Securitatea cibernetică și impactul acesteia asupra SCADA / SMART GRIDS

Dan Tofan

Director Tehnic CERT-RO

CERT-RO?

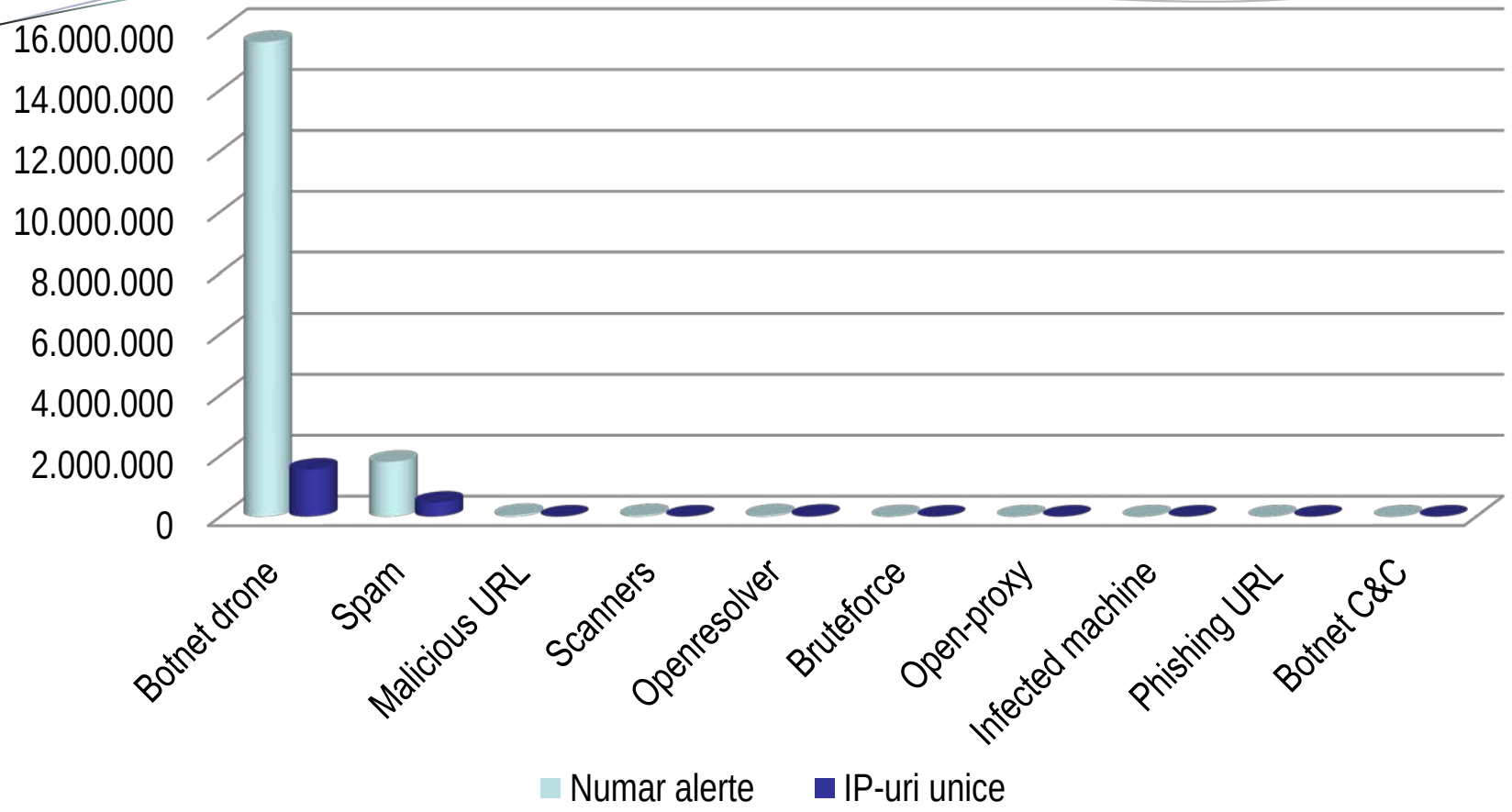
- *Centrul **Național** de **Răspuns** la Incidente de Securitate **Cibernetică** – CERT-RO* este punct național de contact cu privire la incidente de securitate cibernetică.
- CERT-RO se află în coordonarea Ministerului pentru Societatea Informațională și este finanțat integral de la bugetul de stat.

Raport analiză primele 6 luni

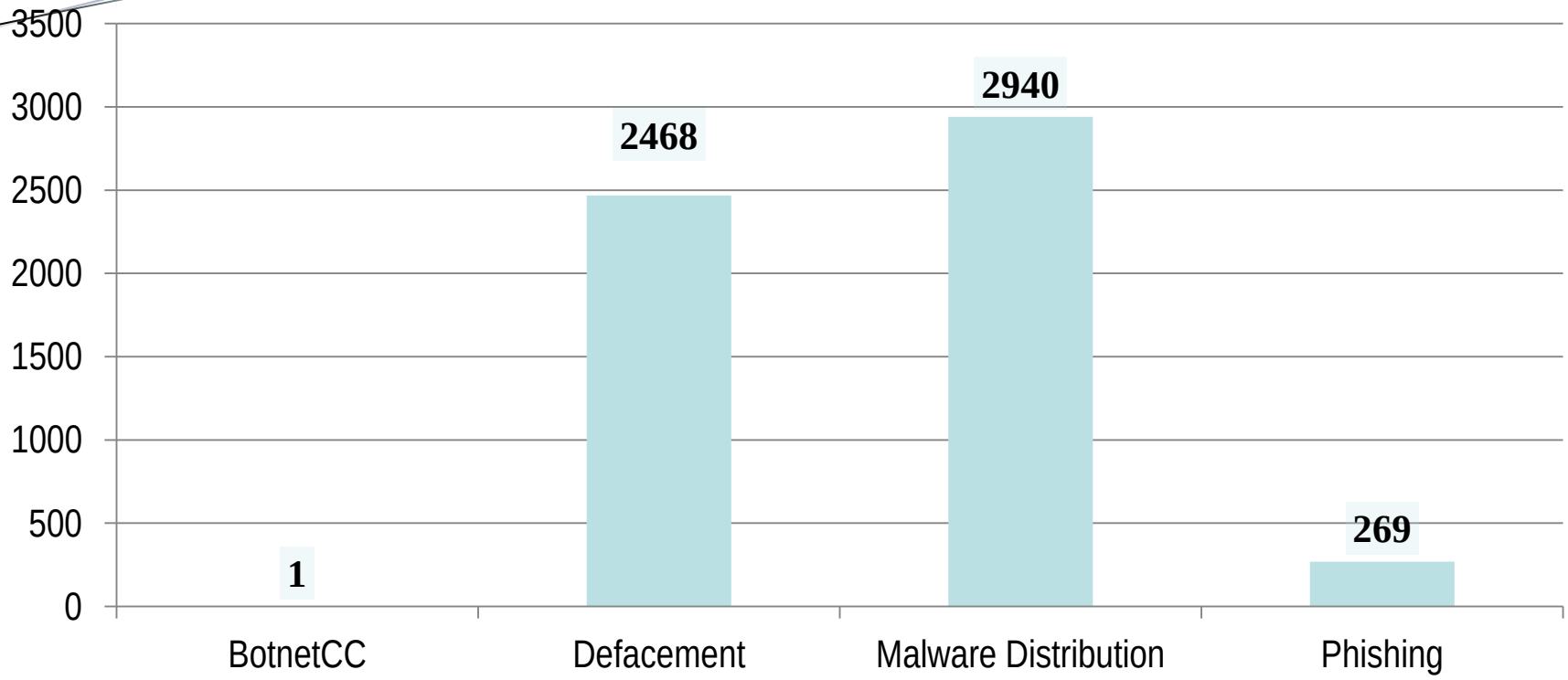
- Scopul raportului este de a prezenta o analiză a incidentelor de securitate cibernetică raportate la CERT-RO în perioada 01.01 – 30.06.2013 şi obţinerea unei *viziuni de ansamblu asupra naturii **şi** dinamicii acestor tipuri de evenimente/incidente*, relevante pentru evaluarea riscurilor de securitate cibernetică la adresa infrastructurilor IT şi de comunicaţii electronice de pe teritoriul naţional al României, aflate în aria de competență a CERT-RO.

- Raport disponibil la: http://www.cert-ro.eu

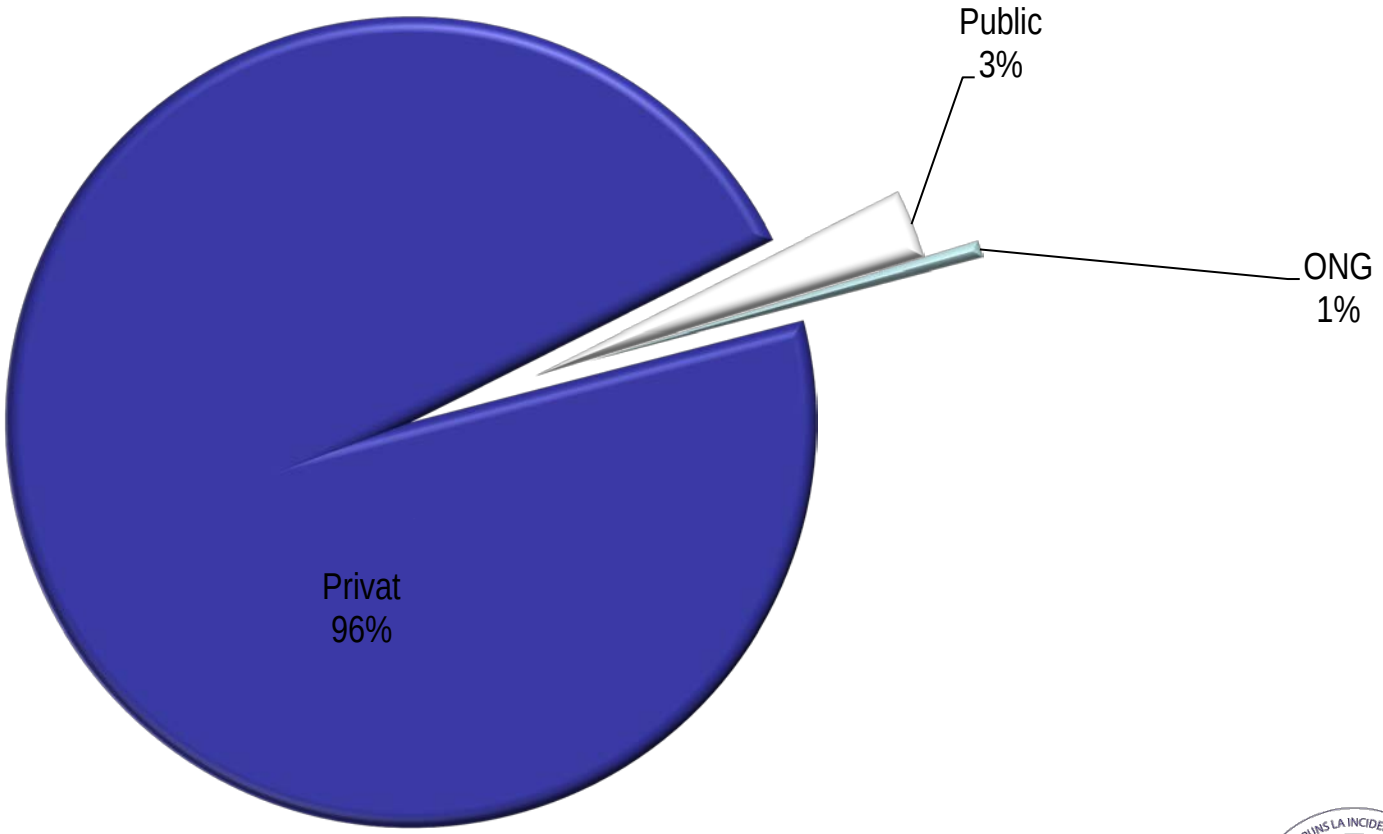
Raport analiză primele 6 luni



Domenii ”.ro” compromise primele 6 luni



Domenii ”.ro” compromise primele 6 luni



Raport analiză primele 6 luni

- Botnet drone - Rețea de sisteme informatice compromise, controlate, de la distanță, de alte persoane/organizații decât deținătorii acestora.

- Microsoft Safety & Security Center: ”Atacatorii folosesc rețelele de tip botnet pentru a trimite spam, a răspândi viruși informatici, pentru a ataca alte computere și servere sau pentru a comite alte tipuri de fraude sau infracțiuni. Dacă computerul tău devine parte dintr-un botnet ai putea în mod involuntar să-i devii complice atacatorului.

http://www.microsoft.com/security/resources/botnet-whatis.aspx

Concluzie raport

- ameninţările, de natură informatică, asupra spațiului cibernetic național s-au diversificat, fiind relevate tendinţe evolutive, atât din perspectivă cantitativă, cât şi din punct de vedere al complexităţii tehnice;
- peste 12,5% din plaja de IP-uri alocată României este infectată cu diverse variante de malware (botnet), ce ulterior sunt folosite în diverse atacuri asupra unor ținte din afara țării, identitatea reală a atacatorului rămânând ascunsă.
- Peste 80% din numărul total al IP-urilor unice raportate, rulează sisteme de operare din familia XP/2000.
- RO nu mai poate fi considerată generatoare de incidente de securitate cibernetică, raportul demonstrând caracterul intermediar/de tranzit

ICS – SCADA – SMART GRID

- Industrial Control Systems - sisteme informatice de comandă și control folosite în cadrul proceselor industriale.

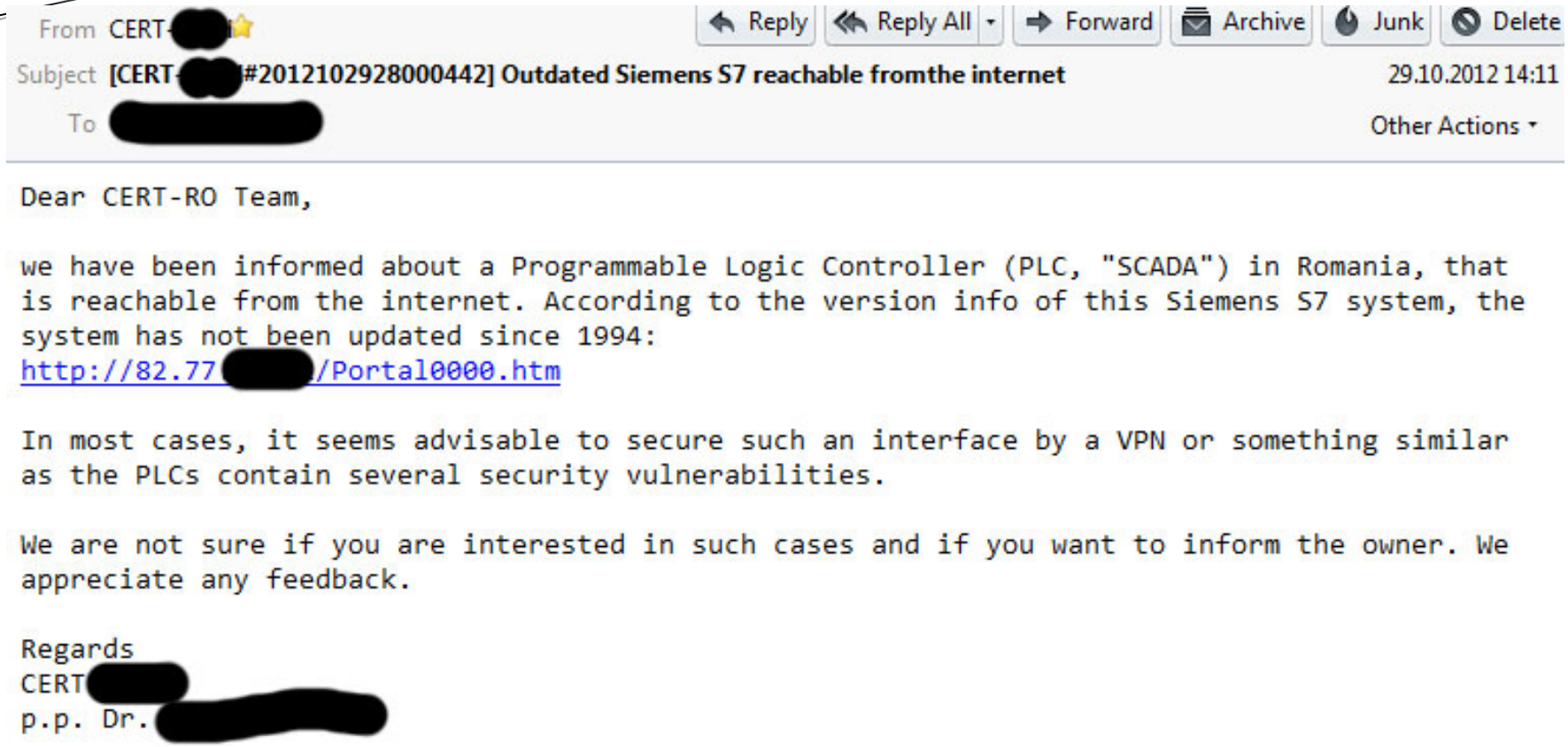
- SCADA (Supervisory Control and Data Acquisition) – cel mai mare subgrup al ICS.

- Smart Grids – rețea electrică modernă ce dispune de capacitate de comunicare bidirecțională între client și furnizor, precum și sisteme complexe de măsurare și monitorizare.

Alerte SCADA in RO

- 6 alerte de securitate ce au implicat SI SCADA din RO în perioada iunie – decembrie 2012.
- IP-uri din RO ce rulau sisteme vulnerabile, care puteau fi oricând compromise de către atacatori.

Alerte SCADA in RO



From CERT-[redacted]

Reply | Reply All | Forward | Archive | Junk | Delete

Subject [CERT-[redacted]#2012102928000442] Outdated Siemens S7 reachable fromthe internet 29.10.2012 14:11

To [redacted] Other Actions

Dear CERT-RO Team,

we have been informed about a Programmable Logic Controller (PLC, "SCADA") in Romania, that is reachable from the internet. According to the version info of this Siemens S7 system, the system has not been updated since 1994:
http://82.77[redacted]/Portal0000.htm

In most cases, it seems advisable to secure such an interface by a VPN or something similar as the PLCs contain several security vulnerabilities.

We are not sure if you are interested in such cases and if you want to inform the owner. We appreciate any feedback.

Regards
CERT[redacted]
p.p. Dr.[redacted]

Alerte SCADA in RO

Fri Jun 22 18:01:28 2012 [redacted] CERT Incidencias - Ticket created

Reply Comment Forward

CC: abuse@cert-ro.eu [lookup email] [lookup "cert-ro.eu"]

Subject: [redacted] #276494] [Scada] INCIDENT REPORT

Date: Fri, 22 Jun 2012 17:01:12 +0200

To: [redacted] [lookup email] [lookup "[redacted]ro"]

From: "[redacted] [ssalan]" <incidencias@[redacted]> [lookup email] [lookup [redacted]"]

****

The [redacted] (Computer Emergency Response Team for SMEs and Citizens), supports the development of national business network and offers the current services of an Incident Response Centre and free, providing reactive solutions to computer incidents, prevention services against possible threats and services of information awareness and training in computer security matters to SMEs and [redacted] citizens.

****

Download (untitled) / with headers
text/plain 2.4k

Dear Sir / a,

We get in touch with you from [redacted], incident response center within the Ministry of Industry, Energy and Tourism, on behalf of the National Critical Infrastructure Protection, Ministry of Interior, CNPIC. We learned that the following IP addresses belong to their network, and allegedly belonging to SCADA systems according to the published text have been made public through the Pastebin service.

The URL where such information is made public as follows: http://pastebin.com/egdxLgvm. [lookup "pastebin.com"] It is possible that when you query the URL, you will not work, because we are working with Pastebin in removing this content from their servers. For this reason, we attach the file further. Txt file that contains data on IP addresses for their network ranges.

Since, for safety reasons, it is possible that these addresses should not be known, I seek your assistance to inform those responsible for services associated with this IP to be aware of the situation.

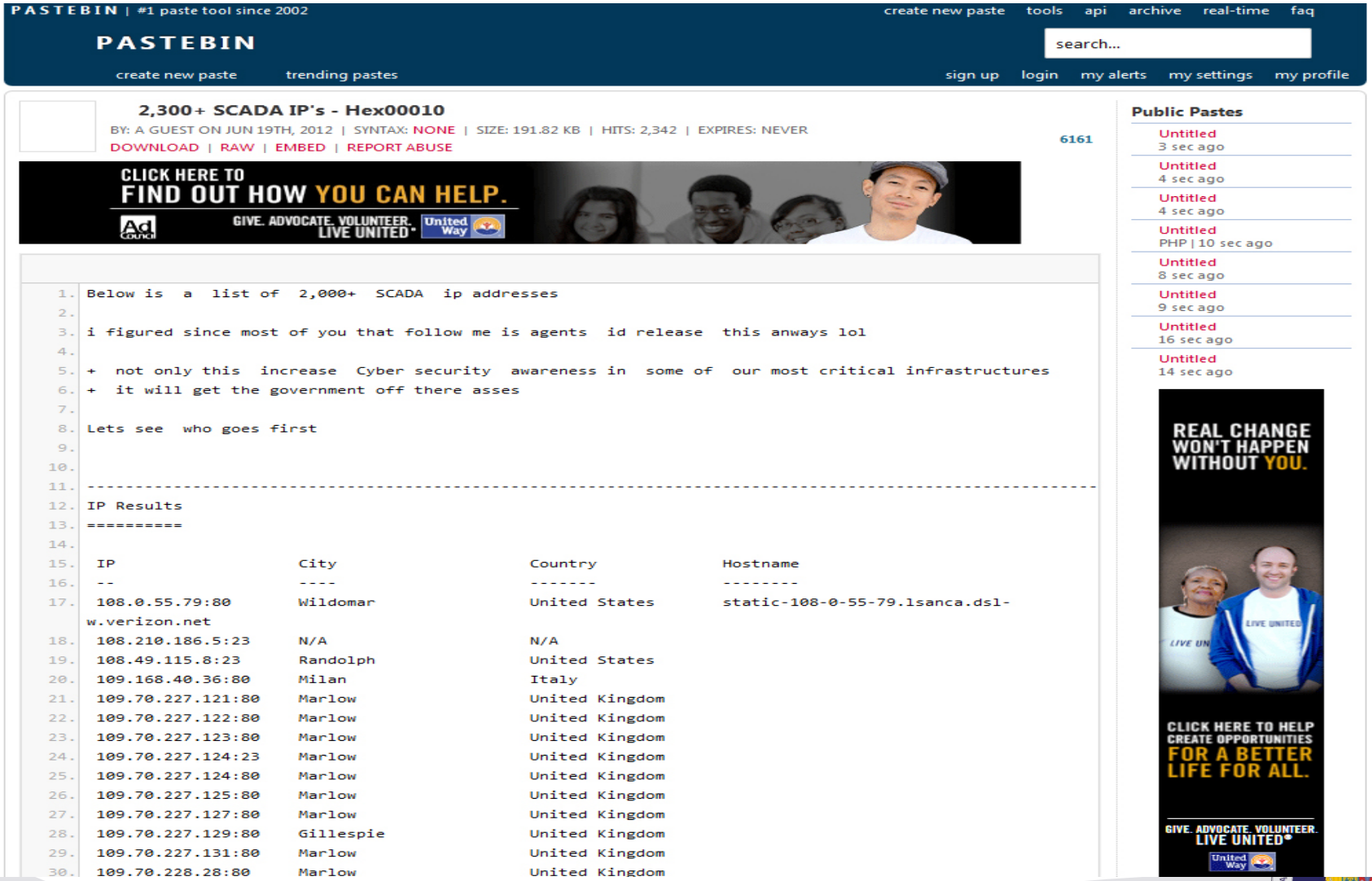
If you need any additional information or assistance please contact us.

For any matter related to this issue include the following reference [$ {} # {$ rtname Ticket-> id}] in the subject line.

Thank you very much.

Regards,

Alerte SCADA in RO



PASTEBIN | #1 paste tool since 2002

create new paste tools api archive real-time faq

PASTEBIN

search...

create new paste trending pastes sign up login my alerts my settings my profile

2,300+ SCADA IP's - Hex00010

BY: A GUEST ON JUN 19TH, 2012 | SYNTAX: NONE | SIZE: 191.82 KB | HITS: 2,342 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE

6161


```
1.  Below is  a  list of  2,000+  SCADA  ip addresses
2.
3.  i figured since most of you that follow me is agents  id release  this anways lol
4.
5.  +  not only this  increase  Cyber security  awareness in  some of  our most critical infrastructures
6.  +  it will get the government off there asses
7.
8.  Lets see  who goes first
9.
10.
11. ----------------------------------------------------------------------------------------------------------------
12. IP Results
13. ==========
14.
15.  IP                  City                Country             Hostname
16.  --                  ----                -------             --------
17.  108.0.55.79:80      Wildomar            United States       static-108-0-55-79.lsanca.dsl-
    w.verizon.net
18.  108.210.186.5:23    N/A                 N/A
19.  108.49.115.8:23     Randolph            United States
20.  109.168.40.36:80    Milan               Italy
21.  109.70.227.121:80   Marlow              United Kingdom
22.  109.70.227.122:80   Marlow              United Kingdom
23.  109.70.227.123:80   Marlow              United Kingdom
24.  109.70.227.124:23   Marlow              United Kingdom
25.  109.70.227.124:80   Marlow              United Kingdom
26.  109.70.227.125:80   Marlow              United Kingdom
27.  109.70.227.127:80   Marlow              United Kingdom
28.  109.70.227.129:80   Gillespie           United Kingdom
29.  109.70.227.131:80   Marlow              United Kingdom
30.  109.70.228.28:80    Marlow              United Kingdom
```

Public Pastes

- Untitled — 3 sec ago
- Untitled — 4 sec ago
- Untitled — 4 sec ago
- Untitled — PHP | 10 sec ago
- Untitled — 8 sec ago
- Untitled — 9 sec ago
- Untitled — 16 sec ago
- Untitled — 14 sec ago

STUXNET - 2010

- Identificat la centrala nucleară iraniană de la Natanz.
- Expoatează 4 vulnerabilități de tip zero-day
- Viermele folosea o serie de parole default ale unor aplicații Siemens (WinCC, PCS7) pentru a accesa sistemele de operare Windows.
- Au reușit modificarea vitezei de rotație a centrifugelor folosite la stabilirea concentrațiilor uraniului.

DUQU - 2011

- Folosește tehnici identice cu cele ale Stuxnet.
- Se pare că a fost creat doar pentru acțiuni de recunoaștere asupra sistemelor de control industriale.

FLAME – 2012

- Aparent dezvoltat de creatorii DUQU.
- Specializat pe furt de informații prin diferite metode din sisteme informatice.
- Descoperit în sisteme informatice ce rulau SCADA din Iran, Liban, Siria, Sudan etc.

Ghiduri ENISA

- Smart Grid Security Recommendations
- http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations

- Appropriate security measures for smart grids
- http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids

Smart Grid Security Recommendations

- 10 recomandări pentru entitățile, publice sau private, implicate în definirea și implementarea rețelelor electrice de tip smart grid:

1. *Improve the regulatory and policy framework*
2. *Foster the creation of a Public-Private Partnership (PPP) entity to coordinate smart grid cyber security initiatives*
3. *Foster awareness raising and training initiatives*
4. *Foster dissemination and knowledge sharing initiatives*
5. *Develop a minimum set of reference standards and guidelines*

Smart Grid Security Recommendations

5. Promote the development of security certification schemes for products and organisational security
6. Foster the creation of test beds and security assessments
7. Refine strategies to coordinate large scale pan-European cyber incidents affecting power grids
8. Involve CERTs to play and advisory role in dealing with cyber security issues affecting power grids
9. Foster research in smart grid cyber security leveraging existing research programmes.

Appropriate security measures for smart grids

O serie de recomandări de securitate pentru operatorii de smart grids:

1. Security governance & risk management;
2. Management of third parties;
3. Secure lifecycle process for smart grid components/systems and operating procedures;
4. Personnel security, awareness and training;
5. Incident response & information knowledge sharing;

Appropriate security measures for smart grids

O serie de recomandări de securitate pentru operatorii de smart grids:

6. Audit and accountability;
7. Continuity of operations;
8. Physical security;
9. Information systems security; and
10. Network security.

http://www.shodanhq.com/

Vă mulțumesc!

Întrebări?

http://www.cert-ro.eu/