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. dubna 2020

VAROVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/31, 616 00 Brno (dále jen „Úřad“), podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“), vydává toto

varování

před hrozbou v oblasti kybernetické bezpečnosti, spočívající v realizaci rozsáhlé kampaně závažných kybernetických útoků na informační a komunikační systémy v České republice, zejména pak na systémy zdravotnických zařízení. Tato kampaň může způsobit závažné dopady na dostupnost, důvěrnost či integritu informací u důležitých informačních a komunikačních systémů.

Realizaci této hrozby lze z informací dostupných Úřadu očekávat v nejbližších dnech, avšak v tuto chvíli disponuje Úřad indiciemi, že přípravná fáze těchto útoků již probíhá, a to zejména prostřednictvím spear-phishingové kampaně.

Národní úřad pro kybernetickou a informační bezpečnost tuto hrozbu hodnotí na úrovni Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná.

Úřad v souvislosti s touto hrozbou důrazně doporučuje provedení následujících úkonů:

- mimořádně upozornit uživatele o hrozbách spear-phishingu a připojit výzvu, aby se uživatelé, kteří v posledních dnech otevřeli podezřelé přílohy, obrátili na správce infrastruktury,
- upozornit uživatele na možnost „maskování“ spustitelných souborů v phishingu, např. „obrazek.png.exe“, „text.txt.exe“, „dokument.pdf.exe“ apod.,
- pokud je to možné, tak pomocí centrálního nastavení zabránit spouštění aktivního obsahu a maker, zejména v .doc a .docx dokumentech,
- okamžitě zablokovat vzdálené přístupy do infrastruktury a zablokovat otevřené služby do veřejné sítě, vyjma těch nezbytně nutných (veřejné IP rozsahy lze zkontrolovat v dostupných

vyhledávačích zařízení připojených do sítě a zjistit tak i historicky otevřené či zapomenuté porty, nebo služby dostupné z veřejné sítě),

- okamžitě vytvořit offline zálohy a postupovat v zálohování dle důležitosti dat v organizaci,
- zkontrolovat konzistenci již vytvořených záloh a okamžitě aktualizovat antivirové řešení v infrastruktuře.

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

File type: Win32 EXE

- MD5 7def1c942eea4c2024164cd5b7970ec8
- SHA-1 b2f4288577bf8f8f06a487b17163d74ebe46ab43
- SHA-256 c3f11936fe43d62982160a876cc000f906cb34bb589f4e76e54d0a5589b2fdb9

File type: Win32 EXE

- MD5 e6ccc960ae38768664e8cf40c74a9902
- SHA-1 d29cbc92744db7dc5bb8b7a8de6e3fa2c75b9dcd
- SHA-256 b780e24e14885c6ab836aae84747aa0d975017f5fc5b7f031d51c7469793eabe

File type: Win32 EXE

- MD5 b1349ca048b6b09f2b8224367fda4950
- SHA-1 44fac7dd4b9b1ccc61af4859c8104dd507e82e2d
- SHA-256 c46c3d2bea1e42b628d6988063d247918f3f8b69b5a1c376028a2a0cadd53986

File type: Win32 EXE

- MD5 0d7dbda706e0048aca27f133d4fc7c51
- SHA-1 1ed9dc8be0f925a5c23e6b516062744931697c78
- SHA-256 ac6b3f9e0848590e1b933182f1b206c00f24c3aa0aa6c62ca57682eff044d079

ODŮVODNĚNÍ

1. Na základě skutečností zjištěných při výkonu své působnosti, stejně tak jako na základě skutečností, které se Úřad dozvěděl od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, i tuzemských partnerů, dospěl Úřad k zjištění hrozby v oblasti kybernetické bezpečnosti, spojené s aktuální kampaní závažných kybernetických útoků na informační a komunikační systémy v České republice, která se zaměřuje na větší množství cílů v České republice, zejména pak na zdravotnická zařízení.

2. Úřad v rámci své činnosti podle § 22 písm. u) zákona o kybernetické bezpečnosti monitoruje a analyzuje hrozby a rizika v oblasti kybernetické bezpečnosti, zároveň v souladu s § 20 písm. b) a f) zákona o kybernetické bezpečnosti přijímá hlášení kybernetických bezpečnostních incidentů od povinných osob ze zákona o kybernetické bezpečnosti, stejně tak jako i od dalších osob, které nemají povinnosti podle zákona o kybernetické bezpečnosti, jakožto i od dalších partnerů. V rámci této činnosti získal Úřad indicie o tom, že přípravná fáze těchto útoků již probíhá, a to zejména pomocí spear-phishingové kampaně.

3. Úřad v současné době pozoruje zvýšené množství kybernetických útoků, jejichž dopady jsou zvláště nebezpečné v kontextu aktuální situace spojené s výskytem koronaviru (označovaného jako SARS CoV-2) na území České republiky, vyhlášeného nouzovému stavu a nezbytnosti zajistit fungování důležitých informačních a komunikačních systémů a jimi podporovaných služeb.

4. Tyto skutečnosti ve svém souhrnu vedou k důvodné obavě z hrozby realizace závažných kybernetických útoků na významné cíle v České republice, a proto Úřad podle § 12 odst. 1 zákona o kybernetické bezpečnosti vydává toto varování.

5. Pravomoc Úřadu je pro vydání tohoto varování dána ustanovením § 22 písm. b) zákona o kybernetické bezpečnosti, které jej zmocňuje k vydávání opatření. Podle § 11 odst. 2 zákona o kybernetické bezpečnosti patří mezi tato opatření i varování podle § 12 zákona o kybernetické bezpečnosti. Varování vydá Úřad podle § 12 odst. 1 zákona o kybernetické bezpečnosti, dozví-li se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti. V souladu s § 12 odst. 2 zákona o kybernetické bezpečnosti Úřad zveřejní varování na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3 zákona o kybernetické bezpečnosti.

6. Úkolem Úřadu je podle § 22 písm. j) zákona o kybernetické bezpečnosti zajišťovat prevenci v oblasti kybernetické bezpečnosti. Součástí této preventivní činnosti je také poskytování informací o zjištěných hrozbách v oblasti kybernetické bezpečnosti. Pokud však hrozba dosahuje takové intenzity, že informování o ní nelze pokrýt běžnými způsoby preventivní činnosti Úřadu, je v souladu s výše uvedeným Úřad nucen přistoupit k vydání varování podle § 12 zákona o kybernetické bezpečnosti.

7. Úřad upozorňuje, že orgány nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, jsou povinny toto varování zohlednit v rámci řízení rizik. Na základě výše uvedeného Úřad považuje hrozbu spojenou s kybernetickými útoky

zmíněnými ve výroku tohoto varování za pravděpodobnou až velmi pravděpodobnou. Orgány a osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, jsou proto povinny tuto hrozbu hodnotit na odpovídající úrovni, tedy na úrovni Vysoká.

Ing. Karel Řehka

Digitálně podepsal Ing. Karel Řehka
Datum: 2020.04.16 10:32:56 +02'00'

Ing. Karel Řehka
ředitel
Národní úřad pro kybernetickou a informační bezpečnost
elektronicky podepsáno