WWW.CERT.RO

CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA
ROMANIAN NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM

2017 Threat Landscape and Romanian cyberspace particularities

Catalin Patrascu
Coordinator of the Incident Handling Team @ CERT-RO
catalin.patrascu@cert.ro
+40-785.257.443

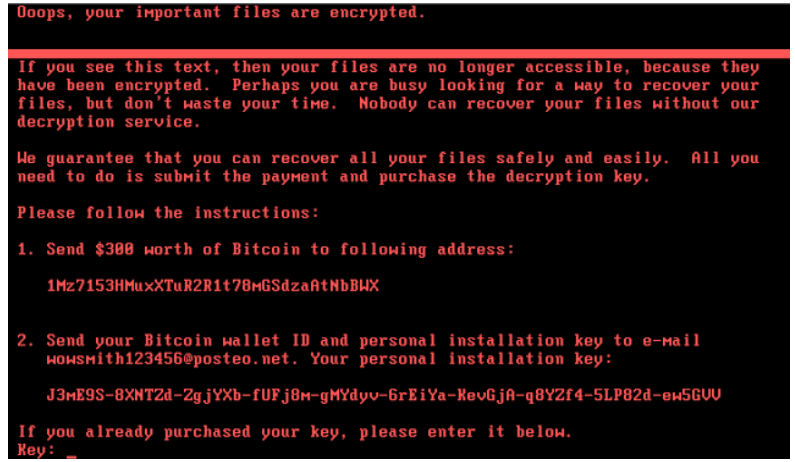
- **Point of contact (PoC)** – receive notifications and reports about cyber security incidents, vulnerabilities and threats
- **Incident response** – technical support for first response, technical analysis, mitigation, information sharing etc.
- **Cooperation** – at national, European and international level
- **Consultancy Services** – cyber security evaluation (and pentests)
- **Trainings** – last one for journalists
- **Awareness campaigns**
- **Coordinated Vulnerability Disclosure**

What was all about in 2017

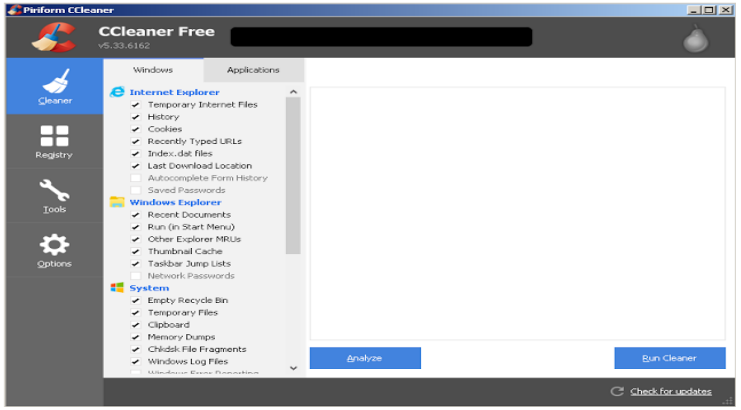
Code Name	Solution
"EternalBlue"	Addressed by MS17-010
"EmeraldThread"	Addressed by MS10-061
"EternalChampion"	Addressed by CVE-2017-0146 & CVE-2017-0147
"ErraticGopher"	Addressed prior to the release of Windows Vista
"EsikmoRoll"	Addressed by MS14-068
"EternalRomance"	Addressed by MS17-010
"EducatedScholar"	Addressed by MS09-050
"EternalSynergy"	Addressed by MS17-010
"EclipsedWing"	Addressed by MS08-067

The Shadow Brokers

WannaCry

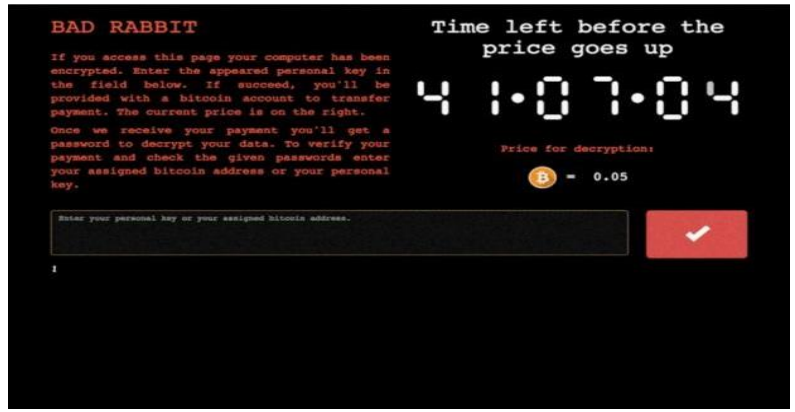


NotPetya



CCleaner

Free vouchers for everything



BadRabbit

Targetted attacks

From Capt.BORCHERT <alistair.BORCHERT@hq.nato.int> Tue Apr 25 03:02:43 2017
Date: Wed, 19 Apr 2017 03:57:36 -0400
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="14930821631.0dDdFe.27498"
Content-Transfer-Encoding: 8bit
Subject: =?utf-8?q?Trump=27s_Political_Report=0D=0A?=
From: Capt.BORCHERT <alistair.BORCHERT@hq.nato.int>
To: <[redacted]@mae.ro>
Message-Id: <20170419075736.D9D0A5FD72@politicspublicity.com>
Received: from SrvBucEDGE02.ma[redacted] by SRVBUCEX003.mae.ro (192.168.101.32) with Microsoft SMTP Server (TLS) id 14.3.319.2; Wed, 19 Apr 2017 10:59:30 +0300
Received: from [redacted] by mail.mae.ro [redacted] with Microsoft SMTP Server id 14.3.319.2; Wed, 19 Apr 2017 10:59:33 +0300
Received: from politicsadvertisment.com (HELO politicspublicity.com) ([89.249.67.22]) by [redacted]h ESMTP; 19 Apr 2017 10:59:28 +0300
Received: from [[redacted]]) by politicspublicity.com (Postfix) with ESMTPS id D9D0A5FD72 for <[redacted]@mae.ro>; Wed, 19 Apr 2017 03:57:36 -0400 (EDT)

Sir/Madam,
In the attachment you can find some information about foreign policy of
Donald J. Trump

"Alistair" BORCHERT
CAPTAIN, USA Navy
IMS Cooperative Security Division
Cooperation Policy and Programmes Branch
Policy and Programmes Section Head
T el: +32 2 707 5317
IVSN: 255 5317
Room: I 223

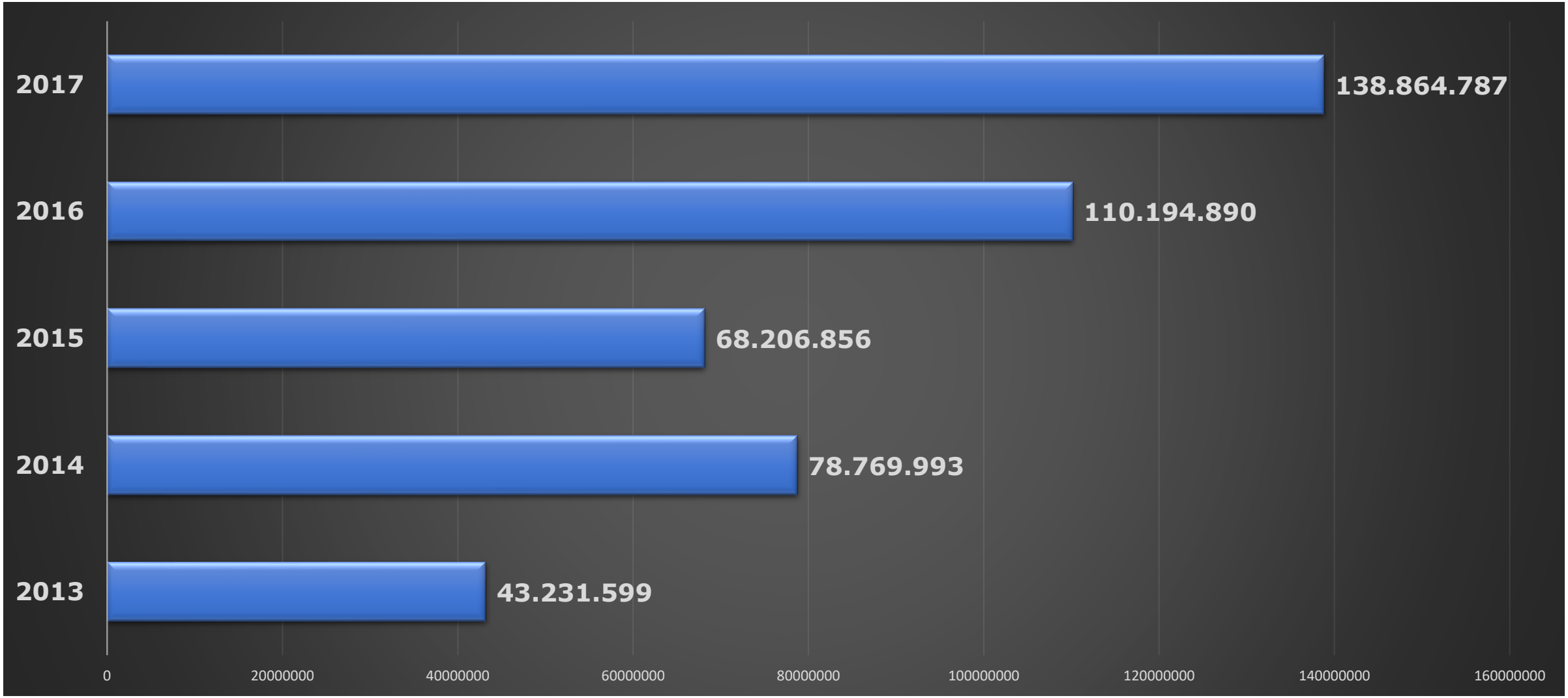
https://www.cyberscoop.com/dnc-hackers-impersonated-nato-attempt-hack-romanian-government/

WannaCry impact in RO

- **514 IP addresses** in RO were identified as making connections to the WannaCry kill switch domain
  - **10 IP addresses** of RO public institutions

- **5 incident notifications** about WannaCry were received by CERT-RO
  - 2 from public institutions
  - 2 from private sector
  - 1 from an individual

Last years evolution of the alerts



2017 Report Preview

- **34% of unique IPs** in RO were involved in at least one cyber security alert
- **83%** of processed alerts refers to **vulnerable systems**
- **10%** pf processed alerts refers to **compromised systems**
- **6%** of processed alerts refers to **botnet threat** (decreasing trend)
- **1,079 „.ro" domains** were reported to CERT-RO as being compromised

Affected systems

Nr. crt.	OS family	(%)
1	Linux	41,02%
2	Unix	30,13%
3	Network Devices Firmware/OS	20,65%
4	UPnP/1.0	7,76%
5	Windows	0,44%

What can we do?

- Sustained and coordinated effort by
  - Users
  - Technology vendors
  - Authorities
  - CERTs/CSIRTs
- Proper Risk Evaluation
- Cooperation and information sharing
- Cyber security legislation

THANK YOU FOR YOUR TIME!

@CERT.RO @CERT_RO /cert.ro @cert.ro