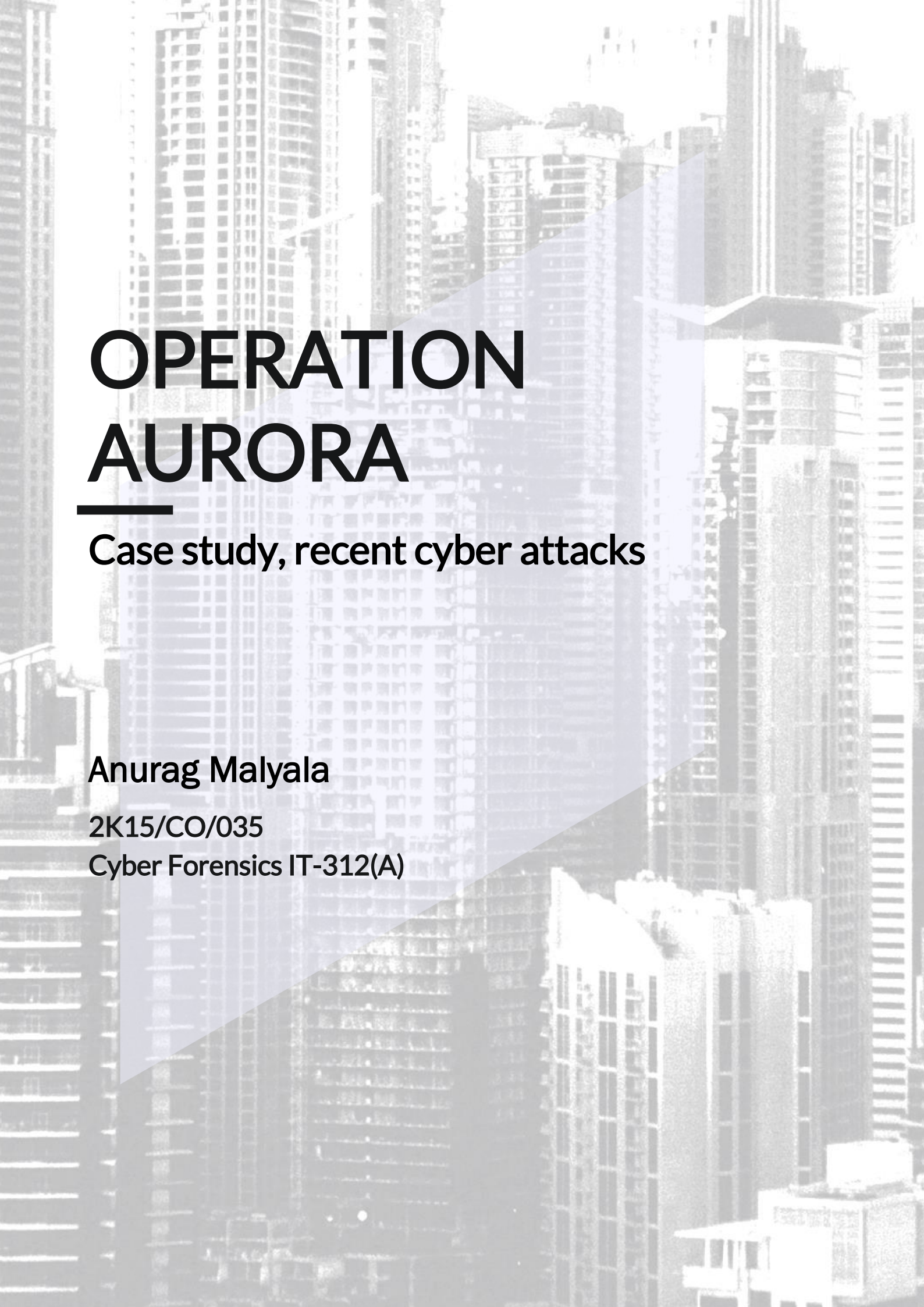


OPERATION AURORA

Case study, recent cyber attacks

Anurag Malyala

2K15/CO/035

Cyber Forensics IT-312(A)

OPERATION AURORA

DRIVING GOOGLE OUT OF MAINLAND CHINA

WHEN:
Jun-Dec 2009

FRONTIER:
World wide

PARTIES:
China (Unknown) USA (Google)

RESULT:
Google; theft of intellectual property,
China; unknown.
Goal of attackers:
Gain Access and modify source codes of Security and defense contractors.
Other Targets:
Adobe Systems, Juniper Networks, and Rackspace

Introduction

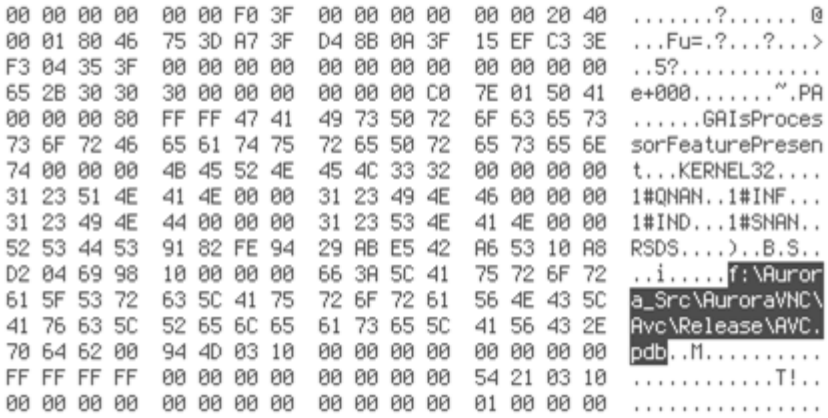
On January 12th, 2010, Google announced that its technology infrastructure had been the target of a series of China-led cyber-attacks. Quote, "highly sophisticated and targeted attack" was discovered. Google shocked everyone using their services, especially mail, and security communities by revealing that they and other companies were attacked, these attacks originated in China and resulted in the theft of Google's own intellectual property. [1]
The attack on Google involved attempts to access the Gmail accounts of Chinese human rights activists, there was no breach of email data, the only data leaked was the account names and create dates. Google also discovered during their investigation that at least 20 other companies were also targeted in a similar manner.
On January 14, 2010 McAfee Labs identified a zero-day vulnerability in Microsoft Internet Explorer that was used as an entry point for Operation Aurora to exploit Google and at least 20 other companies. Microsoft issued a security bulletin and patch immediately.

Background

Operation Aurora was a coordinated attack which included a piece of computer code that exploits the Microsoft Internet Explorer vulnerability to gain access to computer systems. This exploit is then extended to download and activate malware within the systems. The attack, which was initiated stealthily when targeted users accessed a malicious web page, ultimately connected those computer systems to a remote server. Now this connection was used to steal company intellectual property and additionally gain access to user accounts.

Hackers seeking source code from Google, Adobe and dozens of other high-profile companies, the attackers used nearly a dozen pieces of malware and several levels of encryption to burrow deeply into the bowels of company networks and obscure their activity. The encryption was

highly successful in obfuscating the attack and avoiding common detection methods,". "We haven't seen encryption at this level. It was highly sophisticated. [2]
The name comes from references in the malware to the name of a file folder named "Aurora" that was on the computer of one of the attackers. McAfee researchers say when the hacker compiled the source code for the malware into an executable file, the compiler injected the name of the directory on the attacker's machine where he worked on the source code



1 The source of the Name

Platform	IE 6 Vulnerable	IE 7 Vulnerable	IE 8 Vulnerable
Windows 2000	High Risk	N/A	N/A
Windows XP	High Risk	High Risk	Medium Risk (DEP* Enabled w/ SP3)
Windows 2003	Medium Risk (DEP* Enabled)	Medium Risk (DEP* Enabled)	Medium Risk (DEP* Enabled)
Windows Vista	N/A	High Risk	Medium Risk (DEP* Enabled w/ SP1)
Windows 2008	N/A	N/A	Medium Risk (DEP* Enabled)
Windows 7	N/A	N/A	Medium Risk (DEP* Enabled)

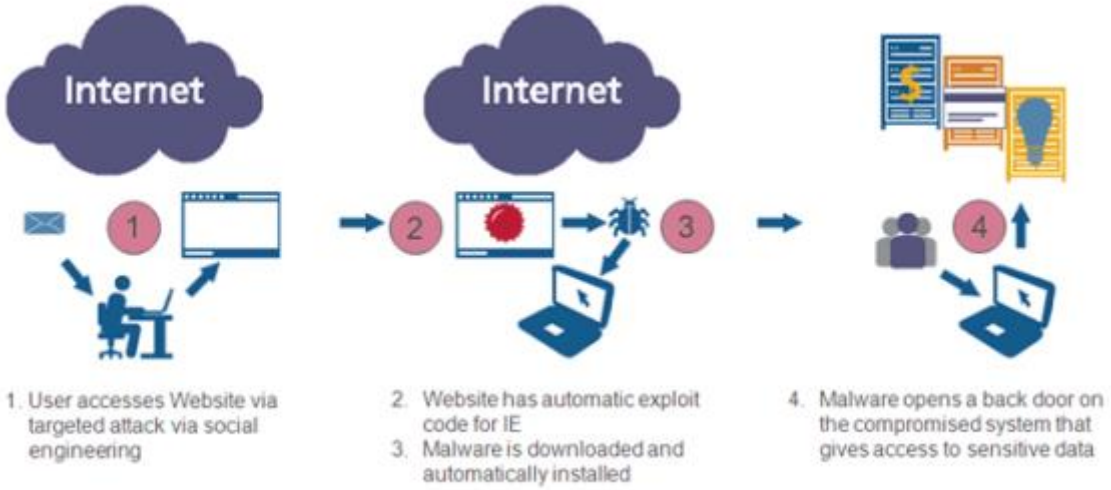
2 Vulnerable systems

How did it happen?

The attack exploited a vulnerability in the Internet Explorer browser, Once the user visited the malicious site, their Internet Explorer browser was exploited to download an array of malware to their computer automatically and transparently. The programs unloaded seamlessly and silently onto the system, like Russian nesting dolls, flowing one after the other. The encryption was such that the security software couldn't detect any kind of malware or even any abnormal activity.
The initial piece of code was shellcode encrypted three times and that activated the exploit. A shellcode is a piece of code which starts from a command shell and helps the attacker control the user's machine. It can spawn new shells and usually acts as a payload to help the attacker expose the vulnerability. This shellcode then executed downloads from an external machine that

dropped the first piece of binary on the host. That download was also encrypted. The encrypted binary packed itself into a couple of executables that were also encrypted.
One of the malicious programs opened a remote backdoor to the computer, establishing an encrypted covert channel that masqueraded as an SSL connection to avoid detection This allowed the attackers ongoing access to the computer and to use it as a beachhead into other parts of the network to search for login credentials, intellectual property and whatever else they were looking for.

[3]
3 The Aurora Life cycle



Lessons from Code analysis

From analyzing the uncompiled files, it was observed that the main backdoor i.e. a trojan called Hydraq was not very old but the Aurora source was in the works for a very long time, nearly back to the Titan Rain attacks, which largely used widely-available trojans that were already known to antivirus companies. Because of using completely original code and then only in highly-targeted attacks, the Aurora code seems to have escaped detection for quite some time.
From the CRCs used in the packages, a link back to China was established.
unusual about this CRC algorithm is the size of the table of constants (the incrementing values in the left pane of the assembly listing). 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.

Titan Rain

The attacks were labeled as Chinese in origin, although their precise nature, e.g., state-sponsored espionage, corporate espionage, or random hacker attacks, and their real identities – masked by proxy, zombie computer, spyware/virus infected – remain unknown. The activity known as "Titan Rain" is believed to be associated with an Advanced Persistent Threat.

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. This CRC-16 implementation seems to be virtually unknown outside of China. [4]

```
SUB ESP,40
PUSH ESI
MOV ESI,DWORD PTR SS:[ESP+4C]
XOR EAX,EAX
TEST ESI,ESI
MOV DWORD PTR SS:[ESP+4],0
MOV DWORD PTR SS:[ESP+8],1021
MOV DWORD PTR SS:[ESP+C],2042
MOV DWORD PTR SS:[ESP+10],3063
MOV DWORD PTR SS:[ESP+14],4084
MOV DWORD PTR SS:[ESP+18],50A5
MOV DWORD PTR SS:[ESP+1C],60C6
MOV DWORD PTR SS:[ESP+20],70E7
MOV DWORD PTR SS:[ESP+24],8108
MOV DWORD PTR SS:[ESP+28],9129
MOV DWORD PTR SS:[ESP+2C],0A14A
MOV DWORD PTR SS:[ESP+30],0B16B
MOV DWORD PTR SS:[ESP+34],0C18C
MOV DWORD PTR SS:[ESP+38],0D1AD
MOV DWORD PTR SS:[ESP+3C],0E1CE
MOV DWORD PTR SS:[ESP+40],0F1EF
JE SHORT <hydraq-a.return_0>
PUSH EBX
PUSH EDI
MOV EDI,DWORD PTR SS:[ESP+50]
MOVZX ECX,BYTE PTR DS:[EDI]
MOV EDX,EAX
SHR EDX,8
MOVZX EDX,DL
SHR EDX,4
MOV EBX,ECX
SHR EBX,4
XOR EDX,EBX
SHL EAX,4
XOR EAX,DWORD PTR SS:[ESP+EDX*4+C]
AND ECX,0F
MOV EDX,EAX
SHR EDX,8
MOVZX EDX,DL
SHR EDX,4
XOR EDX,ECX
SHL EAX,4
XOR EAX,DWORD PTR SS:[ESP+EDX*4+C]
SUB ESI,1
ADD EDI,1
TEST ESI,ESI
JNZ SHORT <hydraq-a.beginCRCLoop>
POP EDI
POP EBX
POP ESI
ADD ESP,40
RETN
```

4 16 bit CRC that gave away the origin

Aftermath

- The German, Australian, and French governments publicly issued warnings to users of Internet Explorer after the attack, advising them to use alternative browsers at least until a fix for the security hole was made. [5]
- January 14, 2010, Microsoft said that attackers targeting Google and other U.S. companies used software that exploits a hole in Internet Explorer. [6]
- To prevent future cyberattacks such as Operation Aurora, Amitai Etzioni of the Institute for Communitarian Policy Studies has suggested that the United States and China agree to a policy of mutually assured restraint with respect to cyberspace. [7]

Works Cited

[1] Google, "A new approach to China," [Online]. Available: https://googleblog.blogspot.in/2010/01/new-approach-to-china.html.

[2] D. Alperovitch, Interviewee, *vice president of threat research, McAfee.* [Interview].

[3] R. Varma, "McAfee Labs: Combating Aurora".

[4] J. STEWART, "Operation Aurora: Clues in the Code," 2010.

[5] TVNZ, ""France, Germany warn Internet Explorer users"," [Online]. Available: http://tvnz.co.nz/technology-news/france-germany-warn-internet-explorer-users-3334330.

[6] CNET, ""New IE hole exploited in attacks on U.S. firms".," [Online]. Available: http://news.cnet.com/8301-27080_3-10435232-245.html.

[7] A. Etzioni, *"MAR: A Model for US-China Relations,",* The Diplomat.