



plk. Mgr. Radek Nezbeda

Ředitel sekce kybernetické kriminality

Národní centrála proti organizovanému zločinu

Služba kriminální policie a vyšetřování

[radek.nezbeda@pcr.cz](mailto:radek.nezbeda@pcr.cz)

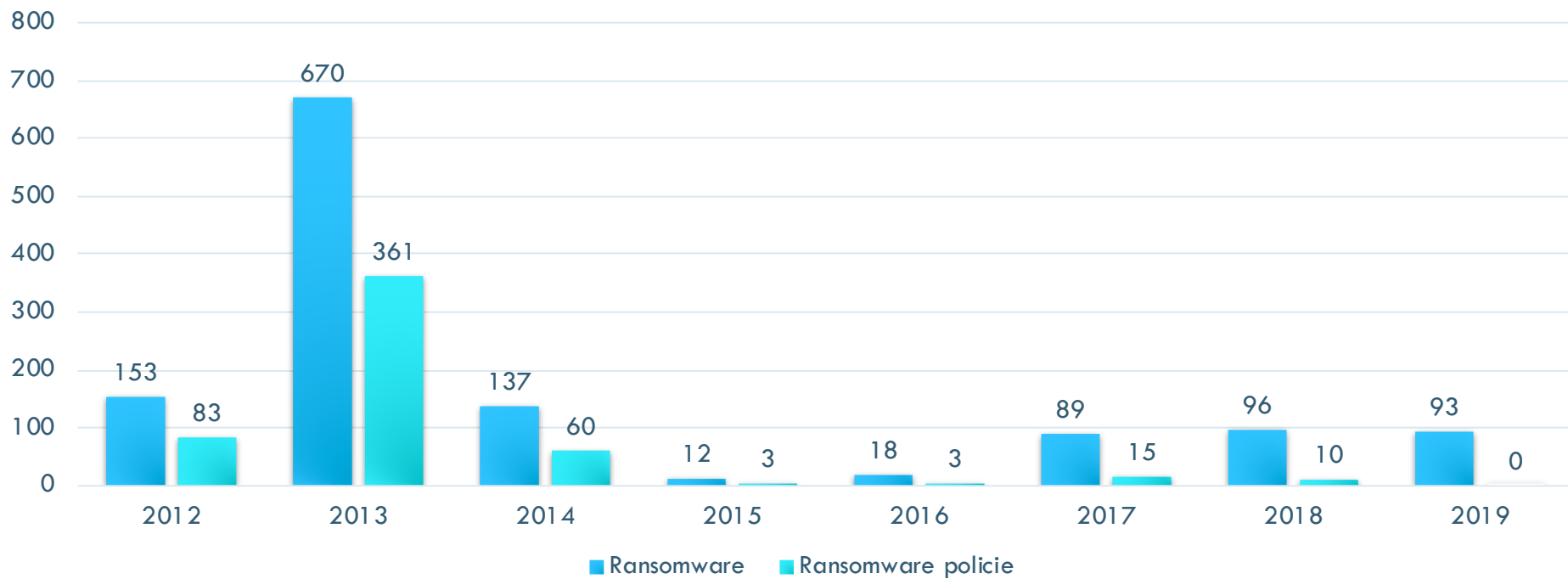


# ORGANIZACE BOJE PROTI KYBER KRIMINALITĚ

- Od 1.8.2016 existuje Národní centrála proti organizovanému zločinu (NCOZ)
- V rámci centrály existuje 5 sekcí a jednou z nich je sekce kybernetické kriminality
- Každé Krajské ředitelství policie má zřízeno Oddělení kybernetické kriminality
- Kybernetická kriminalita neustále narůstá, z 6815 v roce 2018 na 8417 skutků v roce 2019
- §§230-232 tj. neoprávněné přístupy k počítačovému systému pak nárůst z 696 na 930 věcí



# STATISTIKA RANSOMWARE



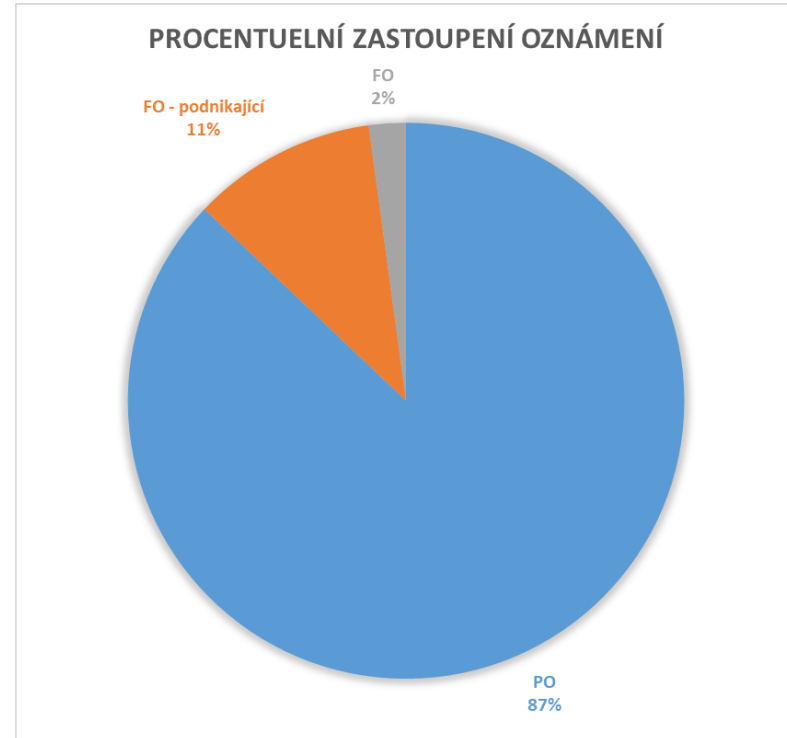
# STATISTIKA OBECNĚ

Jak je vidět, ransomware není na takovém vzestupu, jak by se mediálně mohlo zdát z pohledu závěru roku 2019.

Zřejmá je ovšem velká latence této kriminality zejména u FO

Mnohem více se na oznámení podílí PO či podnikající FO. Toto je pravděpodobně dáno tím, že znemožnění přístupu k datům svých systému nese téměř vždy další sekundární následky a je tedy důležité věc zaevidovat i z důvodu případných následných problémů ve vztahu k orgánům veřejné moci (typicky ztráta účetnictví).

FO si poplácne nad ztrátou fotek z dovolených, ale většinou ji žádné další možné následky nečekají.

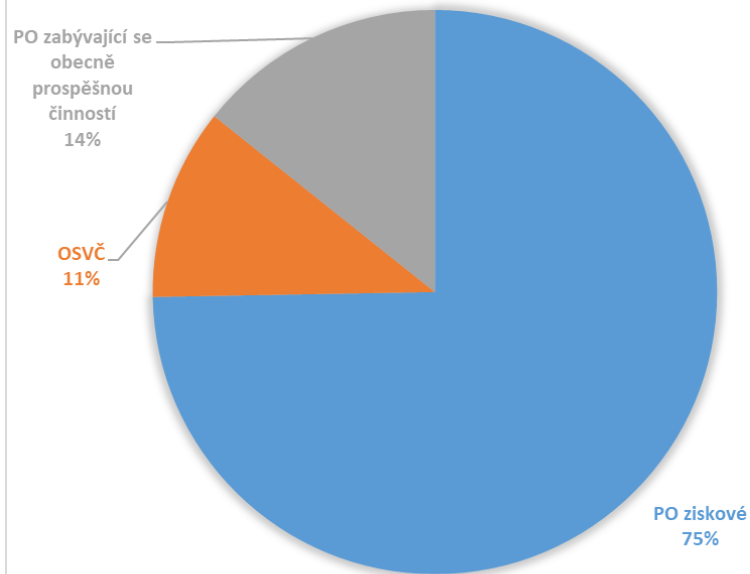


# STATISTIKA OBECNĚ

Zajímavostí může být počet oznamovatelů z řad PO zabývajících se obecně prospěšnou činností, neboť více než polovina z nich jsou vzdělávací a školní zařízení.

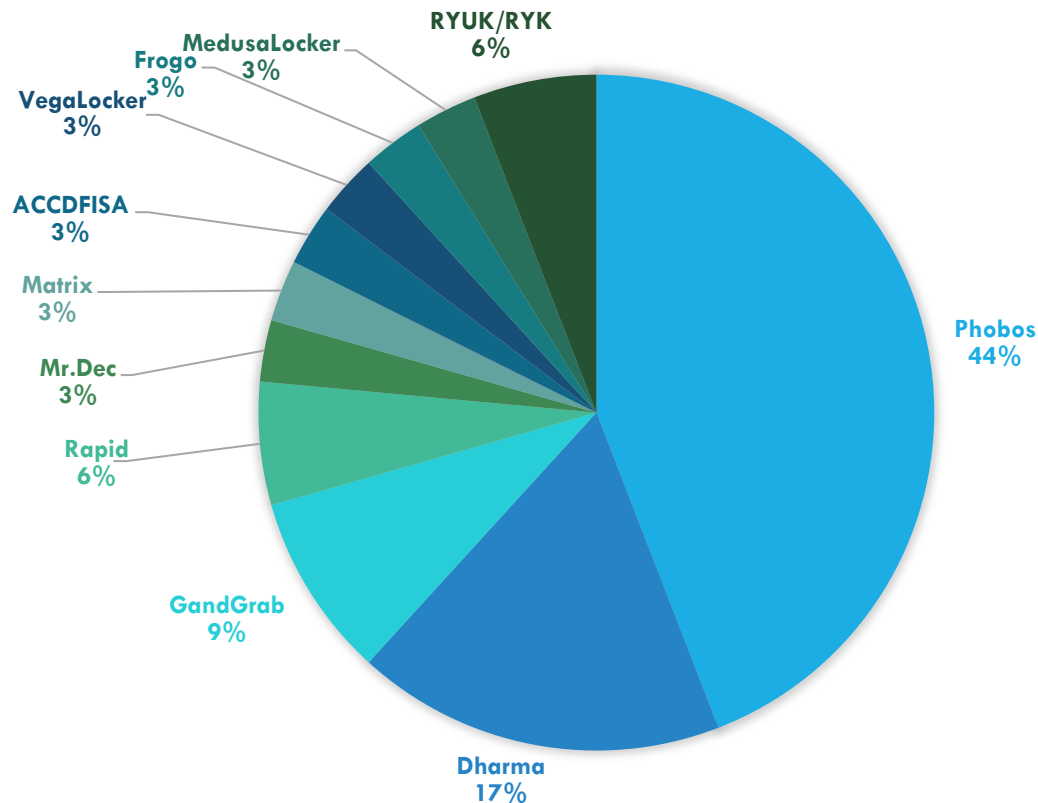


PODÍL OZNÁMENÍ DLE ČINNOSTI



# ZASTOUPENÍ RANSOMWARE FAMILY V ROCE 2019

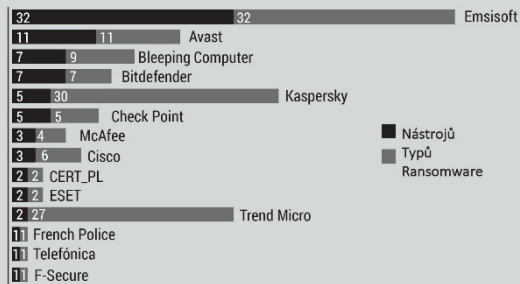
Dle našich statistik nejčastější ransomware v ČR, dle dat Europolu jsme očekávali větší zastoupení ransomware z rodiny Dharma.



# PROJEKT NO MORE RANSOM (EUROPOL EC3)

NCOZ se připojila s podporou, dodáváním dat a českou lokalizací v roce 2017.

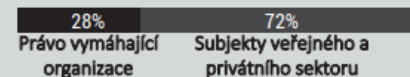
## Nástroje 82



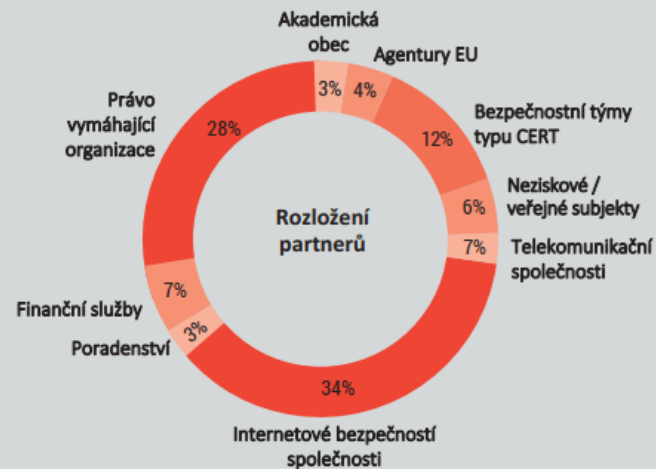
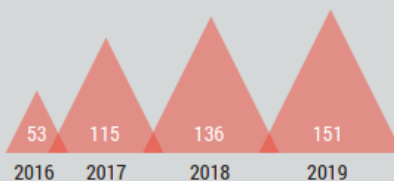
## NO MORE RANSOM!

### Partneři 151

#### Zakládající členové



#### Roční nárůst partnerů



# NOMORERANSOM.ORG

NO MORE RANSOM!

★ čeština

Detektiv Šifra

Ransomware: otázky a odpovědi

Preventivní rady

Dešifrovací nástroje

Nahlášení trestného činu

Partneři

O projektu



## PREVENTIVNÍ RADY

### WannaCry doplňující preventivní doporučení

- 1 **Zákázáním funkce smb v1** dojde k zamezení šíření Wannacry uvnitř Vaší sítě.
- 2 **Instalujte aktualizace produktů Microsoft**, toto také zamezí šíření Wannacry uvnitř Vaší sítě. Pro více informací klikněte [zde](#)

### Jak se bránit útoku ransomware?

- 1 **Zálohovat! Zálohovat! Zálohovat!** Mějte zálohu systému a nákaza ransomware nemůže nikdy zničit Vaše osobní data. Nejlepší je vytvořit dvě záložní kopie: jednu uloženou na cloudu (nezapomeňte použít službu, která automaticky zazálohuje Vaše soubory) a jednu na fyzický nosič (externí pevný disk, flash disk, zvláštní notebook, atd.). Odpojte tato zařízení po provedení zálohy. Vaše záložní kopie přijdou vhod v případě, kdy nešťastnou náhodou smažete důležité soubor nebo v případě havárie pevného disku.
- 2 **Používejte silný antivirový software** k ochraně svého zařízení před ransomware. Nevyvíjejte heuristické funkce, protože tyto napomáhají k zachycení nových typů ransomware, které nebyly doposud oficiálně detekovány.
- 3 **Udržujte veškerý Váš software aktualizovaný.** Jakmile jsou pro Váš operační systém (OS) nebo aplikace uvolněny nové aktualizace, nainstalujte je. A pokud software nabízí možnost automatických aktualizací, využijte ji.

109

typů ransomware  
pokryto

200 tis.

obětem se dostalo pomoci

\$108M

kriminálního zisku uchráněno

188

zemí vstoupilo na portál

NMR



# DOPORUČENÍ

Obecně nedoporučujeme platit výkupné. Zaplacením výkupného vyděračům pouze potvrdíte, že ransomware funguje, a není žádná záruka, že dostanete dešifrovací klíč, navíc zaplacením potvrdíte funkčnost jejich zločinného business modelu a budete je podporovat v dalším vývoji malware a páchaní trestné činnosti.



## ARE YOU A VICTIM OF RANSOMWARE?



**DON'T PAY**



**NO MORE RANSOM!**

[www.nomoreransom.org](http://www.nomoreransom.org)

# ZJIŠTĚNÍ TYPU RANSOMWARE

<https://www.nomoreransom.org/crypto-sheriff.php?lang=cs>

<https://id-ransomware.malwarehunterteam.com/?fbclid=IwAR3iVLCeiHqL6TsYkrsfuEJNvLB1PY2OkyUiXQOYT2zKVWttrUaqzU1g8TM>

RYUK

<https://www.pcrisk.com/removal-guides/13394-ryuk-ransomware>

RYK

[https://www.pcrisk.com/removal-guides/14177-ryk-ransomware?fbclid=IwAR0xKQwC5O08JuZkPSAPleHQBXRj2l4zthU-SaPd\\_UxTnJ3QXFdG1d044](https://www.pcrisk.com/removal-guides/14177-ryk-ransomware?fbclid=IwAR0xKQwC5O08JuZkPSAPleHQBXRj2l4zthU-SaPd_UxTnJ3QXFdG1d044)



# EMAS - EUROPEAN MALWARE ANALYSIS SYSTEM

European Malware Analysis System je služba poskytovaná pro OČTŘ v rámci Europolu a EC3 (European Cybercrime center) kam můžeme zasílat vzorky malware k automatické analýze, což se hodí zejména v případě hackerských útoků a dále slouží k automatizovaným crosscheckům v rámci OČTŘ.



# RANSOMWARE – NEMOCNICE BENEŠOV

Prověřování věci provádí oddělení kybernetické kriminality SKPV KŘP Středočeského kraje

Spolupráce s NÚKIB a ESET + vlastní šetření

Kampaň EMOTET-TRICKBOT-RYUK – vyloučen cílený útok/napadeno více subjektů

Brute – force na RDP – spuštění ransomware RYUK

## **Obecně k ransomware :**

napadené systémy vykazují obdobné zranitelnosti/chyby v zabezpečení

## **Doporučení do budoucna:**

Mediální zdrženlivost všech participujících subjektů – komunikaci ponechat na PČR

# RANSOMWARE – NEMOCNICE BENEŠOV

## **K zamyšlení:**

bezpečnostní management – intenzivnější vliv/metodika i na subjekty mimo KI ???

## **Nejčastější zranitelnosti:**

neopatrnost uživatelů – otevření zavirované přílohy emailu

chybí AVP nebo je špatně nastaveno – nechráněno heslem, vypnuté detekce nebezpečných aplikací, neaktualizování SW, publikace RDP, SSH do internetu

## **Doporučení k bezpečnosti:**

aktualizace AVP, SW apod., firewall, nepublikovat RDP, SSH - používat VPN (2FA) do interní sítě, offline zálohování (strategie 3-2-1), segmentace sítě, ACL mezi vln apod.

# ZÁVĚR

Děkuji za pozornost



plk. Mgr. Radek Nezbeda

ředitel sekce kybernetické kriminality

+420 725 761 140

[radek.nezbeda@pcr.cz](mailto:radek.nezbeda@pcr.cz)