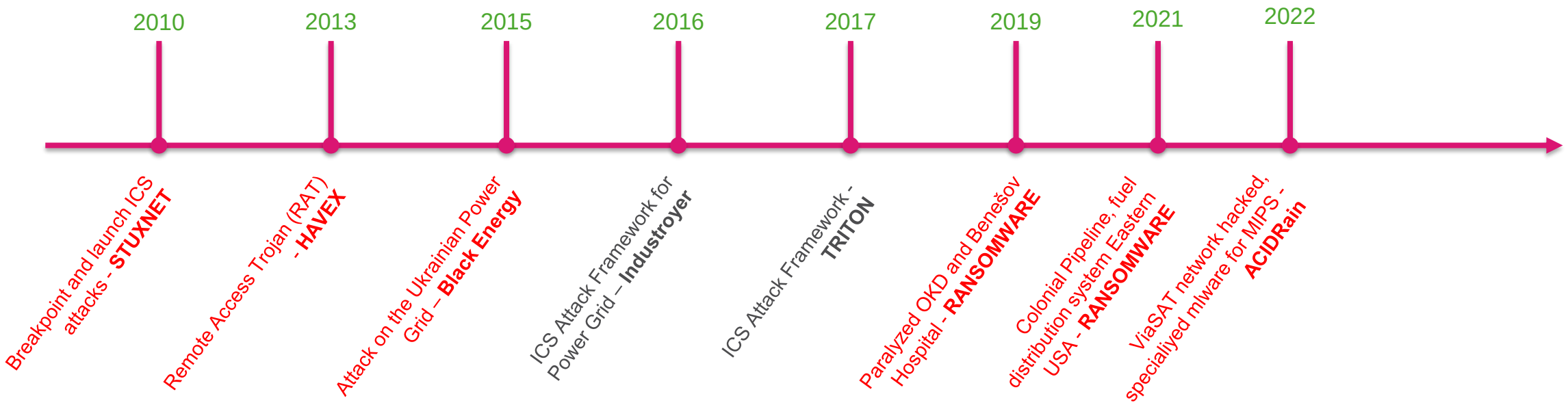
BEZPEČNOSTNÍ RIZIKA PRO PRŮMYSLOVÉ SYSTÉMY: PŘÍPADOVÁ STUDIE

Petr Kadrmas | Security Engineer
pkadrmas@checkpoint.com

YOU DESERVE THE BEST SECURITY

Případy napadení kritické infrastruktury

Historie známých útoků na ICS infrastrukturu



Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure

Attacker can reprogram the SIS to allow an unsafe state

SIS = Safety Instrumented System controllers

Útoky na ukrajinskou energetickou soustavu: 2015

- Dne 23. prosince 2015 hackeři vzdáleně narušili informační systémy tří energetických distribučních společností na Ukrajině a dočasně přerušili dodávky elektřiny spotřebitelům. 30 rozvoden bylo vypnuto a asi 230 000 lidí bylo bez proudu po dobu 1 až 6 hodin.
- Ruská APT skupina „Sandworm“
- Komplexní útok využil následující techniky:
  - 6 měsíců před útokem kompromitace podnikových sítí distribučních společností pomocí spear-phishingových e-mailů s malwarem **BlackEnergy**.
  - Postupné získání přihlašovacích údajů a přístupu k ovládání SCADA systémů
  - dálkové vypnutí rozvoden
  - deaktivace/zničení komponent IT infrastruktury (znemožnění dálkového ovládání rozvoden)
  - zničení souborů uložených na serverech a pracovních stanicích s malwarem KillDisk
  - Rušení telefonních linek společností
  - Denial-of-service útok na call-centrum s cílem odepřít spotřebitelům aktuální informace o výpadku
  - Vypnutí nouzového napájení na operačním středisku energetické společnosti

Black Energy Malware

- Robustní a modulární malware s technikami ochrany proti detekci anti-malwarem:
  - spouštění lokálních souborů
  - stahování a spouštění vzdálených souborů
  - aktualizace a instalace pluginů pomocí CaC
  - Vykonávání příkazů „dye“ a „distroy“
- Black Energy 3, použitý pro útok na ukraině disponuje následujícími moduly:
  - fs.dll — File system operations, si.dll — System information, “BlackEnergy Lite”
  - jn.dll — Parasitic infector, ki.dll — **Keystroke Logging**
  - ps.dll — **Password stealer**, ss.dll — **Screenshots**
  - vs.dll — **Network discovery**, **remote execution**
  - tv.dll — Team viewer, rd.dll — Simple pseudo “**remote desktop**”
  - up.dll — Update malware, dc.dll — List Windows accounts
  - bs.dll — Query system hardware, BIOS, and Windows info
  - dstr.dll — **Destroy system**, scan.dll — **Network scan**

Útoky na ukrajinskou energetickou soustavu: 2016

- Útok ze 17. prosince 2016. Těsně před půlnocí došlo k útoku, který na jednu hodinu odpojil pětinu hlavního města Kyjeva od proudu a byl považován za test kybernetického útoku. Útok byl proveden pomocí malwaru **Industroyer** (také Crashoverride).
- Industroyer je vůbec první známý malware speciálně navržený k útoku na elektrické rozvodné sítě. Zároveň je to po Stuxnetu, Havexu a BlackEnergy čtvrtý malware, který byl veřejně odhalen a zaměřuje se na průmyslové řídicí systémy.
- Analýza kroků útoku naznačuje, že cílem bylo výrazně větší narušení rozvodné sítě s možným dopadem na lidské životy:
  - Útočníci nejprve otevřeli všechny jističe přenosové stanice, což vyvolalo výpadek proudu.
  - Později spustili wiper, který vyřadil počítače rozvodné stanice a zabránil tak zaměstnancům dálkově sledovat systémy stanice.
  - Následně útočníci použili útok na zranitelnost ochranných relé Siprotec, který by deaktivoval funkci těchto zařízení. Záměrem bylo způsobit fyzické poškození transformátorů nebo sítě při následném manuálním zapnutí. Tento krok naštěstí selhal (pravděpodobně chybou útočníků)

Industroyer

- Hlavní backdoor se používá k ovládání všech ostatních součástí malwaru. C&C komunikace.
- Další backdoor poskytuje perzistenci
- Spouštěcí komponenta je samostatný spustitelný soubor odpovědný za spouštění payload komponent a komponent mazání dat. Spouštěcí komponenta obsahovala specifický čas a datum aktivace; analyzované vzorky obsahovaly dvě data: 17.12.2016 a 20.12.2016).
- Čtyři komponenty payloadu se zaměřují na konkrétní průmyslové komunikační protokoly IEC 60870-5-101, IEC 60870-5-104, IEC 61850 a OLE pro Process Control Data Access (OPC Data Access). Funkce komponent payloadu zahrnují mapování sítě a následné vydávání příkazů konkrétním průmyslovým řídícím zařízením.
- Komponenta pro mazání dat je navržena tak, aby vymazala klíčové registry systému a přepsala soubory, aby nebylo možné systém spustit.

- POZN: Další útoky byly zaznamenány po napadení Ukrajiny. V dubnu 2022 pokus vyřadit energetickou soustavu pomocí Malwaru Industroyer2.

Triton (12/2017)

- V srpnu 2017 byl malware použit při útoku na Rafinérii v Saudské Arábii.
- Malware Triton infikoval řídící počítač připojený k SIS (Safety instrumented systems) systému Triconex Schneider Electric a následně se ho snažil přeprogramovat tak aby systém neidentifikovat nebezpečné stavy. (zero day zranitelnost)
- Některé řídící jednotky při útoku vstoupily do nouzového režimu, když se je hackeři pokusili přeprogramovat, což způsobilo zastavení souvisejících procesů a umožnilo zaznamenat útok.
- V prosinci 2017 byl detekován útok na Triconex od Schnider Electric v jedné z elektráren v Saudské Arábii.
- Triton představuje významný posun v kybernetických útocích na ICS. Jako první byl navržený tak, aby umožnil fyzické poškození, dopad na životní prostředí a případné ztráty na životech.
- Malware Triton představuje stále vysoké riziko pro ICS infrastruktury. FBI vydalo varování v březnu 2022.

Colonial Pipeline (05/2021)

- 8 851 km potrubí, pokrývá 45 % dodávek plynu na východní pobřeží USA (denně přepraví 2.5 M barelů)
- Vstupem do sítě byl jeden kompromitovaný, již dlouho nepoužívaný VPN účet bez mutlifaktor autentikace. Vstup do sítě nastal 29.4.
- Infekce ransomwarem identifikovaná 6.5. vedla k exfiltraci 100 GB dat a zašifrování infrastruktury. Útok připisován skupině Darkside
- Proaktivní odstavení OT infrastruktury po zjištění Ransom notifikace.
- Zaplaceno cca 4.4M dolarů jako výkupné (75 BTC, zhruba 2.3M se podařilo získat zpět).
- Útok zapříčinil nedostatek paliva, zvýšení cen, mnoho čerpacích stanic bylo bez pohonných hmot. Obnovení provozu nastalo 12.5. (více než 10t stanic stále bez paliva ještě 18.5.)

Ropné Terminály Německo, Belgie a Nizozemí (02/2022)

- Evropské společností zabývajících se přepravou a skladováním ropy napadeny kybernetickými útoky.
- IT systémy byly přerušeny v ropných terminálech Oiltanking v Německu, SEA-Invest v Belgii a Evos v Nizozemsku.
- Ransomware útok připisován APT skupině BlackCat.
- Sofistikovaný Ransomware as a service který dokáže postihnout specifické systémy.
- Programovaný v jazyce RUST, umožňuje široké pokrytí OS na kterých lze malware spustit.

ViaSAT network hack, tisíce větrných turbín v Německu bez dohledu (05/2022)

- Masivní výpadek satelitního internetu Viasat ve střední a východní Evropě byl zapřičiněn malwarem schopným vymazat data z modemů a routerů.
- Malware, nazvaný AcidRain, je unixový spustitelný program navržený tak, aby cílil na zařízení postavená na architektuře MIPS.
- Útok souvisí s válkou vedenou proti Ukrajině. Dle prohlášení ViaSAT problémy nastaly po útoku na Ukrajinu.
- Jako vedlejší efekt nefunkční sítě ViaSAT došlo k nedostupnosti vzdáleného ovládání tisícú větrných turbín v Německu (reportováno až 5800 turbín s výkonem 11 GW). Turbíny dále v režimu „auto-pilot“ a byly nadále připojené do sítě, ale vzdálené připojení bylo nefunkční.

Jak se bránit proti moderním hrozbám (IT)

Taktiky a techniky útočníků

- Průzkum:
  - Získání kompromitovaných přihlašovacích údajů
  - Využití infrastruktury pro navázání důvěryhodné komunikace (podobné domény, kompromitované emailové účty, účty sociálních sítí)
- Přístup:
  - Externí remote servis (VPN)
  - Spear Phishing
  - Drive-by download
  - Zneužití zranitelností veřejně přístupných systémů
  - Zneužití kompromitovaných admin účtů
  - Replikace s použitím externího média
  - Supply Chain kompromitace

Bezpečnostní technologie

- Síťový provoz
  - Ochrana Perimetru, segmentace
  - IPS, Ochrana proti malwaru
  - Detekce neznámých variant hrozeb
  - Detekce a blokování post-infekční komunikace
  - Detekce anomálií
- Koncové stanice
  - Antimalware, Sandboxing
  - Detekce Phishingu
  - Behavirální detekce
  - Ochrana proti Ransomwaru, automatizované obnovení
  - Automatizovaná náprava incidentu
  - Forenzní analýza/Threat Hunting

THANK YOU

YOU DESERVE THE BEST SECURITY