



# Vývoj trendů v oblasti kybernetické bezpečnosti během Covid-19 krize

Petra Raszková • [petra.raszkova@nic.cz](mailto:petra.raszkova@nic.cz) • 11. 11. 2020



# Covid-19 krize

- **bezprecedentní** krize v historii EU
- restriktivní, izolačních opatření napříč jednotlivými členskými státy EU → **signifikantní dopad** na interní bezpečnost
- rychlá reakce na vývoj krize ze strany útočníků → **adaptace MO**



# Jaké faktory ovlivnily změny?

- **vysoká poptávka** po určitém zboží (*I. vlna: ochranné pomůcky a farmaceutické produkty, II. vlna testovací sady*)
- **omezení pohybu** osob napříč EU
- **omezení veřejného života** → **přesun** do kyberprostoru → **omezenost** řešení, konzultací
- **digitální řešení** (HO, e-škola) x fyzická bezpečnost
- **psychologické faktory**



# Threat landscape

- **široké spektrum** kriminálních aktivit a hrozeb vycházejících z možnosti využití krize
- evaluace stavu na základě jak **reaktivního**, tak **proaktivního přístupu**
- **vysoký zájem o informace** týkající se šíření viru



# Threat landscape

- **sociální inženýrství**, phishing skrz SPAM kampaně, **spear-phishingu** (BEC)
- **phishingové kampaně** distribuující **malware** – **AZORult**, **Emotet**, **Nanore RAT** a **TrickBot** prostřednictvím **URL odkazů** a příloh
- alarmující množství útoků na různé subjekty



# Aktuální hrozby v reálném čase



16:16 Ligue du LOL : les prud'hommes déboutent Alexandre Hervaud, licencié de « Libération »

## Ongoing threats



*"The Trump vision ... opens Judea and Samaria to academic, commercial and scientific engagement with the United States. This is an important victory against all those who seek to delegitimise everything Israeli beyond the 1967 lines"*

*"highly respected senior legal experts, such as former Israeli Supreme Court Justice Salim Joubran,"*

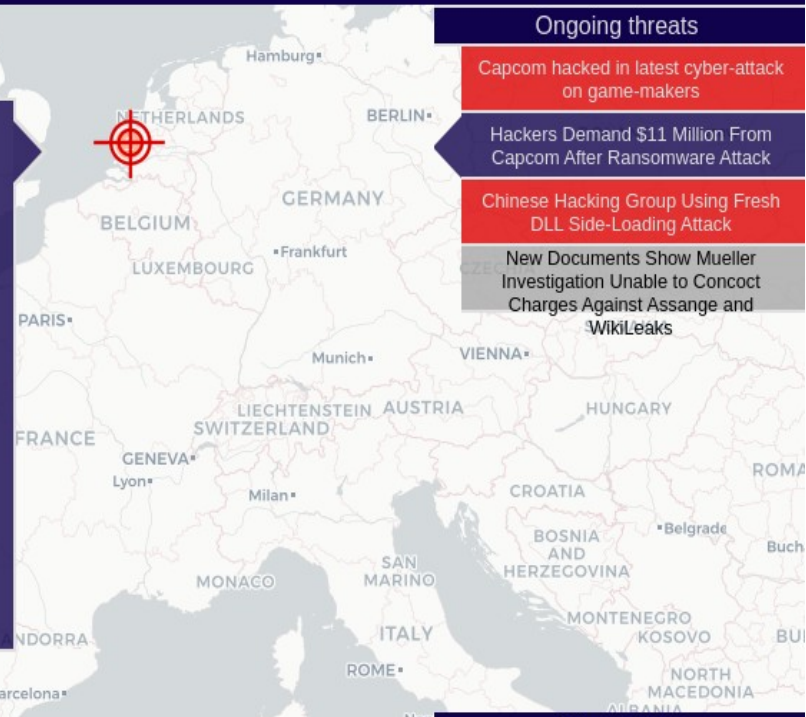
Irwin Cotler	Google	Education Ministry	Red Hat
Richard Branson	Microsoft Windows	Justice Department	Donald Trump
Microsoft	FBI	Symantec	Superior Court
Benjamin Netanyahu	International Business Machines Corp	EU	The Des Moines Register
Xi Jinping			

### Hackers Demand \$11 Million From Capcom After Ransomware Attack

en | SecurityWeek |

Friday, November 6, 2020 16:16

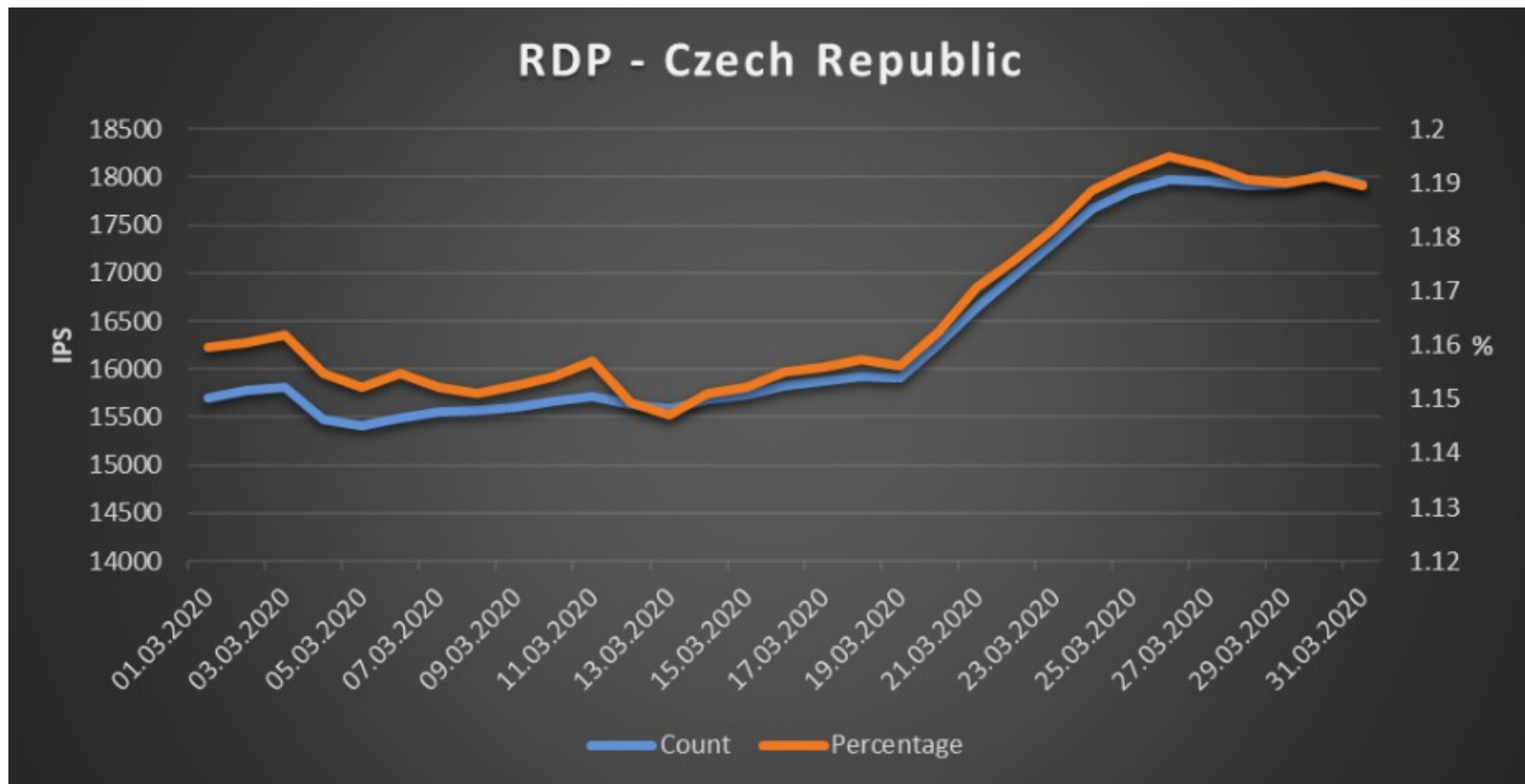
A group of cybercriminals that breached the systems of Japanese video game giant Capcom is demanding \$11 million after deploying ransomware and stealing vast amounts of data. Capcom, which has operations in the US, Europe and East Asia, is best known for games such as Resident Evil, Street Fighter,....



- Ongoing threats
- Capcom hacked in latest cyber-attack on game-makers
- Hackers Demand \$11 Million From Capcom After Ransomware Attack
- Chinese Hacking Group Using Fresh DLL Side-Loading Attack
- New Documents Show Mueller Investigation Unable to Concoct Charges Against Assange and WikiLeaks

- Cyber Crime
- Malware

# Rozšíření threat attack surface: RDP (Alef 0)



# Darkweb

- **ekonomické a logistické restriktce:**
  1. pokles aktivity některých obchodů a tržišť
  2. nárůst cen
  3. orientace na nový druh zboží
- předstíraný prodej **produktů zdravotních a farmaceutických** potřeb (předmět vysoké poptávky)
- THC tabletky na zvýšení imunity, N95 a ochranné masky (*kazuistika*)
- **ITA, CZE, JPN, USA, CAN** (užití národních jazyků)





# Jiné škodlivé/ podvodné aktivity

- **FAKE NEWS:**
- šíření dezinformací
- sociální síť Facebook → dezinformace (*Unmasking America for violating*)
  
- **EXTREMISMUS:**
- *FRA: neonacistický blog*



# Jiné škodlivé/ podvodné aktivity

## PODVODNÉ JEDNÁNÍ:

- platformy AMAZON a eBay → detekování falešných produktů spojených s pandemií

## MEOW útoky:

- nezabezpečené databáze (Mongo DB, Elasticsearch)

```
green open 0sqqpgrfts-meow v_n7UjhMSZycUBCUFm5MGA 1 0
green open luj7hoytod-meow sbYGE7JkSPmZwXlhbr7lwQ 1 0
green open yietudd4fn-meow Jkkd3Zx6TJOXNJDwzYPtRQ 1 0
green open vnwk6uy6ay-meow AUeGARyvRHqAItWb6dspRw 1 0
green open logstash-root_log_test-2020.07.20 1Dic7iJmRU-EE02mnIhwfA 1 0
green open logstash-feedback_record_prod-2020.07.20 24PgZjlQTVysm_JmW-gReA 1 0
green open logstash-firebase_events_prod_cus-2-2020.07.20-s2 GhRBu3S0S-6gZYMxvnXwbA 1 0
```



# Phishing

- prudký nárůst od začátku února
- informace o Covid-19 od světově známých organizací (WHO)
- **nestandardní podoba** → *informace o propuštění ze zaměstnání, nakazím Vás i Vaši rodinu, falešné seznamky*

-----

1. Spear-phishing → BEC

2. **Vishing (voice phishing)** → **9/ USA**

snaha získat VPN kredenciály:

a. telefonicky → **způsob, jak obejít 2FA**

b. na webech napodobujících korporátní VPN portály



# Phishing: statistika CSIRT.CZ

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	sum
<b>Sensor Network*</b>				491	3924	2121	2380	3771	9944	13858	18435	14911	4048	83883
<b>Phishing</b>	65	220	209	144	159	175	368	367	363	409	518	483	704	4184
<b>Spam</b>	47	28	103	26	43	73	159	108	289	121	144	128	188	1457
<b>Malware</b>	53	134	121	10	20	45	117	240	104	99	135	85	95	1258
<b>Other</b>	1	5	13	62	14	75	102	264	182	200	58	85	82	1143
<b>Probe</b>		3	14	25	12	26	86	42	13	26	171	141	56	615
<b>Trojan</b>	66	6	26	5	5	12	56	90	79	94				439
<b>DOS</b>	2	4	2	2	68	72	32	37	12	14	7	16	14	282
<b>Botnet</b>		3	46	5	8	15		4	71	29	20	4	2	207
<b>Virus</b>		84	99											183
<b>Portscan</b>	10	4	1	6	1	3	2	5	6	13	16	3	25	95
<b>Pharming</b>							18	3	2	3	10	9	3	48
<b>sum</b>	244	491	634	285	330	496	940	1160	1121	1008	1079	954	1169	9911



# Falešné webové stránky

- napodobování legitimní snahy informovat občany o vývoji krize
- vznik „dashboardů“ → přístup k aktuálním datům
- dashboardy replikující malware → „*mapa koronaviru*“

## Registrace webových stránek

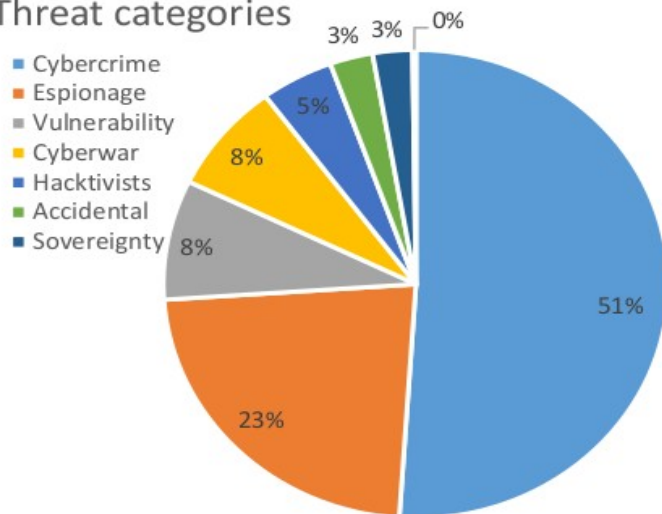
→ projekt ADAM



# Vývoj nových forem malware

- **Emotet a Trickbot - silný nárůst aktivity**

Threat categories



Top 10 malware families

- 1 Emotet
- 2 NjRAT
- 3 Mofksys
- 4 Qbot
- 5 UrSnif
- 6 SilentNight
- 7 Zloader
- 8 Agent Tesla
- 9 Quasar
- 10 TrickBot



# Ransomware

- práce na dálku → zvýšení rizika
  - *informace o vakcíně, informace o vládní pomoci*
- tzv. dvojité vydírání:
  1. šifrování
  2. zveřejňování informací



Figure 1 – The evolution of ransomware coercion tactics



# SCAM

- propojení se sociálním inženýrstvím a phishingovými kampaněmi
- falešné dárcovské kampaně (*prevence, detekování nebo léčba COVID-19*)
- **non-delivery scam:** potřeba zdravotnických pomůcek, předstíraný prodej za účelem profitu
- psychologický faktor: **zneužívání strachu** → nabídka domácích testovacích setů





# DDoS

- 2019 vs. 2020: **nárůst o 350-500%**
- nejsilnější DDoS: **2.5 Tbps**, Google
  - Blackboard, Zoom (**+ fenomén: zoombombing**), Google Classroom, Couseira, edX, Google Meet
- **5/ e-learningové platformy** a doručování jídla



# Závěr: doporučení

- **kontrola infrastruktury**
  - otevřené porty
  - **zálohování a aktualizování**
- **pomoc uživatelům:**
  - **filtrace** zpráv (automatizované technické nástroje)
  - **edukace** uživatelů
  - **2FA**
  - založení **hotline** pro netypické situace/ nedostupný IT-support
  - **nebát se reportovat, požádat o kontrolu, radu**



# Děkuji za pozornost

Petra Raszková • [petra.raszkova@nic.cz](mailto:petra.raszkova@nic.cz)

