THE ANSWER TO THE QUESTION **"WHO?"** WAVES OF VICTIMS OF THE ATTACKS MORE THAN AN ANSWER TO THE QUESTION **"HOW?"**

KASPERSKY lab

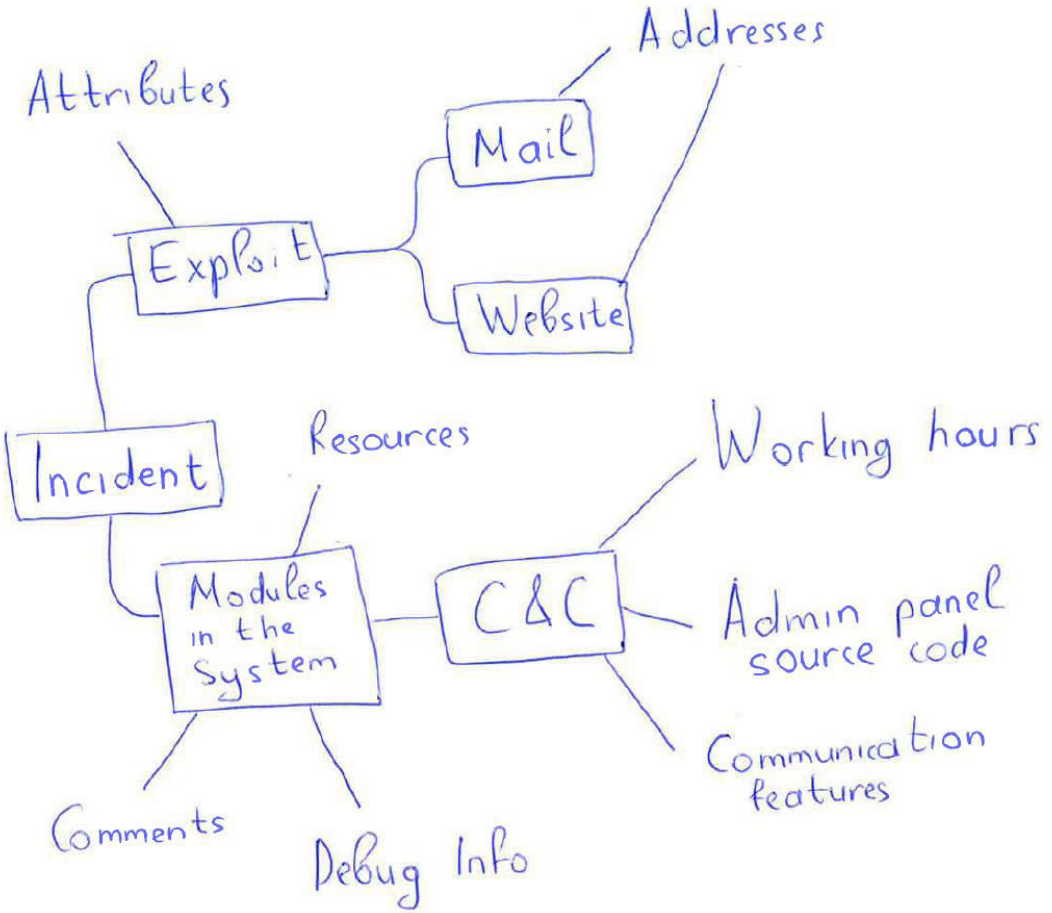
TRUE DETECTIVE
FROM APT ARTIFACTS TO ONE FINGERPRINT

Denis Makrushin (@difezza), Maria Garnaeva
Global Research and Analysis Team

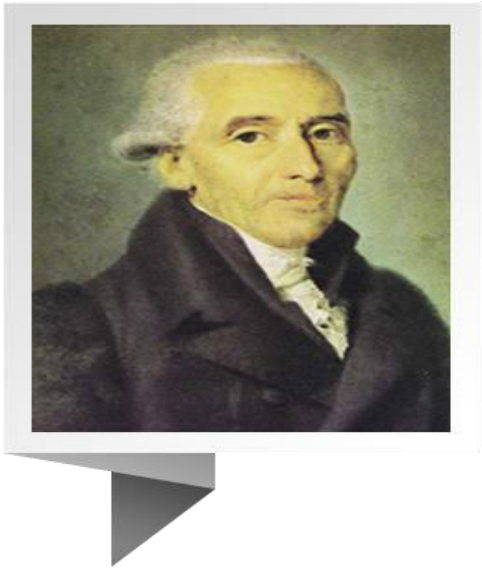
KASPERSKY lab

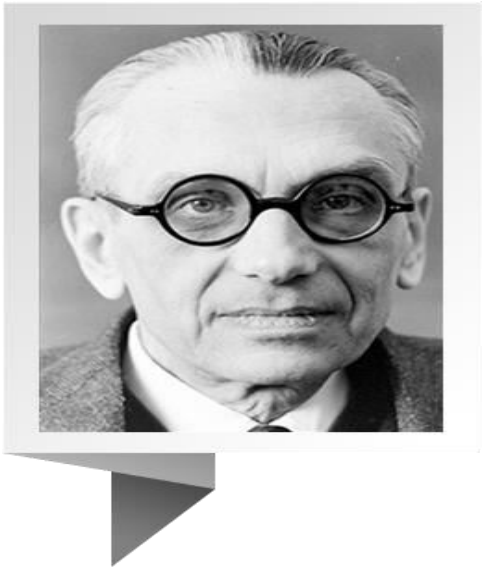
ARTEFACTS OF AN ATTACK

- Address of the sender
- Address of the servers
- Debug information
- Resources
- Comments
- C2s Content
- Communication
- **Linguistics and spelling**

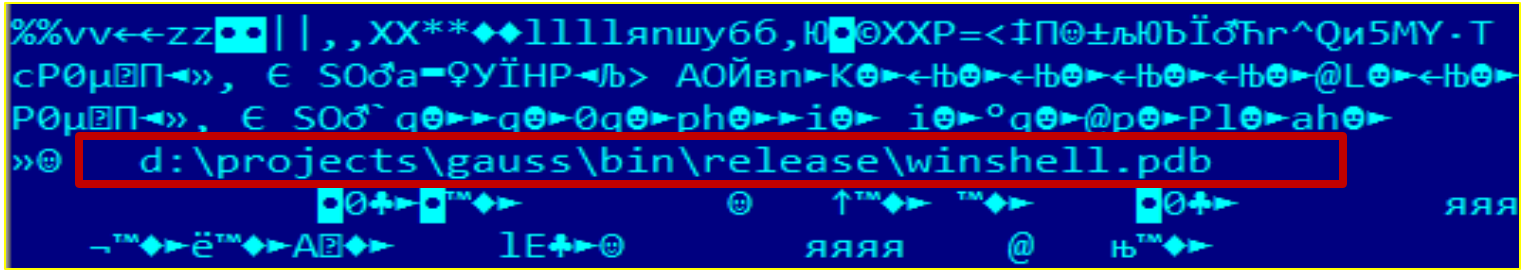


2012 – Gauss





Gauss (debug info)



Вариант	Path to project files
August 2011	d:\projects\gauss
October 2011	d:\projects\gauss_for_macis_2
Dec 2011-Jan 2012	c:\documents and settings\flamer\desktop\gauss_white_1

Gauss (debug info)

c:\documents and settings\flamer\desktop\gauss_white_1\utils\Exceptions.h
.\Manager.cpp c:\documents and settings\flamer\desktop\gauss_white_1\utils\SmartPtr.h
.\Injector.cpp
c:\documents and settings\flamer\desktop\gauss_white_1
\gauss\../Utils/ComUtils.h
.\History.cpp
.\FirefoxPluginInstaller.cpp
.\Telemetry.cpp .\Storage.cpp .\OsUtils.cpp .\ProcessSnapshot.cpp .\Event.cpp
.\GaussThread.cpp .\Buffer.cpp .\RemoteMemoryBuffer.cpp .\File.cpp .\Mutex.cpp .\Waiter.cpp
.\EveryoneSecurityAttributes.cpp .\Catcher.cpp .\BrowserConnector.cpp
c:\documents and settings\flamer\desktop\gauss_white_1
\minime\../Utils/SmartPtr.h .\Assigner.cpp .\IEAbstractElements.cpp .\FormExtractor.cpp
.\COMAbstractDataTypes.cpp

Gauss

Etymology [edit]

The name *Lebanon* comes from the Semitic root *LBN* (لبن), meaning "white", likely a reference to the snow-capped Mount Lebanon.[14]

Occurrences of the name have been found in different texts from the library of Ebla,[15] which date to the third millennium BC, nearly 70 times in the Hebrew Bible, and three of the twelve tablets of the Epic of Gilgamesh (perhaps as early as 2100 BC).[16]

The name is recorded in Ancient Egyptian as *Rmnn*, where *R* stood for Canaanite *L*.[17]

Gauss

- Home
- Organization
- Submission
- Program
- Registration
- Accommodation

MACIS 2011: Fourth International Conference on Mathematical Aspects of Computer and Information Sciences

MACIS is a series of conferences where foundational research on theoretical and practical problems of mathematics for computing and information processing may be presented and discussed. MACIS also addresses experimental and case studies, scientific and engineering computation, design and implementation of algorithms and software systems, and applications of mathematical methods and tools to outstanding and emerging problems in applied computer and information sciences. Each conference focuses on two or three themes.

Important Dates

Submission of papers/extended abstracts	August 10, 2011 (EXTENDED)
Notification of acceptance or rejection	September 5-11, 2011
Conference taking place	October 19-21, 2011
Deadline for full paper submission	December 15, 2011

Follow-up Special Issue of Mathematics in Computer Science (MCS)

See here for further details.

2012 – miniFlame
“Elvis” and his friends

KASPERSKY lab

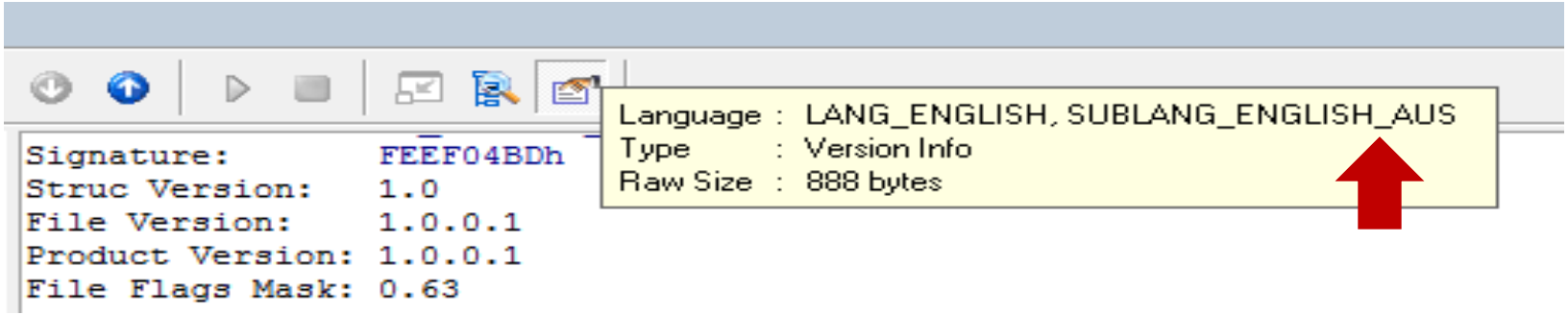
miniFlame (resources)

In all the 4.x versions, the developers used the same “version info” file.

```
Length Of Struc: 0378h
Length Of Value: 0034h
Type Of Struc:   0000h
Info:            VS_VERSION_INFO
Signature:       FEEF04BDh
Struc Version:   1.0
File Version:    1.0.0.1
Product Version: 1.0.0.1
File Flags Mask: 0.63
File Flags:
File OS:         NT (WINDOWS32)
File Type:       DLL
Language/Code Page: 3081/1200
CompanyName:         Microsoft Corporation
FileDescription:     icsvnt32
FileVersion:         1, 0, 0, 1
InternalName:        icsvnt32 (or icsvntu32 for U-module)
LegalCopyright:      Copyright ? 2010
LegalTrademarks:
OriginalFilename:    icsvnt32.ocx  (or icsvntu32 for U-module)
PrivateBuild:
ProductName:         Microsoft Corporation icsvnt32  (or icsvntu32 for U-module)
ProductVersion:      1, 0, 0, 1
SpecialBuild:
Child Type:          VarFileInfo
Translation:         3081/1200
```

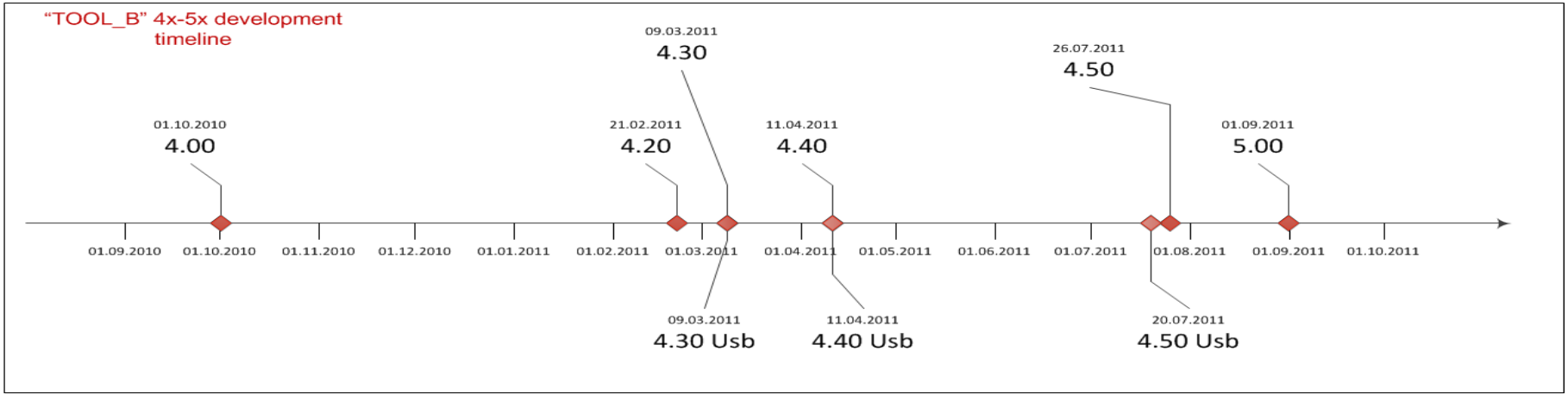
KASPERSKY lab

miniFlame (resources)



ENGLISH_US NEUTRAL

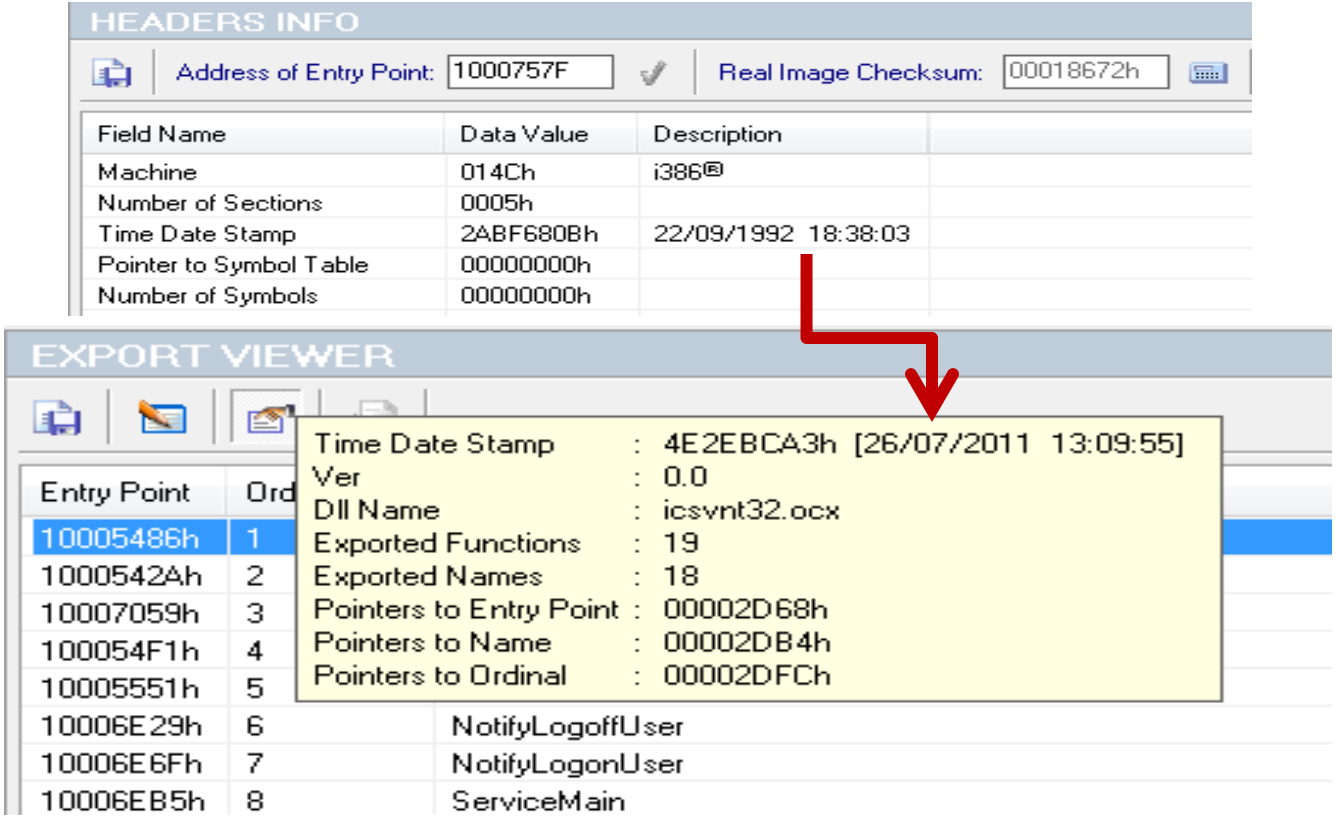
miniFlame (resources)



ENGLISH_US

KASPERSKY lab

miniFlame (resources)



miniFlame (debug)

4D629B52: 21/02/2011 17:05:22

C:\projects\e\SP4.2\general_vob\sp\Release\icsvnt32.pdb

miniFlame (debug)

IBM Rational ClearCase

From Wikipedia, the free encyclopedia

The **Rational ClearCase** family consists of several software tools for supporting software configuration management (SCM) of source code and other software development assets. It is developed by the Rational Software division of IBM. ClearCase forms the base for configuration management for many large and medium sized businesses and can handle projects with hundreds or thousands of developers.

A part of Rational ClearCase is revision control system, which is a feature for end users.

ClearCase supports two kinds of use models, UCM (Unified Change Management), and base ClearCase. UCM provides an out-of-the-box model while base ClearCase provides a basic infrastructure (upon which UCM is built). Both can be configured to support a wide variety of needs. UCM is part of RUP (Rational Unified Process) and therefore all process templates and roles can be used from RUP.

ClearCase can run on a number of platforms including AIX, z/OS, Linux, HP-UX, Solaris, and Windows.[1] It can handle large binary files, large numbers of files, and large repository sizes. It handles branching, labeling, and versioning of directories.

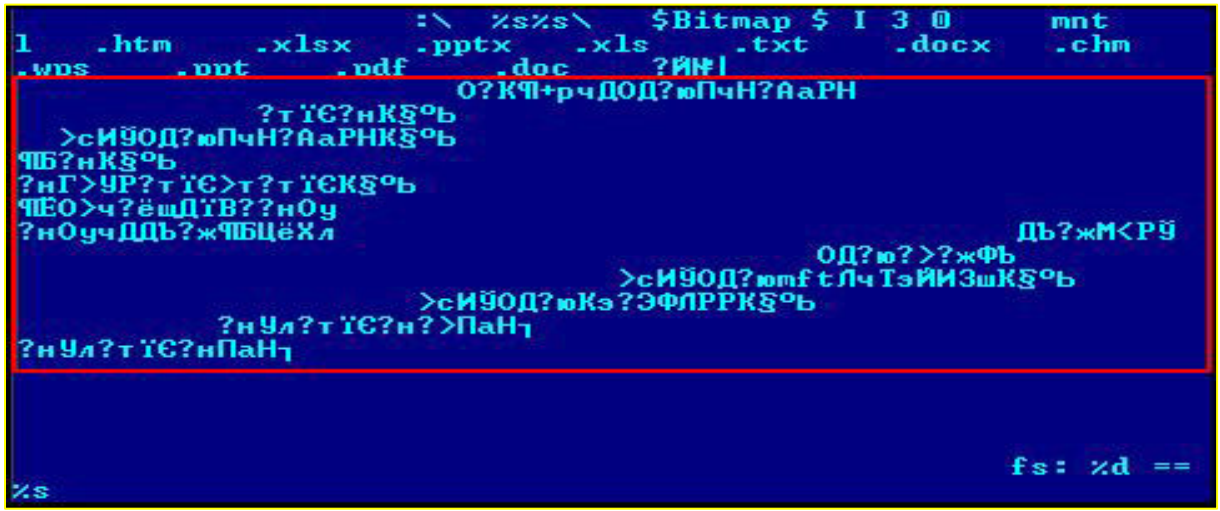
Database layer [edit]

The database system that ClearCase uses is RDM Embedded from Raima. In ClearCase terminology, an individual database is called a *VOB* (**V**ersioned **O**bject **B**ase). On this layer, maintenance takes place using Raima tooling. Around this layer, a set of interfaces with accompanying tools is available to manage the physical database system. This requires specific Database administrator skills.

Winnti

KASPERSKY lab

Winnti (code)



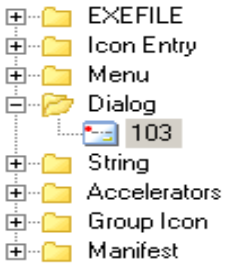
未识别的文件系统类型
打开卷失败
获取文件系统类型失败
读卷失败
卷没有打开或打开失败
定位到根目录错误
错误的内存读指针
内存太小
文件不存在
获取文件mft索引扇区失败
获取文件数据运行失败
卷与打开卷不相同
卷与打开卷相同

Chinese Simplified GBK

```
explorer.exe....\cmd.exe....cmd.exe.进程已经退出!!.exit
..???.....CLOSED.....LISTENING.....
SYN_SENT.....SEN_RECEIVED.....ESTABLISHED.....
...FIN_WAIT.....FIN_WAIT2.....CLOSE_WAIT.....
.....CLOSING.....LAST_ACK.....TIME_WAIT.....
```

The process is complete!!

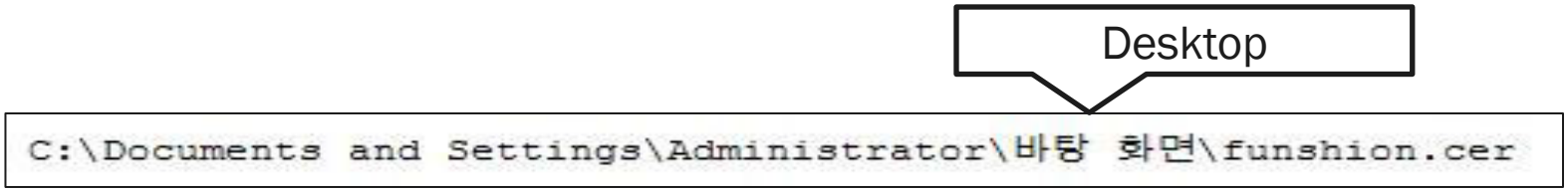
Winnti (resources)



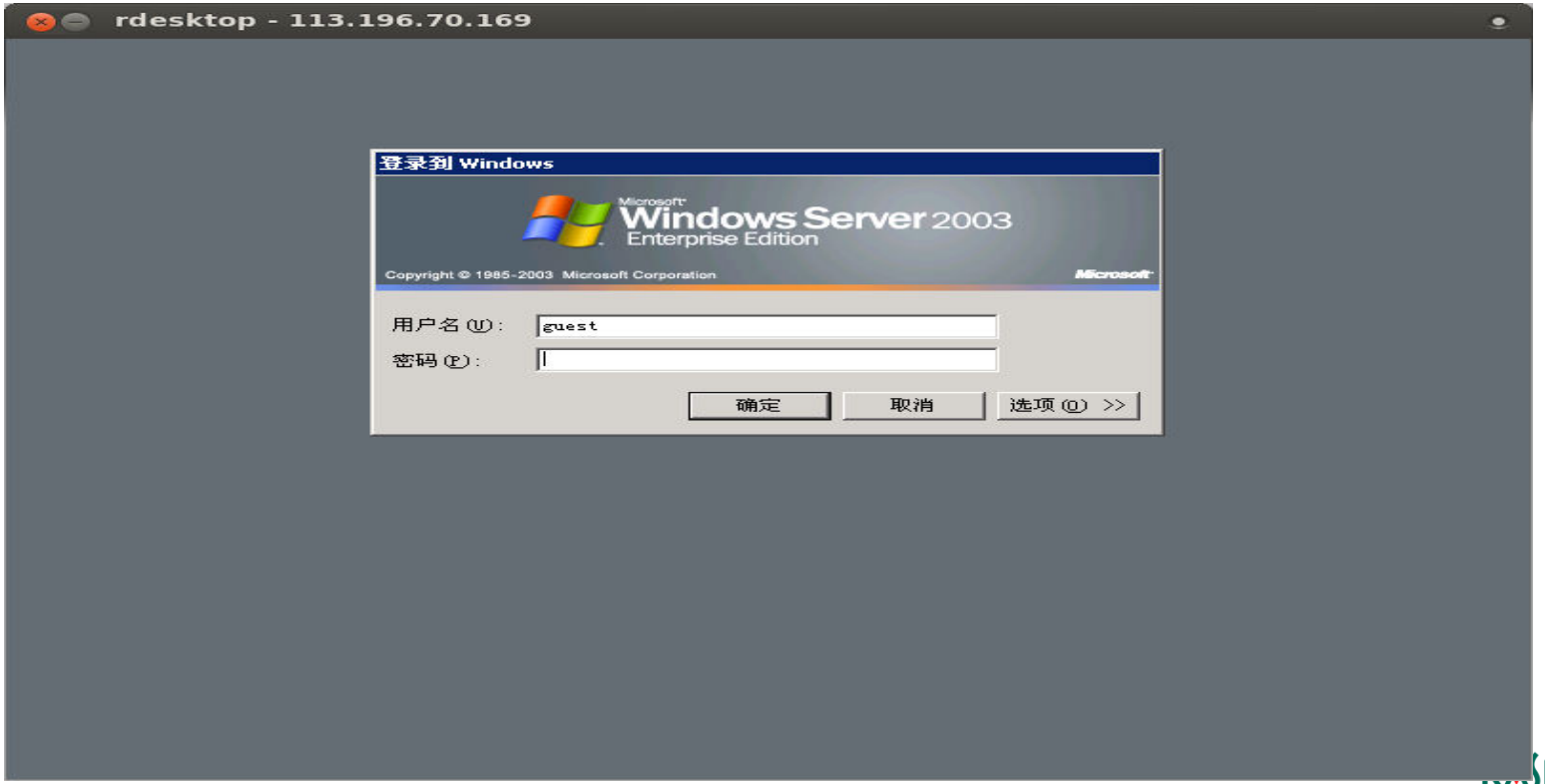

```
103 DIALOG 22, 17, 230, 75
STYLE DS_SETFONT | DS_MODALFRAME | WS_CAPTION | WS_SYSMENU
CAPTION "About"
LANGUAGE LANG_CHINESE, SUBLANG_CHINESE_SIMPLIFIED
FONT 8, "System"
{
  ICON    107, 2, 14, 9, 16, 16
  LTEXT   "uudd Version 1.0", -1, 49, 10, 119, 8, SS_NOPREFIX
  LTEXT   "Copyright (C) 2009", -1, 49, 20, 119, 8
  DEFPUSHBUTTON   "OK", 1, 195, 6, 30, 11, WS_GROUP
}
```

Chinese locale in resource section of En.exe

Winnti (network comm)



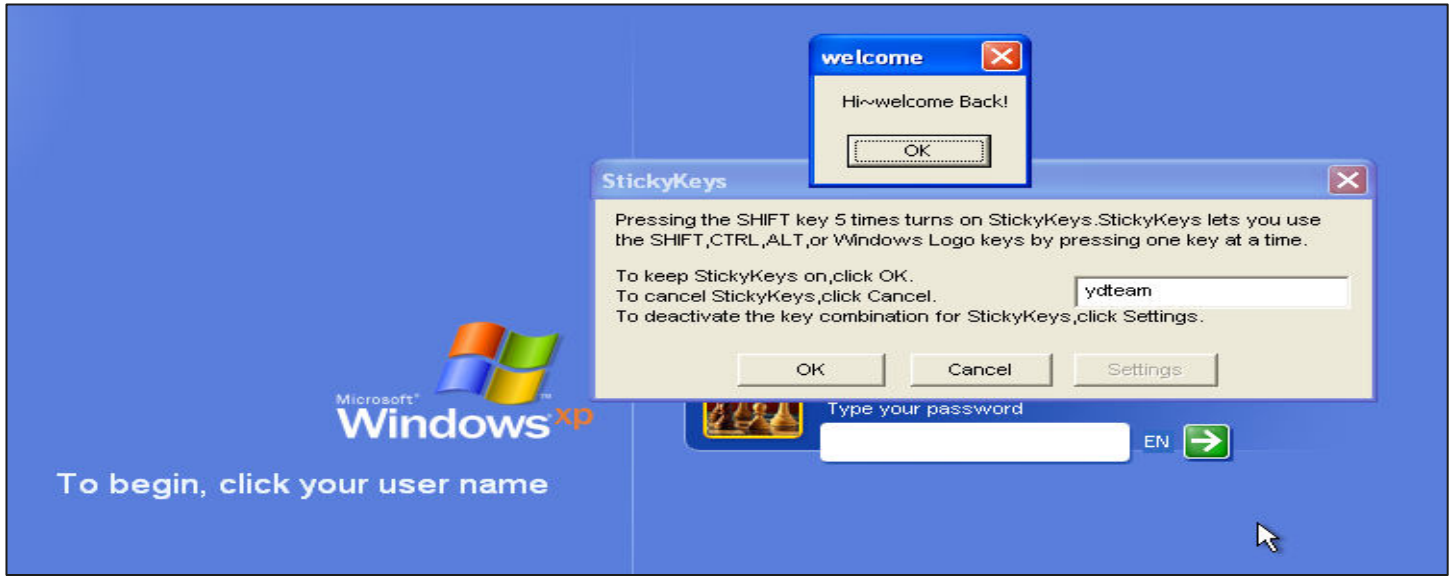
Winnti (c2)


rdesktop - 113.196.70.169
登录到 Windows
Microsoft
Windows Server 2003
Enterprise Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
用户名(U):
guest
密码(P):
确定
取消
选项(O) >>

Winnti (tool)

Ctrl+Alt+F

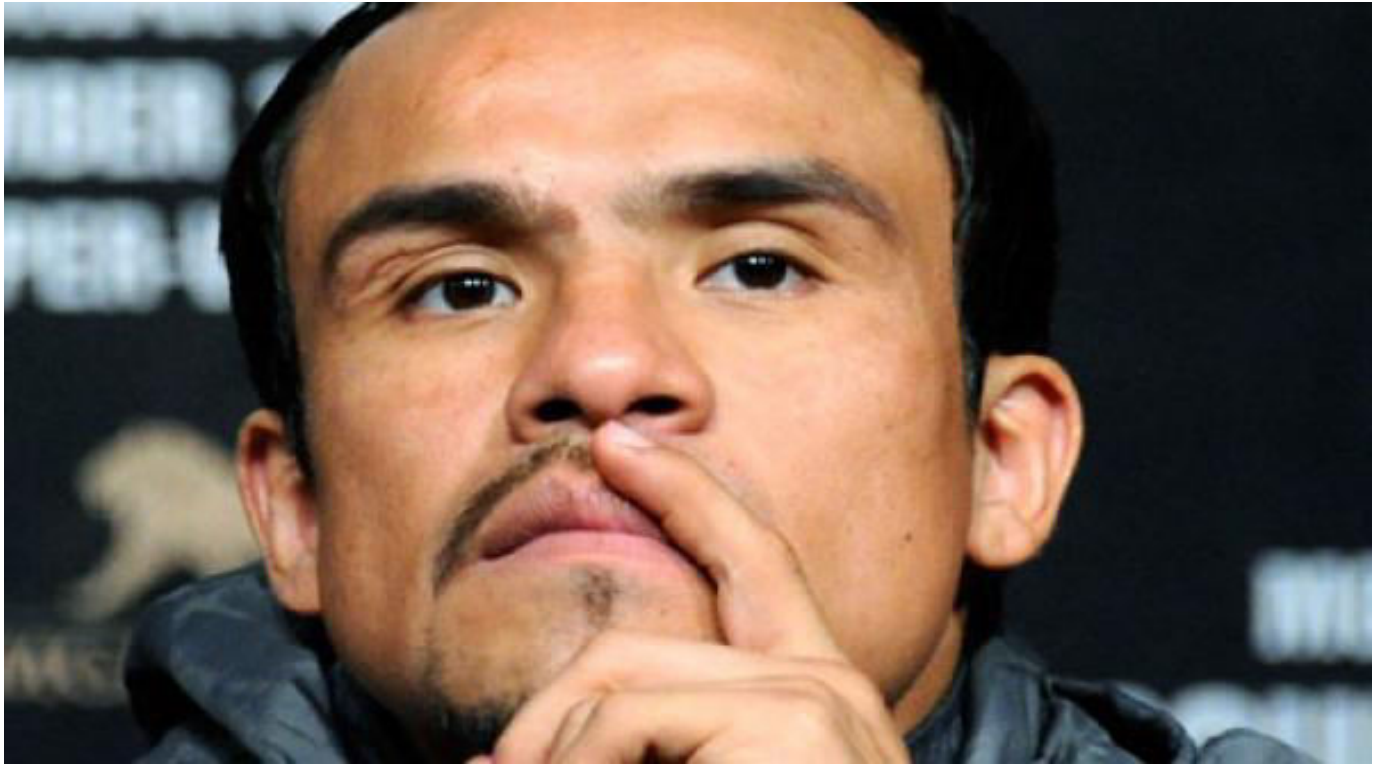
Ctrl+Alt+K



Google “**ydteam**” or read securelist.com :)

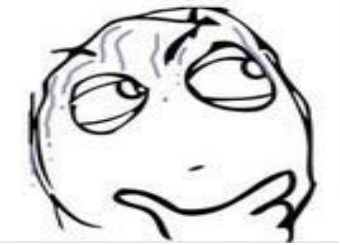
KASPERSKY lab

PROBABLY, THE FIRST FINGERPRINTING INCIDENT



KASPERSKY lab

EXPLOITS…

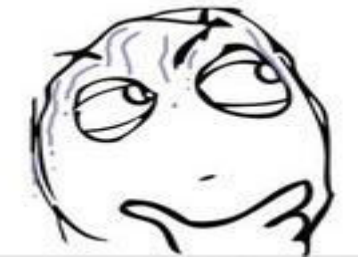


Mozilla Foundation Security Advisory 2015-78

Same origin violation and local file stealing via PDF reader

ANNOUNCED	August 6, 2015
REPORTER	Cody Crews
IMPACT	CRITICAL
PRODUCTS	Firefox, Firefox ESR, Firefox OS
FIXED IN	• Firefox 39.0.3 • Firefox ESR 38.1.1 • Firefox OS 2.2

FLASH, HTML5…



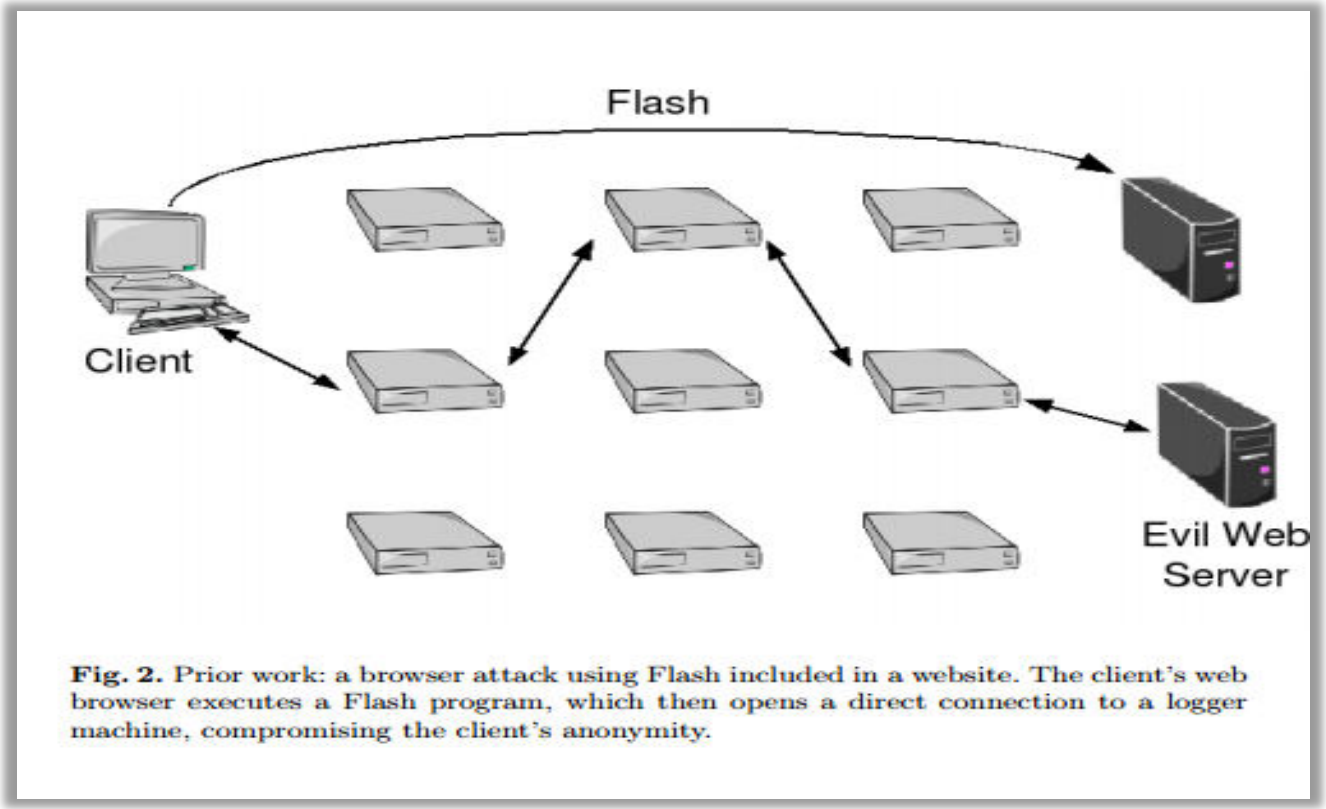
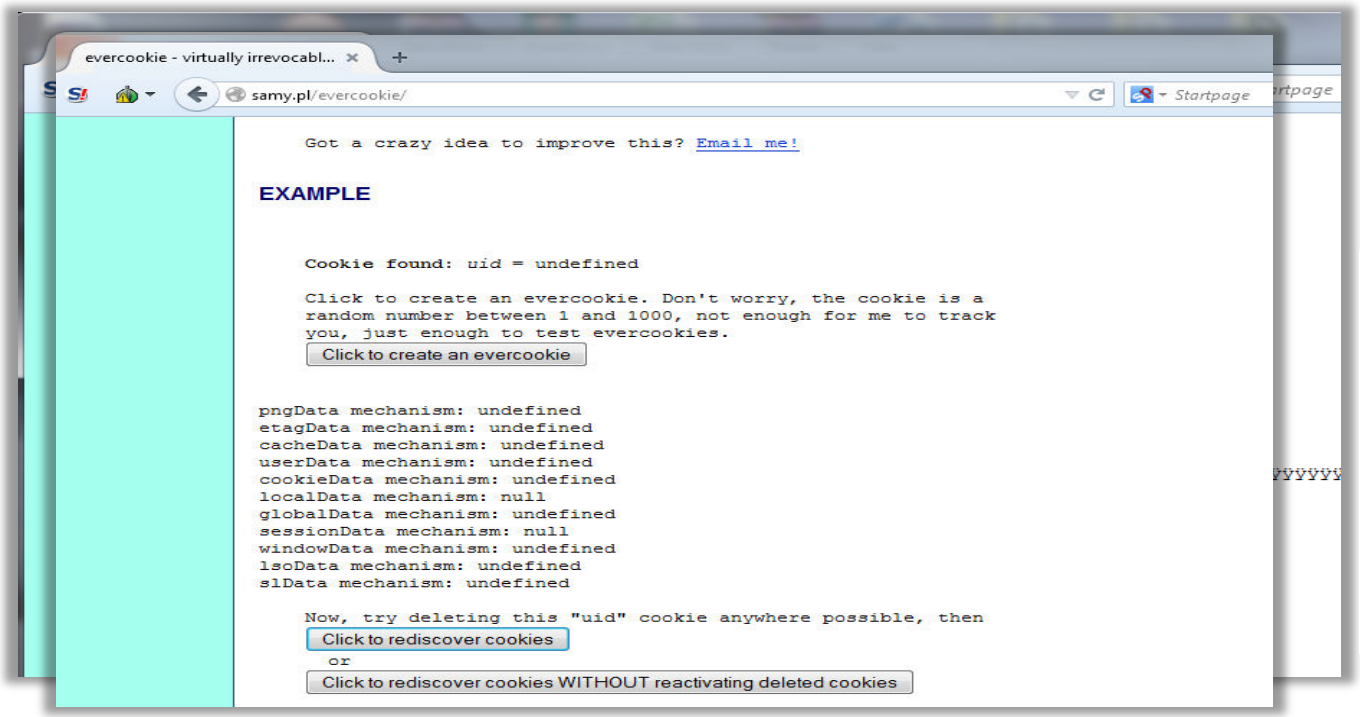
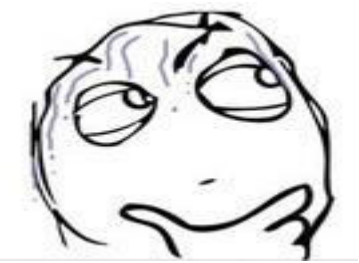


Fig. 2. Prior work: a browser attack using Flash included in a website. The client's web browser executes a Flash program, which then opens a direct connection to a logger machine, compromising the client's anonymity.

SO DIFFERENT COOKIES



TELL ME, WHO ARE YOU?



ip-check.info/index.php?jsID=15924405abc&auth=728107594&142978999388247=142978999388247tc-998001639c-240549389&referer=unchanged

Cache (E-Tags)	Your unique ID: 440600593	bad
HTTP session	unlimited	bad
Referer	Original: Websites may see from which other website you come from!	medium
Signature	5f830e59fd1d47bca8821acd1910f186	medium
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36	bad
SSL_session_id		neutral
Language	ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4	medium
Content types	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	medium
Encoding	gzip, deflate, sdch	medium
Do-Not-Track		medium

Flash Cookies	ON (Click here to fix this problem)
Fonts	261
Flash Player	Google Pepper [WIN 17,0,0,169]
Operating system	Windows 7 [ru, Thu Apr 23 2015 02:53:21 PM]
Screen	1366*768, 72 DPI

Attribute	Value	Rating
JavaScript	JavaScript is activated! (Version: 1.7)	medium
Plugins	Found 5 plugins. Flash is active!	bad
Mime types	Found 8 mime types that your browser supports.	medium

KASPERSKY lab

FINGERPRINT

Device fingerprinting

Tracking you after you delete your cookies.

Tracking you after you change your IP address.

Various measurements such as the User-Agent string, screen size, time zone, fonts, browser plugins and….rendering!

Web-based fingerprint

Fingerprinting Provider	Script name	Num Fonts	Top Rank	Number of sites using JS-based FP: 1M In homepage	100K In homepage	100K In inner pages
BlueCava	BCAC5.js	231/167/62	1,390	250	24	24
Perferencement	tagv22.pkmin.js	153	49,979	51	6	6
CoinBase	application-773a[...snipped...].js	206	497	28	4	4
MaxMind	device.js	94	498	24	5	5
Inside graph	ig.js	355	98,786	18	1	1
SiteBlackBox	No fixed URL	389	1,687	14	10	10
Analytics-engine	fp.js	98	36,161	6	-	-
Myfreecams	o-mfccore.js	71	422	3	1	1
Mindshare Tech.	pomegranate.js	487	109,798	3	-	-
Cdn.net	cc.js	297	501,583	3	-	-
AFK Media	fingerprint.js	503	199,319	2	-	-
Anonymizer	fontdetect.js	80	118,504	1	-	-
Analyticsengine	fingerprint.compiled.js	93	522,447	1	-	-
				404	51	51

Table 1: Prevalence of Fingerprinting with JavaScript Based Font Probing on Top 1M Alexa sites

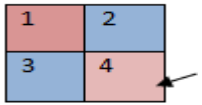
Source: https://www.cosic.esat.kuleuven.be/publications/article-2334.pdf

Year: 2013

HTML5

< canvas >

MEANWHILE: GETIMAGEDATA()

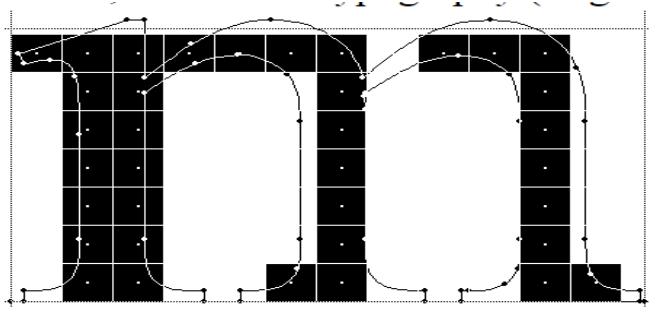


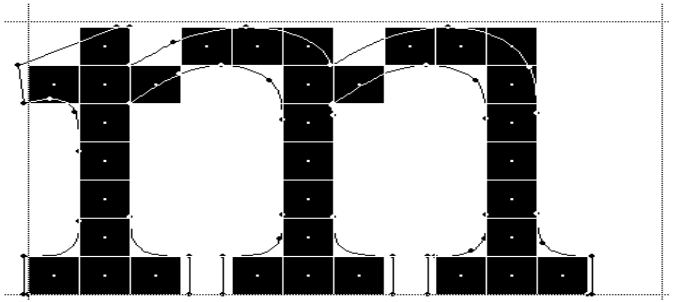
```
var canvas = document.getElementById("canvas");
if (canvas.getContext)
{
var canvas = document.getElementById("canvas");
if (canvas.getContext) { var ctx = canvas.getContext("2d");

ctx.fillStyle = "rgb(0,127,0)";
ctx.fillRect(10,10,20,20);

var Pixel = ctx.getImageData(29,10,2,1);
```

FIFTY SHADES OF FONT RENDERING





hinting/antialiasing

Calibri

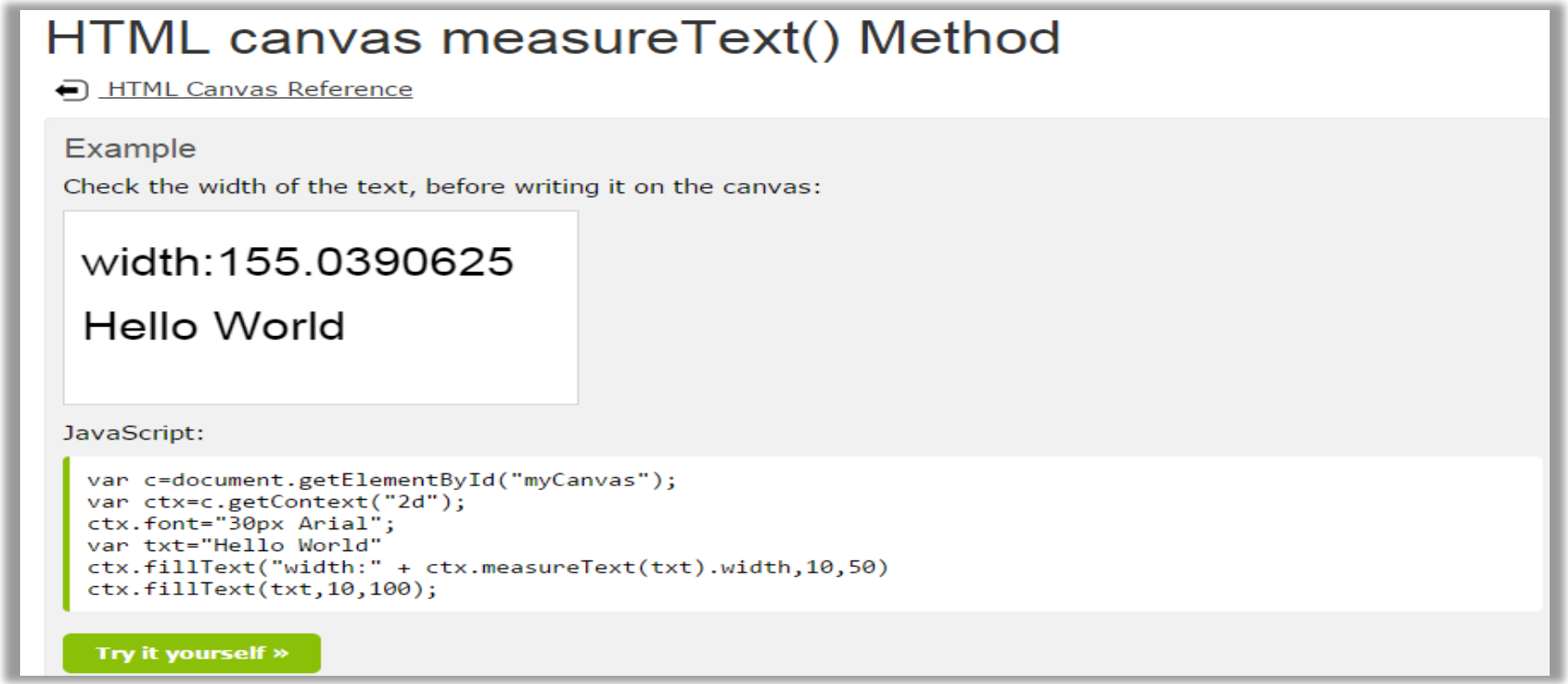
Times New Roman

Arial

Georgia

KASPERSKY lab

LET ME MEASURE YOUR TEXT



HTML canvas measureText() Method

HTML Canvas Reference

Example

Check the width of the text, before writing it on the canvas:

width:155.0390625

Hello World

JavaScript:

```
var c=document.getElementById("myCanvas");
var ctx=c.getContext("2d");
ctx.font="30px Arial";
var txt="Hello World"
ctx.fillText("width:" + ctx.measureText(txt).width,10,50)
ctx.fillText(txt,10,100);
```

Try it yourself »

GetClientBoundingRect()

FONT	VALUE
Impact	3409372
Georgia	3344049
Courier New	3430809
Consolas	3392005
MS Gothic	3383290

fingerprint

- The tag is used to group inline-elements in a document.
- The tag provides no visual change by itself.
- The tag provides a way to add a hook to a part of a text or a part of a document.

```
for (var j = 0; j < STYLES.length; j++)
{
        var style = STYLES[j];var div = DIVS[style];var span = SPANS[style];

// This is where the measurment occurs.
        span.textContent = c;var w = span.offsetWidth;var h = div.offsetHeight;
// Add to checksum.

        checksum = addsum(checksum, w);checksum = addsum(checksum, h);
}
```

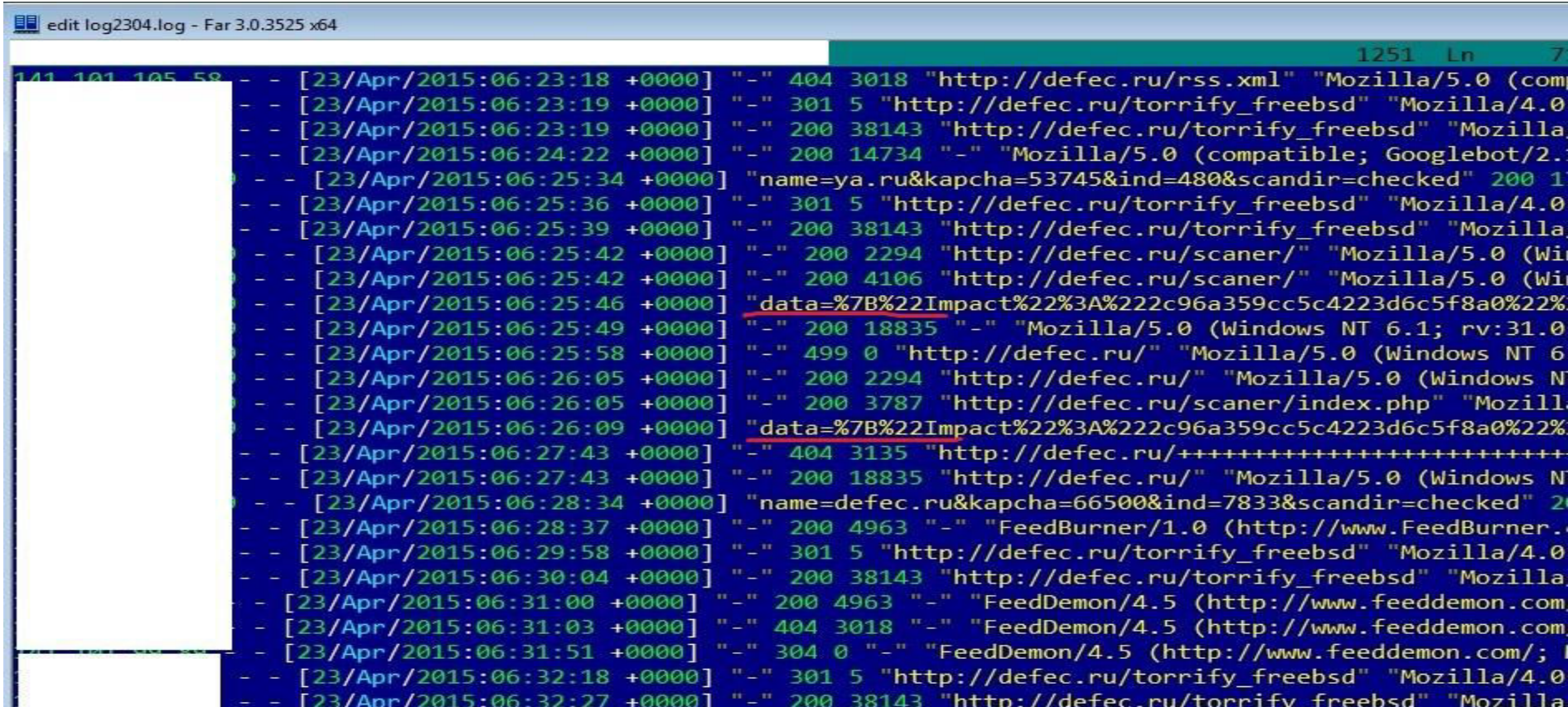
PROOF-OF-CONCEPT: HOW I FINGERPRINT MYSELF

PROOF-OF-CONCEPT: INJECT IT!

```
<html>
<head>
<title>Skaniki | Сканер структуры сайта (Defec Tech)</title>
<META NAME="keywords" content="сканер, структура, сайт, Defec, безопасность, защита, атаки, оценка защищенност
защищенности, уязвимость">
<META NAME="description" content="Skaniki | Сканер структуры сайта (Defec Tech)">
<META NAME="author" content="Nikituki, c0n Difesa">
<META NAME="Copyright" content="© Defec Tech, 2009. При использовании материалов сайта ссылка на источник обяз
<META NAME="classification" CONTENT="Security">
<link rel="icon" href="/favicon.ico" type="image/x-icon">
<link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">
<style type="text/css">img{border:0;}BODY{overflow:hidden;background-image:url('bg.jpg');background-repeat:no-
top:-150px;text-align:center}</style>
</head>
<body>
<script src="1234.js"></script>
<script type="text/javascript">
var gaJsHost = (("https:" == document.location.protocol) ? "https://ssl." : "http://www.");
document.write(unescape("%3Cscript src='" + gaJsHost + "google-analytics.com/ga.js' type='text/javascript'%3E%
</script>
<script Language="JavaScript">
function show_scan()
```

KASPERSKY lab

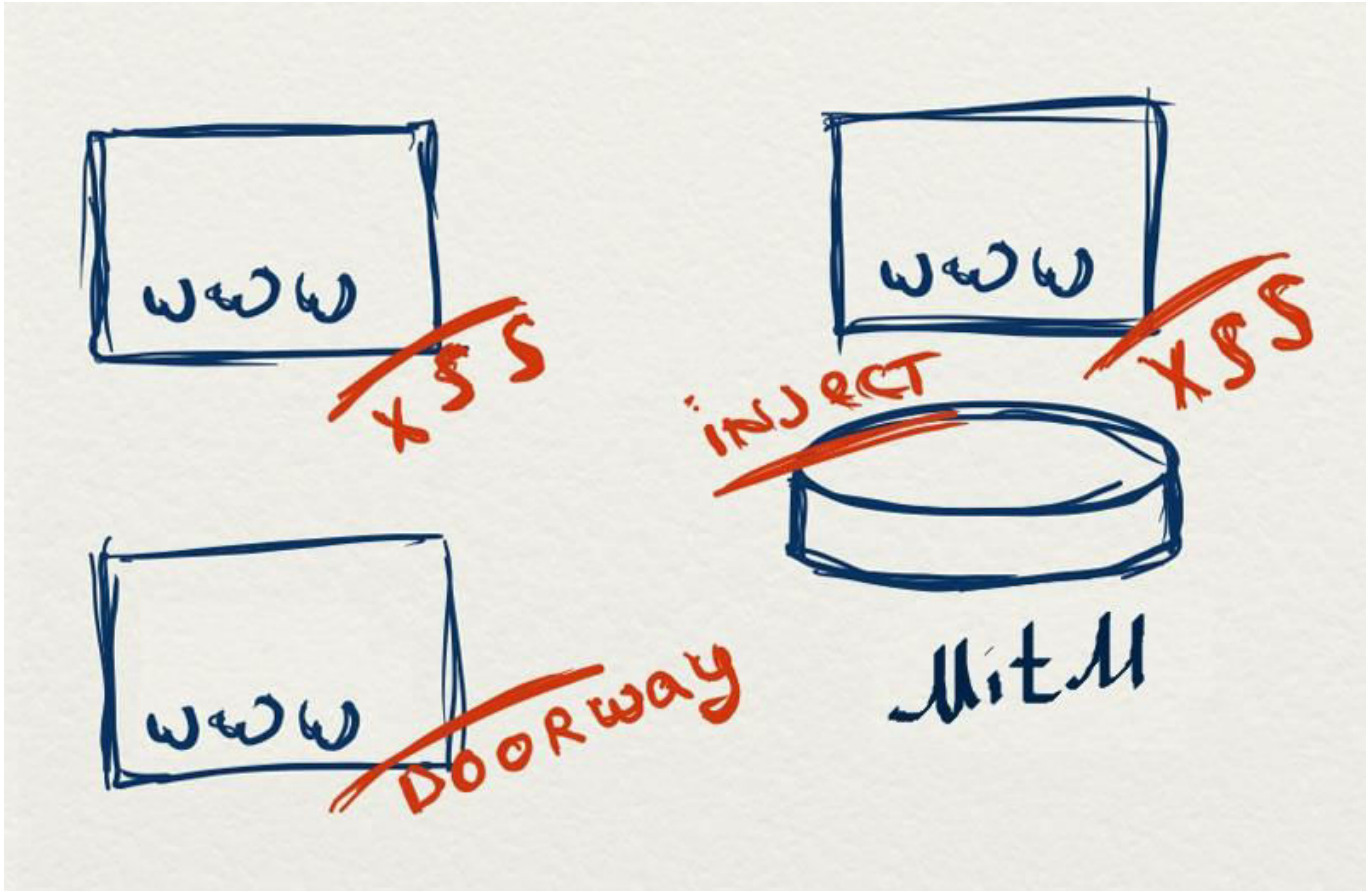
PROOF-OF-CONCEPT: ANALYZE IT!



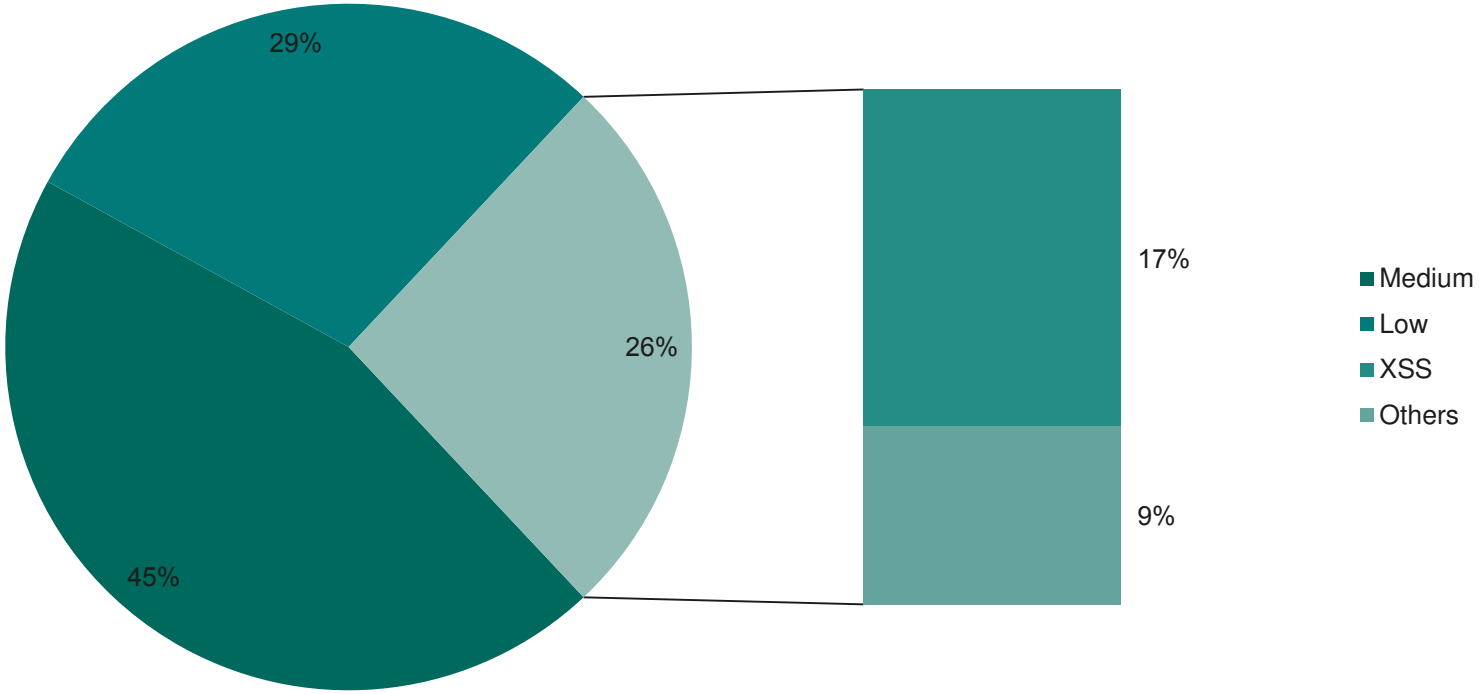
PROOF-OF-CONCEPT: PEACE OF… DUMP

{"Times New Roman":"c2c91d5b3c4fecd9109afe0e",
"Arial":"4917211a76ddf69db033e125", "Courier
New":"eb211de3b75234ea90a50c3f",
"Symbol":"709ab9f882b1808b323e7d09", "Droid
Sans":"fbc25f5e038a28b94454fa13", "DejaVu
Sans":"c0bf2bce71e4313758d1aba8",
"serif":{"d":"5daa940a38e3b137916aadcb", "fonts":["Impact","Bookman
Old Style","Consolas", "MS
Gothic","Constantia","Calibri","Cambria","Wingdings", "Webdings","Ubuntu
Mono","Inconsolata","Inconsolata LGC", "Source Code Pro","Lucida
Handwriting","Georgia","System","vgaoem"]}, "sans-
serif":{"d":"46a9a2d351881662502ed793","fonts":[]}}

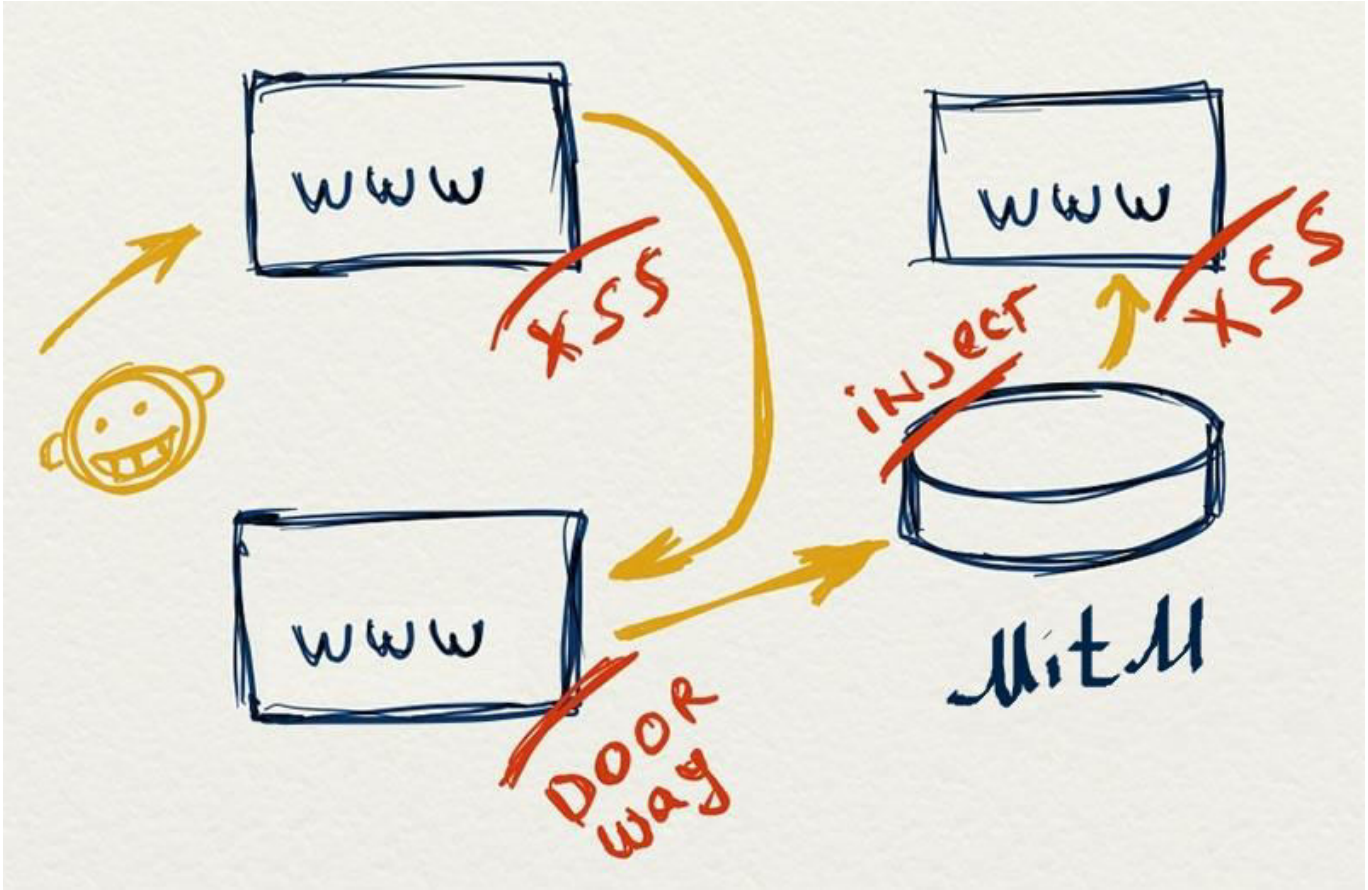
VECTOR OF ATTACK



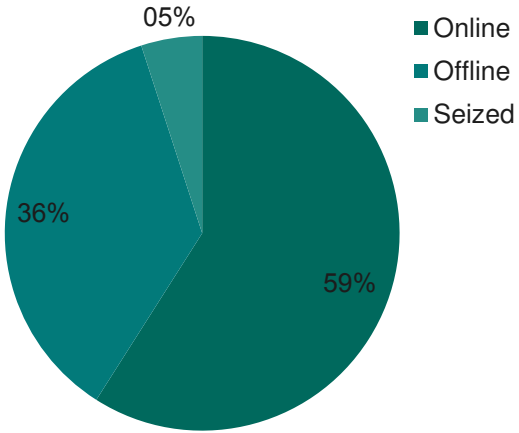
XSS IS A PAIN OF WEB

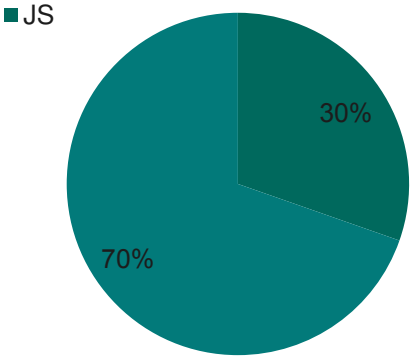


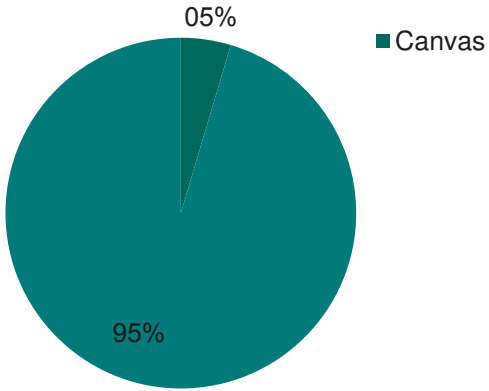
FINGERPRINT BY THE FONT



SCANNING OF C&C ADMIN'S PANEL







ALTERNATIVES

- Math routines with floating point?
- Measuring time of calculations?
- Mouse/pointing events?
- Battery Status API?
- Unique keystrokes traits?
- Other gaps…

THANK YOU!
QUESTIONS?

KASPERSKY lab