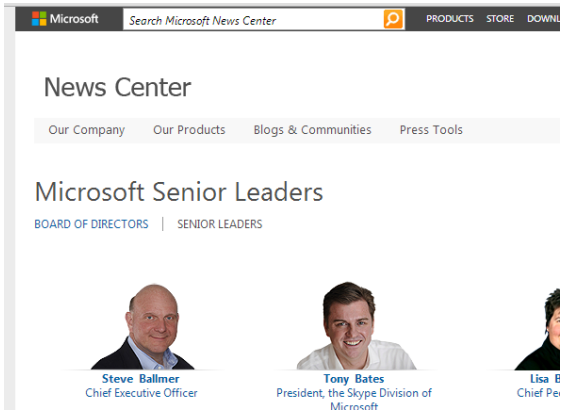
Anatomy of Cyberespionage

Phase1: Research

- Target is analyzed and scoped to identify candidate infiltration vectors
- Human Intelligence:
  - Social media, conferences, company directories, public records
- Network intelligence:
  - Public web site mapping
  - Server scanning and fingerprinting

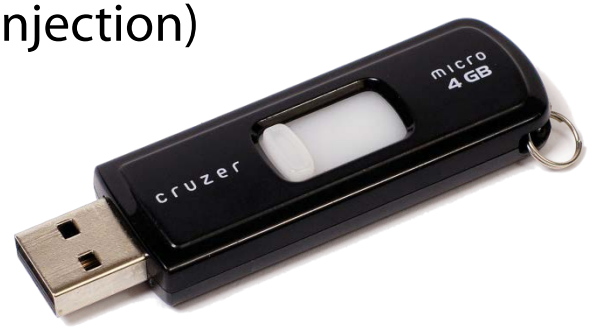
facebook

LinkedIn



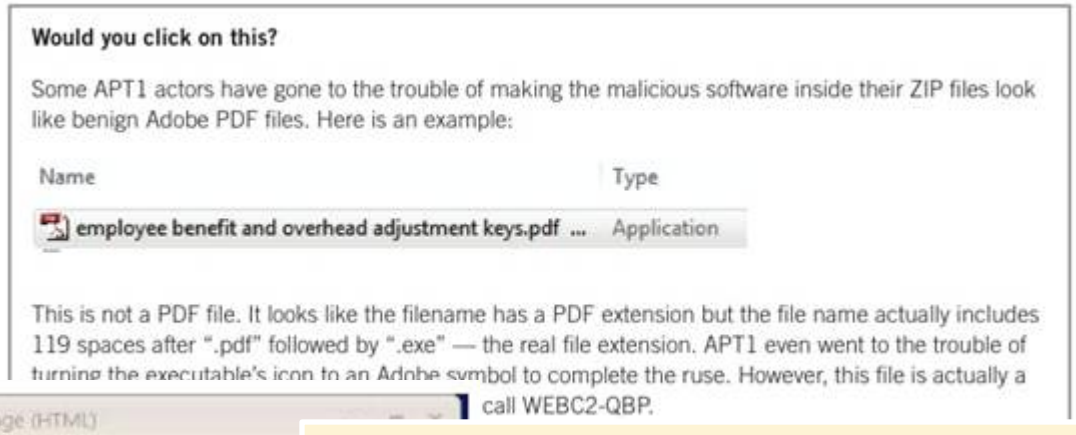
Phase 2: Infiltration

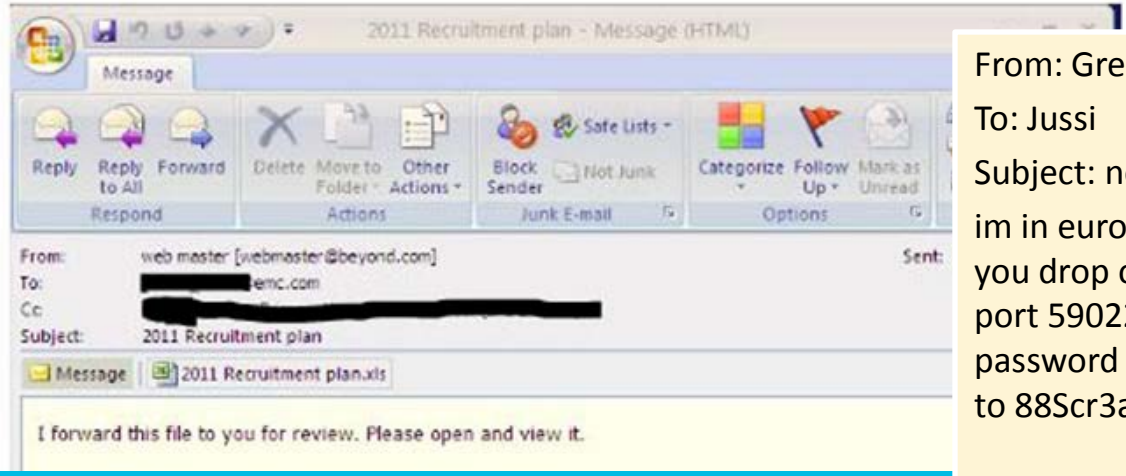
- Common vectors:
  - Application logic vulnerability (e.g. SQL injection)
  - Zero-day/unpatched vuln exploit
  - USB key
  - Insiders
  - Physical access
  - Interactive social engineering
  - “Spear Phishing”
- Goal: get backdoor malware into the target network



Spear Phishing

- The most common entry vector
- Incredibly effective, even after security training





From: Greg

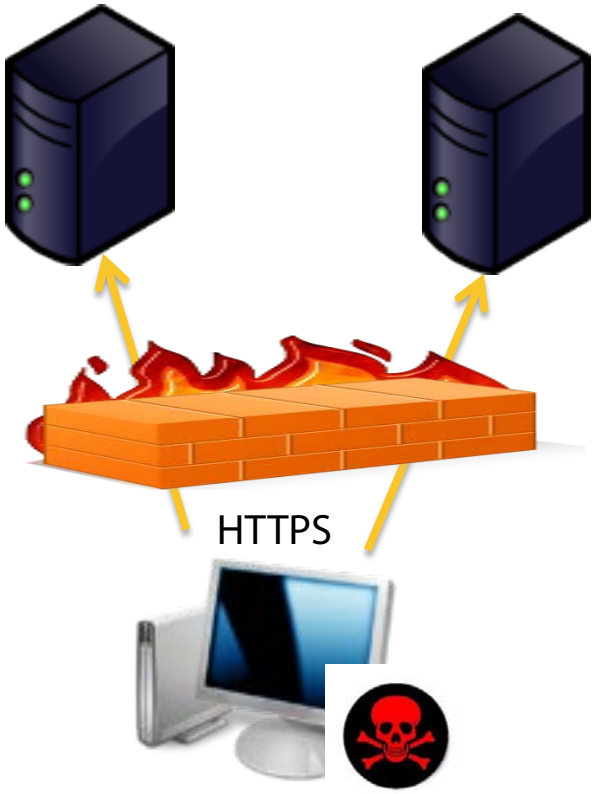
To: Jussi

Subject: need to ssh into rootkit

im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague? and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ? thanks

Phase 3: Beaconing

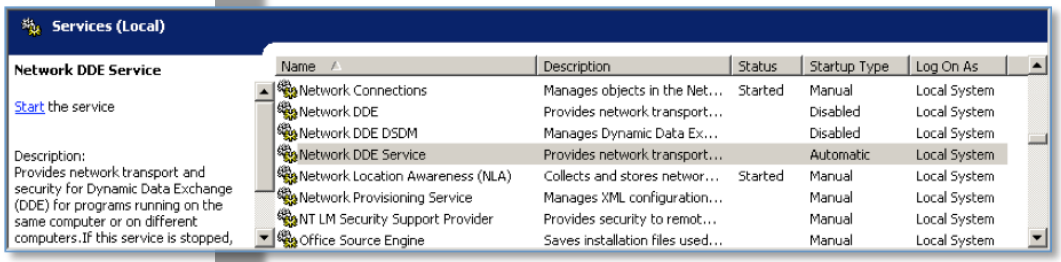
- Once inside a network, malware "beacons" out to a Command and Control (C2) server
  - C2 servers are either compromised or rented
  - Traffic is HTTP or HTTPS and can mimic common protocols
- Operator can use backdoor to inspect host and network



Backdoors

- Commonly implemented as Windows service
- Usually “hide in plain sight”
- Implement simple command set

Filename	netddesrv.exe
File size	73216 bytes
Version metadata	Child Type: StringFileInfo Language/Code Page: 1033/1200 Comments: CompanyName: FileDescription: NetDDESrv FileVersion: 1, 0, 0, 1 InternalName: NetDDESrv LegalCopyright: Copyright ? 2012 LegalTrademarks: OriginalFilename: **msrv.exe** PrivateBuild: ProductName: NetDDESrv ProductVersion: 1, 0, 0, 1 SpecialBuild: Child Type: VarFileInfo Translation: 1033/1200



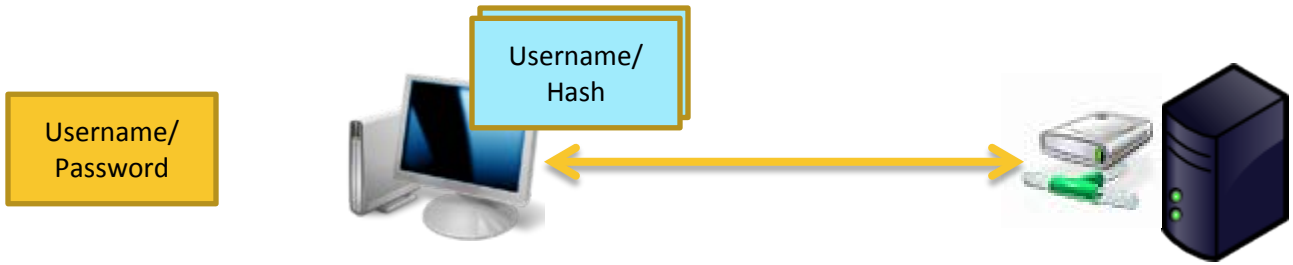
Example from Bit9 breach report

Phase 4: Spreading

- Operator performs internal reconnaissance:
  - Inventory of infected host files
  - Analysis and monitoring of host user activity
  - Dump of Intranet sites
  - Scan of connected systems
- Then moves laterally and attempts to escalate privilege
  - Password logging
  - Pass-the-hash

Pass-the-Hash (PtH)

- "Hash" refers to a cached credential
  - Usually not the "cleartext" credential
  - Hash is treated as the actual credential internally by most systems
  - Can be stored in memory or persisted on disk
- Most operating systems cache credentials for single sign on (SSO)

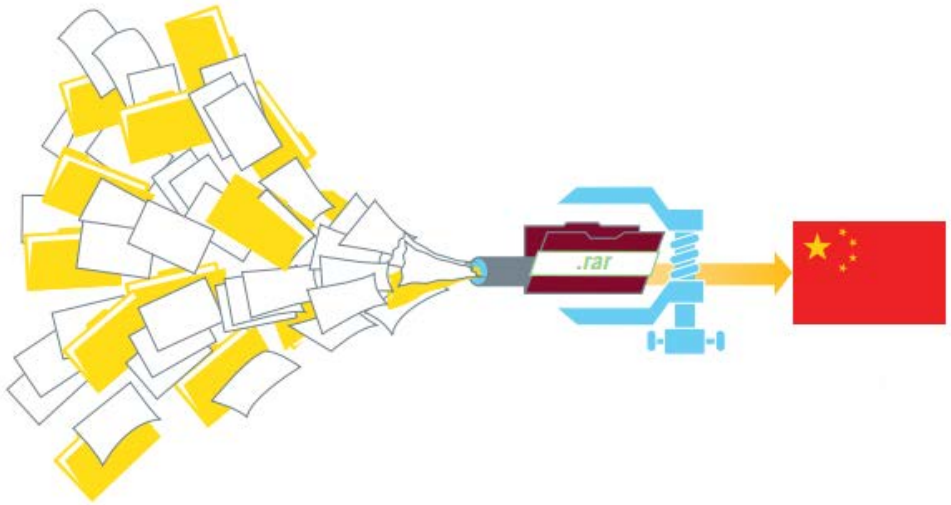


PtH Attacks

- Attacker gains local admin access to initial system
- Then use hashes to move "laterally" through the network
- They pick up additional hashes as they go
  - New hashes give them access to additional systems
  - If they come across a network/domain privileged account: Game Over

Phase 5: Exfiltration/Battlefield Preparation

- Identifies targeted assets and exfiltrates
- Positions itself for persistent presence
  - Remains resident on only a selection of systems
  - Maintains hold of key high-privilege accounts



Graphic from Mandiant APT1 Report

Implications

Chinese Cyberstrategy

- Civilian cyberespionage key to Chinese technological ascendency
- Computer Network Attack (CNA) is a cornerstone of military deterrence
- Blur military and civilian operations for plausible deniability
- Publically condemn cyberespionage and ask for cooperation

"Critical U.S. infrastructure is vulnerable to malicious cyber activity. Chinese military doctrine calls for exploiting these vulnerabilities in the case of a conflict."

The U.S.–China Economic and Security Review Commission 2009

US Cyberstrategy

- Develop offensive and defensive capability as the "fifth domain"
- Use civilian means to deter cyberespionage
  - Deterrence by denial: raise cost and minimize reward
  - Deterrence by interdependence: emphasize global economy
  - Deterrence by association: encourage disclosure to shape normative behavior

US Cyberoperations

USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

The DHS National Cyber Security Division (NCSD) is responsible for the response system, risk management program, and requirements for cyber-security in the U.S. The division is home to US-CERT operations and the National Cyber Alert System.

Protect the United States against cyber-based attacks and high-technology crimes.

US Policy for Protection of Trade Secrets

1. Focus Diplomatic Efforts to Protect Trade Secrets Overseas

"Where every nation plays by the rules…and intellectual property

2. Promote Voluntary Best Practices by Private Industry to Protect Trade Secrets

"In Americ

3. Enhance Domestic Law Enforcement Operations

"Our workers are the most productive on Earth, and if the playing field is level,

4. Improve Domestic Legislation

"Congress should make sure that no foreign company has an advantage over American manufacturing."

5. Public Awareness and Stakeholder Outreach

"What we can do—what America does better than anyone—is spark the creativity and imagination of our people."

—President Barack Obama

ADMINISTRATION ST
ON MITIGATING
THEFT OF U.S. TRADE SECRETS

Department of Defense Strategy for Operating in Cyberspace

Strategic Initiative 1: DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.

"Altho
as the

Strategic Initiative 2: DoD will employ new defense operating concepts to protect DoD networks and systems.

"Defe
netwo

Strategic Initiative 3: DoD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.

"T
al

Strategic Initiative 4: DoD will build robust relationships with U.S. allies and international partn

"Thr
also

Strategic Initiative 5: DoD will leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

"We will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet these challenges."

- 2010 National Security Strategy

Cyberpolicy Evolution

- 140 nations have are or building cyber offense and defense capability
  - Everyone knows cyberspace is important
  - Everyone wants to be perceived as being in the game
- Rules of engagement, magnitude of response are not well defined
  - Was Stuxnet an act of war?
  - Should the US engage in cyberespionage against Chinese companies?
  - What is the appropriate response to a DDOS by state-sponsored "patriotic hackers"?

CIO East Africa (Nairobi)

EMAIL PRINT SHARE

Kenya: National Cyber Security Strategy Launched

BY DENNIS MBUVI, 12 FEBRUARY 2013

RELATED TOPICS

Kenya

Kenya on Tuesday announced the launch of the country's National Cybersecurity Strategy and Master Plan(NCSMP). The NCSMP will be part of the National ICT Masterplan that will be launched on Thursday this week.

Trickle Down Cyberweapons

- Cyberweapons proliferation is already happening
- Most 0-day exploits are discovered and exploited by nation-states

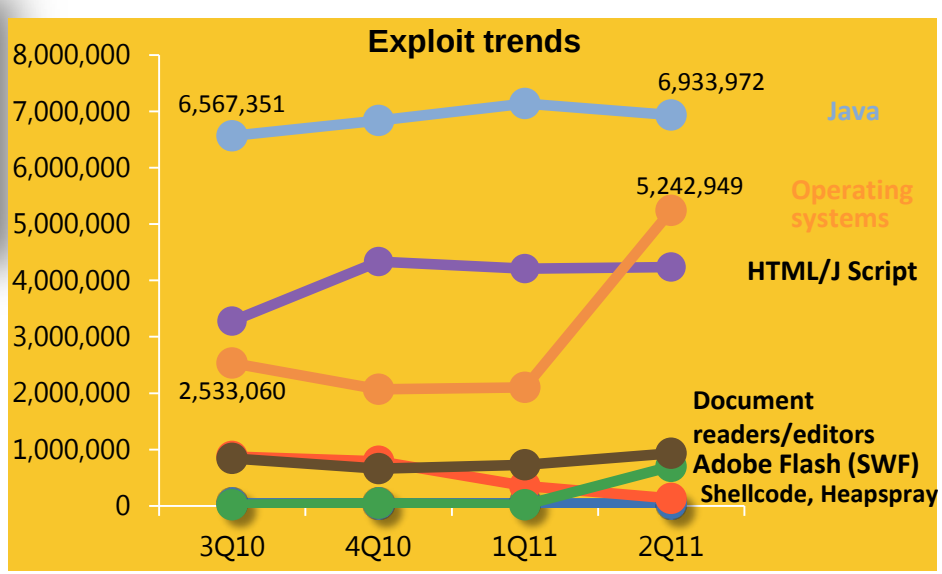
Stuxnet Tricks Copied by Computer Criminals

Techniques used by government-backed malware are surfacing in the code used by ordinary cyber criminals.

6 comments

TOM SIMONITE

Wednesday, September 19, 2012



Geopolitical Interconnections

- WikiLeaks document reveals awakening of Chinese awareness of dependence on foreign technology

C O N F I D E N T I A L SECTION 01 OF 03 BEIJING 000247
SIPDIS
DEPT FOR S, P, D, EAP/CM, EEB, AND H
NSC FOR BADER, MEDEIROS, AND LOI
E.O. 12958: DECL: 01/28/2030
TAGS: ECON [Economic Conditions], EINV [Foreign Investments], PGOV [Internal Governmental Affairs], PREL [External Political Relations], CH [China (Mainland)]

…

¶8. According to another well-respected tech sector analyst here, a number of historical, cultural, and technological factors have coalesced **to put China in a technologically-aggressive state-of-mind**. One contributing factor was **Microsoft's flubbed 2004 "black screen"** strategy to deter intellectual property theft by darkening computer monitors running unlicensed Windows operating software. This consultant believes that example of **U.S. technology effectively wielding power over China's personal computers helped spur China's aggressive campaign for source codes and its own technology.** This, combined with growing Chinese pride, economic clout and influence, and the "weakened" position of the U.S. and its allies after the global economic downturn, are emboldening the Chinese to take ever more aggressive positions in advancing its innovative industries at the expense of foreign ones.

Geopolitical Cyberboundaries

- In 2012 Microsoft Digital Crimes Unit takes down Nitol Botnet

Reaction to Nitol Takedown

A protester destroys an overturned Japanese-brand police car during an anti-Japan protest in Shenzhen, August 19, 2012. (Reuters/Keita Van)

"Does Microsoft sue in U.S. or China?"

Can Microsoft shutdown my domain name (which has 2.85 million users) like this without advanced notification?"

"Microsoft closed a Chinese domain name through the U.S. court, this is more meaningful than Diaoy Island (Senkaku) disputation between China and Japan."

What Can You Do To Protect Your Data?

Assumed Breach Mentality

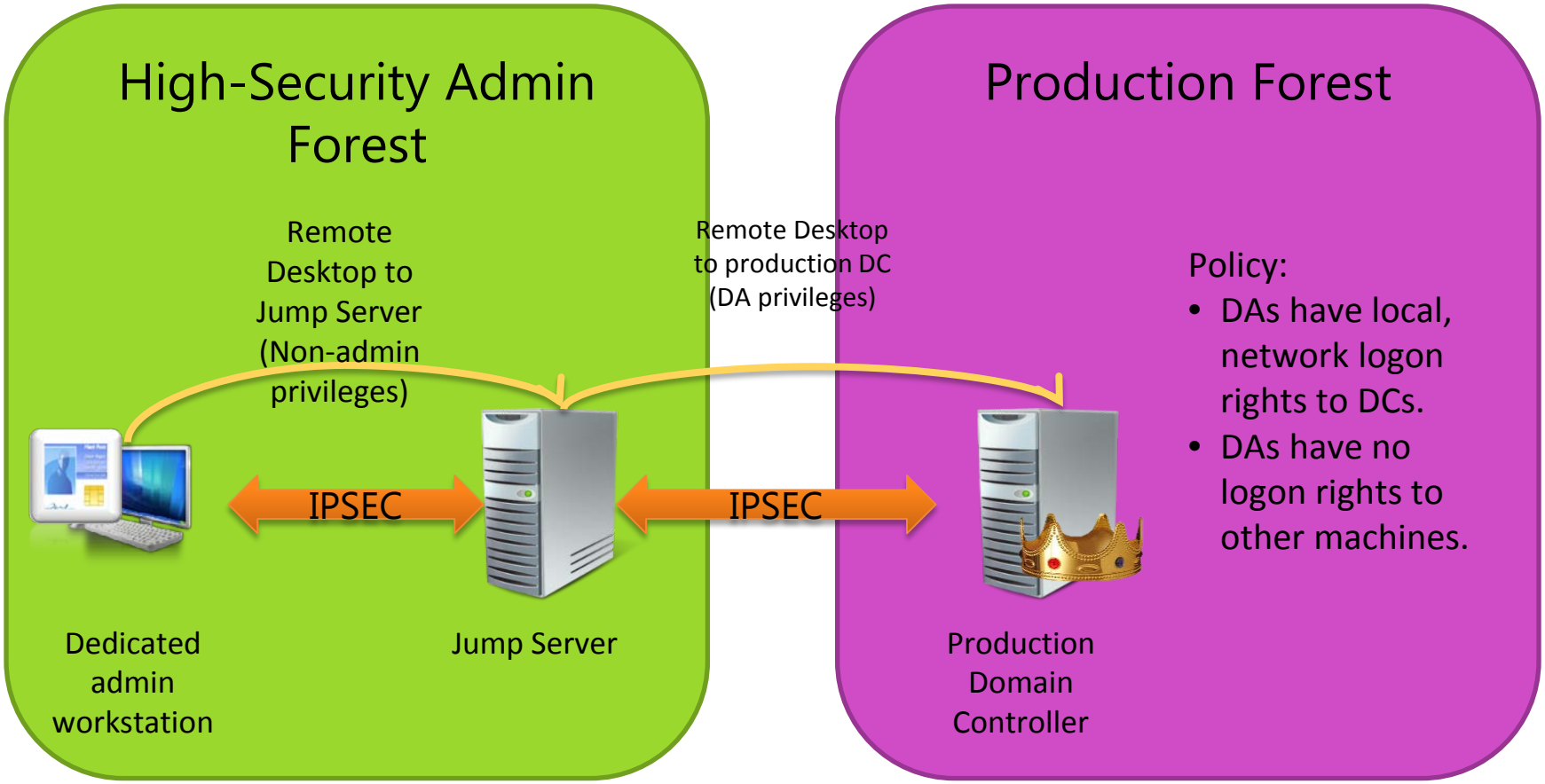
- Typical breach victim:
  - Has intrusion detection systems
  - Has anti-malware
  - Has a Security Event Manager correlating GB of data daily
  - Responds to hundreds of alerts daily
  - *Often learn of compromise from other means*
- Keys to being prepared:
  - Identify, isolate and contain high value resources/accounts
  - Have an incident response plan
  - Do not piece-meal mitigate, quickly execute a holistic plan
  - Run drills and "red team" exercizes

Mitigating Pass-the-Hash

Mitigation	Effectiveness	Effort required	Privilege escalation	Lateral movement
Mitigation 1: Restrict and protect high privileged domain accounts	Excellent	Medium	√	-
Mitigation 2: Restrict and protect local accounts with administrative privileges	Excellent	Low	-	√
Mitigation 3: Restrict inbound traffic using the Windows Firewall	Excellent	Medium	-	√
More recommendations	**Effectiveness**	**Effort required**	**Privilege escalation**	**Lateral movement**
Remove standard users from the local administrators group	Excellent	High	√	-
Limit the number and use of privileged domain accounts	Good	Medium	√	-
Configure outbound proxies to deny Internet access to privileged accounts	Good	Low	√	-
Ensure administrative accounts do not have email accounts	Good	Low	√	-
Use remote management tools that do not place reusable credentials on a remote computer's memory	Good	Medium	√	-
Avoid logons to less secure computers that are potentially compromised	Good	Low	√	√
Update applications and operating systems	Partial	Medium	-	-
Secure and manage domain controllers	Partial	Medium	-	-
Remove LM hashes	Partial	Low	-	-
Other mitigation	**Effectiveness**	**Effort required**	**Privilege escalation**	**Lateral movement**
Disable the NTLM protocol	Minimal	High	-	-
Smart cards and multifactor authentication	Minimal	High	-	-
Jump servers	Minimal	High	√	-
Rebooting workstations and servers	Minimal	Low	-	-

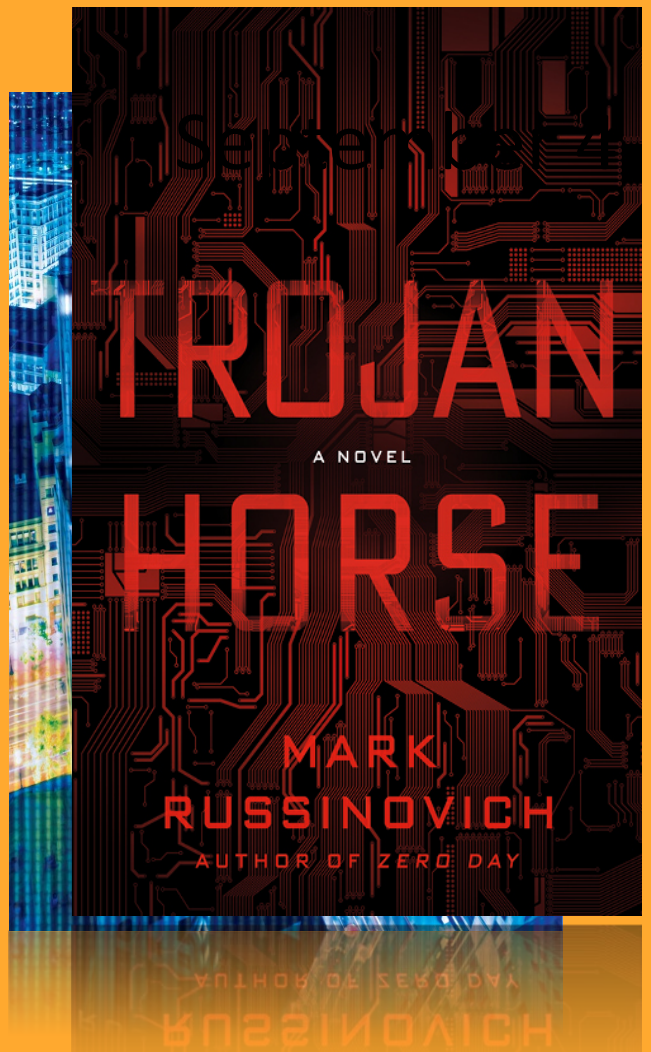
http://blogs.technet.com/b/security/archive/2012/12/06/new-guidance-to-mitigate-determined-adversaries-favorite-attack-pass-the-hash.aspx

Protecting Privileged Accounts



Trojan Horse: A Novel

- A cyberthriller true to the science
  - Forward by Kevin Mitnick
  - Audible bonus of me and Kevin discussing cybersecurity
  - Book signing at 2:20
- www.russinovich.com



Summary and Q&A