KEAMANAN JARINGAN KOMPUTER

"RECONNAISSANCE"

OLEH:

Doni Saputra (09011181520120)

Dosen Pengampuh : DERIS STIAWAN, M.T., PH.D.

Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2019

1. Website Pemerintah

Salah satu contohnya yaitu website departemen keuangan: www.depkeu.go.id.

Dengan menggunakan tools netcraft.com didapatkan bahwa target dari website departemen keuangan memiliki ip address 202.137.230.199 dengan domain depkeu.go.id serta hosting history berisi informasi IP Address, Operating System, Daemon dan tanggal dari awal sampai terakhir diperbaharui.

Background

Site title	*Not Present*	**Date first seen**	October 1998
Site rank		**Primary language**	*Not Present*
Description	*Not Present*		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://www.depkeu.go.id	**Netblock Owner**	Pusat Sistem Informasi dan Teknologi Keuangan (Pusintek)
Domain	depkeu.go.id	**Nameserver**	ns1.telkom.net.id
IP address	202.137.230.199 (VirusTotal)	**DNS admin**	hostmaster@telkom.net.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	*unknown*
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Pusat Sistem Informasi dan Teknologi Keuangan Pusintek Government / Direct member IDNIC Jakarta	202.137.230.199	Linux	Apache/2.2.15 CentOS	2-Dec-2014
Pusat Sistem Informasi dan Teknologi Keuangan Pusintek Government / Direct member IDNIC Jakarta	202.137.230.89	Windows Server 2003	Microsoft-IIS/6.0	1-Jun-2013
IP Bintek Keuangan 6 INDOSATM2 Dedicated Platinum Customer Jakarta	219.83.74.89	Windows Server 2003	Microsoft-IIS/6.0	26-Jan-2010
IP Bintek Keuangan 6 INDOSATM2 Dedicated Platinum Customer Jakarta	219.83.74.89	unknown	Microsoft-IIS/6.0	18-Feb-2009
IP Bintek Keuangan 6 INDOSATM2 Dedicated Platinum Customer Jakarta	219.83.74.89	Windows Server 2003	Microsoft-IIS/6.0	30-Dec-2008
IP Bintek Keuangan 4 INDOSATM2 Dedicated Platinum Customer Jakarta	219.83.74.51	Windows Server 2003	Microsoft-IIS/6.0	14-Jun-2008
IP Bintek Keuangan 4 INDOSATM2 Dedicated Platinum Customer Jakarta	219.83.74.51	unknown	Microsoft-IIS/6.0	26-Sep-2006
IP Bintek Keuangan 4 INDOSATM2 Dedicated Platinum Customer Jakarta	219.83.74.51	Windows Server 2003	Microsoft-IIS/6.0	22-Aug-2006
IP Bintek Keuangan 4 INDOSATM2 Dedicated Platinum Customer Jakarta	219.83.74.51	unknown	Microsoft-IIS/6.0	21-Aug-2006
IP Bintek Keuangan 4 INDOSATM2 Dedicated Platinum Customer Jakarta	219.83.74.51	Windows Server 2003	Microsoft-IIS/6.0	20-Aug-2006

CVE (Common Vulnerabilities and Exposures List)

Jenis OS	CVE Name	Deskripsi
Linux	CVE-2019-7312	Pengungkapan plaintext terbatas ada di PRIMX Zed Entreprise untuk Windows sebelum 6.1.2240, Zed Entreprise for Windows (pengajuan kualifikasi ANSSI) sebelum 6.1.2150, Zed Entreprise untuk Mac sebelum 2.0.199, Zed Entreprise untuk Linux sebelum 2.0.199, Zed Pro for Windows sebelum 1.0.195, Zed Pro untuk Mac sebelum 1.0.199, Zed Pro untuk Linux sebelum 1.0.199, Zed Gratis untuk Windows sebelum 1.0.195, Zed Gratis untuk Mac sebelum 1.0.199, dan Zed Gratis untuk Linux sebelum 1.0. 199. Menganalisis wadah Zed dapat menyebabkan pengungkapan konten plaintext dari file yang sangat kecil (beberapa byte) yang disimpan di dalamnya.
	CVE-2019-7308	kernel / bpf / verifier.c di kernel Linux sebelum 4.20.6 melakukan spekulasi di luar batas yang tidak diinginkan pada aritmatika pointer dalam berbagai kasus, termasuk

		kasus cabang berbeda dengan keadaan berbeda atau batas sanitasi, yang mengarah ke serangan saluran samping.
	CVE-2019-6136	Masalah telah ditemukan di libIEC61850 v1.3.1. Ethernet_setProtocolFilter dalam hal / ethernet / linux / ethernet_linux.c memiliki SEGV, seperti yang ditunjukkan oleh sv_subscriber_example.c dan sv_subscriber.c.

Jenis Daemon	**CVE Name**	**Deskripsi**
Apache/2.2.15 CentOS	CVE-2016-5425	Paket Tomcat pada Red Hat Enterprise Linux (RHEL) 7, Fedora, CentOS, Oracle Linux, dan mungkin distribusi Linux lainnya menggunakan izin yang lemah untuk /usr/lib/tmpfiles.d/tomcat.conf, yang memungkinkan pengguna lokal mendapatkan hak root. dengan memanfaatkan keanggotaan dalam grup kucing jantan.

Hasil Traceroute (www.depkeu.go.id **)**

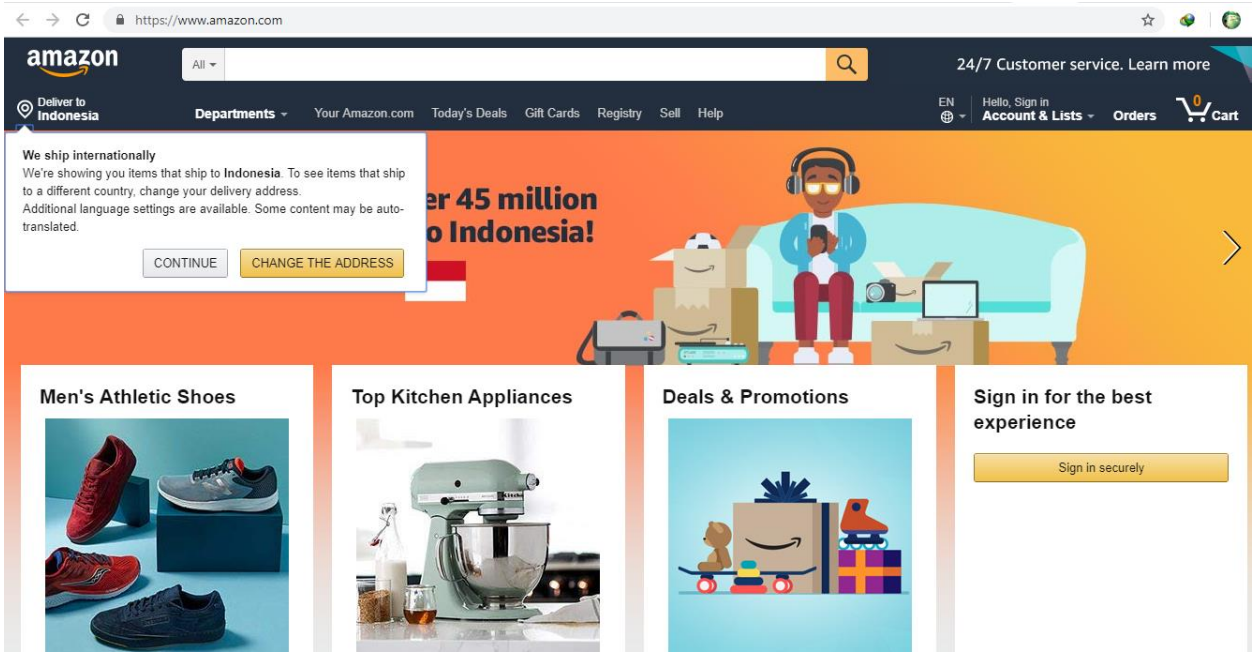
Untuk mengetahui posisi router yang dilewati paket data.

www.depkeu.go.id Timeout 0

#		Country	Town	Lat	Lon	IP	Hostname	L...	D...	Di...	...
1		Indonesia	Jakarta	-6.1744	106.8294	192.168.43.1	(None)	2	53	0	
2		Indonesia	Jakarta	-6.1744	106.8294	172.28.34.85	(None)	83	109	0	
3		Indonesia	Jakarta	-6.1744	106.8294	172.28.2.121	(None)	66	62	0	
4		Indonesia	Jakarta	-6.1744	106.8294	10.45.201.77	(None)	65	53	0	
5		Indonesia	Jakarta	-6.1744	106.8294	10.45.201.82	(None)	65	74	0	
6		Indonesia	Jakarta	-6.1744	106.8294	115.178.161....	(None)	1...	71	0	
7		Indonesia	Jakarta	-6.1744	106.8294	115.178.161....	(None)	1...	56	0	
8		Indonesia	Jakarta	-6.1744	106.8294	115.178.161....	(None)	81	66	0	
9		Indonesia	Jakarta	-6.1744	106.8294	202.43.179.2...	ip-179-217.moratelin...	1...	66	0	
10		Indonesia	Bekasi	-6.2349	106.9896	203.176.181....	ip-203-176-181-198....	82	78	18	
11		Indonesia	Jakarta	-6.1744	106.8294	103.30.172.94	(None)	81	100	18	
12		Indonesia	(Unknown)	-6.175	106.8286	36.66.26.33	(None)	1...	972	0	
13		Indonesia	(Unknown)	-6.175	106.8286	118.97.181.1...	110.subnet118-97-1...	65	115	0	
14		Indonesia	Jakarta	-6.1744	106.8294	202.137.230.7	vpn.kemenkeu.go.id	1...	119	0	
15		Indonesia	Jakarta	-6.1744	106.8294	202.137.230....	(None)	81	84	0	

2. Website luar negeri

Salah satu contohnya yaitu website belanja online luar negeri: www.amazon.com



Dengan menggunakan tools netcraft.com didapatkan bahwa target dari website belanja online luar negeri memiliki ip address 54.230.31.41 dengan domain amazon.com serta hosting history berisi informasi IP Address, Operating System, Daemon dan tanggal dari awal sampai terakhir diperbaharui.

Background

Site title	Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more	**Date first seen**	October 1995
Site rank	228	**Primary language**	English
Description	Online shopping from the earth		
Keywords	Amazon, Amazon.com, Books, Online Shopping, Book Store, Magazine, Subscription, Music, CDs, DVDs, Videos, Electronics, Video Games, Computers, Cell Phones, Toys, Games, Apparel, Accessories, Shoes, Jewelry, Watches, Office Products, Sports & Outdoors, Sporting Goods, Baby Products, Health, Personal Care, Beauty, Home, Garden, Bed & Bath, Furniture, Tools, Hardware, Vacuums, Outdoor Living, Automotive Parts, Pet Supplies, Broadband, DSL		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://www.amazon.com	**Netblock Owner**	Amazon.com, Inc.
Domain	amazon.com	**Nameserver**	dns-external-master.amazon.com
IP address	54.230.31.41 (VirusTotal)	**DNS admin**	root@amazon.com
IPv6 address	*Not Present*	**Reverse DNS**	server-54-230-31-41.dub2.r.cloudfront.net
Domain registrar	markmonitor.com	**Nameserver organisation**	whois.markmonitor.com
Organisation	Amazon Technologies, Inc., P.O. Box 8102, Reno, 89507, United States	**Hosting company**	Amazon
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	US	**Latest Performance**	Performance Graph

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	143.204.185.215	Linux	CloudFront	10-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.193.128	Linux	AkamaiGHost	8-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.4.208.196	Linux	AkamaiGHost	7-Feb-2019
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	52.222.227.7	Linux	CloudFront	7-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.193.128	Linux	AkamaiGHost	5-Feb-2019
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	143.204.185.215	Linux	CloudFront	4-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.251.164	Linux	AkamaiGHost	3-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.193.128	Linux	AkamaiGHost	2-Feb-2019
Akamai Technologies	95.101.84.228	Linux	AkamaiGHost	1-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.131.176	Linux	AkamaiGHost	31-Jan-2019

CVE (Common Vulnerabilities and Exposures List)

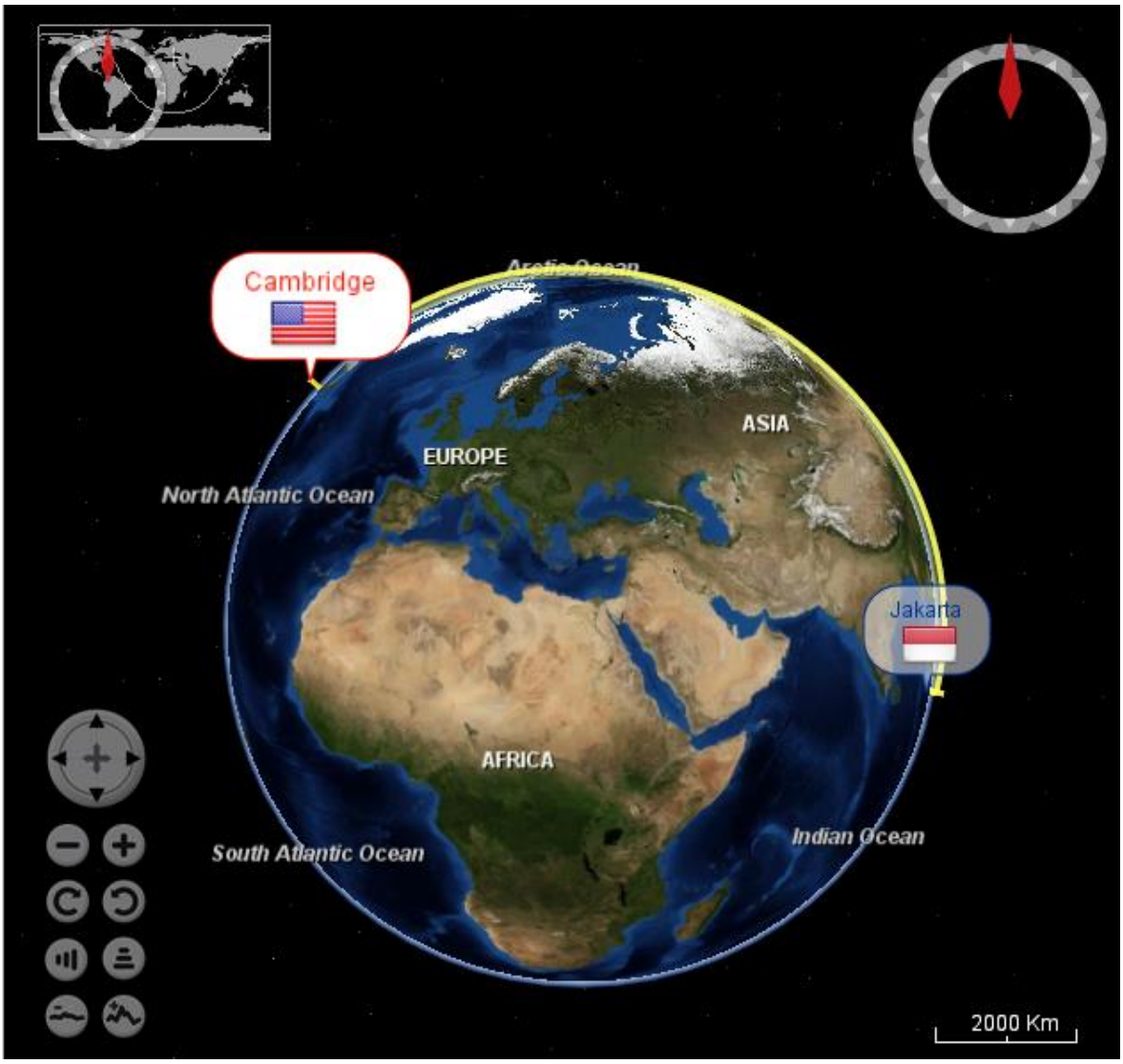
Jenis OS	CVE Name	Deskripsi
Linux	CVE-2019-7312	Pengungkapan plaintext terbatas ada di PRIMX Zed Entreprise untuk Windows sebelum 6.1.2240, Zed Entreprise for Windows (pengajuan kualifikasi ANSSI) sebelum 6.1.2150, Zed Entreprise untuk Mac sebelum 2.0.199, Zed Entreprise untuk Linux sebelum 2.0.199, Zed Pro for Windows sebelum 1.0.195, Zed Pro untuk Mac sebelum 1.0.199, Zed Pro untuk Linux sebelum 1.0.199, Zed Gratis untuk Windows sebelum 1.0.195, Zed Gratis untuk Mac sebelum 1.0.199, dan Zed Gratis untuk Linux sebelum 1.0. 199. Menganalisis wadah Zed dapat menyebabkan pengungkapan konten plaintext dari file yang sangat kecil (beberapa byte) yang disimpan di dalamnya.
	CVE-2019-7308	kernel / bpf / verifier.c di kernel Linux sebelum 4.20.6 melakukan spekulasi di luar batas yang tidak diinginkan pada aritmatika pointer dalam berbagai kasus, termasuk kasus cabang berbeda dengan keadaan berbeda atau batas sanitasi, yang mengarah ke serangan saluran samping.
	CVE-2019-6136	Masalah telah ditemukan di libIEC61850 v1.3.1. Ethernet_setProtocolFilter dalam hal / ethernet / linux / ethernet_linux.c memiliki SEGV, seperti yang ditunjukkan

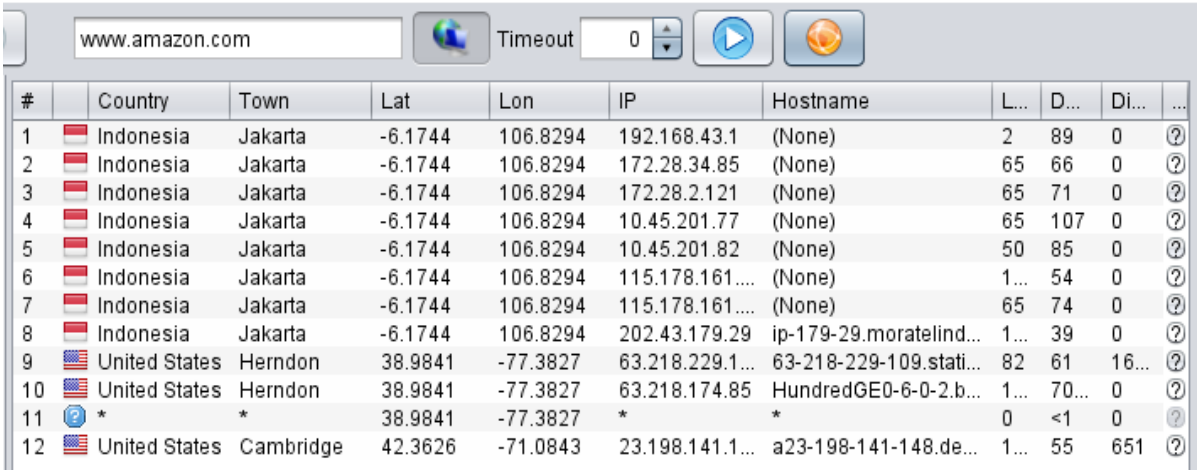
		oleh sv_subscriber_example.c dan sv_subscriber.c.

Jenis Daemon	CVE Name	Deskripsi
CloudFront	-	-

Hasil Traceroute (www.amazon.com**)**

Untuk mengetahui posisi router yang dilewati paket data.

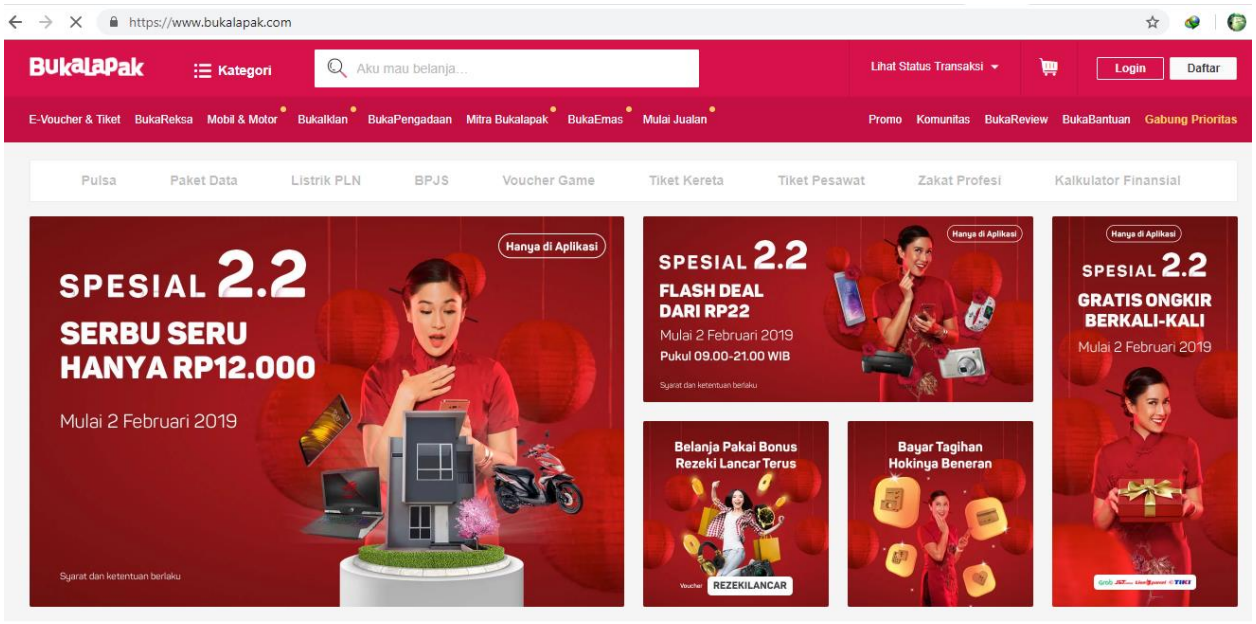




#		Country	Town	Lat	Lon	IP	Hostname	L...	D...	Di...	...
1		Indonesia	Jakarta	-6.1744	106.8294	192.168.43.1	(None)	2	89	0	
2		Indonesia	Jakarta	-6.1744	106.8294	172.28.34.85	(None)	65	66	0	
3		Indonesia	Jakarta	-6.1744	106.8294	172.28.2.121	(None)	65	71	0	
4		Indonesia	Jakarta	-6.1744	106.8294	10.45.201.77	(None)	65	107	0	
5		Indonesia	Jakarta	-6.1744	106.8294	10.45.201.82	(None)	50	85	0	
6		Indonesia	Jakarta	-6.1744	106.8294	115.178.161....	(None)	1...	54	0	
7		Indonesia	Jakarta	-6.1744	106.8294	115.178.161....	(None)	65	74	0	
8		Indonesia	Jakarta	-6.1744	106.8294	202.43.179.29	ip-179-29.moratelind...	1...	39	0	
9		United States	Herndon	38.9841	-77.3827	63.218.229.1...	63-218-229-109.stati...	82	61	16...	
10		United States	Herndon	38.9841	-77.3827	63.218.174.85	HundredGE0-6-0-2.b...	1...	70...	0	
11		*	*	38.9841	-77.3827	*	*	0	<1	0	
12		United States	Cambridge	42.3626	-71.0843	23.198.141.1...	a23-198-141-148.de...	1...	55	651	

3. Website dalam negeri

Salah satu contohnya yaitu website belanja online dalam negeri: www.bukalapak.com



Dengan menggunakan tools netcraft.com didapatkan bahwa target dari website belanja online luar negeri memiliki ip address 103.64.14.17 dengan domain bukalapak.com serta hosting history berisi informasi IP Address, Operating System, Daemon dan tanggal dari awal sampai terakhir diperbaharui.

Background

Site title	Situs Belanja Online dan Jual Beli Mudah Terpercaya | Bukalapak	**Date first seen**	December 2009
Site rank	98207	**Primary language**	Indonesian
Description	Situs jual beli online terpercaya di Indonesia. Belanja online murah, aman dan nyaman dari jutaan toko online pelapak Bukalapak garansi uang kembali		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://bukalapak.com	**Netblock Owner**	PT Bukalapak.com
Domain	bukalapak.com	**Nameserver**	ns-979.awsdns-58.net
IP address	103.64.14.17 (VirusTotal)	**DNS admin**	xinuc@bukalapak.com
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	resellercamp.com	**Nameserver organisation**	whois.markmonitor.com
Organisation	PT Bukalapak.com, Graha Prawira Lantai 2 Jl Mampang Prapatan Raya No 18, Jakarta Selatan, 12720, Indonesia	**Hosting company**	*unknown*
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT Bukalapak.com Corporate / Direct Member IDNIC Gd. Plaza Cityview lt 1 Jl. Kemang Timur No.22 Pejaten Barat Jakarta Selatan 12510	103.64.14.20	Linux	nginx	31-Dec-2018
PT Bukalapak.com Corporate / Direct Member IDNIC Gd. Plaza Cityview lt 1 Jl. Kemang Timur No.22 Pejaten Barat Jakarta Selatan 12510	103.64.14.18	Linux	nginx	12-Dec-2018
PT Bukalapak.com Corporate / Direct Member IDNIC Gd. Plaza Cityview lt 1 Jl. Kemang Timur No.22 Pejaten Barat Jakarta Selatan 12510	103.64.14.21	Linux	nginx	5-Nov-2018
PT Bukalapak.com Corporate / Direct Member IDNIC Gd. Plaza Cityview lt 1 Jl. Kemang Timur No.22 Pejaten Barat Jakarta Selatan 12510	103.64.14.20	Linux	nginx	24-Oct-2018
PT Bukalapak.com Corporate / Direct Member IDNIC Gd. Plaza Cityview lt 1 Jl. Kemang Timur No.22 Pejaten Barat Jakarta Selatan 12510	103.64.14.18	Linux	nginx	3-Sep-2018
PT Bukalapak.com Corporate / Direct Member IDNIC Gd. Plaza Cityview lt 1 Jl. Kemang Timur No.22 Pejaten Barat Jakarta Selatan 12510	103.64.14.17	Linux	nginx	20-Jun-2018
PT Bukalapak.com Corporate / Direct Member IDNIC Gd. Plaza Cityview lt 1 Jl. Kemang Timur No.22 Pejaten Barat Jakarta Selatan 12510	103.64.14.18	Linux	nginx	3-May-2018
PT.BUKALAPAK.COM Biznet Data Center Jakarta	182.253.238.102	Linux	nginx	7-Apr-2017
PT.BUKALAPAK.COM Biznet Data Center Jakarta	182.253.238.100	Linux	nginx	26-Mar-2017
PT.BUKALAPAK.COM Biznet Data Center Jakarta	182.253.238.102	Linux	nginx	24-Mar-2017

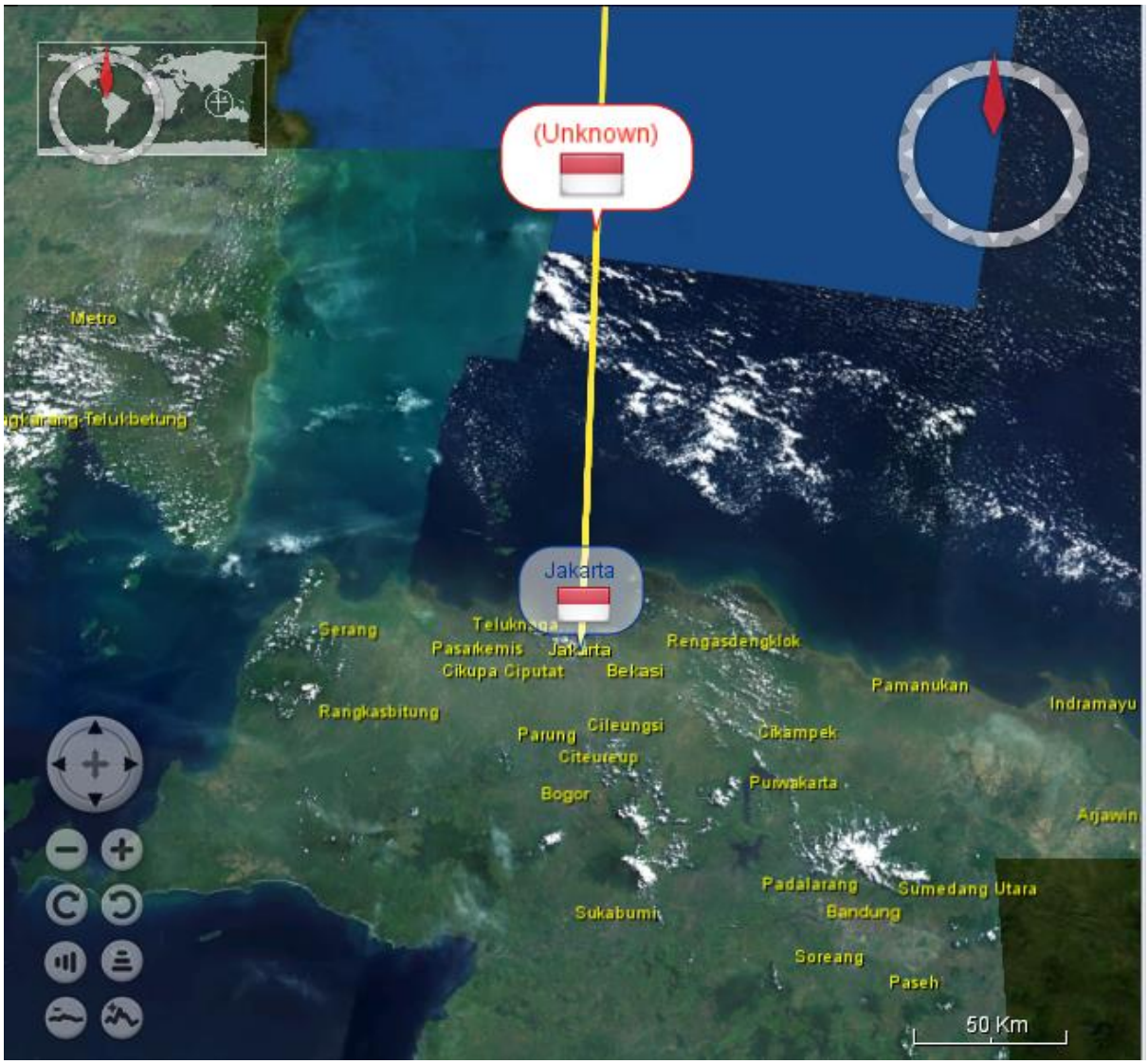
CVE (Common Vulnerabilities and Exposures List)

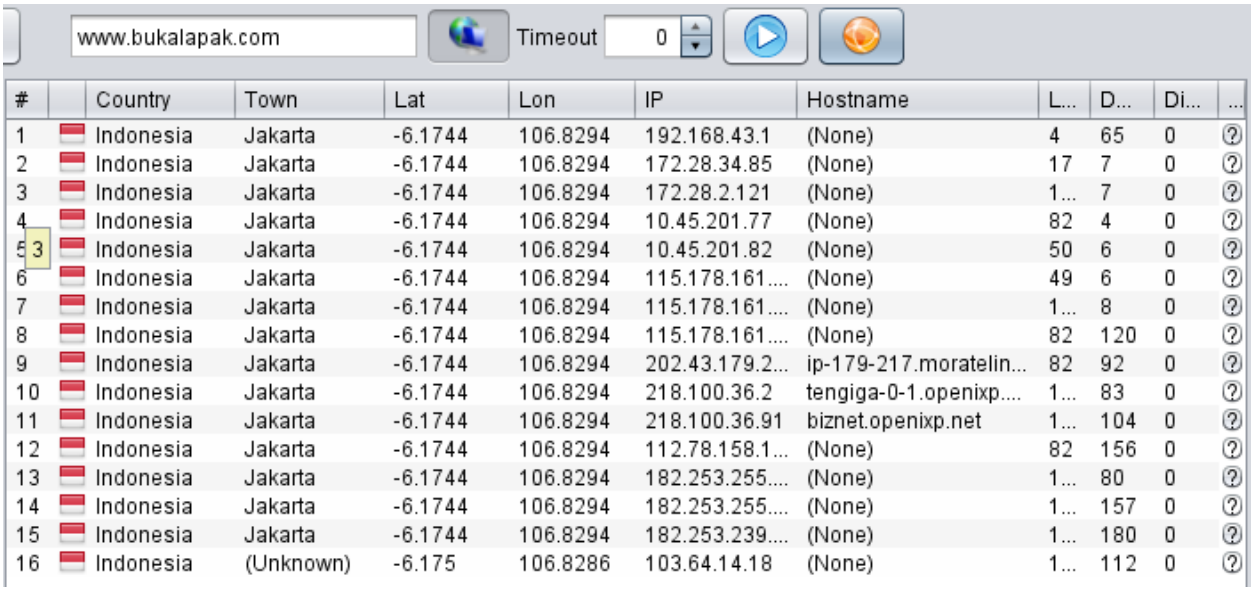
Jenis OS	CVE Name	Deskripsi
Linux	CVE-2019-7312	Pengungkapan plaintext terbatas ada di PRIMX Zed Entreprise untuk Windows sebelum 6.1.2240, Zed Entreprise for Windows (pengajuan kualifikasi ANSSI) sebelum 6.1.2150, Zed Entreprise untuk Mac sebelum 2.0.199, Zed Entreprise untuk Linux sebelum 2.0.199, Zed Pro for Windows sebelum 1.0.195, Zed Pro untuk Mac sebelum 1.0.199, Zed Pro untuk Linux sebelum 1.0.199, Zed Gratis untuk Windows sebelum 1.0.195, Zed Gratis untuk Mac sebelum 1.0.199, dan Zed Gratis untuk Linux sebelum 1.0. 199. Menganalisis wadah Zed dapat menyebabkan pengungkapan konten plaintext dari file yang sangat kecil (beberapa byte) yang disimpan di dalamnya.
	CVE-2019-7308	kernel / bpf / verifier.c di kernel Linux sebelum 4.20.6 melakukan spekulasi di luar batas yang tidak diinginkan pada aritmatika pointer dalam berbagai kasus, termasuk kasus cabang berbeda dengan keadaan berbeda atau batas sanitasi, yang mengarah ke serangan saluran samping.
	CVE-2019-6136	Masalah telah ditemukan di libIEC61850 v1.3.1. Ethernet_setProtocolFilter dalam hal / ethernet / linux / ethernet_linux.c memiliki SEGV, seperti yang ditunjukkan oleh sv_subscriber_example.c dan sv_subscriber.c.

Jenis Daemon	CVE Name	Deskripsi
nginx	CVE-2019-7401	NGINX Unit sebelum 1.7.1 memungkinkan penyerang menyebabkan buffer overflow berbasis heap dalam proses router dengan permintaan yang dibuat khusus. Ini dapat mengakibatkan penolakan layanan (proses router macet) atau mungkin memiliki dampak lainnya yang tidak ditentukan.

Hasil Traceroute (www.bukalapak.com **)**

Untuk mengetahui posisi router yang dilewati paket data.





#		Country	Town	Lat	Lon	IP	Hostname	L...	D...	Di...	...
1		Indonesia	Jakarta	-6.1744	106.8294	192.168.43.1	(None)	4	65	0	
2		Indonesia	Jakarta	-6.1744	106.8294	172.28.34.85	(None)	17	7	0	
3		Indonesia	Jakarta	-6.1744	106.8294	172.28.2.121	(None)	1...	7	0	
4		Indonesia	Jakarta	-6.1744	106.8294	10.45.201.77	(None)	82	4	0	
5	3	Indonesia	Jakarta	-6.1744	106.8294	10.45.201.82	(None)	50	6	0	
6		Indonesia	Jakarta	-6.1744	106.8294	115.178.161....	(None)	49	6	0	
7		Indonesia	Jakarta	-6.1744	106.8294	115.178.161....	(None)	1...	8	0	
8		Indonesia	Jakarta	-6.1744	106.8294	115.178.161....	(None)	82	120	0	
9		Indonesia	Jakarta	-6.1744	106.8294	202.43.179.2...	ip-179-217.moratelin...	82	92	0	
10		Indonesia	Jakarta	-6.1744	106.8294	218.100.36.2	tengiga-0-1.openixp....	1...	83	0	
11		Indonesia	Jakarta	-6.1744	106.8294	218.100.36.91	biznet.openixp.net	1...	104	0	
12		Indonesia	Jakarta	-6.1744	106.8294	112.78.158.1...	(None)	82	156	0	
13		Indonesia	Jakarta	-6.1744	106.8294	182.253.255....	(None)	1...	80	0	
14		Indonesia	Jakarta	-6.1744	106.8294	182.253.255....	(None)	1...	157	0	
15		Indonesia	Jakarta	-6.1744	106.8294	182.253.239....	(None)	1...	180	0	
16		Indonesia	(Unknown)	-6.175	106.8286	103.64.14.18	(None)	1...	112	0	