

Dynamoo's Blog

Malware, spam, scams and random stuff, by Conrad Longmore.

Blogger.com

Dynamoo's Blog


Dynamoo.com

Get Updates on Twitter

Advertisement



KEEP UP WITH A SIM ONLY PLAN



More info

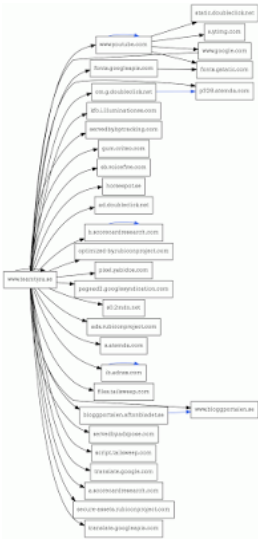
Monday, 21 September 2015


Tainted Network: "kfc.i.illuminations.com/snitch" and VPS Hosting of Latvia (91.226.32.0/23)

I've been seeing some injection attacks since last week utilising hosting services of VPS Hosting in Latvia. These are continuing today, with attacks like [this one](#) [URLquery] which sends traffic to:

[donotclick]kfc.i.illuminations.com/snitch

This is hosted on **91.226.33.54**. The exploit is not clear at this point, but some sources say that this is some sort of TDS kit. The URLquery transaction flowchart shows the attack in action.






EVIL

The injected script sends the keywords and referring site upstream, for example:

[donotclick]kfc.i.illuminations.com/snitch?
default_keyword=Team%20Tyra%20%7C%20The%20most%20popular%20equestrian%20website%20in%20Sweden%2F
Europe&referrer=&se_referrer=&source=www.teamtyra.se

Although the attacks in the past few days only seem to have utilised 91.226.33.54, an [analysis of the netblock](#) [pastebin] shows several bad or spammy sites in **91.226.32.0/23**, so my recommendation is that you banish this range from your network.


Posted by Conrad Longmore at 10:17



+2 Recommend this on Google

Labels: Evil Network, Injection Attacks, Latvia, Malware, TDS

2 comments:

 nelsinchi said...

Hi there, one of my sites was affected with attack, so, I blocked this ip address in my hosting like you recommended. Please keep us informed about this attack.

Thanks a lot.

23 September 2015 at 05:45

 Guruweb Botswana said...

I would recommend reading <https://wordpress.org/support/topic/js-injection-after-wp>


24 September 2015 at 18:22


SoftLayer®

Do You Want a Transparent Cloud Environment? Cloud Experts Can Help

→

Subscribe To

 Posts

 Comments

Popular Posts




Birmingham Fulford "R message"

This sparr from a jou Paul Fulford at the Birr However, it isn't.. it is a malic...




Tainted Network

"kfc.i.illuminations.com VPS Hosting of Latvia (91.226.32.0/23)" I've been seeing some injection attacks since last week utilising hosting services of VPS Hosting in Latvia. These are continuing today.



"Broad Office fake invoice"

UPDATE : there is a fake invoice attached with this with a attachment, please screenshot more details. This sparr



Sprint spa 1.starkres

This fake invoice leads to more 1.starkres

Date: Tue, 09 Oct 2015 +0300 From: "Sprint"



"Fiserv Secure Notification"

This sparr encrypted transaction malware. The password filenames will vary. From Secure Notification...



Malware Varker

[\[mailto:kvarker@notification.com\]](mailto:kvarker@notification.com) / "Invoice from" This fake invoice has a

[Post a Comment](#)

SoftLayer® Cloud

The Cloud Doesn't Have to be Cloudy Get the Cloud with Nothing to Hide!



[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)

attachment: From : Kair [mailto:kvarker@notifica.com] On Behalf Of Kair



Malware s e-mail finc "Stacey G

This sparr malicious

Date : 23 June 2015 : Hope this e-mail finc Good day! Hop...

(More) Domains and bu associated with Michae BizSummits

Following on from this p some business and dor associated with Michae BizSummits , presentec



Top porn s malware

About a ye ago I wrot of malwan

xvideos.com that were | infecting visitor's PCs...



Malware s ROI - Pas activation

"secure.message@rbs. This fake banking sparr from RBS, but is instea forgery with a malicious From "RBS" [s...

Blog Archive

- ▼ 2015 (259)
 - ▼ September (25)
 - Evil network: 64.20.51.16/29 (Interserver Inc
 - Phish: "SHIPMEN LABEL" / "DHL Services [r...
 - Malware spam: "E ROI - Passwor activati...
 - (More) Domains a businesses ass with Mich...
 - Malware spam: "Y Sage subscripti invoice is r...
 - Tainted Network: "kfc.i.illuminatio /snitch"...
 - Malware spam: "Transaction confirmation" / '
 - E.ON "You've got spam
 - Malware spam: hrwfmailerprod hire.gov.uk / R.
 - Malware spam: "S Bill for Week 3&
 - Malware spam: "L Bank - Pendefc Securities ...
 - Malware spam: "F SecureMail" / " receiv...
 - Spam from "Vane Reynolds" / vanessa.reynol
 - Malware spam: "S Order Acknowledgem Order...

Malware spam: "N
- 3901535011"
"UK2Fax" [f...

Malware spam: "F
Received by Int
"Intu...

ipserver.su,
5.133.179.0/24
212.38.166.0/2...

Evil network:
89.144.2.0/24 /
Echo Romeo ...

Something evil on
184.105.163.19
White Falco...

Malware spam: "C
Note CN-60936
Stilwell ...

Malware spam:
"Companies Hc
[WebFiling@co

Malware spam:
"RE:resume" al
happened to yc

DYNAMOO®

Malware spam:
"Complaint of y
Internet activity

Malware spam: "F
message notific
41447"...

- [August](#) (26)
- [July](#) (22)
- [June](#) (23)
- [May](#) (12)
- [April](#) (38)
- [March](#) (34)
- [February](#) (39)
- [January](#) (40)

- [2014](#) (389)
- [2013](#) (565)
- [2012](#) (492)
- [2011](#) (194)
- [2010](#) (151)
- [2009](#) (132)
- [2008](#) (193)
- [2007](#) (52)

Labels

[Spam](#) (1676)
[\(1408\)](#) [Malwa](#)
[Russia](#) (222) [S](#)
[Amerika](#) (216) [EXE](#)
[RU:8080](#) (208) [DC](#)
[Offer Scams](#) (133)
(130) [Money Mule](#)
(114) [Dridex](#) (109)
[Linode](#) (85) [SQL](#)
[Lapatasker](#) (78) [Germa](#)
(71) [Injection Attacks](#)
[GoDaddy](#) (59) [Hetzner](#)
[Turkey](#) (49) [Canada](#) (4
[BBB](#) (43) [Latvia](#) (43) [Pr](#)
[Facebook](#) (40) [L](#)
[ThreeScripts](#) (40)
[Phishing](#) (39) [Dyre](#) (3
[DINETHOSTING](#) (37)
[INTUIT](#) (36) [India](#) (36)
[ADP](#) (33) [Netherlan](#)
[Pharma](#) (31) [Romania](#)
(30) [Korea](#) (30) [Ami](#)
[Spam](#) (29) [Microsoft](#) (
[.SU](#) (26) [Enduranc](#)

Group (26) Scam (26) 1
 (25) IRS (25) Moldova
 Bulgaria (22) Lithuani
 Fallout Enterprises (:
 TheFirst-RU (21) USF
 (20) Malvertising (20
 PayPal (19) Pump and
 (19) Blackhole (18) B
 (18) Joe Job (17) Italy (
 Sweden (16) Thailand (1
 Fraud (15) Dating Scams
 HMRC (15) Leaseweb (
 Taiwan (15) Zbot (15) Fe
 AICPA (12) False Positi
 Poland (12) R5X.org (
 Serverius (12) Somnath E
 (11) GHOSTnet (11) Joll
 (11) US Airways (11) Aust
 Colombia (10) Czech Ri
 (10) Greece (10) Intergen
 NAPPPA (10) Sally Gask
 ISP (10) Transnistria (10)
 (9) CNN (9) Estonia (9)
 eTrust (9) Android (8)
 CyberBunker (8) FedEx
 Pakistan (8) Patches (8)
 Transit (8) Solar VPS (8)
 EK (7) Anti-Virus Softwa
 Black Hat (7) Dropbox (7)
 Fake Anti-Virus (7) Fiji
 Sagade Ltd (7) Switzerl
 UK2.NET (7) inferno.nan
 Advertising (6) Appraise
 Cryptowall (6) IPMA (6) I
 Management America
 Mystery Shopper (6) Net
 (6) Philippines (6) Piradi
 (6) Sky (6) UkrStar ISP (
 Bosnia (5) Crime (5) Df
 Google Maps (5) Hacked
 (5) NetTemps Inc (5) Pes
 (5) Privacy (5) Sidharth St
 (5) Webazilla (5) Xeex
 Austria (4) BBC (4) Blogge
 Bundespolizei (4) Egypt (
 (4) Gary McNeish (4) F
 Lithuania (4) LizaMoon (4)
 (4) Senegal (4) Sparr
 Telecoms (4) Twitter (
 Weather (4) Zeus (4) .hta
 (3) Blogging (3) Botnet (3)
 Dubai (3) Emailmovers L
 F-Secure (3) Finland (3) I
 Streetview (3) HostForW
 (3) Humour (3) Lottery S
 NA3PA (3) Passwords (
 Pizza (3) Police (3) SEO
 Smart Roadster (3) Sv
 Telepests (3) Video (3)
 Waledac (3) Windows (3)
 (3) Yahoo (3) Yohost.org (
 (3) Acid Free Coffee (2) A
 (2) Bob Gatchel (2)
 CareerBuilder (2) (
 Classmates.com (2) Clickt
 (2) DDOS (2) DreamHost
 Fake Postcard (2) Fin
 Hostinger (2) IIS (2) Ii
 Internet Explorer (2) Java
 Maxhosting (2) Mobiquant
 (2) Netdirekt (2) Nuclear
 PHP (2) Palestine (2) Pan
 Pinball Corporation (2) Pin
 (2) Retro (2) Samsung (:
 Real Estate (2) Sinowal (2)
 (2) TDS (2) The Funding li
 Vet (2) Voxility (2) Wikip
 Argentina (1) Art Scam (1)
 (1) Bedfordshire (1) Bel
 Bitcoin (1) Blink (1) Bulgari
 Computer Misuse Act (
 CookieBomb (1) DNS (1) C
 Edis (1) Elections (1) Electr
 Epsilon (1) Escrow (1) Etiqu
 (1) FirefoxOS (1) Friends
 Gawker (1) Ghana (1) Gog
 (1) Google Drive (1) G
 Gumbler (1) HYIP (1) Hotl
 Infographic (1) Ireland (1)
 (1) LBM (1) LNK (1) Le
 LinkShare (1) Luxembou
 Macedonia (1) Macintosh
 Malaysia (1) Maware (1)
 Motorola (1) Mozilla (1) M

2015/9/26

Dynamoo's Blog: Tainted Network: "kfc.i.illuminations.com/snitch" and VPS Hosting of Latvia (91.226.32.0/23)

Najada Ltd (1) Network Op
Networking4Africa.com (1)
Zealand (1) New Zeali
Software Group (1) Parc
Aunger (1) Project Manage
(1) Qatar (1) Relikts BVK (1)
(1) Rootkits (1) SMTP (1) S
Santrex (1) Serverconnect
Skype (1) Slimeware (1)
Spoofing (1) SpyEye (1) S
(1) Sysprep (1) T-Mobile
Tylers Coffees (1) Viruse (1)
Viine Ltd (1) WTF (1) W
YouTube (1) Zero Day
ZoneAlarm (1) gambling
microlines.lv (1) pddomair
(1) theciosummits.org (1)

Links

Retromobe

Mobile Gazette

Petrol Direct

Slimeware

The Truth about Conrac

Never email donotemail@wearespammers.com . Powered by [Blogger](#).

http://blog.dynamoo.com/2015/09/tainted-network-kfciilluminationscomsn.html

5/5