5 tipů, jak chránit svojí organizaci i bez vlastního SOC

Filip Marvan

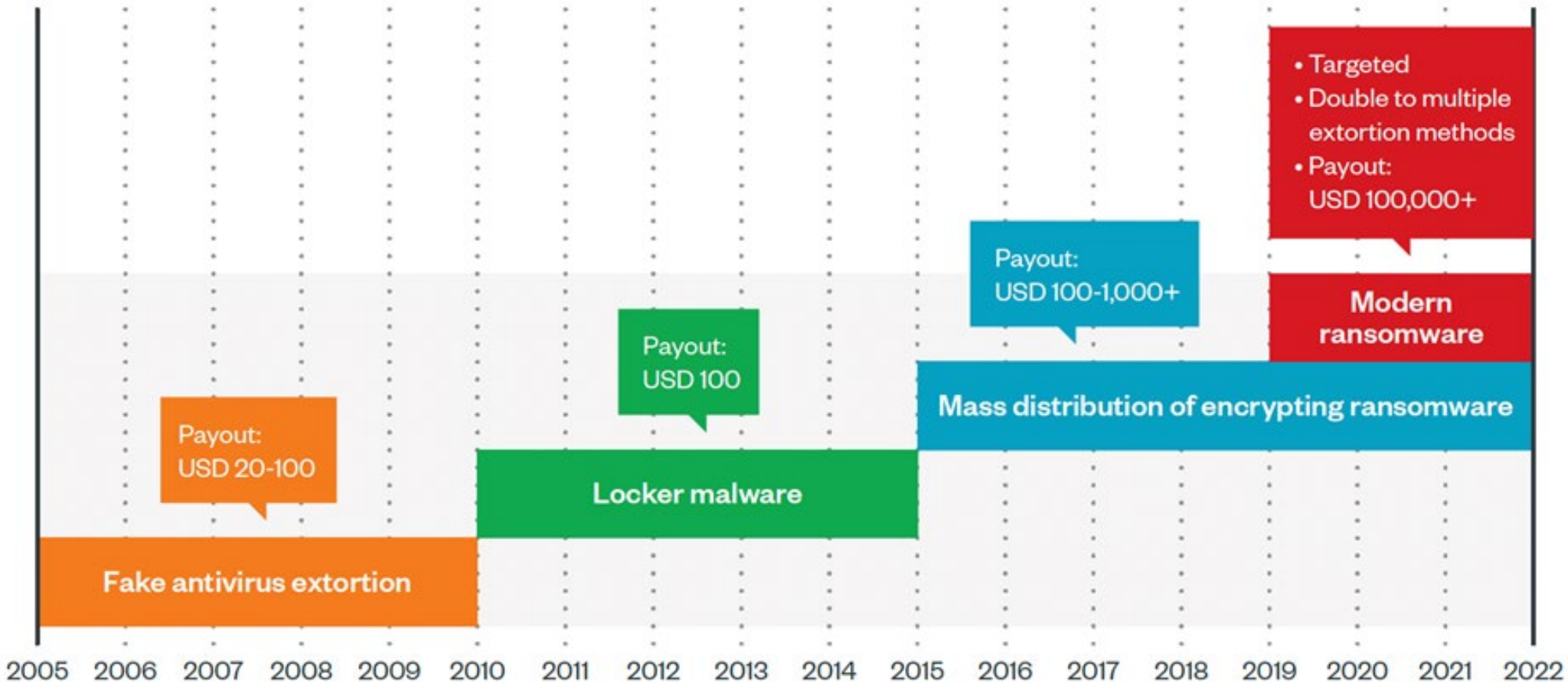
Obsah

- Aktuální hrozby a trendy
- Útočníci a jejich přístup k AI/ML
- Co čekat v budoucnu v oblasti kyberbezpečnosti
- Pět tipů na ochranu proti současným hrozbám

Aktuální hrozby

Vývoj Ransomware, profesionalizace, nové cíle útoků

Vývoj Ransomware

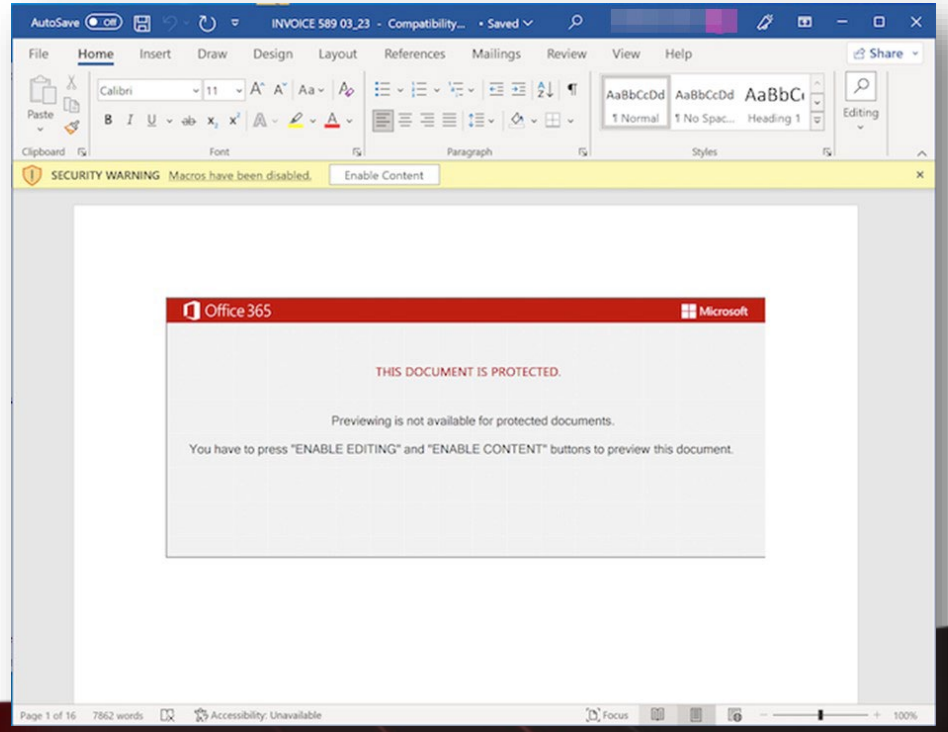


Aktuální trendy

- Roste počet útoků na Linux, IOT, NAS, routery, hypervizory
- Automatizace útoků, především fáze Initial access a lateral movement
- Státem podporované kybernetické útoky maskující se za Ransomware
- Hledání a zneužívání nových zranitelností
- Profesionalizace, vyhlášen bug bounty na ransomware platformu (LockBit)
- V současné době monitorujeme 32 Ransomware aaS skupin. Nejaktivnější: LockBit, BlackCat a Royal

Zajímavé útoky a techniky z roku 2022

- Supply-chain útoky na cloud infrastrukturu, jako například modul ctx (python) nebo phpass (php).
- Útoky na závažné zranitelnosti na VPN branách
- Velmi kvalitní útoky na uživatele
- Útoky na OT infrastrukturu



Hrozby které přináší AI/ML

Zajímavé směry zneužití ML technologie, nejzajímavější PoC

Příklady z minulosti zneužívající ML

- Využití ML pro generování e-mailu, který projde filteringem (2015)
- Analýza dat pro využití útoků Business Email Compromise (2017 Black Hat USA)
- Využití ML pro analýzu detekčních schopností libovolného antimalware a na základě výsledků vytvoření nedetekovaného malware (2017 Black Hat USA, AVPASS, 0% detekcí VirusTotal z 5000 vytvořených vzorků).

Příběh DeepLocker & DeepExploit

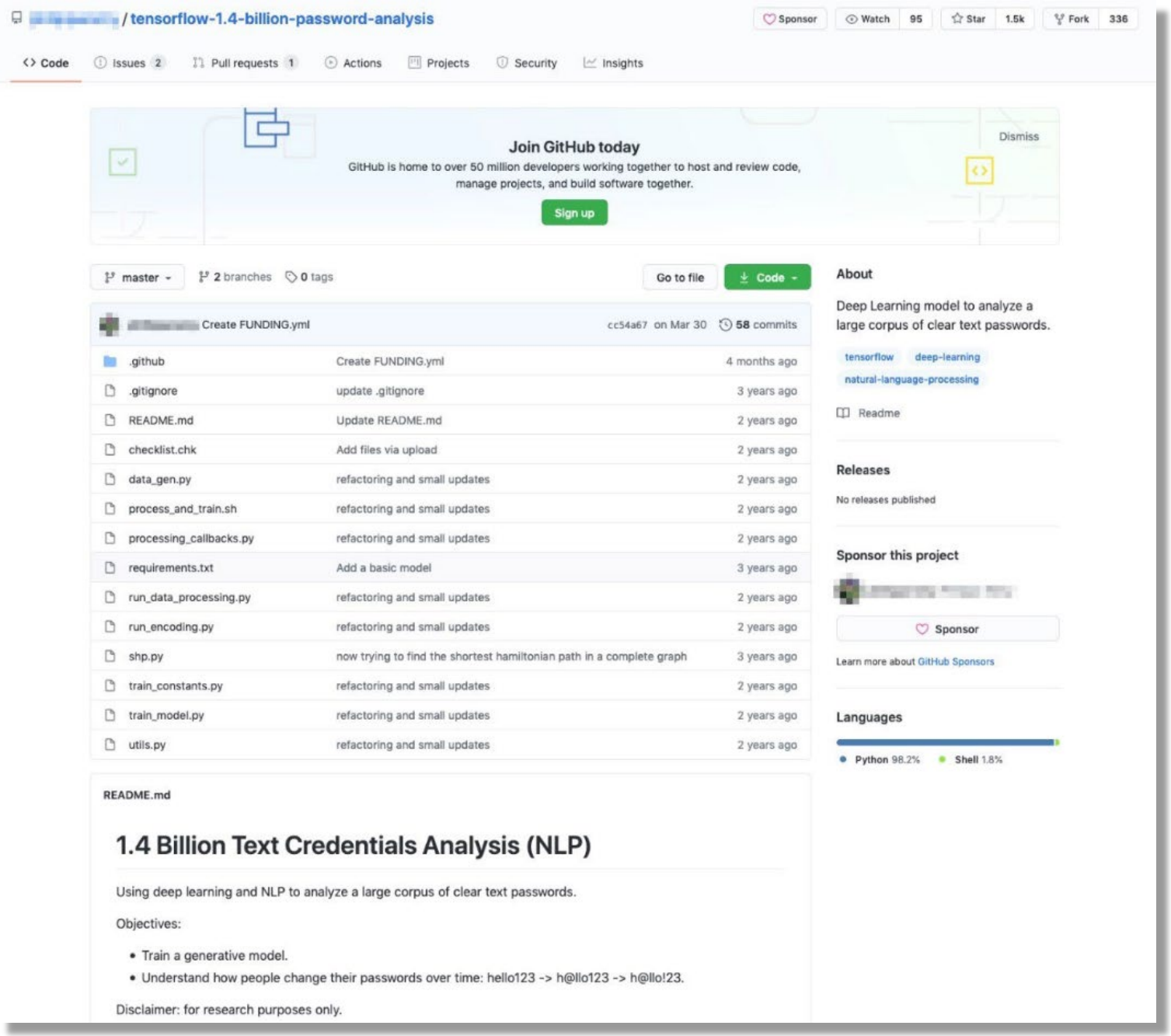
- DeepLocker PoC Malware využívající AI přímo v rámci svého kódu
- Používá DNN (Distributed Neural Network) k určení, zda se nachází na cílovém zařízení a následně dešifruje vlastní kód a obchází prevenční systémy
- DeepExploit využívá ML k automatizaci penetračních testů a automatickém nasazení vhodného exploitu na základě detekovaného prostředí (s využitím Metasploitu)

Aktivní malware obsahující ML model?

- Vytvořili jsme YARA rule na TensorFlow, RapidMiner, PyTorch (open-source ML modely)
- Prohledali jsme celou databázi vzorků nahraných na VirusTotal a hledali alespoň 2+ detekce
- Analýza spojení známých a detekovaných vzorků Trend Micro, zda se spojují na nějakou cloud službu poskytující ML
- Ze stávajících výsledků zatím vyplývá, že využití ML v rámci kódu samotného malware je zatím ve velmi ranné fázi

Využití Machine Learning při útocích na hesla

- Využití ML modelů pro analýzu uniklých hesel ke zpřesnění slovníků
- Generování vzorců, podle kterých si uživatelé vytvářejí hesla
- Například PassGAN systém
  - o 50-70% úspěšnější než HashCat


/ tensorflow-1.4-billion-password-analysis
Sponsor
Watch 95
Star 1.5k
Fork 336
Code
Issues 2
Pull requests 1
Actions
Projects
Security
Insights
Join GitHub today
GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.
Sign up
Dismiss
master
2 branches
0 tags
Go to file
Code
Create FUNDING.yml
cc54a67 on Mar 30
58 commits
.github Create FUNDING.yml 4 months ago
.gitignore update .gitignore 3 years ago
README.md Update README.md 2 years ago
checklist.chk Add files via upload 2 years ago
data_gen.py refactoring and small updates 2 years ago
process_and_train.sh refactoring and small updates 2 years ago
processing_callbacks.py refactoring and small updates 2 years ago
requirements.txt Add a basic model 3 years ago
run_data_processing.py refactoring and small updates 2 years ago
run_encoding.py refactoring and small updates 2 years ago
shp.py now trying to find the shortest hamiltonian path in a complete graph 3 years ago
train_constants.py refactoring and small updates 2 years ago
train_model.py refactoring and small updates 2 years ago
utils.py refactoring and small updates 2 years ago
About
Deep Learning model to analyze a large corpus of clear text passwords.
tensorflow
deep-learning
natural-language-processing
Readme
Releases
No releases published
Sponsor this project
Sponsor
Learn more about GitHub Sponsors
Languages
Python 98.2%
Shell 1.8%
README.md
1.4 Billion Text Credentials Analysis (NLP)
Using deep learning and NLP to analyze a large corpus of clear text passwords.
Objectives:
Train a generative model.
Understand how people change their passwords over time: hello123 -> h@llo123 -> h@llo!23.
Disclaimer: for research purposes only.

Trendy a hrozby, které nás čekají

Aktuální trendy, které vidíme do budoucna

Trendy viditelné na dark webu

- Využití AI u falešných profilů na sociálních sítích
- Manetizace skrz simualci lidského chování například u Spotify
- Podvádění v online hrách (s cílem monetizace)
- Využití AI v Social Engineeringu, například klonování hlasu v reálném čase
- Profilování cílů a automatizovaný sběr citlivých dat

Trendy do budoucna

- Obcházení procesů verifikace (například při vytváření bankovního účtu)
- Vytváření obsahu, například na základě analýzy textu při BEC
- Extrakce zajímavého obsahu z nestrukturovaných dokumentů při exfiltraci dat (Ransomware)
- Manipulace s telemetrickými daty a exploitace samotného ML modelu

DeepFakes a další

- Phishing a další formy Social Engineeringu
- Manipulace (například na finančních trzích), dezinformace
- Podvržení důkazních materiálů (například u soudu)
- Cryptojacking (zaznamenán útok na uživatele DeepFake fóra, zneužívající jejich výkonné počítače k těžbě kryptoměn)

Pět tipů jak čelit aktuálním hrozbám

1. Endpoint Detect Response

- Sběr všech relevantních událostí na koncových stanicích
- Detekce indikátorů v reálném čase
- Response akce, umožňující rychlou reakci na incident (remote shell, izolace agenta, záloha operační paměti, blokace, sběr forenzních dat)
- Důležitá je retence dat pro EDR, ideálně půl roku a více
- Propojení s dalšími zdroji dat v rámci XDR (síť, e-mail, IOT, web…)

2. Network Detect Response

- Analýza síťového provozu včetně inspekce protokolů
- Napojení na data z koncových zařízení (EDR)
- Využití dalších zdrojů Threat Intelligence (STIX, TAXII, MISP, API…)
- Opět důležitá retence dat, ideálně půl roku a více

3. Sandbox

- Možnost plné konfigurace virtuálního prostředí
  - Vlastní jazyková verze OS
  - Možnost instalace vlastních aplikací a vlastního nastavení
  - Desktopové I serverové OS
  - Podpora Windows, Linux, MacOS
- Funkce ručního spuštění testovaného vzorku přes konzoli
- Detekce anti-sandbox technik

4. Lidé

- I ty nejlepší nástroje potřebují schopné a zkušené lidi
- Ani AI (zatím?) člověka nahradit nedokáže
- Kvatliní pravidelné školení
- Capture The Flag soutěže
- Optimalizace počtu dodavatelů bezpečnostních řešení
- Využití Managed služeb jako doplněk při nedostatku lidí

Podpora

- Žádná bezpečnostní opatření nejsou stoprocentní
- Pravdelný Health Check nasazených systémů a pravidelná Best Practice kontrola
- Podpora při řešení problémů
- V případě nouze možnost zavolat na pomoc profesionální Incident Response tým

Filip Marvan

Filip_Marvan@trendmicro.com