Cyber Security and its impact on SCADA / SMART GRIDS

Dan Tofan

Technical Manager CERT-RO

CERT-RO?

- ***Computer Emergency Response Team – CERT-RO*** is a national contact point regarding cyber security incidents.

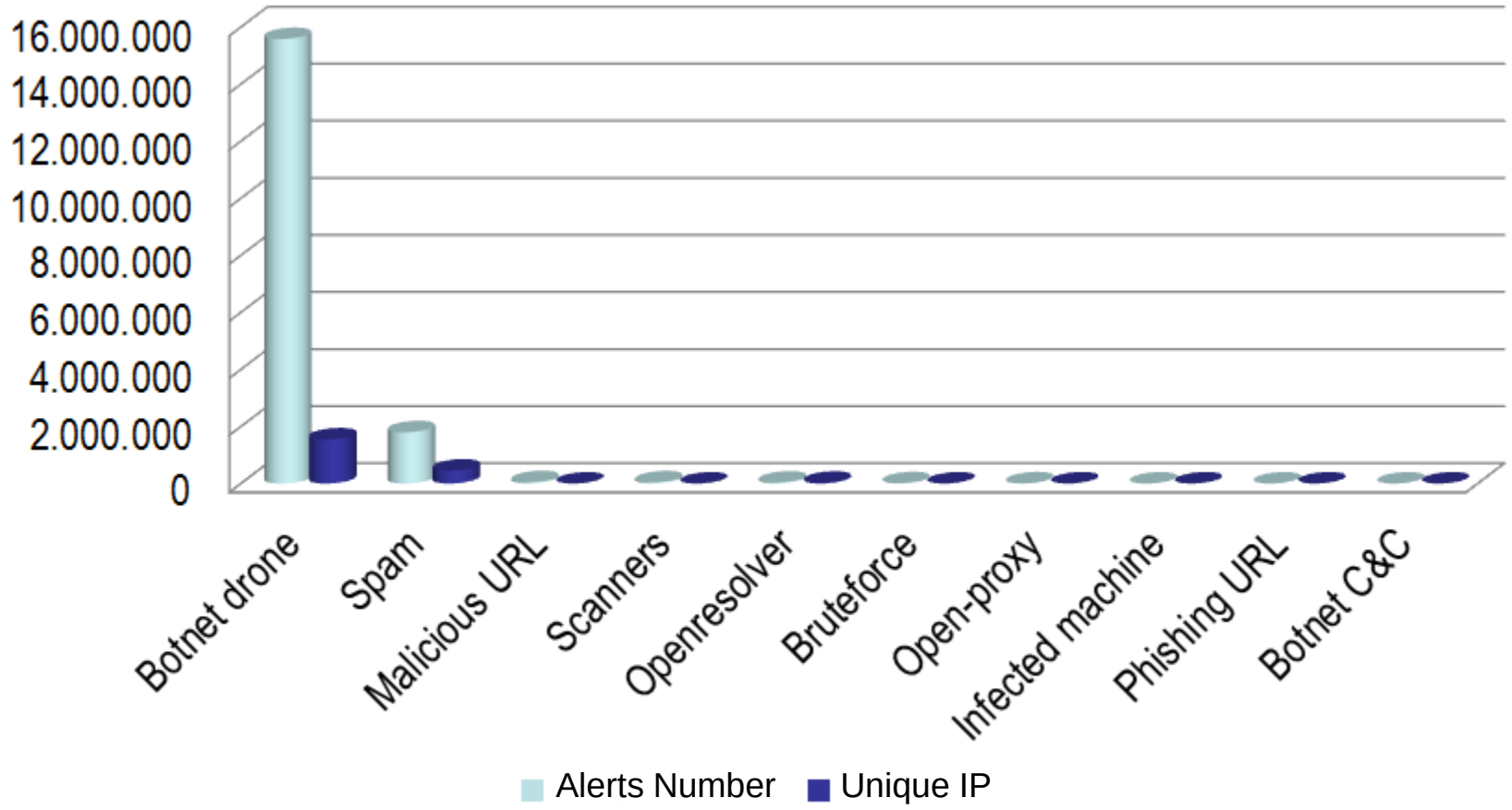
- CERT-RO is coordinated by the Ministry of Information Society and is financed only from the state budget.

Analysis report for the 1st quarter of 2013

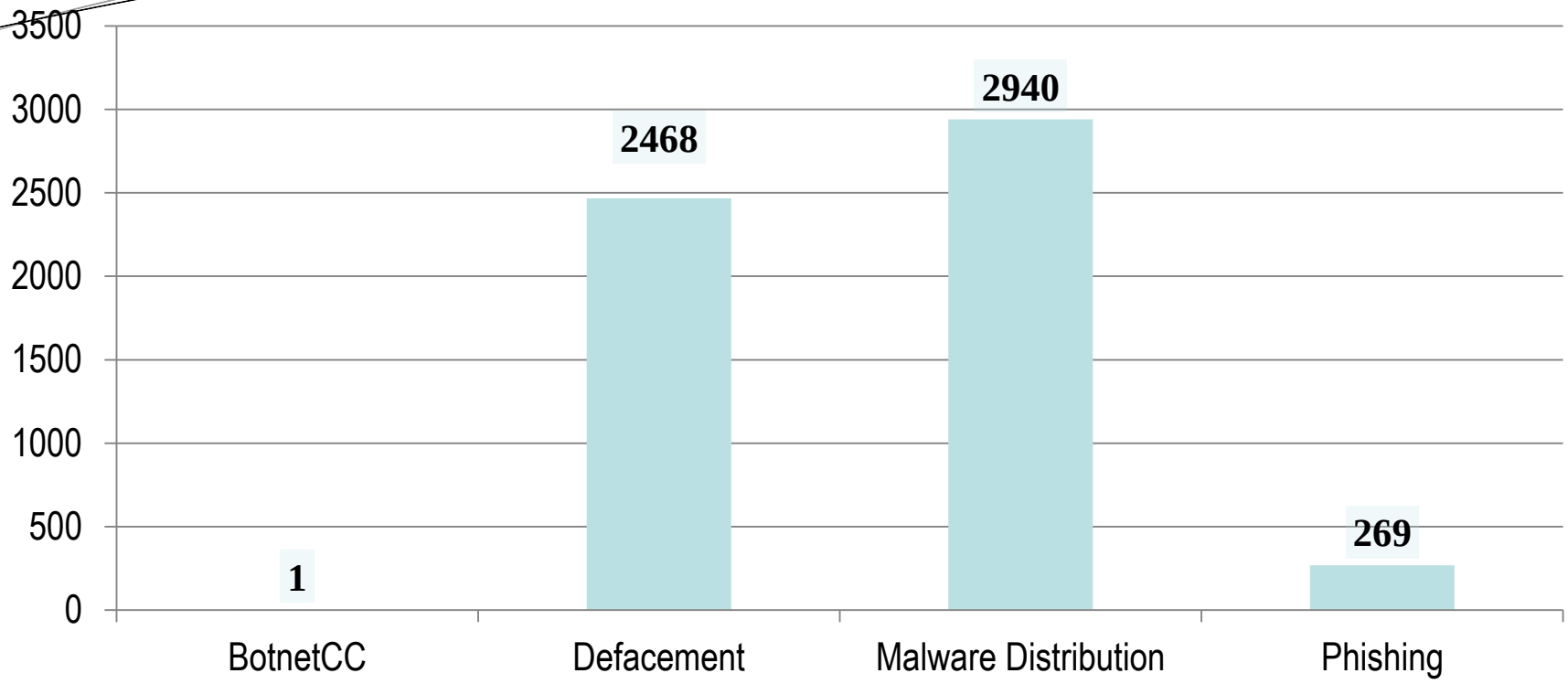
- The scope of this paper is to present a review of the cyber security incidents reported to CERT-RO during the period 01.01 – 30.06.2013 and achieving ***an overview of the nature and dynamics of this type of events/incidents*** which are relevant for cyber security risk assessment concerning the IT&C infrastructure located in Romania, that are under CERT-RO competence.

- The Full Report is available at: http://www.cert-ro.eu/articol.php?idarticol=755

First semester analysis report



First semester compromised ".ro" domains



First semester analysis report

- Botnet drone – Network of compromised computers, remotely controlled from other people/organizations than their owners.

- Microsoft Safety & Security Center: ” Botnets can be used to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If your computer becomes part of a botnet, it might slow down and you might be inadvertently helping criminals.”

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

Conclusions

- Cyber-security threats to our national cyberspace have diversified, evolutionary trends being revealed, both in terms of quantity and in terms of technical complexity;
- Over 12,5% of Romania allocated IP address range is infected with various types of malware (botnet), that are afterwards used in diverse attacks aimed at targets located outside Romania, the identity of the attacker remaining unrevealed.
- For more than 80% of the reported unique IP addresses the operating system is part of Windows XP/2000 family.
- RO can not be considered as an incident source anymore, the intermediate/transit character being substantiated by this report.

ICS – SCADA – SMART GRID

- Industrial Control Systems – command and control networks and systems designed to support industrial processes.

- SCADA (Supervisory Control and Data Acquisition) – the largest subgroup of ICS.

- Smart Grids – an upgraded electricity network depending on two-way digital communications between supplier and consumer that in turn give support to intelligent metering and monitoring systems.

SCADA alerts for RO

June – December 2012 – 6 security incidents that also involved Romanian SCADA infrastructure.

Romanian IP addresses belongs to vulnerable running operating systems that could have been compromised by attackers at any time.

SCADA alerts for 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]

SCADA alerts for 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,

SCADA alerts for 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


```
Below is  a  list of  2,000+  SCADA  ip addresses

i figured since most of you that follow me is agents  id release  this anways lol

+  not only this  increase  Cyber security  awareness in  some of  our most critical infrastructures
+  it will get the government off there asses

Lets see  who goes first


-------------------------------------------------------------------------------------------------------------------------------
IP Results
==========

 IP                  City                Country             Hostname
 --                  ----                -------             --------
 108.0.55.79:80      Wildomar            United States       static-108-0-55-79.lsanca.dsl-
w.verizon.net
 108.210.186.5:23    N/A                 N/A
 108.49.115.8:23     Randolph            United States
 109.168.40.36:80    Milan               Italy
 109.70.227.121:80   Marlow              United Kingdom
 109.70.227.122:80   Marlow              United Kingdom
 109.70.227.123:80   Marlow              United Kingdom
 109.70.227.124:23   Marlow              United Kingdom
 109.70.227.124:80   Marlow              United Kingdom
 109.70.227.125:80   Marlow              United Kingdom
 109.70.227.127:80   Marlow              United Kingdom
 109.70.227.129:80   Gillespie           United Kingdom
 109.70.227.131:80   Marlow              United Kingdom
 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

Questions??


CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ
CERT-RO