TLP WHITE Threat Intelligence Report: Pig Butchering

leave a comment »

This threat intelligence report was created in tandem between Scot Terban and the ICEBREAKER intel analyst created and trained by Scot Terban.

Pig Butchering 杀猪盘

The “Pig Butchering” scam is an increasingly prevalent form of financial fraud that blends elements of romance scams, investment schemes, and cryptocurrency fraud. Originating in

Southeast Asia and known as “Shāz Hū Pán” in Chinese, which literally means pig butchering, this scam involves a series of manipulative steps to defraud victims of their money by exploiting their trust and desire for profitable investments.

Background on Pig Butchering:

Origin and Early Development

The exact inception of pig butchering scams is hard to pinpoint, but they gained notable attention around the mid-2010s. Initially, these scams were localized and primarily targeted individuals in Asian countries. Scammers operated mainly through social media platforms and dating apps, where they could easily create fake profiles to initiate conversations with potential victims.

Current State

Today, pig butchering scams represent a significant and growing threat in the realm of financial fraud. They have become more diverse in their approach, targeting not just individuals looking for romantic connections but also those interested in financial investments and cryptocurrency. The scams have caused billions of dollars in losses worldwide, prompting international law enforcement agencies to take action. However, their decentralized nature, combined with the use of technology to anonymize and automate operations, makes them particularly challenging to combat.

The evolution of pig butchering scams from simple romance scams to complex financial frauds underscores the adaptability of cybercriminals and the need for continuous vigilance and education among internet users globally.

Pig Butchering Manuals on the Internet

In the shadowy corners of the internet, there exists a disturbing trend that fuels the proliferation of pig butchering scams: the availability of comprehensive manuals and guides. These documents, often found on dark web forums, encrypted messaging apps, and even in some cases on public websites, serve as step-by-step instructions for aspiring scammers. They detail methodologies for executing sophisticated financial frauds, specifically targeting individuals across the globe through social engineering tactics.

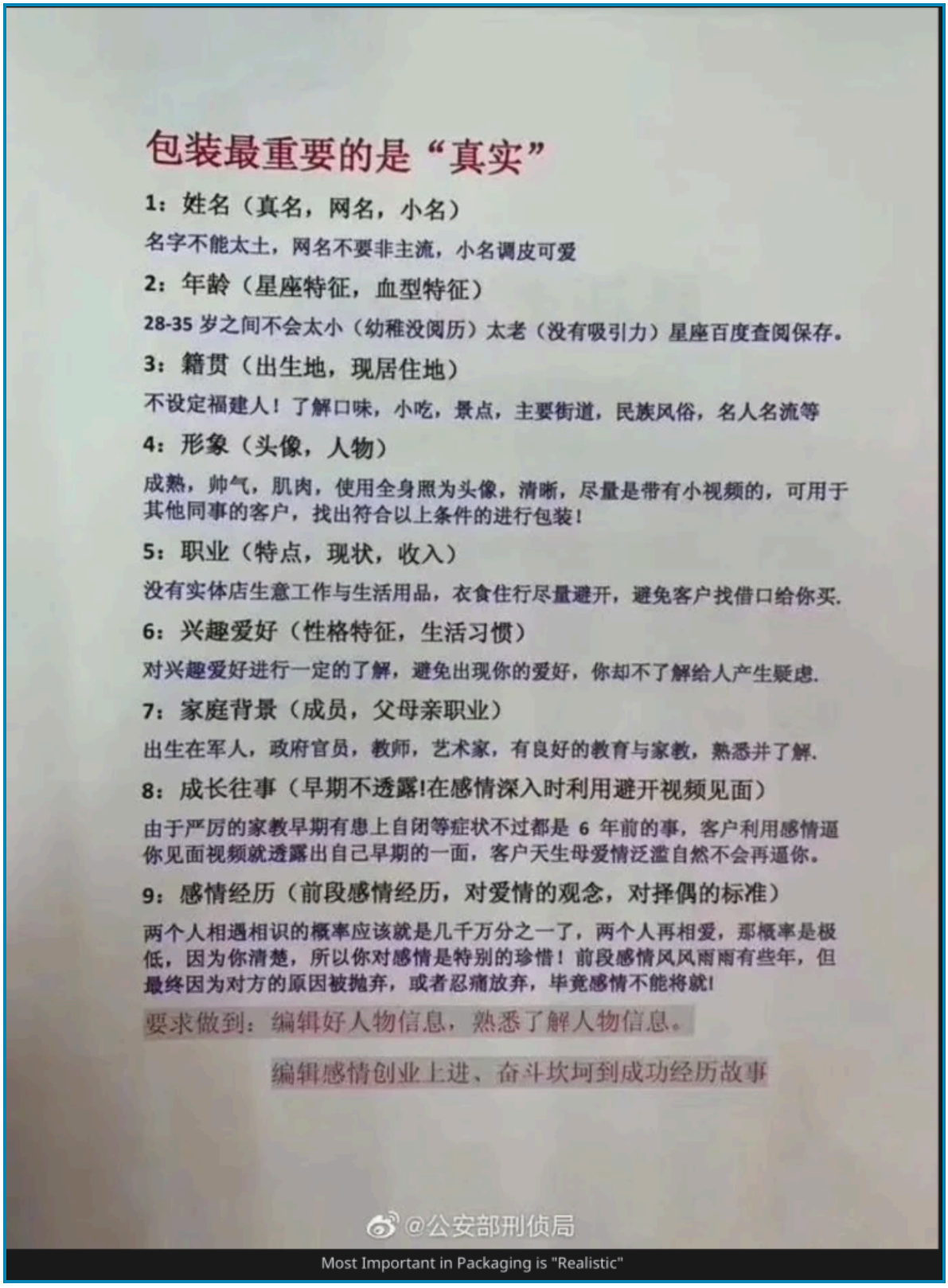
Contents of the Manuals

最新杀猪攻略

（公司机密，严禁外传，后果自负）

二零一九年三月（第四版）

Latest Strategy for Killing Pigs



These manuals are disturbingly thorough, covering aspects such as:

- **Profile Creation:** Instructions on creating believable fake profiles on social media and dating apps, including tips on selecting attractive photos and crafting compelling backstories.
- **Initial Contact Strategies:** Scripts and conversation starters designed to initiate contact with potential victims, often tailored to different personalities and backgrounds to increase the chance of a connection.
- **Trust Building Techniques:** Detailed guides on how to build rapport and trust over time, including how to mimic emotional intimacy and feign shared interests.
- **Investment Fraud Schemes:** Step-by-step guides on luring victims into fake investment opportunities, including the setup of counterfeit cryptocurrency trading platforms and the illusion of profitable returns.
- **Handling Objections:** Advice on how to counter skepticism from potential victims, including psychological tactics to overcome objections and reassure targets of the legitimacy of the investment opportunities.
- **Extraction and Evasion:** Techniques for convincing victims to transfer funds, followed by strategies for disappearing without a trace, including how to launder money and evade law enforcement.

The Dark Marketplace

These manuals are often sold or traded in the darker parts of the internet, acting as a commodity within a marketplace that profits from the spread of fraudulent activities. Their existence highlights a professionalization of online scams, with individuals seeking to capitalize on the knowledge and tools needed to exploit others.

The existence of pig butchering manuals on the internet represents a significant challenge in the fight against online financial fraud. By understanding and addressing the root causes and distribution networks of these manuals, stakeholders can work together to reduce the impact of pig butchering scams on individuals and society.

Tactics, Techniques, and Procedures (TTPs)

Initial Contact and Trust Building: Scammers initiate contact with potential victims through various online platforms, including dating sites, social media, and messaging apps. They often create fake profiles and reach out with friendly messages, sometimes claiming to have received the victim's contact details by mistake or posing as an old acquaintance. This phase can involve a slow build-up of trust over weeks or months, where the scammer engages in regular, personal conversation to establish a rapport.

Introduction to Investment: Once a level of trust is established, the conversation gradually shifts towards investment opportunities. Scammers present themselves as successful investors or share insider tips about lucrative investments, often involving cryptocurrencies. They promise high returns in short periods, using persuasive language and manipulated evidence to make their claims appear legitimate.

Fake Investment Platforms: Victims are then directed to download a specific app or visit a website to make their investments. These platforms are controlled by the scammers and are designed to appear legitimate, often allowing victims to see fake returns on their investments to encourage further deposits.

Increasing Investments: Scammers may allow victims to withdraw a small portion of their "profits" to build further trust. They then encourage victims to invest more money, often citing opportunities for even higher returns. At this stage, victims are deeply entangled, financially and emotionally, making it hard for them to discern the scam.

The Slaughter: When victims attempt to withdraw their funds, they find themselves unable to do so. Scammers may claim that additional taxes or fees need to be paid to access the funds. Eventually, the scammers disappear, and the victims are left with significant financial losses.

Psychological Tactics Used by Pig Butchers

Pig butchering scams exploit a range of psychological tactics designed to manipulate victims into parting with their money. Understanding these tactics can help individuals recognize and resist such scams.

Building Trust and Rapport: Scammers invest significant time in building a relationship with their victims, often posing as a romantic interest or a friend. This creates a sense of trust and lowers the victim's defenses, making them more susceptible to suggestions of investment.

Creating a Sense of Urgency: By presenting investment opportunities as time-sensitive, scammers pressure victims to act quickly, bypassing their usual decision-making processes. This urgency discourages thorough research or consultation with others.

Providing Social Proof: Scammers may share fabricated success stories or use fake profiles to create an illusion of widespread success among investors. This tactic exploits the victim's fear of missing out on a lucrative opportunity.

Exploiting Loneliness or Emotional Needs: By offering companionship or understanding, scammers target individuals who may be feeling lonely or emotionally vulnerable, making them more receptive to the scammer's suggestions.

Mimicking Legitimacy: Using sophisticated fake platforms and documents, scammers create an aura of legitimacy around their investment opportunities. This makes the scam seem credible and reduces skepticism.

Open Source Intelligence (OSINT) Tactics by Pig Butchers

Pig butchering scams, known for their manipulative and deceitful approaches, often involve the use of Open Source Intelligence (OSINT) by scammers to enhance the effectiveness of their schemes. OSINT refers to the collection and analysis of information gathered from publicly available sources to support decision making. In the context of pig butchering scams, scammers leverage OSINT to gather detailed information about potential victims, tailoring their approaches to exploit specific vulnerabilities, interests, and emotional states.

Depth of OSINT Performed

Social Media Analysis: Scammers meticulously comb through potential victims' social media profiles, extracting information about their personal interests, employment history, relationship status, and recent life events. This data allows them to craft personalized and convincing narratives, making their fraudulent propositions more appealing.

Public Record Searches: Utilizing public databases and records, scammers can uncover additional information about a target's financial status, property ownership, and even familial connections. Such details enable a more targeted approach, including investment scams that seem tailored to the victim's financial capabilities and interests.

Data Breach Exploitation: Scammers often exploit data from breaches that include personal information, email addresses, and passwords. By analyzing this data, they can attempt to gain unauthorized access to personal and financial accounts or use the information to bolster their credibility and trustworthiness.

Forum and Group Monitoring: By monitoring discussions in online forums and groups, especially those related to investments or cryptocurrencies, scammers identify potential targets who express interest in investment opportunities or demonstrate a lack of experience in the financial domain.

Employment and Professional Network Analysis: Professional networks like LinkedIn provide a wealth of information about a target's career, professional skills, and network. Scammers use this information to pose as recruiters or potential business partners, offering fraudulent investment opportunities aligned with the victim's professional interests.

Countermeasures and Awareness
To mitigate the risk of falling victim to pig butchering scams amplified by OSINT, individuals and organizations should adopt several countermeasures:

Privacy Settings: Regularly review and adjust privacy settings on all social media and professional networking platforms to limit the amount of publicly accessible information.

Awareness and Education: Stay informed about the latest scam tactics and educate friends and family on the importance of safeguarding personal information online.

Critical Evaluation: Approach unsolicited investment opportunities with skepticism, especially those received from new online contacts or those that appear too good to be true.

Use of OSINT for Self-Assessment: Periodically conduct OSINT on oneself to understand what information is publicly accessible and could potentially be used by scammers.

Reporting and Sharing: Report suspected scam activities to relevant authorities and share experiences within your network to raise awareness and prevent others from becoming victims.

By understanding the depth of OSINT performed by pig butchers and adopting appropriate countermeasures, individuals can better protect themselves against these sophisticated scams.

Counter Tactics for End Users

To counteract these psychological manipulations, end users can be taught several strategies:

Verify Independently: Always verify the identity of new online contacts independently, and be skeptical of investment opportunities shared by them. Use search engines and official websites to check the legitimacy of any investment platform.

Slow Down Decision Making: Resist the urge to make quick investment decisions, especially under pressure. Take time to research and consider the implications of any financial commitment.

Seek Second Opinions: Before making an investment based on an online acquaintance's advice, consult with trusted friends, family, or financial advisors. A second opinion can offer a fresh perspective and identify potential red flags.

Educate About Scams: Awareness and education are powerful tools against scams. Learning about common scam tactics and indicators can help individuals recognize and avoid falling victim to them.

Use Strong Digital Hygiene: Maintain strong privacy settings on social media and be cautious about sharing personal information online. This reduces the likelihood of being targeted by scammers.

Report Suspicious Behavior: Encourage users to report any suspicious behavior or investment propositions to relevant authorities or platforms. Reporting can help prevent scammers from exploiting others.

By teaching these counter tactics, individuals can be better prepared to recognize and resist the psychological manipulations employed by pig butchering scammers.

Emerging Tactics Seen

- **Group Chats and Social Engineering:** Scammers are evolving their strategies by using group chats to target multiple victims simultaneously. They add potential victims to fake investment chat groups, where they promote their schemes before moving to one-on-one conversations to finalize the fraud. This approach allows scammers to cast a wider net and manipulate victims more efficiently.

Prevention and Awareness

To avoid falling prey to pig butchering scams, individuals should be wary of unsolicited investment advice, especially from new online acquaintances. Verify the legitimacy of investment platforms independently and be cautious of any requirement to pay upfront fees or taxes to withdraw investment returns. Always approach online relationships and investment opportunities with skepticism, particularly if they promise guaranteed returns.

This scam highlights the importance of cybersecurity awareness and the need to be cautious when engaging with strangers online or making investments based on advice received through social media or messaging apps.