BEZPIECZEŃSTWO SERWERÓW
BŁĘDY, KTÓRYCH LEPIEJ NIE POPEŁNIĆ W KONFIGURACJI SERWERA

Borys Łącki

25/26.09.2017

BORYS ŁĄCKI

Od ponad 10 lat wykonując testy penetracyjne, ***testujemy bezpieczeństwo i zabezpieczamy*** *zasoby Klientów.*

LOGICALTRUST™

aruba CLOUD

AGENDA

1) Incydenty komputerowe
2) Konfiguracja serwera – najważniejsze problemy
3) DEMO: Błędy w konfiguracji serwera
4) Podsumowanie
5) Sesja pytań od uczestników

NAJCZĘSTSZE PROBLEMY

- Zbędne zasoby
- Błędne uprawnienia
- Brak aktualizacji
- Firewall
- Uwierzytelnianie

ZBĘDNE ZASOBY

0

#33083

Backup of wordpress configuration file found. Leaking database users/passwords

Share:

State	Resolved (Closed)	Severity	No Rating (---)
Disclosed publicly	**December 6, 2014 4:21pm +0100**	Participants	
Reported To	InVision	Visibility	Public (Full)
Scope			
Weakness	Information Disclosure		
Bounty	$300		

Collapse

TIMELINE

internetwache submitted a report to **InVision**. Oct 28th (3 years ago)

Hi there,

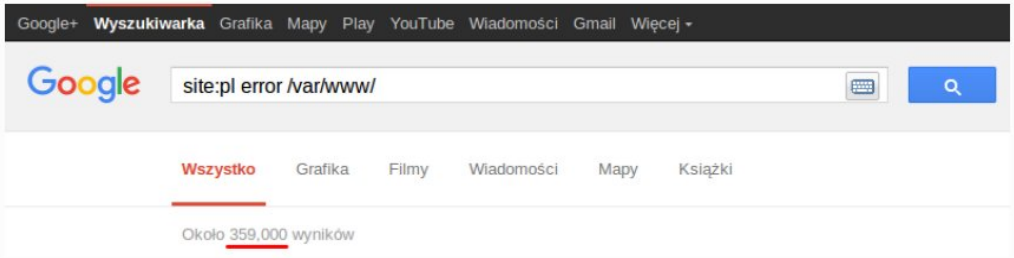
I noticed that there is a backup of the wordpress configuration file `wp-config.php.orig` publicly accessible.

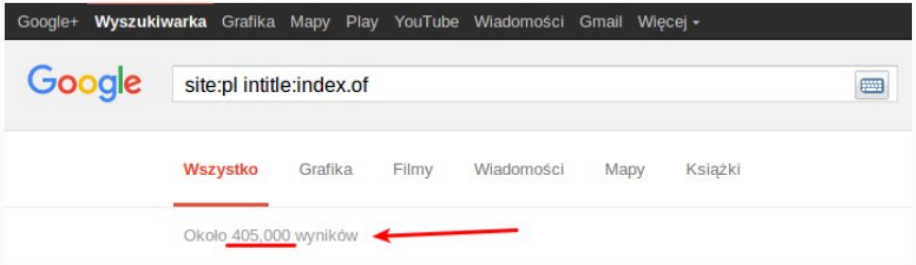
This file contains some sensitive information about your wordpress installation, including database users/passwords and secret tokens

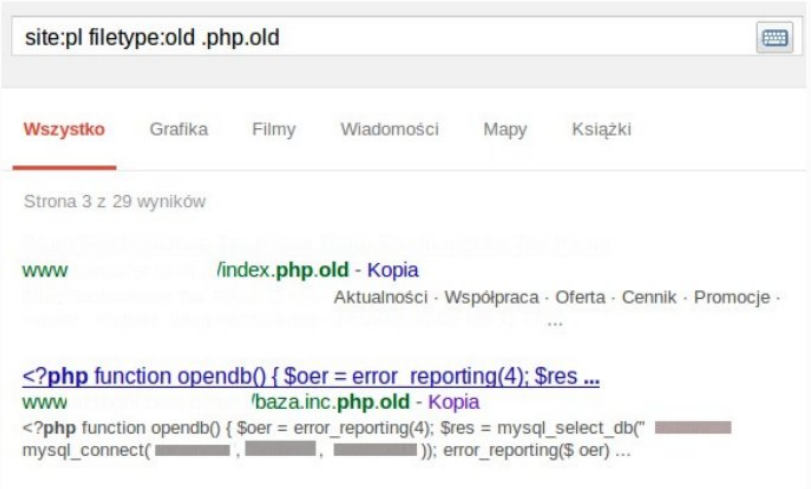
https://hackerone.com/reports/33083

aruba CLOUD

ZBĘDNE ZASOBY







ZBĘDNE ZASOBY

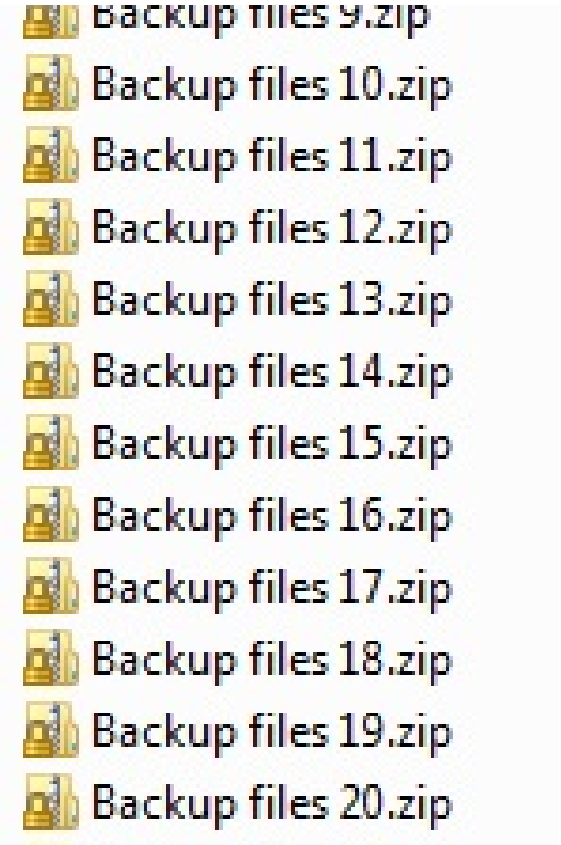
```
ls -ltr /tmp/

-rw-r--r-- 1 root  root   7077888 mar 15  2016 sqldump.tar.bz2
drwx------ 2 root  root      4096 kwi  3  2016 gpg-oqFS5S
-rw-r--r-- 1 root  root  12189696 maj 29 00:00 database.pgsql.gz
drwx------ 2 root  root      4096 wrz 12 00:00 lu9eqlt2.tmp
-rw------- 1 root  root         0 paź 14 08:41 config-err-97zpmD
```

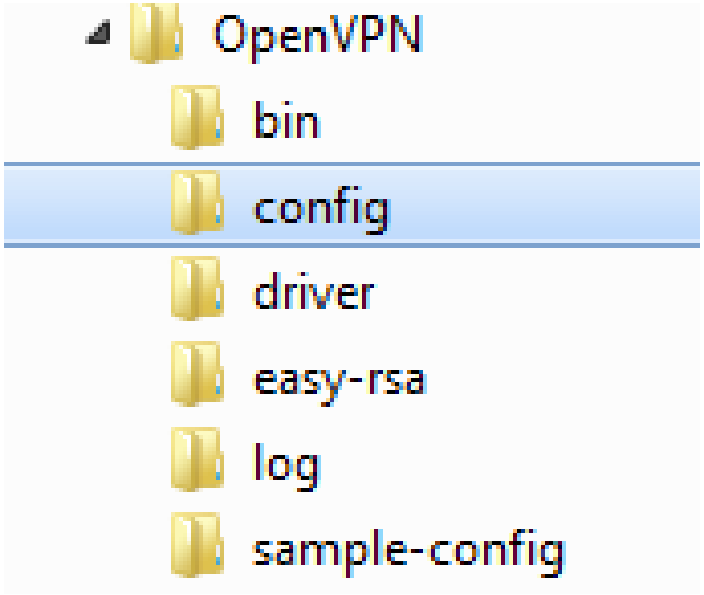
ZBĘDNE ZASOBY + CORE DUMPS

With a scan of the Alexa Top 1 Million domains for exposed core dumps I found around 1.000 vulnerable hosts. I was faced with a challenge: How can I properly disclose this? It is obvious that I wouldn't write hundreds of manual mails. So I needed an automated way to contact the site owners.

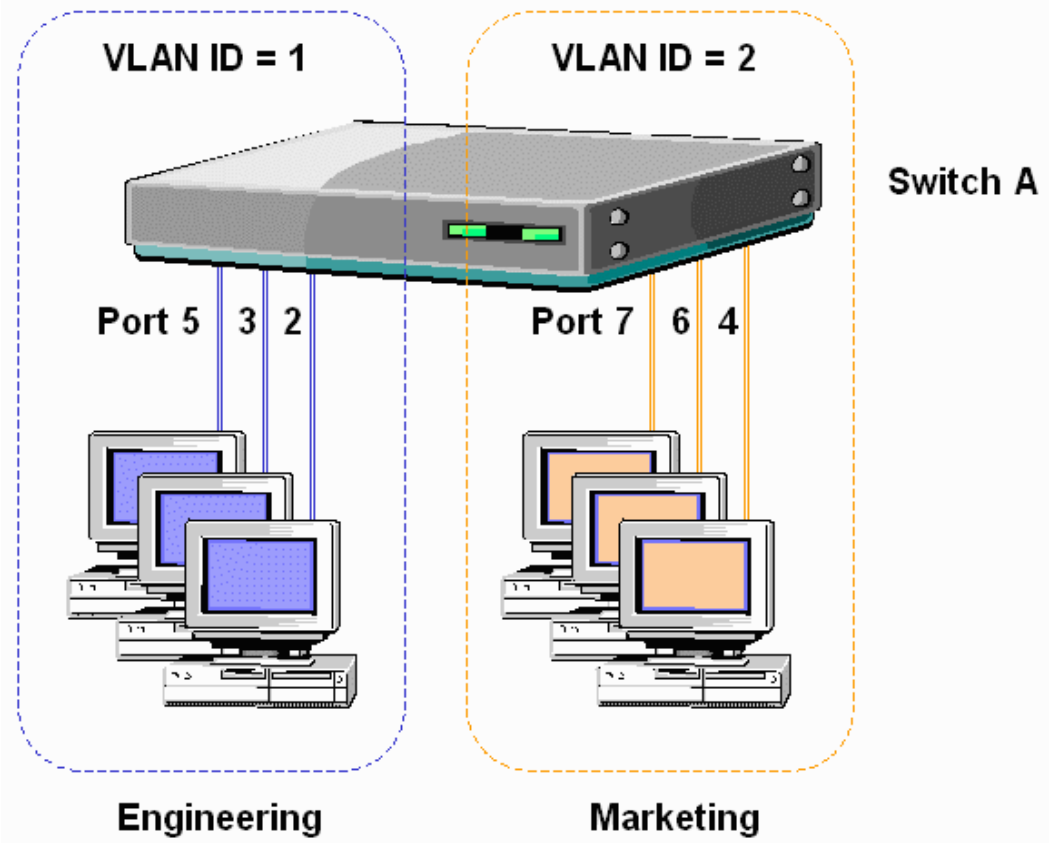
Abusix runs a service where you can query the abuse contacts of IP addresses via a DNS query. This turned out to be very useful for this purpose. One could also imagine contacting domain owners directly, but that's not very practical. The domain whois databases have rate limits and don't always expose contact mail addresses in a machine readable way.

ZBĘDNE ZASOBY





FIREWALL - BACKEND



FIREWALL / AUTH

Approximately 5,800 ATGs were found to be exposed to the internet without a password.

iptables -n -L INPUT

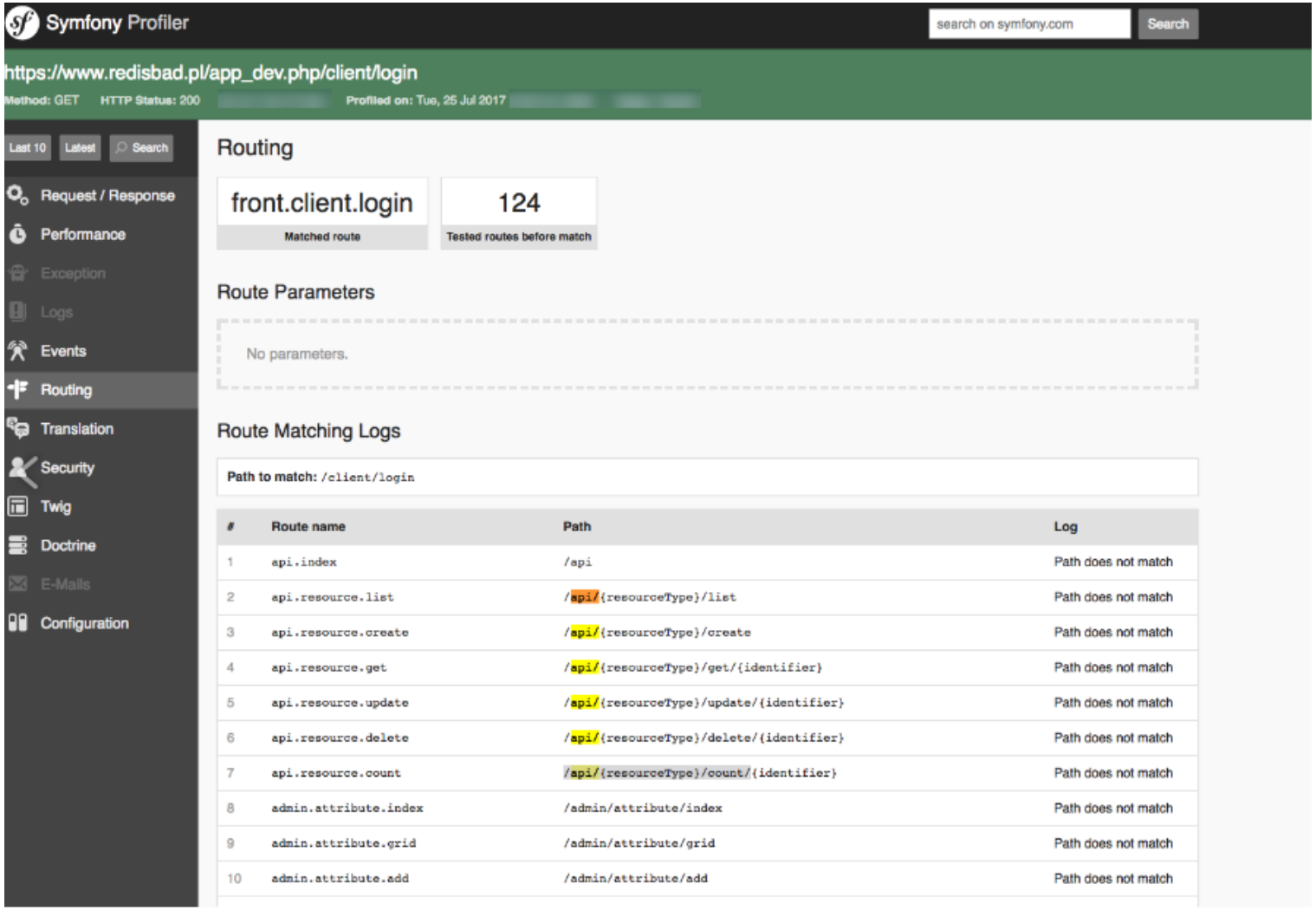
Chain INPUT (policy DROP)

ip6tables -n -L INPUT

Chain INPUT (policy ACCEPT)

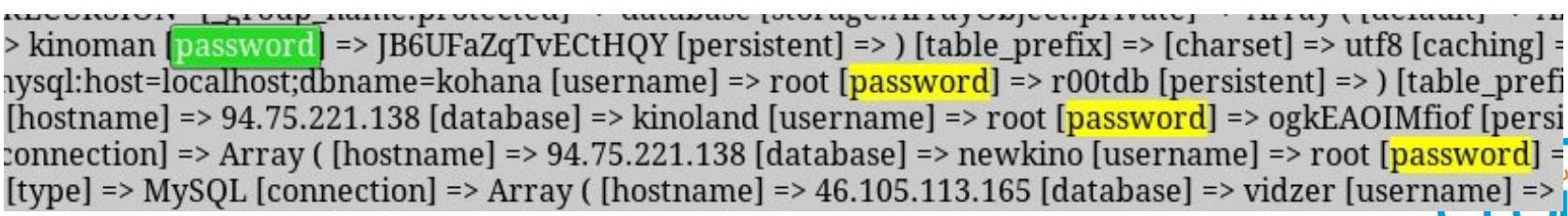
AKTUALIZACJE SYSTEMOWE

DEVEL

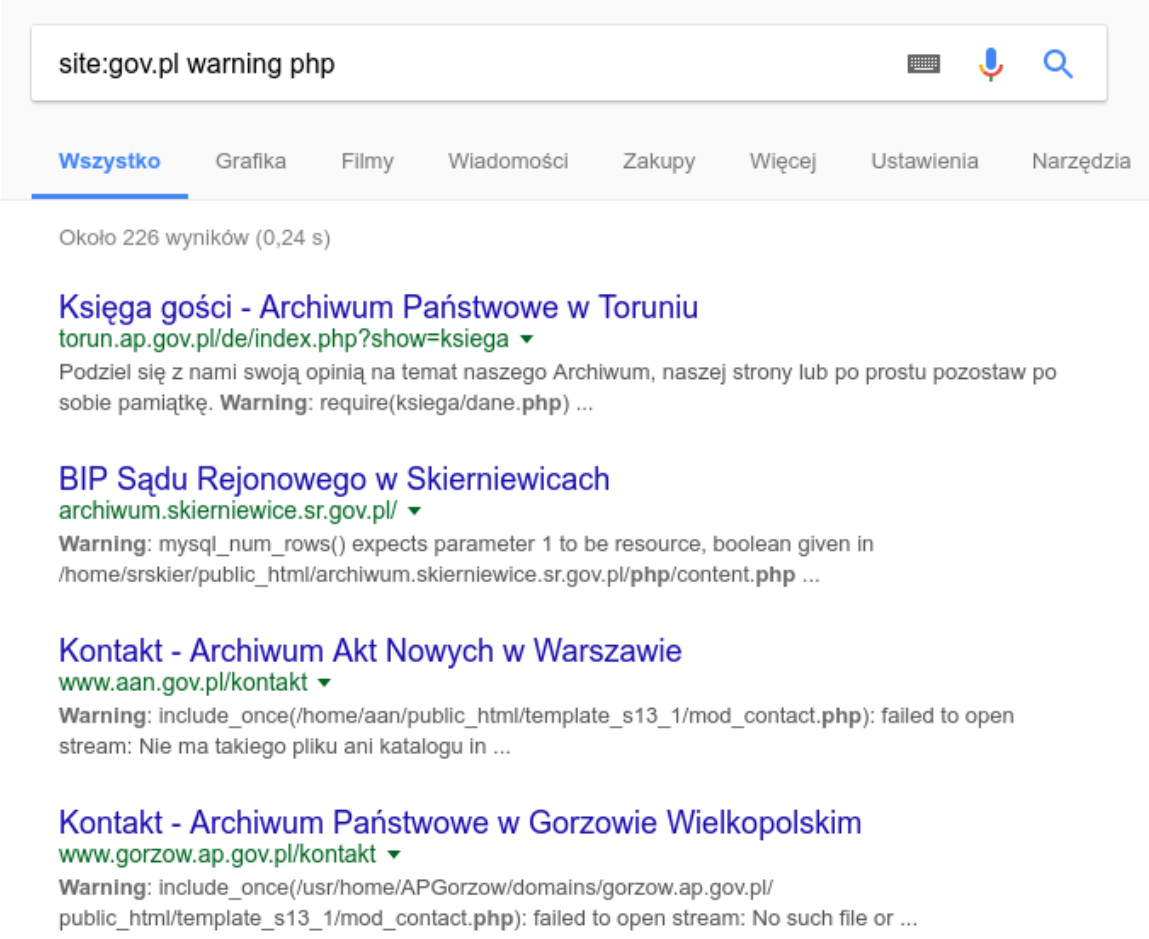

Symfony Profiler
search on symfony.com
Search
https://www.redisbad.pl/app_dev.php/client/login
Method: GET
HTTP Status: 200
Profiled on: Tue, 25 Jul 2017
Last 10
Latest
Search
Request / Response
Performance
Exception
Logs
Events
Routing
Translation
Security
Twig
Doctrine
E-Mails
Configuration
Routing
front.client.login
Matched route
124
Tested routes before match
Route Parameters
No parameters.
Route Matching Logs
Path to match: /client/login
Route name Path Log
1 api.index /api Path does not match
2 api.resource.list /api/{resourceType}/list Path does not match
3 api.resource.create /api/{resourceType}/create Path does not match
4 api.resource.get /api/{resourceType}/get/{identifier} Path does not match
5 api.resource.update /api/{resourceType}/update/{identifier} Path does not match
6 api.resource.delete /api/{resourceType}/delete/{identifier} Path does not match
7 api.resource.count /api/{resourceType}/count/{identifier} Path does not match
8 admin.attribute.index /admin/attribute/index Path does not match
9 admin.attribute.grid /admin/attribute/grid Path does not match
10 admin.attribute.add /admin/attribute/add Path does not match

DEBUG / DEVEL


http://www.kinoman.tv/
password
Find Previous
Find Next
Match case
Match whole word only
Done
Warning: file_put_contents(): Only 0 of 2227 bytes written, possibly out of free disk space in /data/www/kinoman.tv/system/classes/Kohana/Log/File.php on line 90
[[/OFF]] [[/MODE]] [random_vip] => 0 [right_block_cover] => [[MODE=guest]] [[/MODE]])) [cache] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => cache [storage:ArrayObject:private] => Array ([memcache2] => Array ([driver] => memcache [default_expire] => 15000 [compression] => [servers] => Array ([local] => Array ([host] => memcache_server [port] => 11211 [persistent] => [weight] => 1 [timeout] => 5 [retry_interval] => 15 [status] => 1)) [instant_death] => 1) [memcache] => Array ([driver] => memcache [default_expire] => 15000 [compression] => [servers] => Array ([local] => Array ([host] => localhost [port] => 11211 [persistent] => [weight] => 1 [timeout] => 5 [retry_interval] => 15 [status] => 1)) [instant_death] => 1) [file] => Array ([driver] => memcache [default_expire] => 3600 [compression] => [servers] => Array ([local] => Array ([host] => localhost [port] => 11211 [persistent] => [weight] => 1 [timeout] => 1 [retry_interval] => 15 [status] => 1)) [instant_death] => 1))) [inflector] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => inflector [storage:ArrayObject:private] => Array ([uncountable] => Array ([0] => access [1] => advice [2] => aircraft [3] => art [4] => baggage [5] => bison [6] => dances [7] => deer [8] => equipment [9] => fish [10] => fuel [11] => furniture [12] => heat [13] => honey [14] => homework [15] => impatience [16] => information [17] => knowledge [18] => luggage [19] => media [20] => money [21] => moose [22] => music [23] => news [24] => patience [25] => progress [26] => pollution [27] => research [28] => rice [29] => salmon [30] => sand [31] => series [32] => sheep [33] => sms [34] => spam [35] => species [36] => staff [37] => swine [38] => toothpaste [39] => traffic [40] => understanding [41] => water [42] => weather [43] => work) [irregular] => Array ([appendix] => appendices [cactus] => cacti [calf] => calves [child] => children [crisis] => crises [criterion] => criteria [curriculum] => curricula [diagnosis] => diagnoses [elf] => elves [ellipsis] => ellipses [foot] => feet [goose] => geese [hero] => heroes [hoof] => hooves [hypothesis] => hypotheses [is] => are [knife] => knives [leaf] => leaves [life] => lives [loaf] => loaves [man] => men [mouse] => mice [nucleus] => nuclei [oasis] => oases [octopus] => octopi [ox] => oxen [paralysis] => paralyses [parenthesis] => parentheses [person] => people [phenomenon] => phenomena [potato] => potatoes [quiz] => quizzes [radius] => radii [scarf] => scarves [stimulus] => stimuli [syllabus] => syllabi [synthesis] => syntheses [thief] => thieves [tooth] => teeth [was] => were [wharf] => wharves [wife] => wives [woman] => women [release] => releases))) [sphinx] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => sphinx [storage:ArrayObject:private] => Array ([host] => 127.0.0.1 [port] => 9313)) [oauth2] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => oauth2 [storage:ArrayObject:private] => Array ([facebook] => Array ([appId] => 324906367636346 [secret] => 716a984b6b40bbccce9c35cf1628f10d [redirect] => [name] => kinoman.tv) [google] => Array ([appId] => 28875767437-70u7r49v6l3crgmkekqtdcvmh3dcfo9v.apps.googleusercontent.com [secret] => M8qe8ForAl9AxmgC5lvLwJaU [redirect] => http://www.kinoman.tv/google [name] => kinoman.tv))))) [_group_name:protected] => website [storage:ArrayObject:private] => Array ([email_from] => noreply@kinoman.tv [email_from_name] => kinoman.tv [email_to] => help.kinoman@gmail.com [title] => filmy.pl [favicon] => favicon.png [files] => Array ([css] => Array ( ) [js] => Array ( )) [genders] => Array ([1] => Mężczyzna [2] => Kobieta) [avatar_path] => /data/www/kinoman.tv/s/a/ [gg_number] => ----- [player_width] => 631 [player_height] => 425 [static_server] => http://static.kinoman.tv/ [assets_server] => http://www.kinoman.tv/assets2/ [js_server] => http://www.kinoman.tv/ [css_server] => http://www.kinoman.tv/ [photos_server] => http://static.kinoman.tv/ [base_url] => http://www.kinoman.tv/ [plaques] => Array ([1] => Normalny [1] [2] => Zdejmowanie limitu [2] [3] => Film tylko w playerze bez limitu [3] [4] => Tylko dla VIP [4]) [template] => kinoman.tv)) [ads] => Config_Group Object ([_parent_instance:protected] => Config Object ([_sources:protected] => Array ([0] => Config_Database Object ([_loaded_keys:protected] => Array ([website] => Array ([player_height] => player_height [player_width] => player_width) [ads] => Array ([before_play] => before_play [before_wait_seconds] => before_wait_seconds [footer] => footer [footer_ad] => footer_ad [random_vip] => random_vip [right_block_cover] => right_block_cover [under_menu] => under_menu [under_slideshow_main] => under_slideshow_main)) [_db_instance:protected] => default [_table_name:protected] => config) [1] => Config_File Object ([_directory:protected] => config)) [_groups:protected] => Array ([database] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => database [storage:ArrayObject:private] => Array ([default] => Array ([type] => MySQL [connection] => Array ([hostname] => db_prod [database] => kinoman [username] => kinoman [password] => JB6UFaZqTvECtHQY [persistent] =>) [table_prefix] => [charset] => utf8 [caching] => 1) [alternate] => Array ([type] => PDO [connection] => Array ([dsn] => mysql:host=localhost;dbname=kohana [username] => root [password] => r00tdb [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>) [kinolive] => Array ([type] => MySQL [connection] => Array ([hostname] => 94.75.221.138 [database] => kinoland [username] => root [password] => ogkEAOIMfiof [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>) [kinolive_real] => Array ([type] => MySQL [connection] => Array ([hostname] => 94.75.221.138 [database] => newkino [username] => root [password] => ogkEAOIMfiof [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>) [topupload] => Array ([type] => MySQL [connection] => Array ([hostname] => 46.105.113.165 [database] => vidzer [username] => vidzer [password] => JEQFJSUIhasy8dh281 [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =>))) [website] => Config_Group Object ([_parent_instance:protected] => Config Object *RECURSION* [_group_name:protected] => website [storage:ArrayObject:private] => Array ([email_from] => noreply@kinoman.tv [email_from_name] => kinoman.tv [email_to] => help.kinoman@gmail.com [title] => filmy.pl [favicon] => favicon.png [files] => Array ([css] => Array ( ) [js] => Array ( )) [genders] => Array ([1] => Mężczyzna [2] => Kobieta) [avatar_path] => /data/www/kinoman.tv/s/a/ [gg_number] => ----- [player_width] => 631 [player_height] => 425 [static_server] => http://static.kinoman.tv/ [assets_server] => http://www.kinoman.tv/assets2/ [js_server] => http://www.kinoman.tv/ [css_server] => http://www.kinoman.tv/ [photos_server] => http://static.kinoman.tv/ [base_url] => http://www.kinoman.tv/ [plaques] => Array ([1] =>


> kinoman [password] => JB6UFaZqTvECtHQY [persistent] =>) [table_prefix] => [charset] => utf8 [caching] =
ysql:host=localhost;dbname=kohana [username] => root [password] => r00tdb [persistent] =>) [table_prefi
[hostname] => 94.75.221.138 [database] => kinoland [username] => root [password] => ogkEAOIMfiof [persi
connection] => Array ([hostname] => 94.75.221.138 [database] => newkino [username] => root [password] =
[type] => MySQL [connection] => Array ([hostname] => 46.105.113.165 [database] => vidzer [username] =>

DEBUG / DEVEL


site:gov.pl warning php
Wszystko
Grafika
Filmy
Wiadomości
Zakupy
Więcej
Ustawienia
Narzędzia
Około 226 wyników (0,24 s)
Księga gości - Archiwum Państwowe w Toruniu
torun.ap.gov.pl/de/index.php?show=ksiega
Podziel się z nami swoją opinią na temat naszego Archiwum, naszej strony lub po prostu pozostaw po sobie pamiątkę. Warning: require(ksiega/dane.php) ...
BIP Sądu Rejonowego w Skierniewicach
archiwum.skierniewice.sr.gov.pl/
Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in /home/srskier/public_html/archiwum.skierniewice.sr.gov.pl/php/content.php ...
Kontakt - Archiwum Akt Nowych w Warszawie
www.aan.gov.pl/kontakt
Warning: include_once(/home/aan/public_html/template_s13_1/mod_contact.php): failed to open stream: Nie ma takiego pliku ani katalogu in ...
Kontakt - Archiwum Państwowe w Gorzowie Wielkopolskim
www.gorzow.ap.gov.pl/kontakt
Warning: include_once(/usr/home/APGorzow/domains/gorzow.ap.gov.pl/public_html/template_s13_1/mod_contact.php): failed to open stream: No such file or ...

OPOWIEŚCI Z KRYPTY

<yyy> uy mnie w robocie gosc puscil TRUNCATE bazy na produkcji wklejajac sql z neta bez sprawdzenia

<xxx> u mnie puscil update tylko zapomnial dac where :D

OPOWIEŚCI Z KRYPTY

<xxx> prawie zawału dostałem
<xxx> wpadam sprawdzić, czy się dobrze backup zrobił
<xxx> patrzę, jest
<xxx> ale daty się nie zgadzają
<xxx> ostatni backup 04.2015
<xxx> ciśnienie mi się podniosło
<xxx> szukam patrzę
<xxx> a to stary serwer backupu
<xxx> nie zgasiliśmy go
<xxx> i sobie stoi

OPOWIEŚCI Z KRYPTY

postawiłem nowego debiana stretcha
prawie kompletnie z automaty poszło wiele rzeczy
sprawdzam auto firewalla
nie działa
patrze w ipsety - są
patrze w tablesy - są
skrypty patrzę - są
potem się okazało, że debian stretch wprowadził
numerację interfejsów jak ubuntu
enpsp0, a nie eth0
wszystko było
tylko nie było interfejsu
wiec firewall nic nie łapał

aruba CLOUD

BŁĘDNE UPRAWNIENIA

```
ls -ltr /etc/cron.daily/

-rwxr-xr-x 1 root root 15481 paź 28  2014 apt
-rwxr-xr-x 1 root root   625 lip 22  2014 apache2
-rwxr-xr-x 1 root root   123 sty 29  2014 tripwire
-rwxrwxrwx 1 root root   173 kwi  9  2016 database_update.sh
```

BŁĘDNE UPRAWNIENIA

```
-rw-r--r-- 1 root mlocate
20635027 lis  4 12:26
/var/lib/mlocate/mlocate.db
```

PROCESY

Invalid license data. Reinstall is required.

FIREWALL – “NA CHWILĘ WYŁĄCZONY”

Web Application Firewalls like the one that Barracuda Networks manufactures are designed to stop this type of attack from occurring in the first place, however they clearly are not the silver bullet against hackers. On their blog, Barracuda Networks admitted that they made several mistakes, the biggest of which was to unintentionally turn off their own firewall for a few hours. This was a golden window of opportunity which hackers pounced on and immediately exploited.

FIREWALL

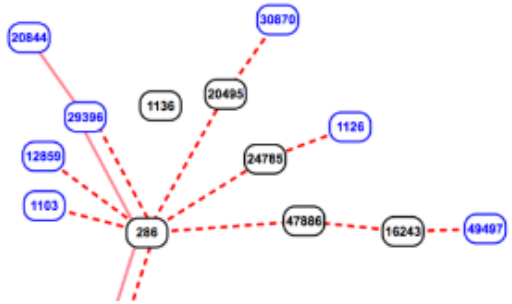
BGP leak causing Internet outages in Japan and beyond.

Posted by Andree Toonk - August 26, 2017 - BGP instability - No Comments

Yesterday some Internet users would have seen issues with their Internet connectivity, experiencing slowness or parts of the Internet as unreachable. This incident hit users in Japan particularly hard and it caused the Internal Affairs and Communications Ministry of Japan to start an investigation into what caused the large-scale internet disruption that slowed or blocked access to websites and online services for dozens of Japanese companies.

In this blog post we will take a look at the root cause of these outages, who was affected and what networks were involved.

Starting at 03:22 UTC yesterday (aug 25) followers of @BGPstream would have seen an increase in alerts involving Google. The BGPstream alerts were informing us that Google was announcing the peering lan prefixes of a few well known Internet exchanges. This in itself is actually a fairly common type of incident and typically indicates something isn't quite right within the networks hijacking those prefixes and so these alerts were the first clues that something wasn't quite right with Google's BGP advertisements.



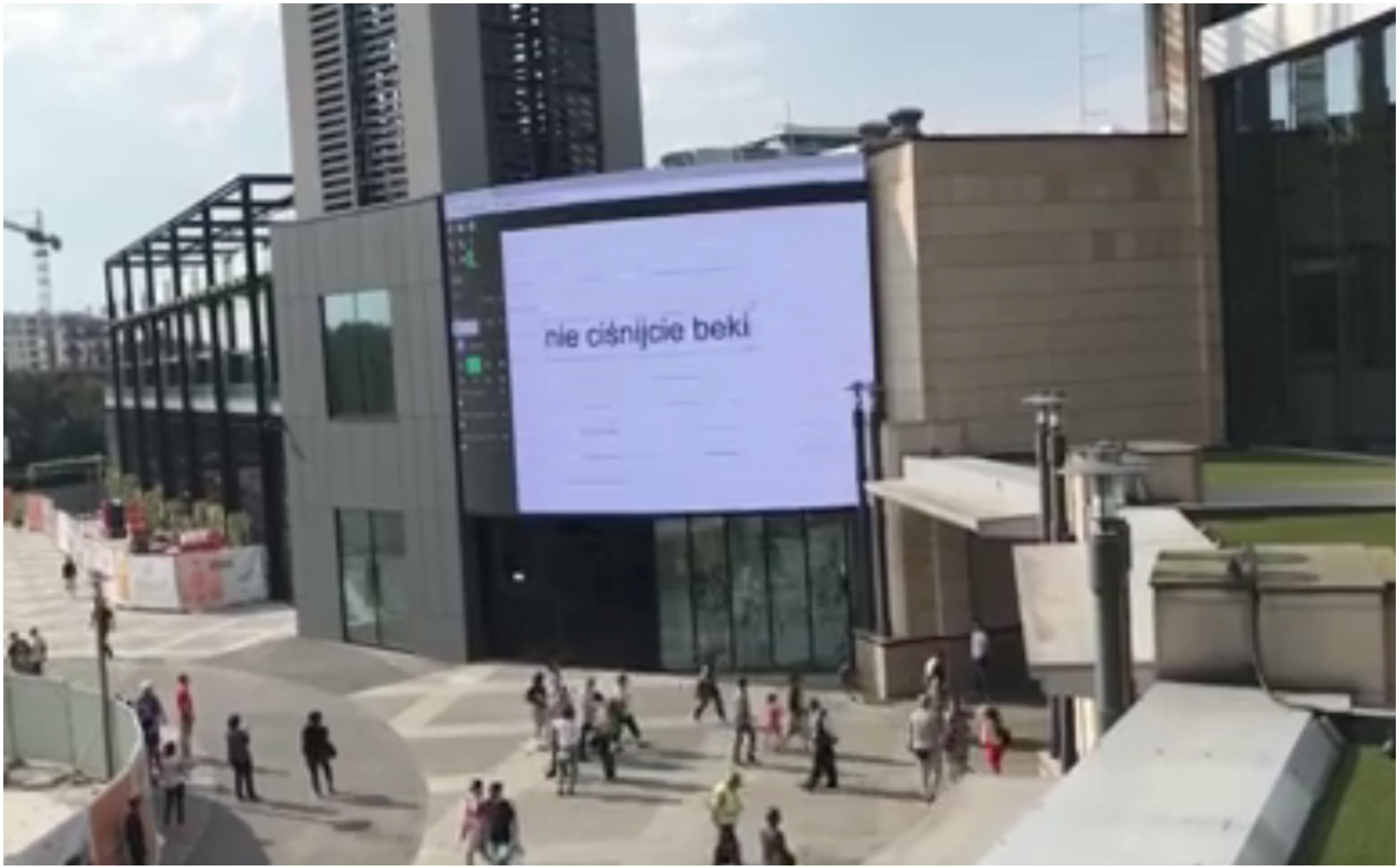
FIREWALL

But then one day, I saw one of the employees goofing off in some random chatroom. He explained that he had found it in the history tab after moving to a new computer. It was the site for a random radio station called Cities FM. I went to my own computer, and found many other sites I could access. The Center for Information Technology Integration. Cities Restaurant. The Cape IT Initiative. Random websites that had one thing in common. They started with the letters CITI.

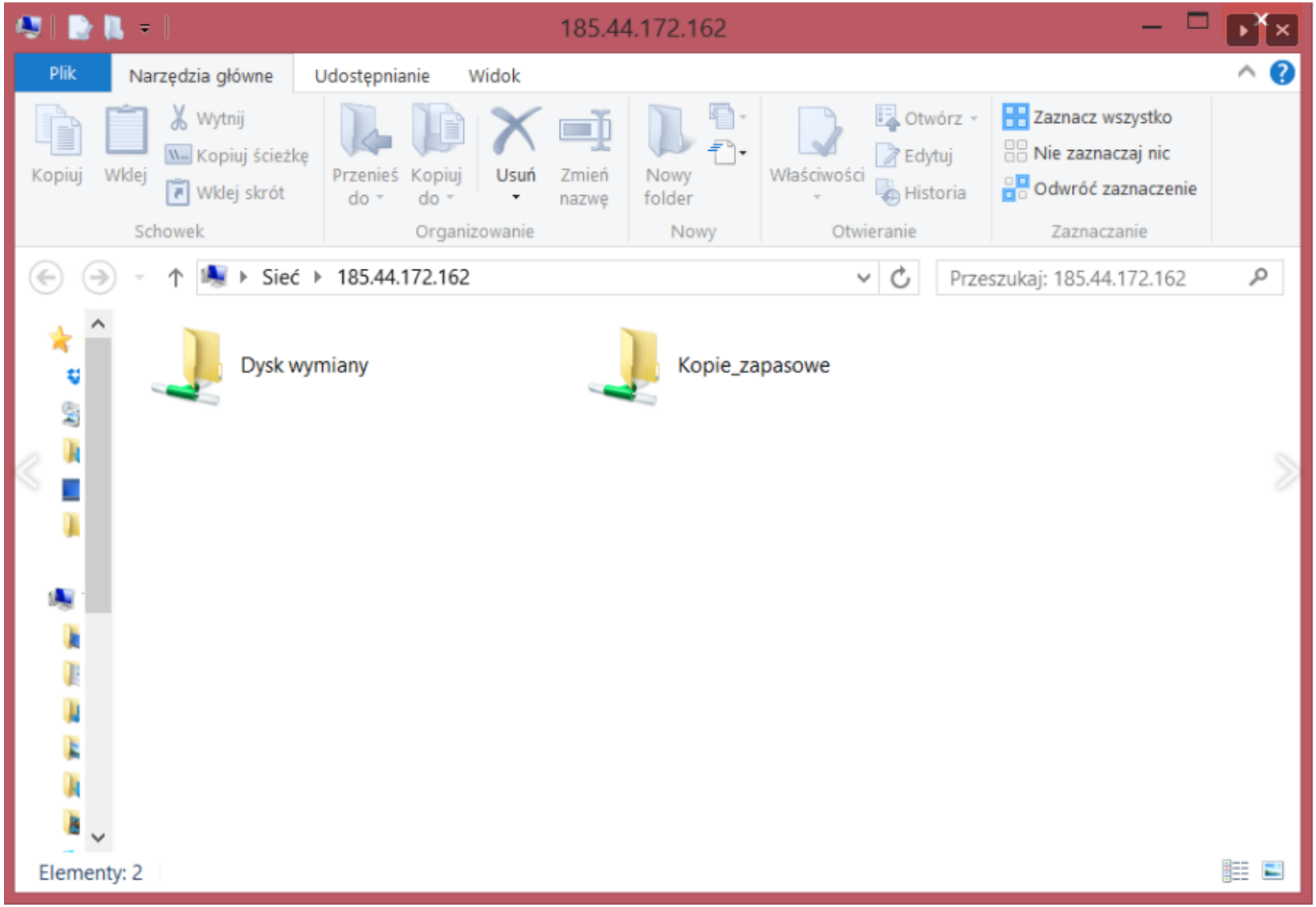
See, the employees needed to access the sites for the company they worked at. CitiBank, CitiMortgage, CitiFinancial... but since the company was constantly expanding, their IT department had decided that rather than keep updating the firewall, they would simply allow any site that started with the letters CITI, assuming that they would probably own it.

That night, I registered citi.MyName.com.

FIREWALL / AUTH



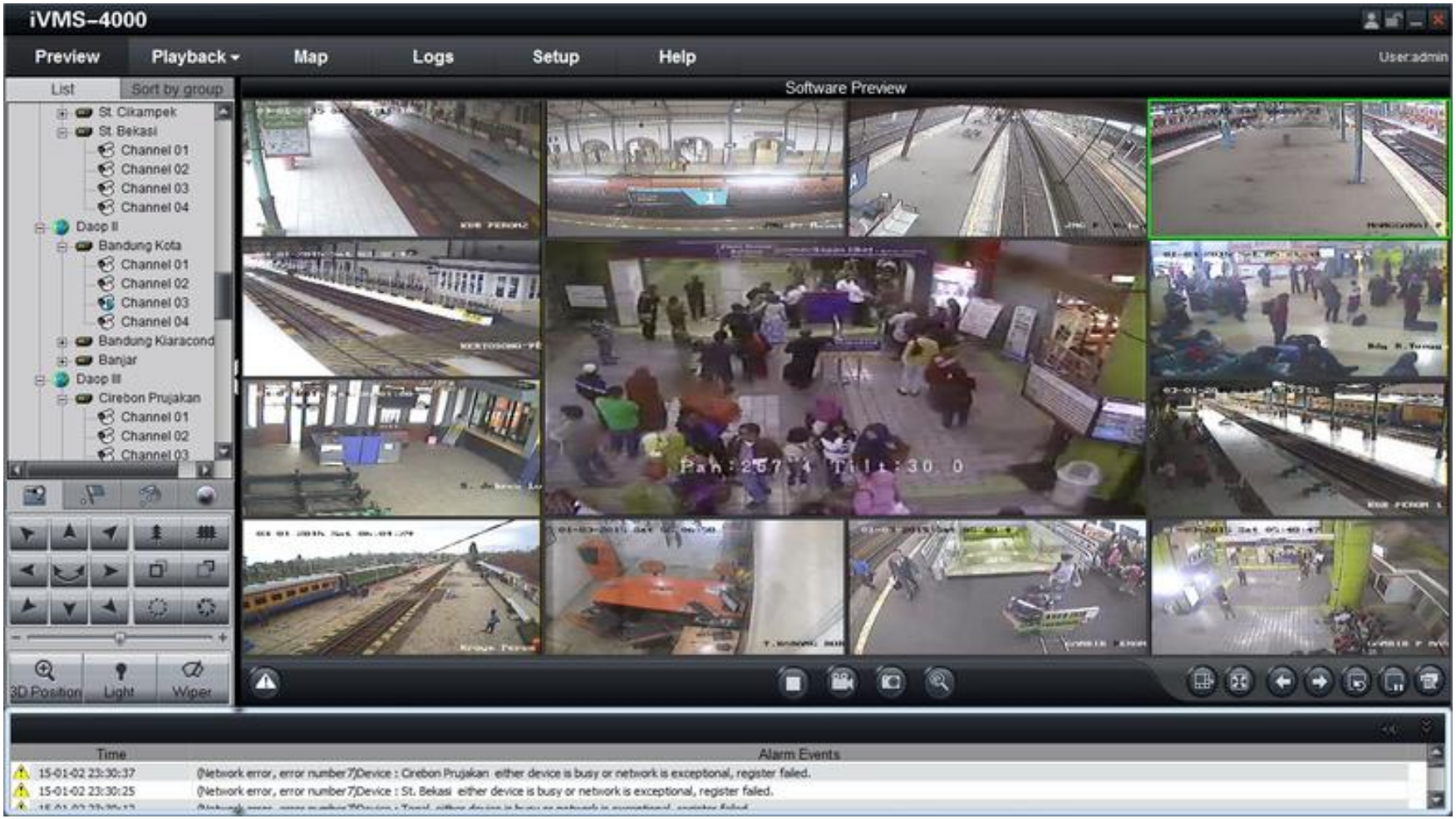
FIREWALL / AUTH



Gathering weak npm credentials

Or how I obtained direct publish access to 14% of npm packages (including popular ones).
The estimated number of packages potentially reachable through dependency chains is 54%.

FIREWALL / AUTH



DEMO

DOBRE PRAKTYKI

- Oddzielaj - sieci
- Aktualizuj - oprogramowanie
- Weryfikuj - ustawienia
- Ograniczaj - uprawnienia
- Porządkuj - dane
- Monitoruj - zasoby
- Dokumentuj - procesy
- Automatyzuj

SZKOLENIA - RABAT

https://z3s.pl/szkolenia/

Atak i obrona:

- **Bezpieczeństwo aplikacji WWW**
- **Bezpieczeństwo aplikacji mobilnych**

-10%

Obowiązuje 10 dni

Hasło: awdz9

Materiały

Odnośniki

- https://www.bleepingcomputer.com/news/security/ex-admin-deletes-all-customer-data-and-wipes-servers-of-dutch-hosting-provider/
- https://zaufanatrzeciastrona.pl/post/sklep-redisbad-udostepnia-bazy-danych-klientow-i-zamowien-bez-autoryzacji/
- https://zaufanatrzeciastrona.pl/post/jak-prosty-blad-wdrozeniowca-mogl-wylaczyc-rafinerie-i-spowodowac-milionowe-straty/
- http://www.antyradio.pl/Technologia/Duperele/Internetowi-zartownisie-zhakowali-gigantyczny-ekran-LED-Arkadii-16966
- https://www.networkworld.com/article/2221989/security/firewall-fail--a-tale-both-funny-and-sad.html
- http://www.zdnet.com/article/hacker-exposes-thousands-of-insecure-desktops-that-anyone-can-remotely-view/
- https://www.acunetix.com/blog/news/barracuda-networks-breached/
- https://bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/
- https://blog.hboeck.de/archives/887-Dont-leave-Coredumps-on-Web-Servers.html
- https://github.com/ChALkeR/notes/blob/master/Gathering-weak-npm-credentials.md
- https://zaufanatrzeciastrona.pl/post/wyciek-danych-wrazliwych-50-tysiecy-pacjentow-polskiego-szpitala/

Ikony: https://www.iconfinder.com/Vecteezy

Dziękuję za uwagę

Borys Łącki

b.lacki@logicaltrust.net

www.arubacloud.pl