Issues in Information Systems
Volume 23, Issue 3, pp. 25-35, 2022

DOI: https://doi.org/10.48009/3_iis_2022_103

Understanding cybercrime: A three-generation approach

Zane Ronald Allan Mooney, *University of North Alabama, zblankenship@una.edu*
Xihui Zhang, *University of North Alabama, xzhang6@una.edu*
John D. Crabtree, *University of North Alabama, jcrabtree@una.edu*

Abstract

Through a three-generation approach, this paper hopes to unambiguously layout cybercrime in a way that could clarify what cybercrime was, is, and the threats it could pose to American households and businesses daily. Throughout the history of the Internet and the World Wide Web, multiple themes, and trends of cybercrime have been realized and rectified through academic and industrial training, taxonomies, and government intervention. However, a dramatic increase of losses and complaints in the past four years reported due to cybercrimes indicate that the integrity of safety while on the Internet is being compromised more now than ever. As technology advances, so do cybercriminals' tactics change to maximize profit and ameliorate or mitigate any consequence that could occur from engaging in illegal activity online. This paper addresses a new generation of cybercrimes not yet seen by the public eye and calls for an immediate resolution to the problem.

Keywords: cyberscam, cyberattack, cybercrime

Introduction

This paper encapsulates cyberattacks and cyberscams under the term *cybercrime*. This paper will address the questions: Do existing taxonomies capture the current state of cybercrime? How can cybercrime be understood more easily? What can cybersecurity experts do to combat new trends of cybercrime? The taxonomy this paper presents is not all-inclusive, rather, it is a tool to help better understand cybercrime, especially for more inexperienced readers, as its approach is taken from chronological order of the many trends and fads that cybercrime has seen over the decades. The types of crimes also will become more evasive and more harmful as the generations are presented in the proposed taxonomy. Cybercrime is elusive. With technology being ever changing, it is impossible for literature to keep itself fully updated on what is transpiring in the cybercrime world. According to the FBI's Internet Crime Complaint Center (IC3), United States businesses lost $13.3 billion due to cybercrime in between the years 2016 and 2020. The IC3 has not released statistics for the year 2021. Cybercrimes have also victimized 791,790 American businesses in 2020, released by the IC3. This paper addresses cybercrime costing US businesses billions per year from a generational perspective. Previously, common aspiring cybercriminals would typically use phishing emails, social engineering, and many other tactics that have been seen in a wave of trends and fads. The public now knows of these common tactics and has become very aware and combative towards these strategies through online training about these tactics. These older generations of cybercrime have been either fixed or have become common knowledge to the public (Al-Khater et al., 2020). However, a new movement of cybercrimes is becoming ubiquitous and less easy to spot. Through online underground economies that sell attack-oriented services for affordable costs, cybercrime is now becoming more accessible to people. A transformation of online criminal activity is coming upon the world, and this paper hopes to reiterate, be consistent with existing literature, and be able to help readers fully comprehend cybercrime and its many facets.

The statistics given from the Federal Bureau of Investigation show a dramatic surge in losses due to complaints of cyberattacks in the last four years (see Figures 1 and 2). From 2016 to 2020, the United States had a 166% increase in complaints and losses that were reported to the IC3 from American businesses and households. This alarming statistic confirms that cybercriminals are profiting more from American businesses and households per year by illegal activities.

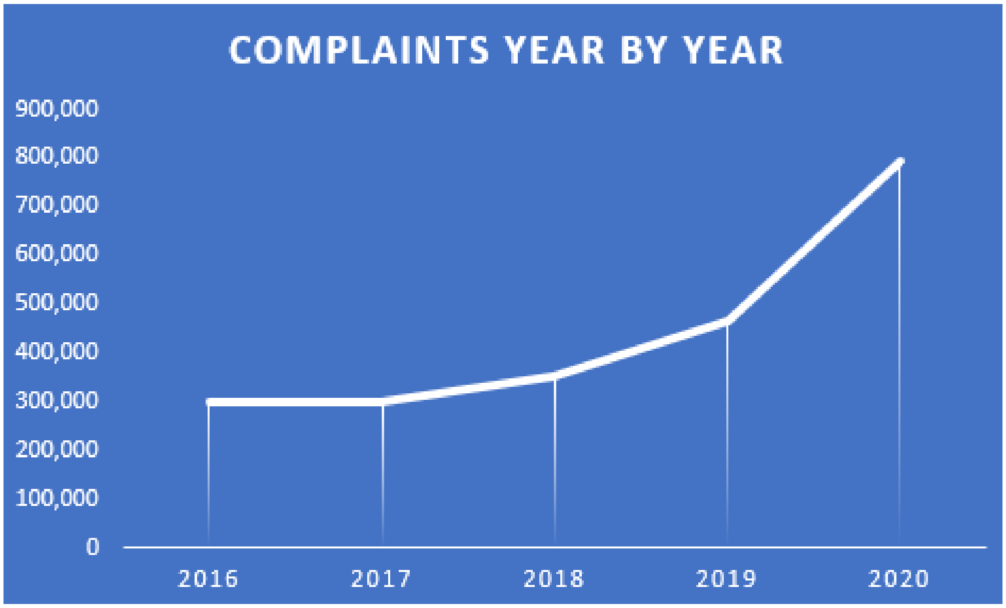


Figure 1: Complaints of Cyberattacks on US Households from a Report by the FBI

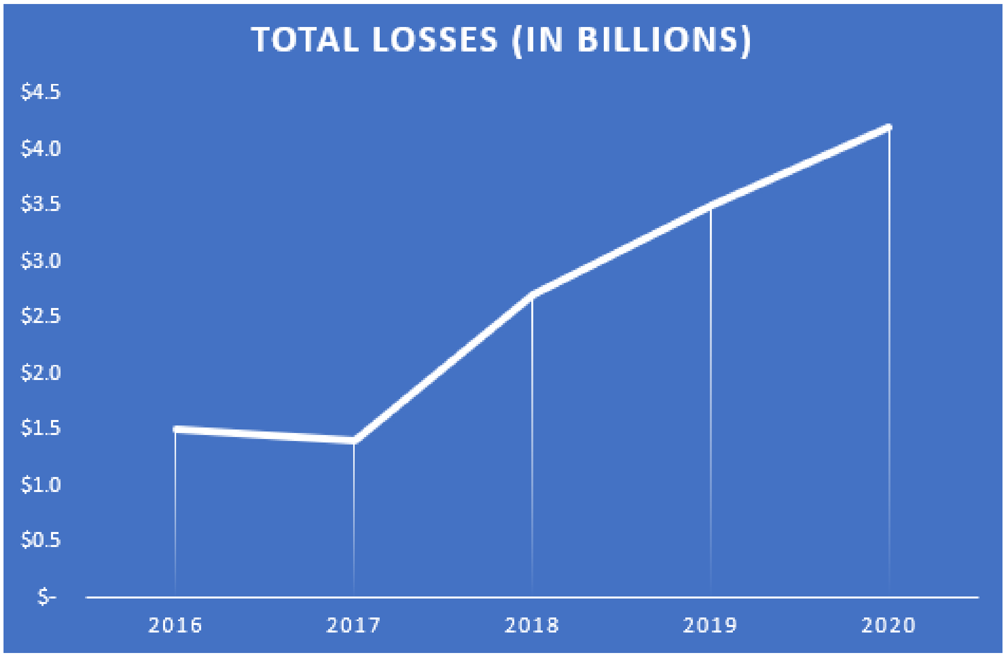


Figure 2: Total Losses Due to Cyberattacks in USD (in Billions) Year-by-Year Released by the FBI

Hypothetically, these increasing losses come from a theorized conclusion that the automation and industrialization of cybercrimes are directly correlated with the significant increase of losses and complaints per year. However, more research is needed to draw a satisfactory conclusion on that statement.

This paper proceeds as follows. Common cybercrime taxonomies will be introduced along with David S. Wall's three-generation approach for background information about cybercrime. Next, our theoretical generations of cybercrimes will be introduced with the context of how all three generations operate, typically supported by statistics. Then, a comparison of the two three-generation models will be discussed along with a discussion based upon a call to an educational and industrial shift to this alarming new generation of cybercrimes.

A brief review of cybercrime taxonomy

Looking at cybercrime at a macro level is challenging. Without a foundation of "a universally-agreed-upon definition, understanding the constituents of cybercrime remain elusive" (Chandra & Snowe, 2020). Prior research provides a multitude of taxonomies of cybercrime to help alleviate confusion when attempting to understand cybercrime; however, most of them are inadequate in fully enveloping all types of cybercrime, just as this one will be. This inadequacy does not come from any author error but is due to the ever-changing world of cybersecurity and cybercrime.

Brar and Kumar (2018) developed a taxonomy by dissecting cybercrime into four categories- cyber violence, peddler, trespass, and squatting. These categories are then given examples by listing different types of cybercrimes. This taxonomy also includes a classification of cyberattacks based on fundamental cybersecurity principles. Brar and Kumar (2018) introduce their classification system based on confidentiality, integrity, or availability attacks.

Donalds and Osei-Bryson (2014), while developing a taxonomy of cybercrime to fit their needs and have "an essential step towards getting a better understanding of the phenomenon of cybercrime in Jamacia," propose nine key characteristics: Victim, Attacker, Objective, Tool & Tatic, Impact, Result, Relationship, Target, and Offence. These characteristics extend into categories that describe the "most current" terminology used for any characteristic. An example is identifying the Attacker as a Script Kiddy, a Corporate Raider, White Hat / Black Hat Hacker.

Baror et al. (2019) developed a cybercrime taxonomy focused on cybercrime attacks in the public cloud. Using categories based on the cybercrime attack approach, Baror et. al (2019) used a technical induced approach, non-technical induced approach, and hybrid induced approach as the three main categories to understand cybercrime in the public cloud.

Numerous cybercrime taxonomies have been developed over the years to alleviate any confusion or misunderstandings about cybercrime. However, the rapidly changing world of the Internet leaves most taxonomies insufficient and deemed inadequate to use as a standard for classifying cybercrime (Donalds, 2015). It is highly improbable for literature to keep itself updated on cybercrime. As more taxonomies are created, a better understanding of cybercrimes and cybercriminals will be established.

David S. Wall in his closing chapter of *Cybercrime,* written in 2007, proposes three generations of cybercrime with little detail. His proposal is as follows:

> "*The first generation of cybercrimes are traditional or ordinary crimes using computers – usually as a method of communication or to gather precursor information to assist in the organization of a crime… the second generation of cybercrimes are hybrid cybercrimes, 'traditional' crimes for which network technology has created entirely new global opportunities. Take away the internet and the behavior continue by other means, but not upon such a global scale or across such a wide span of jurisdictions and cultures. The third generation of cybercrimes are true cybercrimes that are solely the product of the internet. Take away the internet and they vanish- the problem goes away. This last generation includes spamming, 'phishing' and 'pharming', and variations of online intellectual property piracy*" (Wall, 2007, p. 208).

After Wall gives a general synopsis of his proposal, he states that "we need to begin rethinking the meaning of many concepts and values that we cherish and protect, such as security and privacy (but not in this book)" (Wall, 2007, p. 209). This generational approach Wall introduces is an excellent foundation for understanding cybercrime; however, "the need for a stable, comprehensive taxonomy stem from a lack of clarity, understanding, uniformity, and consistency around cybercrime" (Chandra & Snowe, 2020).

Our proposed generations

First generation – Crimes made easier

The first hypothetical generation that we are proposing would follow similarly to the writing of Wall in his second generation. This generation would include every "traditional or ordinary" crime using computers (Wall, 2007). This generation would also denote that if the Internet today were not as commercially available or even invented, these crimes would still happen today. The Internet only helps make the scope of people affected much more significant than what the world was before the Internet was invented. Defined by Merriam-Webster Dictionary, this first generation of cybercrimes would include (see Table 1):

- Cyberbullying is "the electronic posting of mean-spirited messages about a person (such as a student) often done anonymously."
- Spamming is to send "unsolicited usually commercial messages (such as emails, text messages, or Internet postings) sent to a large number of recipients or posted in a large number of places."
- Cyberstalking is the "the use of electronic communication to harass or threaten someone with physical harm."

Table 1: Examples of Generation 1 Cybercrime

Real Life Crime	Cybercrime Counterpart
Bullying	Cyberbullying
Spam Mail	Spamming
Stalking	Cyberstalking

Cyberbullying and cyberstalking have become significant problems that arose with the rise of social media becoming a part of Americans' daily lives. According to a report from Sheridan and Grant (2007), "1051 respondents whose data were analyzed, 47.5% said they had been harassed via the Internet. A total of 40.2% had received unsolicited emails" (p. 11). These crimes have been a problem in our past through physical means. These psychological and ordinary crimes have become more widespread with the Internet's innovations.

This first proposed generation is not as harmful or can cause as much damage as the latter two generations; however, technology has broadened our scope of communication with the world through social media, creating a platform where common psychological crimes can be amplified and made more accessible due to the anonymity that the Internet gives to people.

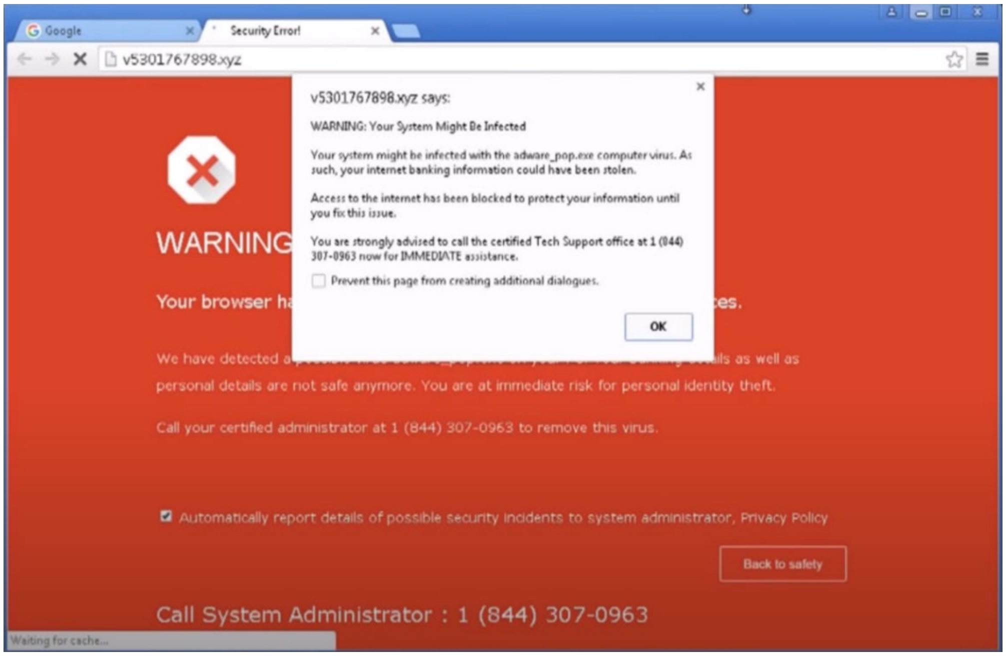
Second generation – Foundations of cybercrime

Our second proposed generation of cybercrimes is defined by the technological advances making these crimes possible and more efficient and profitable to commit. These cybercrimes were some of the first cybercrimes to occur and are still in use today. This generation also includes common cybercrimes brought to the public eye and is now commonly taught through academic classes and industrial training common tactics to avoid becoming a victim to cybercrime. However, the cybercrimes of this generation still pose a significant threat to American households and businesses daily. Defined by Merriam-Webster Dictionary, the proposed second generation of attacks would include:

- Phishing is "the act of sending email that falsely claims to be from a legitimate organization."
- Social engineering is "the practice of tricking a user into giving, or giving access to, sensitive information, thereby bypassing most or all protection."
- Technical support scams are where "cybercriminals attempt to convince users that their machines are infected with malware and are in need of their technical support" (Miramirkhani et al., 2017).

Typical operations of these criminal enterprises are located overseas, where laws and regulations are not as integral as in more developed countries. Phone numbers, emails, addresses, or any form of personal information that is collected throughout the years are typically sold and transferred from one call center to another for a fee. This process is remarkably similar to how companies market their customer's contact information to another company.

A technical support scam attack (see Figure 3) typically starts by the victim being prompted by a webpage with messages stating that their system is being infected with malware, their hard drive will be wiped, and that if the user does not call the number on their screen, they will lose all their data.



v5301767898.xyz says:

WARNING: Your System Might Be Infected

Your system might be infected with the adware_pop.exe computer virus. As such, your internet banking information could have been stolen.

Access to the internet has been blocked to protect your information until you fix this issue.

You are strongly advised to call the certified Tech Support office at 1 (844) 307-0963 now for IMMEDIATE assistance.

☐ Prevent this page from creating additional dialogues.

WARNING

Your browser h es.

We have detected a ils as well as personal details are not safe anymore. You are at immediate risk for personal identity theft.

Call your certified administrator at 1 (844) 307-0963 to remove this virus.

☑ Automatically report details of possible security incidents to system administrator, Privacy Policy

Call System Administrator : 1 (844) 307-0963

Figure 3: Screenshot of a Technical Support Scam Using Pop-ups and Technical Jargon to Scare Victims into Calling the Call Center

Technical support scams use fear tactics to force the victims to "provide scammers with remote access to their machines, who will then 'diagnose the problem,' before offering their support services which typically cost hundreds of dollars" (Miramirkhani et al., 2017). These phrases are commonly used to confuse elderly age groups and others that are at a disadvantage using technology. According to a survey from the AARP, "56 percent of telemarketing fraud victims were 50 years of age or older" (Aziz et al., 2000). With international law so lacking in pursuing these fraud operations, being hosted in under-developed countries, these call centers operate at alarming uptime and continue to steal millions of dollars from United States households yearly. According to the FBI in their Internet Crime Report 2020, technical support scams' total losses equated to $146,477,709 USD.

Social engineering attacks (see Figure 4) commonly start by email or phone calls through "relationships with the victims to play on their psychology and emotion. These attacks are the most dangerous and successful attacks as they involve human interactions" (Salahdine & Kaabouch, 2019).

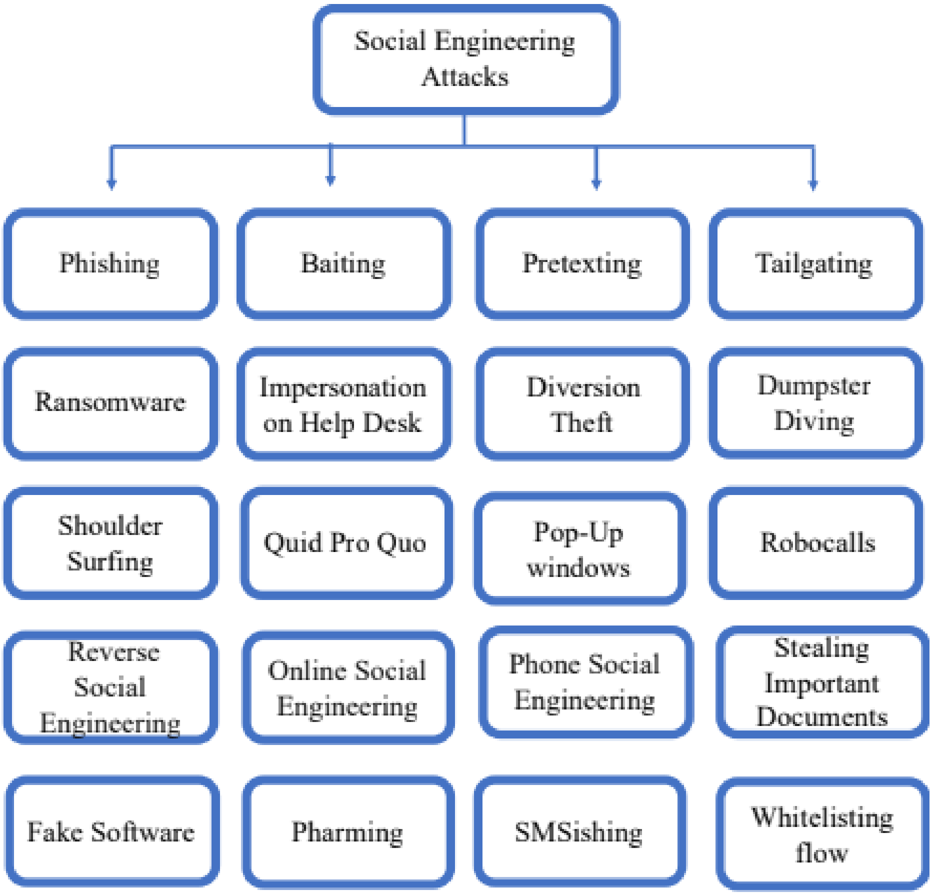


Figure 4: Social Engineering Attacks (adapted from Salahdine and Kaabouch, 2019)

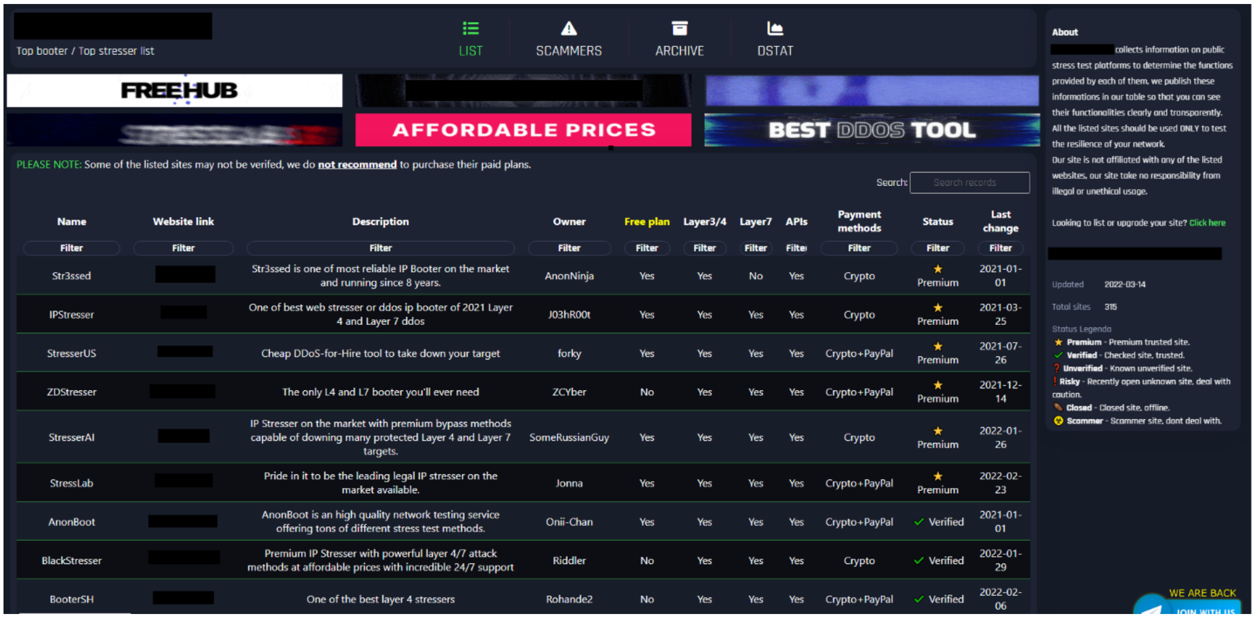
Social engineering attacks have been a problem in the United States for years now. According to a report released by Cyence in 2016, the United States was the country targeted by the most social engineering attacks and had the highest attacking cost followed by Germany and Japan (Salahdine & Kaabouch, 2019).

Though it may be hard to determine all the various cyberattacks that would be classified inside this second generation, the general conclusion is that these cybercrimes are the foundations of cybercrime and the potential the Internet has to harbor such criminal organizations.

Third generation – Hacking as a Service (HaaS) | Enterprising cybercrime

Our third and final proposed generation includes a new trend in commercializing cybercrimes and attacks. Multi-billion-dollar black-market enterprises are being formed on the Internet with the sole goal of industrializing various cybercrime methods. These methods would include:

- Hired botnets - a for-hire service that takes a network of potentially thousands or hundreds of thousands of computers to target embedded systems and Internet of Things (IoT) devices. The most common attack with a botnet is a Denial-of-Service Attack (DDoS) (see Figure 5).
- Website setup services to mask as a legitimate business such as PayPal, Amazon, and many other popular sites, and automatically spam an entered email list or phone number list to potentially phish log-in information.
- Licensed malware (e.g., GonnaCry/WannaCry) where an aspiring cybercriminal can rent access to ransomware to send to a list of potential victims, causing lockage of information on a computer until a determined amount of Bitcoin (BTC) is sent to a specific wallet address.



[redacted]
Top booter / Top stresser list

[redacted]

PLEASE NOTE: Some of the listed sites may not be verifed, we do **not recommend** to purchase their paid plans.

Name	Website link	Description	Owner	Free plan	Layer3/4	Layer7	APIs	Payment methods	Status	Last change
Str3ssed	[redacted]	Str3ssed is one of most reliable IP Booter on the market and running since 8 years.	AnonNinja	Yes	Yes	No	Yes	Crypto	★ Premium	2021-01-01
IPStresser	[redacted]	One of best web stresser or ddos ip booter of 2021 Layer 4 and Layer 7 ddos	J03hR00t	Yes	Yes	Yes	Yes	Crypto	★ Premium	2021-03-25
StresserUS	[redacted]	Cheap DDoS-for-Hire tool to take down your target	forky	Yes	Yes	Yes	Yes	Crypto+PayPal	★ Premium	2021-07-26
ZDStresser	[redacted]	The only L4 and L7 booter you'll ever need	ZCYber	No	Yes	Yes	Yes	Crypto+PayPal	★ Premium	2021-12-14
StresserAI	[redacted]	IP Stresser on the market with premium bypass methods capable of downing many protected Layer 4 and Layer 7 targets.	SomeRussianGuy	Yes	Yes	Yes	Yes	Crypto	★ Premium	2022-01-26
StressLab	[redacted]	Pride in it to be the leading legal IP stresser on the market available.	Jonna	Yes	Yes	Yes	Yes	Crypto+PayPal	★ Premium	2022-02-23
AnonBoot	[redacted]	AnonBoot is an high quality network testing service offering tons of different stress test methods.	Onii-Chan	Yes	Yes	Yes	Yes	Crypto+PayPal	✓ Verified	2021-01-01
BlackStresser	[redacted]	Premium IP Stresser with powerful layer 4/7 attack methods at affordable prices with incredible 24/7 support	Riddler	No	Yes	Yes	Yes	Crypto	✓ Verified	2022-01-29
BooterSH	[redacted]	One of the best layer 4 stressers	Rohande2	No	Yes	Yes	Yes	Crypto+PayPal	✓ Verified	2022-02-06

About

[redacted] collects information on public stress test platforms to determine the functions provided by each of them, we publish these informations in our table so that you can see their functionalities clearly and transparently. All the listed sites should be used ONLY to test the resilience of your network.
Our site is not affiliated with any of the listed websites, our site take no responsibility from illegal or unethical usage.

Looking to list or upgrade your site? Click here

[redacted]

Updated 2022-03-14

Total sites 315

Status Legenda
★ **Premium** - Premium trusted site.
✓ **Verified** - Checked site, trusted.
? **Unverified** - Known unverified site.
! **Risky** - Recently open unknown site, deal with caution.
Closed - Closed site, offline.
☢ **Scammer** - Scammer site, dont deal with.

Figure 5: A Website Selling DDOS Services

This proposed third generation is a shift to automating and marketing the ability to attack and profit off another person with total anonymity and minimal consequence for both the software developers and the consumer of the products. This practice has existed in the past, but the volume of traffic these Dark Web sites generate increases exponentially. According to an article in *The Atlantic*, 25.6% of the Internet traffic in 2021 was done by "software applications that run automated tasks with malicious intent over the internet" (Hasson, 2021). Another article states that "approximately 16-25% of the computers connected to the Internet are members of botnets" (Silva et al., 2013). Cybercriminals still aim to compromise the confidentiality, integrity, and availability of information in an ever-changing world.

In a study produced by Vincet (2017), an examination of 12 DarkWeb sites involved in selling hacking services is performed. This study shows that over 50% of HaaS sites include social media, database, and phone hacking. Services related to malware and ransomware are advertised on less than 30% of these sites. The average demand prices for these services are $873 USD.

These marketplaces that exist on the Internet have been combated and have had recent efforts to attempt to understand these hidden markets (Christin, 2013; Holt & Shirnova, 2014); however, little progress has been made to entirely cease operations of these markets and ultimately develop an understanding of the scale of these websites. The vastness of the Internet poses an exponentially increasing challenge to fathom the potential danger and threat that Hacking as a Service market may pose.

According to an examination of the relationship between Bitcoin and cybercrime done by Sándor and Fehér (2019), from February 2011 to July 2013, the US government listed 9.9 million bitcoins of transactions that occurred over 30 months of observing the Silk Road marketplace. With the development of blockchain technology and many different types of cryptocurrencies, these hidden markets have been given an enabler to ensure buyer and seller safety when conducting any illegal online activity. Bitcoin and other common cryptocurrencies are considered public and decentralized from any form of government, backed by blockchain technology to ensure the integrity of every transaction. This decentralization enables aspiring cybercriminals to negate any consequences one may have from conducting illegal activity online.

This third generation of cybercrimes allows both the end-user and the developers of these botnets to remain anonymous using usernames, cryptocurrency, and a third-party marketplace to be a middleman for the transaction. Simply purchasing a plan designed by the botnet owners for a certain premium fee will allow the end-user to give an IP address, a URL, or any other identifying address to attack a website or another user on the Internet. While some services provided target businesses, most services listed in Figure 5 pertain to attacking a sole individual on the Internet. These websites are typically taken down by various United States government organizations like the FBI and the CIA; however, these communities have multiple backup webservers to use if one of the URLs gets banned or taken down.

This third generation is the most alarming to the public. The more users who have access to these services can pose a significant threat to the general order and safety of being a user on the internet.

Comparison of the two three-generation schemes

The two three-generation approaches that have been discussed in this paper hold a lot of similarities and differences (see Table 2). The most significant difference is within the scope of the cybercrimes examined within these two different perspectives. In our proposed generational perspective, we look at cybercrimes like phishing, tech-support scams, and social engineering attacks as the foundations of cybercrime. Hacking as a Service (HaaS) is a new form of cybercrime that gives more accessibility to users on the Internet to directly attack an end-user or business for payment, which is seen in our third generation we propose. As cybersecurity becomes more robust, the criminals that attack users on the Internet and businesses daily become more advanced. Technology itself seems limitless, including the criminal side of the Internet.

Table 2: Comparison of the Two Three-Generation Schemes

	Wall's Scheme	Our Scheme	Comments
First Generation	"Traditional or ordinary crimes using computers" (Wall, 2007)	Common crimes like hate speech, bullying, and stalking being amplified with the creation of social media and other platforms.	These two generations are the most similar, however, our first generation includes only psychological or any form of crime through social media communication.
Second Generation	"Hybrid cybercrimes- 'traditional' crimes for which network technology has created entirely new global opportunities" (Wall, 2007).	Beginning foundations of cybercrime enterprises, where common scam tactics previously used by other means (e.g., phone, mail, text) moved primarily to the Internet.	We think of Wall's third generation as the beginnings of cybercrime. Tactics like phishing and pharming are practically being phased out with the amount of awareness there is to these attacks.
Third Generation	"True cybercrimes- solely the product of the internet… This last generation includes spamming, 'phishing' and 'pharming'" (Wall, 2007)	Cybercriminal organizations being fully developed and operated to sell illegal services to common people to attack other's online without any consequence.	This third generation that we are proposing could also include the alarming increase of countries fighting in cyberwarfare, however, we wanted to keep the scope of this generation to only include cybercrimes that effects American businesses and households.

Discussion

Our proposed three-generation approach to cybercrime will hopefully be straightforward to understand. Cybercriminals are not stagnant in their efforts to victimize American households and businesses, nor are cybersecurity companies. Variations of cyberattacks and scams are being created to increase profits for cybercriminals. We see a new trend of cybercrime being created under the anonymity of the Internet and call for an immediate shift into arming people against these threats. If more Internet users are allowed access to these markets that sell services to attack others, cybercrime will harm even more businesses and households every year.

Therefore, because of these startling operations, we may have to reconsider our privacy on the Internet. This statement is very similar to Wall's train of thought on the matter - "in addition to the prospect of being faced with 'ubiquitous' and automated victimization, we also face the uncomfortable prospect of being simultaneously exposed to 'ubiquitous law enforcement' and prevention" (p. 209). These markets cannot be allowed to operate entirely without consequence, and it may be time for people to consider more restrictions being imposed on the Internet.

Conclusion

Although we may be gradually learning and adapting to the many new forms of attacks that appear daily, an increasingly more alarming amount of the public is being affected negatively by these crimes. As technology advances, people will be ignorant and quickly be taken advantage of if they are not educated on new trends or attacks of cybercrime. With a further shift of technology toward allowing end-users to pay for a service to profit, damage, or harass another, so should our focus on cybercrime awareness. With this three-generational approach to cybercrime, clarity can be found in attempting to understand the nature of cybercrime and cybercriminals.

Balancing the fine line of user independence and law and order on the Internet is a daunting task that must be determined to ensure safety and privacy for all; however, the inevitability of these black-market enterprises becoming more known can cause a massive outbreak of cybercrimes, potentially costing billions more of American household dollars. The world may be heading in a trajectory where the Internet will be required to be filtered and regulated more heavily than it already is. Without the ability to trace the buyer, seller, and middleman of these services, cybercrime will always run rampant without change in how we track users online. This paper calls for an educational and industrial shift toward this arising problem occurring in today's world. This paper also calls for more insight and research into these black-market websites. Lastly, this paper calls for research on Generation Z and Generation Alpha's victimization numbers. With technology (including the Internet) being introduced in nearly every single facet of life, our younger generation is being pushed into attempting to understand the Internet at a very young age. If more emphasis is put on examining Generation Z and Alpha's victimization through cybercrime, it is theorized that the cybersecurity industry could have an ideal grasp on what types of cybercrime are becoming more prevalent and profitable to do so. This paper theorizes that Generation Z and Generation Alpha's victimization/losses in USD will be comparable to Millennials and Baby Boomers; however, the resources to quantify such data are unavailable.

References

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8*, 137293-137311. https://doi.org/10.1109/access.2020.3011259

Aziz, S. J., Bolick, D. C., Kleinman, M. T., & Shadel, D. P. (2000). The national telemarketing victim call center: Combating telemarketing fraud in the United States. *Journal of Elder Abuse & Neglect*, *12*(2), 93-98. https://doi.org/10.1300/j084v12n02_10

Baror, S. O., & Venter, H. (2019). A taxonomy for cybercrime attack in the public cloud. In *International Conference on Cyber Warfare and Security* (p. 505).

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*, 24-31. https://doi.org/10.1016/S2212-5671(15)01077-1

Brar, H. S., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, *2018*, 1-11. https://doi.org/10.1155/2018/1798659

Chandra, A., & Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, *38*, 100467. https://doi.org/10.1016/j.accinf.2020.100467

Christin, N. (2013). Traveling the silk road. *Proceedings of the 22nd International Conference on World Wide Web - WWW '13*. https://doi.org/10.1145/2488388.2488408

Donalds, C., & Osei-Bryson, K. (2014). A cybercrime taxonomy: Case of the Jamaican Jurisdiction. *CONFIRM 2014 Proceedings*. http://aisel.aisnet.org/confirm2014/5

Federal Bureau of Investigation & Internet Crime Complaint Center. (2021, March). *Internet crime report 2020*, FBI. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Hasson, E. (2021, April 13). *Bad bot report 2021: The pandemic of the Internet | Imperva*. Imperva. https://www.imperva.com/blog/bad-bot-report-2021-the-pandemic-of-the-internet/

Holt, T., & Smirnova, O. (2014, March). *Examining the structure, organization, and processes of the international market for stolen data*. National Institute of Justice. https://nij.ojp.gov/library/publications/examining-structure-organization-and-processes-international-market-stolen

Miramirkhani, N., Starov, O., & Nikiforakis, N. (2017). Dial one for scam: A large-scale analysis of technical support scams. *Proceedings 2017 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2017.23163

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Sandor, B., & Feher, D. J. (2019). Examining the relationship between the bitcoin and cybercrime. *The 13th IEEE International Symposium on Applied Computational Intelligence and Informatics*. https://doi.org/10.1109/saci46893.2019.9111568

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law*, *13*(6), 627-640. https://doi.org/10.1080/10683160701340528

Silva, S. S. C., Silva, R. M. P., Pinto, R. C. G., & Salles, R. M. (2013). Botnets: A survey. *Computer Networks*, *57*(2), 378-403. https://doi.org/10.1016/j.comnet.2012.07.021

Vincent, B. (2017, April). *Understanding hacking-as-a-service markets*. Arizona State University. https://keep.lib.asu.edu/_flysystem/fedora/c7/205805/Vincent_asu_0010N_18336.pdf

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge, UK: Polity.