TLP WHITE: Threat Intelligence Report: GoldPickaxe Malware Family and GoldFactory Cybercrime Group

leave a comment »

Executive Summary

In a comprehensive investigation conducted by Group-IB, a new and sophisticated cluster of banking Trojans, spearheaded by the previously unknown GoldPickaxe malware, has been uncovered. This cluster is part of a concerted effort by a threat actor dubbed GoldFactory, targeting the Asia-Pacific region with a specific focus on Vietnam and Thailand. The GoldPickaxe family, including variants for both Android and iOS platforms, signifies a notable evolution in mobile banking Trojans, incorporating advanced techniques such as the collection of facial recognition data, identity documents, and the interception of SMS to facilitate unauthorized access to victims' banking accounts through the use of AI-driven deepfake technology.

GoldPickaxe Malware Family

The GoldPickaxe family is derived from the GoldDigger Android Trojan and is distinguished by its capability to target both Android and iOS platforms. The malware employs innovative distribution methods, including the use of Apple's TestFlight and the manipulation of victims into installing Mobile Device Management (MDM) profiles, granting attackers full control over affected devices.

Key Capabilities:

- **Collection of Sensitive Information**: Including facial recognition data, identity documents, and SMS interception.
- **Use of Deepfake Technology**: To bypass biometric security measures for banking fraud.
- **Sophisticated Distribution Methods**: Exploiting TestFlight and MDM profiles for distribution.

GoldFactory Cybercrime Group

Attributed to the development and dissemination of the GoldPickaxe malware family, GoldFactory is identified as a well-organized, Chinese-speaking cybercrime group. This group exhibits a high degree of sophistication in its operations, utilizing social engineering, deepfake technology, and a broad arsenal of malware to target financial institutions and their customers.

Connections and Evolution:

- **Connection to Other Malware Families**: Including ties to the Gigabud malware.
- **Geographical Focus and Expansion**: Initially targeting Vietnam and Thailand, with indications of expanding operations.

Indicators of Compromise (IoCs)

The IoCs associated with the GoldPickaxe malware family and GoldFactory group are crucial for detection and prevention efforts. These include but are not limited to:

Files and Hashes:

- **GoldPickaxe.iOS**: `4571f8c8560a8a66a90763d7236f55273750cf8dd8f4fdf443b5a07d7a93a3df`
- **GoldPickaxe.Android**: `b72d9a6bd2c350f47c06dfa443ff7baa59eed090ead34bd553c0298ad6631875`
- **GoldDigger**: `d8834a21bc70fbe202cb7c865d97301540d4c27741380e877551e35be1b7276b`
- **GoldDiggerPlus**: `b5dd9b71d2a359450d590bcd924ff3e52eb51916635f7731331ab7218b69f3b9`

GoldPickaxe / GoldDigger C2 Servers

- `ks8cb.cc`
- `ms2ve.cc`
- `zu7kt.cc`
- `t8bc.xyz`
- `bv8k.xyz`
- `hzc5.xyz`

Gigabud C2 Servers

- `bweri6.cc`
- `blsdk5.cc`
- `nnzf1.cc`
- `app.js6kk.xyz`
- `app.re6s.xyz`
- `app.bc2k.xyz`

These domains are suspected of being part of the malware's infrastructure for command and control purposes. They play a critical role in the malware's ability to receive commands, exfiltrate data, and manage infected devices.

Recommendations

- **For Financial Organizations**: Implement session monitoring, educate customers about mobile malware risks, and use Digital Risk Protection platforms.
- **For End Users**: Exercise caution with links, download apps from official sources, review app permissions carefully, and be vigilant for signs of malware infection.

Future Threat Landscape: Facial Recognition Exploitation by Cybercriminals

Overview

The evolution of the GoldPickaxe malware family and the activities of the GoldFactory cybercrime group highlight a disturbing trend in cyber threats targeting mobile users. Specifically, the exploitation of facial recognition technology for banking fraud presents a significant challenge. As society grows increasingly reliant on biometric authentication methods for a range of functions from banking to personal device security, the likelihood of attacks exploiting these technologies is set to increase. This section explores the implications of these developments and the potential future threats to users of facial recognition and related biometric authentication methods.

Exploitation of Facial Recognition Technology

Facial recognition technology, while offering convenience and enhanced security in many respects, also introduces new vulnerabilities. Cybercriminals, as demonstrated by the GoldFactory group, are already finding ways to exploit these vulnerabilities, using deepfake technology and stolen biometric data to bypass security measures. The following are key factors contributing to the increased risk:

- **High-Value Target**: Biometric data, once compromised, cannot be changed like a password, making it a high-value target for cybercriminals.
- **Sophistication of Attacks**: The use of AI and machine learning by attackers to create deepfakes or mimic biometric data is becoming more sophisticated and accessible.
- **Widespread Adoption of Biometrics**: The increasing use of facial recognition across various applications, from banking to smartphone security, expands the attack surface for cybercriminals.

Future Threats and Considerations

As biometric authentication technologies become more ingrained in our daily lives, the potential for their exploitation by cybercriminals grows. The following are anticipated future threats tied to the use of facial recognition and biometrics:

- **Broader Application Compromise**: Beyond banking, facial recognition is used in various applications, including access control systems, healthcare, and personal device security. The successful compromise of biometric data could lead to a wide range of fraudulent activities.
- **Permanent Compromise of Biometric Identifiers**: Unlike passwords, biometric data is immutable. Once stolen and replicated, it poses a lifelong threat to the victim.
- **Deepfake-Assisted Social Engineering**: The use of deepfake technology can enhance traditional social engineering attacks, making them more convincing and difficult to detect.
- **Increased Targeting of Biometric Databases**: As biometric authentication becomes more common, the databases storing this sensitive information will become increasingly attractive targets for cybercriminals.

Mitigation and Adaptation Strategies

To counteract the growing threat to biometric authentication methods, the following strategies are recommended:

- **Layered Security Measures**: Employing a multi-factor authentication approach, combining biometrics with other forms of verification, can reduce reliance on a single point of failure.
- **Biometric Liveness Detection**: Incorporating advanced liveness detection features can help differentiate between real users and replicas or deepfakes.
- **Public Awareness and Education**: Educating users about the potential risks and indicators of biometric data compromise is crucial for early detection and response.
- **Continuous Security Evaluation**: Regularly assessing and updating security measures for biometric systems to counteract evolving cyber threats.

Conclusion

The exploitation of facial recognition and other biometric authentication methods by cybercriminals represents a significant and growing threat. The adaptability of threat actors, as evidenced by the GoldFactory group’s activities, underscores the need for vigilance and innovation in cybersecurity practices. As we move forward, balancing the convenience of biometric technologies with the imperative of securing biometric data will be paramount in mitigating the risks posed by these emerging cyber threats.

This report serves as a concise overview of the GoldPickaxe malware family and the associated GoldFactory cybercrime group. It provides stakeholders with the necessary information to understand the threat and take appropriate action based on the provided IoCs and recommendations.