Aug 26 2023

NETMANAGEIT

Intelligence Report

Ransomware Roundup – Trash Panda and A New Minor Variant of NoCry

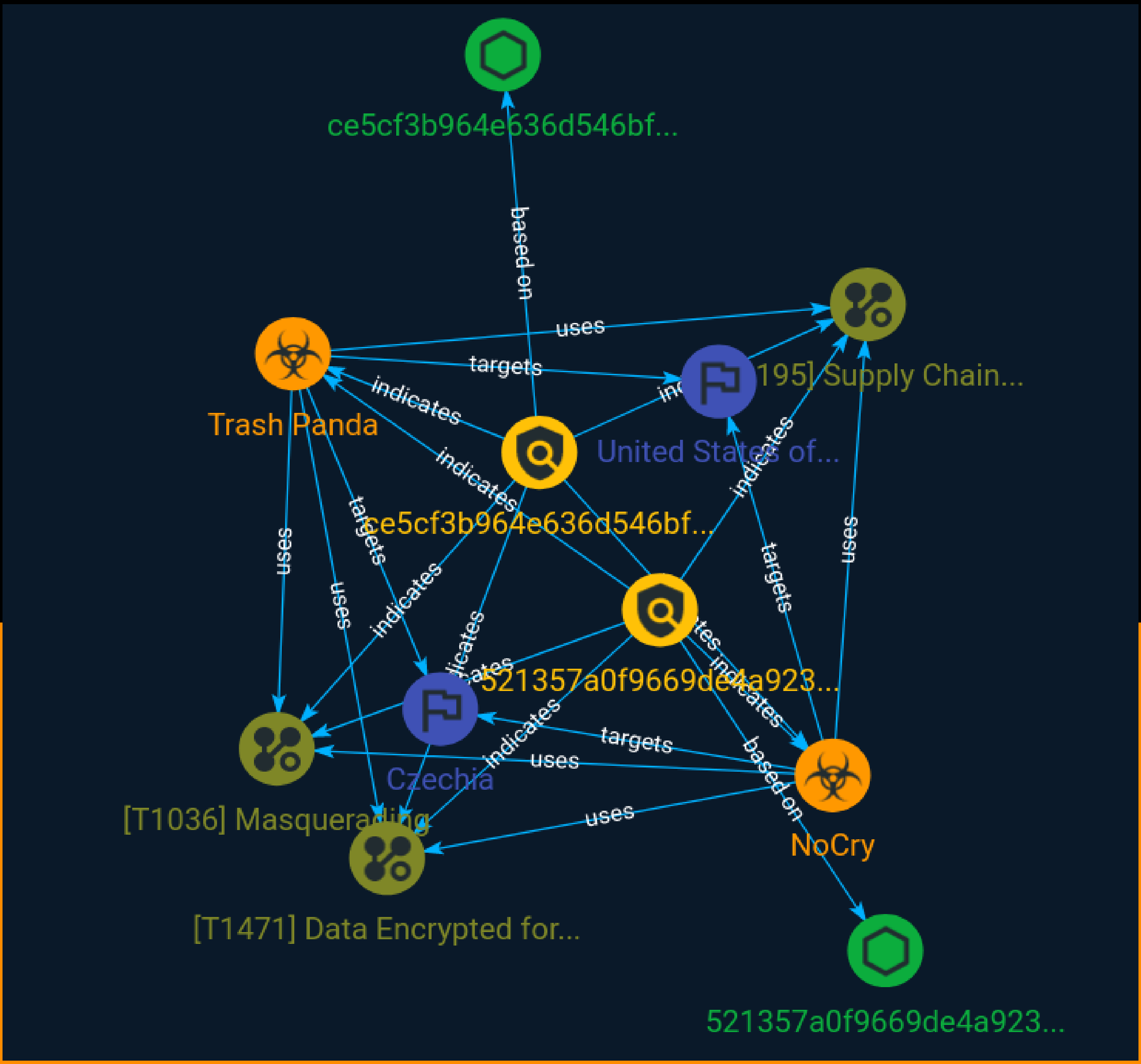

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Trash Panda is a ransomware that runs on the Windows platform that was first spotted in early August. It encrypts files on compromised machines, replaces the desktop wallpaper, and drops a ransom note that includes politically themed messages.

Confidence

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

15 / 100

Indicator

Name

ce5cf3b964e636d546bf2c52423296bda06b7fe47e6f8a757f165a3be93c88db

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'ce5cf3b964e636d546bf2c52423296bda06b7fe47e6f8a757f165a3be93c88db']

Name

521357a0f9669de4a9233feeef7a3c5299c51de4a2531c56aacc807c0fd25a6a

Description

Ransom:MSIL/Cryptolocker.DV!MTB

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'521357a0f9669de4a9233feeef7a3c5299c51de4a2531c56aacc807c0fd25a6a']
```

Malware

Name
Trash Panda

Name
NoCry

Country

Name
Czechia

Name
United States of America

Attack-Pattern

Name
Masquerading
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)
Name
Supply Chain Compromise
ID
T1195
Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Name

Data Encrypted for Impact

ID

T1471

Description

An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

StixFile

Value
ce5cf3b964e636d546bf2c52423296bda06b7fe47e6f8a757f165a3be93c88db
521357a0f9669de4a9233feeef7a3c5299c51de4a2531c56aacc807c0fd25a6a

External References

- https://otx.alienvault.com/pulse/64e871b6dddd2e4fbb0ce3b6
- https://www.fortinet.com/blog/threat-research/ransomware-roundup-trash-panda-and-nocry-variant