MUNI
ICS

Vejdi a neútoč…

A když už chceš útočit, tak se odpoj!

Tomáš Plesník, CSIRT-MU

CESNET | Seminář bezpečnosti sítí a služeb

8. 3. 2022

Masarykova univerzita

- **Dvojka** na trhu VVŠ v ČR
- Celkem **10** fakult
  - PrF, LF, PřF, FF, PedF, FarmF, ESF, FI, FSS, FSPS
- Celkový počet zaměstnanců: **6 383** (3 363)
- Celkový počet studentů: **30 756** (19 275)
- Celkový počet uživatelů: **37 139** (22 638)
- Celkový počet komunikujících IP adres: **~30 000/denně**

Vývoj situace

- **Ve čtvrtek (dne 24. 2. 2022)** brzy ráno začíná invaze Ruské federace na Ukrajinu

Vývoj situace

- **Ve čtvrtek (dne 24. 2. 2022)** brzy ráno začíná invaze Ruské federace na Ukrajinu
- **Čtvrtek 11:55** masivní DDoS proti jedné IP na MUNI (volá málo kdy překvapený T. Košňar)
  - Zachyceno Cesnetem, přesměrováno pomocí BGP Flowspec do čističky (Scrubbing Center)
  - Cílem IP adresa v síti Eduroam, toho času přidělena zahraničnímu studentovi (Erasmus)
  - **Potvrzeno jako KB incident, nicméně nenalezena souvislost s děním na Ukrajině**

Vývoj situace

- **Ve čtvrtek (dne 24. 2. 2022)** brzy ráno začíná invaze Ruské federace na Ukrajinu
- **Čtvrtek 11:55** masivní DDoS proti jedné IP na MUNI (volá málo kdy překvapený T. Košňar)
  - Zachyceno Cesnetem, přesměrováno pomocí BGP Flowspec do čističky (Scrubbing Center)
  - Cílem IP adresa v síti Eduroam, toho času přidělena zahraničnímu studentovi (Erasmus)
  - **Potvrzeno jako KB incident, nicméně nenalezena souvislost s děním na Ukrajině**
- **Čtvrtek 12:07** začínají chodit desítky detekcí skenování interní sítě MUNI z VPN
  - Porty 137, 139 (NetBIOS), 389 (LDAP), 445 (SMB), 8003 (SCCM)
  - Analýzou odhalena příčina ve špatné konfiguraci jedné fakultní učebny (první hodina semestru v dané učebně)
  - **Nejednalo se o KB incident, ale provozní problém**

Vývoj situace

- **Ve čtvrtek (dne 24. 2. 2022)** brzy ráno začíná invaze Ruské federace na Ukrajinu
- **Čtvrtek 11:55** masivní DDoS proti jedné IP na MUNI (volá málo kdy překvapený T. Košňar)
  - Zachyceno Cesnetem, přesměrováno pomocí BGP Flowspec do čističky (Scrubbing Center)
  - Cílem IP adresa v síti Eduroam, toho času přidělena zahraničnímu studentovi (Erasmus)
  - **Potvrzeno jako KB incident, nicméně nenalezena souvislost s děním na Ukrajině**
- **Čtvrtek 12:07** začínají chodit desítky detekcí skenování interní sítě MUNI z VPN
  - Porty 137, 139 (NetBIOS), 389 (LDAP), 445 (SMB), 8003 (SCCM)
  - Analýzou odhalena příčina ve špatné konfiguraci jedné fakultní učebny (první hodina semestru v dané učebně)
  - **Nejednalo se o KB incident, ale provozní problém**
- **Aktivace krizového řízení na univerzitě, intenzivní monitorování situace**

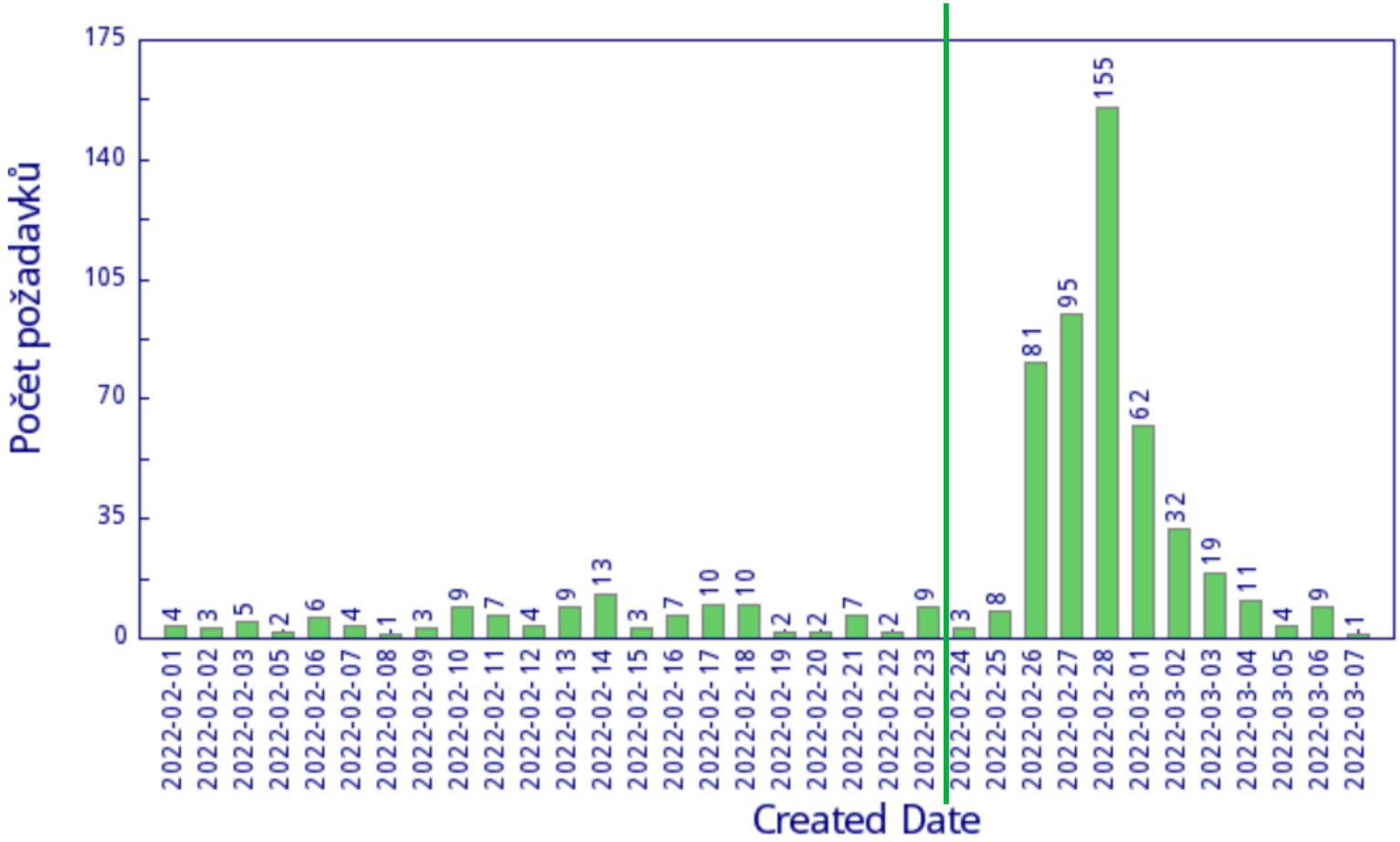
Vývoj situace

S příchodem víkendu se nám ale začíná rozmáhat takový nešvar...

Vedení: *„Odkud to přišlo?“*

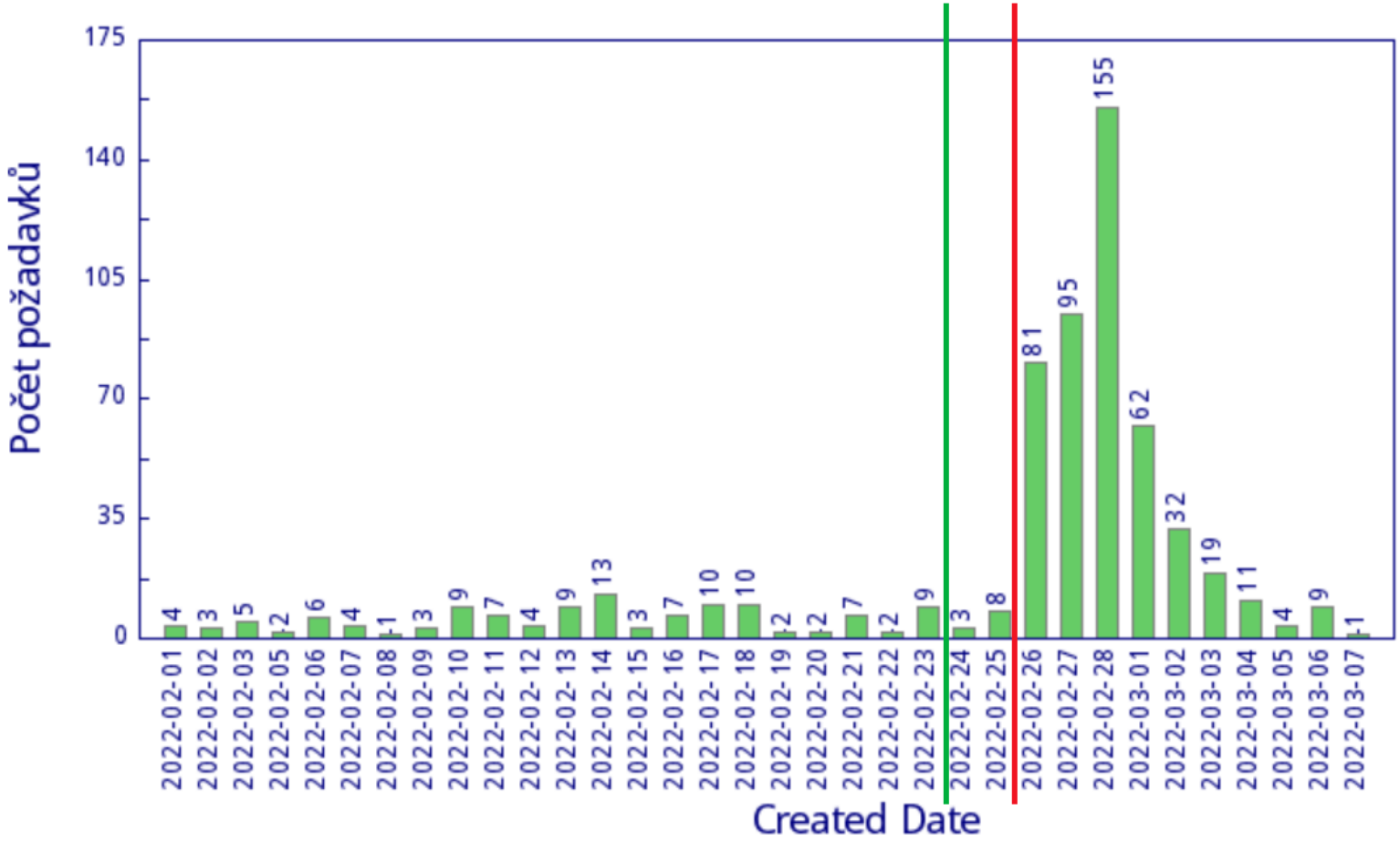
CSIRT-MU: *„Od nás to nemají…“*

Detekované události ze sítě MUNI



MUNI ICS

Detekované události ze sítě MUNI



CSIRT-MU:WHITE

MUNI ICS

Analýza incidentů

- Množství více jak **176 KB událostí přes víkend** odstartovalo hlubší analýzu

Analýza incidentů

- Množství více jak **176 KB událostí přes víkend** odstartovalo hlubší analýzu
- Aktivistické **komunitní DDoS útoky** proti Ruské federaci

Analýza incidentů

- Množství více jak **176 KB událostí přes víkend** odstartovalo hlubší analýzu
- Aktivistické **komunitní DDoS útoky** proti Ruské federaci
- **Akce uživatelů**
  - Připojení do sítě
  - Komunikace se sociálními sítěmi (hlavně Facebook)
  - Návštěva webu pro zprostředkování DDoS
  - Záplava dotazů na webové stránky ruských státních institucí, novin, bank či energetických společností

Analýza incidentů

- Množství více jak **176 KB událostí přes víkend** odstartovalo hlubší analýzu
- Aktivistické **komunitní DDoS útoky** proti Ruské federaci
- **Akce uživatelů**
  - Připojení do sítě
  - Komunikace se sociálními sítěmi (hlavně Facebook)
  - Návštěva webu pro zprostředkování DDoS
  - Záplava dotazů na webové stránky ruských státních institucí, novin, bank či energetických společností
- Od pondělí (28.2.) detekce **i z učeben** z vícero fakult

Analýza incidentů

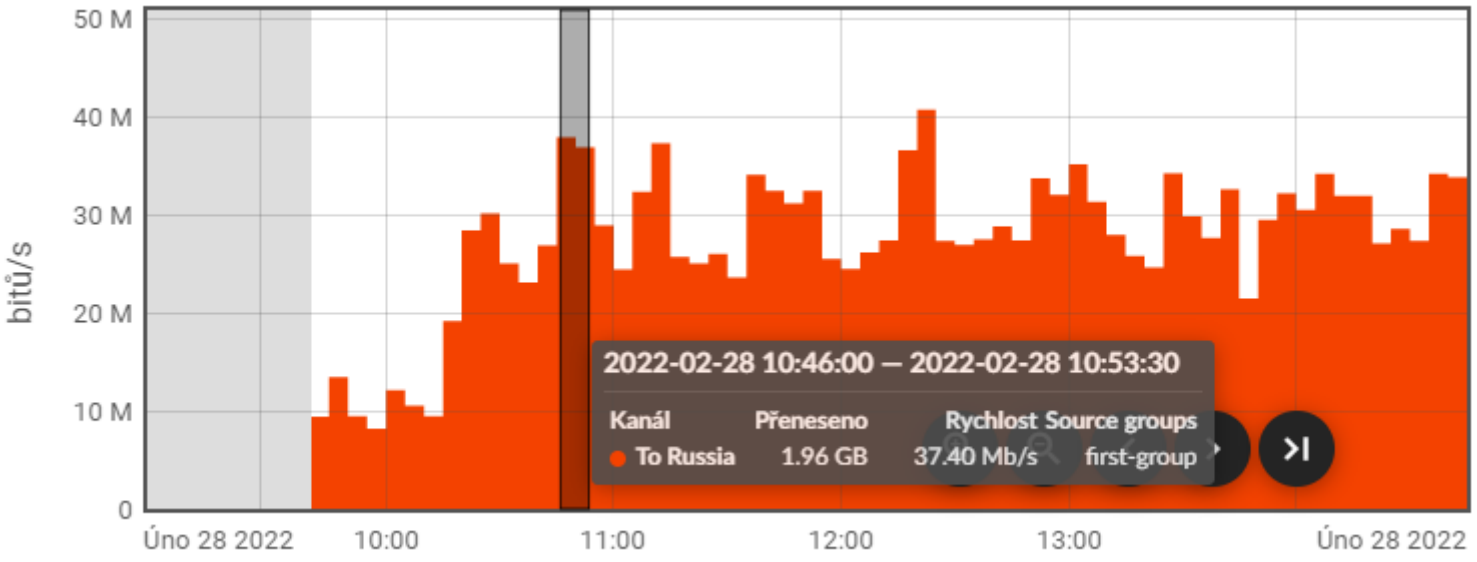
- Množství více jak **176 KB událostí přes víkend** odstartovalo hlubší analýzu
- Aktivistické **komunitní DDoS útoky** proti Ruské federaci
- **Akce uživatelů**
  - Připojení do sítě
  - Komunikace se sociálními sítěmi (hlavně Facebook)
  - Návštěva webu pro zprostředkování DDoS
  - Záplava dotazů na webové stránky ruských státních institucí, novin, bank či energetických společností
- Od pondělí (28.2.) detekce **i z učeben** z vícero fakult
- Celkově více než **450 detekcí od ~130 unikátních uživatelů**

Hlášení incidentů

- Detekce z MUNI jsou **dlouhodobě v manuálním režimu**
  - Ruční kontrola/analýza a odeslání, žádné blokace
- Prvotní vlna ihned nereportována koncovým uživatelům
  - **Informováno vedení univerzity**, čekáme na oficiální stanovisko
  - Obratem připraven **automatický systém hlášení pouze tohoto typu incidentu** (detekce s cílem útoku ze seznamu vytipovaných ruských IP)
  - Uživatele chceme upozornit na riziko, **nechceme je perzekuovat**

Zátěž pro síť MUNI

- Prakticky žádná
- Komunikace celé MUNI do Ruské federace v řádech desítek Mb/s

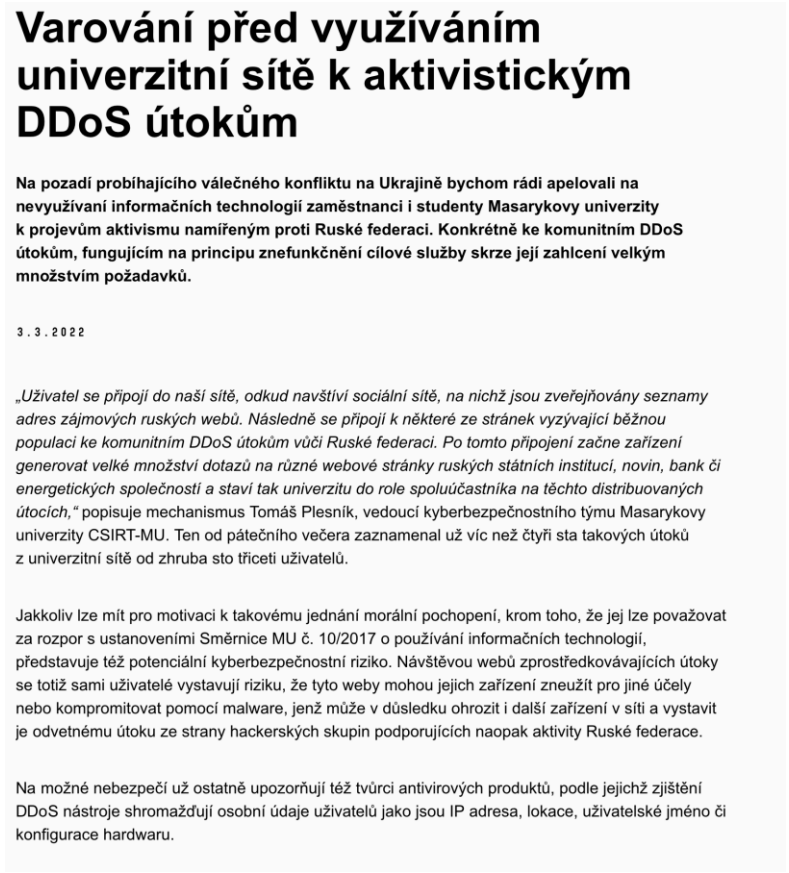


MUNI ICS

Možná rizika

- Upozornění slovenského vládního CERTu
  - https://www.sk-cert.sk/sk/upozornenie-na-podozrive-stranky-vykonavajuce-ddos-utoky/index.html
- Útočná stránka **nemusí být důvěryhodná**
  - Riziko dalšího zneužití zařízení uživatele i pro jiné než inzerované účely, nákazy zařízení, úniku dat
- Vědomé zapojení do DDoS útoků **může být protiprávní**
  - § 230 z. č. 40/2009 Sb. (???)
- Riziko **odvetných útoků** ze strany skupin podporujících ruský režim
  - https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/hackeri-skodi-na-ukrajine-cele-skupiny-se-pridavaji-na-stranu-ruska-40388627

Varování před zneužíváním univerzitní sítě



Varování před využíváním univerzitní sítě k aktivistickým DDoS útokům

Na pozadí probíhajícího válečného konfliktu na Ukrajině bychom rádi apelovali na nevyužívaní informačních technologií zaměstnanci i studenty Masarykovy univerzity k projevům aktivismu namířeným proti Ruské federaci. Konkrétně ke komunitním DDoS útokům, fungujícím na principu znefunkčnění cílové služby skrze její zahlcení velkým množstvím požadavků.

3.3.2022

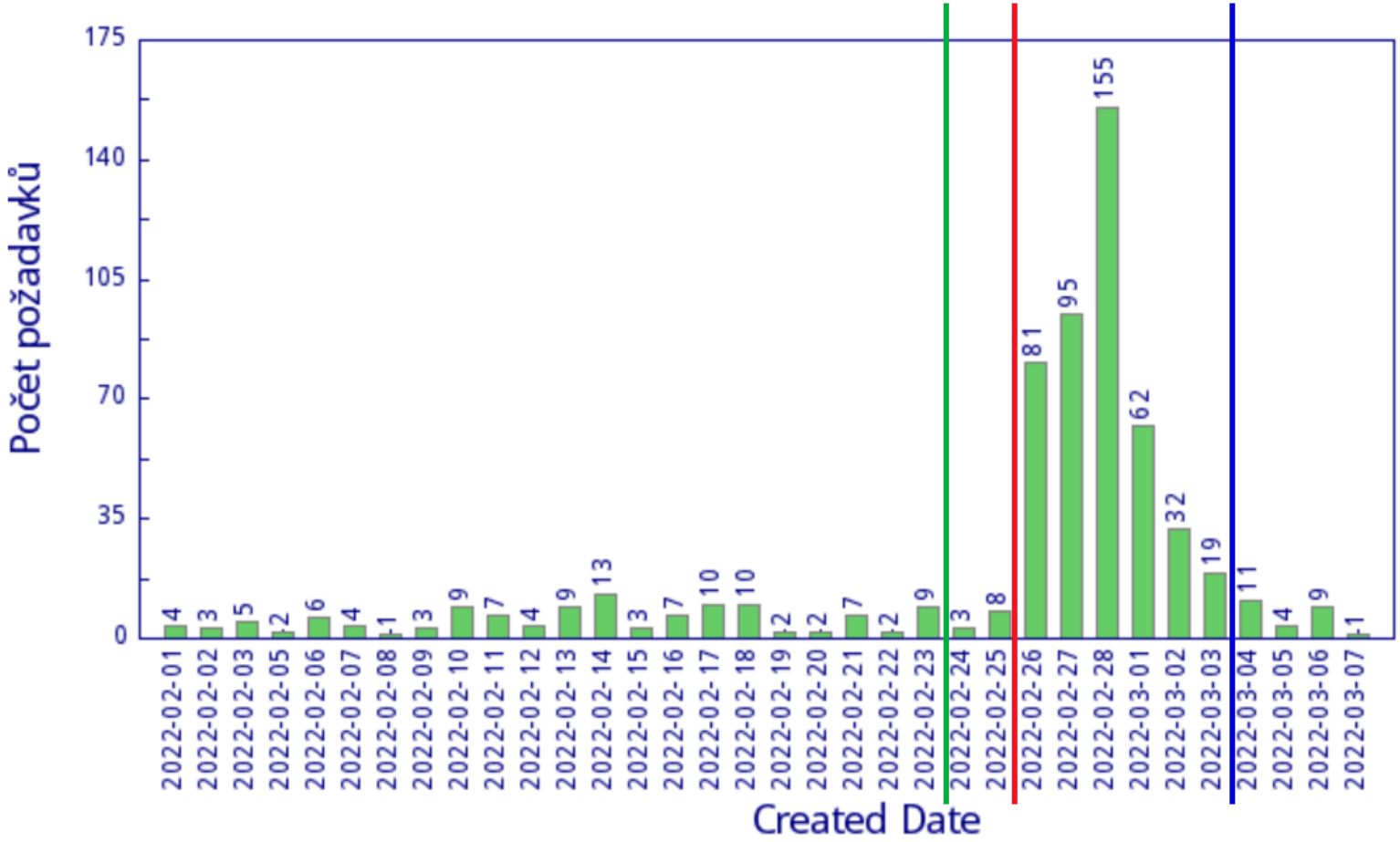
„Uživatel se připojí do naší sítě, odkud navštíví sociální sítě, na nichž jsou zveřejňovány seznamy adres zájmových ruských webů. Následně se připojí k některé ze stránek vyzývající běžnou populaci ke komunitním DDoS útokům vůči Ruské federaci. Po tomto připojení začne zařízení generovat velké množství dotazů na různé webové stránky ruských státních institucí, novin, bank či energetických společností a staví tak univerzitu do role spoluúčastníka na těchto distribuovaných útocích,“ popisuje mechanismus Tomáš Plesník, vedoucí kyberbezpečnostního týmu Masarykovy univerzity CSIRT-MU. Ten od pátečního večera zaznamenal už víc než čtyři sta takových útoků z univerzitní sítě od zhruba sto třiceti uživatelů.

Jakkoliv lze mít pro motivaci k takovému jednání morální pochopení, krom toho, že jej lze považovat za rozpor s ustanoveními Směrnice MU č. 10/2017 o používání informačních technologií, představuje též potenciální kyberbezpečnostní riziko. Návštěvou webů zprostředkovávajících útoky se totiž sami uživatelé vystavují riziku, že tyto weby mohou jejich zařízení zneužít pro jiné účely nebo kompromitovat pomocí malware, jenž může v důsledku ohrozit i další zařízení v síti a vystavit je odvetnému útoku ze strany hackerských skupin podporujících naopak aktivity Ruské federace.

Na možné nebezpečí už ostatně upozorňují též tvůrci antivirových produktů, podle jejichž zjištění DDoS nástroje shromažďují osobní údaje uživatelů jako jsou IP adresa, lokace, uživatelské jméno či konfigurace hardwaru.

- Varování vydáno 3. 3. 2022
- Vysvětlení postupu uživatelů
- Upozornění uživatelů na rizika
- Apel na nevyužívání IT MUNI
- Upozornění na porušení univerzitní směrnice

Detekované události ze sítě MUNI



MUNI ICS

Diskuze

§ 230 z. č. 40/2009 Sb.

MASARYKOVA
UNIVERZITA