F-Secure Threat Intelligence: Scam Tactics & Techniques Framework

INTRODUCTION

F-Secure Scam Tactics & Techniques Framework is a breakdown of how modern-day online scammers operate. According to Global Anti-Scam Alliance, over $1 trillion was lost to scams in 2023. The internet without clear-cut regional borders and worldwide access has become a hotbed for cybercrime that targets consumers globally, every day.

We at F-Secure believe in sharing knowledge. We want to provide a systematic understanding of various types of scams. With this we aim to build a detailed and rich knowledge database about scams, breaking down the high-level tactics and more detailed techniques. This framework is meant to be a formal foundation for researching and building defenses against scams.

This work has been inspired by the MITRE ATT&CK® framework, developed by the MITRE Corporation.

Terminology

Tactics

These represent the broad goals of an adversary. A tactic tells us what the adversary aims to achieve after completing that particular step. For example, the reconnaissance and target acquisition tactic is a collection of all techniques that an adversary may use to gather information about the victim. Tactics make up the columns of the matrix.

Techniques

These represent the methods used by an adversary to achieve a particular goal or tactic. For example, phishing is a technique that can be used as a part of a reconnaissance tactic to gain potentially private information. Techniques make up the rows of the matrix.

F-Secure Scam Tactics & Techniques Framework

This framework consists of 7 tactics and a total of 32 groups of techniques.

1. Reconnaissance and Target Acquisition (4)	**2. Resource Development (6)**	**3. Victim Contact and Engagement (5)**	**4. Persistence of Scam (5)**	**5. Access and exfiltrate information (5)**	**6. Lateral Movement (3)**	**7. Monetization (4)**
Goal: Identify potential victims, based on: ○ Suitability to scam ○ Availability of data ○ Personal interests ○ Demographics	**Goal: Build or acquire resources needed to conduct the scam, including:** ○ Infrastructure ○ Software ○ Services ○ Personas ○ Bait	**Goal: Make contact with victim to deliver bait and engage victim with the bait**	**Goal: Get the scam to persist for as long as needed**	**Goal: Get access to any victim information that is needed to complete the scam**	**Goal: Grow the scam in size**	**Goal: Turn scam into money**
1.1 Establish target pool based on suitability to scam	**2.1 Acquire infrastructure** ○ 2.1.1 Email infrastructure ○ 2.1.2 SMS infrastructure ○ 2.1.3 Telephone infrastructure ○ 2.1.4 Domain services ○ 2.1.5 Website hosting ○ 2.1.6 Other cloud resources ○ 2.1.7 C2 infrastructure	**3.1 Contact and engage victim via email**	**4.1 Psychological manipulation of victim** ○ 4.1.1 Assert authority ○ 4.1.2 Likeability, seduction ○ 4.1.3 Scarcity, urgency ○ 4.1.4 Shaming, intimidation, extortion ○ 4.1.5 Community building, peer pressure ○ 4.1.6 Gradual commitment, positive reinforcement ○ 4.1.7 Reciprocity, create obligation	**5.1 Victim divulges information**	**6.1 Promote scam to victim's contacts**	**7.1 Directly transfer funds from victim to scammer**

1.2 Build manual profiles of targets	**2.2 Develop Software** ○ 2.2.1 Custom malware ○ 2.2.2 OSS project code ○ 2.2.3 Website and script development (victim-side, adversary-side) ○ 2.2.4 Custom platform bots	**3.2 Contact and engage victim via SMS**	**4.2 Modify scammer’s virtual presence**	**5.2 Scammer steals victim information by deploying malware**	**6.2 Compromise victim’s additional online accounts**	**7.2 Indirectly transfer funds from victim**
1.3 Build or acquire target list through automated data collection	**2.3 Acquire services** ○ 2.3.1 Acquire human personnel ○ 2.3.2 Acquire "XYZ“-as-a-Service	**3.3 Contact and engage victim via telephone**	**4.3 Change platform used to communicate with victim**	**5.3 Scammer gains remote digital access to victim’s device**	**6.3 Leverage victim’s access rights**	**7.3 Sell victim assets for profit**
1.4 Build or acquire target list from internet databases / sources	**2.4 Acquire personas & accounts** ○ 2.4.1 Create or acquire real world identities ○ 2.4.2 Create or acquire service identities and accounts ○ 2.4.3 Create or acquire financial accounts	**3.4 Contact and engage victim via online service controlled by 3rd party**	**4.4 Employ malware persistence techniques**	**5.4 Scammer accesses victim information via account takeover or digital impersonation**		**7.4 Engage victim in investment scheme**
	2.5 Develop the bait ○ 2.5.1 Create Bait Email/SMS message ○ 2.5.2 Create Bait Website ○ 2.5.3 Create Bait Ads ○ 2.5.4 Create Bait Reviews, Likes, Engagement ○ 2.5.5 Create Bait Posts ○ 2.5.6 Create Bait Mobile App	**3.5 Contact and engage victim via online services controlled by scammer**	**4.5 Change victim account information**	**5.5 Scammer exfiltrates victim information** ○ 5.5.1 C2 channel ○ 5.5.2 Chat services ○ 5.5.3 Email forwarders ○ 5.5.4 Cloud services		
	2.6 Improve credibility of the bait ○ 2.6.1 Improve Bait with AI ○ 2.6.2 Improve accuracy of brand impersonation ○ 2.6.3 Mask Suspicious URLs ○ 2.6.4 Leverage SEO poisoning ○ 2.6.5 Write social engineering scripts		**4.6 Avoid platform detection or reprisals**			

Phase 1. Reconnaissance and target acquisition

Summary

The goal of this phase is to identify potential victims, based on their personal interests, demographics, online accounts, or contact details. Depending on the scam, this could be a very targeted group, or the scammer may cast a wider net to target a whole population based on their proximity to news events, current events, calendar activities, or the like. The techniques vary, but could include manually hunting for victim details from social media (name, address, interests, etc.), performing automatic data collection, or purchasing personal data of victims from closed sources like illegal marketplaces on the internet. At this phase the scammer may also attempt to perform basic psychological profiling, such as looking for people more likely to fall for the given scam.

Techniques

1.1 Establish target pool based on suitability of scam

Some scams may require a large potential target population that is likely to be susceptible in some way to the scam. The target pool may be constructed because it is potentially affected by a scam-relevant news item, or because the population lives in a particular timezone, region, or is proximal to a particular scam-relevant event. The target population could also be chosen because they are likely to use a scam-relevant piece of software or platform.

Examples:

- Tax Season Scams in the US
  - "The Internal Revenue Service has reported that scammers are impersonating the IRS and texting taxpayers asking for personal information."
- Spain and Portugal Power Outages Spark a Surge in Phishing Attacks
  - "the email is mimicking TAP Air Portugal official communication that informs the victim that they may be eligible for a refund due to the EU's "Air Passengers Rights Regulation"... "The link embedded in the email directs to a credential phishing page designed to steal victims' personally identifiable information (PII) and credit card details."
- Beware of Scammers impersonating Malwarebytes
  - "The download from the fake website was an information stealer with a filename that resembled that of the actual Malwarebytes installer."
- Scammers Exploit Ukraine War & Japan Earthquake Fears to Spread Malware on X
  - "scammers have recently begun to diversify their bait, using sensational news stories to lure users"
- Phony job scams target new graduates
  - "new grads are targets because they may not know how real job offers are handled."

1.2 Build manual profile(s)

An adversary may manually gather information about potential victims in order to build a targeted profile of them. Personal details, such as victim's contact networks, location, nationality, political inclination, religious beliefs, hobbies, sexual orientation, etc., recent breakups or family tragedies, are used in profiling by adversaries to formulate specific strategies to scam victims. Additionally, scammers may specifically look for victims who have accounts on particular apps, websites, or discussion groups. For example, an online account on a dating website or app indicates that the user is possibly open to a relationship. Similarly, accounts on crypto mining websites indicate interest in cryptocurrency.

Examples:

- How scammers are targeting your age group
  - Shows each age demographic and the scams that work best for those
- How modern identity thieves profile victims
  - "Just by using a regular web browser, they can find many of your online accounts, your photos, possibly your place of work, information about your educational and work history, and much more besides. They can use this information to get into your accounts, find people close to you, and ***generally 'get to know you.'***"
- Profile of a scam victim
  - "...while I might look overwhelmingly average, ***there are actually certain things about me that criminals target*** when choosing their next victim."

1.3 Acquire information about target(s) through automated data collection

To build lists of targets or to acquire personal details of targets, adversaries may perform automated data collection to gather large amounts of raw data, which can then be further filtered and polished to desired granularity. Such automated data collection can be performed on various online resources, each with a different result.

Adversaries may scrape websites or social media sites to acquire personal information about victims. If the scammer already has an existing list of targets, they may scrape websites or social media sites to find additional personal details about them that can be used in the scam. Or, the scammer may use web scraping to generate a list of potential victims. In either case, the end goal is always to get more information about targets of the scam. The data gathered in this phase can also be misused in the later stages of the scam, such as helping the scammer to build fake social media profiles, to create fake product listings on shopping sites, or to apply for loans by impersonating the victim. Data such as photos, videos and voice might also be used to create fake online identities or to create AI-generated content such as voice clones or video deepfakes.

Examples:

- For sale: Your personal profile via web scraping
  - "***Web scraping, or crawling***, is a huge data mining operation that both crooks and legitimate operators use to get hold of every personal detail about you that they can."
- Six arrested for AI-powered investment scams that stole $20 million
  - "***Victims were chosen via algorithms that selected persons whose profiles matched the cybercriminal's targeting requirements*** and subsequently targeted by AI-generated deepfake ads."

- AI-generated phishing scams target corporate executives
    - "British insurer Beazley and ecommerce group eBay have warned of the rise of fraudulent emails containing ***personal details probably obtained through AI analysis of online profiles"***
    - "[AI] can also ***scrape a victim's online presence and social media activity to determine what topics they may be most likely to respond to*** — helping hackers generate bespoke phishing scams at scale."

1.4 Acquire information about targets from internet databases or special sources

Adversaries may purchase lists of targets or data about targets from special-purpose sources such as illicit marketplaces, people search databases or data brokers, insider-produced lists / "lead generation" services, or public records.

Examples:

- How to Get Off a Scammer's 'Sucker List'
    - "A sucker list is an aggregate list of names, addresses, phone numbers, and other ***personal information that is created, sold, and bought by scammers***, spammers, and dishonest telemarketers."
- SoK: Digging into the Digital Underworld of Stolen Data Markets
    - "We look back at the past 15 years of research on ***stolen data markets*** to uncover the underlying patterns and trends, documented by researchers."
- Infostealer Malware: An Introduction
    - Describes the sale of ***infostealer logs for credential harvesting*** – even when the data is past its prime, it is still useful for scam targeting
- Kazakhstan detains over 140 for allegedly selling citizens' data via Telegram channels
    - "The networks primarily targeted Russian citizens, promising high returns on cryptocurrency investments. In reality, victims lost their life savings."
- Following the AnyDesk Incident: Customer Credentials Leaked and Published for Sale on the Dark Web
    - "The availability of this ***data for cybercriminals*** could serve as a catalyst for new attacks, including targeted phishing campaigns."
- Michigan person collects fraudulent loan amounts by misusing data from BeenVerified
    - "Investigators say he bought large amounts of personal information on the site, using the data as a foundation to open bank accounts in as many as 51 people's names."
- Firms sell elderly Americans' data to telemarketing con artists
    - "Richard Guthrie, a 92-year-old U.S. Army veteran ...was on scam artists' lists because his name, like millions of others, ***had been sold by large companies to telemarketing criminals***, who then turned to a major bank to steal his life's savings."
- Data Brokers, Elder Fraud, and Justice Department Investigations
    - "Three data brokers ***knowingly sold Americans' data to scammers***—and the Department of Justice charged them."

Phase 2. Resource Development

Summary

The goal of this phase is to build or acquire resources needed to conduct the scam, including technical infrastructure used to run the scam, as well as the bait used by the scammer to lure the victim. These resources could include physical entities such as computers and human scammers, or it could include virtual resources such as websites, social media accounts, malware, and the like.

Techniques

2.1 Acquire infrastructure

Adversaries may set up, purchase, or steal a variety of technical infrastructure needed to run the scam. Infrastructure may be built for conducting specific scam attacks or it could be generalized for reuse in other scams.

2.1.1. Email infrastructure

Adversaries may require email services for different phases of the scam, for example to send phishing emails. These email services may be purchased, rented, or stolen. Adversaries may also subscribe to SMTP relay services or bulk email services to accomplish the scam.

Examples

- Analyzing Email Services Abused for Business Email Compromise
    - "We observed services offered by Gmail, Hotmail, and Outlook as the top choices for BEC campaigns."
- Scam of the Week: Spoofed SMTP Relay Services

2.1.2. SMS infrastructure, SMS gateways

If the scam requires SMS contact with victims, an adversary could purchase, rent, or construct an SMS gateway. SMS gateways are used to mass send text messages to phone number(s) at a relatively low price.

Examples:

- SMS Gateways allow cybercriminals to flood phones with smishing messages

2.1.3. Telephone infrastructure

Adversaries may require telephone infrastructure as part of the scam. For example, in order to dial multiple numbers in quick succession, they may need to use robodialers or phone number spoofing technology. Voice-over-IP (VoIP) technology and SIM/eSIM technology can be used to assist with navigation between global telephone providers. For some advanced scams, adversaries may even attempt to spoof a cellular base station in order to intercept communications, using equipment and services often referred to as “SMS Blasters” or IMSI catchers.

Examples:

- Phone number spoofing
- Bangkok Police Arrests Scammers Carrying IMSI-catchers

2.1.4. Domain services

For scams that require a web domain, adversaries may purchase domains or may employ free-to-use domain names. Adversaries use several techniques to make their domains appear more legitimate: they may compromise existing domains, they may “typosquat” by registering a domain name that resembles a legitimate domain, or they may purchase established domains with lapsed registrations. Adversaries may also employ domain generating algorithms to create and register hundreds of domains at a time. To improve the quality of the scam with HTTPS-enabled connection, adversaries either purchase SSL certificates for the domain names from Certificate Authorities or generate free certificates using services such as Let’s Encrypt. Domains and websites without SSL certificates (i.e. HTTP connections) prompt errors and might not function on modern browsers, so encrypting website connections with HTTPS has become standard for adversaries.

Examples:

- What is typosquatting?
- Phishing Trends Report
  - “An increasing number of phishing sites now use HTTPS to appear legitimate. In 2024, approximately 80% of phishing websites feature HTTPS, complicating detection for users.”

2.1.5. Website hosting

Adversaries use websites to serve malicious content, redirect to other websites, insert forms for stealing information or serve malware. Websites can be hosted on a physical server, cloud-based server or using serverless technologies. Adversaries can also rent servers from bulletproof hosting providers that have lax terms and conditions and refuse takedown requests from international or local law enforcement.

Examples

- Phishing with CloudFlare Workers: Transparent phishing and HTML smuggling
- Details of bulletproof hosting
- Cloaking services (example mentioned here: https://www.malwarebytes.com/blog/threat-intelligence/2023/04/massive-malvertising-campaign-targets-seniors-via-fake-weebly-sites)

2.1.6. Cloud resources

Adversaries may acquire resources in the cloud to host malicious content. Adversaries may purchase such resources or use or abuse publicly available resources for malicious purposes. For example, adversaries can use Content Delivery Networks (CDNs) or DDoS protection to hide the original IP address of their malicious site or C2 server. File hosting offered by cloud services can be used to host malicious websites. IP Tunneling can be used by adversaries to make a website hosted on computer localhost available to the public internet. The tunneling works by setting up a daemon of, for instance, Cloudflare on the server or computer where the website is hosted and it can be exposed to the internet. They can also exploit misconfigured cloud services for e.g. spamming. Finally, DDoS protection services, such as CloudFlare and similar, can also be used to hide source IP address.

Examples:

- Domain fronting to hide C2 server
- Cloudflare abused in the wild
- Microsoft warns top file hosting services hijacked for email scams
- Misconfigured AWS accounts are fuelling phishing campaigns

2.1.7 C2 infrastructure

Adversaries may choose to develop and deploy Command and Control (C2) server, or use free-to-use C2 servers developed by other adversaries. Some C2 server capabilities can also be rented or bought. C2 server is used together with malware installation to issue further commands to malware on victim's device. C2 can also be used to harvest and store victim's personal information. In the latter example, C2 server can be used as a database or a "dashboard" for accessing and cataloguing stolen information.

Examples:

- Google services misused for C2 servers
- Telegram as C2 server

2.2. Develop software

Adversaries may need to develop and deploy their own custom software to accomplish the scam.

2.2.1 Custom malware

Adversaries may write custom malware that is deployed as a part of the scam. Some custom malware templates can be obtained for free online. Such malware will conduct malicious activities on the victim's device such as information stealing, file encryption or destruction for ransoming, and so on. Since custom malware can be quite expensive to create and maintain, this is less commonly used in scams, and when it is, it is usually reserved for high-value targets such as people with large cryptocurrency holdings. For alternatives, see "2.3 Acquire Services."

Examples

- Slow Pisces Targets Developers With Coding Challenges and Introduces New Customized Python Malware
  - "In this campaign, Slow Pisces ***engaged with cryptocurrency developers on LinkedIn***, posing as potential employers and sending malware disguised as coding challenges."
- StilachiRAT analysis: From system reconnaissance to cryptocurrency theft
  - "Scans for configuration data of 20 different ***cryptocurrency wallet extensions*** for the Google Chrome browser" in addition to other data such as credentials and cookies.

2.2.2 OSS project code

Some scams involve malicious custom code deployed into open source software (OSS) repositories or open source libraries used in other software packages. An unsuspecting user will run the code and be infected with malware.

Examples:

- Malware found in NPM packages with 1 million weekly downloads
  - 17 popular Gluestack '@react-native-aria' packages with over 1 million downloads ***were compromised to include malicious code*** that acts as a remote access trojan (RAT)
- Malicious code on GitHub: How hackers target programmers
  - "We discovered over ***200 repositories with fake projects on GitHub***. Using them, attackers distribute stealers, clippers, and backdoors."
- Large Scale Campaign Created Fake GitHub Projects Clones with Fake Commit Added Malware
  - "a large-scale campaign ***targeting random GitHub repositories with project clones*** containing credential stealing malware and remote shell execution on top of the original code"

2.2.3 Website and script development

Many scams require a website, whether to provide an interface to collect phishing details or as a shield of legitimacy for a fake company. Website development can include static pages, victim-side scripts that run in the browser, and adversary-side scripts that control the backend functions of the website. Shopping carts, payment software, and chatbot software can also be integrated into websites to give a veneer of legitimacy to the site. When phishing tools are bundled together and sold as a product, they are sometimes called a "phishing kit." Other website-located malware, such as Magecart attacks, inject malicious code into legitimate websites in order to steal user information.

Scam Website Examples:

- List of scam websites in 2025: 25 suspected fake shopping sites
  - 25 screenshot examples of fake shopping websites
- Karen Bags Scam Exposed: How This Fake Store Is Stealing from Shoppers

    - “Investigations reveal that Karen-Bags.com is part of a larger ***network of fraudulent online stores***. These sites often share similar layouts, product offerings, and marketing strategies, indicating a coordinated effort to defraud consumers.”
- Guide to Chatbot Scams and Security: How to Protect Your Information Online and at Home
    - “If they clicked on the email link, they were eventually directed to a chatbot. The chatbot conversation may have seemed trustworthy to some users since it included a captcha form, email and password prompts, and even a photo of a damaged package.”

Phishing Website and Phishing Kit Examples:

- Phishing Examples
    - Dozens of screenshot examples of phishing websites
- Phishing Kit Trends and the Top 10 Spoofed Brands of 2023
    - “Each phishing kit deployment corresponds to a single phishing attack, and a kit could be redeployed many times during a phishing campaign.”
- How Phishing Kits Work: Unpacking Cybercriminal Tools in 2024
    - “[Phishing kits are] “all-in-one” solutions that include fake website templates, scripts for data collection, tools to evade detection, and detailed setup instructions.”

Malicious Website Script Examples:

- JavaScript-Enabled Phishing Attacks: Unmasking the Deceptive Layers of Malicious Sites
    - "***JavaScript can be manipulated to display phishing content*** and, more alarmingly, redirect unsuspecting users to number generator gambling games”
- How we train AI to uncover malicious JavaScript intent and make web surfing safer
    - “new AI model that allows us to detect the exact ***malicious intent behind each script***...provides deeper visibility into client-side threats”
- The Art of Concealment: A New Magecart Campaign That’s Abusing 404 Pages
    - "In this campaign, all the victim websites we detected were directly exploited, as the ***malicious code snippet was injected*** into one of their first-party resources.”
- What is Magecart?
    - “Magecart attackers ***copied JavaScript payment forms*** from [website] and then modified the form to make it send the payment information to a server controlled by the actors.”

2.2.4 Custom platform bots

Some scams require victims to interact with malicious bots on instant messaging platforms, websites or social media. These bots can be custom-made, obtained for free online or purchased.

Custom Platform Bot Examples

- Phishing with Telegram bots
    - “...hackers used a [Telegram] bot known as SMSRanger to pose as representatives from banks and companies like PayPal, Apple Pay, Google Pay, and commonly used mobile carriers. ...***the bot calls and convinces the user to give up personal information***, bank account logins, passwords, and even two-factor authentication (2FA) codes.”
    - How Scammers Use Telegram for Phishing Calls, a Breakdown (video)
- Scammers are using Telegram verification bots to inject crypto-stealing malware
    - Fake Telegram Verification Bots steal crypto (X post)
    - “Once in the Telegram group, users are asked to verify through “OfficialSafeguardBot,” ***a fake verification bot*** that “creates artificial urgency” with short verification windows”..."The bot then injects a malicious PowerShell code that downloads and runs malware to compromise computer systems and crypto wallets.”
- These 11 New Discord Scams Can (and Will) Steal Your Data
    - “You may receive ***multiple DMs from a bot*** about securing free Nitro — however, Discord does not create giveaway bots that make this offer.”

2.3 Acquire Services

Adversaries might require additional capabilities, resources, or know-how to facilitate the scam.

2.3.1 Acquire Human Personnel

Human personnel are used to scale operations to reach multiple victims. Adversaries can recruit other individuals on online forums and pay them to develop malware, translate text, or conduct social engineering attacks. These groups are loosely affiliated and typically not associated with traditional organized crime families or gangs. However, some large scale scam operations also have been found running in physical locations that resemble call centers. Scammers have been known to staff these locations with both paid labor and forced labor. Operating this type of large-scale “scam center” or “scam compound” is sometimes associated with organized crime groups, since they bring skills in related criminal enterprises such as money laundering and human trafficking.

Examples:

- Cyber Crime ‘Help Wanted’: Job Hunting on the Dark Web
  - “Wannabe hackers will create threads in specific sections of a forum for topics, such as malware and phishing, and explain their skillsets in order to find work. And criminal groups, or even individual threat actors looking for help, will also announce when they are seeking assistance and then outline the requirements.”
- Diamonds, Dior and Dubai vacations: The Luxurious Lives of Georgia’s Call-Center Scammers
  - “From their nondescript offices in the center of Tbilisi [Georgia], this group of around 85 scammers and support staff brought in $35.3 million from over 6,100 “customers” around the world between May 2022 and February 2025, according to internal spreadsheets used to track incoming funds and office expenses.”
- Cyber Scamming Goes Global: Sourcing Forced Labor for Fraud Factories
  - “So-called “fraud factories” have their roots in Southeast Asia’s gambling industry and are closely tied to Chinese organized crime groups....After the victims travel to the location of the “job,” traffickers confiscate their passports, lock them in heavily guarded compounds, and force them to conduct scams.”

2.3.2 Acquire XYZ-as-a-Service

Adversaries who lack certain technical expertise can also purchase or rent these services, such as malware-as-a-service or phishing-as-a-service. The ‘XYZ’ here indicates any service that enables the adversary to conduct scams. Such service models allow adversaries to leverage advanced malware and phishing capabilities, while outsourcing the development and maintenance to external developers.

Examples:

- Android Malware-as-a-scam service being used by scammers
  - “Developers use different applications to load different phishing pages, which are eventually sold to scammers. In our research, more than 100 unique phishing URLs and more than 100 unique C2 URLs are created in these malicious applications. It means that each scammer can carry out scam activities independently.”
- Infostealer Malware: An Introduction
  - “Modern infostealers operate within a sophisticated Malware-as-a-Service (MaaS) ecosystem....”
- Pakistan Arrests 21 in ‘Heartsender’ Malware Service
  - Heartsender is “a once popular ***spam and malware dissemination service*** that operated for more than a decade. The main clientele for HeartSender were organized crime groups that tried to trick victim companies into making payments to a third party...”
- The Telegram phishing market
  - “Support includes providing updates on a regular basis for the phishing tools, anti-detection systems and links generated by the phishing kits.”

2.4 Acquire personas and accounts

2.4.1 Create or acquire real world identities

To further the scam or obfuscate related criminal activities, adversaries may create fake personas and identities or they may steal other people’s identities. Fake identifications can include fabricated or stolen passports, national ID cards, driving licenses, utility bills, and other documents. Fake identities serve multiple purposes from obscuring identities from victim(s) and law enforcement, to opening financial accounts for monetary transactions or money laundering or setting up shell companies for illegal business use-cases and so on. Fake personal identification might involve creation of new identities using a combination of real and fake data – this is often referred to as ‘Synthetic Identity Fraud’.

Examples:

- The Top 10 Most Forged ID Documents (2022)
  - “Fraudsters fake documents from certain countries depending on existing loopholes, document security levels, and how often fraud occurs in a given jurisdiction.”
- Synthetic Identity Fraud: Creating Fake Identities for Crime
  - “…scammers, who build a new identity with a combination of real and fake information, create a phony identity by starting with single legitimate information, unlike traditional identity fraud.”
- Scams to steal college financial aid are using AI for identity theft
  - “In January, Wayne Chaw started getting emails about a class he never signed up for at De Anza Community College, where he had taken coding classes a decade earlier. Identity thieves had obtained his Social Security number and collected $1,395 in financial aid in his name.”

2.4.2 Create or acquire online identities or accounts

Depending on the scam, adversaries may require a variety of accounts at various service providers, including online services, social media, sales platforms, payment processors, and the like. In addition to creating entirely new online personas and accounts to further the scam, some adversaries may also steal accounts with established identities, or they may create accounts that impersonate well-known brands, celebrities, or influencers.

Email Account Examples:

- Threat Spotlight: Bait attacks
  - "Moreover, to avoid being detected, the attackers typically use ***fresh email accounts from free services***, such as Gmail, Yahoo, or Hotmail, to send the attacks."
- What Is Email Age Score and Why It Matters
  - "The Email Age Score ... serves as a proxy for risk – newer, low-activity email addresses often correlate with ***fake or fraudulent signups***."
- Millions of Stolen US University Email Credentials for Sale on the Dark Web
  - "They also can use them for ***phishing or gaining further access*** to university financial, research, and other potentially lucrative information."

Messaging and Social Media Account examples:

- Google finds 10,000 fake listings on Google Maps, sues alleged network of scammers
  - "The lawsuit, announced Wednesday, claims a man working within a wider network, ***created and sold fake business profiles*** on Google Maps."
- These 11 New Discord Scams Can (and Will) Steal Your Data
  - "One of the most common Discord Nitro scams starts with a direct message (DM) from an unknown contact..."
- The 'fake' Google review scam causing chaos in Manchester
  - "One day a scam company will have 1.5k reviews but the next day will drop down to around 500 because the AI system took them down. But the problem is a few days later they are back up, so it never really ends."

Advertising Service Account Examples:

- Malvertising Scam Uses Fake Google Ads to Hijack Microsoft Advertising Accounts
  - Google said "that it takes steps to prohibit ads that seek to dupe users with the goal of stealing their information, and that it has been actively working to enforce countermeasures against such efforts"
- What are Fake Ads?
  - Google "may ask you to verify ownership of a business by providing details about business operations or upload documentation…." On Facebook and Instagram, "Scammers will usually first create several fake profiles, 'borrow' images from real brands, then start running targeted ads to scam unsuspecting users."

Seller Accounts Examples:

- Fake address, fake name, fake deal: Facebook Marketplace scams are rampant. Here are some to watch out for
  - "The three people Machado messaged all appeared to be Toronto locals with 50 to 100 photos of themselves on their Facebook profile page."
- Amazon Blocked Opening of 800,000 Fake Seller Accounts in 2022
  - "The downward trend in bogus seller accounts is clear as Amazon said criminals' attempts to create new selling accounts fell from six million in 2020 to 2.5 million in 2021 to 800,000 last year."

App Store and Developer Accounts Examples:

- Meet The Fakers - Profiles Of Suspected Fake Apple App Store User Accounts
  - "Scammers setup computers that maintain a ton of bogus user accounts (also known as bots) to download an app multiple times so that the app seems popular and will start appearing on the Top Charts and will have better visibility in App Store search."
- Apple's tightly controlled App Store is teeming with scams
  - "In a recent news release, Apple said it employed new tools to verify the authenticity of user reviews and last year kicked 470,000 app developer accounts off the App Store. Developers, however, can create new accounts and continue to distribute new apps."

2.4.3 Create or acquire financial service accounts

In order to pay for services related to the scam or to plan for eventual monetization of the scam, an adversary may need to set up accounts to handle financial transactions. Brick-and-mortar banks, online-only banks, peer-to-peer (P2P) payment services, and cryptocurrency exchange accounts are all options for transferring funds, but different companies can have different expectations for how much customer legitimacy is required. Traditional, legitimate banks typically follow "Know Your Customer" laws, which require documentation of a customer's identity. They also place strict limits on how much money can be moved without triggering alerts. However, adversaries might still leverage traditional bank accounts for criminal activities, particularly when the scam involves a money launderer or "money mule" participating in the scam. Online banks, sometimes referred to as “neobanks” or “digital banks”, operate fully online with no physical bank locations, which might make it easier for adversaries in some situations to skirt around rules and regulations, use fraudulent identification, and the like. Peer-to-peer payment services can facilitate easy transfer of funds between victim and scammer, and in some instances the services might lack fraud protection and investigatory power of traditional banks and credit card companies. Cryptocurrency exchanges can assist a scammer in moving money between virtual and fiat currency, but can vary widely in their level of adherence to regulatory requirements about identification and fraud prevention.

Banking Examples:

- Keeping up with Fraud: How Neobanks Can Identify and Prevent Them
  - “Fraudsters try to open new accounts by mimicking legitimate customers or using stolen or synthetic identities to obtain a line of credit.”
- Romance scammers turn victims into “money mules”, creating a legal minefield for investigators
  - “In the first months of her online relationship with a man calling himself Frank Borg, Laura Kowal was showered with love notes and spent hours on giddy phone calls. By year two, those exchanges were methodical and transactional, with Frank instructing Kowal how to set up fake companies and bank accounts to move money.”
- The Scammer’s Manual: How to Launder Money and Get Away With It
  - “The money mule can be a person or a shell company that controls a local bank account or a cryptocurrency wallet.

Peer-to-peer Examples:

- Avoid Scams with Peer-to-Peer Payments
  - “Because the money being sent is available to the recipient almost immediately, P2P platforms are popular options for scammers, and many of these apps lack the fraud protections of traditional banks and credit cards.”
- PayPal ‘Friends and Family’ payment scams
  - “If a seller is encouraging you to send a 'Friends and Family' payment when you're buying a good or service, you should refuse. You could be dealing with a scammer who knows that your payment won't be covered by [PayPal’s] Purchase Protection if it's a 'Friends and Family' payment.”

Cryptocurrency Exchange Examples:

- Introduction to Cryptocurrency Exchange Compliance
  - “A large part of crypto-related compliance ...includes implementing local and international anti-money laundering and countering the financing of terrorism (AML/CFT) measures to prevent abuse of their products and services.”
- Crypto exchange OKX latest target of DOJ, hit with $505M penalty over AML, KYC failures
  - “One of world’s largest cryptocurrency exchanges agreed to pay more than $500 million in penalties and plead guilty to anti-money laundering (AML) and Know Your Customer (KYC) violations, along with failing to register as a money transmitting business with the U.S.”

2.5 Develop the bait

As part of the scam, the adversary sometimes will create “bait” that is sent to the victims to act on. Whether the bait takes the form of an email, message, advertisement, or some other artifact, it needs to be crafted carefully so that the victim engages with it.

2.5.1 Create Bait Email or SMS Message

Emails and SMS messages are both common delivery methods for scam bait. Emails have an advantage in that consumers already receive many legitimate emails from businesses, and there are fewer length and content issues than with SMS. However, SMS messages have a high open rate, making it likely the potential victim could actually engage with the message. Scammers can purchase phishing kits to help them craft effective email and SMS messages.

Examples

- Smishing Statistics 2025: The Latest Trends and Numbers in SMS Phishing
  - “Mobile users are expected to receive an estimated 147 million smishing texts per day in 2023, representing a 20% increase over the previous year.”
- CryptoChameleon: New Phishing Tactics Exhibited in FCC-Targeted Attack
  - “this kit enables attackers to build carbon copies of single sign-on (SSO) pages, then use a combination of email, SMS, and voice phishing to trick the target into sharing usernames, passwords, password reset URLs and even photo IDs from hundreds of victims”
- Anatomy of a Phishing Kit

2.5.2 Create Bait Website

For some scams, adversaries will build a fake website designed to covertly extract users' personal or financial information. Other websites will be designed to give an air of legitimacy to a scam, such as with a fake shopping website or product review scam. Adversaries may create such websites manually or may use phishing kits to automate the development process.

Examples

- Quick, cheap and dangerous: how scammers are creating thousands of fake pages using phishing kits
  - "Using phishing kits, even an inexperienced phisher can create hundreds of phishing pages in a short time."
- How to Recognise a Copycat Website
  - "The copycat site appears to be the 'authorised' government site and gets the mouse click by a consumer."

2.5.3 Create Bait Advertisement

Adversaries may purchase online advertisements that have been produced specifically for scamming victims, or they may build their own advertisements. Potential victims will sometimes see scam ads as sponsored search engine results, or the ads might be delivered personally to victims via social media profiles or popular messenger services.

Examples

- Massive malvertising campaign targets seniors via fake Weebly sites
  - "The threat actor is creating hundreds of fake websites via the Weebly platform to host decoy content to fool search engines and crawlers while redirecting victims to a fake computer alert."
- 75% of top brands fall victim to fraud in Google Search Ads.
  - "Scammer trick consumers by impersonating the targeted brand's domain and ad copy. They intentionally pay for ad placements that show up when users search for those brands."
- Android users lose $2.4 million to malware scams that use Facebook and TikTok ads as bait
  - "After victims leave their contact details to indicate their interest in particular goods or services on a Facebook or TikTok advertisement, scammers would contact their victims through WhatsApp messaging and request a token sum as membership fee"
- Meta faces increasing scrutiny over widespread scam ads
  - "a major report revealed that thousands of fraudulent ads have been allowed to run on its platforms"

2.5.4 Create Bait Product Reviews, Likes, Engagement

Adversaries may purchase fake reviews, stars, subscriptions, and likes.

Examples

- Inside the Underground Market for Fake Amazon Reviews
  - "The Facebook groups Oak discovered were ***marketplaces where reviews and ratings were bought and sold***. Agents shared lists of products available for reviewers—one of the spreadsheets Oak saw had more than 10,000 products on it"
- Instagram virus creates fake 'likes' and followers in lucrative marketing scam
  - "A virus typically used to steal credit card information has been repurposed to target Instagram, ***generating fake "likes" and followers, and selling them*** online. As Reuters reports, these fake "likes" are then sold in batches of 1,000 on online forums, and can fetch surprisingly high prices. According to security firm RSA, 1,000 Instagram followers sell for around $15 online, while 1,000 "likes" selling for $30"

2.5.5 Create Bait Posts

Scammers can create fake social media or platform posts in order to boost the likelihood of more potential victims seeing the bait, or in order to spread malicious links.

Examples:

- Bump This Post: How this social media scam preys on your desire to help other people
  - “Better Business Bureau spokesperson Melanie McGovern says the goal of these posts is to get as much engagement as possible before editing them to look like something completely different.”
- Beware of scammers changing Facebook posts after you share them
  - “Once people have shared the posting, the scammer edits it to show the scam post.”
- Cyberattackers Hide Infostealers in YouTube Comments, Google Search Results
  - “Threat actors are posing as "guides" offering legitimate software installation tutorials to ***lure viewers into reading the video descriptions or comments***, where they then include links to fake software downloads”
- Beware! YouTube Videos Promoting Cracked Software Distribute Lumma Stealer
  - “This is not the first time pirated software videos on YouTube have emerged as an effective bait for stealer malware.”

2.5.6 Create Bait Mobile App

Adversaries may create fake apps for popular mobile platforms. These apps may carry out a variety of tasks such as providing fake functionality, stealing information, etc. As part of scam campaigns, adversaries may target victims using their smartphones, enticing them to install such scam apps and further continue with the scam attack. A quick way for scammers to build such mobile apps is to copy real apps and add malicious code.

Examples:

- Scam Apps – What Are They and How to Avoid Them?
  - “scammers copying legitimate smartphone applications but injecting them with malicious code to spy on users and steal personal data”
- How to spot and avoid fake apps
  - “A cybercriminal can register themselves as a developer on any app store, download a legitimate app, and rewrite it using malicious code. Then, they can upload their fake app to the app store.”

2.6 Improve credibility of the bait

The better the quality of the bait, the more likely it will be that the potential victim will engage with it. The adversary can use AI or other techniques to create more realistic scam bait.

2.6.1 Improve Bait with AI

Scammers use artificial intelligence to create convincing images and texts. They also use it to create voice clones and video deepfakes. All of these improvements lend additional credibility and authenticity to the scam bait.

- Deepfake YouTube Ads of Celebrities Promise to Get You ‘Rock Hard’
  - “The ads ...have been running since at least November 12 and have around 300 variations according to Google’s Ad Transparency Center.”
- How ‘Deepfake Elon Musk’ Became the Internet’s Biggest Scammer
  - “An A.I.-powered version of Mr. Musk has appeared in thousands of inauthentic ads, contributing to billions in fraud.”

2.6.2 Improve Quality of Brand Impersonation

When impersonating a brand, whether in a phishing email, an advertisement, or a fake website, scammers have figured out different techniques to create copycat content that closely resemble the originals.

- Beware of scammers impersonating Malwarebytes
  - A “cybercriminal is using fake websites for security products to spread malware...The download from the fake website was an information stealer with a filename that resembled that of the actual Malwarebytes installer.”
- New Morphing Meerkat Phishing Kit Mimics 114 Brands Using Victims' DNS Email Records
  - “new phishing-as-a-service (PhaaS) platform ... to serve fake login pages that impersonate about 114 brands”
- Classic DHL scam
- Fake axis bank app scam

- Elon Musk fake account scams

2.6.3 Mask Suspicious URLs

In order to hide suspicious URLs from the potential victim, an adversary may generate a QR code or use a URL shortening service.

Examples:

- Link shortening service used for scams
    - “Researchers found... a three-year-old link shortening service that is catering to phishers and malware purveyors”
- BEWARE: Fake parking ticket scam targets Atlanta drivers
    - “According to ATL DOT, real city issued parking tickets will not have QR codes like the fake tickets do.”
- Beware of 'Quishing': Criminals Use QR Codes to Steal Data
    - “The scammers slapped stickers with fake QR codes on the pay stations. Drivers who scanned them were directed to a website that asked them to enter their credit card or bank account information.”

2.6.4 Leverage SEO Poisoning

Adversaries may create content that tries to manipulate search engine rankings so that their malicious content appears among the top results.

Examples:

- Scammers are optimizing SEO results to lure victims
    - “Scammers have realized that they can also use SEO to find more victims and convince them into clicking on a link if their websites appear higher in search engine results.”
- Pope Francis’ Passing Triggers Surge of Phishing, SEO Poisoning, and Fake Images
    - “Here, bad actors pay to elevate their fake websites to the top of search results, making them appear legit.”

2.6.5 Write social engineering scripts

Scammers will often write social engineering scripts that they can use when interacting with victims over the telephone or on other platforms. By having a pre-planned, professional-sounding script, the scammer can design a process that is fool-proof and easily replicable. The script can then be used by multiple people working as a group or as part of a scam call center.

Examples

- Understanding Scam Strategies
    - “We analysed 341 conversations between scammers and scam baiters sourced from YouTube.”
- Investment Fraud Script (NY, 2022)
    - “We are about to listen in on a telephone conversation between a boilerroom scam artist and a potential investor. The swindler is lying.”
- Medicare scam script (training skit; fiction)
    - “Below is a sample skit demonstrating a common scenario with the new Medicare card phone scam
- Scam script examples

Phase 3. Victim Contact and Engagement

Summary

The goal of this phase is to make contact with the victim in order to deliver the bait and to further engage victim with the scam.

Techniques

3.1 Contact and engage victim via email

Adversaries may send malicious links directly in email to the potential victim, or they may also include email attachments containing malicious links, malware, fake invoices, and the like.

Examples

- Fake Norton Invoice / Subscription Renewal Scam
  - “Emails and text messages that impersonate Norton often try to create a sense of urgency by threatening to charge your credit card unless you respond.”
- Avoid losing your Netflix account via fake "Update Your Payment Details" email
  - “The goal of this phishing email is to obtain the account's log-in credentials and potentially the victim's financial information.”
- About fake X emails (X official)
  - “some people may receive fake or suspicious emails that look like they were sent by X. These emails might include malicious attachments or links to spam or phishing websites.”
- Phishing Campaign Using Private Video Sharing (Youtube official)
  - “We’re aware that phishers have been sharing private videos to send false videos, including an AI generated video of YouTube’s CEO Neal Mohan announcing changes in monetization.”
- 5 Common Email Scams, with Examples

3.2 Contact and engage victim via SMS

Adversaries may send phishing SMS messages that trick users into starting a conversation or that contain malicious links. Phishing SMSs use the same tactics as in emails, with the exception that they tend to be more concise.

Examples

- 7 Smishing Examples and How to Protect Yourself
  - “And only 65% of Americans say they would delete a text if it came from an unknown sender. With these kinds of numbers, the odds are in hackers’ favor.”
- 15 Spam Text Message Examples & How to Identify them
  - “Criminals use phishing text messages to attain usernames and passwords, social security numbers, credit card number,s and PINs to commit fraud or identity theft. Other attacks focus on duping people into downloading viruses or malware by clicking seemingly innocent links.”
- How many robotexts are Americans getting?
  - Up-to-date statistics on the proliferation of robotexting

3.3 Contact and engage victim via telephone

Adversaries may make fake calls to victims, or some scams have the victims call the adversary. Phone calls happen in real-time, and can convey a sense of trust, urgency, or danger, which may not be possible via other techniques.

Examples

- Bogus customer service is just the latest online scam you need to be aware of
  - “Scammers know too well how to build a trap by planting fake customer service numbers online for well-known major airlines, banks, insurance companies, cable companies, online retailers and more.”
- Example of Phone Call Phishing Scam (Script)
- How To Spot, Avoid, and Report Tech Support Scams
  - “Tech support scammers often call and pretend to be a computer technician from a well-known company. They say they’ve found a problem with your computer.”
- Scammers Use Fake Emergencies To Steal Your Money
  - “Someone calls or contacts you saying they’re a family member or close friend. They say they need money to get out of trouble.”
- Crocodilus malware adds fake entries to victims' contact lists in new scam campaign
  - “The malware’s latest version can ***insert fake entries into victims’ contact lists***, allowing attackers to impersonate trusted sources — such as bank support lines — and trick users into answering fraudulent calls”

3.4 Contact and engage victim via online service controlled by a third party

Adversaries might contact victims directly via social media or instant messaging platforms. The potential lures used on such platforms include fake celebrity endorsements, fake product offers, fake job interview calls, fake lottery winnings, etc. For some scams, such as romance scams and investment scams, the adversary may target victims and make initial contact with them on a specialty site such as an online dating platform or cryptocurrency enthusiast website.

Examples

- LinkedIn List of Scams (LinkedIn official)
  - “These scams typically involve people pretending to be recruiters or employers offering high-paying jobs for little work. These can include mystery shopper, work from home, or personal assistant scams.”
- Avoiding Scams on Facebook (Facebook official)
- Romance Scams: How to Protect Yourself Online (Tinder official)
- Woman Says She Was Conned By Scammers On Facebook, And Social Media Giant Won't Remove Post

3.5 Contact and engage victim via online services controlled by the scammer

In some scenarios, the scammer does not reach out directly to the potential victim. Instead, the victim finds the scammer’s malicious website or app through other means such as targeted advertising, links in comments sections of a website, or by lookalike web domains or lookalike app names.

Examples

- Watch out for "free" movie and television scams during big events
  - Cybercriminals “are baiting users with the offering of free first run movies, popular television shows and events. Using shortened links such as bit.ly to mask the true URL, once a victim clicks on the link, they are redirected to a false site that claims to provide the content.”
- BBB Tip: How to identify a fake website
  - “One way fake websites trick people is by using a domain name that is extremely close to a real business’ or organization’s domain name. Upon closer examination, you might notice that two letters are swapped or it’s just slightly misspelled.”

Phase 4. Persistence of Scam

Summary

The goal in this phase is to ensure that the scam is able to be completed. The scammer will employ various techniques to persist the scam for as long as is necessary.

Techniques

4.1 Psychological manipulation of victim

Whether scams involve direct or indirect contact, the scammer may employ a variety of psychological manipulation techniques on the victim in order to get them to comply.

4.1.1 Assert authority

- Scam Alert: Pretending to be a local authority
  Posing “as an authority figure, such as a police officer, government official, or bank representative, ...scammers may use official-sounding language and threaten you with fines or arrest in order to scare you into giving them money or information.”

4.1.2 Employ likeability, seduction

- Expert explains the devastating psychology of romance scams after “Brad Pitt” fraud case
  - “Although it is mocked and misunderstood, romance fraud is based on complex psychological mechanisms that exploit victims’ trust, emotions and vulnerability.”
- "When can we be together - forever?" A deep dive into emotional scamming
  - “a scammer builds an emotional connection with someone, often on dating platforms, with the intention of exploiting their trust for financial gain.”

4.1.3 Create scarcity, urgency

- How the Scarcity Principle is Used in Online Scams and Attacks
  - “one of the reasons the scarcity principle works is because ‘things that are difficult to attain are typically more valuable.’ As the result, humans use the availability of an item as a heuristic for assessing its quality.”
- Analysing urgency and trust cues exploited in phishing scam designs
  - “this paper uses deductive thematic analysis to examine how phishing scam designs employ urgency and trust cues”

4.1.4. Exploit victim's shame

- Threats and extortion scams
  - "Once the scammer has an intimate image or video of you, they threaten to share it with your family, friends, or people you know unless you give them money."
- Sextortion scams are trending — here's how to deal with them
  - "The main purpose of the message is to establish fear in the victim that some-one has been monitoring their online activities that many find "humiliating" or "embarrassing".

4.1.5 Build peer pressure, social validation

- The Psychological Tactics Behind Fraud - How Scammers Exploit Human Behavior
  - "Another frequently employed technique is the use of social validation, wherein scammers leverage peer pressure to convince victims of the legitimacy of their requests. By citing other supposed victims or success stories, they create a herd mentality that facilitates compliance."

4.1.6 Leverage gradual commitment, positive reinforcement

- The Psychology of Being Scammed
  - "Scammers ask their potential victims to make small steps of compliance to draw them in, and thereby cause victims to feel committed to continue sending money."

4.1.7 Create obligation or reciprocity

- The Psychology Behind Scams: 7 Manipulation Techniques to Watch Out For
  - "Scammers might send you a small gift or offer a free service in hopes of triggering this feeling and making you more likely to comply with their requests later."
- Reciprocity: An Antecedent to Fraud Compliance and Unethical Behavior
  - Scammers exploit "the social norm of reciprocity is that we feel obligated to repay those who have provided a favor to us"

4.2 Modify scammer's virtual presence

In order to persist the scam, the scammer may delete, change, or add new scam personas or online presences. This can include introducing new characters into the scam, removing online comments, advertisements, taking down malicious websites, and so on.

Examples:

- The life cycle of phishing pages
  - "In most cases, phishing pages remain unchanged throughout their active period, although they can change.", "half of the links were already inactive within less than a week after detection", "Cybercriminals have to adapt their phishing pages to keep up with these offers and make the pages as convincing as possible."
- Behind the Screens: Real-World Examples of Thread Hijacking and Multi-Persona Attacks
  - "attackers are now also executing multi-persona hijacking by assuming multiple identities or personas to build trust with targets—often across multiple communication channels."

4.3 Change platform used to communicate with victim

Another technique to keep the scam going as long as possible is to convince the victims to move conversations to a different messenger under the pretext of greater safety and security.

Examples:

- Why Scammers Move from Social Media to Messaging Apps: Understanding the Tactics and Risks
  - "Scammers often try to move their targets off of social media platforms" in order to have less platform oversight, to build trust in a private setting, and to execute a wider range of scams.
- Pig butchering scam asking to move to messengers of the adversary's choice
  - "Pig butchers prefer to interact with potential victims via messaging services instead of on social media platforms"

4.4 Employ malware persistence techniques

For scams that are malware-based, the scammer may employ common techniques for extending the life of the malware and avoiding detection by the victim.

- 11 Critical Malware Persistence Mechanisms You Should Be Familiar With!
  - "The goal of persistence is to evade detection and removal by security software or the user and to continue to cause harm to the system and its user."
- Awesome Malware Persistence

    - “Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.”

4.5 Change victim account information

For an account-based scam, one of the first things a scammer will do when they get access to a victim’s account information is to change password and password recovery details for the account. This ensures that they will have a longer amount of time to work with the account to accomplish their scam. They may also change contact details, change account recovery options, and enable or change multi-factor authentication (MFA) settings on the account.

- How To Tell If Your Facebook Has Been Hacked Right Now
    - “In many cases, you’ll know immediately that your Facebook account has been hacked when you can’t log in by using your usual password. In other scenarios, Facebook hackers may want to hide their actions by working in the background — without locking you out of your account.”
- Port-Out Fraud Targets Your Private Accounts
    - Scammers will “con the victim's phone company into believing the request to port out the number is from the authorized account holder. If the scam is successful, the phone number will be ported to a different mobile device or service account set up by the scammer”

4.6 Avoid platform detection or reprisals

Shopping scammers will often use fake tracking numbers in order to buy themselves time with a victim who has not received a package. Tracking number fraud also allows the scam seller to claim innocence when their victim reports the transaction as “Item Not Received.” Scammers can generate fake tracking numbers, or they might re-use tracking numbers from a prior delivery, or they might ship a low-cost, low-weight item so they can claim that the package did arrive.

- How To Know If You’ve Received a Fake USPS Tracking Number
    - “The USPS tracking number was for a package that had already been delivered to a different address.”
- Can a tracking number be fake?
    - “Fake tracking numbers are created by scammers to mislead recipients into believing their packages are on the way.”

Phase 5. Access and Exfiltrate Information

Summary

The goal of this phase of the scam is to get access to any victim information that is needed to complete the scam. The information a scammer is seeking can take many forms, and the scammer may need multiple kinds of information in a single scam.

Techniques

5.1 Victim divulges information

In this technique, adversaries lure or deceive the victims into sharing their own sensitive information.

Examples

- Social engineering scams
    - “criminals trick victims into giving out confidential information and funds”
- What Is Pretexting?
    - “Like any other type of social engineering, the perpetrator’s goal is to convince their victim to give them something—generally information, access, or money—under false pretenses.”

5.2 Scammer steals victim information by deploying malware

In this technique, the adversary deploys malware onto a victim’s device to steal information.

- Malware Scams: A Complete Guide
- How Spyware and Malware Are Used in Online Credit Card Fraud
    - “Without your knowledge, spyware runs in the background recording your Internet browsing habits and keystrokes, monitoring the programs you use and collecting your personal information. This can lead to serious consequences such as credit card fraud and identity theft.”
- Banking scams sent on WhatsApp
    - Scam leverages “Whats-App direct messages that encourage targeted users to down-load malicious Android installation files.”

5.3 Scammer gains remote digital access to victim’s device

Here the adversary uses screen sharing software or a remote access tool to access the victim’s device.

- What are Remote Access Scams?
    - “Once the victim is persuaded [that they need technical support help], the scammer instructs them to download and install a legitimate remote desktop access tool like TeamViewer, AnyDesk, or UltraViewer.”
- How to Avoid Remote Access Scams (AnyDesk official)
    - “scammers can try to misuse AnyDesk (or any other remote access software) to connect to your computer and steal data, access codes, and even money”
- TeamViewer can be used to exfiltrate files from victims’ devices

5.4 Scammer accesses victim information via account takeover or device impersonation

An adversary may attempt recovery of accounts using compromised information, or may impersonate the victim’s devices. One technique is SIM card swapping, wherein the adversary orders a new SIM card with the victim’s details, thus giving the scammer control over the victim’s phone number.

- SIM swapper gets 18-months for involvement in $22 million crypto heist
    - “The funds were stolen following a January 2018 SIM swap attack that allowed Truglia's co-conspirators to hijack Terpin's phone number and fraudulently transfer roughly $23.8 million in cryptocurrency from his crypto wallet to an online account under Truglia's control.”
- What Is Account Takeover Fraud (ATO)?
    - “ATO fraud is not limited to banking and credit card accounts. Attackers can also use rewards cards and services, including stored points on hotel accounts and airline miles.”

5.5 Scammer exfiltrates victim information

The adversary may exfiltrate data from the victim by simply downloading it, by syncing the victim’s cloud storage data, by setting an email forwarder, or by leveraging command-and-control (C2) infrastructure.

5.5.1 Exfiltrate victim information with C2 channel

In this technique, adversaries establish a channel with a command-and-control (C2) server either by using existing resources or building their own server from scratch. The data acquired from the victim is sent to such a C2 server either in plaintext, archived, or encrypted and archived form. The C2 channel can be custom or could use a publicly available service (such as Google Drive, Amazon, etc.) for hosting. Using a publicly available service provides the adversary with an advantage of hiding in plain sight.

Examples

- What is C2? Command and Control Infrastructure Explained
    - “C2 channels are often bidirectional, meaning an attacker can download or “exfiltrate” data from the target environment in addition to sending instructions to compromised hosts.”
- Inside FireScam : An Information Stealer with Spyware Capabilities
    - “The malware is disguised as a legitimate app to trick users into installing it, where it then steals sensitive information and exfiltrates data to Firebase C2 endpoint.”
- Lazarus Group Targets Bitdefender Researcher with LinkedIn Recruiting Scam
    - "This [login] data was then exfiltrated to a malicious IP address that appeared to contain other malicious files on the server.”
- Detecting Malware Abusing Google for Command-and-Control
    - “Although Google Sheets offers significant capabilities for users, it has inadvertently become a valuable tool for threat actors and malware for command-and-control (C2).”
- Detecting Malicious C2 Server Traffic via Google Calendar Phishing Attack Using Wazuh & Suricata

- Hiding in the Cloud: Cobalt Strike Beacon C2 using Amazon APIs
    - “Researchers at Rhino Security Labs have developed a way to use Amazon’s AWS APIs for scalable malware Command and Control (C2)”

5.5.2 Exfiltrate victim information using a chat or messaging service

Messaging and communication platforms such as Telegram or Discord have easy-to-operate bot APIs and are often misused by adversaries to become C2 servers to exfiltrate and store sensitive data.

- Cybercriminals Use Telegram Bots to Exfiltrate Data In Phishing Kit Campaign
    - “cross-platform phishing campaign that utilizes Telegram as its primary exfiltration channel”

5.5.3 Exfiltrate victim information using email forwarders

- Email forwarding rule
    - “Adversaries routinely create email forwarding rules in compromised email accounts to collect sensitive information while hiding suspicious email activity from legitimate users.”

5.5.4 Exfiltrate victim information to cloud services

- Exfiltration Tools: How Cybercriminals Make Off with Your Data
    - “Threat actors prefer Rclone due to its fast data-transfer capabilities and versatility. Rclone can integrate with numerous cloud services, including Google Drive, Amazon S3, and Mega

Phase 6. Lateral Movement

Summary

The goal of this phase is to grow the scam in size, either in number of victims or potential value of information gained.

Techniques

6.1 Promote the scam to victim’s contacts

The adversary may promote the scam using the victim’s email contacts, SMS contacts, or social media contacts, sometimes impersonating the victim to make contact with these new potential victims. The scammer may also use the victim’s identity to create social media posts, comments, and direct messages to promote the scam and find additional victims.

Examples

- What To Do If You're Getting Spoofed Calls From Your Contacts
    - “spoofers abuse the technology and make fake calls from your contact list to get your personal or financial details”
- Scam 'missed parcel' SMS messages: advice on avoiding malware
    - “The malware will also attempt to access your contact list, and send scam SMS messages to these numbers as well”
- FluBot analysis study
    - “Once the device is infected, FluBot sends the contact list in the user’s address book to the C2. From this point, the C2 operators can decide to start the SPAM operation, sending SMS to the victim’s contacts and later blocking said numbers to prevent the infected users from noticing unusual behaviour”

6.2 Compromise victim’s other online accounts

The adversary may attempt to gain additional leverage by compromising the victim’s other accounts. To do this, the scammer may attempt password resets, password stuffing (using the credentials of one service on another service), or compromising the victim’s Single-Sign-On (SSO) privileges.

Examples

- Port-Out Fraud Targets Your Private Accounts
    - After a successful port out fraud with the phone company, “the scammer, by receiving the victim's private texts and calls, ***tries to reset the access credentials for as many of the victim's financial and social media accounts as possible*** before the victim realizes they have lost service on their device. Once the scammer has access, they attempt to drain the victim's bank accounts. In another variation, the scammers may attempt to sell or ransom back to the victim access to their social media account”

6.3 Leverage victim’s access rights

The scammer will attempt to gain elevated privileges, for example by accessing the victim’s administrator or employee privileges, in order to spread the scam to other accounts, to gain additional information from the victim, or to find additional victims.

- What Is Privilege Escalation? Types, Examples, and Prevention
- FBI warns of gift card fraud ring targeting retail companies
    - “Upon infiltrating an employee's account, ***the attackers move laterally through the network***, trying to identify the gift card business process and pivoting towards compromised accounts linked to this specific portfolio.”

Phase 7. Monetization

Summary

The goal of this phase of the scam is to turn data or access into money.

Techniques

Adversaries work on a “for-profit” mindset, so all the previous tactics employed by the adversary necessarily lead to this end goal of monetizing the scam. Depending on timing, geography, technology availability, risk aversion, and many other factors, the scammer will attempt to both extract as much money as possible from the victim while also ensuring compliance by the victim.

7.1 Directly transfer funds from victim

In some scame, it may be possible for the adversary to gain funds directly from the victim, in the form of a credit card payment, bank transfer, cryptocurrency payment, peer-to-peer payment service transaction.

Examples

- Bank impersonation scams robbing Australians of their life savings
    - “The caller will tell you to ***transfer money to a different account*** to ‘keep it safe’ or for ‘further investigation’."
- Advance Fee Fraud: The Emergence of Elaborate Crypto Schemes
    - “Cashing out the full balance, however, ***requires the victim to first deposit some Bitcoin to the platform***, which is the point of the scheme.”
- Don't Be Fooled by These Devious Venmo, Cash App and Zelle Scams
    - “Apps like Zelle, Venmo, Cash App and PayPal make it easy to send money to others. ***With a click of a button, your cash is gone*** -- and it can be nearly impossible to get it back if you send it to a scammer.”

7.2 Indirectly transfer funds from victim

Some scams require an indirect monetization scheme, in which the adversary indirectly extracts funds from the victim. For example, the scammer might clone the victim’s credit card in order to make purchases or withdraw cash, or the scammer might force the victim to buy gift cards which the scammer can convert to cash.

Examples

- What is carding? How this type of fraud works and how businesses can prevent it
    - “Carding is the illegal practice of obtaining, trafficking or using credit card information without authorisation – often to purchase gift cards or prepaid cards.”
- How criminals use Uber and Airbnb to launder money stolen from your credit card
    - “they recruit Airbnb hosts or Uber drivers to turn fraudulent funds into clean cash”
- Why would a scammer want a Steam card?
    - “Once the scammer obtains the card's code, they can quickly redeem it on their own Steam account or sell it on the black market.”
- About gift card scams (Apple official)
    - “If someone asks you to use Apple gift cards to purchase something not sold by Apple, you might be the target of a scam.”

7.3 Sell victim assets for profit

An even more indirect method of monetization might involve the scammer attempting to profit from the victim's assets or information. For example, the adversary could steal the victim’s identity to take out bank loans. The adversary could sell the victim’s stolen data or other assets, including physical or virtual property. The scammer might also use victim resources for cryptocurrency mining.

Examples

- Telegram is a hotspot for the sale of stolen financial accounts
  - “Telegram is increasingly abused by cybercriminals to set up underground channels to ***sell stolen financial details*** to pseudonymous users.”
- Loan Fraud Explained: How Scammers Get Free Money In Your Name
  - “If a criminal steals your identity, ***they can get loans*** on cars, homes, and businesses in your name.”
- Kaspersky: more than 36 million AI & gaming credentials compromised by infostealers in 3 years
  - “These accounts are often initially stolen using data-stealing malware and then leaked on the dark web via infostealer log-files, ***where they can be further monetized as valuable asset***s within the realm of cybercriminal activity.”
- What is cryptojacking? An overview + prevention tips
  - “Cryptojacking is a form of malicious cryptomining that allows cybercriminals to mine cryptocurrency using another entity’s computing power.”

7.4 Engage victim in investment scheme

The adversary could get money from a victim as part of one or more shady investment schemes.

Rug pulls, exit scams, and pump and dump schemes are all types of fraud in which perpetrators disappear with a victim’s funds—whether by draining a crypto project's liquidity (rug pull), shutting down a business without delivering promised goods/services (exit scam), or artificially inflating an asset's price through false promotion before selling at the peak (pump and dump).

A Ponzi scheme is a fraudulent investment operation that pays returns to existing investors using capital from new investors rather than from legitimate business profits, inevitably collapsing when new recruits become insufficient.

A pyramid scheme is a business model that recruits members with promises of payments for enrolling others into the scheme rather than from selling legitimate products, creating an unsustainable structure that enriches early participants at the expense of later ones.

Fake cryptocurrency trading platforms are apps that purport to help “investors” make profits in online trades. The apps show the victim graphs and balance sheets indicating that they have earned profits, but the balances and graphs that the victim sees are fake. Once the victim tries to withdraw their "gains", the scammer disappears with all the money and the app becomes inaccessible.

Examples

- Latest evolution of ‘pig butchering’ scam lures victim into fake mining scheme
  - “These scams promise regular income at high rates of return for investment in a “liquidity pool” that loan cryptocurrency to make contract-based trades between different cryptocurrencies possible.”
- The Cryptory Ponzi Scheme (Bitcointalk) and Cryptocurrency Scams: Analysis and Perspectives