Five Years of Persistent Threats

Maarten Van Horenbeeck
Senior Program Manager

Microsoft Security Response Center
Trustworthy Computing
七夕

七夕（七月七日）Ci Si

七月立秋，處暑雨節氣中，剛好各在七夕、中元兩節日。七月七日的七夕節，是個流傳久遠的佳節，所以人們期盼能在此夜，在情空中望見牛郎、織女相會。台灣的七月節俗，其於農業社會男耕女織的生活習慣有關。有關牛郎、織女的傳說也普遍流傳，自哥倫布兩人明清的一一等神仙話化，說成一對戀人因相愛而愁於工作，被罰分居河水兩岸，就只等一年一度的橋樑相會。藉此勸農勸織，勉勵世間兒女既要愛情，也要工作。這一篇麗的故事結合星辰信仰，被稱為「情人節」。

七夕有乞巧的儀式，在月下設香案，備針線、瓜果、鮮花之類，向牛郎、織女雙星乞巧。穿針乞巧的習俗，早在漢朝末年就有記載，從漢宮到民間都曾流行鬥巧的比賽與遊戲。織女既是聰明而善織的星神，自會保佑女子勤於女紅。此外又將祭拜的白粉高高揚起，粉落在臉上則為美貌之兆，都是女子的心願。

七夕在台灣也是七娘媽誕辰，稱為「七娘媽生」。七娘媽就是七星娘娘，為織女兒的守護神。台南市有奉祀七娘媽的開福宮，在彰化鹿港一帶至今仍有紙錢站作「七娘媽亭」。民間相信十六歲就要在這一天「脱簪」，到開福宮或在自家門口，掛好香案供拜眾神，香花（頭花花、鳳仙花等）及壓紙、白粉、麵紙、棕衣及金紙、娘媽衣等，祭拜後在七娘媽亭，並燒化七娘媽亭。稱為「出婆娘間」，表示成年，感謝七娘媽婆媳的護佑。過港人也將白粉、胭脂等，投擲屋上。此外也有稱此日為「慶母生」，供拜雞酒油飯，燒紙母衣，也是感謝母子之意，求女性神保佑幼子的成長，農業社會醫藥較不發達時，借此祭拜神祇祈護佑子女成長，也是為人父母的願望。
Nyílt napja
2009. március 21-én, szombaton
13.30 – 18.00 óráig
Solymáron, a Waldorf Tanárképzés épületeiben
(József A. u. 41.sz. alatt)

A NAP PROGRAMJA:
13.30 – 14.00 Érkezés, regisztráció, az épület megtekintése
14.00 – 14.15 Köszöntés, a nap programjának ismertetése

PETROCARIBE en los medios
Jueves, 22 de enero de 2009

Jamaica

TITULO Can Obama walk the talk?
MEDIO The Observer
IMPACTO: Negativo

BỘ TRƯỞNG BỔ GIÃO DỤC VÀ ĐÀO TẠO

Căn cứ Nghị định số 178/2007/NĐ-CP ngày 03 tháng 12 năm 2007 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ, cơ quan ngang Bộ;

Căn cứ Nghị định số 32/2008/NĐ-CP ngày 19 tháng 3 năm 2008 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Giáo dục và Đào tạo;
jasistatikke kekentalan kajari, kajari (Aege erau B) ke
keke elu paneli kekentalan suatu, kajari, keke etaka, keke elu paneli kekentalan keke elu paneli kekentalan keke elu paneli kekentalan

| ji-eC-eni |
| axali ambebi saagento |
| Tbilisi, Leoluizas qoCa #1; |
| teL (995 32) 43 77 43 |
| e-mail: ghn@ghan.ge www.ghan.ge |

merve gamoSeva

axali ambebi

nika gilauri Turqmene TSi gaemgavara

Tbilisi.22.04.09. "ji-eC-eni". saqarTvelos premier-ministri nika gilauri Turqmene TSi gaemgavara. gilauri aSxabadi si ori dRc daCeba.

| Bod gyal lo 2136 lo yi ring la, |
| Tashi deleg phun sum tsog, |
| Ama bardro kunkham zang, |
| Tendu dewa thob par shog, |
Agenda
Agenda

• Introduction to file format based attacks
• Why do these attacks work?
• Have they grown more complicated?
• How do attackers hide their activities?
• What can we do?
Growth of Attacks

Total Submissions By Year

- 2005 Totals
- 2006 Totals
- 2007 Totals
- 2008 Totals
- 2009 Totals

250% increase
250% increase
135% increase

Source: Microsoft Malware Protection Center (MMPC)
Methodology

E-mail server

Compromised machine

Web proxy

Control server
Methodology

Free webmail

Compromised machine

Control server
Social Engineering
Social Engineering

-----Original Message-----
From: [Redacted]
Sent: Wednesday, May 14, 2008 8:48 AM
Subject: May update on China/HK economics

Attached please find the China and Hong Kong sections of DB Asia Economics Monthly. Regards

CHINA: Headline inflation will likely ease in May, although upward pressures from rice prices as well as raw materials and labor costs remain. Fixed asset investment growth may rebound in coming months, supporting demand for construction materials. RMB appreciation decelerated in April and will likely remain slow in the remainder of the year.

HONG KONG: Inflation is volatile, partly due to policy decisions, but we think it will peak in Q2 at just above 5% and be down around 3% in Q4. Growth likely slowed to 6% in Q1 from 6.7% in 2007Q4. External demand really hasn’t slowed down yet. Consumption growth is already soft.

(See attached file: China-HK AEM MAY2008.pdf)
Social Engineering

- Clever use of **social engineering** techniques
  - Cognitive dissonance
  - Mimicking writing styles
  - Matching content to interest
  - Convincing users to forward messages
  - Backdooring “memes” and viral content
  - Creating a trusted resource
The Attack
How Content-Type Attacks Work

Malicious document

Vulnerability

Shellcode

Shellcode

Embedded binary

Clean document with same context

Encrypted stub or packed binary

Loaded after successful exploitation
Generations of exploits

• Major changes:
  - Shellcode attempts to evade antivirus and Intrusion Detection
  - Obfuscation techniques
  - File types being exploited
  - The goal and payload of attacks
  - “Phone home” methods

• Quality and reliability of exploits
  - Depends on the vulnerability being exploited
  - Did not change drastically
Generations of packing - avoiding detection

PE header in plain sight.

Simple XOR obfuscation

XOR followed by ROL/ROR

Custom encoders
Generations of shellcode—avoiding detection

- Most static shellcode detectors work by identifying common GetPC patterns
Generations of shellcode- Anti-emulation

```
0000016F 68 3D 40 00+    push  403Dh
00000174 6A FF          push  0FFFFFFFh
00000176 6A FF          push  0FFFFFFFh
00000178 3E DB 2C 24 fild tbyte ptr ds:[esp] ; tbyte = 10bytes = 80bit
00000178 ; push the 80-bit value we just put on the stack
00000178 ; on the FPU register stack
00000178 ; why does it do this? evade emulation and distract
00000178 ; us. most emulators do not support FPU
0000017C 50              push eax ; eax = ebp from before.. put that on the stack
0000017D 50              push eax ; same thing
0000017E 54              push esp ; now put a ptr to all of that on the stack
0000017E ; this is the parameter to the function
0000017F FF 56 20 call dword ptr [esi+20h] ; call [esi+0x20] => GetSystemTimeAsFileTime
0000017F ; this fills in the time (a var on the stack)
00000182 8B C4          mov   eax, esp ; save result in EAX
00000184 68 FF FF FF+    push  0FFFFFFFh
00000189 68 FF FF FF+    push  0FFFFFFFh
0000018E 54              push esp ; 2nd argument to CompareFileTime (our current time)
0000018F 50              push eax ; 1st arg to CompareFileTime
0000018F ; this is the MAX TIME (ffff...)
00000190 FF 56 1C call dword ptr [esi+1Ch] ; call CompareFileTime(currenttime, maxtime)
00000190 ; -1 = First file time is earlier than second file time.
00000190 ; 0 = First file time is equal to second file time.
00000190 ; 1 = First file time is later than second file time.
00000193 48              dec   eax ; decrement the return value
00000194 75 03           jnz  short loc_199 ; if it is non-zero go there
00000196 FF 56 10 call dword ptr [esi+10h] ; if it is ZERO, call ExitThread()
00000196 ; why do they do this? anti-emulation again
00000196 ; most emulators will return 1 by default ;
00000199 FF 56 1C call dword ptr [esi+1Ch] ; call CompareFileTime(currenttime, maxtime)
0000019C 64 8B 19 mov   ebx, fs:[ecx] ; get the PEB
```

Microsoft Corporation | Trustworthy Computing (TWC)
Generations of shellcode- API Hooks

```assembly
6A 1A      push 1Ah
6A 0D      push 0Dh
6A 80      push 0
88 C5      mov eax, ebp
            ; EBP = peb+0x400 = buffer that we just copied data to
            ; ebx = 1 => OSMinorVersion
            ; this is eax = eax+[esp+ebx*4] = eax+[esp+4] = d
            ; (we just pushed D on the stack)
            ; why are they doing this?
03 04 9C  add eax, [esp+ebx*4+4+var_4]
            ; 2wCreateProcessEx
            ; overwrite the first byte to 2wCreateProcessEx with 0x68
            ; 2wCreateProcessEx is actually a syscall
            ; ntdll!2wCreateProcessEx:
            7c90d769 b830000000 mov eax, 30h
            0:000> u @edi L8
            ntdll!2wCreateProcessEx:
            7c90d769 b830000000 mov eax, 30h
            7c90d76e ba0003fe7f mov edx, offset SharedUserData!SystemCallStub (7ffe0300)
            7c90d773 ff12 call dword ptr [edi]
            7c90d775 c22400 ret 2Ah

C6 07 68    mov byte ptr [edi], 68h ; 'h' ; EDI is a function ptr to 2wCreateProcessEx
            ; This is actually change how the function works.. so all 2wCreateProcessEx will be useless
47 inc edi
48 AB       stosd
C6 07 C3    mov byte ptr [edi], 0C3h ; '+' ; put C3 at that byte.. C3 = return
            ; what they are doing here is PATCHING 2wCreateProcessEx
```
The Trojan
The Trojan
The Trojan
Phone Home Methods

(1) DNS Lookup

(2) Response: 60.248.79.226

(3) Control connection

Compromised target

DNS Server

Control server

(1) DNS Lookup

(2) Response: 127.0.0.1

(3) Control connection

Compromised target

DNS Server

Control server
Phone Home Methods: split horizon

Responder

DNS Server

Victim
Case Study
Dear Phuntsok,

I have arrived Nepal safely, don't worry about me. Here is the latest video about the Ihasa conflict recorded by my mobile, I hope it will be useful. The other files about it you can find in my blog.

Regards,
Steve

Ihasa.zip (64.6 KB)
Case Study

- v_080310.asd
  Nokia_7650_video_en.doc

- Connects to uprise.lamaon1.com
- Host name already disabled

Microsoft Security Bulletin MS08-028 – Critical
Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)
Published: May 13, 2008 | Updated: July 16, 2008

Version: 1.3

General Information

Executive Summary
This security update resolves a security vulnerability in the Microsoft Jet Database Engine (Jet) in Windows. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.
April 9, 2008

Drive-by exploit on the web site of a UK organization

This web location

- Identifies the user’s web browser
- Offers an exploit specifically for that version
- Downloads and runs “ipsec.exe” from a server in Taiwan
- Connects to control server:

  freetibet.lamalive.com

This hostname stopped resolving after 48 hours
Case Study

• Five months later

+ 2008-07-12 10:20 | freetibet.lamalife.com | 218.30.103.68
- 2008-08-14 17:46 | freetibet.lamalife.com | 218.30.103.68
+ 2008-09-21 04:16 | freetibet.lamalife.com | 69.64.155.78
- 2008-09-25 06:45 | freetibet.lamalife.com | 69.64.155.78
- 2008-09-26 00:37 | freetibet.lamalife.com | 208.73.210.32

+ 2008-07-12 09:59 | uprise.lamaon1.com | 218.30.103.68
+ 2008-09-21 04:23 | uprise.lamaon1.com | 69.64.155.75
+ 2008-09-25 05:08 | uprise.lamaon1.com | 69.64.155.78
Defense
Roles and opportunities

• Software vendors
  ▪ Opt-in to operating system mitigations
  ▪ Have a defined software incident response process
  ▪ Build security into the development lifecycle

• CERTs, WARPs, ISACs
  ▪ Promote sharing of technical incident information
  ▪ Define a process that allows learning during response

• Enterprise
  ▪ Network deployment & design
  ▪ Intelligence-driven Risk Management
What Microsoft is doing

- **Build secure software**
  - Software Development Lifecycle
  - Significant investment in mitigation technology

- **Improve security response**
  - Information sharing programs (MAPP, DISP)

- **Empower customers**
  - Windows Server: ESC, Core installation
  - MOICE, Office File Validation
  - Forensic and mitigation tools
Office

- Office 2003 SP3 security push

```
<table>
<thead>
<tr>
<th>Microsoft Office Version</th>
<th>MS06-027</th>
<th>MS06-028</th>
<th>MS07-014</th>
<th>MS07-015</th>
<th>MS07-025</th>
<th>MS08-014</th>
<th>MS08-042</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 2000 RTM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Office XP RTM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Office 2003 RTM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Office 2007 RTM</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Office 2000 SP3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Office XP SP3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Office 2003 SP3</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Office 2007 SP1</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```

Source: Security Intelligence Report (2009)

- Office File Validation and Protected View

*Protected View* Office has detected a problem with this file. Editing it may harm your computer. Click for more details.
Exploit mitigations

- Internet Explorer: ASLR Opt-in, DEP Opt-in
- Office: ASLR Opt-in, DEP Opt-in
- Windows: DEP, Heap, ASLR, Heap (v2), SEHOP
- Visual Studio: /GS, /GS (v2), /GS (v3)

Years:
- 2003: VS 2003, SafeSEH
- 2005: VS 2005, /GS (v2)
- 2008: IE 8, Server 2008, Office 2010
- 2009: VS 2010, /GS (v3)
- 2011:
## System Status

- **Data Execution Prevention (DEP)**
  - Always On
- **Structured Exception Handler Overwrite Protection (SEHOP)**
  - Application Opt Out
- **Address Space Layout Randomization (ASLR)**
  - Application Opt In

## Running Processes

<table>
<thead>
<tr>
<th>Process ID</th>
<th>Process Name</th>
<th>DEP</th>
<th>Running EMET</th>
</tr>
</thead>
<tbody>
<tr>
<td>5744</td>
<td>taskeng</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>3888</td>
<td>Ucmapi</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2360</td>
<td>MsitTpmSvc</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>3932</td>
<td>taskhost</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2944</td>
<td>CcmExec</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>1756</td>
<td>sftdcc</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>768</td>
<td>explorer</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>4904</td>
<td>SearchIndexer</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>3524</td>
<td>svchost</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>368</td>
<td>smss</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>1744</td>
<td>AEADISRV</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>560</td>
<td>csrss</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>5316</td>
<td>audioldg</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>6664</td>
<td>iexplore</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2920</td>
<td>SynTPLpr</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>4692</td>
<td>SynTPEnh</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>944</td>
<td>MsMpEng</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>548</td>
<td>wininit</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>540</td>
<td>svchost</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
EMET: Heap spray pre-allocation
MAPP program
Enterprise
Mitigation framework

- **Compromise**
  - E-mail server
  - Compromised machine

- **Infiltration**
  - Web proxy
  - Control server

- **Exfiltration**

- **Data Access**
Mitigation framework

Basic:
• E-mail security policy
• Security awareness training
• Filter external e-mails from the organizational domain

Enhanced:
• Employ Sender-ID or SPF technology
• Enhanced awareness training for high value targets
• Sharing intelligence on attack patterns

Strong:
• Digitally sign e-mails
• Web site whitelisting
Mitigation framework

Basic:
- Anti-virus deployed on the gateway
- Blocking suspicious attachment types
- Spam filtering

Enhanced:
- Re-scan previously accepted attachments on the mail server

Strong:
- Dynamic execution and validation of attachments
- Web site whitelisting
Mitigation framework

**Basic:**
- Anti-virus
- Security updates
- Reduce user privileges on the system
- Disable document macros

**Enhanced:**
- Anti-virus with Host Intrusion Prevention
- Enable DEP and SEHOP system-wide
- Harden applications (e.g. block Javascript execution)
- Use MOICE for Office document security
- Office File Validation

**Strong:**
- Deploy EMET for internet-facing applications
- Application whitelisting
Mitigation framework

Basic:
- Log access to data resources
- Deploy split horizon DNS

Enhanced:
- Audit access to data resources
- Deploy Extended Protection for Authentication (EPA)
- Correlate data access with network logins

Strong:
- Multi-factor authentication
- Segregation of data stores and untrusted network access
Mitigation framework

Basic:
• Log access to web sites
• Block outbound network access
• Use of a content-aware web proxy

Enhanced:
• Exchange information with CERTs, law enforcement and/or industry partners
• DNS monitoring, correlation and log analysis
• Black-list access to specific web sites
• Deploy DRM and/or data loss prevention tools

Strong:
• White-list access to specific web sites
Thank you!

Maarten Van Horenbeeck
maarten.vanhorenbeeck@microsoft.com

Featuring work by:

Bruce Dang
Jonathan Ness
Matt Miller

Microsoft Security Response Center
secure@microsoft.com
http://www.microsoft.com/security

© 2011 Microsoft Corporation. All rights reserved. Microsoft and Microsoft Office are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.