Nejzajímavější bezpečnostní incidenty v roce 2015

Michal Prokop • michal.prokop@nic.cz • 28.5.2015

CSIRT.CZ

CSIRT.CZ
powered by CZ.NIC

- Národní CSIRT tým pro ČR
- Založen v rámci plnění grantu MV ČR „Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky“ (2007 – 2010)
- V letech 2008 – 2010 provozován sdružením CESNET
- CZ.NIC provozuje pracoviště CSIRT.CZ od 1.1.2011
  - Status „akreditovaný“ u TI
  - Aktuálně 8 stálých členů týmu, další zdroje dle potřeby
- Vznik na základě Memoranda s MV ČR, poté s NBÚ

Honeypoty

- Od dubna 2015
- Zaznamenávání uploadu malwaru
- Více než 2 300 unikátních IP adres
  - Duben 1474
  - Květen 877
- Kontaktováno 46 zemí

2015-05-14 21:55:53.015348 GMT +0000,217.31.192.19,445,XXXXXXXXX,3214,Worm/Downadup,https://www.virustotal.com/search/?query=9013a966ea22aa85f5ae581a34139f86

Trojský kůň Geodo

- Původně Feodo, známý také jako Cridex/Bugat
  - Rozesílání falešných faktur v roce 2014
  - Deutshe Telekom, O2, Vodafone
- Geodo – nová verze Feodo
  - Ukradeno více než 50 000 SMTP credentials
  - Jiný kód
  - Stejné šifrování a stejný C&C server
  - 1 900 unikátních IP adres v ČR

Volně dostupné databáze

- Redis a Memcached
- Cachovací software webových aplikací
- Volně dostupné na 614 IP adresách v ČR

- Mongo databáze
- Dokumentově orientovaná NoSQL databáze
- Volně dostupná na 113 IP adresách v ČR

Ferret a Madness

- Malware pro OS Windows XP, 7, 8
- Stroje použity na DDoS
- Ferret – více než 60 000 strojů
- Madness – více než 70 000 strojů
- Oba malwary známe od roku 2013
- V ČR na více než 80 IP adresách

DHL

- E-mail o převzetí zásilky "DHL Logistik-Team"
- Trojský kůň v příloze
- 395 URL v 18 zemích

INFORMATIONEN ZU IHRER SENDUNG

Verehrte Frau, verehrter Herr,

Ihre unter der Nummer **216592874442** erfaßte Sendung wurde von DHL in Empfang genommen und voraussichtlich für den **24.03.2015** zur Auslieferung vorgesehen.

Wenn Sie weitere Informationen über den Sendungsstatus benötigen, können Sie eine direkte Statusabfrage über den folgenden Link starten: Die Sendung wurde im Ziel-Paketzentrum bearbeitet.

Mit freundlichen Grüßen,
Ihr DHL Team

Spolupráce s Policií ČR

- V průběhu roku několik phishingových stránek
- Malware na doménách mimo ČR
- Aplikace pro Android

- On-line obchody
- Ukradená čísla kreditních karet a jejich CVV
- 28 domén v 7 zemích

Sony

- Korejský národní CERT tým
- Malware "volgmer" → Zombie PC
- Útoky na Sony pictures
  - Údajně ohledně filmu Interwiev
- Další možné útoky
  - Sbírání údajů – credentials, kreditní karty
  - DDoS útoky
  - Útoky na HDD v síti

Zahraniční CSIRT/CERT týmy

- Taiwan - IP adresy z ČR komunikují s botnetem
- Kanada - šíření malwaru Sakula přes iframe
- Cert-RO - jednoduché/žádné heslo na routeru
- CERT-FR - veřejně dostupné ICS/SCADA
- Abuse.ch - neznámý Trojský kůň 1200 IP v ČR
- Prostřednictvím komunity TI
  - DDoS na banku v Gruzii

Statistika

Druhy incidentů (otevřené a zavřené)

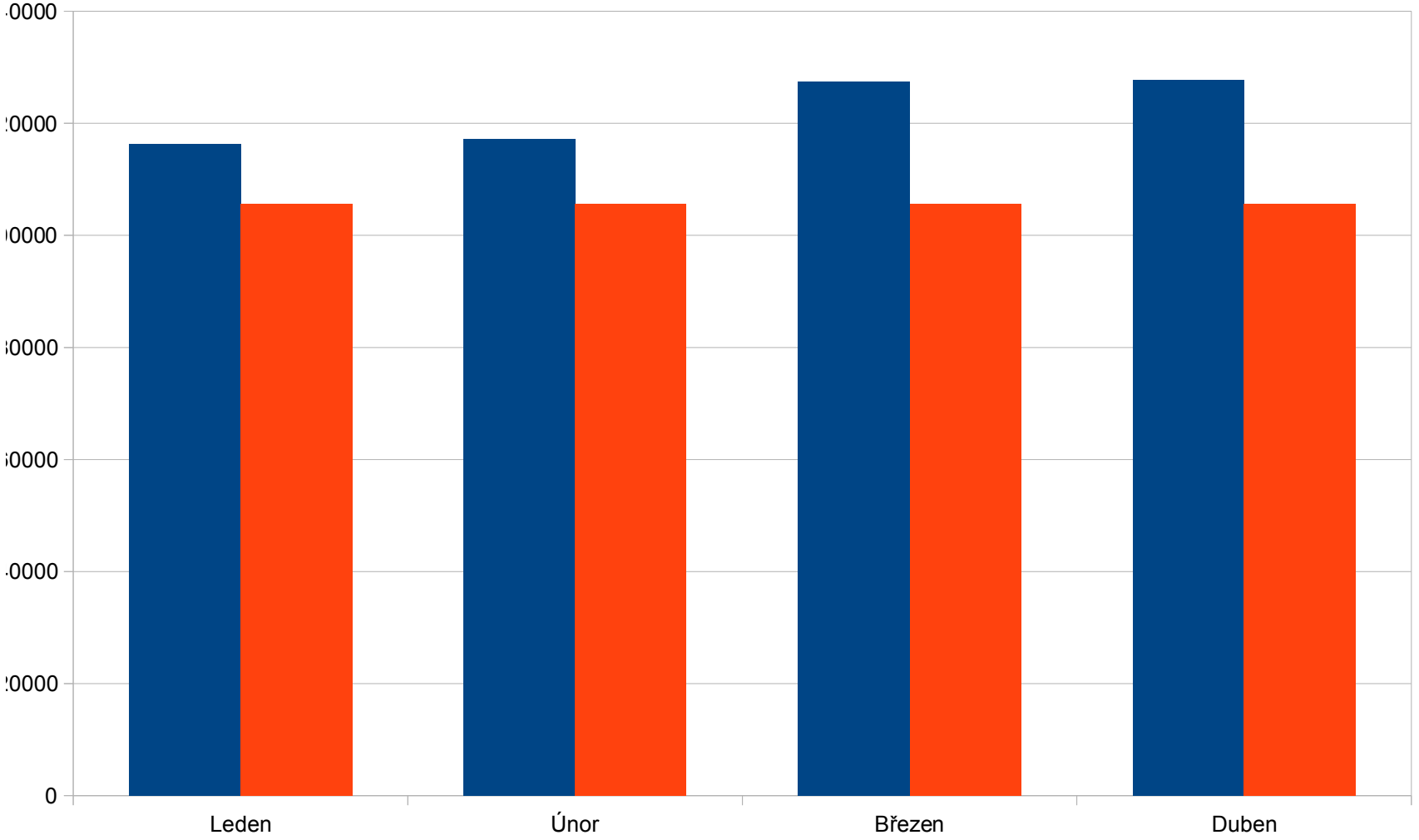
	2008	2009	2010	2011	2012	2013	2014	2015	sum
IDS				491	3924	2121	2380	1231	10147
Phishing	65	220	209	144	159	175	368	181	1521
Spam	47	28	103	26	43	73	159	50	529
Malware	53	97	42	9	19	44	117	107	488
Other	1	5	8	62	13	75	101	138	403
Virus		121	178	1	1				301
Trojan	66	6	26	5	5	12	56	24	200
DOS	1	4	2	2	68	72	32	18	199
Probe		3	14	25	12	26	86	16	182
Botnet		3	46	5	8	15		1	78
Portscan	10	4	1	6	1	3	2	1	28
Pharming							18		18
Crack	1		4						5
Copyright			1		1				2
sum	244	491	634	776	4254	2616	3319	1767	14101

Způsob uzavření incidentů

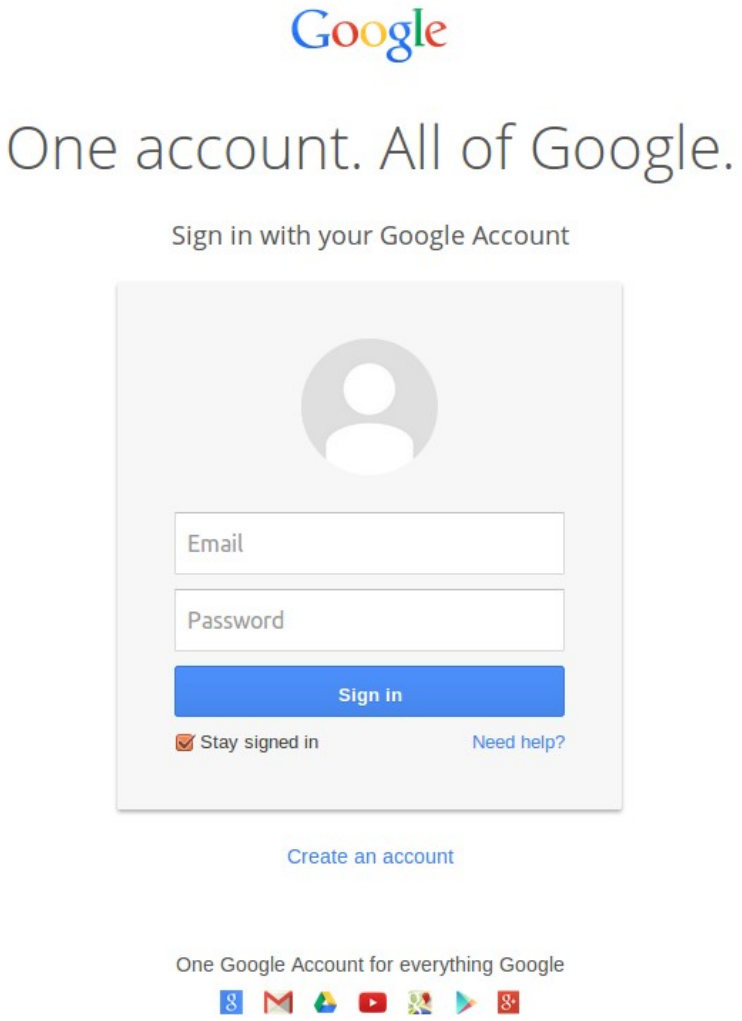
	2008	2009	2010	2011	2012	2013	2014	2015	sum
IDS Informed						2106	2374	1229	5709
Successful	64	149	67	622	4085	180	288	121	5576
Positive change		24	185	119	130	188	413	267	1326
We are informed	164	245	203	20	32	95	176	116	1051
Unsuccesful	1	41	20	10	7	47	67	19	212
Warning	15	32	158	5					210
Admin unable to solve			1						1
sum	244	491	634	776	4254	2616	3318	1752	14085

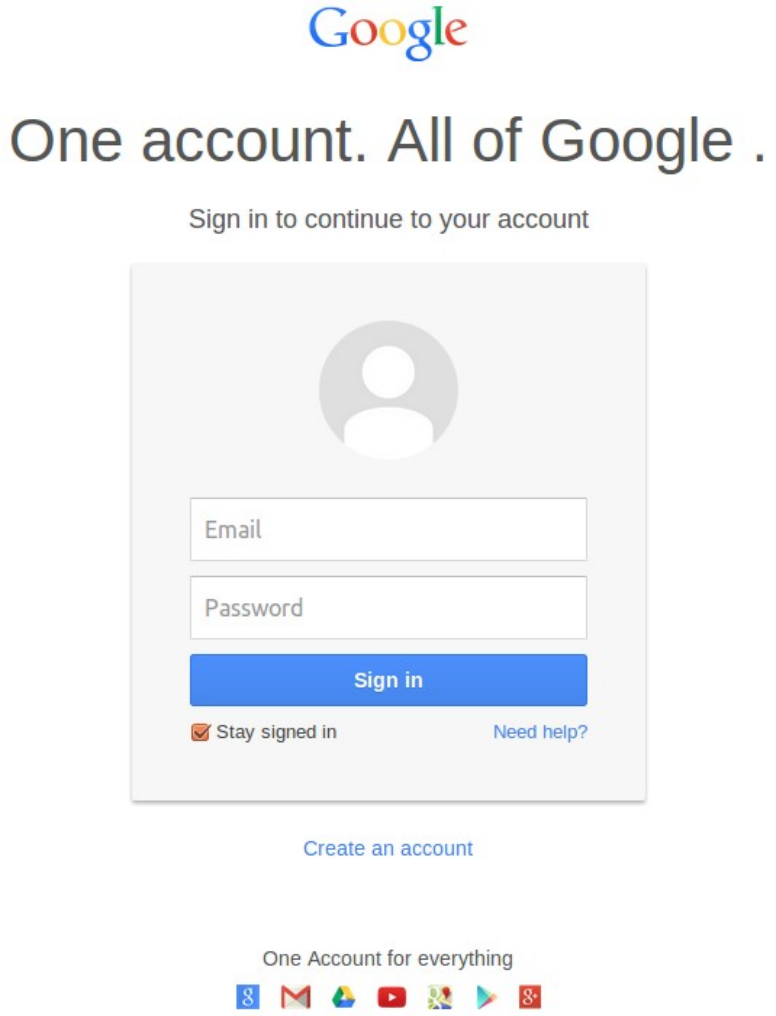
Aktuální statistiky na internetových stránkách csirt.cz

Statistika MDM 2015



Phishing


Google
One account. All of Google.
Sign in with your Google Account
Email
Password
Sign in
Stay signed in
Need help?
Create an account
One Google Account for everything Google


Google
One account. All of Google .
Sign in to continue to your account
Email
Password
Sign in
Stay signed in
Need help?
Create an account
One Account for everything

Děkuji za pozornost

Michal Prokop • michal.prokop@nic.cz • 28.5.2015