Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS559

L25: Presentations

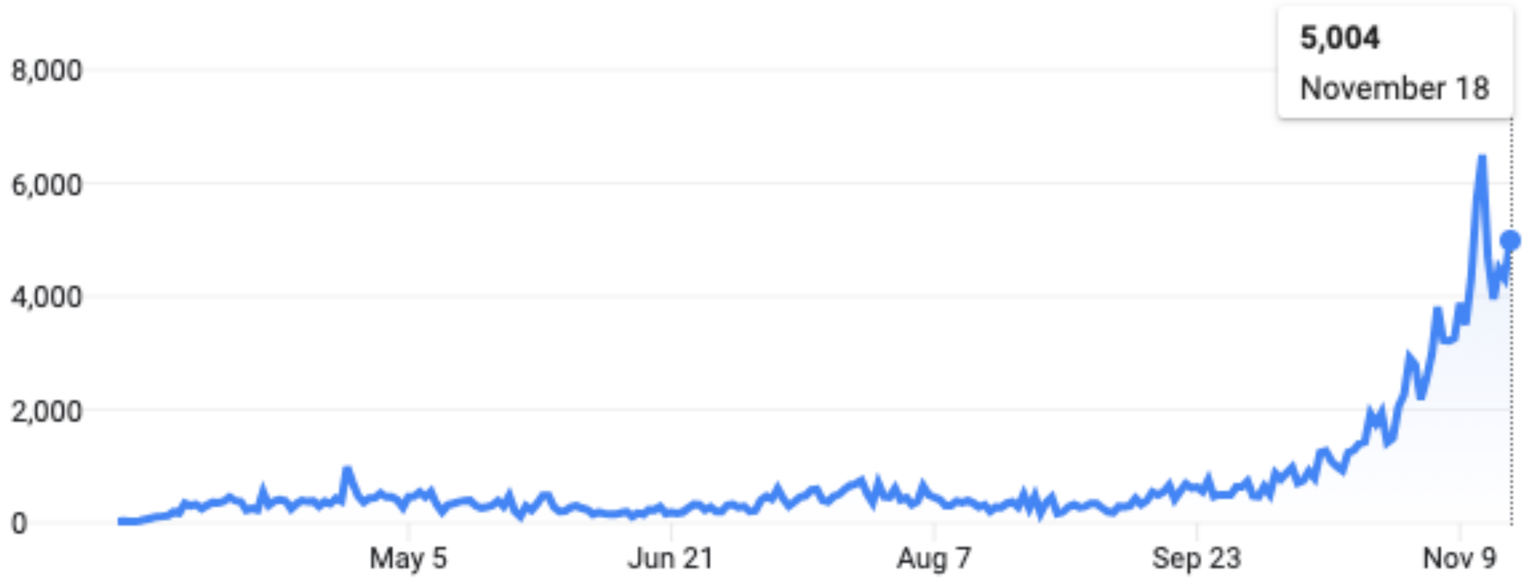
CSU Cybersecurity Center
Computer Science Dept

Presentations

- Each presentation is limited to 10 minutes and two minutes are allowed for discussions. I suggest using no more than 20 slides. You should practice and time your presentation.
- These sessions will be live using MS Teams. Everyone is required to participate, ask questions and take notes. Distance students who are working full time need to provide a video with link sent to cs559@cs.colostate.edu at least **24 hours** before the presentation (to allow us to ensure it works properly).
- This is a research oriented project. Please mention significant recent work and cite researchers, and identify current trends challenges.
- Students with closely related presentations should coordinate among themselves to minimize overlap.
- Everyone: fill the peer-review form, and submit through canvas on

Personal

- Please be very cautious. New Covid-19 cases in Colorado.



Colorado State University

Presentations/Final Report

Th Nov 19, 2020

1. Al Amin, Md. **Quantitative Modeling of Economics of Ransomware**
2. Neumann, Don. **Quantitative Modeling of Economics of Ransomware**
3. Haynes, Katherine, **Combining Adversarial Synthesized Data and DeepNeural Networks to Improve Phishing Detection**
4. Houlton, Sarah, **Cyber Crime and Criminals: Their Methods and Motivations**
5. Jepsen, Waylon, **Motivation and Methods of North Korea's Cyber Criminals**
6. Rodriguez, Luis, **A Quantitative Examination of Phishing**

Colorado State University

Project

Final report (8-12 pages, submit using Canvas/Turnitin): It needs to be publication quality. It should include

- the title, name of the author(s), name of the class and professor,
- an abstract,
- description of what is your contribution and what is new in your report,
- introduction (modification, background and related work, objectives and methods),
- description of assumptions/schemes/models/problem-formulation,
- comparison/discussion/derivation etc. of the results,
- conclusions (findings and suggestions for improvements) and
- references.
- Report must include appropriate figures and must have some hard data (tables/plots/screen-shots/algorithms etc.).

- Evaluation: significance and originality, thoroughness of research, depth of understanding displayed and presentation.

We will continue

- Have a great Thanksgiving.
- Continue working on your project.
- Schedule for the rest of the presentations will be shared soon.

Quantitative Modeling of Economics of Ransomware

MD AL AMIN and Don Neumann

CS559 Fall20

Topic Introduction

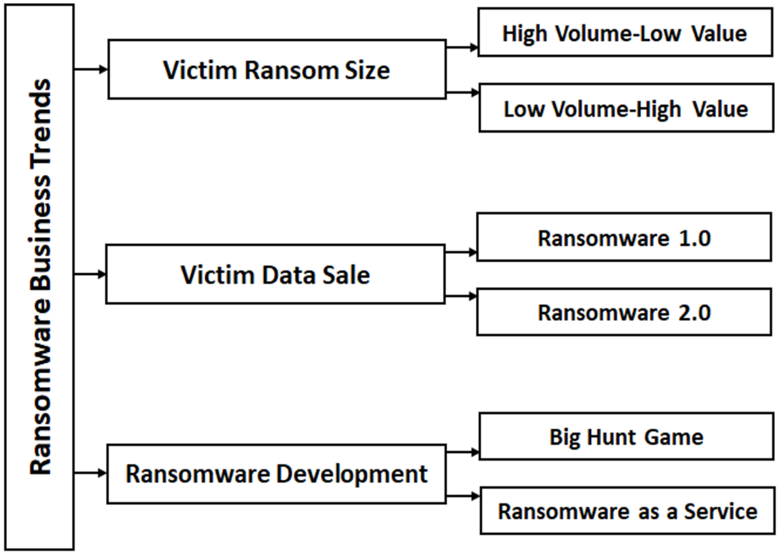
- Ransomware attacks are increasing every year
- Multiple attack vectors - phishing, social engineering, hacking
- Phishing and social engineering hard to identify
- High data recovery cost
- Ransom payment does not guarantee recovery
- Cyber insurance is an emerging trend
- Government, regulatory, criminal sanctions

Related Work

- Victim focus on backups, attacker focus on attack/ransom demand (Laszka et. al [2])
- Economics and price discrimination tactics (Hernandez-Castro et. al [4])
- Attacker reputation, whether to pay ransom demand (Caporusso & Zarifis et. al [11] [12])
- Defensive measures against ransomware 2.0 and data value (Li et. al [13])
- Impact of bitcoin (Paquet-Clouston & Conti et. al [6] [16])
- User awareness based preventative measures (Luo & White et. al [14] [15]

Ransomware Business Trends

- HVLV - Random, low ransom [17]
- LVHV - Targeted, high ransom [17]
- Ransomware 1.0 - Encrypts victims data [13]
- Ransomware 2.0 - Copies victims data [13]
- Big Hunt Game - Targeted, sophisticated [17]
- RaaS - Affiliate networks [21]



Two Phase-Three Player Hide and Seek (TPHS)

- Introducing third party influence
- Insurance company, government, volunteer organizations
- Modeling victim cost and risk minimization
- Modeling attacker effort and effect

TPHS Game model

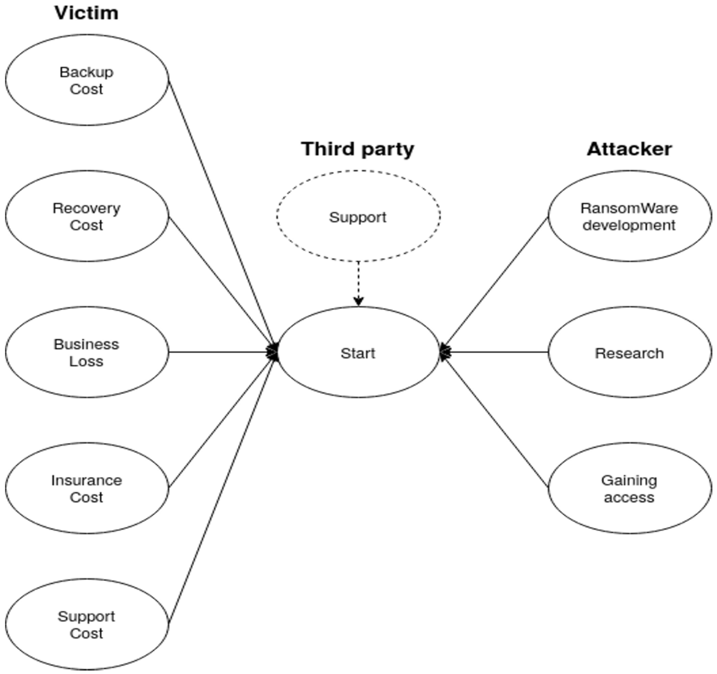
- Players: Victim, Attacker, Third Party (TP)
- Stages: Hide Phase, Seek Phase
- Game mode: With TP, without TP
- Hide Phase: Preparation
- Seek Phase: Performance
- Attacker target: maximize expected payoff
- Victim target: minimize expected cost
- TP target: support victim to minimize expected cost

Reference: [8]

Hide Phase - Attacker Preparation

- Ransomware development
- Research
- Gaining access

- Expected ransom demand
- Ransom negotiation
- Victim data sensitivity
- Victim security measures



Hide Phase - Victim Preparation

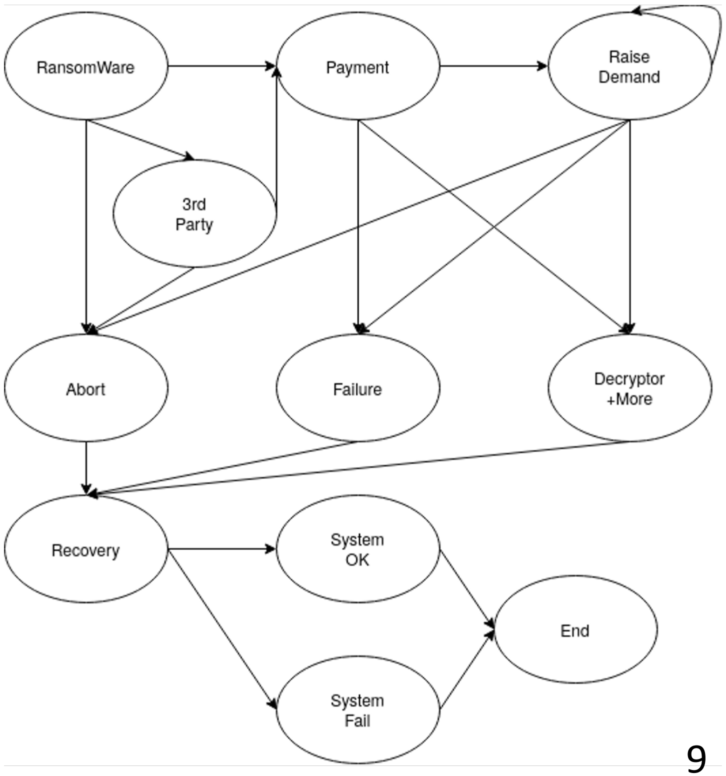
- Backup_Cost = Onsite storage cost + Offsite storage cost + Human cost
- Recovery_Cost = Data recollection cost + Backup recovery cost + Decryption tool cost
- Business_Loss = Revenue loss + Compensation cost + Fines + Reputation loss
- Insurance_Cost = Premium Cost + Loss coverage + Ransom payment
- Support_Cost = Law enforcement cost + Lawyer cost + Investigation cost

Hide Phase - TP Preparation

- Insurance company - Considers victim data sensitivity, security measures, employee awareness, risk management, business continuity
- Government - Security and risk recommendations, sanctions, cooperation with international community
- Volunteer orgs - Ransomware research and public awareness

Game Model - Seek Phase

- Markov Chain (Ransomware is Start)
- Payment
- Raise Demand
- Third Party
- Decryptor
- Failure
- Abort
- Recovery
- System Fail / OK

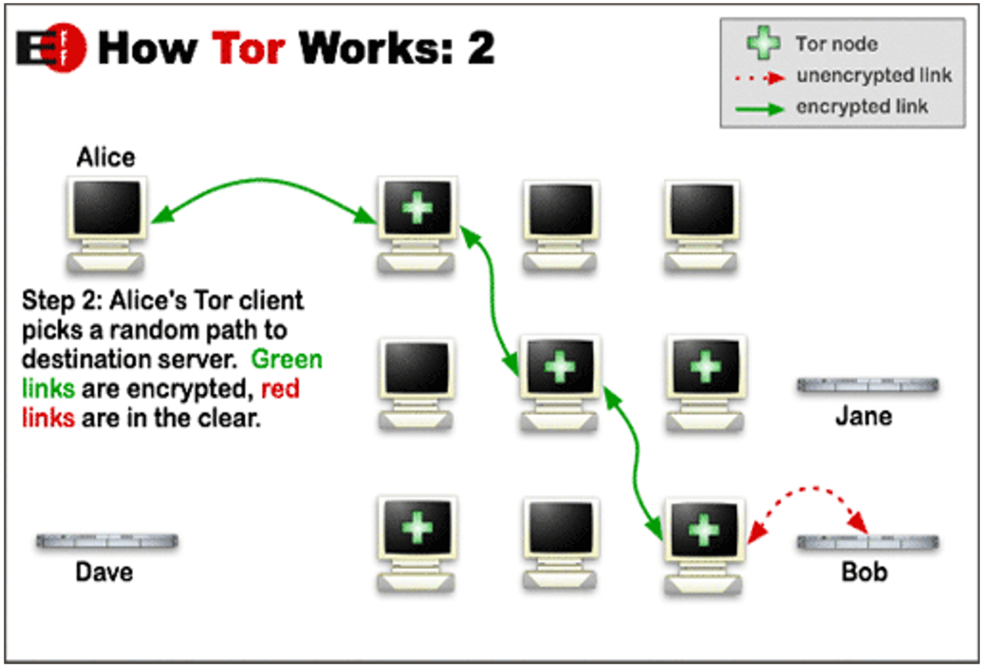


Considerations

- Ransomware payment - no guarantee, demand raise, data sold, infected again
- System restore - May be compromised, air-gapped or offline backup necessary
- Decryption and recollection - time and resource consuming
- Compensation service - clients and business associates
- Legality - Government, regulatory, and criminal sanctions
- Legality - Client and business associate lawsuits

Difficult to catch

- Anonymous communication: ToR
- Cryptocurrency like Bitcoin



Reference: https://2019.www.torproject.org/about/overview.html.en

References

[2] A. Laszka, S. Farhang, and J. Grossklags, "On the Economics of Ransomware," Lecture Notes in Computer Science Decision and Game Theory for Security, pp. 397–417, 2017.

[4] J. Hernandez-Castro, E. Cartwright, and A. Stepanova, "Economic Analysis of Ransomware," SSRN Electronic Journal, 2017.

[6] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the Bitcoin ecosystem," Journal of Cybersecurity, vol. 5, no. 1, 2019.

[11] N. Caporusso, S. Chea, and R. Abukhaled, "A Game-Theoretical Model of Ransomware," Advances in Intelligent Systems and Computing Advances in Human Factors in Cybersecurity, pp. 69–78, 2018.

[12] A. Zarifis and X. Cheng. "The Impact of Extended Global Ransomware Attacks on Trust: How the Attacker's Competence and Institutional Trust Influence the Decision to Pay," Proceedings of the Americas Conference on Information Systems (AMCIS), 2018.

[13] Z. Li and Q. Liao, "Ransomware 2.0: To sell, or not to sell. A Game-theoretical Model of Data-selling Ransomware," Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020.

[14] X. Luo and Q. Liao, "Awareness Education as the Key to Ransomware Prevention." Information Systems Security, vol. 16, no. 4, pp. 195-202, 2007, doi: 10.1080/10658980701576412.

[15] G. White, G, "Information Security Education Relationships on Incidents and Preventions: Cyber Assurance Literacy Needs." Proceedings of the 2012 Annual Information Systems Educators Conference (ISECON), 2012.

[16] M. Conti, A. Gangwal, and S. Ruj, "On the economic significance of ransomware campaigns: A Bitcoin transactions perspective," Computers \& Security, vol. 79, pp. 162–189, 2018.

[17] "Ransomware Attack Methods Alter as Threat Actors Grow in Sophistication," Mar-2020. [Online]. Available: http://www.cybcube.com/wp-content/uploads/2020/03/Understanding-Ransomware-Trends-Report.pdf. [Accessed: 08-Nov-2020].

[21] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The Ransomware-as-a-Service economy within the darknet," Computers \& Security, vol. 92, p. 101762, 2020.

Thank you

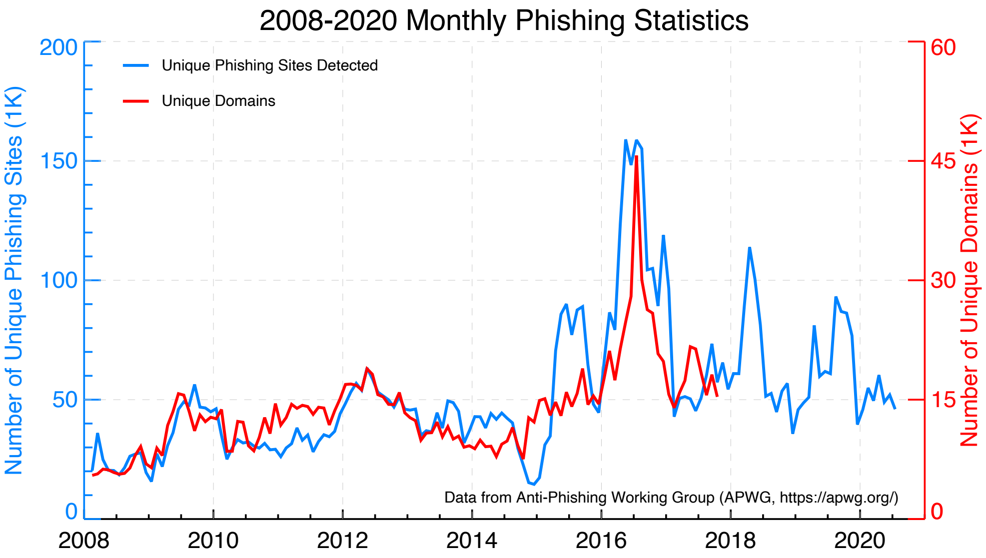
Colorado State University

Combining Adversarial Synthesized Data and Deep Neural Networks to Improve Website Phishing Detection

Katherine Haynes
CS 559
November 19, 2020

Website Phishing

- Fraudulent replication of trusted websites
  - Acquire sensitive personal information
  - Top internet crime by victim count in 2019 [9]



Machine Learning

- Flexible
- Predictive
- Able to use variety of information
  - URL statistics
  - Domain information
  - Website content
- Numerous classification methods

- Decision Tree (DT)
- Gradient Boosting (GB)
- k-Nearest Neighbor (k-NN)
- Majority Voting (MV)
- Naïve Bayes (NB)
- Random Forest (RF)
- Support Vector Machine (SVM)

What about Neural Networks?

Artificial Neural Networks (ANNs)

- Prior to 2019, ANNs criticized
  - Significant time involvement
  - Difficult to understand
- Surge in research in past 2 years
  - Adaptive strategy to design network structure [15]
  - Fuzzy-based approach [16]
  - Dynamical parameter tuning [27]
  - Optimal feature selection [36, 37, 19]

Machine Learning Weaknesses

- Reliance on pre-classified data
- Continual data gathering and training
- Adversarial phishing
  - Attackers exploit trained classifier
  - Manipulations able to bypass trained model

Recent approach: Synthetic Data

- Developed by Shirazi et al. (2019) [24]
- Mimic new phishing websites
  - Combine clustering and autoencoder
  - Augment training
  - Aid classifier robustness to adversarial attacks

Project Goal

Extend experiments in [21] to deep ANNs

- Feature, architecture, and parameter search
- Repeat experiments
- Compare results

ANNs with Synthetic Data [1/7]

- Data
  - "Original": Created by Tan in 2018 [26]
    - 47 features
    - 5,000 phishing and 5,000 legitimate websites
  - "Synthetic": Created by Shirazi in 2019 [24]
    - Uses adversarial sample generation (autoencoder)
    - 10,000 phishing and 10,000 legitimate websites
  - 80% Training, 20% Testing
- ANN Models
  - Scikit-Learn and Tensorflow in Python
  - Guided search using Hyperopt [5, 6] on Google Colab
  - Searched 100 models, saved top 40

ANNs With Synthetic Data [2/7]

- Experiments
  - Data

Name	Training Data	Testing Data
TOTO	Original	Original
TOTS	Original	Synthetic
TOSTO	Original & Synthetic	Original
TOSTS	Original & Synthetic	Synthetic

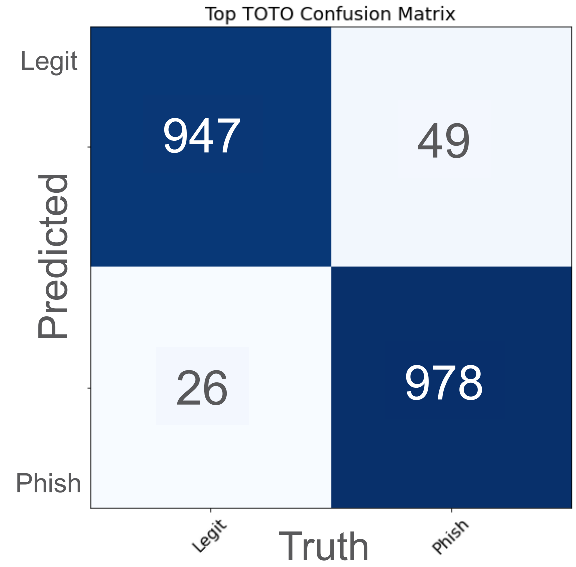
  - Model

Name	Description
M1	Model Search on Original Training Data
M2	Model Search on Synthetic Training Data

ANNs With Synthetic Data [3/7]

- Base Results (TOTO) on Original Dataset (M1)
  - Top 40 ANN models achieved accuracy > 91%

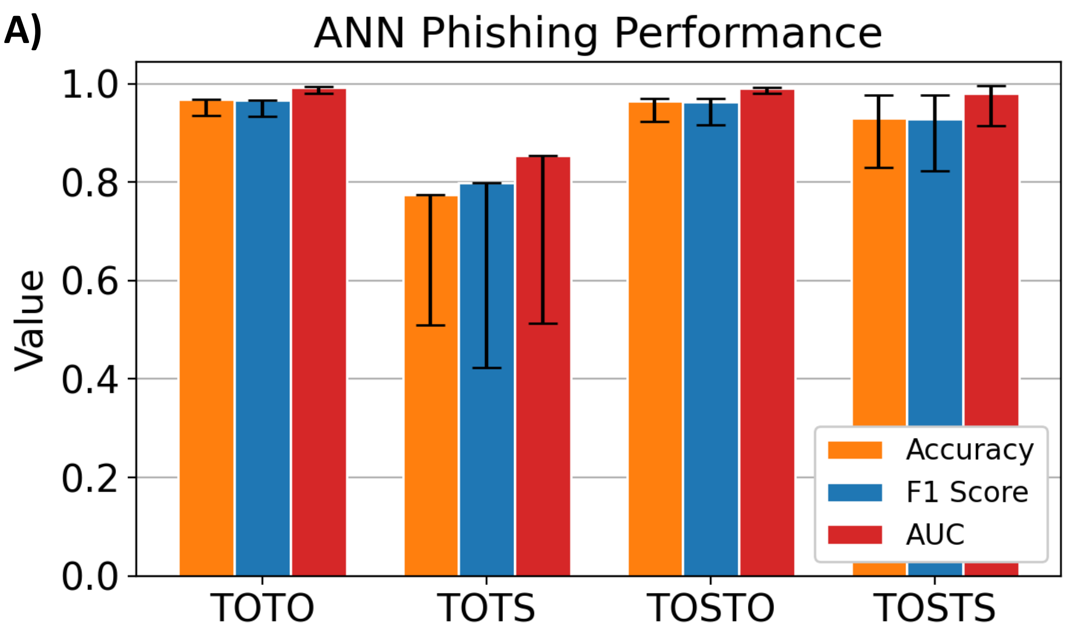
	Test Acc	NLayers	NEpochs	NFeatures	Optimizer
1	0.974902	4	60	11	Adam
2	0.974010	4	40	39	Nadam
3	0.973974	4	60	39	Adam
4	0.969792	4	120	44	Adam
5	0.969301	4	120	22	Adam
6	0.968098	5	60	45	Adam
7	0.965552	4	40	39	Nadam
8	0.965282	3	150	12	Adam
9	0.964462	4	40	32	Adam
10	0.964227	8	60	13	Adam



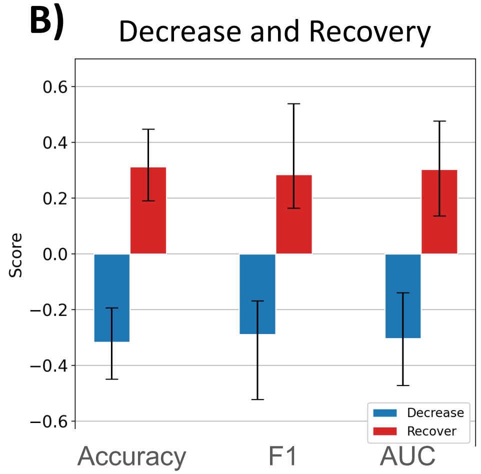
- Majority of samples correctly predicted
- False positive rate higher than false negative
  - Higher tendency to predict legitimate websites as phishing

ANNs With Synthetic Data [4/7]

A)

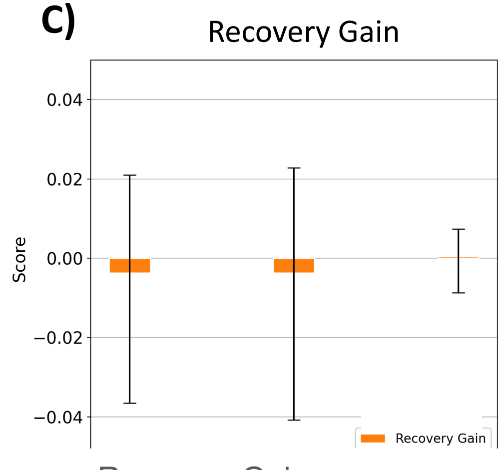


B)



Decrease = TOTS – TOTO
Recovery = TOSTO - TOTS

C)



Recovery Gain =
Decrease + Recovery

Adversarial Phishing Detection (M1)

- Lower performance in presence of adversarial phishing websites (TOTS)
  - Large range of drop
- All ANNs recover within 0.035 when synthetic data included during training
- Performance predicting adversarial phishing websites improves substantially when synthetic data is included during training
  - From ~0.78 to ~0.93

ANNs With Synthetic Data [5/7]

Adversarial Phishing Detection F1 Score

By Classifier Type

Model	TOTO	TOTS	TOSTO	TOSTS	Decr	Recov
ANN	**0.974**	**0.799**	**0.964**	**0.929**	**0.289**	**0.285**
GNB	0.84	0.37	0.65	0.82	0.48	0.47
GB	0.98	0.36	0.96	0.92	0.48	0.47
MV	0.96	0.39	0.93	0.92	0.57	0.54
SVML	0.93	0.45	0.93	0.91	0.47	0.37
SVMG	0.93	0.45	0.93	0.91	0.62	0.58

How do deep neural networks compare to other classifiers?

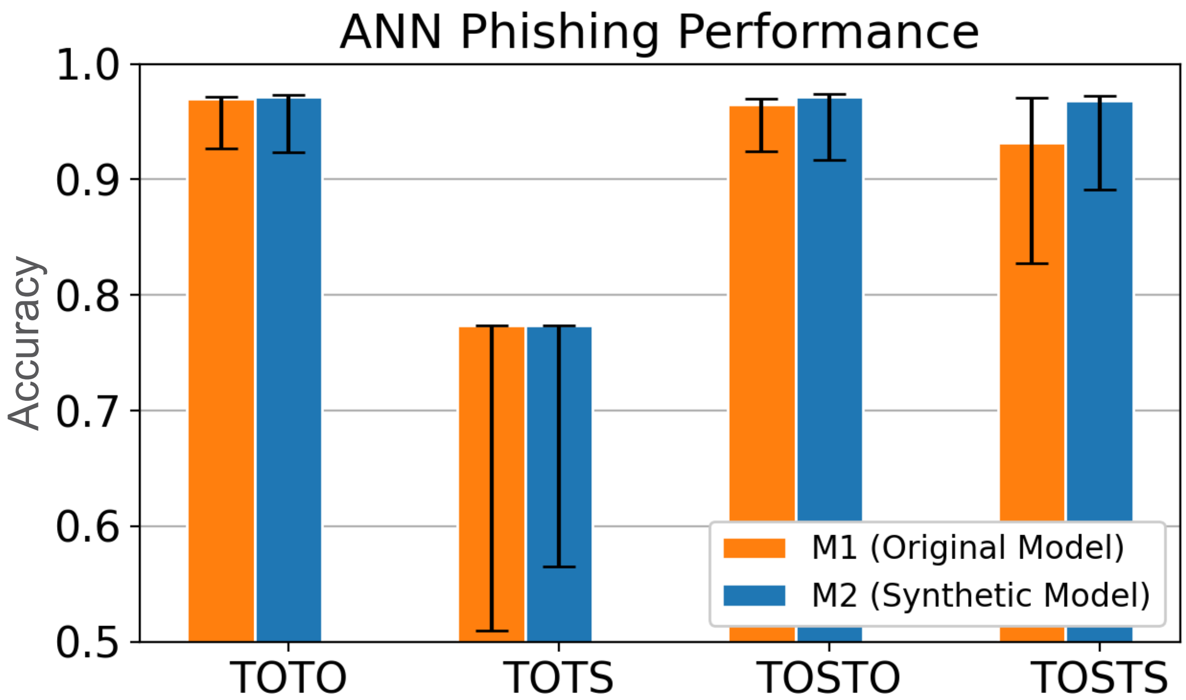
- Similar performance to top classifier on TOTO (GB)
- Outperform other classifiers in presence of adversarial phishing (TOTS)
- Recover better than other classifiers (TOSTO and TOSTS)

Can we do any better predicting adversarial phishing websites?

ANNs With Synthetic Data [6/7]

Adversarial Phishing Detection Accuracy

M1 versus M2



Developing optimal models using adversarial synthetic data:

- Improves performance
- Makes more robust models

ANNs With Synthetic Data [7/7]

Conclusions

- Deep ANNs predict phishing using feature data with ~96% accuracy
  - Perform as well as other common classifiers
- Model performance worsens in presence of adversarial phishing
  - Recovery is possible training on synthetic phishing data
  - Degradation is less than other common classifiers
    → ANNs may be more robust
- Model architecture guidance may help build higher performing ANNs
  - Optimizing model setup with the aid of synthetic data designed to simulate adversarial phishing websites yields higher-performing ANNs that may be less susceptible to adversarial attacks

Future Work

- Expand synthetic data to different types of adversarial attacks
- Try GANs to develop adversarial phishing websites

References [1/2]

Frame of an animation by the U.S. Federal Trade Commission that was intended to educate people about phishing tactics. From Wikipedia (https://en.wikipedia.org/wiki/Phishing).

[1] N. Abdelhamid, F. Thabtah, & H. Abdel-jaber, "Phishing detection: a recent intelligent machine learning comparison based on models content and features," 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, 2017, pp 72-77, https://doi.org/10.1109/ISI.2017.8004877.

[2] M.A. Adebowale, K.T. Lwin, E. Sanchez, & M.A. Hossain, "Intelligent web-phishing detection and protection scheme using integrated features of images, frames, and text," *Expert Systems With Applications*, **115**, 2019, 300-313, https://doi.org/10.1016/j.eswa.2018.07.067.

[3] A. AlEroud & G. Karabatis, "Bypassing detection of URL-based phishing attacks using generative adversarial deep neural networks," In *Proceedings of the Sixth International Workshop on Security and Privacy Analytics (IWSPA '20)*. Association for Computing Machinery, New York, NY, USA, 53-60, https://doi.org/10.1145/3375708.3380315.

[4] A.C. Bahnsen, I. Torroledo, L. Camacho, & S. Villegas, "DeepPhish: Simulating Malicious AI," 2018 APWG Symposium on Electronic Crime Research (eCrime), 2018.

[5] J. Bergstra, R. Bardenet, Y. Bengio, & B. Kegl, "Algorithms for Hyper-Parameter Optimization," In *NIPS*24*, 2546-2554, https://papers.nips.cc/paper/2011/file/86e8f7ab32cfd12577bc2619bc635690-Paper.pdf.

[6] J. Bergstra, D. Yamins, & D.D. Cox, "Making a science of model search: hyperparameter optimization in hundreds of dimensions for vision architectures," In *Proceedings of the 30th International Conference on Machine Learning*, Atlanta, Georgia, USA, http://proceedings.mlr.press/v28/bergstra13.pdf.

[7] J. Devlin, M.-W. Chang, K. Lee, & K. Toutanova, "BERT: Pre-training of deep bidirectional transformers for language understanding," arXivLabs, Cornell University, New York, USA, https://arxiv.org/abs/1810.04805.

[8] F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han, & J.Q. Wang, "The application of a novel neural network in the detection of phishing websites," *Journal of Ambient Intelligence and Humanized Computing*, 2018, https://doi.org/10.1007/s12652-018-0786-3.

[9] Federal Bureau of Investigation (FBI) Internet Crime Complaint Center, "2019 Internet Crime Report," Washington, D.C., USA, 2020, https://pdf.ic3.gov/2019_IC3Report.pdf.

[10] K.M.Z. Hasan, M.Z. Hasan, & N. Zahan, "Automated prediction of phishing websites using deep convolutional neural network," International Conference on Computer, Communication, Chemical, Materials, and Electronic Engineering (IC4ME2), Rajshahi, Bangladesh, 2019, pp 1-4, https://doi.org/10.1109/IC4ME247184.2019.9036647.

[11] Y. Huang, Q. Yang, J. Qin, & W. Wen, "Phishing URL detection via CNN and attention-based hierarchical RNN," 18th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications, 2019, https://www.doi.org/10.1109/TrustCom/BigDataSE.2019.00024.

[12] G.J.W. Kathrine, P.M. Praise, A.A. Rose, & E.C. Kalaivani, "Variants of phishing attacks and their detection techniques," Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019), Tirunelveli, India, 2019, https://doi.org/10.1109/ICOEI.2019.8862697.

References [2/2]

[13] H. Le, Q. Pham, D. Sahoo, & S.C.H. Hoi, “URLNet: learning a URL representation with deep learning for malicious URL detection,” Cornell University, New York, USA, 2018, https://arxiv.org/abs/1802.03162.

[14] Y. Li, Z. Yang, X. Chen, H. Yuan, & W. Liu, “A stacking model using URL and HTML features for phishing webpage detection,” *Future Generation Computer Systems*, **94**, 2019, 27-39, https://doi.org/10.1016/j.future.2018.11.004.

[15] R.M.A. Mohammad, “Predicting phishing websites based on self-structuring neural network,” *Neural Computing and Applications*, **25**(2), 2014, pp.443-458, http://eprints.hud.ac.uk/19220/.

[16] L.A.T. Nguyen, B.I. To, & H.K. Nguyen, “An efficient approach for phishing detection using neuro-fuzzy model,” *J. Autom. Control Eng.*, **3**(6), 2015, https://doi.org/10.12720/joace.3.6.519-525.

[17] G. De La Torre Parra, P. Rad, K.-K.R. Choo, & N. Beebe, “Detecting Internet of Things attacks using distributed deep learning,” *Journal of Network and Computer Applications*, **163**(102662), 2020, https://doi.org/10.1016/j.jnca.2020.102662.

[18] I. Qabajah, F. Thabtah, & F. Chiclana, “A recent review of conventional vs. automated cybersecurity anti-phishing techniques,” *Computer Science Review*, **29**, 2018, pp. 44-55, https://doi.org/10.1016/j.cosrev.2018.05.003.

[19] P. Saravanan & S. Subramanian, “A framework for detecting phishing websites using GA based feature selection and ARTMAP based website classification,” *Procedia Computer Science*, **171**, 2020, 1083-1092, http://doi.org:/10.1016/j.procs.2020.04.116.

[20] J. Saxe & K. Berlin, “eXpose: a character-level convolutional neural network with embeddings for detecting malicious URLs, file paths, and registry keys,” Cornell University, New York, USA, 2017, https://arxiv.org/abs/1702.08568v1.

[21] B. Sabir, M.A. Babar, & R. Gaire, “An evasion attack against ML-based phishing URL detectors,” Cornell University, New York, USA, 2020, https://arxiv.org/abs/2005.08454.

[22] H. Shirazi, B. Bezawada, I. Ray, & C. Anderson, “Adversarial sampling attacks against phishing detection,” 33rd IFIP Annual Conference on Data and Applications Security and Privacy (DBSec), Charleston, SC, USA, 2019, https://doi.org/10.1007/978-3-030-22479-0_5.

[23] H. Shirazi, L. Zweigle, & I. Ray, “A machine-learning based unbiased phishing detection approach,” 17th International Conference on Security and Cryptography (SECRYPT 2020), Paris, France, 2020.

[24] H. Shirazi, S.R. Muramudalige, I. Ray, & A.P. Jayasumana, “Improved phishing detection algorithms using adversarial autoencoder synthesized data,” Proc. IEEE 45th Conference on Local Computer Networks (LCN2020), Sydney, Australia, 2020.

[25] C. Singh & S. Meenu, “Phishing website detection based on machine learning: a survey,” 6th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 398-404, https://doi.org/10.1109/ICACCS48705.2020.9074400.

[26] C.L. Tan, “Phishing dataset for machine learning: feature evaluation,” Mendeley Data, V1, http://dx.doi.org/10.17632/h3cgnj8hft.1.

[27] F. Thabtah, R.M. Mohammad, & L. McCluskey, “A dynamic self-structuring neural network model to combat phishing,” 2016 International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, 2016, pp. 4221-4226, http://doi.org/10.1109/IJCNN.2016.7727750.

[28] R. Vinayakumar, K.P. Soman, & P. Poornachandran, “Evaluating deep learning approaches to characterize and classify malicious URLs,” *Journal of Intelligent & Fuzzy Systems*, **34**, 2018, 1333-1343, http://doi.org/10.3233/JIFS-169429.

[29] W. Wei, Q. Ke, J. Nowak, M. Korytkowski, R. Scherer, & M. Wozniak, “Accurate and fast URL phishing detector: a convolutional neural network approach,” *Computer Networks*, **178**(107275), 2020, http://doi/org/10.1016/j.comnet.2020.107275.

[30] X. Xiao, D. Zhang, G. Hu, Y. Jiang, & S. Xia, “CNN-MHSA: a convolutional neural network and multi-head self-attention combined approach for detecting phishing websites,” *Neural Networks*, **125**, 2020, 303-312, http://doi.org/10.1016/j.neunet.2020.02.013.

[31] P. Yang, G. Zhao, & P. Zeng, “Phishing website detection based on multidimensional features driven by deep learning,” *IEEE Access*, 2019, https://doi.org/10.1109/ACCESS.2019.2892066.

[32] L. Yang, J. Zhang, X. Wang, Z. Li, Z. Li, & Y. He, “An improved ELM-based and data preprocessing integrated approach for phishing detection considering comprehensive features,” *Expert Systems with Applications*, **165**(113863), 2021, http://doi.org/10.1016/j.eswa.2020.113863.

[33] V.M. Yazhmozhi & B. Janet, “Natural language processing and machine learning based phishing website detection system, Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 2019, pp. 336-340, https://doi.org/10.1109/I-SMAC47947.2019.9032492.

[34] S.Y. Yerima & M.K. Alzaylaee, “High accuracy phishing detection based on convolutional neural networks,” 3rd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2020, pp. 1-6, https://doi.org/10.1109/ICCAIS48893.2020.9096869.

[35] X. Zhang, D. Shi, H. Zhang, W. Liu, & R. Li, “Efficient detection of phishing attacks with hybrid neural networks,” 18th IEEE International Conference on Communication Technology (ICCT), Chongqing, 2018, pp 844-848, https://doi.org/10.1109/ICCT.2018.8600018.

[36] E. Zhu, Y. Chen, C. Ye, X. Le & F. Liu, “OFS-NN: an effective phishing websites detection model based on optimal feature selection and neural network,” *IEEE Access*, **7**, 2019, https://10.1109/ACCESS.2019.2920655.

[37] E. Zhu, Y. Ju, Z. Chen, F. Liu, & X. Fang, “DTOF-ANN: an artificial neural network phishing detection model based on decision tree and optimal features,” *Applied Soft Computing Journal*, **95**(106505), 2020, https://doi.org/10.1016/j.asoc.2020.106505.

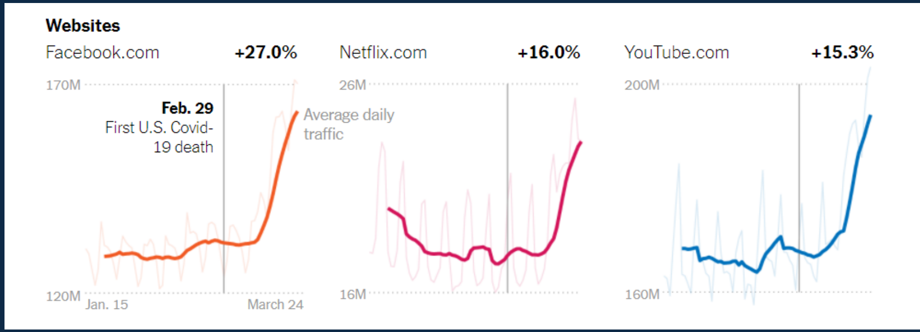
CYBERCRIME AND CYBERCRIMINALS: THEIR METHODS AND MOTIVATIONS

Sarah Houlton

shoulton@rams.colostate.edu

Introduction

- The prevalence of cyber attacks is rising as more and more of our information gets stored on the web.
- Online banking, shopping, working, and social interaction has gained popularity over time, especially as the pandemic worsens
- Bigger online presence means bigger cybercrime threat
- To mitigate risk, we should focus on the attackers rather than the victims
    - Better defenses
    - Smaller sample size



Source: https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html

Attacker Categories

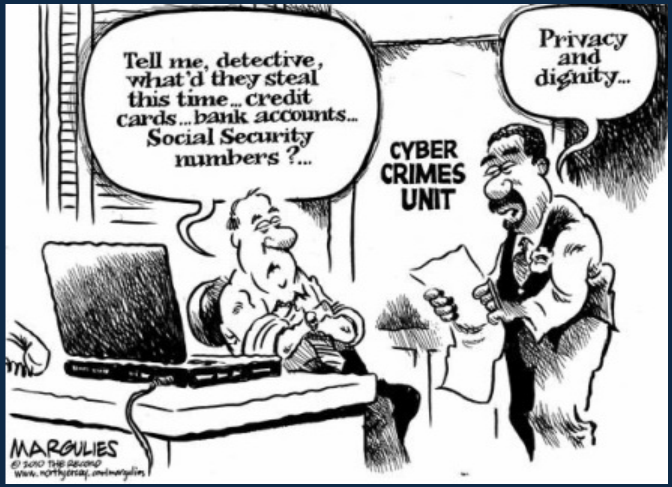
- Black Hat Hackers
  - Motivated by hate, anger, or power
  - No issue causing harm to others
  - Cyber criminals
- Grey Hat Hackers
  - Generally reformed black hat hackers
  - Now working legitimately as security experts
- White Hat Hackers
  - Work as security experts
  - Work within the law
  - “Do no harm”

Attacker Classes

- Elite
  - Highest level – longevity or well-known exploit
- Script Kiddies
  - Youngest and most inexperienced, using tools created by the elite
- Virus Writers
  - Script writers who exploit known vulnerabilities
- Cyber Terrorists
  - Use stenography/cryptography to swap secrets online and commit terrorism
- Disgruntled employees/ ex-employees
  - Feel scorned and work against a company to undermine or steal secrets
- Hacktivists
  - Tend to deface websites, launch DOS attacks, or release secrets to satisfy moral obligation (Anonymous)
- Suicide Hackers
  - Want to take down critical infrastructure, don't care about going to jail
- Hacker Taggers
  - Deface websites to leave a calling card to gain notoriety
- Spy hackers
  - Hired to get through the defenses of a competitor to steal information
- State-sponsored Hackers
  - Hired by the state to attack other governments

Attacker Motivations

- Revenge
  - Disgruntled employees, hacktivists
- Exposure
  - Hacker Taggers
- Hacktivism
  - Hacktivists
- Ego
  - Hacker Taggers
- Monetary Gain
  - Spy hackers, state-sponsored hackers
- Entertainment
  - Hacker Taggers
- Personality Disorder
- Extortion and Exploitation
  - Cyber terrorists, disgruntled employees
- Blackmail
  - Disgruntled employees
- Sabotage
  - Suicide hackers, cyber terrorists, disgruntled employees
- Espionage
  - Spy hackers, state-sponsored hackers



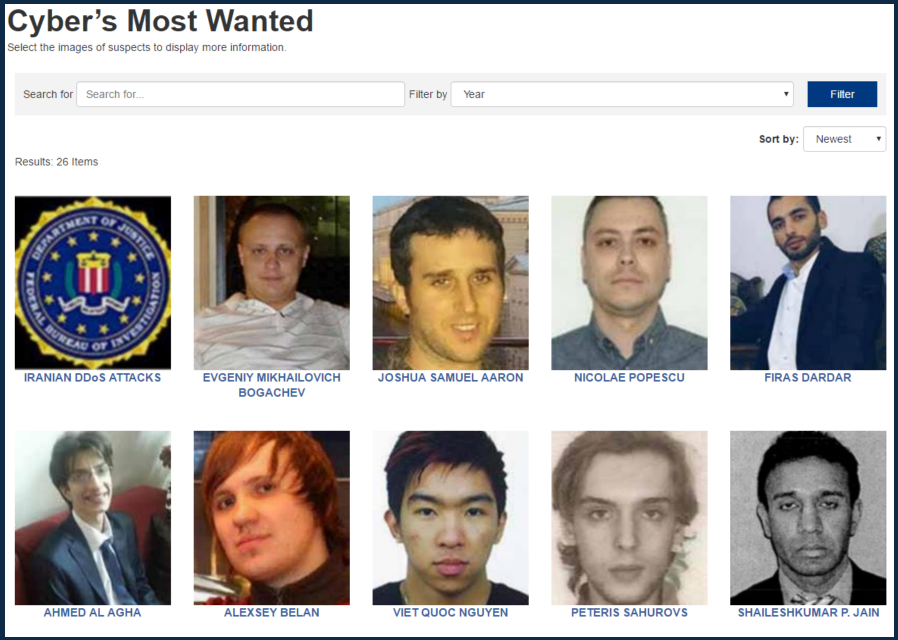
Source: http://kinyohga.weebly.com/internet-safety-blog/cyber-crimes

How do attackers start cybercrime

- Largely based off Will Gragido's book, Blackhatonomics
- Cost of entry into cybercrime
  - Laptop: $199.99 from www.pcexchange.com
  - Wireless connection: free by using www.wififreespot.com/tex.html
  - ZeuS Builder, a crimeware tool for building and configuring a ZeuS bot: $7,000
  - Anonymous proxy service: $102.96 from http://provpnaccounts.com/Buy_VPN_Account-118-articles
  - $7302.95 for a decent kit
  - A kit like this can result in a return on investment of $6,000,000
- Skills needed
  - Social Engineering
    - People are generally trusting
    - 8/10 researchers were able to enter a Fortune 500 company and get on the network with a story
    - UK study: 70% of people gave their computer password to an interviewer in exchange for chocolate
      - 80% offered personal info (mother's maiden name, birthday, etc.)
- Consequences
  - Cybercrime is hard to prosecute
    - Few cybercrime experts in the law enforcement field
    - The law regarding cybercrime is still new and relatively hard to prosecute
    - Cybercriminals are unlikely to be caught, unlikely to be prosecuted, and unlikely to serve full sentences

Future of this project

- Outlining the type of attacks
  - Based on the types of attacks, what is the likely motivation
  - What types of attacks do each category of hacker tend to use
- Categorizing a recent attack
  - Finding a recent attack from the news and attempting to assign possible categorization and motivations based on the type of attack and other details



Source: https://www.fbi.gov/wanted/cyber

References

- E. Koeze and N. Popper, “The Virus Changed the Way We Internet,” 07-Apr-2020. [Online]. Available: https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html. [Accessed: 18-Nov-2020].
- S. Back, J. LaPrade, L. Shehadeh, and M. Kim, “Youth hackers and adult hackers in South Korea: An application of cybercriminal profiling ,” in 2019 IEEE European Symposium on Security and Privacy (EuroS & P), IEEE., 2019, pp. 410–413.
- T. J. Holt, J. D. Freilich, and S. M. Chermak, “Exploring the Subculture of Ideologically Motivated Cyber-Attackers,” *Journal of Contemporary Criminal Justice*, vol. 33, no. 3, pp. 212–233, 2017.
- R. Sabillon, J. Cano, V. Cavaller, and J. Serra, “Cybercrime and Cybercriminals: A Comprehensive Study,” *International Journal of Computer Networks and Communications Security*, vol. 4, no. 6, pp. 165–176, Jun. 2016.
- E. U. Opara and M. T. Hussein, “Cyber Security, Threat Intelligence: Defending the Digital Platform,” *Journal of international technology and information management*, vol. 26, pp. 138–160, Jan. 2017.
- T. J. Holt, R. Leukfeldt, and S. V. D. Weijer, “An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites,” *Criminal Justice and Behavior*, vol. 47, no. 4, pp. 487–505, 2020.
- “Iran at Center of Cyber Crime Charges in Three Cases,” *FBI*, 18-Sep-2020. [Online]. Available: https://www.fbi.gov/news/stories/iran-at-center-of-cyber-crime-charges-in-three-cases-091820. [Accessed: 10-Oct-2020].
- C. Yang, R. Harkreader, J. Zhang, S. Shin, and G. Gu, “Analyzing spammers' social networks for fun and profit,” *Proceedings of the 21st international conference on World Wide Web - WWW '12*, pp. 71–80, Apr. 2012.
- N. Garcia, "The use of Criminal Profiling in Cybercrime Investigations." Order No. 10839020, Utica College, Ann Arbor, 2018.
- A. Kigerl, “Profiling Cybercriminals: Topic Model Clustering of Carding Forum Member Comment Histories,” *Social Science Computer Review*, vol. 36, no. 5, pp. 591–609, 2017.
- E. R. Leukfeldt, E. R. Kleemans, and W. P. Stol, “A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists,” *Crime, Law and Social Change*, vol. 67, no. 1, pp. 21–37, 2016.
- A. Bednarz, “Profiling cyber criminals: A PROMISING BUT IMMATURE SCIENCE.,” *Network World*, vol. 21, no. 48, pp. 46–48, 29-Nov-2004.
- W. Gragido, *Blackhatonomics: an inside look at the economics of cybercrime*. Amsterdam: Syngress, 2013.
- “Data Thieves The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.” 2018.

MOTIVATION AND METHODS OF NORTH KOREA'S CYBER CRIMINALS.

Waylon Jepsen

CYBER CRIME

Unaffiliated Groups

- Hacktivists
- Free acting agents

Nation State Sponsored

- NSA
- Russia
- North Korea

ORIGINS

- In 2009 there was the formation of the Reconnaissance General Bureau by North Korea
- .The Bureau has 8 known departments one of which is Bureau 121 which is responsible for all cyber military campaigns.

FOURTH OF JULY INCIDENT

- The first suspected cyber attack conducted by North Korea was on July 4th, 2009
- Distributed Denial of Service (DDos) attack
- hit an estimated 35 governmental and commercial websites from South Korea and the United States
- botnet is used to target the IP addresses of the victims >15,000 machines
- Master Boot Record wiped and written with 512 bytes "Memory of Independence Day”
- Utilized MyDoom to infect machines.

TEN DAYS OF RAIN

- In March of 2011, exactly 20 months after the Fourth of July Incident
- DDos attack was launched from North Korea
- highly specific targets
- pre-configured attack time of ten days
- Cryptographic diversity
- 14 overlapping targets to 4th of July
- Unclear motivation
- Speculation of North Korean Testing tools

ATTACK AGAINST SOUTH KOREAN NONGHYUP BANK

- result of undisclosed in March 2010 infecting machines
- Of the infected machines pertaining to valuable assets, one was the laptop of an IBM employee who did IT at work at the bank
- The infected laptop gathered classified information about target IP's and system passwords until it was utilized along with other bots to perform a DDos on the banks servers resulting in the destruction of 273 out of the 583 total servers by wiping their Master Boot Records
- The attack prevented the bank from carrying out its services for its 30 million customers until systems were recovered
- Identical IP addresses from 4th of July attack

DARK SEOUL

- March 20, 2013 at 2pm local time South Korean broadcasting companies and financial institutions were the victim of an aggressive cyber attack
- The Trojan used in this attack was compiled on January 26, 2013, and that the tool used to wipe the master boot records was compiled on January 31st
- Similar wiping tool used in the past 3 incidents.
- Spear phishing campaign downloaded the Trojan
- The attack rendered many ATMs across Seoul to be unusable

OPERATIO N TROY

- Title of persistent previous connected attacks
- Operation Troy appeared to have started back in 2009 where spyware had been traced back too.
- The operation was all based on the same code and sequentially attempted to target and infiltrate South Korean targets.
- The operation was called Troy because of the frequent use of the word Troy in the compile path strings.
- Different versions of the Troy Trojan were found to have Dynamic Linked Library(dll) files and when analyzed, produced almost identical signatures.

KIMSUKY OPERATIO N

- In June 2013 detection of spyware was reported by security company Kaspersky labs.
- The victims are the Sejong Institute, a nonprofit private organization leading in security research and international economy; the Korea Institute For Defense Analyses (KIDA); Ministry of Unification; and Hyundai Merchant Marine.
- The attackers utilized Metasploit Framework's open source Win7Elevate allowing them to open a remote command prompt with elevated privileges
- Then the attackers injected the malicious code into explorer.exe
- The executable injected then decrypts the spying library and saves it to disk.
- The infected machines communicate information via the Bulgarian web-based free email server (mail.bg)
- Master emails associated with names "kimsukyang" and "Kim

COMPROMISE OF THE SEOUL SUBWAY SYSTEM

- March of 2014 to August of 2014 threat actors compromised servers
- 5.2 million passengers a day
- Two servers were compromised
- Attack signatures matched Dark Seoul ‘
- Point of infiltration still a mystery

OPERATION BLOCKBUSTE R

- November 24, 2014 "Guardians of Peace" (GOP) hacked Sony Pictures Entertainment
- Cost more than $15 Million USD
- Torrent links were published leaking the films Annie, Mr. Turner and To Write Love on Her Arms collectively downloaded over 100,000 times
- On December 5th SPE received a demand from the GOP not to release the film The Interview
- The FBI indicted North Korea

HACK ON KOREA HYDRO & NUCLEAR POWER

- December 2014, South Korea's nuclear power plant was hacked
- The hack was conducted by a group calling themselves "Who am I = No Nuclear Power"
- Personal employee information as well as technical information about the operation was released
- Workers were spear phished with emails containing the Kimsuky malware
- It was suspected that the goal of this attack was to create civil unrest

COMPROMISE OF SOUTH KOREAN MINISTRY OF NATIONAL DEFENSE

- In August 2016 over 200GB of data was extracted from the defense ministry networks
- Included was stolen information of the US-South Korean military plans in case of a war with North Korea
- There is currently no available technical analysis of this attack.

BANGLADESH BANK HEISTS

- 2016, North Korean Cyber Criminals stole $81 Million Dollars from the Bangladesh International bank
- The attack likely started in 2015 with spear phishing emails.
- 3 separate employees opened the spear phishing emails and at least one maybe more was infected
- Three types of malware:
  - a backdoor into the bank network,
  - an encrypted channel to pull stuff out of the back door,
  - scan and navigate across the banks network
- Exploited Society of Worldwide Interbank Financial Telecommunication (SWIFT)

COMPROMISE OF CRYPTOCURRENCY EXCHANGES IN SOUTH KOREA

- April of 2017, attacks were launched targeting multiple cyptocurrency exchanges in South Korea with the purpose of stealing money
- It was reported by security company that personal information of over 31,000 users was stolen including emails and phone numbers
- The perpetrators then contacted users directly over the phone to conduct social engineering to gain access to the users' funds

WANNACR Y

- May of 2017, a Malware dubbed WannaCry began infecting over 200,000 machines from 150 different countries
- Fake Ransomware
- Eternal Blue which
- Shadow Brokers
- Kill Switch
- Marcus Hutchins found and registered the first kill switch.
- The DOJ indicted North Korean hackers, for WannaCry

TAIWAN FAR EASTERN INTERNATIONAL(TFEI) BANK HEIST

- October 2017 North Korea's Lazarus group stole $60 Million dollars from the Taiwan Far Eastern International Bank
- SWIFT
- Most of the funds had been recovered and two suspects had been arrested in Shri Lanka
- Spear phishing
- Security researchers at fire eye conclude the North Korean Lazarus group is behind this attack

ATTACK OF U.S. ELECTRIC COMPANIES

- October 2017, security company FireEye disclosed a report detailing phishing attacks targeting U.S. Electric Companies
- While no industrial controllers were actually compromised, the attacked raised some serious concerns about the security of Cyber physical Systems where physical resources can be manipulated
- The attack was concluded to be conducted by North Korean sponsored actors the Lazarus group

APT 37 & APT 38

- Advanced Persistent Threat(APT) 37 also known as ScarCruft, Group123 and Reaper is North Korean attack group with primary targets of South Korean, Japan, Vietnam and, the middle East
- APT 38 The Lazarus group is also known as Zinc(by Microsoft), hidden cobra, and whois. The Lazarus group has been tied to almost all swift bank attack heists in the world. They have attempted to steal $1.2 Billion and have been successful in stealing $122 Million. The Lazarus group is known to primarily target financial institutions and have a variety of custom malware families. These malware families include backdoors, tunelers, data miners, and wipers.
- APT 38 has conducted attacks in over 16 organizations and and 11 different countries

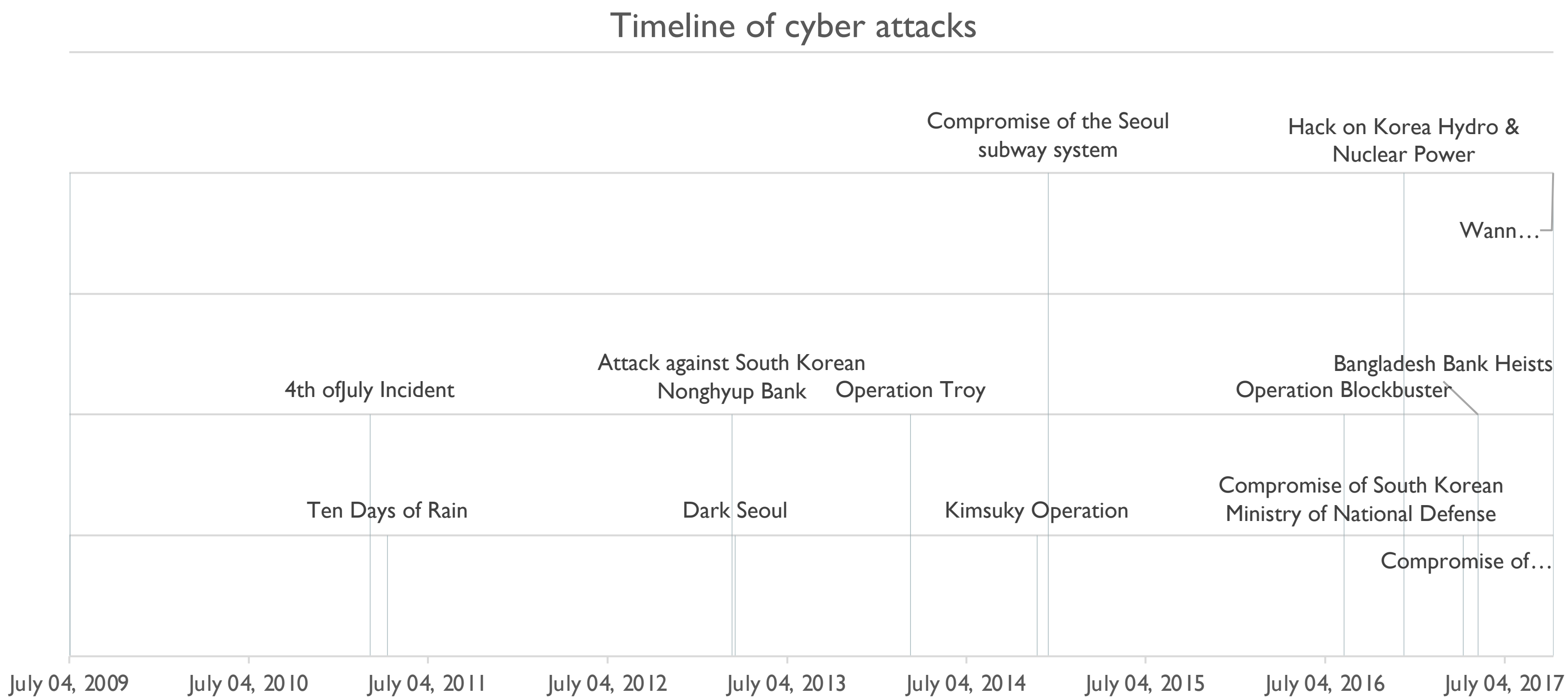
ANALYSIS

Lazarus Group

- Bangladesh bank Heist
- Operation Block Buster
- Attack of U.S. electric companies
- Taiwan Far Eastern International(TFEI) Bank heist

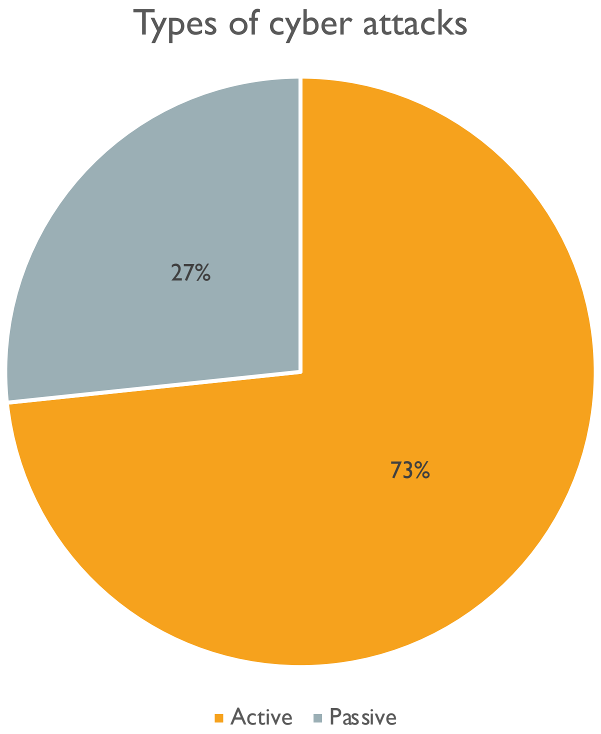
Operation Troy

- Dark Seoul
- 4th of July
- 10 days of rain
- Attack against South Korean Nonghyup Bank



TIMELINE OF NORTH KOREAN CYBER ATTACKS

ATTACK TYPE



Phishing during a Storm:

A Quantitative Examination of Phishing during a Crisis

Luis Rodriguez

Contents

1. Introduction
2. Current Phishing Trends
3. Prevention Models
4. Conclusion

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTRMrbs9hWhXEg3OY3ts7drEmWCZpdJtvvWdg&usqp=CAU

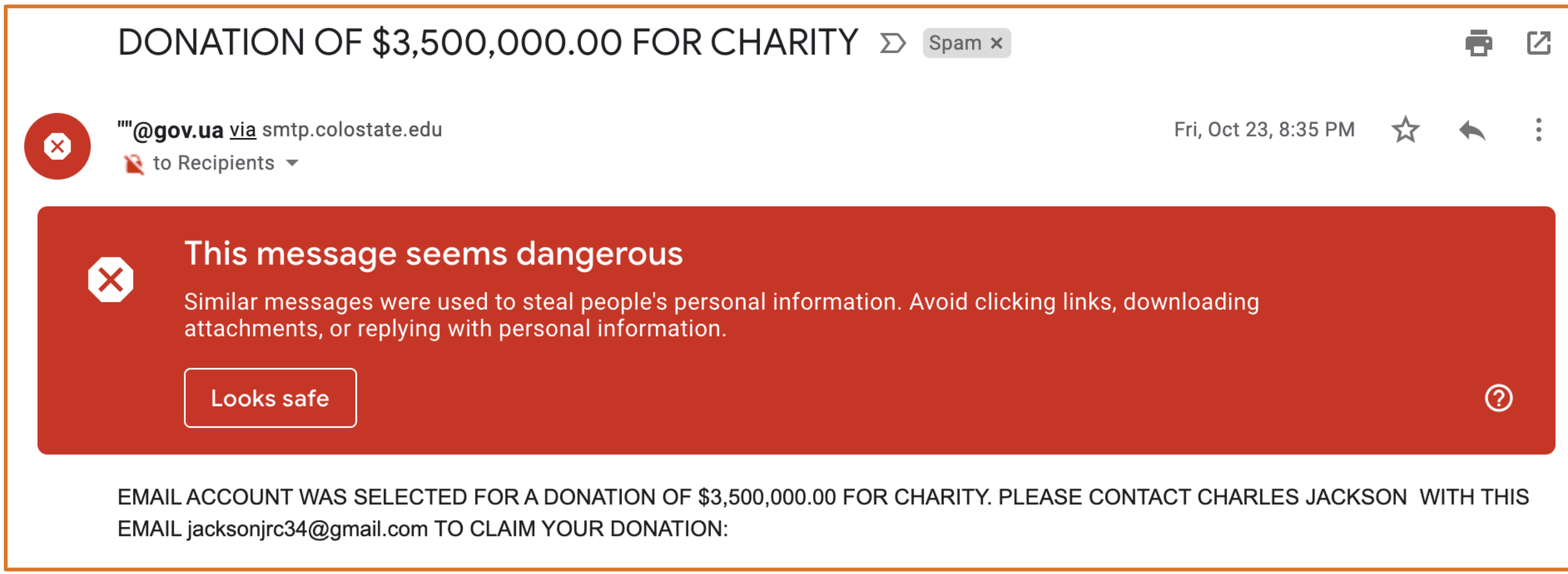
Phishing – What is it?

Social Engineering attack revolving around deceiving a victim into giving personal data/money. [1][2]

Types

- Email Phishing
- Spear-phishing
- Mass Phishing (campaigns)
- Whaling

Phishing (cont.)


DONATION OF $3,500,000.00 FOR CHARITY   Spam ×

""@gov.ua via smtp.colostate.edu   Fri, Oct 23, 8:35 PM
to Recipients

This message seems dangerous

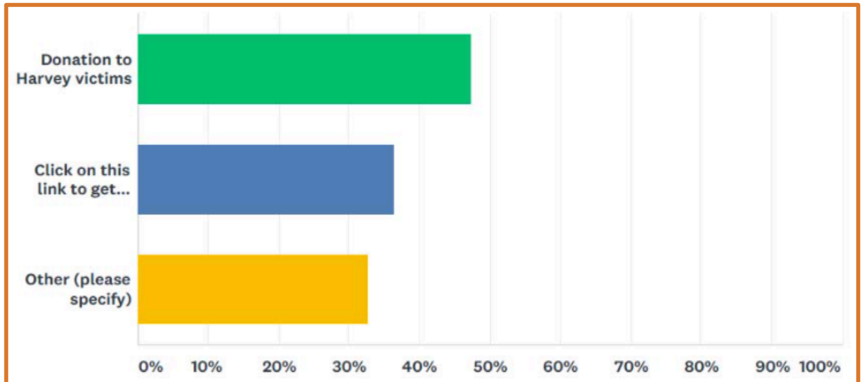
Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe

EMAIL ACCOUNT WAS SELECTED FOR A DONATION OF $3,500,000.00 FOR CHARITY. PLEASE CONTACT CHARLES JACKSON WITH THIS EMAIL jacksonjrc34@gmail.com TO CLAIM YOUR DONATION:

Phishing in a Crisis

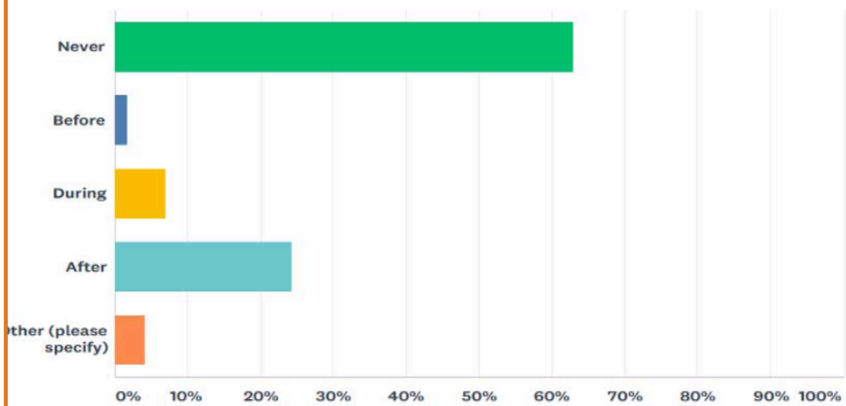
- "Ambulance" phishing
  - Exploiting disaster/pandemic victims with promise of relief
- Hurricane Harvey study indicate increases in phishing attempts after a natural disaster [3]
  - 10.72% of respondents were badly affected by disaster
  - Only 6.3% of respondents clicked links they wouldn't have in normal circumstances
- A set of nine questions given to University of Houston students, faculty, and staff after hurricane
- Multitude of emails based around FEMA support



ANSWER CHOICES	RESPONSES	
Donation to Harvey victims	47.35%	116
Click on this link to get help	36.33%	89
Other (please specify)	32.65%	80
Total Respondents: 245		

Q9) Were there new examples of attacks that you haven't seen before?

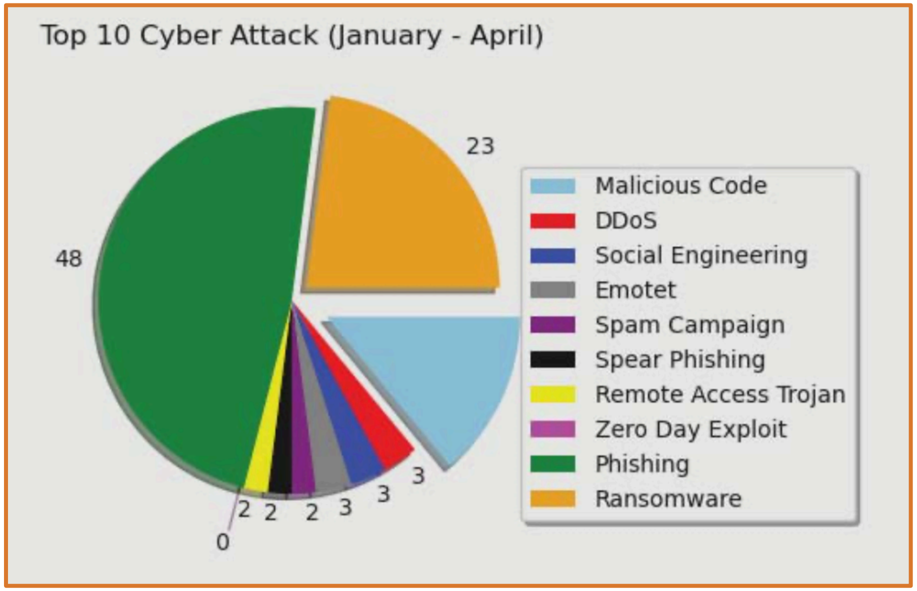
Q4) When did you get any spam regarding
the hurricane (select all that apply)?

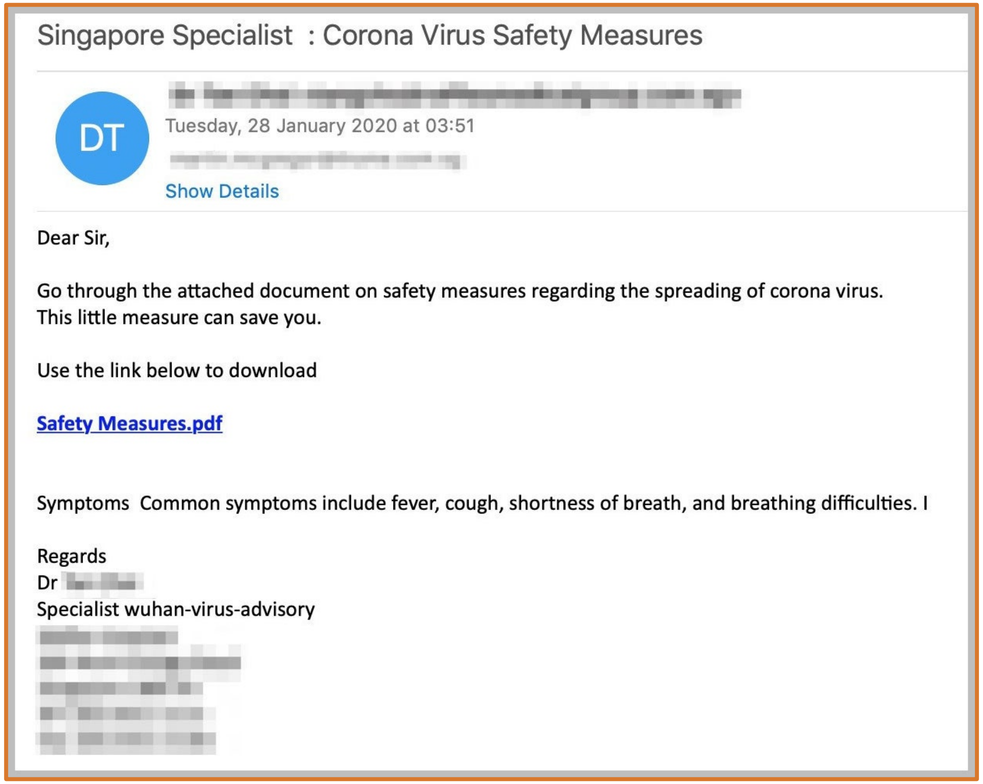


ANSWER CHOICES	RESPONSES	
Never	62.97%	199
Before	1.58%	5
During	6.96%	22
After	24.37%	77
Other (please specify)	4.11%	13
TOTAL		316

Phishing in a Crisis (cont.)

- Mandal and Khan display susceptibility increases from the transition to online [6]
  - 1.2 billion students, faculty and staff member have come online
  - Dependent on conferencing and remote access applications
    - “Zoom-bombing” [7]
- The most prominent attack in the first four month of 2020 were phishing [4]





Singapore Specialist : Corona Virus Safety Measures

Tuesday, 28 January 2020 at 03:51

Show Details

Dear Sir,

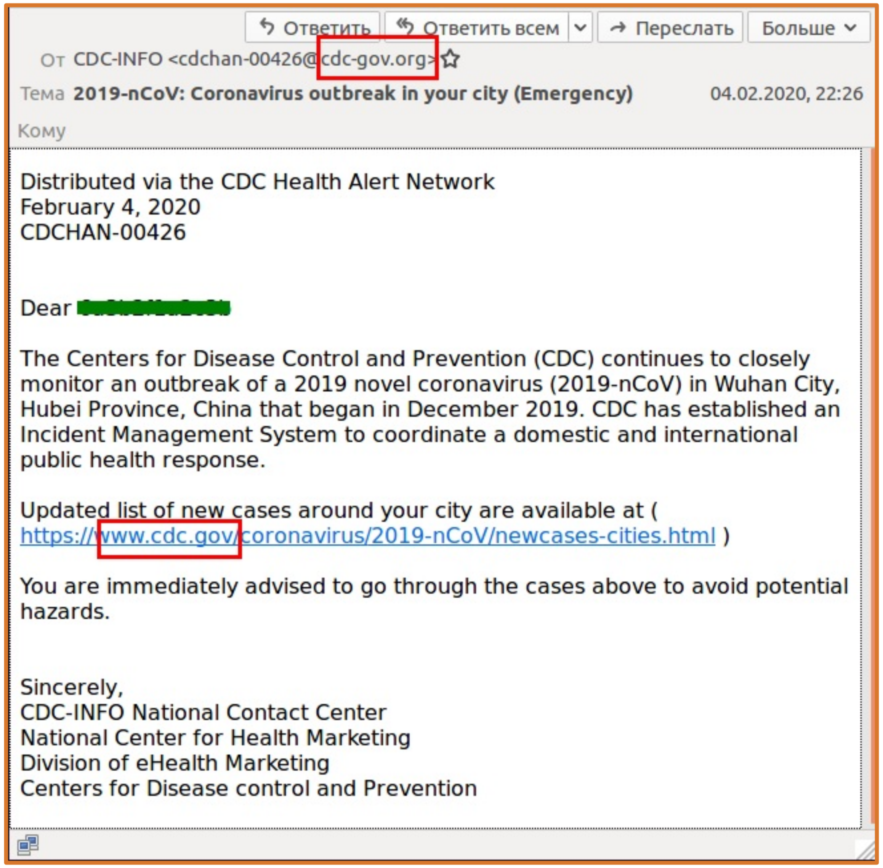
Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

[Safety Measures.pdf]

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr
Specialist wuhan-virus-advisory



Ответить | Ответить всем | Переслать | Больше

От CDC-INFO <cdchan-00426@cdc-gov.org>
Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26
Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

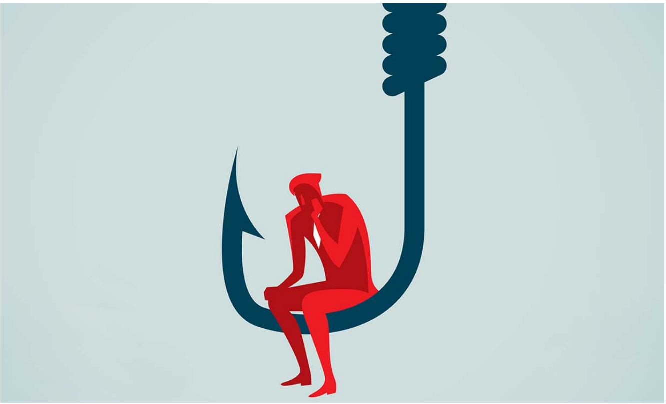
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

Phishing Trends

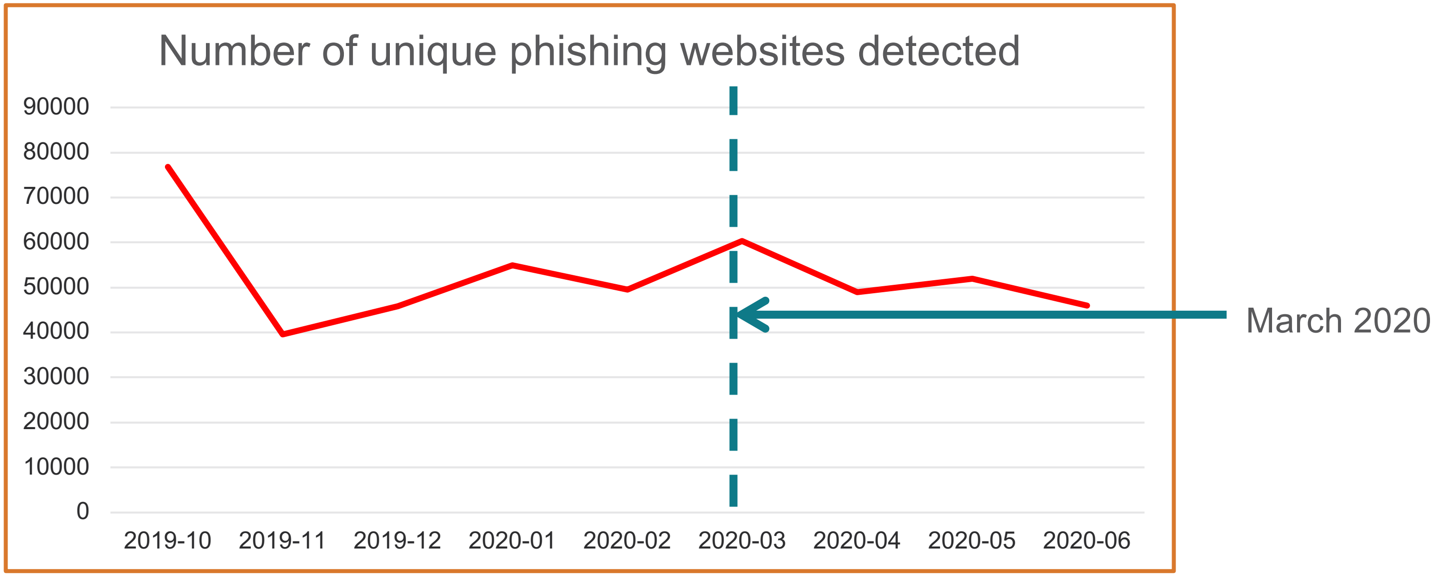


Anti-Phishing Working Group (APWG) gathers data every year on phishing trends

Spikes in data

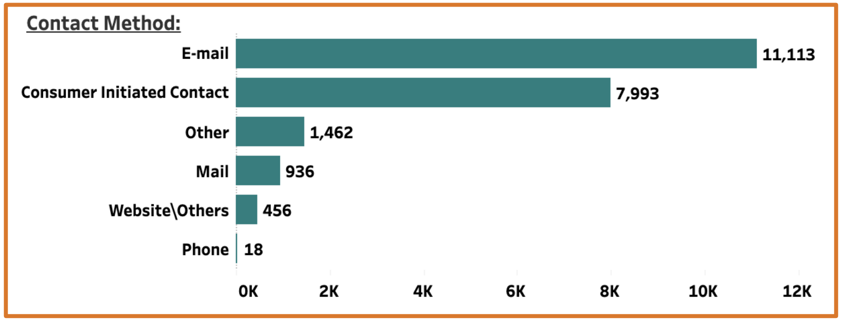
- COVID-related unique phishing emails around March 8 [2][4]
- Number of unique phishing sites around March 2020

Phishing Trends (cont.)

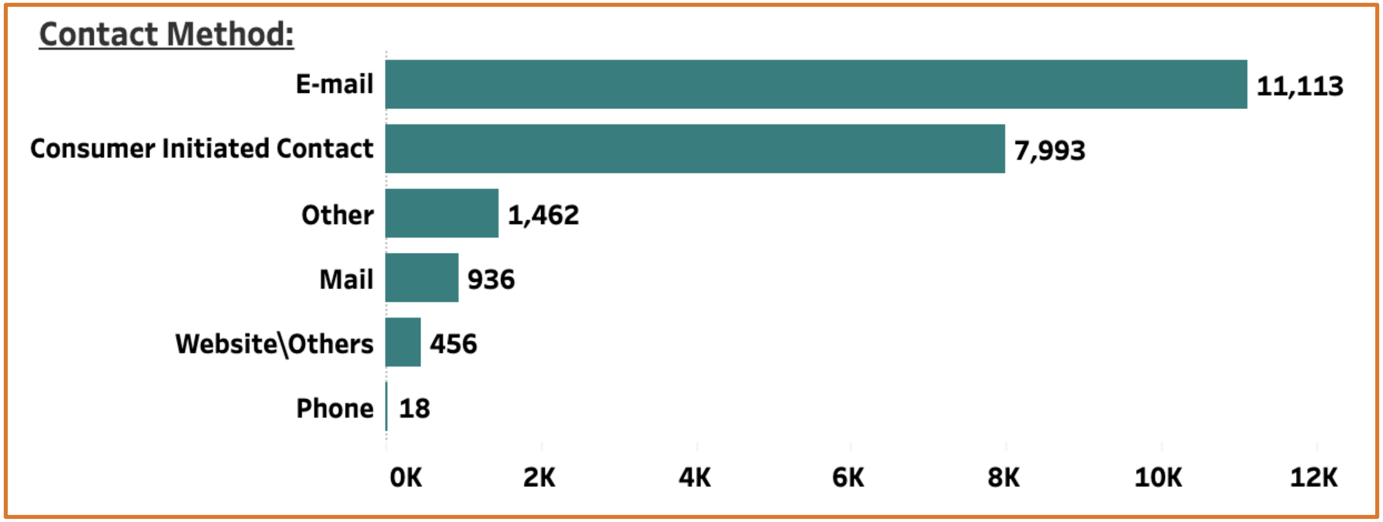


Phishing Trends (cont.)

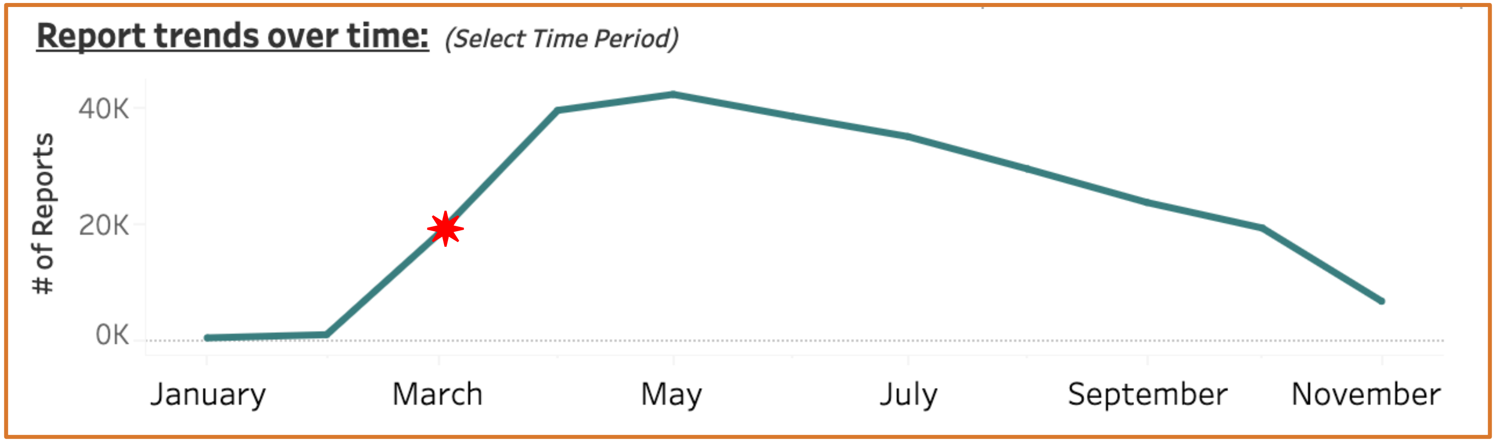
- Federal Trade Commission (FTC) report on COVID-19 and Stimulus related scam
  - **50.5%** of successful pandemic scams initially contacted by email
  - **$182.92M** in total reported losses
- Large number of COVID-19 and stimulus relief related incidents [4][5]



Phishing Trends (cont.)



Phishing Trends (cont.)



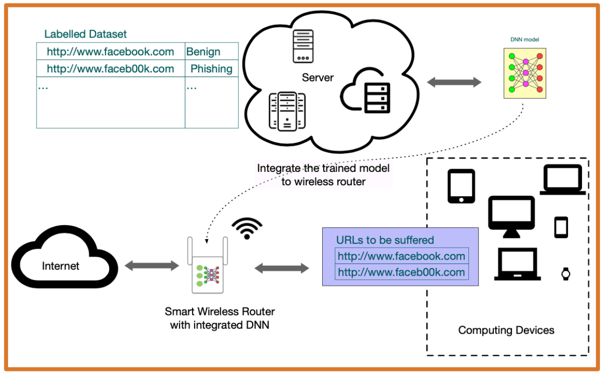
Anti-Phishing Models

- Lightweight
- Client-side preferred
- Handle URLs and/or HTML webpages

Wei et al.'s Phishing Sensor

Results

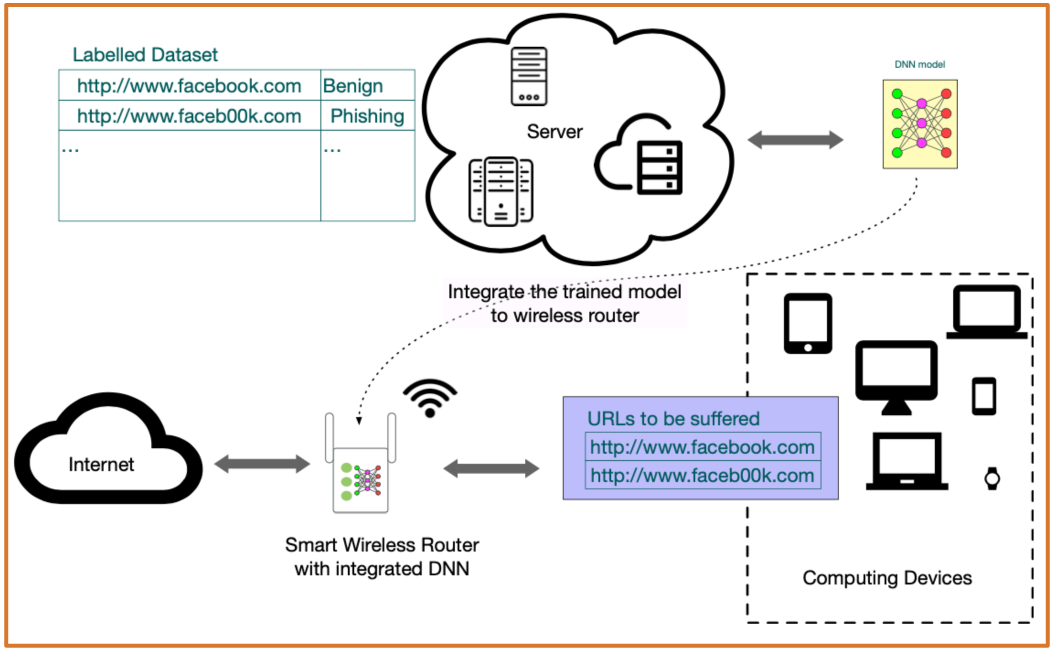
- 86.630% accuracy from DNN model
- ~108 ms in execution times for DNN inference



Details

- Embeddable to smart routers and resource constrained devices

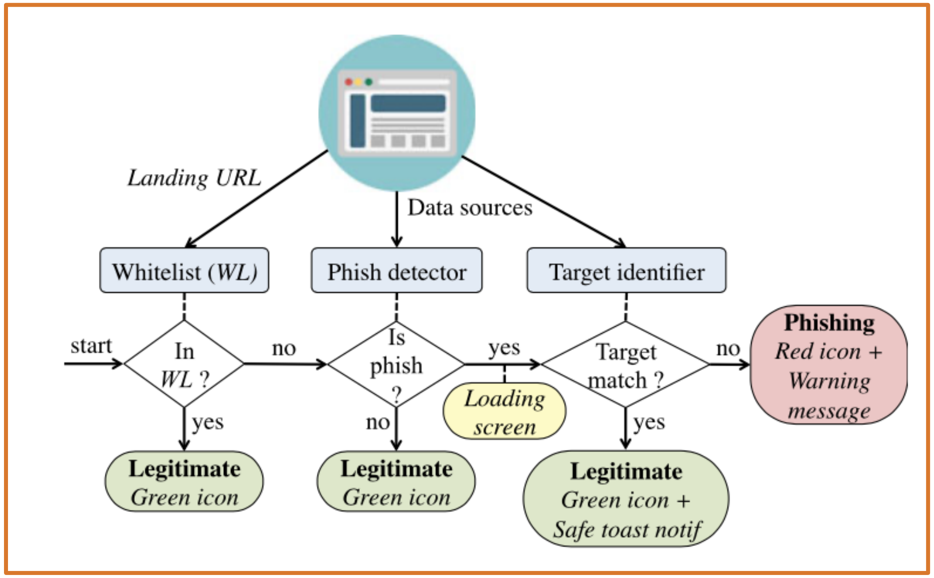
Wei et al.'s Phishing Sensor (cont.)



Off-the-Hook

Results

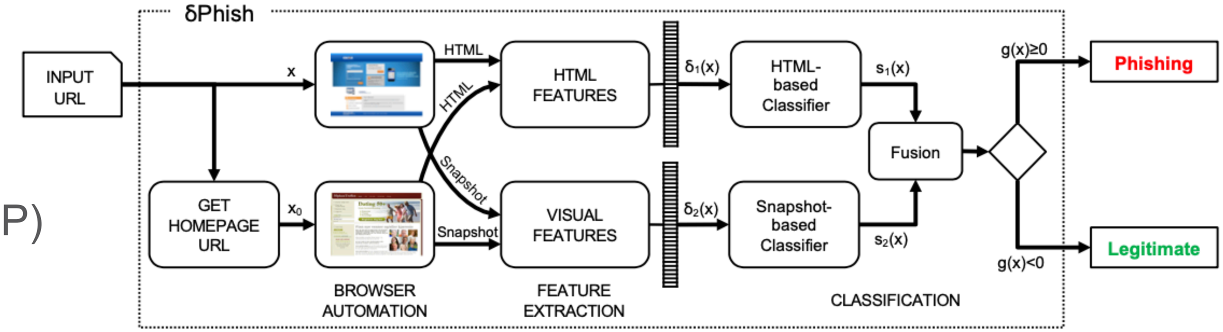
- 90-97% accuracy
- Consists of detector & target identifier



Details

- Lightweight, client-based
  - Can run on simple Raspberry Pi devices
  - Advertised as browser extension

DeltaPhish



Results

- HTML: 97% accuracy (TP)
  - 0.5% FP
- Snapshot: ~80%
  - 1% FP

Details

- HTML and visual based classification
- Implemented on modern personal computer specs

Conclusion

- Light weight, client-side-only models needed
- Education for most vulnerable groups
  - Help lower success rate
- Invest in security in wake of increased attacks

References

1. Qabajeh, F. Thabtah, and F. Chiclana, “A recent review of conventional vs. automated cybersecurity anti-phishing techniques,” Computer Science Review, vol. 29, pp. 44–55, Aug. 2018, doi: 10.1016/j.cosrev.2018.05.003.
2. Datto, How to Recognize and Protect Against Phishing Attacks, Channel Futures Nov. 2, 2020. Accessed on: Nov. 5, 2020. [web] Available: https://www.channelfutures.com/from-the-industry/how-to-recognize-and-protect-against-phishing-attacks
3. R. Verma, D. Crane, and O. Gnawali, “Phishing During and After Disaster: Hurricane Harvey,” in 2018 Resilience Week (RWS), Denver, CO, Aug. 2018, pp. 88–94, doi: 10.1109/RWEEK.2018.8473509.
4. Federal Trade Commission, “COVID-19 and Stimulus Reports,” Accessed on Nov. 12, 2020. Available: https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/Map.
5. “IRS warns of new COVID relief phishing scam,” TristateHomepage.com. Nov. 6, 2020. Accessed on: Nov 6, 2020. [web] Available: https://www.tristatehomepage.com/news/national-news/irs-warns-of-new-covid-relief-phishing-scam/
6. S. Mandal and D. A. Khan, “A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic,” in 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, Sep. 2020, pp. 837–842, doi: 10.1109/ICOSEC49089.2020.9215374.

References (cont.)

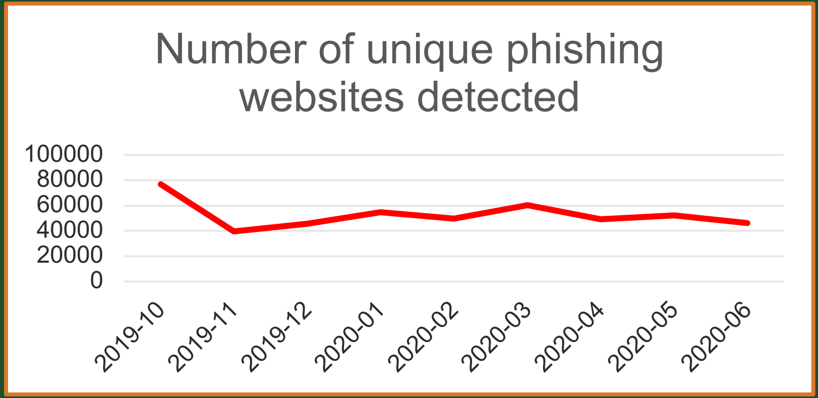
6. L. O'Donnell, "Ransomware And Zoom-Bombing: Cyberattacks Disrupt Back-to-School Plans," ThreatPost. Sept. 10 2020. Accessed on Sept. 10, 2020. Available: https://threatpost.com/ransomware-zoom-cyberattacks-school/159093/
7. "COVID-19 Related Cyber Attacks", ITCSecure. April 1, 2020. Accessed on Nov. 10, 2020. Available: https://itcsecure.com/covid-19-related-cyber-attacks/
8. I. Corona et al., "DeltaPhish: Detecting Phishing Webpages in Compromised Websites," arXiv:1707.00317 [cs], Jul. 2017, Accessed: Nov. 16, 2020. [Online]. Available: http://arxiv.org/abs/1707.00317.
9. S. Marchal, G. Armano, T. Grondahl, K. Saari, N. Singh, and N. Asokan, "Off-the-Hook: An Efficient and Usable Client-Side Phishing Prevention Application," IEEE Trans. Comput., vol. 66, no. 10, pp. 1717–1733, Oct. 2017, doi: 10.1109/TC.2017.2703808.
10. B. Wei et al., "A Deep-Learning-Driven Light-Weight Phishing Detection Sensor," Sensors, vol. 19, no. 19, p. 4258, Sep. 2019, doi: 10.3390/s19194258.

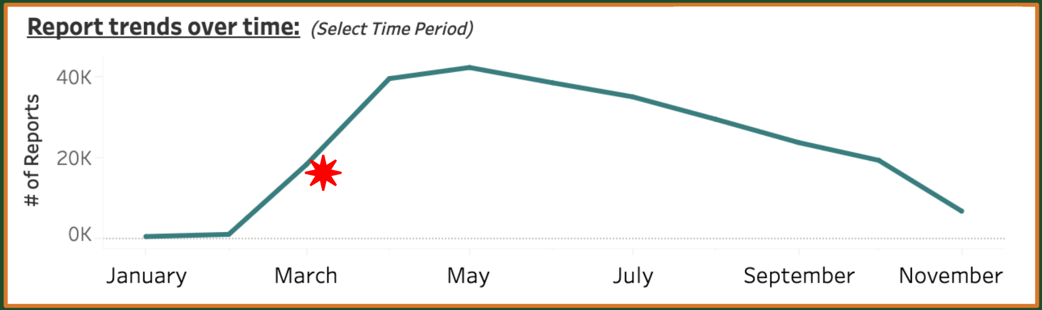
Thank you

Colorado State University

Questions?

Thank you





Colorado State University