OPERATION AURORA

IST623 – Introduction to Information Security

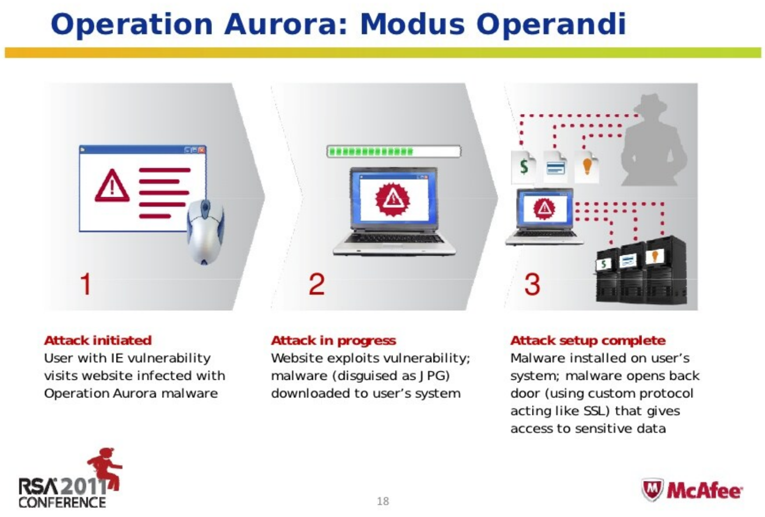
School of Information Studies
SYRACUSE UNIVERSITY

ISSUES IN CONTEXT

- Hackers used a Trojan called "Aurora"
  - Chinese Human Rights Advocates were attacked, and their Gmail accounts were infiltrated
  - The attackers wanted to uncover the identities of clandestine Chinese agents operating in the United States
  - Unveiling this information would give attackers insight on active FBI investigations and other law enforcement activities
  - Gives attackers the advantage to destroy information and help people escape the country

ISSUES IN CONTEXT

- The Process:
  - A targeted user received a link in an email or message from a "trusted" source
  - The user clicked on the link which led the user to a website hosted in Taiwan that contained a malicious JavaScript payload
  - The user's browser downloaded the malicious JavaScript which in turn included a binary disguised as an image from Taiwan servers and executed the payload
  - The payload set up a backdoor and connected to command-and-control servers in Taiwan
  - As a result, the attackers had complete access to internal systems



Operation Aurora: Modus Operandi

Attack initiated
User with IE vulnerability visits website infected with Operation Aurora malware

Attack in progress
Website exploits vulnerability; malware (disguised as J PG) downloaded to user's system

Attack setup complete
Malware installed on user's system; malware opens back door (using custom protocol acting like SSL) that gives access to sensitive data

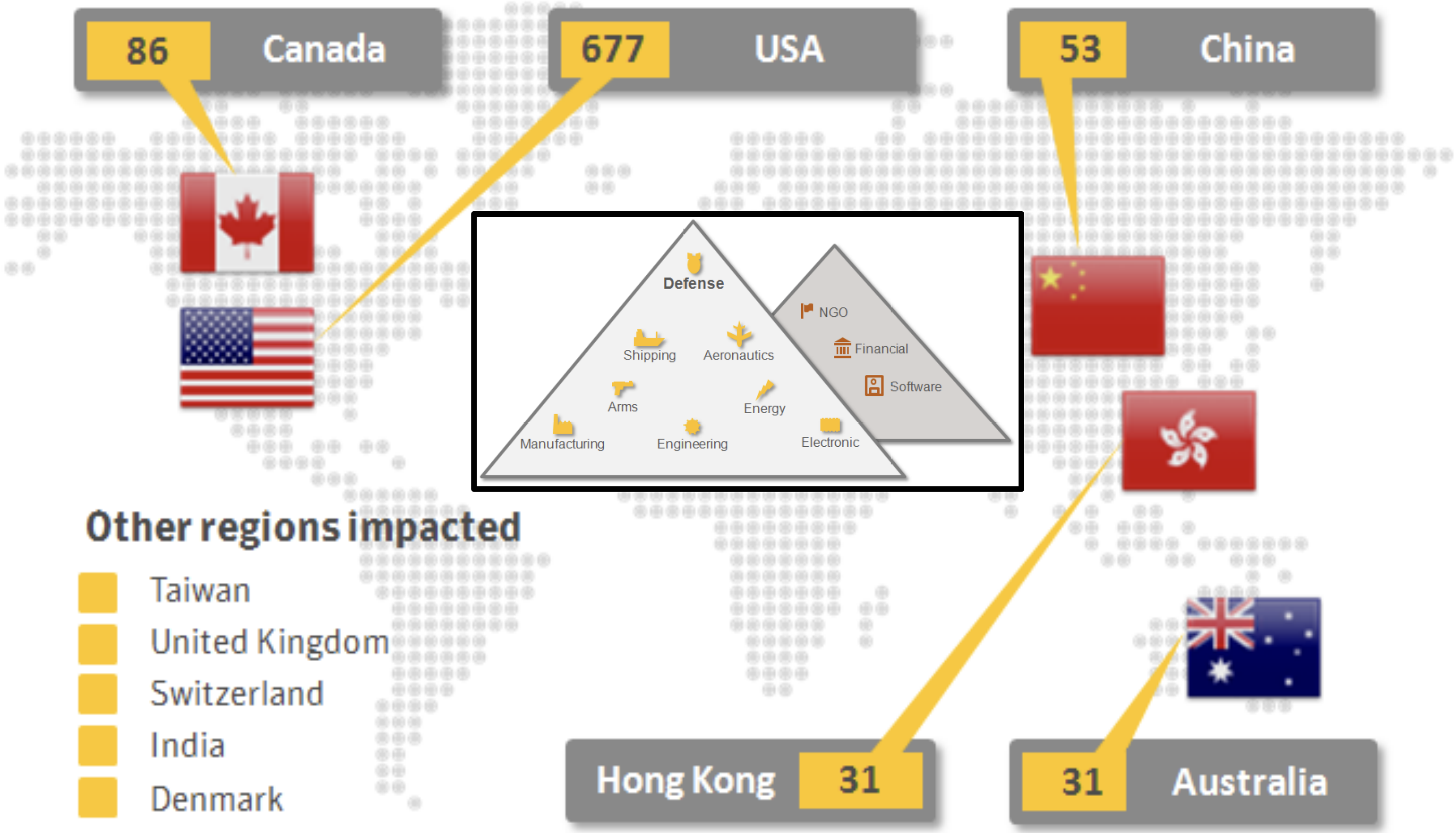
RSA 2011 CONFERENCE

18

McAfee

CHALLENGES

- ✓ Varied Targets



86 Canada

677 USA

53 China

Hong Kong 31

31 Australia

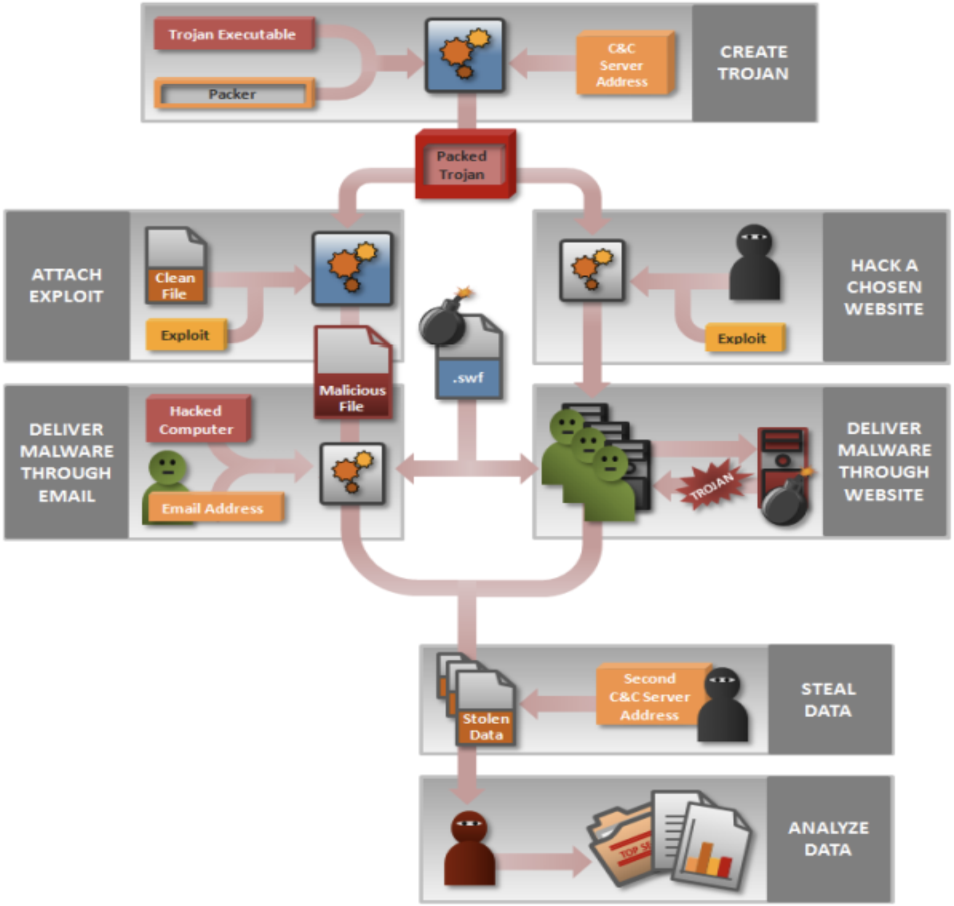
Other regions impacted

- Taiwan
- United Kingdom
- Switzerland
- India
- Denmark

School of Information Studies
SYRACUSE UNIVERSITY

CHALLENGES

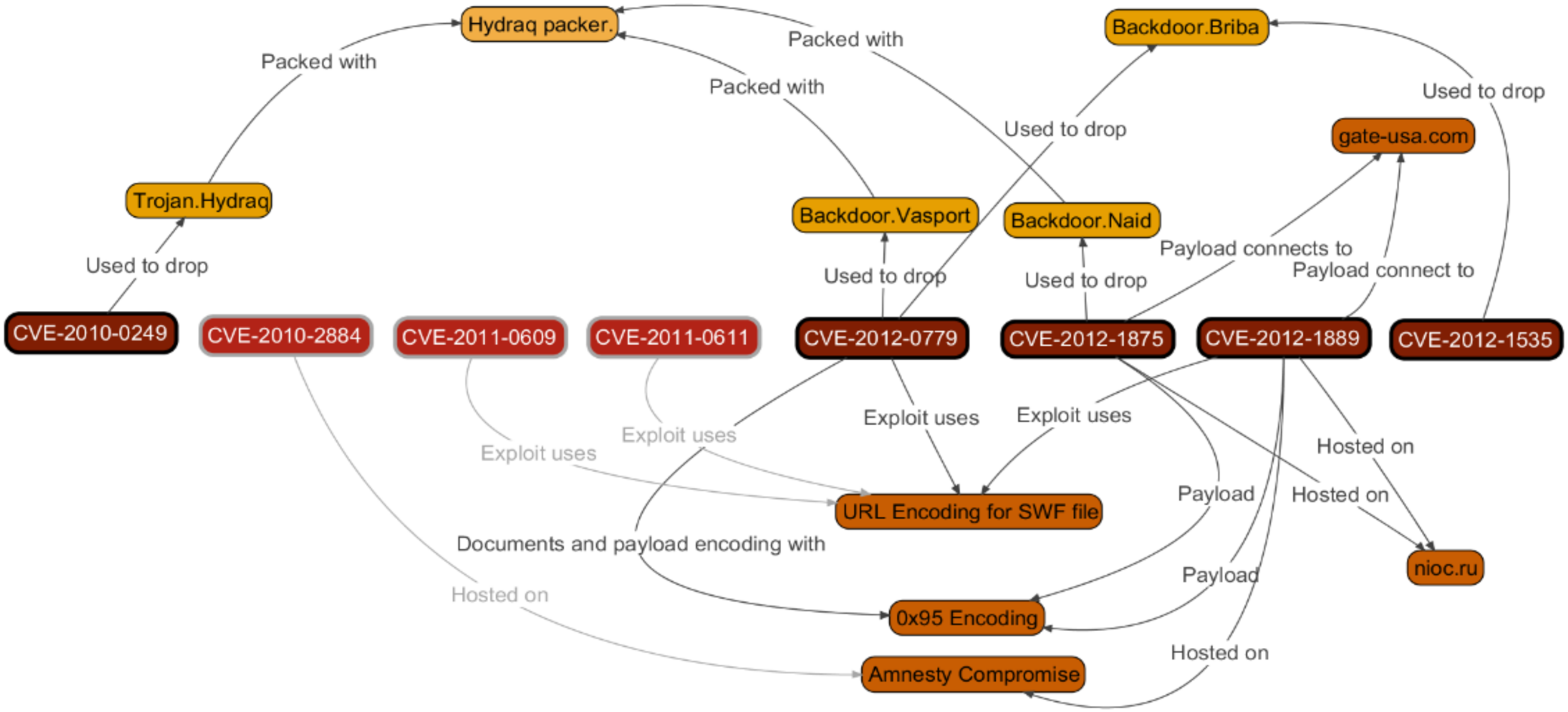
- ✓ Varied delivery techniques



School of Information Studies
SYRACUSE UNIVERSITY

CHALLENGES

- ✓ Varied delivery timing



School of Information Studies
SYRACUSE UNIVERSITY

CHALLENGES

- ✓ Weak security

Rational software

PERFORCE

$

SharePoint Online

CHALLENGES

Slow rate of updates and security patches:

A week after the report by McAfee, Microsoft issued a fix for those 0-day issue.

Microsoft also admitted that they had known about the security hole used since September of previous year.

Along of IE, vulnerability can be exploited by including an ActiveX control in a Microsoft Access, Word, Excel, or PowerPoint file.

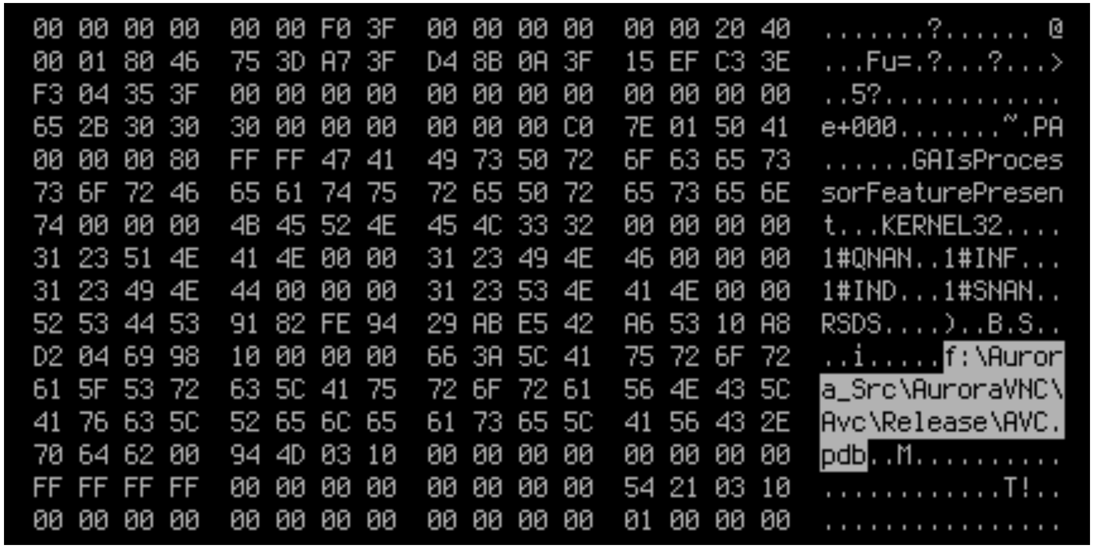
The Internet Explorer exploit code used in the attack has been released into the public domain and has been incorporated into the Metasploit Framework penetration testing tool.

The public release of the exploit code increases the possibility of widespread attacks using the Internet Explorer vulnerability.

Researchers have created attack code that exploits the vulnerability in Internet Explorer 7 (IE7) and IE8—even when Microsoft's recommended defensive measure (Data Execution Prevention (DEP)) is turned on.

CHALLENGES

Who were responsible?



```
00 00 00 00  00 00 F0 3F  00 00 00 00  00 00 20 40  .......?...... @
00 01 80 46  75 3D A7 3F  D4 8B 0A 3F  15 EF C3 3E  ...Fu=.?...?...>
F3 04 35 3F  00 00 00 00  00 00 00 00  00 00 00 00  ..5?............
65 2B 30 30  30 00 00 00  00 00 00 C0  7E 01 50 41  e+000.......~.PA
00 00 00 80  FF FF 47 41  49 73 50 72  6F 63 65 73  ......GAIsProces
73 6F 72 46  65 61 74 75  72 65 50 72  65 73 65 6E  sorFeaturePresen
74 00 00 00  4B 45 52 4E  45 4C 33 32  00 00 00 00  t...KERNEL32....
31 23 51 4E  41 4E 00 00  31 23 49 4E  46 00 00 00  1#QNAN..1#INF...
31 23 49 4E  44 00 00 00  31 23 53 4E  41 4E 00 00  1#IND...1#SNAN..
52 53 44 53  91 82 FE 94  29 AB E5 42  A6 53 10 A8  RSDS....)..B.S..
D2 04 69 98  10 00 00 00  66 3A 5C 41  75 72 6F 72  ..i.....f:\Auror
61 5F 53 72  63 5C 41 75  72 6F 72 61  56 4E 43 5C  a_Src\AuroraVNC\
41 76 63 5C  52 65 6C 65  61 73 65 5C  41 56 43 2E  Avc\Release\AVC.
70 64 62 00  94 4D 03 10  00 00 00 00  00 00 00 00  pdb..M..........
FF FF FF FF  00 00 00 00  00 00 00 00  54 21 03 10  ............T!..
00 00 00 00  00 00 00 00  00 00 00 00  01 00 00 00  ................
```

The "Elderwood" group was named by Symantec.

McAfee named this attack Operation Aurora, based on unique strings present in codebase of malware(Shown here).

Link TO PRC:

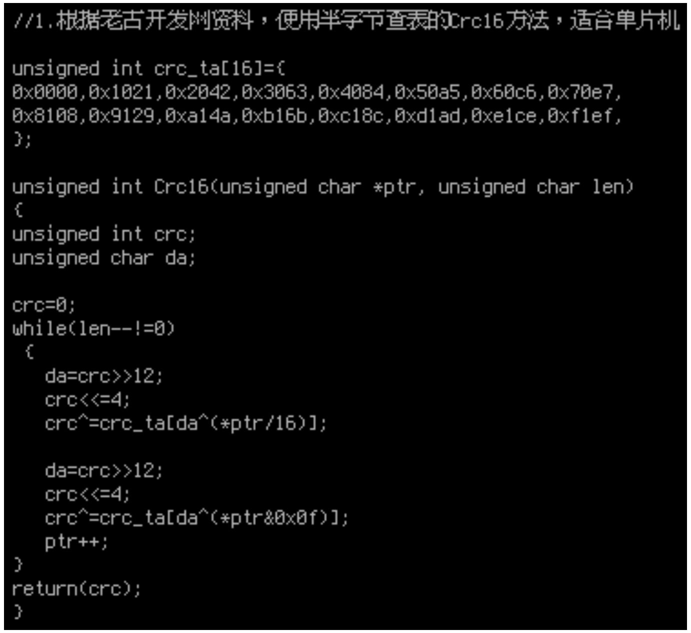
The **Hydraq binary** can point attack to mainland China.

The CRC algorithm is the size of the table of constants, Most 16 or 32-bit CRC algorithms use a hard-coded table of 256 constants. The CRC algorithm used in Hydraq uses a table of only 16 constants; basically, a truncated version of the typical 256-value table.

By decompiling the algorithm and searching the Internet for source code with similar constants, operations and a 16-value CRC table size, "CRC-16 XMODEM“ fully matches the structural code implementation in Hydraq and it also produces the same output when given the same input:

CHALLENGES

Who were responsible? Ctd.



```
//1.根据老古开发网资料，使用半字节查表的crc16方法，适合单片机

unsigned int crc_ta[16]={
0x0000,0x1021,0x2042,0x3063,0x4084,0x50a5,0x60c6,0x70e7,
0x8108,0x9129,0xa14a,0xb16b,0xc18c,0xd1ad,0xe1ce,0xf1ef,
};

unsigned int Crc16(unsigned char *ptr, unsigned char len)
{
unsigned int crc;
unsigned char da;

crc=0;
while(len--!=0)
 {
   da=crc>>12;
   crc<<=4;
   crc^=crc_ta[da^(*ptr/16)];

   da=crc>>12;
   crc<<=4;
   crc^=crc_ta[da^(*ptr&0x0f)];
   ptr++;
}
return(crc);
}
```

The most interesting aspect of this source code sample is that it is of Chinese origin, released as part of a Chinese-language paper on optimizing CRC algorithms for use in microcontrollers.
The full paper was published in simplified Chinese characters, and all existing references and publications of the sample source code seem to be exclusively on Chinese websites. At the time of this attack, This CRC-16 implementation seems to be virtually unknown outside of China, as can be seen by a Google search for one of the key variables, **"crc_ta[16]".**

The use of this unique CRC implementation in Hydraq is evidence that someone from within the **PRC authored the Aurora codebase.**

CHALLENGES

Detection:

Even though, The code behind the main backdoor trojan (called **Hydraq** by antivirus companies) of Operation Aurora appear to be no older than 2009.
It appeared that development of Aurora had been in the works for quite long as some of the custom modules in the Aurora codebase have compiler time stamp that dated back to May 2006. That is only a year or so after the big Titan Rain attacks, which largely used widely-available trojans that were already known to antivirus companies.

As a result of utilization of **completely original code** and then only **organizing the highly-targeted attacks**, the Aurora code escaped detection for quite some time.

https://www.secureworks.com/blog/research-20913

CHALLENGES

To prevent future cyber-attacks like Operation Aurora:

China and the United States agree to a policy of mutually assured restraint with respect to cyberspace.

Allow both these commitments party to take the measures they deem necessary for their self-defense while simultaneously agreeing to refrain from taking offensive steps.

Periodically run an independent scrutinizing of these commitments.

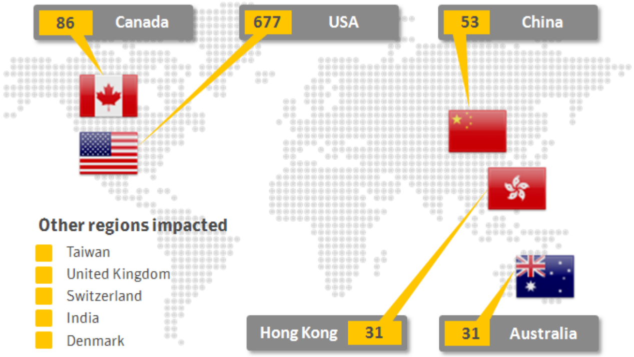
Refrain from installing any kind of back door to the any product for purpose of cyber espionage.

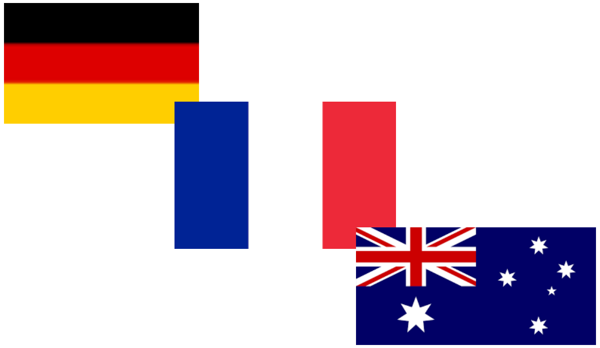
As soon as existence of Venerability is known, make it the top priority work to fix it.

OUTCOMES

- Various governments publicly issued warnings to users of Internet Explorer after the attack, advising them to use alternative browsers.

- The Internet Explorer exploit code used in the attack has been released into the public domain and has been incorporated into the Metasploit Framework penetration testing tool.





School of Information Studies
SYRACUSE UNIVERSITY

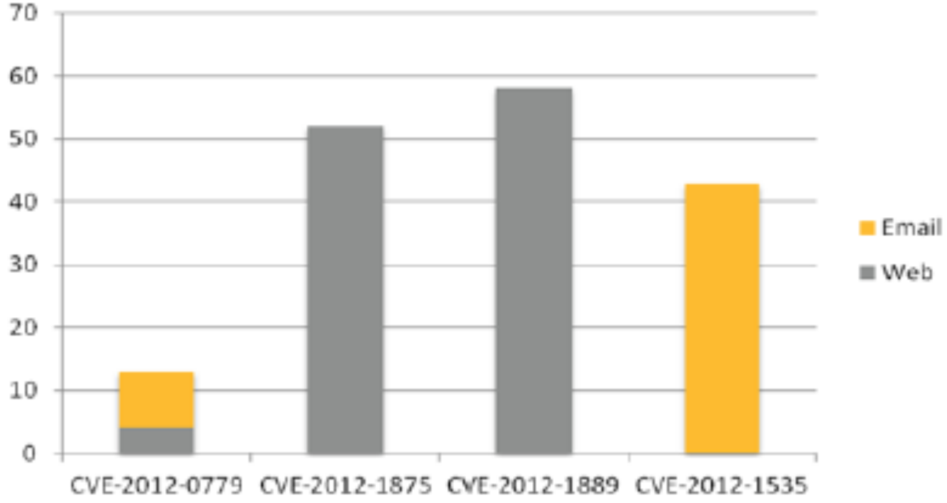
OUTCOMES

- CVE's patch, security holes plugged. But only a hiccup in security arms race.

- For enterprise organizations, just patching browsers and software is not enough. When organizations can coordinate multiple zero-day exploits, penetration testing becomes a necessity.

Figure 4

Number of targeted companies (Email) and compromised websites (Web) per exploit



OUTCOMES

- Security professionals outlook on the attack created a posture change in information security practices. Contributing to a paradigm shift in some industries.

- Proactive rather than reactive security policies are the only way to defend against sophisticated and targeted attacks like the one in operation Aurora.

OPERATION
AURORA
JANUARY 12, 2010
Google first publicly discloses Operation Aurora, a series of cyberattacks conducted by advanced persistent threats with ties to the Chinese People's Liberation Army.
GOOGLE

QUESTIONS?

RESOURCES

- https://www.sciencedirect.com/topics/computer-science/operation-aurora
- https://cyware.com/news/everything-you-need-to-know-about-operation-aurora-5c5f5b99
- https://www.govconexec.com/2011/02/01/auroras-aftermath/
- https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf
- https://www.secureworks.com/blog/research-20913
- https://attack.mitre.org/groups/G0066/
- https://attack.mitre.org/groups/G0025/
- https://en.wikipedia.org/wiki/Five_Poisons

School of Information Studies
SYRACUSE UNIVERSITY