Cracking Xpaj: code and payload

Andrea Lelli

Senior Software Engineer

Security Response

Agenda

- File infection
- Code encryption & obfuscation
- Network communication
- Payload functionality
- Conclusion

Introduction

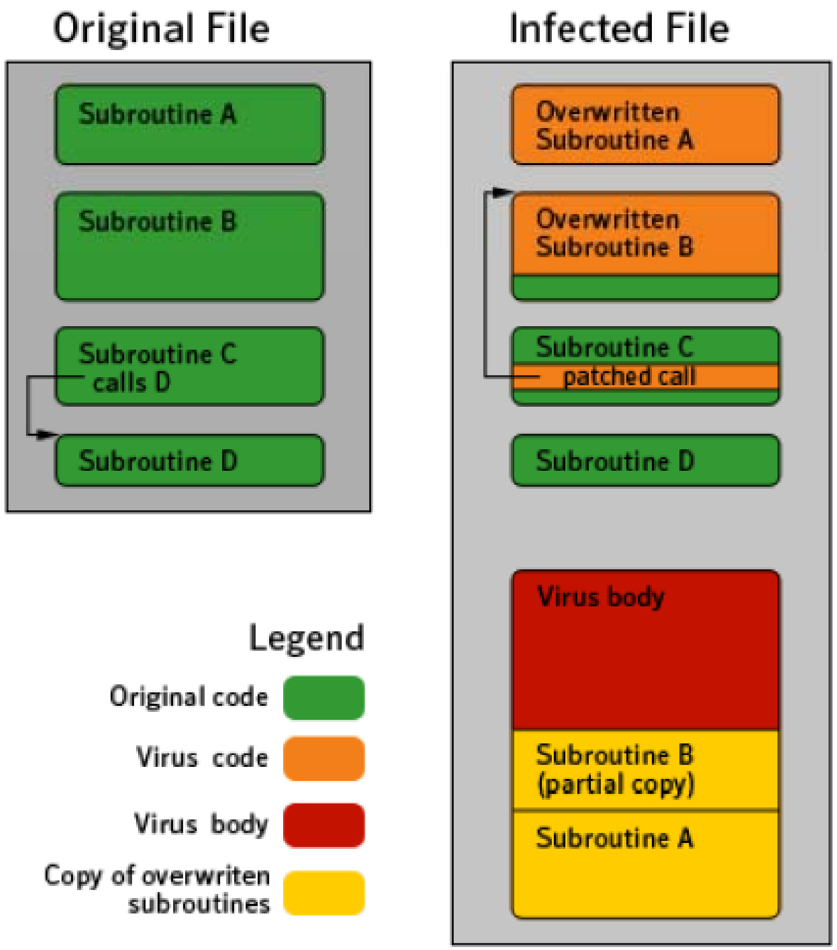
- Xpaj.B is difficult to:
  - Detect
  - Repair
  - Analyze

- Complex infrastructure
  - Encrypted communication
  - Ad-clicking scam

- Shows periodic evolution

File infection

User mode infector

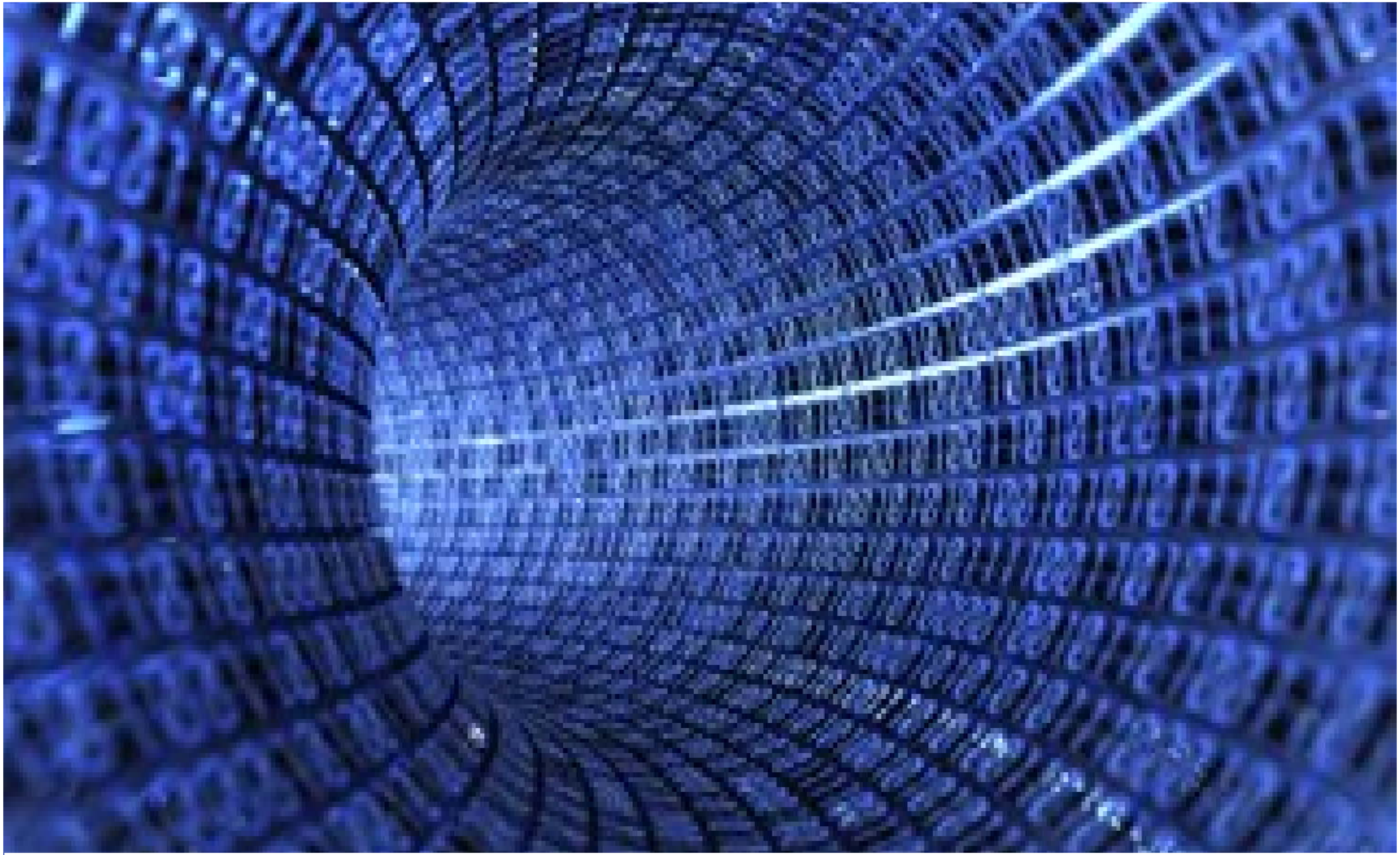


- Infects random subroutines
- Variable size
- Virus body is fully encrypted
- Appends itself to an existing section (usually the end of .data)
- Virus body position is randomized, placed inside random data
- Original code is buried within the body virus

Kernel mode infector

- Kernelmode code exists in the virus
  - used for injecting a thread into new processes
  - Injected thread will
    - Download updates from C&C
    - Spread over network/removable drives

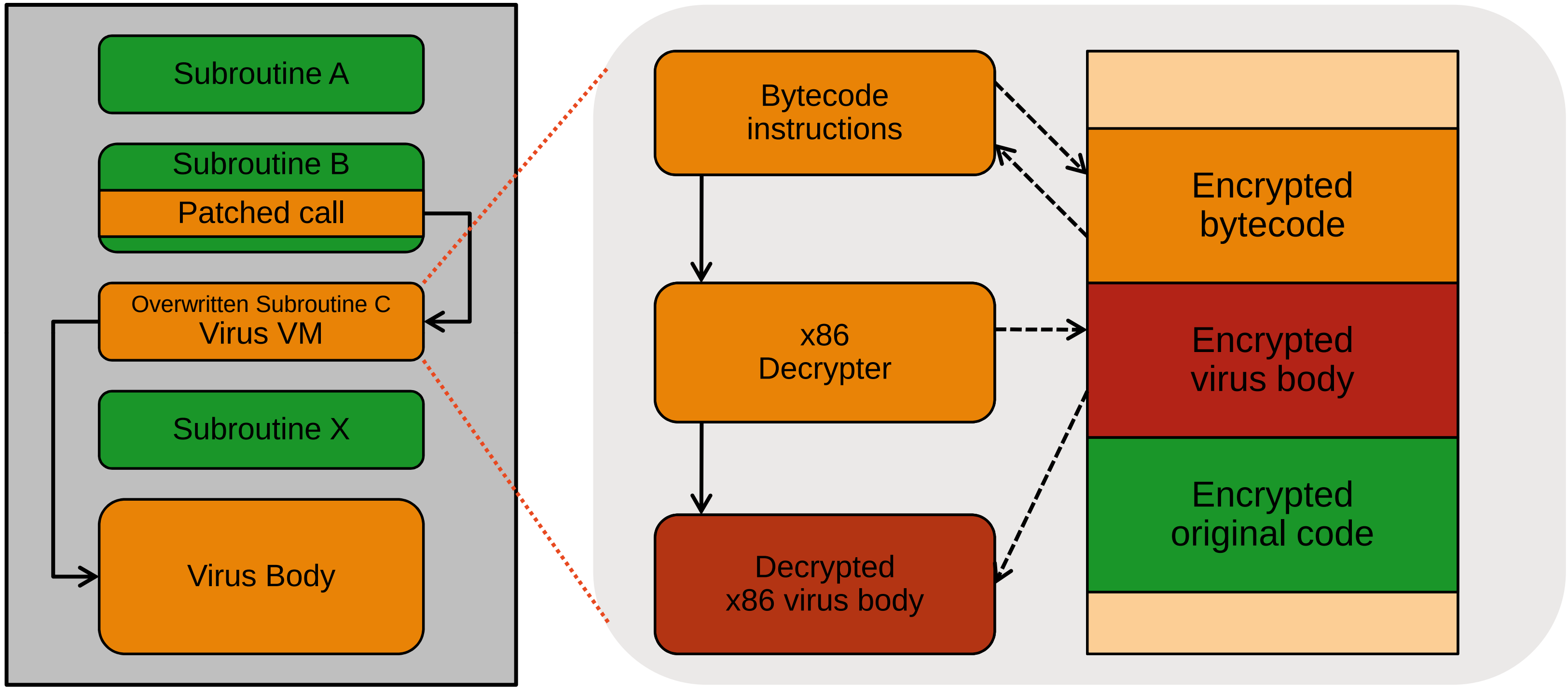
- Xpaj does search and parse drivers, but:
  - It specifically avoids their infection
  - No infected drivers have been observed



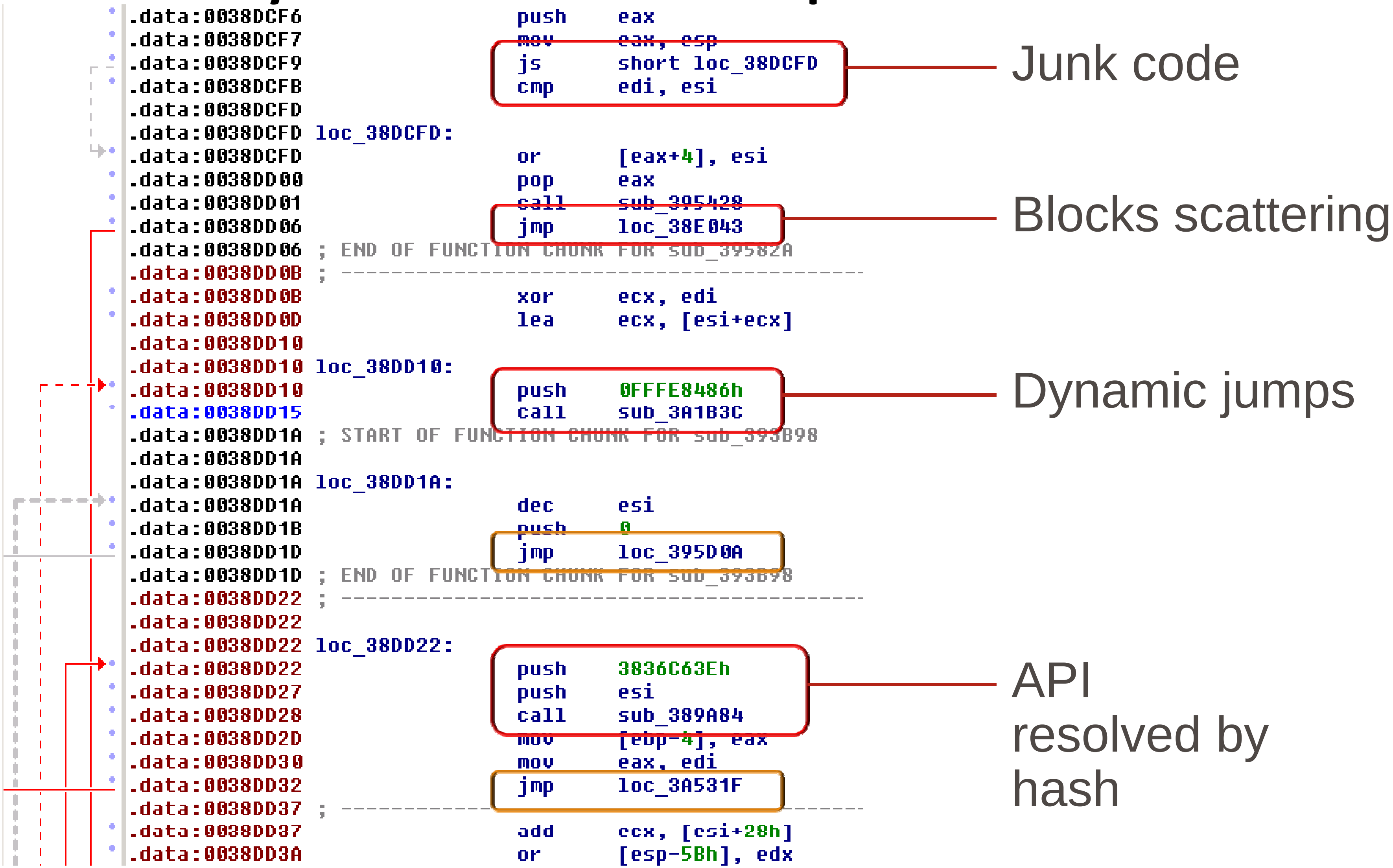
Code encryption & obfuscation

First layer: stack based virtual machine

- Infection entry points are calls to the VM
- VM code and handlers are obfuscated
- Bytecode and viral body are encrypted



Second layer: obfuscation example



```
.data:0038DCF6                 push    eax
.data:0038DCF7                 mov     eax, esp
.data:0038DCF9                 js      short loc_38DCFD
.data:0038DCFB                 cmp     edi, esi
.data:0038DCFD
.data:0038DCFD loc_38DCFD:
.data:0038DCFD                 or      [eax+4], esi
.data:0038DD00                 pop     eax
.data:0038DD01                 call    sub_395428
.data:0038DD06                 jmp     loc_38E043
.data:0038DD06 ; END OF FUNCTION CHUNK FOR sub_39582A
.data:0038DD0B ; ---------------------------------------------
.data:0038DD0B                 xor     ecx, edi
.data:0038DD0D                 lea     ecx, [esi+ecx]
.data:0038DD10
.data:0038DD10 loc_38DD10:
.data:0038DD10                 push    0FFFE8486h
.data:0038DD15                 call    sub_3A1B3C
.data:0038DD1A ; START OF FUNCTION CHUNK FOR sub_393B98
.data:0038DD1A
.data:0038DD1A loc_38DD1A:
.data:0038DD1A                 dec     esi
.data:0038DD1B                 push    0
.data:0038DD1D                 jmp     loc_395D0A
.data:0038DD1D ; END OF FUNCTION CHUNK FOR sub_393B98
.data:0038DD22 ; ---------------------------------------------
.data:0038DD22
.data:0038DD22 loc_38DD22:
.data:0038DD22                 push    3836C63Eh
.data:0038DD27                 push    esi
.data:0038DD28                 call    sub_389A84
.data:0038DD2D                 mov     [ebp-4], eax
.data:0038DD30                 mov     eax, edi
.data:0038DD32                 jmp     loc_3A531F
.data:0038DD37 ; ---------------------------------------------
.data:0038DD37                 add     ecx, [esi+28h]
.data:0038DD3A                 or      [esp-5Bh], edx
```

Junk code

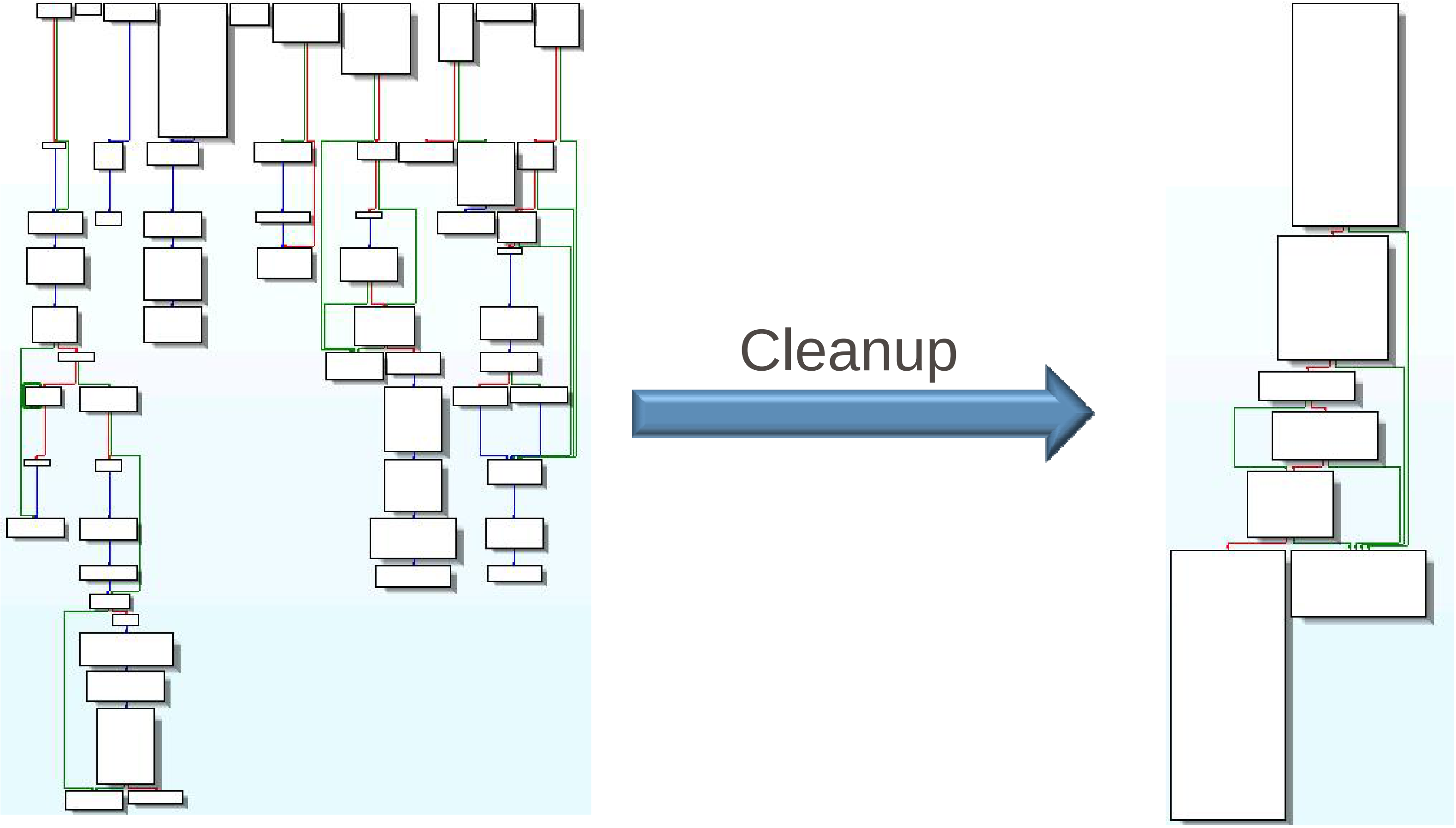
Blocks scattering

Dynamic jumps

API
resolved by
hash

Second layer: obfuscation example

Just to give you an idea:



Cleanup

Obfuscated

Deobfuscated

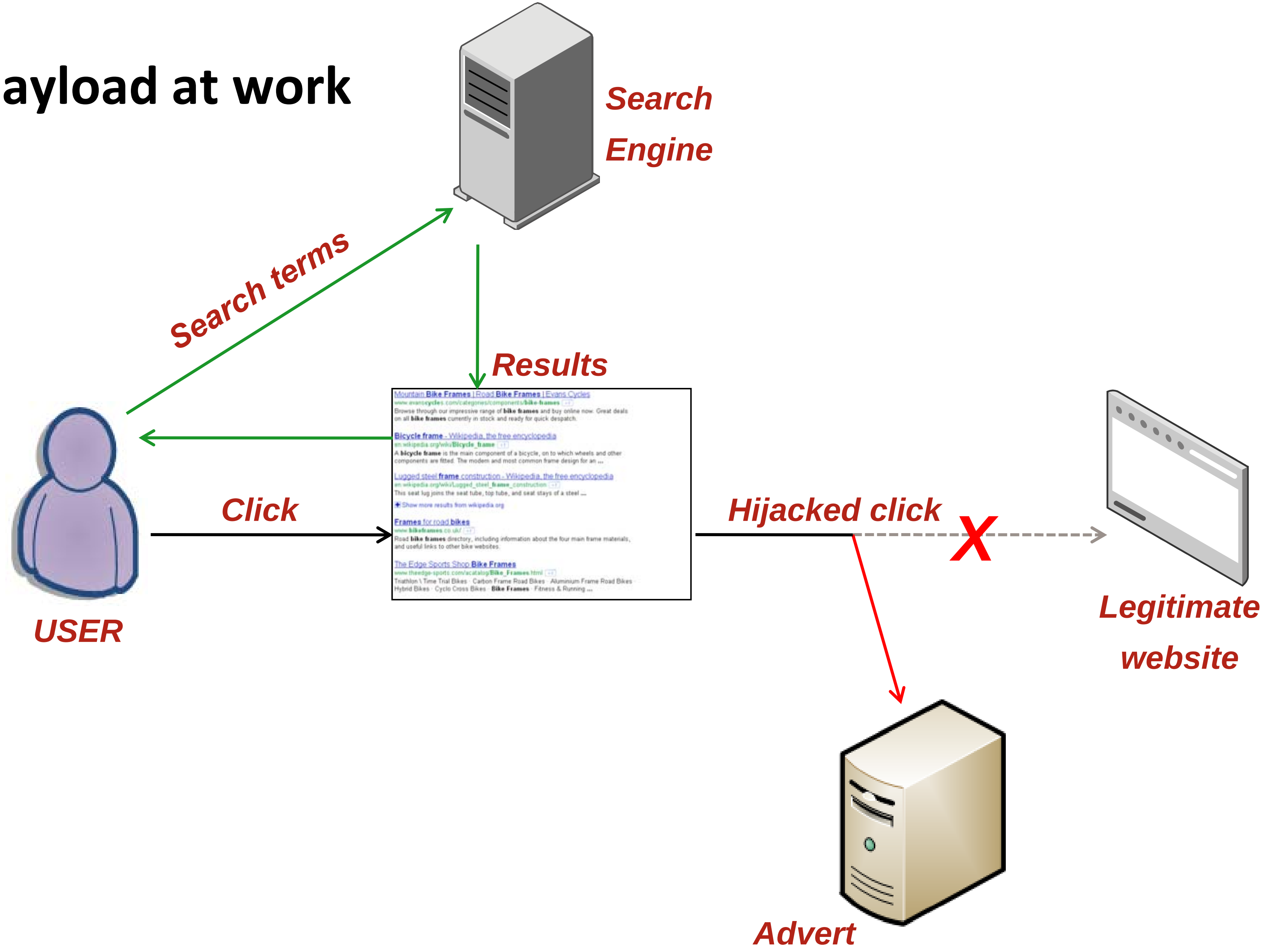
Network Communication

C&C Communication

- C&C address in embedded configuration
  - send/receive data BLOBs
- Pseudo-random domain generator
- BLOBs are encrypted and verified
- BLOBs may contain:
  - New configuration data
  - Updated worm binary
  - Payload DLLs
  - Infection tracking information
  - Data about search terms hijacking

Payload functionality

Payload at work



Mountain **Bike Frames** | Road **Bike Frames** | Evans Cycles
www.evans**cycle**s.com/categories/components/**bike-frames**
Browse through our impressive range of **bike frames** and buy online now. Great deals on all **bike frames** currently in stock and ready for quick despatch.

Bicycle frame - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/**Bicycle_frame**
A **bicycle frame** is the main component of a bicycle, on to which wheels and other components are fitted. The modern and most common frame design for an ...

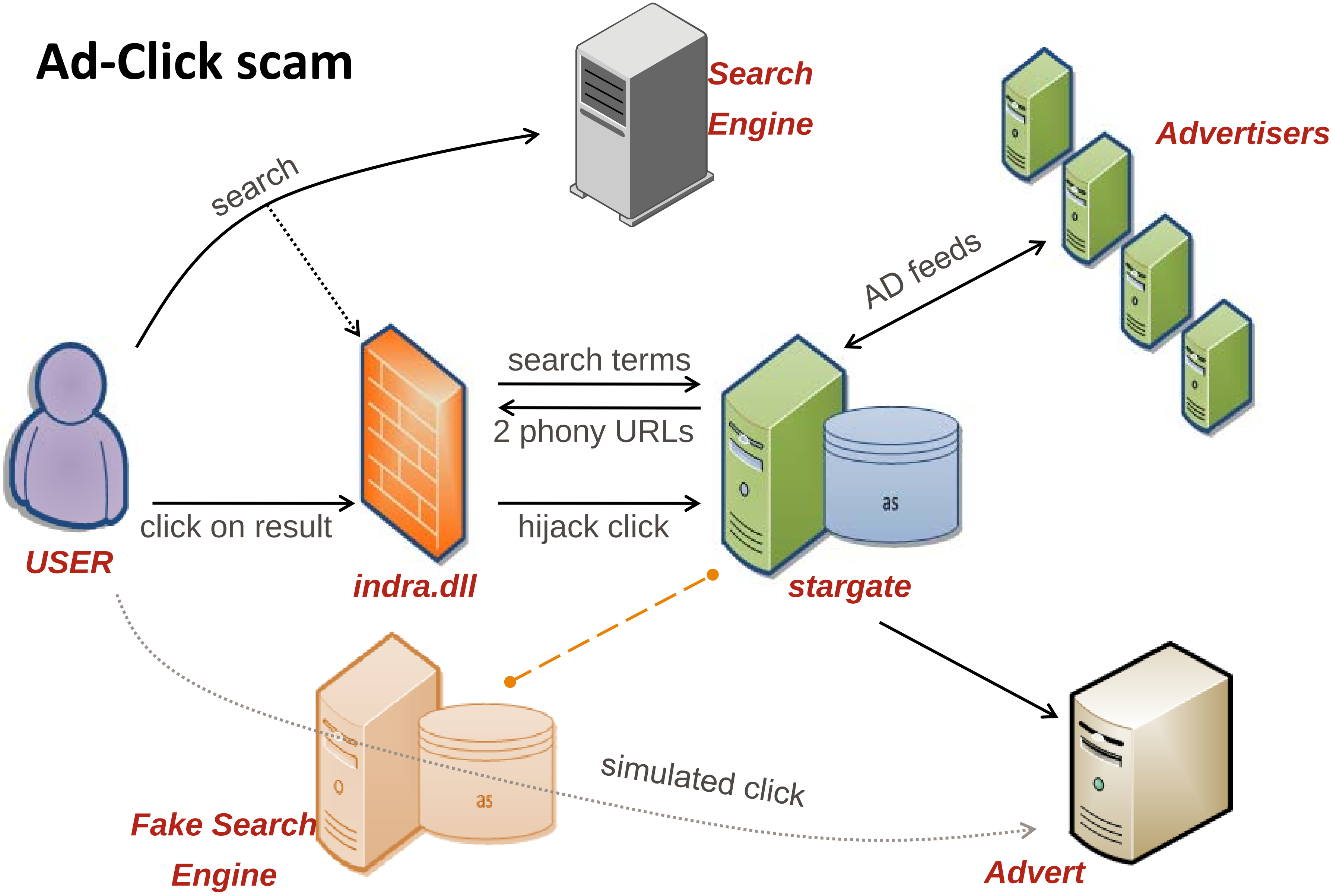
Lugged steel **frame** construction - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Lugged_steel_**frame**_construction
This seat lug joins the seat tube, top tube, and seat stays of a steel ...

Show more results from wikipedia.org

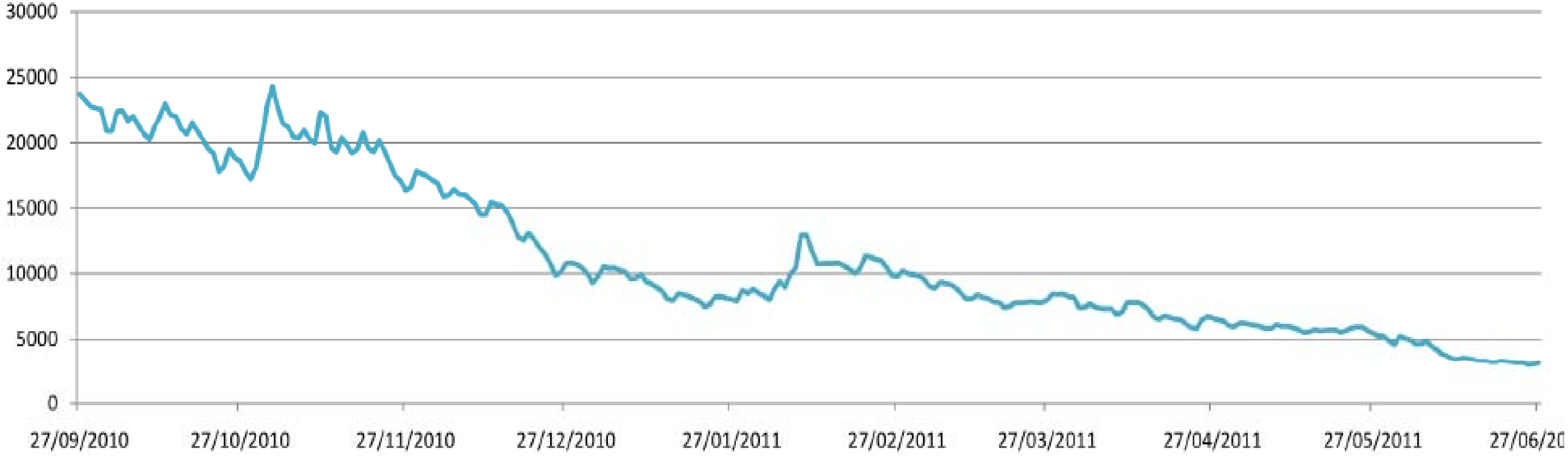
Frames for road **bikes**
www.**bikeframes**.co.uk/
Road **bike frames** directory, including information about the four main frame materials, and useful links to other bike websites.

The Edge Sports Shop **Bike Frames**
www.theedge-sports.com/acatalog/**Bike_Frames**.html
Triathlon \ Time Trial Bikes · Carbon Frame Road Bikes · Aluminium Frame Road Bikes · Hybrid Bikes · Cyclo Cross Bikes · **Bike Frames** · Fitness & Running ...

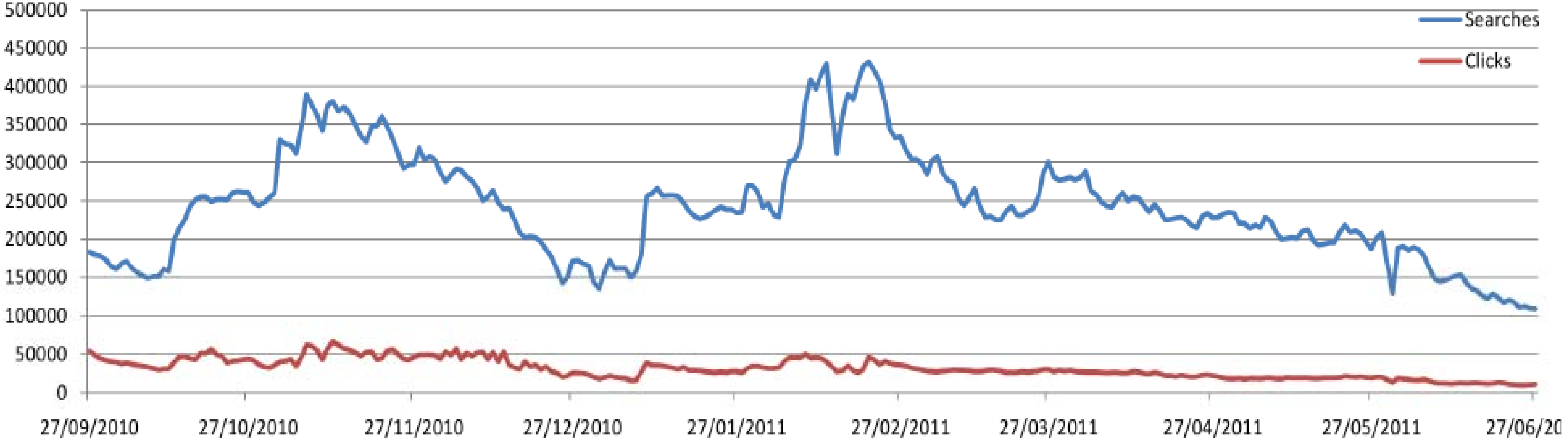
Ad-Click scam



Number of unique IP connections per day

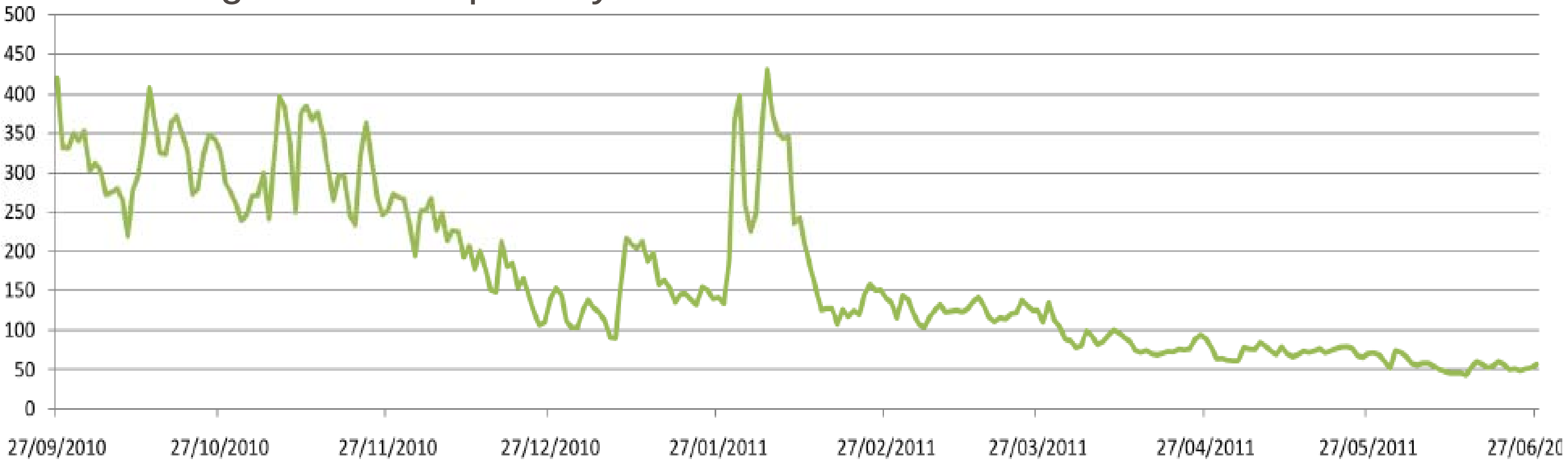


Number of clicks and searches over time



Inside the C&C server: AdClicking scam

Earnings over time per day in USD



Total earnings in observed period of time: $46404

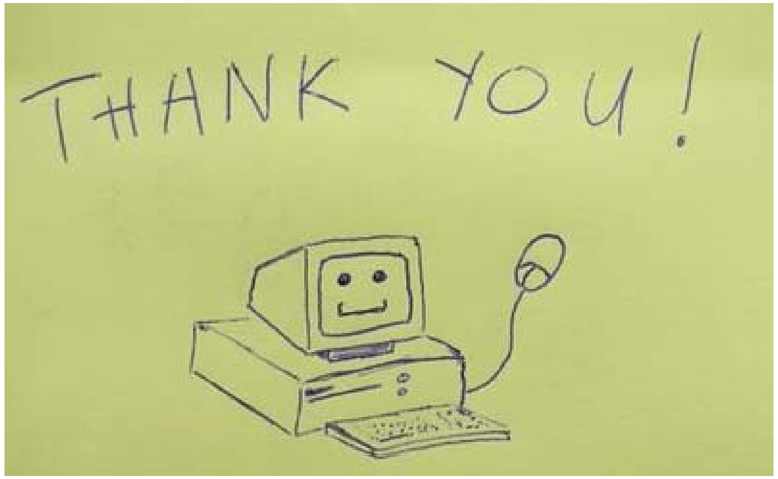
Conclusion

Conclusion

- In time Xpaj added:
  - Encryption of virus body
  - Virtual Machine
  - Compression

- In the future?
  - Kernelmode infection
  - P2P functionality
  - Parse Http commands

... maybe!



This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Questions

Reference

A detailed whitepaper about W32.Xpaj.B is available from Symantec’s website:

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_xpaj_b.pdf