iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XI **Month of publication:** November 2022

DOI: https://doi.org/10.22214/ijraset.2022.47473

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XI Nov 2022- Available at www.ijraset.com

Advanced Social Engineering Attack Techniques

Jody Holeton
Eastern Michigan University

***Abstract:** This paper explains the emergence of Social Engineering techniques that can be deadly and effective and are being heavily watched by the Department of Defense and the FBI. The increased use of the Internet and cell phones has made it possible for most people to communicate, surf the web, or transfer data anywhere in the world. Social engineering only requires a computer with Internet access or a working smartphone/iPhone. With online forums, the Dark Web, a thousand hacker books on Amazon, these social engineering techniques are being tweaked and modified into techniques that rival the deadliest cookie monster virus or malware.*

The FBI has found that criminals can use low-tech mediums, like Motorola cell phones, use a historically winning script (Microsoft software fix, or an endangered child) and people will give up personal information, money, or even use deadly force. Finally, this paper describes these new techniques and how they are evolving more effectively in this post-covid and Internet-focused world.

I. INTRODUCTION

These days hackers are 3X more likely to attempt an attack like phishing or vishing rather than identity theft or extortion. The 2021 FBI Crime Report states that Social Engineering attacks have the highest number of cyber-attacks. In 2021 the FBI reported that its Internet Crime Complaint Center saw losses exceeding $6.9 billion in 2021 (an increase of 7% from last year) and had the highest number of complaints received since the IC3 was started in 2000. The FBI's IC3, gets more than 500,000 complaints a year and has seen a pattern developing where traditional hackers, state actors, independent agents, and corporate entities perfect their social engineer attacks and manipulation scripts.

II. ASEAT

More and more American businesses, economic institutions, and individual users are being targeted by some social engineering attack. With so many how-to-hack sites, online forums, cyber security boot camps, and Amazon kindle specials, getting into people's data is becoming commonplace. Places like discord and reddit.com have thousands of users offering information, giving advice, and even offering classes of known exploits and methods. YouTube itself has become the most accessible form of cyber craft training; social engineering has hundreds of channels with podcasters who make their living off of teaching cyber essentials and also are in a competition to show off the latest hack trick. SQL injections, brute force password hacks, Kali software with all its wondrous tools, Malware that can hold mega corporations' networks hostage, why is social engineering so popular, and why has it become so influential? Michael Erbschloe states in his book "Social Engineering" that "Social engineering is an incredibly effective process of attack with more than 80% of cyber attacks, and over 70% of those being initiated and executed by exploiting humans rather than computer or security flaws." Social engineering is manipulating people into doing something or sharing sensitive information.

Every day we see TV shows and read the headlines about hackers stealing millions of dollars, private pictures from iPhones, and government passwords to super-secret-squirrel information. Nowadays, people are warned of con artists, and most businesses and government work offer cyber awareness training. Most Americans learned not to talk to strangers and had "stranger danger" training. The FBI and the Department of Defense have intensive social engineering protection classes, online software, and operation centers that protect people from bad agents. Despite all these protections, social engineering works because most people are overwhelmed with information to verify every communication they receive. Verifying bad agents is a skill most people do not have; Social Engineering has evolved into advanced forms of attack that can not only manipulate but cause physical harm and even kill. Advanced Social Engineering Attack Techniques (ASEAT) have evolved from basic attacks (phishing, vishing, scareware, phone phreaking, and piggybacking) to specific scripts and choreographed moves that novice hackers can use with positive and deadly results. ASEAT is more than a simple ruse of manipulating someone to do something or give you some information is a time-honored tradition of grifters, pick-up artists, and con men they are real attacks and they are growing in popularity because they work.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XI Nov 2022- Available at www.ijraset.com

III. WEAPONIZED BUREAUCRACIES

Weaponized bureaucracies have created ASEATs that not only steal money and data but can hold people hostage and even cause them physical harm. Certain institutions like State governments, US Navy, and townships have specific laws that only apply to their specific members or residents. When laws are broken, like statutory rape, drug ownership, or child endangerment, specific leaders must be notified, and some form of investigation must be started. Stars and Stripes wrote in its September 2021 issue about dozens of prisoners in one South Carolina prison who extorted hundreds of thousands of dollars from American military men using fake dating profiles on dating apps. This form of extortion is called "sextortion" where a person is catfished and then has their bureaucracies' rules against them. For example, any form of sexual harassment or sexual assault must be investigated in the Department of Defense (DOD), any claim of impropriety is sent up a chain of command (from 3 to more than a dozen personnel), and that person has to be investigated (which lasts from six months to two years). In the DOD, a service member may not move to a different job, receive awards, or receive additional training until their investigation is complete and the service member has a commanding officer and his staff reviews their case. Most service members would pay most extortions not to go through that exposure in their personal life.

While sextortion can extort money from individuals (and possibly have targets commit suicide), another example of ASEAT is called "swatting." This form of social engineering is where law enforcement is manipulated into conducting a police raid on an individual or residence (SWAT, FBI raid, ATF inspection). Swatting would have bad agents use laws and a specific script against an individual or group, wherein a phone call would have some form of law enforcement conduct an investigation, usually forcibly with weapons. Law enforcement agencies, like the US military, have precise protocols and rules of engagement when certain crimes are committed. Crimes like child endangerment, significant drug involvement, or even things like suicidal veterans have a heavily armed and staffed law enforcement response.

The FBI's ARTIC newsletter announced in 2021 a whole bag of tricks for social engineering. Tricks that not only effect Soldiers but ordinary civilians and even children as well. Technology has evolved to the point where everyone can buy a supercomputer that fits in their back pocket, pirate the latest photoshop software, learn the latest exploit from a YouTuber, or even buy a hacking kit off of Amazon. Events like the South Carolina inmate in September 2022 that exploited hundreds of military personnel out of thousands of dollars or the deepfake video of President Trump saying Jeffrey Epstein didn't kill himself. Artificial Intelligence has grown with the technology and is being used by bad agents to augment pictures, videos, and audio files. The next decade we will see more Advanced Social Engineering Attack Techniques (ASEAT) with more refined strategies.

IV. TOP 5 FBI CYBER THREATS 2021

1) Business Email Compromise (BEC)
2) Confidence Fraud/Romance Scam
3) Ransomware
4) Cryptocurrency
5) Tech support fraud

In 2021 the FBI stated that Business E-mail Compromise (BEC), also known as E-mail account compromise, cost American taxpayers more than $2.4 billion.

BEC attacks a business or individual and socially engineers a money transfer. BEC is considered the most damaging of Internet crimes because of the prevalence of email use for personal and business use. This becomes ASEAT when bad agents find contact information about a target and create an email.

Getting bank information is a particular script that has to be played out for a particular target. Having the bad agent present the right subterfuge to put that script into play is just a matter of open-source research and phishing a target.

Confidence Fraud/Romance scams target an individual's heartstrings. According to the FBI, these attacks have cost Americans more than $250 million and affected more than 24,000 people. Scammers attempt to create intimate connections with victims and gain their trust quickly. Scammers create a romantic connection with their victims, which leads to them sending the scammer money. A common trend with scams is that the scammer pretends that they work internationally or are a deployed Soldier in war. Scammers will commonly digitally kidnap specific pictures and use proven attractive dating profiles. As more people use dating apps, romance scammers will be more of a threat, especially within our global community where we can connect to the Internet anywhere and, with the push of a button, use anyone's identity and picture.

Ransomware is a type of cyber-attack that targets data and computer systems for extortion. Usually, ransomware (a form of Malware) is delivered via e-mail, embedded in a file, or attached to a link embedded in a website. Once the file or link is clicked and opened, the target's information, network, or computer system becomes locked, encrypted, or even deleted. An activated ransomware incident usually has a popup message that directs the target to pay a recovery fee to a bank account, a location, or a cryptocurrency.

The 2021 report states that cryptocurrency has cost users more than $2.1 billion. Cryptocurrency is a digital currency designed to be exchanged on the Internet and not reliant on a bank or government to maintain its worth. Cryptocurrency scams feature grifts like using a fake photo of a celebrity to market a currency, inflating a cryptocurrencies price, then after an investment dumping the currency, putting up fake cryptocurrency wallets that have investors' money funneled into bake accounts, having a Ponzi scheme where investors get friends to invest in a currency. Romance scammers are using cryptocurrencies as part of their scams, so their victims can send money anywhere without leaving a banking trail. Having a currency that relies on the Internet to hold its value is rife to be used against naive investors, lovelorn individuals, and those working on the Internet.

Tech support fraud is a scam where individuals target people over problems invented for their technology or software. The FBI's IC3 saw a massive increase in tech support fraud of the elderly, a 70% increase in attacks from 2020, and 2021 saw losses of $1.7 billion in losses from 92,000 victims who reported. The FBI and the National Council of aging say that tech support fraud agents target the elderly because it is believed that senior citizens have large pensions; they usually have older technology. Bad agents like to impersonate famous brands to get access to their fake repairs.

V. NEW ATTACKS OLD SOCIAL ENGINEERING TECHNIQUES

A. Sextortion

Sextortion is where someone threatens to expose an individual's private or personal information (like pictures, legal history, and eating habits) unless they receive money, naked pictures, or sexual favors. In 2022 Ohio's Internet Crimes Against Children task force and the FBI reported an increase in blackmail attacks against children for pictures. Bad agents have found that fear and shame are ways to get American children to pay their blackmail demands. Also, sextortion can also be a scam within a scam if a bad agent sends multiple photos and asks, "does picture number 1 look familiar?" and that picture is a virus or a piece of Malware. In September 2022, a Minnesota man was sentenced to life for the sextortion of more than 1,100 girls by impersonating a female and using common social media apps.

B. Swatting

Swatting is an act of contacting law enforcement (usually a 911 call). This SEAT starts with a bad agent complaining of extreme violence, gunfire, or a scenario like child endangerment and some form of emergency public safety response against an individual or business. Swatting attacks use "doxing" (the discovery and use of personal information) and often target live-streaming Internet personalities so that the attack can be caught on a live video feed. Some swatters have even faked the victims themselves and their phone numbers. A famous Swatting case in August 2020 involved a Black Lives Matter leader named Melina Abdullah, the attackers made 911 call and then live-streamed police surrounding the victim's house.

C. Deepfakes

Deepfake is an image, video, or audio file created by an individual or AI used to impersonate or alter a specific individual or the representation of that individual. In 2017, a Reddit user named "deepfakes" supposedly made naked pictures and videos of Gal Gadot using her face superimposed over a model's image. Nowadays, the level of deepfake craft has created Elvis voiceovers singing new songs, famous actors switching roles (Jim Carey in the Shining), and politicians saying specific things (Donald Trump doing a Breaking Bad skit). Deepfakes can be used to create fake products in another person's name, extort money, devalue a company by creating bad press, or even grow dissent for a country. A perfect example of using a deepfake is the video of the Ukrainian President Zelensky telling his Soldiers to lay down their arms.

D. Digital Kidnapping

Digital kidnapping is where a bad agent uses an individual's picture or online profile until their targeted victim pays them. These attacks can be as simple as a fake Twitter account making racist remarks or even escalate to a kidnapped loved one by sending falsified pictures with ransom demands at a specific time. While the person in the photo may not be physically harmed, having a stranger present that pictures on social media or altering it is disconcerting to most people, especially when children are involved.

VI. ASEAT SCRIPTS

ASEAT is about using influence and persuasion to get information from people. We have received automated phone calls about our car's warranty and e-mails about drinking water from Camp Lejuene; it's the words these message use to get people (targeted audience) to contact them. Since the dawn of humanity, people have used specific marketing techniques and words to get people to do what they want or have individuals or business entities give them cash. For example, a script for a sextortion attempt against a U Army Soldier with a digitally kidnapped picture of a minor would go, "PVT Snuffy, you have received pictures from my underage daughter, and unless you pay me $200 for her pain, and suffering, I will contact your commander." This short script could be sent in a text message, said over the phone, put on a note on a windshield, and even deadlier, in an official-looking e-mail. That script uses contact information gleaned from a target (phone number, real name, or military unit), local laws (weaponized bureaucracy), a payment amount that the target would quickly pay, and the correct term for that Soldier's boss (commander, first sergeant, boss, human resources, or even parents). Already there are thousands of scripts like this one, found in software (like Caine) or passed around chat groups and are used by hackers, con men, and government entities. The real danger of ASEATs is bad agents finding the right script that makes the opening get their technique into play.

VII. HYBRIDS

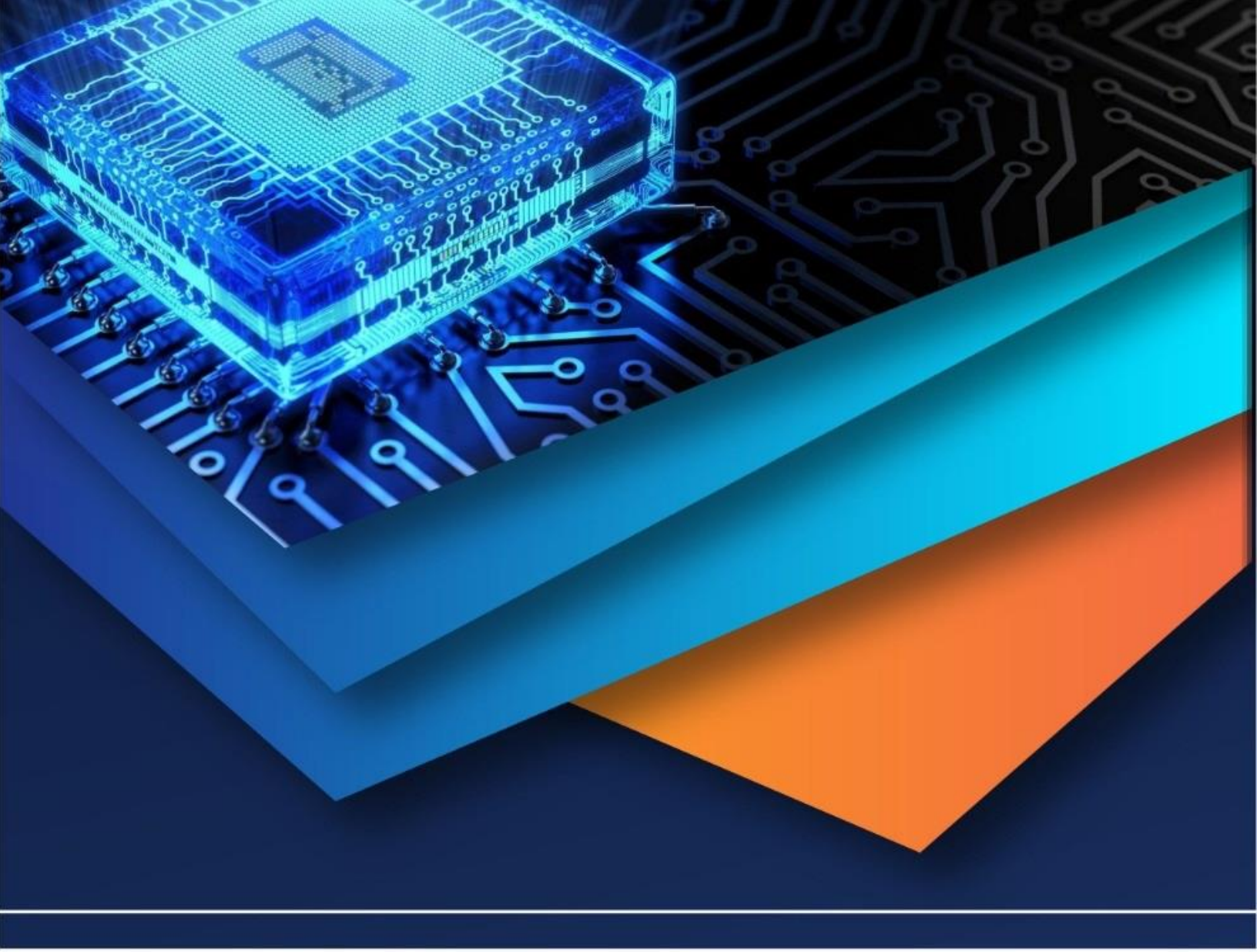
Each of these SEAT types is dangerously profitable by itself, and if you add in parts of the others, find a script that works, and use a honeypot site (fake webpage or server) to show one-off, you have a more effective technique. As bad agents and hackers use their attacks, you will see more combinations of techniques and technology, like a deepfake advertisement in an e-mail leading to a fake webpage holding a MALWARE script. Combining a malware attack with the payment of a specific cryptocurrency and then offering to fix that victim's computer system magically would be very profitable. Bad agents need to use their imaginations on how complex they want their attack to be.

VIII. CONCLUSION

It is 2022, and we carry supercomputers in our pockets; most people use e-mail for communication, we are bombarded by texts daily, and bad agents are using those tools against everyday people. ASEATs make people their worst enemies by having their emotions and common sense tricked by the things they trust. Getting a phone call from their phone company asking about an online transaction is considered normal. Most Americans use online dating apps that advertise people's personal lives and information. Elderly Americans, by definition, are out of touch with current technology and would love to pay a third party to fix their gizmos and help them with a video conference. American police have particular rules of engagement. A 911 call with a screaming child in danger would see an aggressive police response and maybe even a SWAT team engaged in a whole rescue mission. ASEAT is the future of Social Engineering. These techniques and scripts will be more refined and deadly as technology improves. Most of these techniques are easily found for free on the Internet in dubious forums, online classes, and with organized crime. As ASEAT becomes more refined, you will see more attacks, just like the FBI predicted in their 2021 report.

REFERENCES

[1] Singer, P.W., Brooking, Emerson. Like War. (Houghton Mifflin Harcourt Publishing Company 2016), p 53-82.
[2] Murdoch, Don. Blue Team Handbook: Incident Response Edition. (Don Murdoch 2018), p 101-133.
[3] Murdoch, Don. Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases Notes from the Field (V1.02). (Don Murdoch 2018), p 61-245.
[4] Diogenes, Yuri, Ozkaya, Erdal. Cybersecurity-Attack and Defense Strategies. (Packt Publishing 2019), p 377-494.
[5] Federal Bureau of Investigation. FBI Internet Crime Report 2021. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[6] Santos, Omar. Developing Cybersecurity Programs and Policies. Pearson IT Cybersecurity Curriculum, 2018.
[7] Thompson, Eric. Designing a HIPAA-Compliant Security Operations Center: A Guide to Detect and Responding to Healthcare Breaches and Events. Apress, 2020.
[8] Clifford, Ted. SC inmate sentenced for ‘sextortion’ scheme that targeted military. Stars and Stripes, 21, September 2021.
[9] US Army. AR 15-6 Officer’s Training Guide. April 2016. https://usacac.army.mil/sites/default/files/documents/sja/15_6Investigation.pdf
[10] Department of Homeland Security. Increasing Threat of Deepfake Identities. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf
[11] Foley, Joseph. 18 Deepfake examples that terrified and amused the Internet. CB Creative Bloq, 13, September 2022. https://www.creativebloq.com/features/deepfake-examples



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY