

# Experiences with Paste-Monitoring

## OWASP BeNeLux Day 2016



**CIRCL**  
Computer Incident  
Response Center  
Luxembourg

Michael Hamm - *TLP:WHITE*

[info@circl.lu](mailto:info@circl.lu)

17.-18. March 2016;  
Esch-Belval, Luxembourg



**CIRCL**

Computer Incident  
Response Center  
Luxembourg

- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.
- CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg.

# CERT point of view

---

- Help
  - Acts like a fire brigade
  - Take all reported incidents serious
  - Help: triage, analysis and response
  - Help: technical investigation
  - Reliable and trusted point of contact
  - No duty to report to the police
  - Victim's duty to file a complaint
- Prevent incidents
  - Early detection
  - Proactive security

## CERT services/tools

---

- Malware Information Sharing Platform - MISP
  - <https://www.circl.lu/services/misp-malware-information-sharing-platform/>
- URL Abuse Testing
  - <https://www.circl.lu/services/urlabuse/>
- Dynamic Malware Analysis Platform - DMA
  - <https://www.circl.lu/services/dynamic-malware-analysis/>
- Paste Monitoring & Analysis of Information Leaks Framework - AIL
  - <https://github.com/CIRCL/pystemon>
  - <https://github.com/CIRCL/AIL-framework>

# Paste Monitoring

---

- Example: <http://pastebin.com/>
  - Store text online, easy sharing
  - Used by programmers
  - Source code & configuration information
- Abused by attackers to store:
  - Exploit code
  - Results of running malicious code
  - D0x
  - List of open proxys
  - Anouncements OP...
  - ->Examples: #OpAlQeeq #OpIsrael #OpSaveGaza

# Paste Monitoring: General examples

---

```
text 1.79 KB raw download clone embed report print
1. ████████████████████████████████████████████████████████████████
2. impact-mailorder.de hacked by National Sozialistische Hacker Crew
3. ████████████████████████████████████████████████████████████████
4. Seid gegrüsst Zeckenpack!!
5. Da ihr hinterlistigen Abschaum-Gestalten immer wieder Angriffe auf unsere Shops und unsere Seiten unternimmt und
   anschließend die Daten online stellt, dachten wir uns, wir drehen den Spieß mal um!
6.
7. Wir haben nun Namen, Adressen und Telefonnummern, allen die jemals in diesem Shop bestellt haben.
8. Wir werden davon 40'000 sofort veröffentlichen.
9. Die restlichen werden wir noch behalten.
10. Mit jedem Hackerangriff von linksgerichteten Ursprungs auf nationale Adressen werden weitere 10'000 Daten
    veröffentlicht!
11.
12. Es grüsst der Nationale Widerstand, alle Kameraden!
13.
14. Und euch Zeckenpack sei gesagt: WE ARE WATCHING YOU!
15. ████████████████████████████████████████████████████████████████
16. Die ersten 40'000 Daten
17. Formation:
18. Name:Vorname:Nachname:Strasse:Ort:Land:Nummer:Email
19. Download Links:
20. http://krautchan.net/files/1421870955001.zip
21. https://neuschwabenland.org/m/src/1421870955001.zip
22. http://ww67.zippyshare.com/v/P9hVIhBK/file.html
```

# Paste Monitoring: General examples

---

[#OpISIS- Expose & Destroy By Anonymous RedCult - Pastebin.com](#)

[pastebin.com/d8ND4rvV](https://pastebin.com/d8ND4rvV)

Feb 8, 2015 ... **We are Anonymous**. We are Legion, We do not forgive, We do not forget, Expect us. -Now, Some of ISIS's Twitter accounts, Sites, Emails that ...

[OPisis \*\*WE ARE ANONYMOUS\*\* - Pastebin.com](#)

[pastebin.com/PkM9A6iv](https://pastebin.com/PkM9A6iv)

OPisis **WE ARE ANONYMOUS**. a guest Jan 3rd, 2016 60 Never. rawdownload cloneembedreportprint text 2.36 KB. These are isis accounts and supporter ...

[Greetings citizens of the world. \*\*We are anonymous\*\*. The Flint water ...](#)

[pastebin.com/1VHdK8MM](https://pastebin.com/1VHdK8MM)

Jan 29, 2016 ... **We are anonymous**. The Flint water crisis has drawn the attention of anonymous. Anonymous would first like to pay respect to the victims of this ...

[We are Anonymous #opjapane - Pastebin.com](#)

[pastebin.com/59RVYN9f](https://pastebin.com/59RVYN9f)

12 hours ago ... **We are Anonymous**. #opjapane. RAW Paste Data. **We are Anonymous** # opjapane. create new paste / api / trends / syntax languages / faq ...

[Hundreds of ISIS Accounts! - Pastebin.com](#)

[pastebin.com/N9rPZ3Ar](https://pastebin.com/N9rPZ3Ar)

Nov 15, 2015 ... **We Are Anonymous**.. We Do Not Forgive.. We Do Not Forget.. Expect us! We are the collective today we bring you a mass amount of isis twitter ...

[\[APT Sources\] \*\*We are #Anonymous\*\* - Pastebin.com](#)

[pastebin.com/8EF3NyhM](https://pastebin.com/8EF3NyhM)

Aug 12, 2015 ... Kancolle Summer Event 2015: Limited Time Area "Counter Attack! Second SN Operation" will start soon! The operation will last around 20 days ...

# Paste Monitoring

---

- Results of running malicious code
  - Results of port- and vulnerability scans
  - Lists with vulnerable sites
  - Lists with compromised sites
  - Database dumps
  - Credit Card details
  - Leaked 3rd party credentials



# Paste Monitoring: General examples

---

```
22. [*] Nmap scan report for 1[REDACTED].p.de (85[REDACTED] 227.180)
23. Host is up (0.016s latency).
24. Not shown: 64983 closed ports
25.
26. PORT      STATE SERVICE
27. 21/tcp    open  ftp
28. 80/tcp    open  http
29. 111/tcp   open  rpcbind
30. 139/tcp   filtered netbios-ssn
31. 443/tcp   open  https
32. 445/tcp   filtered microsoft-ds
33. 3306/tcp  open  mysql
34. 4224/tcp  open  xtell
35. 5666/tcp  filtered nrpe
36. 8193/tcp  open  sophos
37. 25561/tcp open  unknown
38. 25565/tcp open  minecraft
39. 25665/tcp filtered unknown
40. 33517/tcp open  unknown
41. 36123/tcp open  unknown
42. 44121/tcp open  unknown
43. 47084/tcp open  unknown
```

# Paste Monitoring

---

- Statistics
  - Monitoring up to 30 sources
  - Average 1.800.000 pastes/month
  - >100 keywords (constituency)
  - Leads to 5.250 tickets/month
  - Leads to 35 incidents/month
  - Leads to 140 investigation/month
  - Average 7 investigations/day
  - One investigation: 5 minutes - 1 hours
- Challenges
  - Unstructured data

# CIRCL #219393 List of URLs

---

<http://www.gasxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://burytoxxx.co.uk/images/jdownloads/screenshots/spy.gif>  
<http://sheriasxxx.coop/images/jdownloads/screenshots/spy.gif>  
<http://www.exxxx.org/images/jdownloads/screenshots/spy.gif>  
<http://www.bexxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://south-xxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://ixxx.org/images/jdownloads/screenshots/spy.gif>  
<http://www.exxxx.com.au/images/jdownloads/screenshots/spy.gif>  
<http://www.alphamxxxxxxxx.co.za/images/jdownloads/screenshots/spy.gif>  
<http://www.tablemxxxxxxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://www.dubairealdxxxxxxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://www.world-xxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://www.nepalmxxxxxxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://www.proxxx.xxx.gov.ph/images/jdownloads/screenshots/spy.gif>  
<http://www.ajxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://www.fcfmixxxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://mdxxxx.org/images/jdownloads/screenshots/spy.gif>  
<http://www.lsxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://pxxxx.com/images/jdownloads/screenshots/spy.gif>  
<http://www.contxxxx.net/images/jdownloads/screenshots/spy.gif>  
<http://info.farmixxxxx.fi/images/jdownloads/screenshots/spy.gif>  
<http://www.flxx.be/images/jdownloads/screenshots/spy.gif>  
<http://www.solidxxx.at/images/jdownloads/screenshots/spy.gif>  
<http://www.xxxx.xtc.br/images/jdownloads/screenshots/spy.gif>  
<http://www.fexxxx.at/images/jdownloads/screenshots/spy.gif>  
<http://ontarioxxxxxxxx.ca/images/jdownloads/screenshots/spy.gif>

# CIRCL #219393 What is behind this URLs?

---

<http://www.pxxxxx.xxx.gov.ph/images/jdownloads/screenshots/spy.gif>

<http://www.xxxxx.gov.zm/images/jdownloads/screenshots/spy.gif>

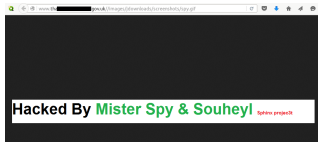
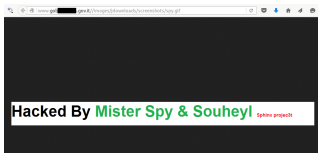
<http://www.xxx.gov.zm/images/jdownloads/screenshots/spy.gif>

<http://www.xxxxx.gov.zm/images/jdownloads/screenshots/spy.gif>

<http://www.xxxxxxxxxxxx.gov.it/images/jdownloads/screenshots/spy.gif>

<http://www.xxxxxxxxxxxx.gov.uk/images/jdownloads/screenshots/spy.gif>

<http://www.gxxxxxxxxxxx.gov.it/images/jdownloads/screenshots/spy.gif>



# CIRCL #223483 What is behind this URLs?

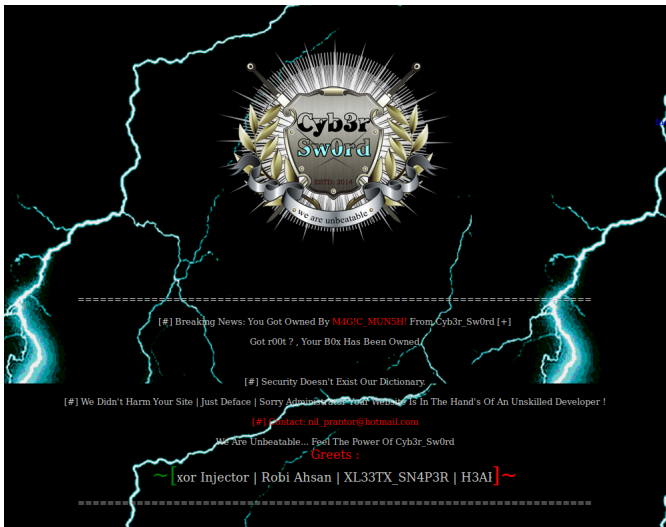
---

 **BirthDay Wish...**  
A GUEST MAR 15TH 2016 @ 10 NEVER

```
text 15:03:00 [row]
1. http://www. [redacted] -sursubu.com/
2. http://club [redacted] hen.com/
3. http://image [redacted]
4. http://wdd [redacted] .html
5. http://law [redacted] index.html
6. http://shop [redacted] com/index.html
7. http://med [redacted] eslondon.com/
8. http://host [redacted] s.tk/
9. http://best [redacted] ing.tk/
10. http://soc [redacted] es.com/
11. http://we [redacted] t.tk/
12. http://cr [redacted] ore.tk/
13. http://be [redacted] efor-home.tk/
14. http://exp [redacted] an1ic.com/
15. http://hea [redacted] rowoman.com/
16. http://soc [redacted] l/
17. http://the [redacted] s.tk/
18. http://best [redacted] dserver.nl/
```

# CIRCL #223483 Defacements

---



## Results of running malicious code

---

- How can we help?
  - Report to the website owner (constituency)
  - -> Give advices to them
  - Report to other CERTs
- What we can not do?
  - Contact all website owners outside our constituency

# CIRCL #215347 The posting

---

Target = cpluxxxxxxxxx.com

zul.xxxxx@ymail.com:5a9ac42d67ab0f139848bb0404355051e0dc6fcd10a22e2ca  
ziyanxxxx@yahoo.com:46fe7a6944f6f2bfcfbfdef6f06850d94eec1dc02b7722504  
xxxxx@teclait.com:092cb6b0a6fb718f20f7704b41173ed52e938432f34a6f389  
bscxxxx@yahoo.com:d93999a44413a63f2dd4e176a349728a23f73aac492a69fcc  
yxxxxx@yahoo.com:e1171a55671a08ec2350902199ba774f82e95f34efe762616  
yoogesxxxx@yahoo.com:451a40fb63d53411f86f4f49b21cc468b058c59a4d41f2fe2  
yixxxxx@upei.ca:614a858c8643cf7e307fd634364f7d6c235f96837c49d0bd4  
yinguxxxxx@ou.edu:e85962e3ee35e3f90fb356485c8ebe5b9ec042bac77f1c190  
ygxxxxxx@gmail.com:80674b810fc53e53e048f6aacc3c055ddeb349998b9fc5b1a  
yemioyxxxx@yahoo.com:80a0a943d1f509925c7c5552842b4624c2b8effa0d2ec1791  
yanninxxxx@hotmail.com:c18d74cdda28c86615474636d20e2dc5c0b6f2605d570717a  
yanghxxxx@gmail.com:bd4ccc43e5eeee42ec13879f9b0dfd3c5f519658638f3f90  
yahya.xxxxx@gmail.com:e61a87f807ec0e2d3f936a7cec7cb5dca8291060ddd212b4b  
bendehbia.xxxxx@hotmail.fr:65324f3ad8e3e85a51740787cf1d1d4bba5c0b84e130e7c60  
write2sxxxxxxxx@gmail.com:20404051a1d5e96aa0f3a038bd15ce8854b8bbc9b67c2883c  
wmsxxxx@comcast.net:334780689a0ff89ee1034e909bb0bb0bfb4fd732afd7658cf  
wincyxxx@hotmail.com:681505cf1cb3907277a081c34c1b72df800d0279d48804e38  
jacktxxxx@yahoo.com:51d94e5885764f3aec7058ba3f28107bcf49c5e79401c3fd6  
whitegxxxxx@yahoo.com:79918c71701ab71bae7d700d67fd286d21b2f9c3ec513b7e1  
whitegxxxxx@gmail.com:bc3950cf307a9bc54f103a7ed5275bf724b485c6f1b406bdd



# Leaked 3rd party credentials

---

- How can we help?
  - Report to the ISPs (constituency)
  - ->Advice victims to change this password
  - ->Change it everywhere
  - Report to the targeted website owner
  - Report to other CERTs

## What to avoid to report?

- Re-postings
- Old passwords
- Issues that are already fixed
- Unknow targeted site
- Encrypted passwords
- ->We can give no advices

# CIRCL #215347 The posting

---

Target = cpluxxxxxxxxx.com

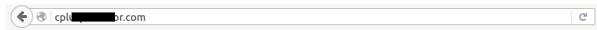
zul.xxxxx@ymail.com:5a9ac42d67ab0f139848bb0404355051e0dc6fcd10a22e2ca  
ziyanxxxx@yahoo.com:46fe7a6944f6f2bfcfbfdef6f06850d94eec1dc02b7722504  
xxxxx@teclait.com:092cb6b0a6fb718f20f7704b41173ed52e938432f34a6f389  
bscxxxx@yahoo.com:d93999a44413a63f2dd4e176a349728a23f73aac492a69fcc  
yxxxxx@yahoo.com:e1171a55671a08ec2350902199ba774f82e95f34efe762616  
yooGesxxxxx@yahoo.com:451a40fb63d53411f86f4f49b21cc468b058c59a4d41f2fe2  
yixxxxx@upei.ca:614a858c8643cf7e307fd634364f7d6c235f96837c49d0bd4  
yinguxxxxx@ou.edu:e85962e3ee35e3f90fb356485c8ebe5b9ec042bac77f1c190  
ygxxxxxx@gmail.com:80674b810fc53e53e048f6aacc3c055ddeb349998b9fc5b1a  
yemioyxxxxx@yahoo.com:80a0a943d1f509925c7c5552842b4624c2b8effa0d2ec1791  
yanninxxxxx@hotmail.com:c18d74cdda28c86615474636d20e2dc5c0b6f2605d570717a  
yanghxxxxx@gmail.com:bd4ccc43e5eeee42ec13879f9b0dfd3c5f519658638f3f90  
yahya.xxxxx@gmail.com:e61a87f807ec0e2d3f936a7cec7cb5dca8291060ddd212b4b  
bendehbia.xxxxx@hotmail.fr:65324f3ad8e3e85a51740787cf1d1d4bba5c0b84e130e7c60  
write2sxxxxxxxxx@gmail.com:20404051a1d5e96aa0f3a038bd15ce8854b8bbc9b67c2883c  
wmsxxxxx@comcast.net:334780689a0ff89ee1034e909bb0bb0bfb4fd732afd7658cf  
wincyxxx@hotmail.com:681505cf1cb3907277a081c34c1b72df800d0279d48804e38  
jacktxxxxx@yahoo.com:51d94e5885764f3aec7058ba3f28107bcf49c5e79401c3fd6  
whitegxxxxxx@yahoo.com:79918c71701ab71bae7d700d67fd286d21b2f9c3ec513b7e1  
whitegxxxxxx@gmail.com:bc3950cf307a9bc54f103a7ed5275bf724b485c6f1b406bdd

# CIRCL #215347 Analysis Stage 1

---

- What do we get
  - Email addresses : encrypted passwords
  - Bingo: Target site is quoted

Review the site:



The website is down for maintenance for a few days.  
Thank you for your patience.

# CIRCL #215424 The posting

---

SEC\_EMAIL\_ADDRESS.csv

EMAIL\_ADDRESS,ENCRYPT\_PWD,FIRSTNAME

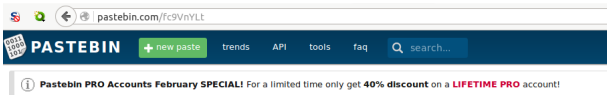
kente@prairiexxxxxxxx.us,74364AD466A3A97E4D1F7E90490FAE13,Kent  
diann@westxxxxxxxx.com,354FA3FB52AAEDAE860431979286EDF0,Diann  
klpetxxx@mixxxxxxxxx.edu,67357C6CDE1E652C250A75D3764208D8,Kevin  
jjamxx@dxxxxx.com,B8AAFA55304D218D9EB11FEE6ADED315,Jim  
xxxxhambrick@exxxxx.com,788F54A6D2CA11FA21A3DEE3F85D3BC9,Jim  
xxnope@chxxxx.net,558EFB24130D85DA042B45CFD2EA94A8,Judith  
margexxxxxxk@ttx.com,AFBF5EEDB77DE36B8B559F5F896CDEB6,Marge  
ganderxxx@dataxxxx.com,9D9D1E968BC9BA76E5F8D8E8AE4B9CCA,Gisela  
bexx@primaryxxxxxxxx.com,22FF6D707D7319F1A0AF8543503D5BC5,Albert  
moniquexxxxxx@ixxx.com,48ABE46CC4C64E840061EC8F65C0AFDD,Monique  
deedeexxxxxxx@cxccccccccsparks.com,D2AEB85EA85A812D06B849F787074587,Dee dee  
xxxlmer@deyxxxxxx.com,3C7AB6E445E176DD48D4B954FAB1FB31,Johanna  
xxxxxxxxxxxxwilson@hotmail.com,359FCF260D068B42AE7CED3B8C91FD7C,Heather  
mhamxxxx@xxxxview.org,A1926ADE8BAE523F9A0990613992065E,Mark  
rebecca.xxxxxxxxx@xx.org,6E1DCB3D49E345DAF44A418E7515480B,Rebecca  
marshallxxxxxx@vxxx.com,E6CE602050FEF4B62AEBD637CE356B47,Marshall  
awaxxxx@hotmail.com,6590B4DC32FE183748680EC7E75D5FE3,Andrew

...//

# CIRCL #215424 Analysis Stage 1


---

- Review the posting to gather additional information
- Unfortunately already suspended



# CIRCL #215424 Analysis Stage 1

- Ask Google
- Leads to 1 hit at kickasspastes.com

**gov leak #2 Part 5**  
By Guest on 14th February 2016 10:34:30 AM | Syntax: TEXT

[New paste](#) | [Download](#) | [Copy text to clipboard](#)

```
tomoko [REDACTED].com_F78C6799F3CBA2B21E12646E25068FD, Tomoko
061ic [REDACTED].com_80156302440A851A71699F6340E8E20, Ertweto
katy_w [REDACTED].com_5760AE1901A589F846E6447C2F430D9, Katy
mary_7 [REDACTED].com_2E960A58E0D77383767396C2158AF5E, Mary
dchr [REDACTED].com_117C3A8F54E1A23E38725377AAA1A0A2F7846949C05F28, Denise
20227 [REDACTED].com_808E2146EB812087A8F7168A16886186, Contact
20243 [REDACTED].com_808E2146EB812087A8F7168A16886186, Contact
20244 [REDACTED].com_808E2146EB812087A8F7168A16886186, Contact
20251 [REDACTED].com_808E2146EB812087A8F7168A16886186, Contact
20258 [REDACTED].com_808E2146EB812087A8F7168A16886186, Contact
20260 [REDACTED].com_808E2146EB812087A8F7168A16886186, Contact
20263 [REDACTED].com_808E2146EB812087A8F7168A16886186, Contact
lisa_1 [REDACTED].com_EC838194841346C812F6212CF21D6E, June
joyce [REDACTED].com_866889968E87878830C30480C80F2E2, Joyce
j1165 [REDACTED].com_826658265895429864D725C808A0903, Jia
nio8p [REDACTED].com_0668CEC2288894048D65E26E33464D, Nicolas
greg_w [REDACTED].com_058E368448261011F03E1780A0C04, Greg
crystal [REDACTED].com_2809C887D068D30F, Crystal
jmar1 [REDACTED].com_8096529AA7E6727513E0590D916C818A978120C24495A2, Jovita
salene [REDACTED].com_1100C3BC29C4027FE2351EE66192, Patricia
cancr [REDACTED].com_1041808E4FACAA064605733C0955803, Sue
acctg [REDACTED].com_746133420891745367CE23899527FD, Mary kay
4349 [REDACTED].com_808E2146EB812087A8F7168A16886186, Contact
43574 [REDACTED].com_808E2146EB812087A8F7168A16886186, Contact
[REDACTED]
```

# CIRCL #215424 Search for "\*\*\*\*\*s.gov leak"

https://www.google.lu/#q=\*\*\*\*\*s.gov+leak+Part

gle "\*\*\*\*\*s.gov leak" Part

Alle Bilder News Videos Maps Mehr Suchoptionen

Ungefähr 29 Ergebnisse (0,37 Sekunden)

- [gov leak #1 Part 6 | KickAssPastes - Fast and Free ...](#)  
sites.com/11836/ • Diese Seite übersetzen  
SA&\_LISA-S1721A.M.SERVICES.ANNUAL.SURVEYS.EPWireless  
Fications.Carriers.(except.Satellite).JANUARY.30.DAYS.A.P...
- [gov leak #1 Part 2 | KickAssPastes - Fast and Free ...](#)  
sites.com/11832/ • Diese Seite übersetzen  
- 20121112111742.1229.260735.1229.2018028554.NULL.MAIN.TW.074.  
Thank you Erick for your reply. I have form TW-48490.
- [gov leak #2 Part 7 | KickAssPastes - Fast and Free ...](#)  
sites.com/11843/ • Diese Seite übersetzen  
Board. (M+C on Mac) No line numbers will be copied. Guest. Census.gov  
#17. By Guest on 14th February 2016 10:37:39 AM | Syntax: TEXT
- [gov leak #2 Part 2 | KickAssPastes - Fast and Free ...](#)  
sites.com/11838/ • Diese Seite übersetzen  
Board. (M+C on Mac) No line numbers will be copied. Guest. Census.gov  
#12. By Guest on 14th February 2016 10:31:20 AM | Syntax: TEXT
- [gov leak #1 Part 3 | KickAssPastes - Fast and Free ...](#)  
sites.com/11833/ • Diese Seite übersetzen  
#1  
#AF03.78.2611434.611.2005414054.NULL.MAIN.MC.074.2012UL."The only  
pictured by us last year was one 169alboat ...
- [gov leak #1 Part 5 | KickAssPastes - Fast and Free ...](#)  
sites.com/11835/ • Diese Seite übersetzen  
#1 - 20130328161202.1508.2615226.NULL.2018767811.NULL.MAIN.LU.074.  
#1 Fei.Vin/vi've entered all the date for the Census but ...
- [gov leak #1 Part 4 | KickAssPastes - Fast and Free ...](#)  
sites.com/11834/ • Diese Seite übersetzen  
#1 - C [2007887775]ed authorize the U.S. Census Bureau to release data  
submitted for the company identified above and for the survey ...
- [gov leak #2 Part 4 | KickAssPastes - Fast and Free ...](#)  
sites.com/11840/ • Diese Seite übersetzen  
Board. (M+C on Mac) No line numbers will be copied. Guest. Census.gov  
#14. By Guest on 14th February 2016 10:33:35 AM | Syntax: TEXT
- [gov leak #1 | KickAssPastes - Fast and Free ...](#)  
sites.com/11831/ • Diese Seite übersetzen  
gov leak #1. By Guest on 14th February 2016 10:24:40 AM | Syntax: TEXT

## CIRCL #215424 Analyze the set

---

```
wc -l fc9VnYlt.txt
```

- 7103

```
grep -i "\.mil\," fc9VnYlt.txt
```

- 1

```
grep -i "\.gov\," fc9VnYlt.txt
```

- 175

```
grep -i "\.gov\," fc9VnYlt.txt |cut -f1 -d"," |cut -f2  
-d"@"|sort |uniq -c |sort -n
```

- 1 \*\*\*\*\*hs.gov

- 1 \*\*\*\*\*a.gov

- 3 \*\*\*.gov

- 170 \*\*\*\*\*s.gov



## CIRCL #219989 Posting already suspended

---

```
wc -l BvMacKhC.txt
```

```
->5728
```

```
grep -i "\.mil\:" BvMacKhC.txt
```

```
->34
```

```
grep -i "\.gov\:" BvMacKhC.txt
```

```
->43
```

Google search for one of the leaked MD5 value

->Leads to 1 hit in Google Cache

# CIRCL #219989 From Google cache

altre[REDACTED].com db leak by troy hunt p1

A GUEST MAR 1ST, 2016 56 NEVER

text 395.81 KB raw download

```
1. 8128[REDACTED]ent.inholland.nl:01972C35C719574C05EB86F328D0E4
2. 8295[REDACTED]yu.edu.hk:07278F3D4AF6C35F98EBC08EE7AAB
3. 83394[REDACTED]an.qc.ca:0472C93F8E11A022EF4057D61281B1
4. 12341[REDACTED]com:0070AC05698118F039751D42FFE358
5. 12345[REDACTED]me:025547CE50D71A65917A09389EA9E6
6. 12877[REDACTED]net.puk.ac.za:12971472AC1834FC97D250EA482767
7. 1201[REDACTED]5641ACCF4C29F71D810CC0F28
8. 1312[REDACTED]a.sun.ac.za:14257088F548A377912393A68945AD
9. 1858[REDACTED].com:081898DFAC2E5035A85F1431D883A
10. 1@et[REDACTED]98251A65F876F72ED9A40F4E187
11. 1vki[REDACTED]tbi.com:085711016E374D0C81849185602653
12. 1zah[REDACTED]er.ru:09368562D088C3C5211F100207893
13. 22@[REDACTED]org:15DE7858823E642AFD385660E7301
14. 2430[REDACTED]entall.com:019E5F0F2D001E8B72111ED2242923
15. 24cj[REDACTED]ay.rr.com:01E6C14E7746466743CE3A88CF8AB8
16. 2793[REDACTED]isel.ipl.pt:025928616EB9C17FA8B92898419CB6
17. 2off[REDACTED].com:12ADC07324201CDC29C545A12520AB
18. 3298[REDACTED].com:017AF9000253496888181E4F9C0208
19. 3deve[REDACTED]tron.ca:04A5F83E398FAD7AA28A31483ED44
20. 3dpar[REDACTED]hy.qc.ca:12ABA9E38BD07D0F895EAFFEC9BF8
21. 3dte[REDACTED]t.net:05EDAF1240FF532E4DEF1DA82DF47
22. 3roff[REDACTED]cway.com:078052F4617F0E4508CF9145DCFC0D
23. 3r03[REDACTED]s1:17714071869980892470EFA8287F1B
24. 444[REDACTED]711878545AC38ECA0707CEA0427AD
25. 49for[REDACTED].l.com:0062FBEDA4408E6890FDFD81DC1758
26. 4RUT[REDACTED]:02185CD7DAEF2E58964994E90D8940
```

## CIRCL #219989 Validate the finding

---

```
grep -i altrx BvMacKhC.txt
```

```
angela.xxxxxxx@altrxxxxxxx.com:10D56F79CD9DA6496A8627455006FF  
chris.xxxx@altrxxxxxxx.com:01E16299BC2ADD4679111FCF0E13A8  
dan.xxxxxx@altrxxxxxxx.com:19104E6A08A4DD4C579CFCD8AB7249  
dimitrios.xxxxxxxx@altrxxxxxxx:00A4AB56F3F68987E34360DE4B8498
```

```
whois altryyyyyyyyyyyy.com
```

```
Registrant Organization: Altrx Indxxxxxxx xxxxxx
```

```
...
```

```
whois altrxxxxxxx.com
```

```
Admin Organization: Altrx Indxxxxxxx xxxxxx
```

```
...
```

## CIRCL #215558 [pastebin.com/hbjc03Yw](https://pastebin.com/hbjc03Yw)

---

- Grep for ".mil\:"
  - ryan.xxxxxx@xxxxxxxxxx.af.mil:chronic
  - Patrick.xxxxxx@xxxxxxxxxxxx.af.mil:patrick
  - 48fwxxx@xxxxxxxxxxxx.af.mil:chapel
  - phillip.xxxxx@xxxxxxxxxx.af.mil:allen
- Grep for ".gov\:"
  - kerrixxx@xxxx.xxi.gov:kerri
- Grep for ".gov"
  1. Leads to 98 hits mainly gov.uk
  2. 1x .gov.ie
  3. 1x .gov.za

# CIRCL #215558 Password Frequency Analysis

---

...

...

20 password

22 arsenal

22 daniel

24 george

26 joshua

29 charlie

30 matthew

38 123456

43 111

43 liverpool

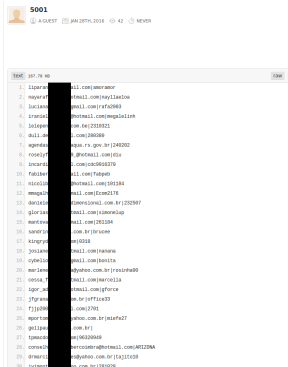
121 snooker

## CIRCL #215558 Analysis Stage 2

---

- What do we know
  - Related: co.uk
  - Related: Snooker
- How to find targeted site?
  - Google search for: "site:co.uk snooker login"
  - >Unfortunately no helpful results
- What can we do
  1. Go back to the data set
  2. Grep for "snooker"
  - >BINGO

# CIRCL #210401 The posting



# CIRCL #210401 Analysis Stage 1

---

- What do we got
  - Date
  - Email addresses | passwords
  - -> Leaked 3rd party credentials
  - Obviously many .BR accounts
- What do we miss
  - Usefull information in the header
  - Target details in the posting
- What can we do
  1. Search for interesting accounts
  2. Identify targeted site
  3. Notify our partners in BR



## CIRCL #210401 Analysis Stage 2

---

### Search for interesting accounts

graziani.xxxx@xxx.mar.mil.br—Aprovada

agendaxxxxx@xxxxxxx.rs.gov.br—240202

CLAUDIAxxxxxxx@xxxxx.GOV.BR—9395

hellenxxxxxxx@xxxxxxx.se.gov.br—33917841

Ocea@xxxxxxxxx.gov.br—180283

escolaxxxxx@xxxxxxx.mg.gov.br—171151

nelxxx@xxxxxx.gov.br—np201356

maicxxx@xxx.rs.gov.br—061188

...

...

26 gov.br users

## CIRCL #210401 Analysis Stage 3

---

Find target: By analyzing the leaked Passwords?

```
cut -f2 -d"|" qzQF6ib5.txt |sort |uniq -c |sort -n
 4 010203
 4 12345678
 4 hospital
 5 123456789
 6 12345
 6 gabriel
 7 medicina
 8 123
 8 compras
 8 telediu
13 1234
79 123456
```

## CIRCL #210401 Analysis Stage 3

---

Find target: By analyzing the leaked Passwords?

```
cut grep -i teledi qzQF6ib5.txt
```

```
...
```

```
8x telediu
```

```
...
```

```
vanessxxxxxxxx@gmail.com—Telediu84
```

```
cluciaxxxxxxxx@hotmail.com—teledil
```

```
tarsisxxxxxxxx@hotmail.com—telediu71
```

```
amarilxxxxxxxx@gmail.com—rodtelediu
```

```
heldexxxxxxxxx@yahoo.com.br—telediu11
```

```
andrexxxxxxxx@yahoo.com.br—telediu150
```

```
dentxxxxxxxx@telexxxxxxxxxx—233748p
```

```
thainapegxxxxxxxx@telexxxxxx—74697649
```

# AIL

---

- Monitoring Module: Input feeds
- Analysis Module: Deduplication, Indexing, Classification
- Output Module: ZMQ, Redis

# AIL

## Analysis Information Leak framework -- Dashboard

Search Paste

Dashboard

WordsTrendsings

Queue Name	Amount
------------	--------

filestduplicate	6
-----------------	---

creditcard_catecards	0
----------------------	---

mails_catemails	0
-----------------	---

102feed	0
---------	---

wordscateg	65
------------	----

filestline	6
------------	---

wordscurve	0
------------	---

onion_categor	0
---------------	---

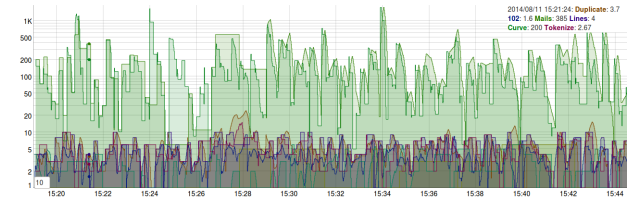
web_categoris	0
---------------	---

filestindexer	0
---------------	---

Shortlinestokenize	0
--------------------	---

filestattributes	6
------------------	---

### Queues Monitor



### Logs

to  INFO WARNING CRITICAL

Channel	Level	Script Name	Source	Date	Paste name	Message
Script	INFO	Categ	pastebin.com	20140811	T5qu3ub1.gz	Detected 1 http
Script	INFO	Categ	pastebin.com	20140811	qmjgEHWm.gz	Detected 9 http
Script	INFO	LH1	pastebin.com	20140811	T5qu3ub1.gz	3 Valid url detected
Script	INFO	Categ	pastebin.com	20140811	vULV0yM.gz	Detected 2 https
Script	INFO	Categ	pastebin.com	20140811	vULV0yM.gz	Detected 1 http
Script	INFO	Categ	pastebin.com	20140811	BqEgyXvH.gz	Detected 1 http
Script	INFO	Categ	pastebin.com	20140811	BqEgyXvH.gz	Detected 1 password
Script	INFO	LH1	pastebin.com	20140811	qmjgEHWm.gz	9 Valid url detected
Script	INFO	LH1	pastebin.com	20140811	vULV0yM.gz	3 Valid url detected
Script	INFO	LH1	pastebin.com	20140811	BqEgyXvH.gz	1 Valid url detected

# Conclusion

---

- There are no small incidents
- Want access to services: [info@circl.lu](mailto:info@circl.lu)
- ->search for past issues?