Peisajul amenințărilor și vulnerabilităților în spațiul cibernetic național

Cătălin Pătrașcu

Șef Serviciu Securitate Informatică și Monitorizare | CERT-RO

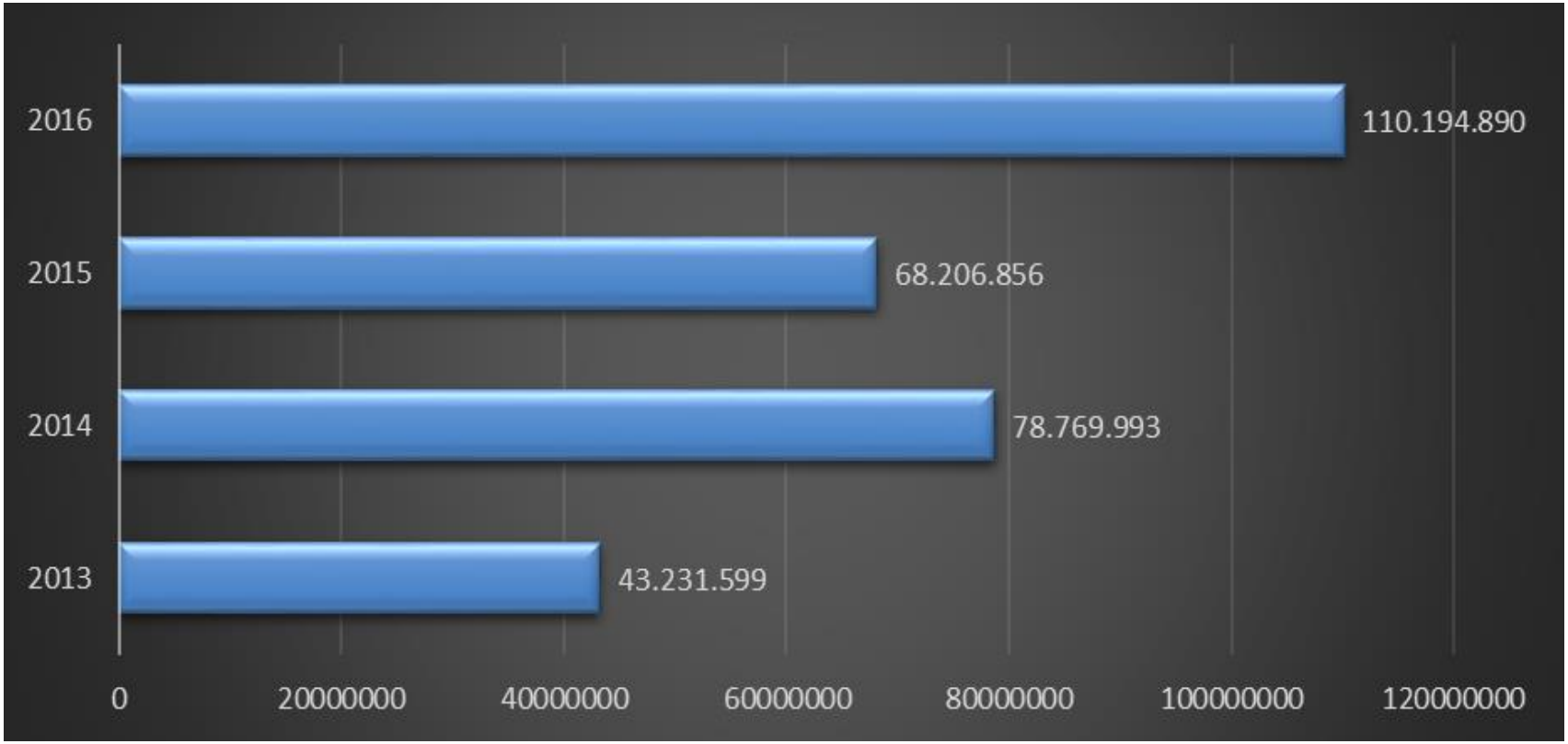
catalin.patrascu@cert.ro

Monday, 15 May 2017

Statistică privind alertele de securitate în 2016

- **110+ mil.** de alerte procesate
  - 1.363 procesate manual
  - Majoritatea sunt procesate automat
- **38% (2,9 mil.)** dintre adrese IP unice utilizate anul trecut în România au fost raportate în cel puțin o alertă de securitate cibernetică
- **81% (89 mil.)** dintre alertele procesate se referă la sisteme informatice/ servicii vulnerabile
- **13% (14 mil.)** dintre alertele procesate se referă la rețele botnet
- **10,639 de domenii „.ro”** au fost raportate ca fiind compromise în 2016

Evoluția numărului de alerte în ultimii 4 ani



Incidente în anul 2016

Nr. crt.	Tipul incidentului	Număr	Procent
1	Vulnerabilități	2,380,120	58.98%
2	Botnet	1,653,096	40.96%
3	Malware	2,071	0.05%
4	Altele	158	0.01 %

După de-duplicarea alertelor am obținut în jur de 4 mil. de incidente pe parcursul anului 2016

Incidente raportate la CERT-RO în anul 2016

Nr. crt.	Clasa incidentului	Tipul incidentului	Număr	Procent
1	Fraud	Phising	505	37,05 %
2	Malware	Malicious Url	363	26,63 %
3	Malware	Infected IP	256	18,78 %
4	Botnet	Botnet Drone	84	6,16 %
5	Botnet	Botnet CC	42	3,08 %
6	Cyber Attacks	Bruteforce	37	2,71 %
7	Information Gathering	Scanner	23	1,69 %
8	Vulnerabilities	Other	23	1,69 %
9	AbusiveContent	Spam	17	1,25 %
10	Compromised Resources	Infected IP	13	0,95 %

Tipuri de malware

CERT.RO

Nr. crt.	Familia de malware	Număr de alerte asociate	Procent din total
1	Sality	4.953.615	34,16%
2	Downadup	2.570.006	17,72%
3	Nivdort	1.979.510	13,65%
4	Ramnit	1.081.592	7,46%
5	Dorkbot	830.914	5,73%
6	Mirai	522.377	3,60%
7	Zeroaccess	312.785	2,16%
8	Virut	277.460	1,91%
9	Conficker	244.371	1,69%
10	Tinba	187.556	1,29%

Sisteme de operare afectate

Nr. crt.	Tip de OS	Procent
1	Linux	42,96%
2	Network Devices Firmware/OS	22,91%
3	Unix	24,02%
4	UPnP OS	8,08%
5	Windows	0,57%

Tipuri de sisteme informatice afectate

Nr. Crt.	Tipul sistemelor afectate	Procent alerte
1	Rețele/Sisteme informatice	34%
2	Site-uri web	32%
3	Stații de lucru	22%
4	Servicii de tip banking/payment	7%
5	Echipamente de rețea	5%

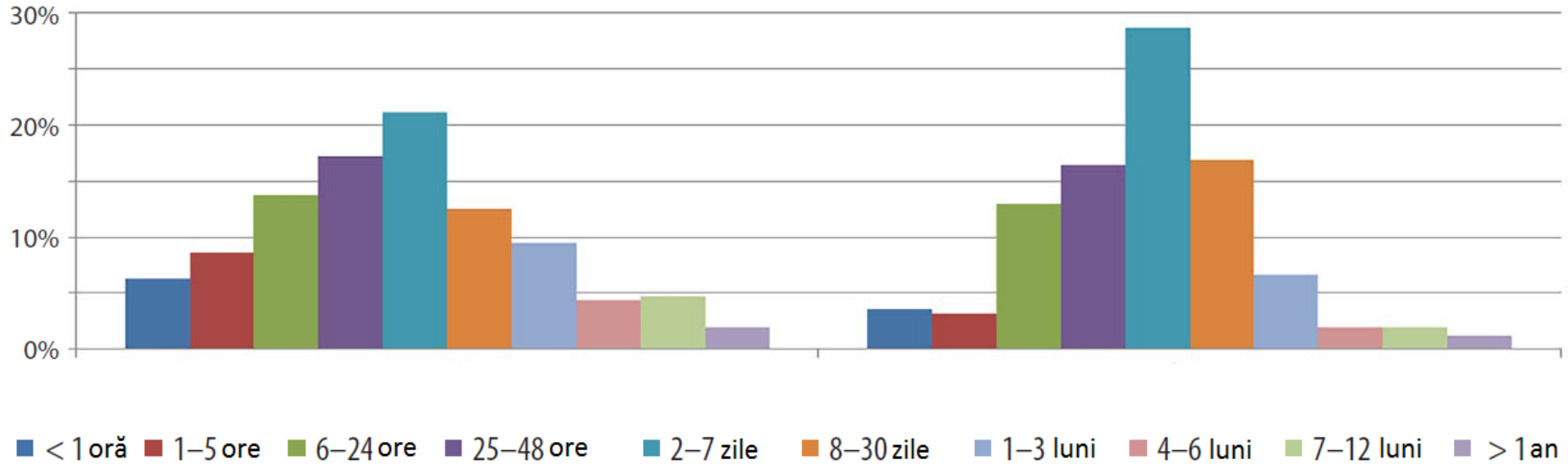
Majoritatea acestor tipuri de platforme/sisteme informatice procesează/stochează în mod obișnuit date cu caracter personal.

Astfel, de foarte multe ori incidentele de securitate informatică au ca și consecință afectarea securității datelor cu caracter personal.

Timpii de detectare și remediere a incidentelor

Timpul scurs
de la compromitere până la detectare

Timpul scurs
de la detectare până la remediere



* The 2016 SANS Incident Response Survey

Vă mulțumesc!
Întrebări?

Cătălin Pătrașcu

Șef Serviciu Securitate Informatică și Monitorizare | CERT-RO

catalin.patrascu@cert.ro