cesnet

Hugo (aneb sdílejte data)

Pavel Valach
CESNET-CERTS

únor 2024
Praha

cesnet

HONEYPOTY

- **Zachytáváme nezvané hosty.**
- **Umístíme návnadu (např. otevřené SSH či SQL) na strategickou pozici v síti.**
  - A pak čekáme.

- **Každé připojení je platná událost.**
  - Kdo se pokouší připojit?
  - Omyl, nebo záměr?
  - Pokusy o prolomení hesla? Jaké údaje použili?
  - O co se pokusí, jakmile dostanou přístup?

Dionaea Muscipula – Mucrow (CC-BY-SA 3.0)

Pavel Valach, CESNET-CERTS

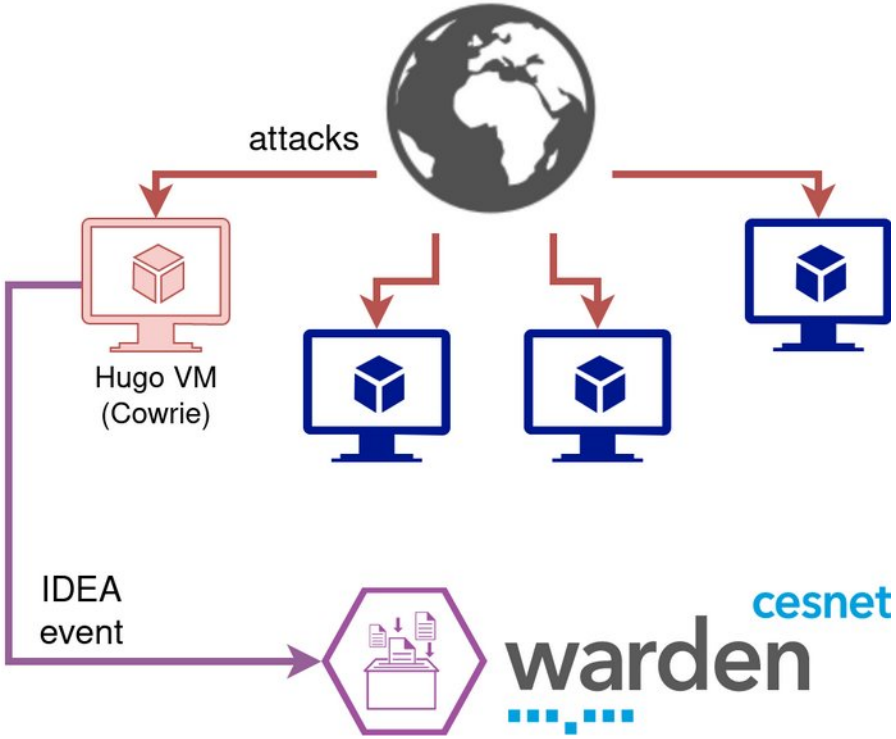
UŽITEČNÉ INFO Z HONEYPOTŮ

- Zdrojové IP adresy
- Použité přihlašovací údaje
- Příkazy
- Stažený malware a jeho URL,
- atp. atp.

→ ochrana sítě (blocklist známých zdrojů útoku)
→ zdroj pro reputační databáze (např. NERD.cesnet.cz)
→ korelace dat v rámci výzkumných činností
→ detekce škodítek ve vlastní síti

Pavel Valach, CESNET-CERTS

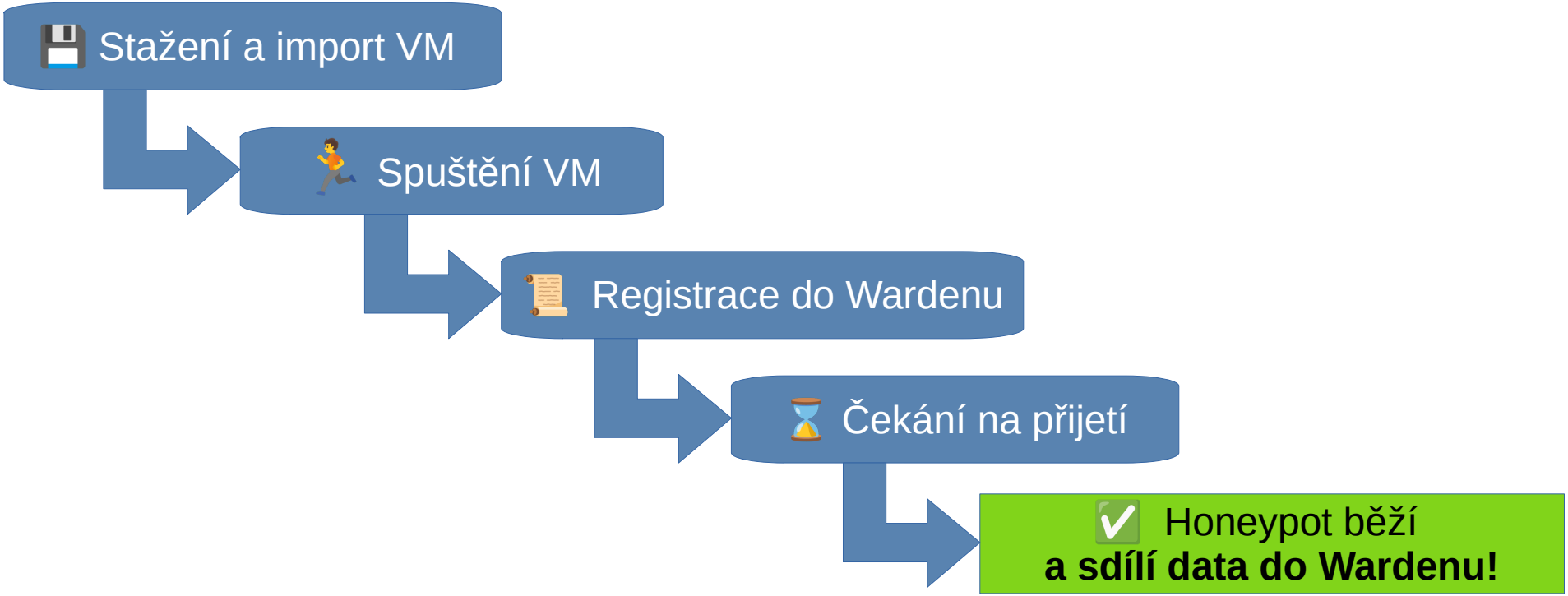
CÍLE HUGO



- **Samočinný sběr dat o útocích ze zapojených organizací**
  - Datový zdroj pro Warden
  - Každá událost je platná
- **Cíl: co nejjednodušší start**
  - Import VM & nastavit & spustit
- **Zatím v omezeném testovacím provozu**

Pavel Valach, CESNET-CERTS

IDEÁLNÍ PŘÍPAD REGISTRACE



COWRIE, DIONAEA

Cowrie

- SSH, Telnet
- Fiktivní "Debian" – některé unixové příkazy fungují (ping, wget), jiné částečně (ifconfig, dmesg), další předstírají (apt-get)
- **Nahrávky útoku, stažené soubory, jejich URL**

Cypraea caputserpentis – NOAA (Public domain)

Dionaea

- SMB, MSSQL, (T)FTP, MySQL, HTTP(S), SIP
- Emulace shellcode (libemu)
- Emulace cmd.exe (bind/connectback)
- P0f, Pcap – **pasivní fingerprinting útočníkova systému**
- **Nahrávky útoku, stažené soubory, jejich případné zdroje**

Dionaea Muscipula – Mucrow (CC-BY-SA 3.0)

cesnet

POMOZTE NÁM

Máte zajímavý zdroj dat? **Podělte se a přispějte komunitě!**

https://warden.cesnet.cz/

warden-info @ cesnet.cz

únor 2024

Pavel Valach, CESNET-CERTS

cesnet

DĚKUJI ZA POZORNOST
DOTAZY?

pavel.valach @ cesnet.cz