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
• Please be very cautious. New Covid-19 cases in Colorado.
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*
Final report (8-12 pages, submit using Canvas/\texttt{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
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

References


Thank you
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)
  - Majority Voting (MV)

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
Extend experiments in [21] to deep ANNs

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

- **Data**

<table>
<thead>
<tr>
<th>Name</th>
<th>Training Data</th>
<th>Testing Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOTO</td>
<td>Original</td>
<td>Original</td>
</tr>
<tr>
<td>TOTS</td>
<td>Original</td>
<td>Synthetic</td>
</tr>
<tr>
<td>TOSTO</td>
<td>Original &amp; Synthetic</td>
<td>Original</td>
</tr>
<tr>
<td>TOSTS</td>
<td>Original &amp; Synthetic</td>
<td>Synthetic</td>
</tr>
</tbody>
</table>

- **Model Configurations**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>Model Search on Original Training Data</td>
</tr>
<tr>
<td>M2</td>
<td>Model Search on Synthetic Training Data</td>
</tr>
</tbody>
</table>
ANNs With Synthetic Data [3/7]

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

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

- 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)**  
**ANN Phishing Performance**

- **Value**

- **TOTO**
  - Accuracy: Blue
  - F1 Score: Red
  - AUC: Orange

- **TOTS**
  - Accuracy: Blue
  - F1 Score: Red
  - AUC: Orange

- **TOSTO**
  - Accuracy: Blue
  - F1 Score: Red
  - AUC: Orange

- **TOSTS**
  - Accuracy: Blue
  - F1 Score: Red
  - AUC: Orange

**B)**  
**Decrease and Recovery**

- **Score**

- **Accuracy**: Decrease = TOTS – TOTO
  - Recovery = TOSTO – TOTS

- **F1**: Decrease
  - Recovery

- **AUC**: 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
Adversarial Phishing Detection F1 Score

By Classifier Type

<table>
<thead>
<tr>
<th>Model</th>
<th>TOTO</th>
<th>TOTS</th>
<th>TOSTO</th>
<th>TOSTS</th>
<th>Decr</th>
<th>Recov</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANN</td>
<td>0.974</td>
<td>0.799</td>
<td>0.964</td>
<td>0.929</td>
<td>0.289</td>
<td>0.285</td>
</tr>
<tr>
<td>GNB</td>
<td>0.84</td>
<td>0.37</td>
<td>0.65</td>
<td>0.82</td>
<td>0.48</td>
<td>0.47</td>
</tr>
<tr>
<td>GB</td>
<td>0.98</td>
<td>0.36</td>
<td>0.96</td>
<td>0.92</td>
<td>0.48</td>
<td>0.47</td>
</tr>
<tr>
<td>MV</td>
<td>0.96</td>
<td>0.39</td>
<td>0.93</td>
<td>0.92</td>
<td>0.57</td>
<td>0.54</td>
</tr>
<tr>
<td>SVML</td>
<td>0.93</td>
<td>0.45</td>
<td>0.93</td>
<td>0.91</td>
<td>0.47</td>
<td>0.37</td>
</tr>
<tr>
<td>SVMG</td>
<td>0.93</td>
<td>0.45</td>
<td>0.93</td>
<td>0.91</td>
<td>0.62</td>
<td>0.58</td>
</tr>
</tbody>
</table>

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?
Developing optimal models using adversarial synthetic data:

- Improves performance
- Makes more robust models
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).


References [2/2]


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

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

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](http://www.pcexchange.com)
  - Wireless connection: free by using [www.wififreespot.com/tex.html](http://www.wififreespot.com/tex.html)
  - ZeuS Builder, a crimeware tool for building and configuring a ZeuS bot: $7,000
  - $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

- “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
• 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.
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.
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 bank's 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
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.
• 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.
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
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
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
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.
• 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)
April of 2017, attacks were launched targeting multiple cryptocurrency 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.
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
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 a North Korean attack group with primary targets of South Korean, Japanese, Vietnamese, and Middle Eastern countries.

- APT 38, also known as Zinc (by Microsoft), Hidden Cobra, and Whois, has been linked to almost all Swift bank heists in the world. They attempted to steal $1.2 billion and were successful in stealing $122 million. The Lazarus group primarily targets financial institutions and uses a variety of custom malware families, including backdoors, tunelers, data miners, and wipers.

- APT 38 has conducted attacks in over 16 organizations 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 cyber attacks

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 04, 2009</td>
<td>4th of July Incident</td>
</tr>
<tr>
<td>July 04, 2010</td>
<td>Ten Days of Rain</td>
</tr>
<tr>
<td>July 04, 2011</td>
<td>Attack against South Korean Nonghyup Bank</td>
</tr>
<tr>
<td>July 04, 2012</td>
<td>Operation Troy</td>
</tr>
<tr>
<td>July 04, 2013</td>
<td>Dark Seoul</td>
</tr>
<tr>
<td>July 04, 2014</td>
<td>Kimsuky Operation</td>
</tr>
<tr>
<td>July 04, 2015</td>
<td>Compromise of South Korean Ministry of National Defense</td>
</tr>
<tr>
<td>July 04, 2016</td>
<td>Hack on Korea Hydro &amp; Nuclear Power</td>
</tr>
<tr>
<td>July 04, 2017</td>
<td>Compromise of...</td>
</tr>
</tbody>
</table>

TIMELINE OF NORTH KOREAN CYBER ATTACKS
ATTACK TYPE

Types of cyber attacks

- Active: 73%
- Passive: 27%
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
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

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

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
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)?
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]
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.

Regards
Dr
Specialist wuhan-virus-advisory

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

Dear [name]

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.)

Number of unique phishing websites detected

March 2020
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.)

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail</td>
<td>11,113</td>
</tr>
<tr>
<td>Consumer Initiated Contact</td>
<td>7,993</td>
</tr>
<tr>
<td>Other</td>
<td>1,462</td>
</tr>
<tr>
<td>Mail</td>
<td>936</td>
</tr>
<tr>
<td>Website/Others</td>
<td>456</td>
</tr>
<tr>
<td>Phone</td>
<td>18</td>
</tr>
</tbody>
</table>
Phishing Trends (cont.)

Report trends over time: (Select Time Period)
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


Thank you
Questions?

Thank you