Systém včasného varování

Jakub Onderka

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Jakub Onderka

Bezpečnostní analytik, GovCERT.CZ
Národní úřad pro kybernetickou a informační bezpečnost

E-mail: j.onderka@nukib.cz
PGP: 2EEF A5E6 CAB0 A87F 4531 1FC3 B158 F39D C523 01CD

Jakub Onderka

- Vládní CERT (GovCERT.CZ)
- Národní centrum kybernetické bezpečnosti
- NÚKIB

- Bezpečnostní analytik
- Řešení incidentů (když je třeba)
- Vývojař
- Příprava národních kybernetických cvičení (Cyber Czech, TTX)
- Kontroly kritické informační infrastruktury (techická část)
- Příprava bezpečnostních regulací (techická část)

rmx.news/article/article/cyber-attack-paralyzes-czech-hospital

REMIX

NEWS COMMENTARY HUNGARY POLAND CZECH REPUBLIC CORONAVIRUS

CZECH REPUBLIC | CYBERSECURITY | HEALTHCARE | MEDICINE | CYBERCRIME | NEWS

Cyberattack paralyzes Czech hospital

Due to a cryptovirus, a hospital in the city of Benešov has been out of service for the second day

editor:
REMIX
author:
CZECH NEWS AGENCY
via:
LIDOVKY.CZ

A cryptovirus has completely paralyzed the operations of a hospital in the Czech city of Benešov, about 40 kilometers southeast of Prague.

The virus attacked the hospital system starting on Tuesday night this week but the hospital's network is still locked. Computers first began to slow down at the surgical clinic, and shortly thereafter, the IT systems in the entire hospital stopped working. The virus overcame the hospital's firewall as well as two antivirus systems.

Hospital management announced that patients' health and lives are not at risk, although IT workers and cybersecurity experts have not been able to remedy the problem as of Thursday.

12. března 2020

www.vlada.cz/en/media-centrum/aktualne/due-

GOVERNMENT OF THE CZECH REPUBLIC

home
members of the government
government meetings
media centre
european affairs
advisory and working bodies
office of the government

search

česká verze

June 20, 2020

Press Advisories

12. 3. 2020 18:41

Due to the spread of the coronavirus the government has declared a state of emergency and on 12 March 2020 further tightened preventive measures

Prime Minister Andrej Babiš announced a state of emergency and other preventive measures at a press conference, 12 March 2020.

Media Centre

Press Advisories
Scheduled Events
Press Releases
Press Conferences
Introducing
Government Meetings
Important Documents
Important Information
Contacts

Important information

Reasonable Europe
Czech Presidency of the Visegrad Group 2019/2020

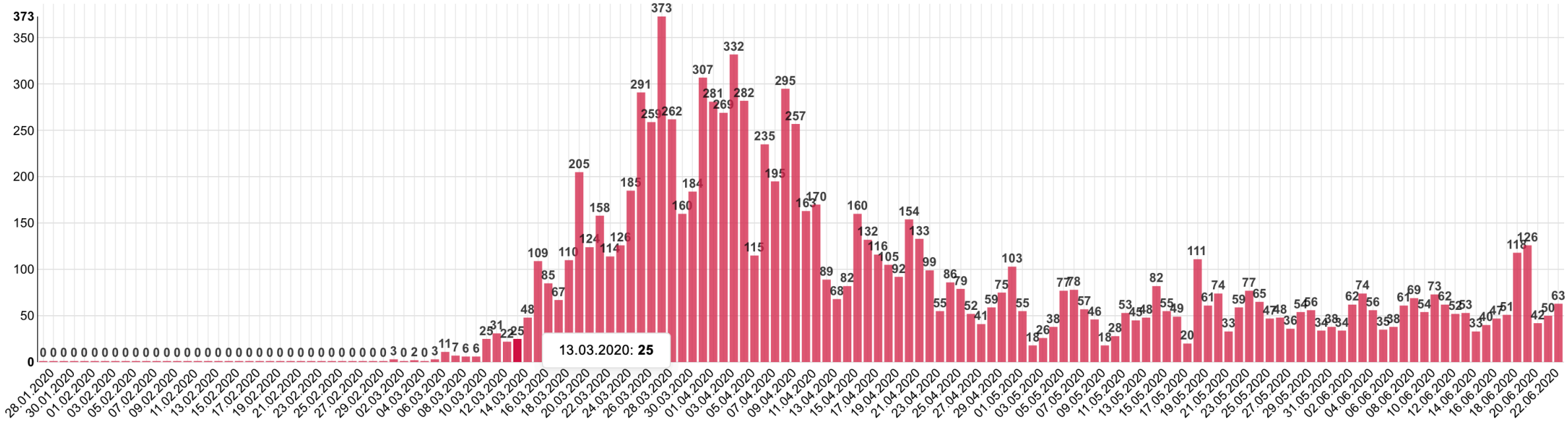
EUROSKOP.CZ

1918 100 2018

13. března 2020

Denní přehled počtu osob s nově prokázaným onemocněním COVID-19 dle hlášení krajských hygienických stanic a laboratoří

Přehled za posledních 14 dní | Kompletní přehled za celé období | Tabulkový přehled



13. března 2020

https://www.zdnet.com/article/czech-hospital-hit-by-cyber-

ZDNet | AFRICA | UK | ITALY | SPAIN | MORE | NEWSLETTERS | ALL WRITERS

Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak

One of the Czech Republic's biggest COVID-19 testing laboratories hit by mysterious cyberattack.

By Catalin Cimpanu for Zero Day | March 13, 2020 -- 17:36 GMT (17:36 GMT) | Topic: Coronavirus: Business and technology in a pandemic

Image via Google Street View

NEWSLETTERS

ZDNet Announce UK

ZDNet's Announcements newsletter offers a mix of stories, special offers and members-only benefits.

Your email address SUBSCRIBE

SEE ALL

MORE RESOURCES

Supercharged Cybersecurity Bundle 2018

Training from ZDNet Academy

13. března 2020

- **Fakultní nemonice Brno**, druhá největší nemocnice v Česku a největší v Brně
- Testovací centrum COVID-19
- Ransomware útok, šifrování dat začalo mezi 12. a 13. březnem (pátek)
- **Všechny systémy mimo provoz, fungovaly jen pracovní stanice bez centrálních systém**
- S „vyšetřováním" jsme začali v pátek ráno spolu s zaměstnanci nemocnice a partnery
- Náše hlavní cíle:
  - Pomoci s obnovou systemů (ověřit, které systémy nebyly napadeny)
  - **Získání identifikátorů kompromitace (IOCs) pro ověření, jestli se podobný útok nechystá na ostatní nemocnice**

Není těžké napadnout české nemocenice

Popis stavu

- nemocnice je IT prorostlá a na IT závislá, že bez PC nejsou prakticky schopni léčit,
- v Pelhřimovské nemocnici je 700 zaměstnanců, 340 lůžek, za 2019 celkem 80k ambulantních vyšetření a 14k hospitalizací,
- IT oddělení má 4 zaměstnance,
- v síti mají 400 stanic a 40 serverů + ještě telefony, ústředny, tiskárny, 40 IT systémů,
- vyvíjí si sami interní www systémy (30),
- mají cca 50 IT zásahů za den (volání a žádosti zaměstnanců),
- na nic jiného není čas,
- podfinancování, špatné personální zabezpečení, starý HW,
- legislativa si vynutí nový systém, tak se pořídí, ale pak se už o něj nikdo nestará,
- mají 400 stanic a ještě dnes mají 60 stanic s Windows XP,
- po v médiích propíraných kauzách se trochu hnuly ledy a do HW se začalo trochu investovat, za poslední 4 měsíce vyměnili 70 stanic,
- nikdy nekončící nářek, za 10 let se mu nepovedlo prosadit jednoho IT člověka navíc,

Zdroj: https://blog.kamil-zmeskal.cz/2020/09/jak-vypada-it-v-nemocnici-v-pelhrimove.html

Není těžké napadnout české nemocenice

FN Hradec Králové

FN Motol (Praha)

Zdroj: https://twitter.com/matesfm/status/1235974604637835265

Zdroj: https://twitter.com/krcmar/status/1264814764095672326

Co je to identifikátor komprimitace

- Jakýkoliv technický údaj, který je spojen s útokem.

- **IP adresa:** 8.8.8.8, 8.8.0.0/16, 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- **Doména:** www.attacker.com
- **URL:** https://atacker.com/a/vbztx
- **Hash:** 9e107d9d372bb6826bd81d3542a419d6
- **E-mailová adresa:** info@attacker.com
- **Název souboru:** faktura-fn.docm
- **Umístění v registru systému Windows**
- a další

Jak sdílíme IOCs

- Pomocí e-mailů 😖
  - **Komplikováné** – vyžaduje ruční kopírování identifikátorů do bezpečnostních systémů
  - **Nezabezpečené** – téměř nikdo nepoužívá PGP nebo S/MIME pro podepisování a šifrování e-mailů
  - **Nespolehlivé** – nedokážeme zjistit, zda byl e-mail opravdu doručen
    - Někdy neznáme aktuální kontaktní informace, jelikož subjekty neplní své zákonné povinnosti
  - **Náchylné na chyby** - překlepy, poslání e-mailu s e-mailovými adresami v kopii, zapomenutí na obfusakci identifikátorů

Jak sdílíme IOCs

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky
IČO: 05800226
ID datové schránky: zzfnkp3

Spisová značka:
350 - 231/2020
Číslo jednací:
2066/2020-NÚKIB-E/350

Brno, 16

VAROVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/3
(dále jen „Úřad"), podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečn
souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické
vydává toto

Úřad dále pro možné prověření škodlivé činnosti uvádí hashe škodlivých souborů:

File type: Win32 EXE

- MD5 28e1786bd652942f0be31080a9452389
- SHA-1 44cb931ee16f1f6e3b408035efcd795d8aa0c9be
- SHA-256 7aa996ff7551362f42ba31d4cd92d255a49735518b3f4dc33283fdd5c5a61b42

File type: Win32 EXE

- MD5 e20ee9bbbd1ebe131f973fe3706ca799
- SHA-1 4e92e5cbe9092f94b4f4951893b5d9ca304d292c
- SHA-256 f632b6e822d69fb54b41f83a357ff65d8bfc67bc3e304e88bf4d9f0c4aedc224

File type: Win32 EXE

- MD5 9dbbfa81fe433b24b3f3b7809be2cc7f
- SHA-1 b87405ff26a1ab2a03f3803518f306cf906ab47f
- SHA-256 dfbcce38214fdde0b8c80771cfdec499fc086735c8e7e25293e7292fc7993b4c

Obfuskace údajů

- Zabránění omylům, kdy příjemce klikne na malware URL v e-mailu
- Ochrana před použitím automatizovaných nástrojů detekce

- **IP adresa:** 8.8.8.8 -> 8[.]8.8.8
- **Doména:** attacker[.]com
- **URL:** hxxps://attacker.com
- **E-mail:** info[@]attacker.com

Potřebujeme něco lepšího…

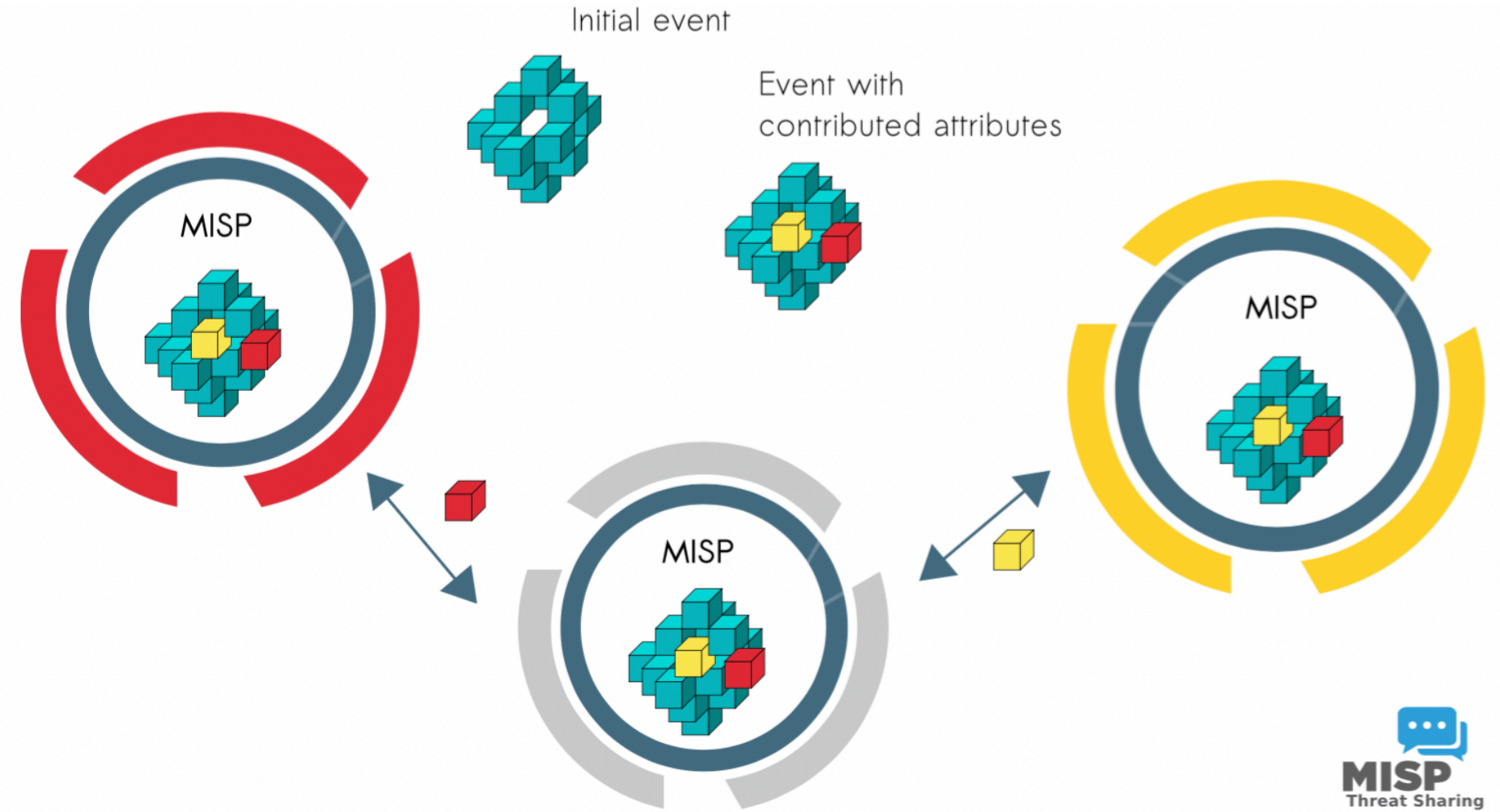
- Potřebujeme nástroj, kterým bychom sdíleli IOC pro naši konstituency (zákazníky):
  - **Jednoduše** – z webového rozhraní, jen s několika manuálními kroky
  - **Automatizovaně** – zákazníci se můžou připojit do system skrz automatizované API pomocí existujících formátů (STIX2, MISP, …)
  - **Bezpečně** – všechna komunikace musí být šifrovaná
  - **ACL** – některá IOCs chceme sdílet jen určité skupině organizací
  - **KII** – systém musí splňovat pravidla pro kritickou infromační infrastrukturu
- „Nice to have”
  - **Zpětná vazba** – konstituence s náma může kooperovat
  - **UX** – uživatelské rozhraní musí být srozumitelné

Naše rozhodnutí

- Externí vývoj nového systému
  - drahé
  - časově náročné
  - nejistý výsledek
- Interní vývoj
  - nemáme kapacity
- **Rozhodli jsme se vybat existující systém – MISP**

Proč jsme vybrali MISP

- De facto průmyslový standard
  - Mezinárodní partneři (NATO 🇪🇺 🇩🇪 🇧🇪 🇱🇺 🇳🇱 🇹🇷 a další)
  - Národní partneři
  - Některé organizace v naší kostituency
- Open-source
- Používáme tento systém pro vnitřní použití
- **Téměř splňuje naše požadavky**
- **Nesplňoval požadavky pro KII**
- **Musíme systém upravit pro naše potřeby**


Initial event
Event with
contributed attributes
MISP
MISP
MISP
MISP
Threat Sharing

You are currently logged in as a site administrator and about to edit an event not belonging to your organisation. This goes against the sharing model of MISP. Use a normal user account for day to day work.

View Event
View Correlation Graph
View Event History

Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Populate from...
Enrich Event
Merge attributes from...
Propose Attribute
Propose Attachment

Publish Event
Publish (no email)
Publish event to ZMQ
Download as...

List Events
Add Event

laskowski-tech.com

Racoon Stealer

Event ID	780
UUID	5e5709a4-8850-453e-9f11-275a0a0a020f
Creator org	laskowski-tech.com
Owner org	Testovaci organizace
Email	admin@admin.test
Tags	keylogger/infostealer x racoon x tlp:white x
Date	2020-02-27
Threat Level	Low
Analysis	Initial
Distribution	All communities
Info	Racoon Stealer
Published	No
#Attributes	31 (4 Objects)
First recorded change	2020-02-27 00:14:02
Last change	2020-08-31 12:42:47
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Related Feeds

CIRCL OSINT Feed (1)

− Pivots | − Galaxy | + Event graph | + Event timeline | + Correlation graph | + ATT&CK matrix | − Attributes | − Discussion

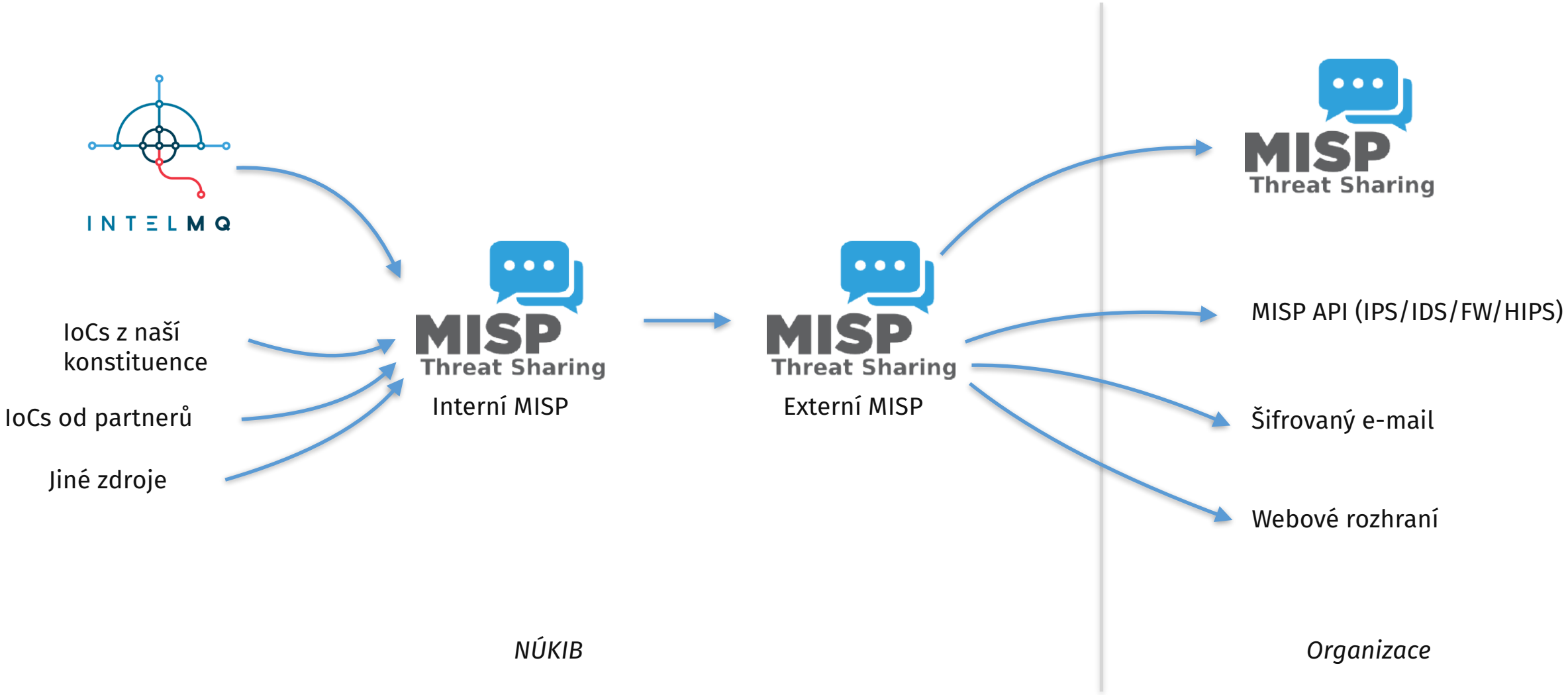
780: Racoon...

Galaxies

Attack Pattern

+ Spearphishing Attachment - T1193
+ PowerShell - T1086
+ Command-Line Interface - T1059
+ Commonly Used Port - T1043

Jak to bude fungovat



Jak se připravit?

- Pokud jste KII/VIS/PZS subjekt nebo dodavatel
  - Zjistit si, jak MISP funguje (https://www.misp-project.org)
  - Ověřit, zda vaše sonda/FW/IDS/IPS/SIEM podporuje standardní formáty a rozhraní pro import IOCs (STIX, STIX2 nebo MISP)
  - Při nákupu nových technologií vyžadovat podporu standardních formátů

  - V případě velkých organizací s bezpečnostním týmem si vyzkoušet vlastní instanci (https://www.misp-project.org/2019/09/25/hostev-vs-own-misp.html)

Jakub Onderka

Bezpečnostní analytik, GovCERT.CZ
Národní úřad pro kybernetickou a informační bezpečnost

E-mail: j.onderka@nukib.cz
PGP: 2EEF A5E6 CAB0 A87F 4531 1FC3 B158 F39D C523 01CD