مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

DeceptiveDevelopment Campaign Targeting Freelance Developers

Tracking #:432316908

Date:26-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed researchers have uncovered a sophisticated cyber campaign, dubbed DeceptiveDevelopment, targeting freelance software developers through fake job offers and trojanized coding challenges.

TECHNICAL DETAILS:

ESET researchers have uncovered a sophisticated cyber campaign, dubbed **DeceptiveDevelopment**, targeting freelance software developers through fake job offers and trojanized coding challenges. The campaign, attributed to North Korea-aligned threat actors, aims to steal cryptocurrency wallets, login credentials, and sensitive data from developers working on blockchain and cryptocurrency projects.

The attackers pose as recruiters on job-hunting and freelancing platforms, luring victims with fake job opportunities. As part of the "interview process," victims are asked to complete coding tasks using malicious project files hosted on platforms like GitHub. These files contain hidden malware, including **BeaverTail** (an infostealer and downloader) and **InvisibleFerret** (a modular Python-based backdoor). The malware exfiltrates sensitive data, establishes persistence, and enables remote access to compromised systems

Details:

Threat Assessment:

- **Threat Actor:** DeceptiveDevelopment, a North Korea-aligned activity cluster.
- **Motivation:** Primarily financial gain through cryptocurrency theft, with potential cyber espionage motives.
- **Targets:** Freelance software developers, especially those involved in cryptocurrency and DeFi projects, regardless of geographical location.
- **Impact:**
    - Loss of cryptocurrency funds.
    - Compromise of sensitive login credentials.
    - Backdoor access to developer systems, potentially leading to further attacks on related projects or organizations.
    - Reputational damage.

Technical Details:

- **Initial Access:**
    - Spearphishing via fake recruiter profiles on platforms like LinkedIn, Upwork, Freelancer.com, We Work Remotely, Moonlight, and Crypto Jobs List.
    - Trojanized project files (hiring challenges, cryptocurrency projects, games with blockchain functionality) delivered via GitHub, GitLab, Bitbucket, or direct file transfer.
    - Malicious code hidden within benign components of projects, often appended to long comments to avoid detection.
    - Fake conferencing software distributed through cloned websites.
- **Malware:**
    - **BeaverTail:**
        - First-stage infostealer and downloader.

- JavaScript and native (C++ with Qt) versions.
- Targets Windows, Linux, and macOS.
- Extracts saved login information and cryptocurrency wallet data from browsers (Chrome, Edge, Opera, Brave).
- Identifies and exfiltrates data from cryptocurrency wallet browser extensions like MetaMask, BNB Chain Wallet, Coinbase Wallet, TronLink, Phantom, Ronin Wallet, Coin98 Wallet, and Crypto.com Wallet.

- **InvisibleFerret:**
  - Second-stage modular Python-based malware.
  - Spyware and backdoor capabilities.
  - Downloads and installs AnyDesk for remote access.

- **Infrastructure:**
  - Command and Control (C&C) servers with IP addresses varying, but often using ports 1224 or 1244.
  - GitHub, GitLab, and Bitbucket repositories hosting trojanized projects.
  - Cloned websites mimicking legitimate conferencing platforms.
- **Tactics, Techniques, and Procedures (TTPs):**
  - Use of fake recruiter profiles with copied or fabricated personas.
  - Social engineering to entice developers with fake job offers or bug bounty opportunities.
  - Distribution of trojanized codebases disguised as legitimate projects.
  - Hiding malicious code using long comments to move it off-screen.
  - Use of publicly available obfuscation tools.
  - Impersonating existing projects and companies by using similar names.

Indicators of Compromise (IOC):
Attached File

RECOMMENDATIONS:

- **Establish Secure Coding Practices:** Enforce secure coding practices, including code reviews and security testing, for all projects, including those involving freelance developers.
- **Provide Security Awareness Training:** Offer regular security awareness training to freelance developers, covering topics such as phishing, malware, and social engineering.
- **Implement Access Controls:** Restrict access to sensitive systems and data based on the principle of least privilege.
- **Monitor Freelancer Activity:** Monitor the activity of freelance developers on network for suspicious behavior.
- **Use Secure Communication Channels:** Establish secure communication channels for sharing code and project files with freelance developers.
- **Implement Vendor Risk Management:** Incorporate freelance developers into your vendor risk management program, including security assessments and due diligence.
- **Have Incident Response Plan:** Develop and maintain an incident response plan to address potential security breaches involving freelance developers.
- **Utilize Threat Intelligence:** Subscribe to threat intelligence feeds to stay informed about emerging threats and TTPs used by threat actors targeting developers.

- Independently verify the legitimacy of job offers, recruiters, and clients before engaging in any project or downloading files.
- Use trusted platforms and avoid sharing personal or financial information with unverified parties.
- Avoid downloading and executing project files from untrusted or unverified sources.
- Use virtual machines or sandbox environments to test unknown code before running it on primary systems.
- Review system logs and network traffic for signs of malicious activity.
- Use the provided IOCs to scan systems and identify potential infections.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.welivesecurity.com/en/eset-research/deceptivedevelopment-targets-freelance-developers/?&web_view=true