Outline

• Olympic Games exploits
  – Duqu, Flame, Regin
  – Equation Group

• Other important cyber events
Olympic Games Software

• Stuxnet discovered in July 2010
• Duqu discovered in September 2011
  – Collects control system info; similar to Stuxnet
• Flame discovered in May 2012
  – Designed primarily for reconnaissance
• Regin discovered in 2014
  – Designed to gather long-term intelligence stealthily
• Equation Group identified by Kaspserky in 2015
Other Important Cyber Events

• 2012 Shamoon attack
  – Designed for espionage
  – But wiped 30K Saudi Aramco computers
  – Required 1-2 weeks to bring systems back
• 2013 Mandiant APT1 report
  – Appendix describes stages of advanced persistent threat
• 2014 DDoS attacks on US Banks
• 2014 Massive Sony attack
Olympic Games Exploits

Duqu
Duqu Malware

• Reconnaissance only for later Stuxnet-style attacks
  – Discovered 9/1/11 by Hungarian computer scientists
  – Targeted suppliers of industrial facilities
  – Primarily a remote access tool (RAT)
  – Symantec says lots of code is common with Stuxnet
  – Stuxnet compiled 6/09-3/10, Duqu 11/3/10, later

• At least 6 orgs in 8 countries were infected
  – At least 15 variants discovered

• Designed to disappear in 30 days, can be extended

Duqu Malware
Duqu Malware

• Has Installer, Driver, DLL, Config File, Shellcode
• Installer exploits MSFT kernel 0-day
  – One dropper invoked 0-day via a Word file
• Installer registers driver so it will be executed on system initialization
• Driver injects the DLL into services.exe
• The main DLL extracts files embedded in it.
• These files are injected into various processes
Duqu Command & Control

- HTTP, HTTPS used to reach C&C servers
  - But Duqu can also use peer-to-peer communication
- Traffic from Duqu to C&C servers is forwarded
- Traffic back to C&C servers is used to download executables, e.g. infostealer
- C&C sends encrypted data inside .jpg files
- One Duqu driver signed by Taiwanese certificate
- Evidence indicates it postdates Stuxnet
Duqu Purpose

• Seeks info on industrial control systems
• But, it could be used destructively
  – On personal computers it has erased files and, in some cases, has erased disks
• It tries to steal certificates to hide future attacks
Olympic Games Exploits

Flame
Flame is Enormous!

- AKA Flame, Flamer, sKyWIper, Skywiper
- CrySyS Lab, Budapest University of Technology & Economics analyzed it at request of the ITU and on May 28, 2012 declared:
  - Flame "is certainly the most sophisticated malware we encountered during our practice; arguably, it is the most complex malware ever found."

- Kaspersky Lab:
  - Flame reported to be 20 MB in size, 20 × size of Stuxnet
  - Is also highly modular – truly sophisticated malware
Flame Big Picture

• Kaspersky: Flame in the wild since Feb 2010
• CrySyS: Main component of Flame seen 2007
• Symantec: On June 8, 2012 Flame was sent a “kill” command to eliminate all traces of it
• Countries most affected: Austria, Hong Kong, Hungary, Iran, Israel, Lebanon, Palestinian Territories, Russia, Sudan, Syria, Saudi Arabia, and Egypt
Flame Functionality

- Written in Lua & compiled C++
- Uses 5 encryption methods & SQLite DB
- Code unlike Duqu or Stuxnet
- But uses two 0-days exploited by Stuxnet
- Customizes its behavior to reduce AV detection
- Uses fake audio driver to maintain persistence
- Has “kill” function that eliminates all its files
- Has software to “wipe” disks

Coders Behind the Flame Malware Left Incriminating Clues on Control Servers, K. Zetter, Wired, 9/17/12
Flame Deployment

• It evades detection through use of rootkit
• Spreads via local networks or USBs
• It can record audio, screenshots, keyboard activity, network traffic, and Skype sessions
• Appears to be used purely for generic espionage
• Kaspersky: its targets primarily in Iran, looking for AutoCAD drawings, PDFs, and text files
• Access via 80 servers in Asia, Europe, N. America
Flame Origins

• 6/19/2012, Washington Post: Part of classified Olympic Games effort started ≥ 5 years earlier, i.e. started in 2007 or earlier

• Kaspersky: Sees connection with early version of Stuxnet. About same code used by both for USB propagation and both used the same 0-day.

• Snowden leak says NSA and GCHQ responsible
Olympic Games Exploits

Regin
Regin*

• Revealed in 2014, targets MSFT Windows
• Very stealthy long-term intelligence-gathering
  – Uses encrypted virtual file system (EVFS), inside single file
• “In the world of malware threats, only a few rare examples can truly be considered groundbreaking and almost peerless.”
• Regin is multi-staged, modular threat
  – Multi-stage: modules depend on other modules
  – This makes analysis difficult

* Regin: Top-tier espionage tool enables stealthy surveillance, Symantec, November 24, 2014
Regin*

- Its modular approach is common with Flame
- Its multi-stage loading architecture similar to that of Duqu and Stuxnet.
- It differs from traditional advanced persistent threats (APTs) in techniques and purpose.
  - APTs typically seek specific information, such as IP
  - Regin both collects data and does continuous monitoring

* Regin: Top-tier espionage tool enables stealthy surveillance, Symantec, November 24, 2014
Regin* Payloads

• RAT takes screenshots, controls point-and-click
• Password theft, traffic monitoring, collect info on processes and memory utilization
• Scans for deleted files and retrieve them
• Collects traffic to MSFT IIS servers and admin traffic to telephony base station controllers
• Can parse mail from Exchange databases

* Regin: Top-tier espionage tool enables stealthy surveillance, Symantec, November 24, 2014
Regin* Targets

• Targeted private individuals & small businesses (48%) followed by telecom backbones (28%)
• Targeted Russia (28%), Saudi Arabia (24%), etc
• May have spied on Belgacom, a Belgian telecom
• Found on USB owned by Angela Merkel staffer

* Regin: Top-tier espionage tool enables stealthy surveillance, Symantec, November 24, 2014
Regin Architecture

- 6-stages, only first stage driver is visible
- Stages 1, 2: load driver
- Stage 3: load encryption, networking and EVFS
- Stage 4: Uses EVFS to load kernel drivers
- Stage 5: Main payloads and data files
Extensive Regin C&C

• Bidirectional communications to and from C&C
• Compromised computers can serve as proxies
• C&C can be done peer-to-peer
• All communications are strongly encrypted
  – Both control and data path are established
• Regin logs data
Examples of Regin Payloads

• Rootkit, DLL injection, network packet filter
• Network port blocker and capture
• Password stealer, SSL comms,
• Gathers system info: CPU Memory, drives, shares, devices, installed software, processes
• UI manipulation, file system forensic software
Olympic Games Exploits

Equation Group
Equation Group*

• Kaspersky Lab says Equation Group active since at least 2001, maybe 1996.

• “(P)robably one of the most sophisticated cyber attack groups in the world.” They have a “love for encryption algorithms and obfuscation strategies and (a) sophisticated methods”

• They can reprogram disk drive firmware
  – Making it extremely difficult to detect or remove

* Equation Group: Questions and Answers, Kasperky Lab, February 2015
Equation Group’s Exploits
Other Notable Attacks
Shamoon Attacks on Oil Producers

• The Shamoon malware, found in August 2012, corrupts files and overwrites the Master Boot Record making a computer unusable.

• 30,000 Saudi Aramco machines wiped for 1-2 weeks
  – Biggest OPEC producer!
  – Production not halted but valuable info lost.
  – Attacker took control of one computer, propagated malware to others, then disabled them together.

• Retaliation for Flame attack against Iran?

• RasGas, Qatari LNG firm, was also hit at same time
2013 Mandiant Report

- Mandiant has investigated APT groups since 2004.
- Concludes Chinese group (APT1) most prolific.
  - Active since 2006; collects most information
  - Publishing report because of APT1’s scale and impact
- Mandiant has examined ~150 attacks on victims.
- Has uncovered APT1 attack infrastructure, C&C, and modus operandi (TTP)
- Has also identified three APT1 personnas.
Mandiant Report (cont.)

• Says APT1 is likely government-sponsored and one of China’s most persistent threat actors.
• Tracked APT1 back to the Peoples Liberation Army (PLA) Unit 61398 in a Shanghai building.
• APT1 has stolen hundreds of terabytes of info from 141 organizations.
• Can steal simultaneously from dozens of orgs.
• Maintains about 1,000 C&Cs around the world.
2012-13 DDoS Attacks on US Banks

• Islamic group called Cyber Fighters of Izz ad-Din al-Qassam launched multiple waves of DDoS attacks against banks & financial institutions
  – Targets: Wells Fargo, U.S. Bank, Bank of America, JPMorgan Chase, PNC Bank, Principal Financial, Ameriprise, State Street, Charles Schwab, etc.

• Criminals have used such attacks to distract managers so they can launch wire transfers
2014 Sony Attack

• High profile attack against Sony in late 2014, ostensibly a protest against *The Interview*.
• Terabytes of data exfiltrated, which must have taken months.
• Disks were wiped and networks disabled.
• Very embarrassing to Sony and leadership.
• US claims North Korea responsible.
• Others attribute to disgruntled former employees.
Outline

- Olympic Games exploits
  - Duqu, Flame, Regin
  - Equation Group
- Other important cyber events
  - Shamoon, Mandiant APT1, Bank DDoS, Sony