Vědci převádí do obrazů počítačové viry a učí umělou inteligenci je rozpoznat

Ostrava (11. června 2024) - **Propojení užitečného s krásným. Tak by se dal ve zkratce popsat výzkum vědců z Fakulty elektrotechniky a informatiky (FEI) VŠB-TUO, kteří zaměřili svoji pozornost na počítačové viry, červy a další typy software navržené k poškození, narušení či neoprávněnému přístupu k počítačovým systémům. Pomocí matematické metody je výzkumníci převedli do vizuální podoby a následně předali umělé inteligenci. Ta dokáže velmi úspěšně odhalit, zda se jedná o „dobrý" nebo nebezpečný software, tedy malware. Vedle vizuálně poutavého zobrazení počítačových záškodníků zvyšuje navržená metoda přesnost jejich detekce a přináší nové poznatky o jejich chování.**

„Vyvinuli jsme metodu, která dokáže monitorovat dynamické chování malware a převést je pomocí fraktální geometrie, což je odvětví matematiky zabývající se velmi členitými útvary a jejich zobrazením, do velmi hezké vizuální podoby. Následně se obrazy probírala umělá inteligence a učila se rozeznávat špatný software od dobrého. Předali jsme jí asi 130.000 obrázků ve dvou typech experimentů, z toho polovina byl goodware a polovina malware. Poté jsme jí předložili zcela neznámé viry a chtěli po ní vyhodnocení. Dokázala malware rozeznat s úspěšností až 91 procent a stále se zlepšuje," popsal metodu její autor Ivan Zelinka z FEI, který výsledky spolu s kolegy publikoval v odborném časopise Mathematics and Computers in Simulation.

Studie otevírá nové cesty ve výzkumu malware a ukazuje, že fraktální geometrie může výrazně zlepšit jejich vizualizaci a klasifikaci. „Vzhledem k tomu, že se oblast kybernetické bezpečnosti vyvíjí a stále se objevují nové hrozby, budou podobné interdisciplinární metody zásadní pro to, abychom si před těmito nebezpečími zachovali náskok. Proto ve výzkumu pokračujeme a po dynamických analýzách se zaměřujeme i na ty statické, které jsou pro odhalení nebezpečných virů v praxi rychlejší," objasnil Zelinka.

Řadu přínosů má ale i jím vyvinutá metodika na základě dynamické analýzy. Poskytuje totiž informace i o řadě detailů v chování malware v reálném čase. „Metoda s pomocí dynamické analýzy je důležitá pro další výzkum, aby odborníci mohli ex post virus analyzovat a zkoumat. Navíc se nám otevřela řada dalších zajímavých odborných otázek," doplnil informatik a kybernetik Zelinka.

Fraktální geometrie a fraktály se využívají v řadě vědeckých oborů, ale inspiruje se jimi i řada výtvarníků. Ostravský vědec se mezi umělce sice neřadí, ale zálibu ve výtvarné umění a fraktály přiznává. „Jedná se o velmi krásné obrazce a já jsem rád, když velmi abstraktní pojmy, nebo v tomto případě digitální chování v kyberprostoru, mohou získat takovouto vizuální podobu. V tomto případě to navíc není samoúčelné, ale získali jsem i účinný nástroj pro další rozvoj kyberbezpečnosti," uzavřel Zelinka.

Vizualizace jsou dostupné na https://youtu.be/GPjaIkO9fzg

Kontaktní osoby:

Ivan Zelinka – vedoucí výzkumného týmu, člen týmu projektu REFRESH
Fakulta elektrotechnicky a informatiky VŠB-TUO, Katedra informatiky
ivan.zelinka@vsb.cz, M: 775 161 965

Martina Šaradínová
PR manažerka projektu REFRESH
martina.saradinova@vsb.cz, M: 705 698 288