» The **Patcher** Case«

Peter Kruse (pkr@csis.dk), Head of CSIS eCrime and Research & Intelligence Unit

PGP-ID: 0x715FB4BD
Agenda – Patcher

» What is Patcher?
» Patcher naming?
» Man in The Browser functions
» Patcher – fresh variants with new twists
» Patcher – Domain Generating Algorithm (DGA)
» Blind drop data transport overview
» Infrastructure and C&C setup
» Point of infection, Ecosystem and affiliates
» Separation of duties
» Money Mule campaign
» Statistics
» How we battled them and challenges
What is Patcher?

» Highly complex Banker-Trojans

» Patcher is a “User land Kernel Rootkit” modifying several critical Windows system files in the past (current versions modify only in memory).

» Installs BHO (Browser Helper Object).

» The biggest isolated and targeted attack against Denmark ever – with more than 50,000 unique infections counted since September 2008.

» Tailor made for certain eBanking applications and very capable of performing complex Man in The Browser (MiTB) functions.

» Patcher was the first - and for now the only malware family to utilize “Man in The Java”
What is Patcher?

» Many variants, low AV-detection

» Involved in at least two large incidents stealing more than 2 mill. DKK from SMB sized Danish companies (that is approx. EUR 275,000).

» Highly motivated IT-criminals with technical knowledge covering several different technologies spanning from Assembler, C++, TCP/IP, database and PHP.

» Also involved in attacks aimed against: Holland, Greece, US, Ireland and Germany

» Uses a domain name generating algorithm similar to Torpig/Sinowal/Anserin/Mebroot.
Patcher naming

We named it Patcher on account of its functionality. Patching system files. Other names used for this malware family include:

» Trojan-Banker.Win32.Banker
» TR/Banker.MultiBanker
» W32/Banker
» PSW.Banker5
» Trojan-Banker.Win32.MultiBanker
» TrojanSpy:Win32/Nadebanker

» Hacktool/Patcher
» PWS-Banker
» Trojan-Banker.Win32.Banker
» Win32:Patched
» Win32/Spy.Bankpatch
Patcher naming?

Patcher was actively patching four system files:

» dnsapi.dll (implemented Q3 2009)
» kernel32.dll
» powrprof.dll
» wininet.dll
Patcher – why the name?

» Installs keylogging functionality

» Grabs keylog data + entire traffic sessions related to targets + HTTPS sessions hooked “below” encryption level

» Contains a constantly updated list of approx. 140 targets on which it activates form and content grabbing.

» Installs itself and ensures that it starts on reboot by adding to:
  “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon”
  “[%windows systemfolder%]\userinit.exe, [%windows systemfolder%]\appconf32.exe,“

» Hooks into all processes - except some predefined;
  (Primary security/AV applications).

» Instead of previous versions, where the group physically patched “wininet.dll”, “kernel32.dll”, “Powrprof.dll”, they are now doing this in memory like ZeuS/Zbot and SpyEye (!).
Patcher – Man in the Browser

When Patcher is installed it detects which browser is default e.g. IE or FF.

» If IE is default browser a dedicated BHO is installed and Java is uninstalled

» Anything besides IE part of the JRE is uploaded to the gang, modified and returned

» Patcher camouflage transactions to give a broader “Window of opportunity”

» Stores balances locally to hide that money was transferred from account

```
lea    eax, [esp+574h+var_520]
push   eax
mov    edi, offset aTDolspan$Summ ; "<td colspan="5">Summe Haben</td>"
call   sub_10002745
and    [esp+574h+var_4], 0
lea    eax, [esp+574h+var_524]
push   eax
mov    edi, offset aTDolspan$Su_0 ; "<td colspan="5">Summe Soll</td>"
call   sub_10002745
lea    eax, [esp+574h+var_520]
push   eax
mov    edi, offset aTDolspan$Str" ; "<td colspan="5"><strong>Gesamtsaldo</strong></td>"
call   sub_10002745
lea    eax, [esp+574h+var_516]
push   eax
mov    edi, offset aKontenUndKarte ; "Konten und Karten</a></th>"
call   sub_10002745
lea    eax, [esp+574h+var_538]
push   eax
loc_10001707: ; Src
push   ecx
mov    eax, esp
mov    [esp+578h+var_560], esp
push   eax
mov    edi, offset aTotalParsed ; "total parsed"
call   sub_10002745
call   sub_10002F6
push   ecx
mov    eax, esp
mov    [esp+578h+var_560], esp
lea    edi, [esi-28h]
push   eax
```

10-06-2011
Patcher – fresh variants with new twists

» Avoiding infecting DLLs
» Hooking API in memory and inject threads into browser processes

“\textit{Down\&update}” function reveals the “Domain Generating Algorithm” (DGA) in action:

GET request for the file "lodupgd.jpg" using user-agent:
"Opera/11.1 (Windows NT 5.1: U: en)"

Regkeys in “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\” are:

Internet Settings\ver: "400"
Internet Settings\vendor: "Old"
Internet Settings\prd: "http://kwojstasche.com"
Internet Settings\w8: "USA_MDAwMDAwMDAwMDAwMDAwMTA="
Internet Settings\prh\prh: "http://kwojstasche.com"
Patcher – Domain Generating Algorithm (DGA)

» Patcher installs hooks in `wininet.dll`
» Patcher drops “`wincode.dat`” and injects it into `wininet.dll`
» Upon loading `wininet.dll`, and calling for instance, `InternetCrackUrl`, the changed library will resolve API functions based on unique function hashes, and load the `wincode.dat` into memory.
» It then proceeds with the unpacking of its contents using the following algorithm:

```plaintext
roughly translated pseudo-code:
xor_key = contents[0]
for (i = 1; i < len(contents); i++)
    current = contents[i] ^ xor_key
    xor_key = ror(xor_key,1)
    contents[i] = current
```

```plaintext
wininet.dll:76296A80
wininet.dll:76296A80  loc_76296A80:
wininet.dll:76296A80  mov al, [edi]
wininet.dll:76296A82  xor al, cl
wininet.dll:76296A84  ror cl, 1
wininet.dll:76296A86  stosb
wininet.dll:76296A87  dec edx
wininet.dll:76296A88  jnz short
```
Patcher – Domain Generating Algorithm (DGA)

» Next it reads the content of the decrypted wincode.dat at offset 0x18 and then reads the Patcher base domain added to registry.

» Finally the code creates multiple threads, one of which is responsible for generating additional domains according to this variant’s algorithm.

» Based on this behavior we designed a tool which performs a crypto-attack on the contents of the binary and this way we can predict future domains.

» Finally: Gone sinkholing ...
Patcher – Blind drop transport

Files are stored locally until they can be delivered to either of the C&Cs.
Patcher - Infrastructure

The backend webservice validates the client and the request resources before passing along. If the request does not compile or if VMware is detected, the IP gets blacklisted.

The firewall allows specific hosts to access the backend.
Patcher - Infrastructure

The backend is designed with MySQL and uses the structure below:

- Apps
- Appsdb
- Auto_balances
- Auto_drops
- Auto_wires
- Black
- Bots
- Guids
- Hide_ejb
- Hide Ny
- Hosts
- Loads
- Tasks
- Tasks_del
- Tasks_hide
- Test_table

The Database consists of the following 16 tables:
Patcher – Infrastructure (C&C domains)

As already demonstrated Patcher uses DGA for rotation. Active base domains:

- minmont.com
- glam.com
- syskland.com (Danish word for Germany)
- irish.com
- anta.com
- newnacion.com
- ancldnk.com
- stug.com
- volveras.com
- stasche.com
- nema.com
- sbaks.com
- newdnkas.com
Patcher - Point of infection - Ecosystem

Location of user: Germany, Ukraine

Payload: Trojan

Malicious site: Phoenix Exploit's Kit

Iframe redirect: New site users exploited through OpenX banners
Patcher – Point of infection - Ecosystem

The Patcher group is not handling the infection themselves. They have “outsourced” this part to certain “Pay-per-install/Iframe trafficker” services.

Some of the vendors have previously been used by the Torpig gang, especially an individual using the handle “JaguarC”

So far the Patcher gang has been using the following “vendors”:

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Vendor</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC_DK</td>
<td>JagUarcIE2</td>
<td>TraffUS2</td>
</tr>
<tr>
<td>CeoTraff</td>
<td>JagUarcIE3</td>
<td>Yaguar</td>
</tr>
<tr>
<td>CorvIE</td>
<td>JagUarcIE4</td>
<td>ZargusDK</td>
</tr>
<tr>
<td>ie7exp</td>
<td>JagUarcUS1</td>
<td>ZargusDK2</td>
</tr>
<tr>
<td>ieexp</td>
<td>Odd</td>
<td>ZargusDK3</td>
</tr>
<tr>
<td>JagUarcDK</td>
<td>SCashDK1</td>
<td>ZargusDK4</td>
</tr>
<tr>
<td>JagUarcDK4</td>
<td>SCashIE1</td>
<td>ZargusDK5</td>
</tr>
<tr>
<td>JagUarcDK5</td>
<td>SCashUS1</td>
<td>ZargusDK6</td>
</tr>
<tr>
<td>JagUarcDK6</td>
<td>SCashUS2</td>
<td>ZargusDK7</td>
</tr>
<tr>
<td>JagUarcDK7</td>
<td>Traff</td>
<td>ZargusIE1</td>
</tr>
<tr>
<td>JagUarcIE</td>
<td>TraffUS</td>
<td></td>
</tr>
</tbody>
</table>

10-06-2011
Patcher – Separation of duties

Bank specific add on .dll

Bank A
Account Balance: + € 50,000

Bank B
Account Balance: + € 65,000
Money Mule campaign

Financial assistant, home employment

Xoom Global Money Transfer
(Not a real job listing)

Job title: Financial assistant
Tasks: Managing and monitoring customer accounts, handling customer inquiries, and managing financial documents.

Job requirements:
- At least 2 years of experience in customer service
- Fluent in English and Danish
- Ability to handle multiple tasks simultaneously

Salary: 15000-22000 DKK (variable)

Closing date: 18000000

Contact: (phone number)
Statistics on distributed Patcher samples 2011

- January: 50
- February: 70
- March: 120
- April: 180
- May: 150
- June: 40
Patcher – Amount of infections

As of 1-03-2011 the infection stats look like this:

- DE: 30000
- US: 25000
- DK: 10000
- ES: 5000
- IE: 2000
- GR: 1500
- CY: 1000
- NL: 500
- SE: 200
- IS: 100
Patcher – How we battled them!

» By doing static analysis on the code and infecting PCs to observe any changes (dynamic approach).

» We worked 24/7 putting pressure on the hosting providers – flooding their online forums and chats with requests, spammed their abuse boxes and constantly phoned them. They didn’t like that very much!

» Shared information and worked closely together with the AV-industry and the security community in general.

» We worked closely together with local LE and ISPs to do a coordinated null-route of all known active C&C and drop servers, closely synchronized with the sinkhole project.

» Released a free detection tool to spot all known variants of this specimen (https://www.csis.dk/dk/media/Detector.zip). More than 1,002,137 downloads so far!
Patcher – Challenges in the battle!

International corporation could be improved.
» Bullet-proof hosting.
» Getting all the binaries from the C&C.
» International LE involvement (progress is slow).
  » Finding bank suffering loss.
  » Contact LE in that country.
  » LE needs to contact Interpol.
  » Interpol needs to contact LE.
  » LE needs to contact ISP/Hosting.