VYŠETŘOVÁNÍ KYBERNETICKÝCH ÚTOKŮ A KYBERNETICKÉ TRESTNÉ ČINNOSTI

RANSOMWARE

pplk. Lukáš Vilím

Sekce kybernetické kriminality

Národní centrála proti organizovanému zločinu SKPV

LEGISLATIVA

Trestní zákoník:

- § 230 **Neoprávněný přístup k počítačovému systému a nosiči informací**

Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

- Kdo získá přístup k počítačovému systému nebo k nosiči informací a
- v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
- v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.
- spáchá-li čin jako člen organizované skupiny,
- způsobí-li takovým činem značnou škodu,
- **způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,**
- získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo
- způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.
- způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu

LEGISLATIVA

- **§ 311 Teroristický útok**

✓Kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla,

✓písm e) vložením dat do počítačového systému nebo na nosič informací anebo vymazáním nebo jiným zničením, poškozením, změněním nebo potlačením dat uložených v počítačovém systému nebo na nosiči informací, snížením jejich kvality nebo učiněním jich neupotřebitelnými provede útok proti počítačovému systému, jehož narušení by mělo závažný dopad na fungování státu, zdraví osob, bezpečnost, hospodářství nebo zajištění základních životních potřeb obyvatel, útok s dopadem na větší počet počítačových systémů s využitím počítačového programu vytvořeného nebo přizpůsobeného pro takový útok anebo útok, kterým způsobí značnou škodu,

RANSOMWARE 2020

- Narůstá sofistikovanost útoků (SOCIÁLNÍ INŽENÝRSTVÍ)
- Cílené útoky na státní sektor (úřady ministerstva), veřejný sektor (společnosti, zdravotnictví - nemocnice, výzkumné instituty), ekonomický sektor (strojírenské a chemické závody),
- Získávání cenných informací, přístup do systému (e-špionáž)
- Přesměrování na jiné sektory– není možné predikovat vývoj (middle business companies)
- V souvislosti s pandemií SARS-CoV-2 byla zaznamenán nárůst šíření ransomwaru např. cestou malwaru, EC3 tento fenomén označuje za jednu z významných hrozeb.
- Cílem těchto útoků nebyly pouze lékařská zařízení (nemocnice) a akademické instituty (IZS, civilní sektor-zaměřeno více na společnosti, než na jednotlivce)

15 NEJVÝZNAMNĚJŠÍCH HROZEB 2020 (ENISA)

NOVÉ TRENDY:

Contains accounting documents, and accounts, plus a lot of important information that may be of value to competitors or interested parties. All files of actual information. Also in the archive you will get several databases that are no less interesting.

Archive in zip format
1. Files pdf,docx,xlsx - 22328
2. Database - 3

When the auction is over, you will be provided with a download link from the cloud with the following deletion.

Minimum deposit:	$5,000	**Top bet:**	--
Start price:	$50,000	**Blitz price:**	$100,000

Opened Time left: 6 days, 18 hours, 33 minutes and 12 seconds

A partial screenshot from the REvil ransomware group's Dark Web blog.

DOPORUČENÉ POSTUPY PŘI NAPADENÍ

• jako OČTŘ chápeme, že poškozená společnost potřebuje co nejdříve **obnovit provoz** a **obnovit co možná nejvíce dat,**

• infikované počítače okamžitě **odpojit od vnitřní sítě,** pokud to situace umožňuje (např. nejedná-li se o servery, ke kterým jde přistupovat pouze vzdáleně) a vypnout je (v ranní fázi je možné, že se podaří zabránit tomu, aby byla zašifrována veškerá data)

Nastavení kvalitní spolupráce je zásadní – sdílení DAT

•nejenom policie, ale také další subjekty (NUKIB, externí společnost pro analýzu incidentu apod.), které mohou být přizvány ke spolupráci budou potřebovat obdobná data jako OČTŘ.

DATA A JEJICH DŮLEŽITOST PRO OČTŘ

- síťová komunikace (netflow) za období, kdy je předpoklad, že došlo ke kompromitování vnitřní sítě (málokdo má k dispozici)
- záznamy jakékoliv logování činnosti na infikovaných zařízeních
- bitová kopie disků (minimálně systémového, kde mohou být důležité informace v systémových registrech či přímo soubor s aktivním malwarem)
- je téměř jedno o jaký formát se jedná (zda je to nekomprimovaný image *.img, *.dd, *.qcow2 či přímo forensní EWF s příponami *.E01)

DATA

◦ důležité je, aby byla **offline** (nikoliv na spuštěném systému) **bitová kopie disku** pořízena co nejdříve a určitě předtím, než se do souboje s malwarem pustí nějaký antivirový systém (který odstraní většinu zájmových dat ve snaze vyléčit počítač)

◦ ke každé bitové kopii si připravit **stručný popis toho, co bitová kopie obsahuje** a **k čemu systém sloužil** (operační systém a verzi, zda byl pravidelně aktualizován, informace o použitém antiviru, co bylo doposud zjištěno atd.)

• zamyslet se nad vektorem útoku – jakým způsobem mohlo dojít k napadení (dnes nejčastěji otevřením zavirované přílohy či škodlivého odkazu); **zúčastnění většinou nechtějí přiznat svou chybu**, ovšem zjištění vektoru útoku

RANSOMWARE - PHOBOS

RANSOMWARE - PHOBOS

- k infekci dochází téměř vždy **prostřednictvím e-mailu** se škodlivým odkazem / přílohou

- po kompromitaci systému (oběť otevře odkaz/přílohu e-mailu) se na pozadí začne provádět násobné šifrování dat

- u zašifrovaných dat je ve složkách přítomen textový soubor s informací na jaké BTC adresy a v jaké výši převést bitcoiny (po určité době se částka může i zvyšovat) - pachatelé využívají anonymizačních služeb (firemail.cc, tutanota.com, protonmail.com a další) na které často přistupují prostřednictvím druhotné anonymizace (např. použitím TORu)

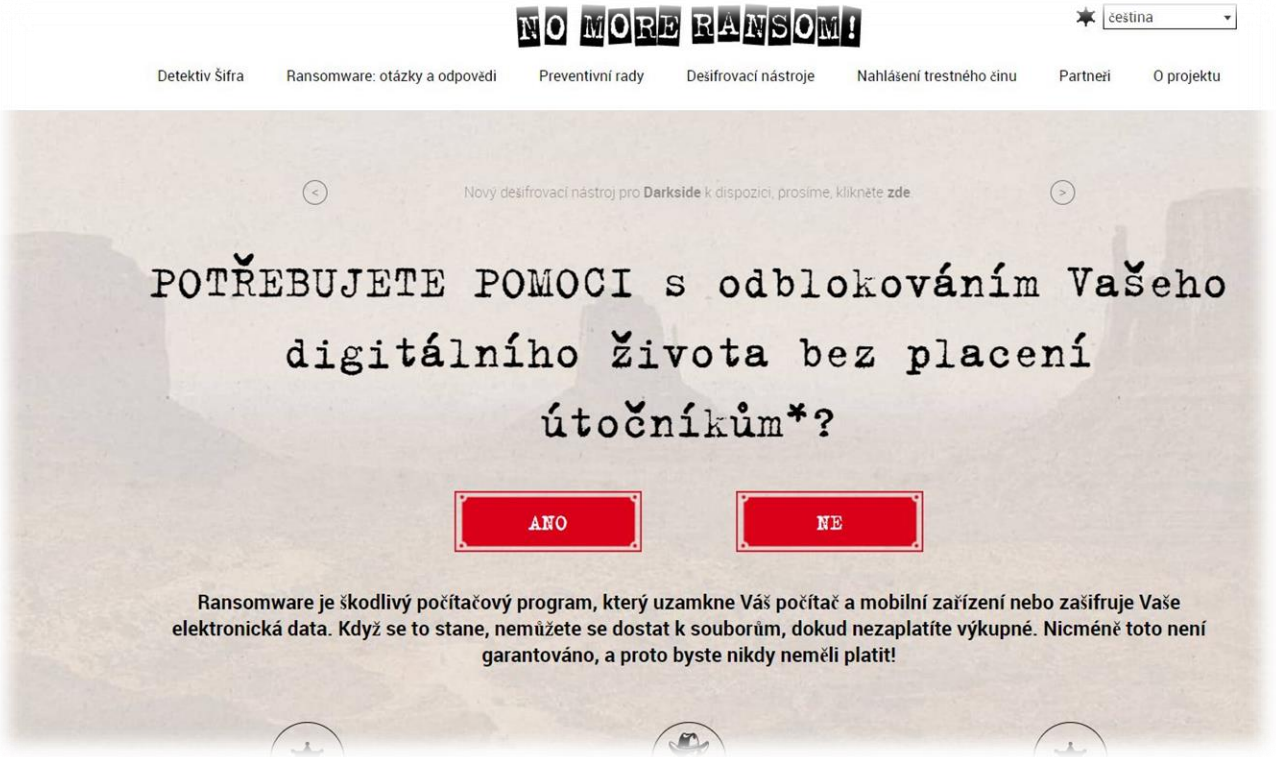
RANSOMWARE – PHOBOS – OPĚTOVNÝ ÚTOK

- pokud se oběť rozhodne zaplatit, obdrží zpravidla dešifrovací klíče (ale ze zahraničí jsou známy i případy kde k dešifrování dat nedošlo)
- nezřídka kdy se stávají případy, kdy oběť zaplatí a získá pocit, že si "alespoň koupila zpět svá data" a dále nevěnuje počítači pozornost -> může dojít k opětovnému zašifrování vlivem z důvodu nevěnování pozornosti (daný systém by pro jistotu měl být vždy opětovně nainstalován na zformátovaný disk)

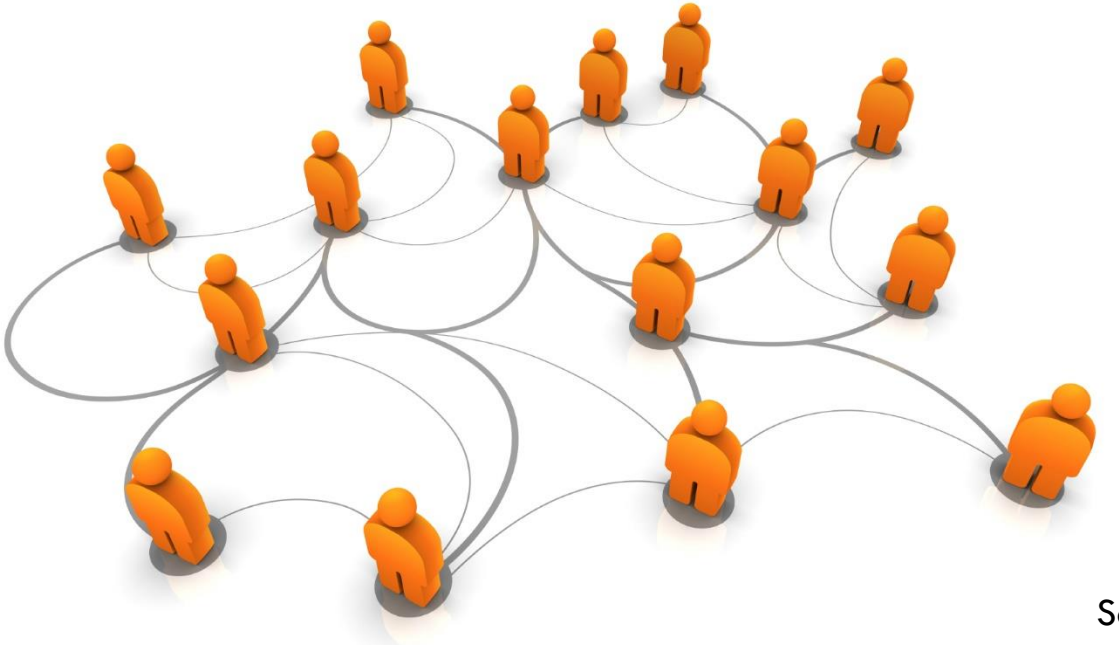
RANSOMWARE - PHOBOS

- v ČR bylo v minulém roce oznámeno okolo 10 případů infekce ransomwarem Phobos, kdy se většinou jedná o společnosti střední velikosti (pachatel zřejmě předpokládá nejvyšší šanci, že oběť zaplatí)
- žádný z případů neskončil úspěšným odhalením pachatelů
- situace ve světě je velice obdobná; když už se někdo dostane k nějakým identitám (většinou trasováním krypto adres a následným dotazem na směnárny) tak skončí tím, že dalším nutným krokem je spolupráce s východním blokem, který není příliš vstřícný ve své spolupráci

WWW.NOMORERANSOM.ORG



DĚKUJI ZA POZORNOST



pplk. Lukáš Vilím

Sekce kybernetické kriminality