Nov 03 2023

NETMANAGEIT

Intelligence Report

Elastic catches DPRK passing out KANDYKORN

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Elastic Security Labs is disclosing a novel intrusion targeting blockchain engineers of a crypto exchange platform. The intrusion leveraged a combination of custom and open source capabilities for initial access and post-exploitation.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
User Execution
ID
T1204
Description
An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)
Name

TA0011

ID
TA0011

StixFile

Value
2360a69e5fd7217e977123c81d3dbb60bf4763a9dae6949bc1900234f7762df1
3ea2ead8f3cec030906dcbffe3efd5c5d77d5d375d4a54cca03bfe8a6cb59940
927b3564c1cf884d2a05e1d7bd24362ce8563a1e9b85be776190ab7f8af192f6

IPv4-Addr

Value
23.254.226.90
192.119.64.43

Url

Value
http://tp-globa.xyz//OdhLca1mLUp/lZ5rZPxWsh/7yZKYQI43S/fP7savDX6c/bfC

External References

- https://otx.alienvault.com/pulse/6544c2bcf5e36d7d9585075f
- https://www.elastic.co/security-labs/elastic-catches-dprk-passing-out-kandykorn