Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS559

Quick Research Presentations Tu b

CSU Cybersecurity Center
Computer Science Dept

Tuesday

- Everyone must participate
  - Share questions/comments
  - Take notes
- Presenters: limit yourself to 5 minutes, 1 minute for q/c
  - Upload your slides and be ready to present
- Ujwal will run videos/presentations by some distance students
- The Peer Review Form (Canvas Assignments) due on Sat. Novelty/ Interest, Technical/ Research, Presentation

Presentations Today

T1 Quant. modeling of impact of availability of patches,
Katherine Haynes

T6 Quant. Relationship between Cost of security improvements and the degree of additional security level achieved,
Brett Mulligan

T4 Mitre ATT&CK framework,
Saja Alqurashi,
Suraj Eswaran
Shwetha Gowdanakatte

T12 Economics of ransomware
Jacinda Li
Upakar Paudel
Md Al Amin

T11 Quant. examination of phishing
Qingyi Zhao
Tony Shang
Shree Harini Ravichandran

Analyze the Economics of Ransomware from Different Perspectives

Jacinda Li

CS559

The history and economic status of ransomware

- **In 2005, GPCoder and Archievus**
- **In 2013-2015, CryptoLocker**

In 2009-2012, Vundo

In 2016-Now, CryptoWall and Cryptoworm

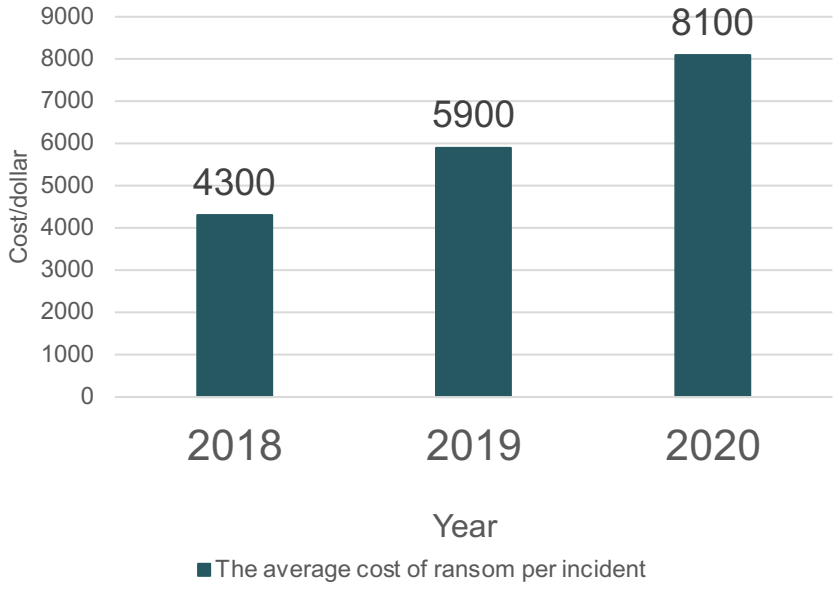


Figure 1: The average cost of ransomware per incident in 2020[1].

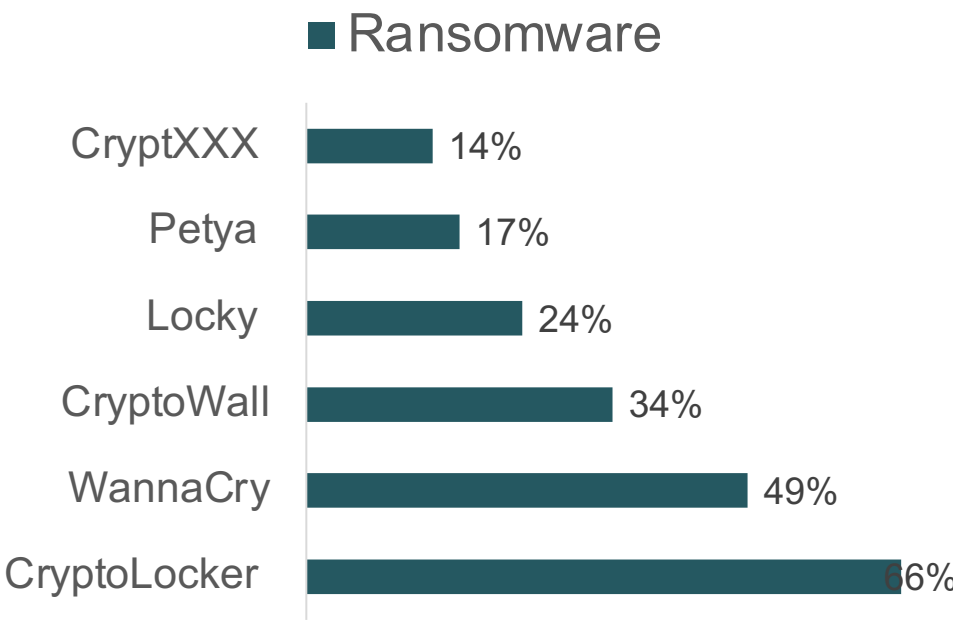


Figure 2: Most common types of ransomware attacks in 2020[3].

The Criminal Perspective

- ***Uniform Price***

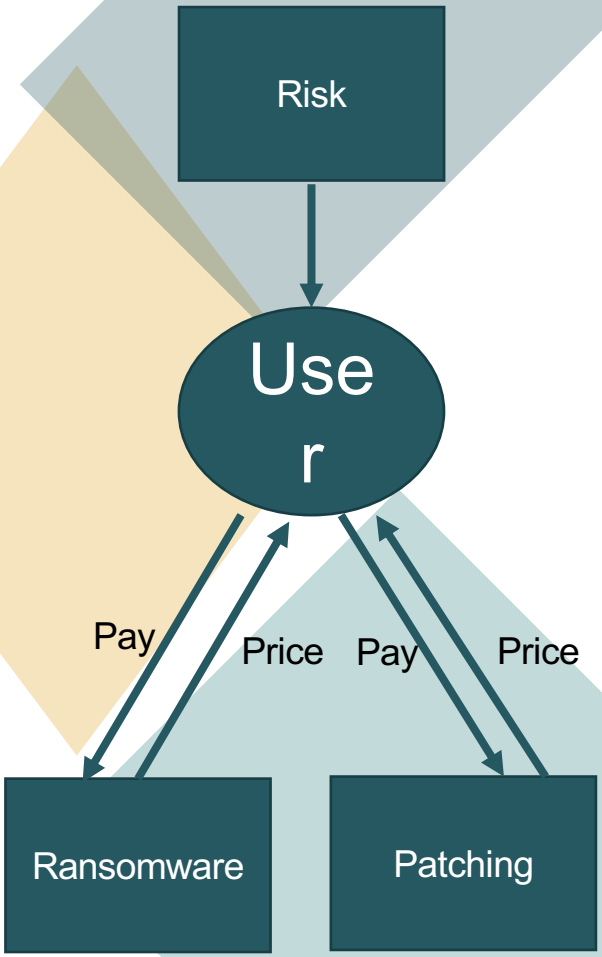
- Set the ransom price
- Set an expected profit
- Use valuation requirements to change the trial price
- Obtain a higher price

- ***Price Discrimination***

- On willingness to pay (WTP)
- The ransom pricing will become more personalized

The Computer User Perspective

- Situation:
- The potential losses are large and the risks are high
- The potential risk is low and the ransom demand is low enough
- A low risk estimate for their computer and have not purchased a patch
- **Conclusion:**
- **Under the most suitable pricing, the patch pricing is balanced in the computer market.**
- **Users at moderate risk are more likely to pay a ransom [1].**
- The above situation is based on the user after the ransom payment, the criminal will provide the key as promised [1].



Software Vendor Perspective

- According to the research from the Journal of Cybersecurity, Software vendors are constantly checking for bugs and posting patches on their web sites [6].
- Social welfare
- In addition, when risk valuations are high, vendors tend to set software prices much lower [6].

Conclusion

- **(1) The criminal perspective.**
- **(2) The computer user perspective.**
- **(3) Software vendor perspective.**

- **Harm of Future**
- Self-driving cars,
- Daily life, and so on
- Ransomware may use SQL injection to encrypt databases on web servers

- **Suggestion**
- Unsolicited emails
- Phishing sites
- Update software on time

Thanks.

REFERENCES

[1] J. Hernandez-Castro , E. Cartwright , A. Stepanova
" Economic Analysis of Ransomware, " School of Computing, Cornwallis South, University of Kent, UK. [Online] Available:https://ssrn.com/abstract=2937641

[2] Y. Fareed Fahmy Bayoumy, P. Hakon Meland, G. Sindre1,
" A Netnographic Study on the Dark Net Ecosystem for Ransomware," Norwegian University of Science and Technology, Trondheim, [Online] Available: https://ieeexplore.ieee.org/document/8551424

[3] Technical Marketing Team,"Ransomware: Past, Present, and Future,". Trend Labs Ransomware Roundup [Online]. Available: https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf

[4] J. Hernandez-Castro1, A. Cartwright2 and E. Cartwright3 (2019).
" An economic analysis of ransomware and its welfare consequences,", Conf. Royal Society Open Science ISSN: 2054-5703 [Online] *Available:* https://doi.org/10.1098/rsos.190023

[5] T. August, D. Dao, S. Laube, & M.F. Niculescu, (2017). Economics of Ransomware Attacks. Conf. Rady School of Management, University of California, Vol. 65, Issue 11: 1009-1015(2020) [Online] Available:https://doi.org/10.1360/TB-2020-0159

[6] M. Paquet-Clouston1, B. Haslhofer, B. Dupont,
" Ransomware payments in the Bitcoin ecosystem," J. Journal of Cybersecurity, 2019, Vol.5. [Online] Available: https://doi.org/10.1093/cybsec/tyz003

Economics of Ransomware

Upakar Paudel

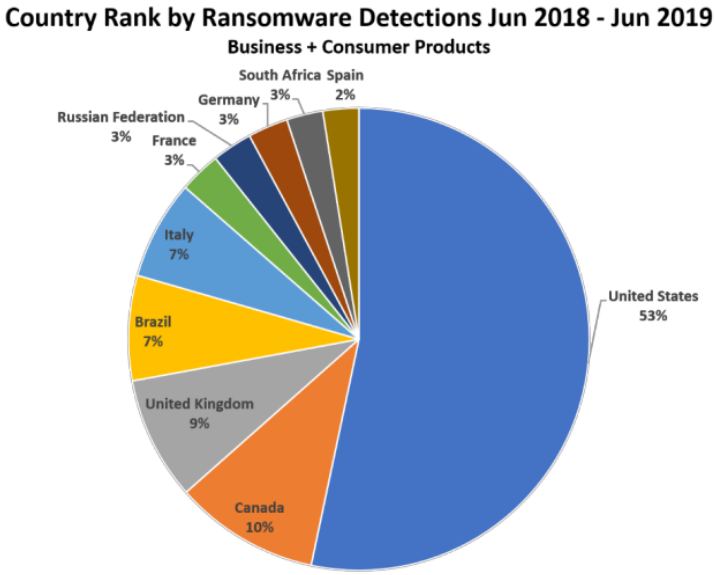
Colorado State University

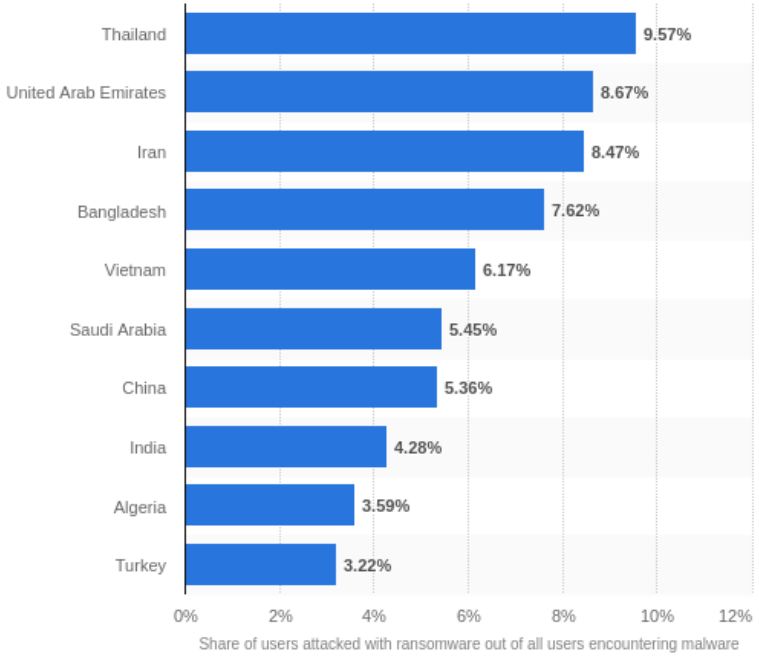
Introduction

- Encrypts victim file and then ask for ransom to access it
- Introduced by Adam Young and Prof. Moti Yung from Columbia University
- After advent of cryptolocker, in around 2013, ransomware industry surged
- Various other families of ransomware like TeslaCrypt, CryptoWall, Cerber etc

Current Scenario

- Victim's system are mostly infected by phishing or some social engineering
- Bitcoin proved as a strong tool for ransomware attackers to perform financial transaction


Country Rank by Ransomware Detections Jun 2018 - Jun 2019
Business + Consumer Products
South Africa 3%
Spain 2%
Germany 3%
Russian Federation 3%
France 3%
Italy 7%
Brazil 7%
United Kingdom 9%
Canada 10%
United States 53%


Thailand 9.57%
United Arab Emirates 8.67%
Iran 8.47%
Bangladesh 7.62%
Vietnam 6.17%
Saudi Arabia 5.45%
China 5.36%
India 4.28%
Algeria 3.59%
Turkey 3.22%
0%
2%
4%
6%
8%
10%
12%
Share of users attacked with ransomware out of all users encountering malware

Economics of Ransomware

- Uniform Pricing
- Price Discrimination
- Bargaining
- Determinants of Willingness to Pay

Thank you

Colorado State University

Economics of Ransomware

MD AL AMIN

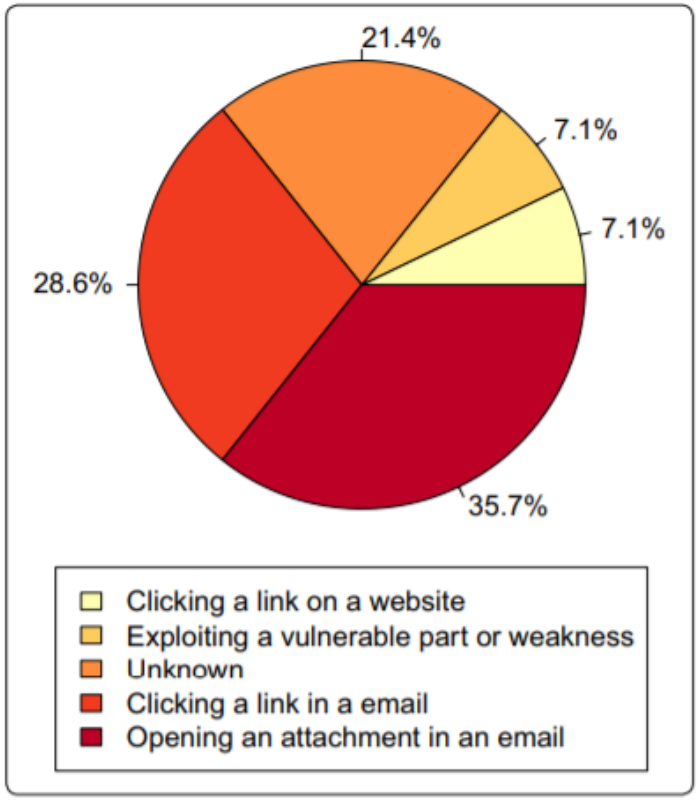
CS-559: Quantitative Security, Fall-2020

Colorado State University

Abstract

Ransomware attacks are increasing yearly. Ransomware threat agents infect the victims' machines through malicious email links, email attachments, website links, exploiting system vulnerabilities, etc. Government offices, financial, and business organizations are the main targets of the ransomware attacks. Since the government offices process and contain sensitive information, which is the national security concern. Financial and business organizations run business, store customers data, and generate revenue. These organizations are very inclined to pay the ransom money. After a ransomware attack, to overcome the challenges, we must consider many factors. However, these vary depending on the attack's impact and whether it was against an organization or individual. **Loss of money**, **Loss of Reputation**, **Theft of Identity**, and others are the significant effects of ransomware attacks. Many organizations tried to recover data without paying ransom money. In those cases, organizations spent huge money than the ransom money. Most of the victims recovered data from backup data and using supporting tools. Recover of data paying ransom money is very small. After spending ransom money, only 92% of data are recovered with decryptor, and 8%v are lost forever. Bitcoin is used by 99% attackers to receive the ransom money and 1% by other cryptocurrencies.

Ransomware Infection Vectors [1]



Ransomware Attacks Campaigns [2-3]

Campaigns	Year	Campaigns	Year
Reveton	2012	Locky	2016
CryptoLocker	2013	TowerWeb	
Globe		CryptoXXX	
CryptoLocker.F	2014	JigSaw	
Crypto Defense		Flyper	
TorrentLocker		WannaCry	2017
CryptoWall		Petya	
Teslacrypt	2015	Bad Rabbit	
DMA Locker		Syskey	
Fusob		Samsam	2018

1. G. Hull, H. John, and B. Arief, "Ransomware deployment methods and analysis: views from a predictive model and human responses," *Crime Sci.*, vol. 8, no. 1, p. 2, 2019.
2. A. Zimba and M. Chishimba, "On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems," *Eur. J. Secur. Res.*, vol. 4, no. 1, pp. 3–31, 2019.
3. M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the bitcoin ecosystem," *J. Cybersecurity*, vol. 5, no. 1, p. tyz003, 2019.

Notable Paid Ransomware Incidents [1]

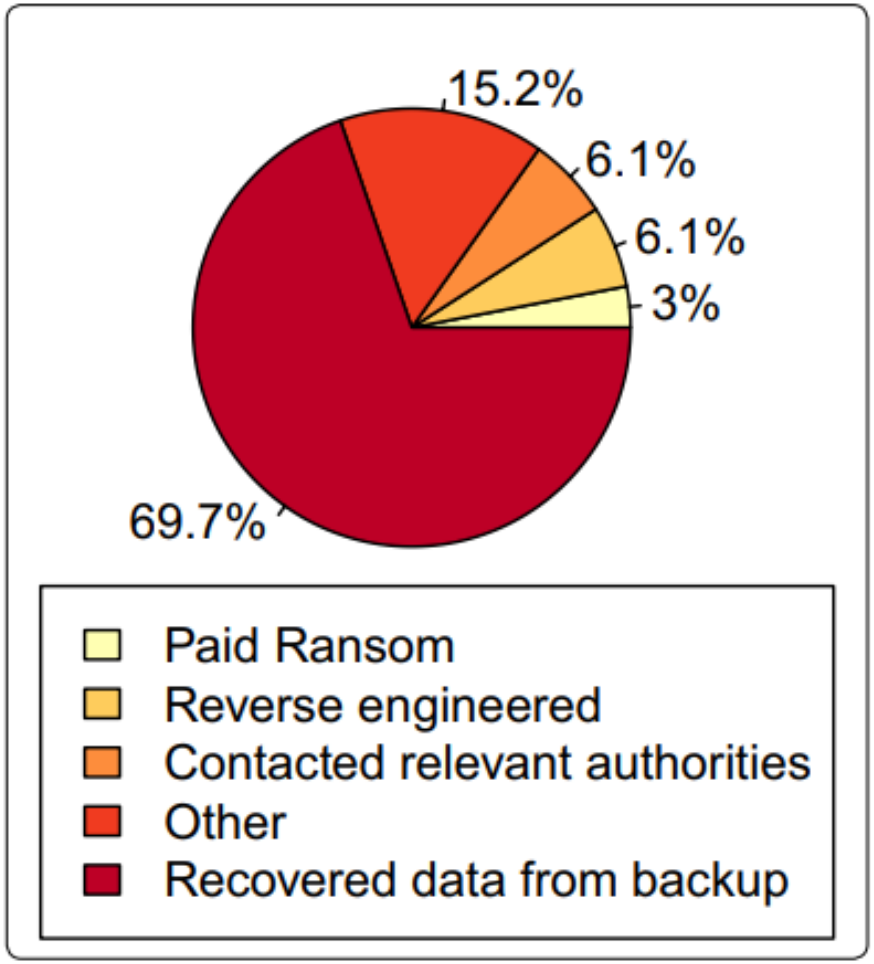
Victim	Economic sector	Campaign	Infection vector	Amount paid	Period
Nayana (Chirgwin 2017)	ICT services	Erebus	EK	$1.01 million	June 2017
Hancock Health (Snell 2018)	Health	SamSam	RDP	$55,000	January 2018
Los Angeles Community College District (Pauli 2017)	Education	Undisclosed	Undisclosed	$28,000	January 2017
University of Calgary (CBS News 2016)	Education	Undisclosed	Undisclosed	$28,000	June 2016
Hollywood Presbyterian Medical Center (Bisson 2016)	Health	Locky	Email	$17,000	February 2016

Financial Losses due to Recovery Efforts and Loss of Production [1]

Victim	Economic sector	Campaign	Infection vector	Ransom demand	Estimated recovery cost	Period
City of Atlanta	Government	SamSam	RDP	$50,000	$3 million	March 2018
Merck	Health	NotPetya	EK	$50,000	$310 million	June 2017
Colorado transp. dept.	Government	SamSam	RDP	$51,000	$1.5 million	February 2018
Maersk	Transport	NotPetya	EK	$51,000	$300 million	June 2017
FedEx	Transport	NotPetya	EK	$51,000	$300 million	June 2017
Nuance Communications	Health, finance	NotPetya	EK	$50,000	$92 million	June 2017

EK-Exploit Kit and **RDP**-Remote Desktop Protocol

1. A. Zimba and M. Chishimba, "On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems," *Eur. J. Secur. Res.*, vol. 4, no. 1, pp. 3–31, 2019.



Recovery from Ransomware Incidents [1]

- ✓ Backup-69.7%
- ✓ Other-15.2%
- ✓ Authority-6.1%
- ✓ Reverse Engineered-6.1%
- ✓ Ransom Money-3%

1. G. Hull, H. John, and B. Arief, "Ransomware deployment methods and analysis: views from a predictive model and human responses," *Crime Sci.*, vol. 8, no. 1, p. 2, 2019.

Cumulative Ransomware Payments to Specific Bitcoin Address [1]

Campaign	BTC amount	USD value	Grace period	Period
CryptoWall	5351	$2.2 million	72 h	January 2014–January 2018
Erebus	397.6	$1.01 million	7 days	June 2017
CryptoLocker	1404	$450,000	72 h	September 2013–February 2014
DMA Locker	340	$179,000	96 h	December 2015–September 2016
WannaCry	52	$140,000	72 h	May–August 2017

Sector-Wise Ransomware Incidents in 2019 [2]

Sector	%	Sector	%
Energy and Utility	**32**	**Government**	**14.1**
Manufacturing	**13.8**	**Business Services**	**8.3**
Transportation and Storage	**5.9**	**Retail**	**5.6**
Software and Internet	**5**	**Healthcare, Pharmaceuticals**	**4.4**
Financial Services	**2.6**	**Education**	**1.9**
Telecommunications	**1.4**	**Real Estate and Construction**	**1.4**
Miscellaneous	**3.6**	**Total**	**100**

1. A. Zimba and M. Chishimba, "On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems," *Eur. J. Secur. Res.*, vol. 4, no. 1, pp. 3–31, 2019.
2. "2020 Cybersecurity Outlook Report: Key Findings (Part 1 of 2) | Security Blog | VMware," Security & Compliance Blog, Mar. 09, 2020. https://blogs.vmware.com/security/2020/03/2020-cybersecurity-outlook-report-key-findings-part-1-of-2.html (accessed Sep. 06, 2020).

Data recovery rate with a Ransomware Decryptor

Cryptocurrencies to Pay for Ransomware

Fight Against Ransomware

- Awareness, Education, and Training.
- Update OS Security Patches.
- Backup Sensitive Data/Files Regularly.
- Antivirus , Anti-Malware, and Malware-Remover.
- Building firewall rules and updating.
- Limit file sharing right.
- Remove any suspicious software.
- Install and use secured browser.
- Install spam filter on e-mail accounts.
- Monitor System Resources for Resources Anomalies.

Thank you

T11 Quant. Examination of Phishing

Qingyi Zhao
Tony Shang

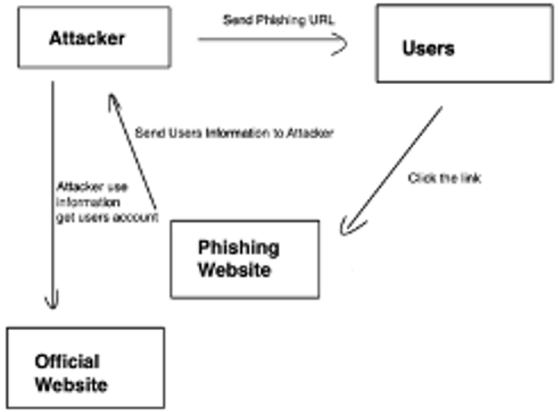
Colorado State University

Outline

- Background & Introduction
- What is the current status of technology in this field?
- What development have taken place recently, say past 2-4 years.
- What are current products and mature technologies available?
- Identify 3 organizations (industry, research labs or academic) that seem to have an influential role in advancing the field.
- References

Background & Introduction

What is phishing? Take a phishing website as an example: the attacker prepares a webpage that imitates the official website in advance and fails to send it to the server to make the webpage accessible, and sets up a channel for transmitting user information. Induce users to phishing web pages through emails, text messages, or hiding links in other web pages. After the user fills in the personal information and clicks the "Submit" button, the data is sent to the location designated by the attacker for storage. The following figure shows the flow of this series of attacks.



The current status of technology

- Computer virus and network security early warning monitoring system
- Early warning and monitoring
- The domain name and IP address are monitored
- Spam emails are filtered
- New authentication mechanism is adopted

Statistical Highlights for 2nd Quarter 2020

	April	May	June
Number of unique phishing Web sites detected	48,951	52,007	46,036
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	43,282	39,908	44,497
Number of brands targeted by phishing campaigns	364	352	363

Development recently

In the past few years, many browsers have begun to add the recognition function of phishing websites: when a user visits a page of a suspected phishing website, the browser will issue a warning and block access to the page. At the same time, a special authentication mark will appear when visiting the official page to facilitate users to distinguish. Many websites have begun to use Https secure links. The data transmitted by such links are encrypted and authenticated by SSL certificates. But applying for an SSL certificate is very simple. Many phishing websites now also apply for certificates in order to increase their credibility. In addition, security software and system firewalls are continuously updated to identify phishing websites. In recent years, machine learning has developed rapidly, and some scholars have studied the use of machine learning to identify and classify phishing websites and normal websites.

Current technologies

- The browser compares the currently visited URL
- Phishing recognition technology based on page text features.
- Identification based on domain name registration information.
- Targeting Hosting Sites
- Web Browser Toolbars
- Strong Authentication and Authorization

CS 559 QUANTITATIVE SECURITY

QUICK RESEARCH TOPIC:
Quantitative Examination of Phishing

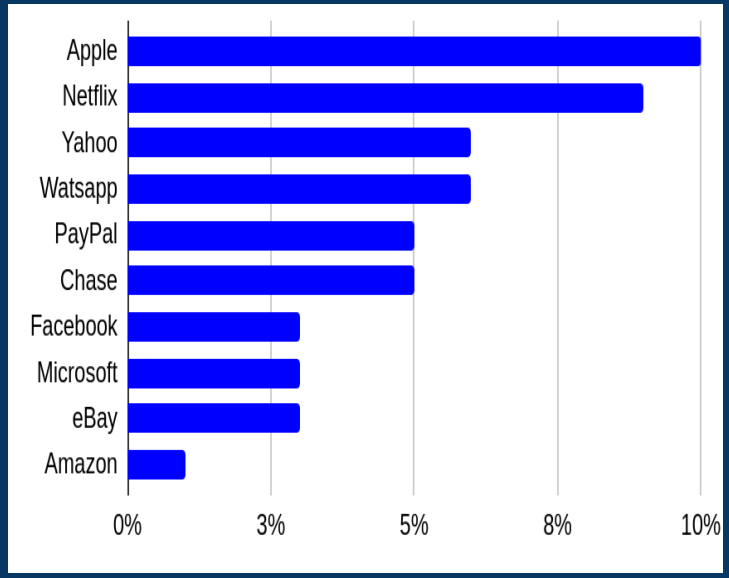
By: Shree Harini Ravichandran

Introduction

- Phishing is a fraudulent activity where the attacker tries to acquire sensitive information from the victim
- **Phishing Attacks:** Through emails. In recent times smishing and vishing have been on a rise
- **Phishing Scams:** According to a research survey by Cybersecurity Insiders, more than half of the professionals working in the IT sector have seen a surge in phishing scams since the start of the pandemic

Current Status

- According to Verizon 2020 Data Breach Investigation Report, 22% data breach was due to phishing
- There is a difference between a phishing scam attempt and a successful attack
- Over 65% of organizations in the United States have experienced successful phishing attacks
- On average, a breach costs $3.93 million and these numbers vary by company size
- Interpol predicts a 59% increase in phishing attacks due to COVID



Top ten phishing brands in 2020

Recent Developments

- Bartoli et al., have analysed Phishing Pages visual looks [1]. They assess the visual similarity between the two web pages using a similarity metric called NCD.

- Van Der Heijden et al., [2] use quantitative metrics of cognitive vulnerability triggers in phishing email scams to detect the degree of success of an attack.

- Thakur et al., propose a hybrid model that uses Natural Language Processing techniques for defending against phishing attacks[3]. They have improved the Topic Blacklist (TBL) model with additional features.

- Higbee et al. [4] detect a phishing message by a collective response technique from users who have received the message. A numerical ranking technique is followed to indicate the probability of a phishing attack.

Current Products and Mature Technologies

- Web Browsers play a vital role in detecting and blocking malicious content. The best web browsers that protect against phishing are Mozilla Firefox, Microsoft Edge, Brave, and Safari
- Anti-Phishing Softwares: BitDefender AntiVirus Plus, Norton Antivirus Plus, Kaspersky AntiVirus, Webroot SecureAnywhere Antivirus
- Anti-Phishing Toolbar: Cloudmark Anti-Fraud Toolbar, Google Safe Browsing, McAfee SiteAdvisor, Microsoft phishing filter, SpoofGuard, NetCraft Anti-Phishing toolbar
- Barracuda Networks, an IT security company has an AI- based product for email protection.
- The email app of Edison Mail has new security features that act as a defense against phishing attacks.

Organizations that have Influential Role

- Anti-Phishing Working Group offers resources and education to stop phishing attacks
- MSI Simple Phish tool by MicroSolved, allows organizations to run phishing tests
- A phishing simulation platform by PhishMe, reports phishing emails by doing a threat analysis
- Companies like MediaPro, IronScales, BlackFin, PhishLine offer training and education to act better when there are such social engineering attacks.
- GreatHorn is a company that provides cloud-native security platforms to stop phishing attacks on cloud email platforms like G Suite and Office 365.

References

[1] Bartoli, A., De Lorenzo, A., Medvet, E. and Tarlao, F., 2018. How Phishing Pages Look Like?. Cybernetics and Information Technologies, 18(4), pp.43-60.

[2] Van Der Heijden, Amber, and Luca Allodi. "Cognitive triaging of phishing attacks." In 28th {USENIX} Security Symposium ({USENIX} Security 19), pp. 1309-1326. 2019.

[3] Thakur, Kutub; Shan, Juan; Pathan, Al-Sakib Khan. International Journal of Communication Networks and Information Security; Kohat Vol. 10, Iss. 1, (Apr 2018): 19-27.

[4] Higbee, Aaron, Rohyt Belani, and Scott Greaux. "Collaborative phishing attack detection." U.S. Patent 9,591,017, issued March 7, 2017.

THANKS

Three organizations that have an influential role in advancing the field.

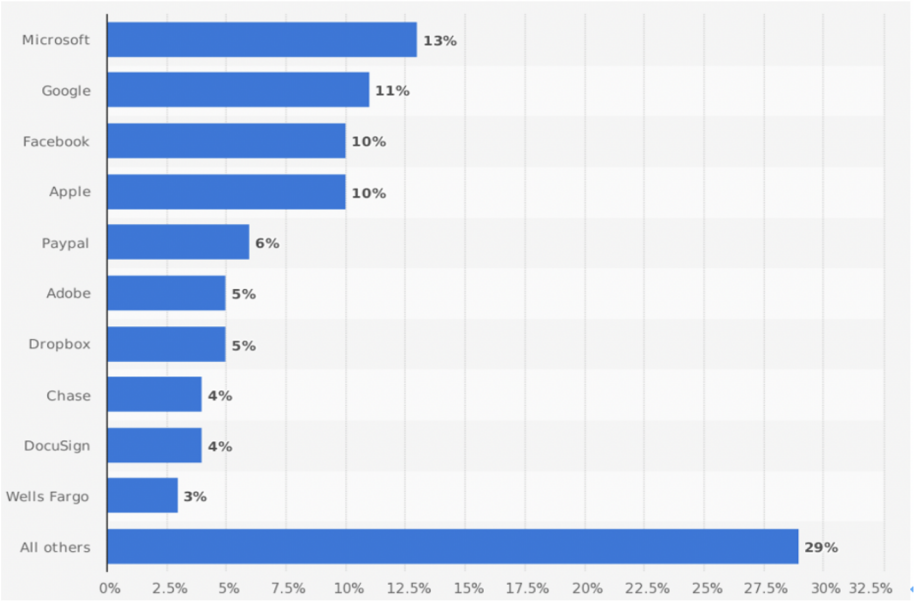


Fig1

- Fig1 show that leading organizations impersonated by phishers worldwide as of October 2019.
- The smaller the percentage of counterfeiters, the better the company's defense.
- Chase, DocuSign, and Wells Fargo organizations have an influential role in advancing the field.

Reference

[1] Apwg.org. 2020. APWG | Unifying The Global Response To Cybercrime. [online] Available at: <https://apwg.org> [Accessed 7 September 2020].

[2] Su, K., Wu, K., Lee, H. and Wei, T., 2013. Suspicious URL Filtering Based on Logistic Regression with Multi-view Analysis. 2013 Eighth Asia Joint Conference on Information Security.

[3] Afroz, S. and Greenstadt, R., 2011. PhishZoo: Detecting Phishing Websites by Looking at Them. 2011 IEEE Fifth International Conference on Semantic Computing.

[4] Agarwal R, Sinha AP, Tanniru M (1996) Cognitive fit in requirements modeling: A study of object and process methodologies. J. Management Inform. Systems 13(2):137–164.

[5] Alexander PA (1992) Domain knowledge: Evolving themes and emerging choices. Educational Psych. 27(1):33–51.

[6] Allen GN, March ST (2006) The effects of state-based and event-based data representations on user performance in query formulation tasks. MIS Quart. 30(2):269–290.

[7] Arisholm E, Sjoberg DIK (2004) Evaluating the effect of a delegated versus centralized control style on the maintainability of object-oriented software. IEEE Trans. Software Engrg. 30(8):521–534.

[8] Barron TM, Chiang RHL, Storey VC (1999) A semiotics framework for information systems classification and development. Decision Support Systems 25:1–17.

Thank you