Detekcia foriem sociálneho inžinierstva v emailovej komunikácii

Eva Marková

3Ib, 2018 - 2019

Abstrakt. Človek je najslabším článkom bezpečnosti. Jednou z najväčších hrozieb v dnešnom virtuálnom svete je sociálne inžinierstvo, ktoré sa zameriava práve na zraniteľnosti človeka. Sociálne inžinierstvo je „nástroj“ na zisk citlivých údajov z informačných systémov bez akýchkoľvek technických schopností. Hlavným cieľom tejto práce je analyzovať existujúce prístupy na detekciu sociálneho inžinierstva, ich porovnanie a navrhnutie a implementácia systému, ktorý by bol schopný detegovať podvrhnuté emaily.

Kľúčové slová: človek, sociálne inžinierstvo, detekcia

1 Úvod

V dnešnej dobe emailovú schránku využíva takmer každý človek, ktorý je spôsobilý pracovať na počítači. Veľmi veľa útokov pomocou sociálneho inžinierstva sa vykonáva práve prostredníctvom emailov. Útočníci si uvedomujú, nakoľko zraniteľní sú ľudia prostredníctvom emailovej komunikácie, a preto využívajú tento spôsob na zisk osobných údajov, poprípade na zisk informácií o organizácii.
Pomocou tejto práce by sme postupne chceli predchádzať týmto únikom dát a pomôcť ľuďom, ktorí si nie sú istí či sú obeťami sociálneho inžinierstva, alebo nie.
V emailovej komunikácii rozlišujeme niekoľko foriem sociálneho inžinierstva, napríklad spam, hoax, phishing, spearphishing apod. Cieľom tejto práce je analyzovať tieto formy a nájsť efektívny spôsob na detekciu foriem sociálneho inžinierstva. V pláne je aj implementovať systém, ktorý rozozná či ide o legitímny alebo podvrhnutý email a následne ho tiež aj kategorizovať.

Cieľmi tejto práce sú:

1. Analýza a spracovanie foriem sociálneho inžinierstva v emailovej komunikácii.
2. Porovnanie a spracovanie aktuálnych prístupov k ochrane voči sociálnemu inžinierstvu v emailovej komunikácii.
3. Návrh a implementácia systému na detekciu foriem sociálneho inžinierstva v emailovej komunikácii a jeho otestovanie.

1.1 Sociálne inžinierstvo

V [1] sa spomína, že Kevin Mitnick je zakladateľom sociálneho inžinierstva aj napriek tomu, že presviedčanie človeka, aby prezradil citlivé údaje, poznáme od nepamäti. Sociálne inžinierstvo je nástroj, pomocou ktorého sociálni inžinieri získavajú citlivé údaje o osobách alebo organizáciách bez použitia akýchkoľvek technických nástrojov. Primárnym cieľom sociálneho inžinierstva je zisk dôvery cieľových osôb.

1.1.1 Spam

Podľa [2] spam je irelevantná alebo nevyžiadaná správa rozposielaná cez Internet typicky veľkému množstvu užívateľov za účelom reklamy, phishingu, šírenia malvéru a podobne.

1.1.2 Phishing

Phishing [3] je nástroj používaný na oklamanie užívateľov, aby poskytli svoje osobné alebo finančné údaje útočníkovi. Phishingové útoky sú iniciované cez emaily, pričom obsahujú napríklad linky na škodlivé domény, ktoré sa zdajú byť legitímne. Útočníci sa snažia presvedčiť svoju obeť, aby navštívila falošnú stránku. Táto stránka je vytvorená za účelom stiahnutia malvéru do počítača a podobne.

1.1.3 Spearphishing

"Podvodná praktika rozosielania emailov zdanlivo od známeho alebo dôverného odosielateľa s cieľom prezradiť dôverné informácie." [4]

1.1.4 Hoax

Hoaxy [5] sú známe tým, že nie sú škodlivé pre akýkoľvek systém. Hoax sa považuje za nevyžiadanú poštu, ktorá môže používateľom alebo čitateľom e-mailu poskytnúť zavádzajúce informácie. Prenášajú klamlivé informácie, pričom ich predstavujú ako pravdivé. S postupom času hoaxy vyzerajú presvedčivejšie, a práve preto sa veľa ľudí nechá oklamať.

1.1.5 Scam

Nigérijský scam [6] inak známy aj ako ‘419‘ scam je populárna forma podvodu, pri ktorej podvodník presviedča obeť, aby zaplatila určitú sumu peňazí na základe sľubu budúcej väčšej odmeny.

2 Prístupy na detekciu phishingu v emailovej komunikácii

Poznáme rôzne prístupy na detekciu phishingu v rámci emailovej komunikácie, ktoré ale stále nie sú stopercentné. Problém tiež spočíva v tom, že v rôznych výskumoch sa zameriavajú len na phishing a teda nekategorizujú emaily podľa toho, o akú formu sociálneho inžinierstva sa jedná. Na rozdiel od týchto prác, my budeme implementovať systém, ktorý by sa neskôr mal nasadiť do prevádzky v rámci univerzity, poprípade aj v rámci iných organizácií.

Tabuľka 1. Porovnanie rôznych prístupov na detekciu phishingu.

Článok	Počet príznakov	Aké príznaky	Veľkosť datasetu	Použitý algoritmus	Presnosť	Možnosť multijazyčnosti
[7]	16	Telové URL Textové	4598 P + 5940 NP	**Random forest,** J48,…	99,1%	nie
[8]	18	Telové URL Textové	2000 P + 2000 NP	Neural Network with Backpropagation Algorithm	99,9%	nie
[9]	23	Hlavičkové Telové URL	4559 P + 4559 NP	J48	98,11%	áno
[10]	6	Telové URL	7714 P + 6656 NP	Neural Network	94,4%	áno
[11]	23	Hlavičkové Telové URL Textové	1384 P + 20071 NP	CS-SVM	99,52%	nie
[12]	9	Hlavičkové Telové URL Textové	500 P + 500 NP	SVM	97,25 %	nie
[13]	15	Telové URL Textové	500 P + 2550 NP	**Random forest**, SVM, kNN	96,07%	nie

[14]	7	Telové URL Textové	46525 P + 613048 NP	**Decision tree,** Random forest, MLP, SVM,...	99,8%	nie
[15]	61	Telové URL Textové	5260	**Multi-classifier** (SVM, RF, LogitBoost)	99%	nie

P – Phishing
NP – Non-phishing

2.1 Algoritmy použité na spracovanie extrahovaných dát z emailov

Existuje niekoľko spôsobov na spracovávanie dát extrahovaných z emailov. Tieto algoritmy strojového učenia sa líšia len v niektorých vlastnostiach, čo je ale dôležité - vieme ich použiť na rovnaký zámer.

2.1.1 Náhodný les

Náhodné lesy [16] sú kombináciou stromových prediktorov. Každý strom závisí od hodnôt náhodného vektora. Chyba generalizácie pre lesy konverguje. až kým sa počet stromov v lese nestane obrovským. Táto chyba závisí od intenzity jednotlivých stromov v lese a korelácie medzi nimi.

2.1.2 Lineárny Support Vector Machine

Princípom SVM [17] je rozdelenie tréningových dát zakreslených v bodovom diagrame zväčša na dve oblasti patriace triedam dát. Support Vector Machine rozdeľuje oblasť tzv. nadrovinou na bodovom diagrame na dve triedy a určuje, ktoré body patria do ktorej triedy. Máme súbor tréningových príkladov a pre každé, i = 1,2, ..., n, v tréningovej množine, pozorujeme vstupný vektor x, ktorý patrí do Rn. Cieľom je naučiť sa klasifikačné pravidlo z tréningovej množiny, aby sme mohli v budúcnosti priradiť konkrétnu triedu všetkým novým subjektom.

2.1.3 J48

J48 [18] vytvára rozhodovací strom zo súboru tréningových údajov, kde každý uzol stromu je realizovaný funkciou, ktorá najúčinnejšie rozdeľuje sadu vzoriek do podsúborov. Rozhodovací strom je užitočný pri klasifikácii problému. Jedná sa o Java implementáciu algoritmu C4.5. Akonáhle je strom vytvorený, je aplikovaný na každú ticu v databáze a výsledkom je klasifikácia pre danú ticu.

2.1.4 kNN

KNN [19] klasifikačný algoritmus založený na k-najbližšej metóde susedov, je jednoduchá, efektívna a neparametrická metóda klasifikácie textu. Nevyžaduje konzistentnosť údajov. Najprv je potrebné predbežné spracovanie tréningového textu, extrakcia funkcie a následne tvorba klasifikátora kNN.

Tabuľka 2. Porovnanie najčastejšie používaných algoritmov.

Algoritmus	**Objem dát**	**Využitie**	**Odhad časovej zložitosti**	**Poznámka**
Náhodný les	Veľké množstvo	Klasifikácia, regresná analýza	O(ntree * d * n*log(n))	Náhodný výber príznakov
Lineárny SVM	Malé množstvo	Klasifikácia, regresná analýza	O(m)	Binárna klasifikácia
J48	Malé množstvo	Klasifikácia, štatistická klasifikácia	$O(m*d^2)$	Java implementácia C4.5
kNN	Veľké množstvo	Klasifikácia	O(m*d*log(d))	

ntree – počet stromov
d – počet príznakov
n – počet záznamov
m – počet dimenzií

Literatúra

[1] REYNOLDS, Vince. Social Engineering: The Art of Psychological Warfare, Human Hacking, Persuasion & Deception. 2015.

[2] Projekt Spam [online]. [cit. 2019-02-15]. Dostupné z: https://en.oxforddictionaries.com/definition/spam

[3] CHAUDHRY, Junaid Ahsenali; RITTENHOUSE, Robert G. Phishing: Classification and CounterMeasures. In: *Multimedia, Computer Graphics and Broadcasting (MulGraB), 2015 7th International Conference on*. IEEE, 2015. p. 28-31.

[4] Projekt Spearphishing [online]. [cit. 2019-02-15]. Dostupné z: https://en.oxforddictionaries.com/definition/spear_phishing

[5] ISHAK, Adzlan; CHEN, Y. Y.; YONG, Suet-Peng. Distance-based hoax detection system. In: *Computer & Information Science (ICCIS), 2012 International Conference on*. IEEE, 2012. p. 215-220.

[6] ISACENKOVA, Jelena, et al. Inside the scam jungle: A closer look at 419 scam email operations. *EURASIP Journal on Information Security*, 2014, 2014.1: 4.

[7] YASIN, Adwan; ABUHASAN, Abdelmunem. An intelligent classification model for phishing email detection. *arXiv preprint arXiv:1608.02196*, 2016.

[8] KATHIRVALAVAKUMAR, Thangairulappan; KAVITHA, Krishnasamy; PALANIAPPAN, Rathinasamy. Efficient Harmful Email Identification Using Neural Network. *British Journal of Mathematics & Computer Science,(1)*, 2015, 58.

[9] SMADI, Sami, et al. Detection of phishing emails using data mining algorithms. In: *Software, Knowledge, Information Management and Applications (SKIMA), 2015 9th International Conference on*. IEEE, 2015. p. 1-8.

[10] MORADPOOR, Naghmeh; CLAVIE, Benjamin; BUCHANAN, Bill. Employing machine learning techniques for detection and classification of phishing emails. In: *Computing Conference, 2017*. IEEE, 2017. p. 149-156.

[11] NIU, Weina, et al. Phishing Emails Detection Using CS-SVM. In: *Ubiquitous Computing and Communications (ISPA/IUCC), 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on*. IEEE, 2017. p. 1054-1059.

[12] FORM, Lew May, et al. Phishing email detection technique by using hybrid features. In: *IT in Asia (CITA), 2015 9th International Conference on*. IEEE, 2015. p. 1-5.

[13] YADAV, Dhirendra Pratap, et al. A Novel Ensemble Based Identification of Phishing E-Mails. In: *Proceedings of the 9th International Conference on Machine Learning and Computing*. ACM, 2017. p. 447-451.

[14] MA, Liping, et al. Detecting phishing emails using hybrid features. In: *Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on*. IEEE, 2009. p. 493-497.

[15] SHYNI, C. Emilin; SARJU, S.; SWAMYNATHAN, S. A Multi-Classifier Based Prediction Model for Phishing Emails Detection Using Topic Modelling, Named Entity Recognition and Image Processing. *Circuits and Systems*, 2016, 7.09: 2507.

[16] BREIMAN, Leo. Random forests. *Machine learning*, 2001, 45.1: 5-32.

[17] LIN, Yi; LEE, Yoonkyung; WAHBA, Grace. Support vector machines for classification in nonstandard situations. *Machine learning*, 2002, 46.1-3: 191-202.
[18] PATIL, Tina R.; SHEREKAR, S. S. Performance analysis of Naive Bayes and J48 classification algorithm for data classification. *International journal of computer science and applications*, 2013, 6.2: 256-261.
[19] WANG, Lijun; ZHAO, Xiqing. Improved KNN classification algorithms research in text categorization. In: *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*. IEEE, 2012. p. 1848-1852.