May 02 2024

NETMANAGEIT

Intelligence Report

Distribution of Infostealer Made With Electron

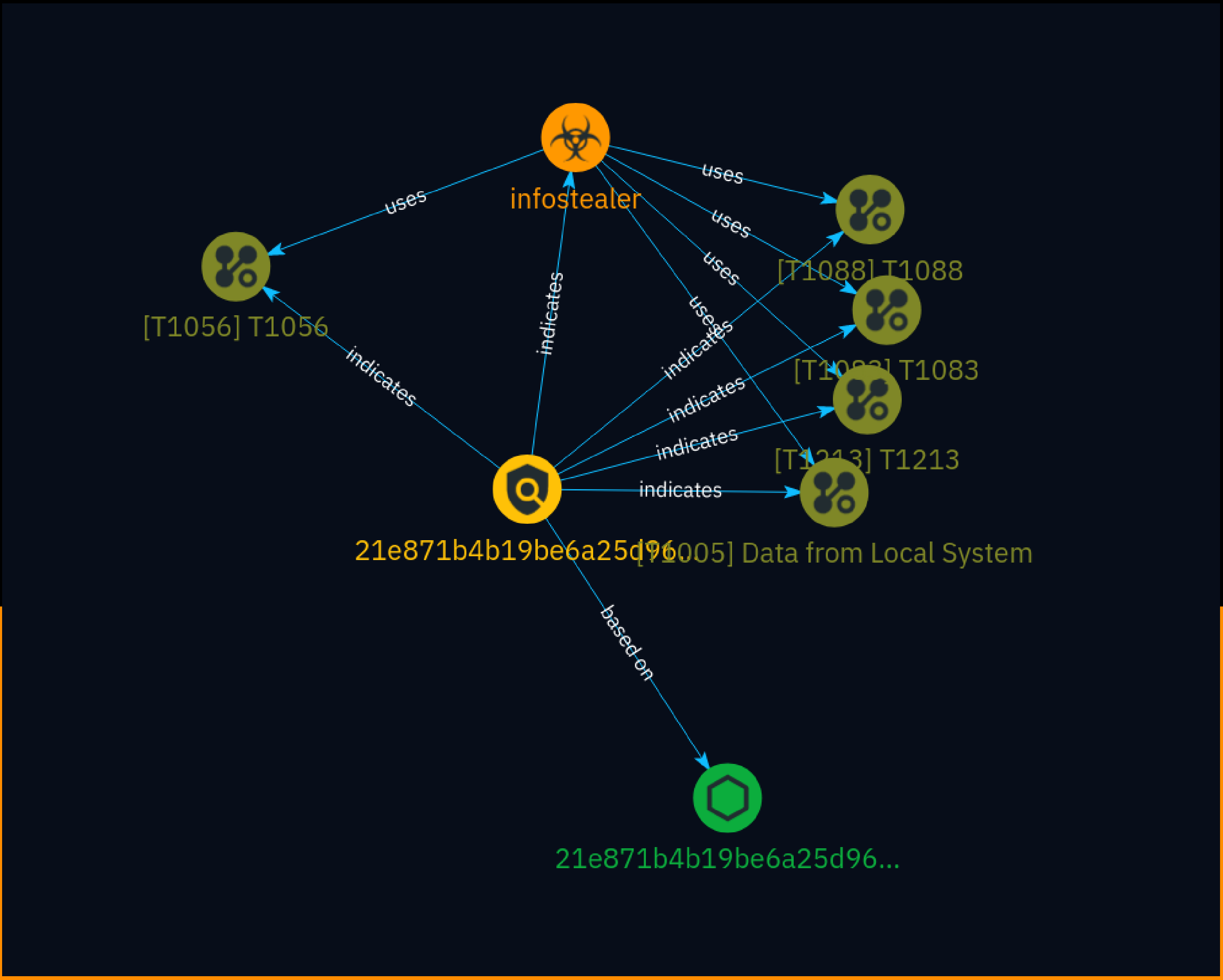

Table of contents

Overview

Entities

Observables

External References

Overview

Description

AhnLab Security Intelligence Center (ASEC) has discovered an Infostealer malware strain developed using the Electron framework, which allows the creation of applications using JavaScript, HTML, and CSS. The malware is distributed through Nullsoft Scriptable Install System (NSIS) installer format. Once executed, it installs an Electron application that interacts with the operating system via Node.js, where the malicious behaviors are defined. The report describes two cases, one involving user information collection and the other uploading collected data to a file-sharing service. The malware strains are difficult to detect due to their Electron structure.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
21e871b4b19be6a25d9674194bd0411a4374ca8693bd7f6af9ba1c34f57d18ab
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '21e871b4b19be6a25d9674194bd0411a4374ca8693bd7f6af9ba1c34f57d18ab']

Attack-Pattern

Name

T1088

ID

T1088

Name

T1213

ID

T1213

Description

Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, or direct access to the target information. Adversaries may also abuse external sharing features to share sensitive documents with recipients outside of the organization. The following is a brief list of example information that may hold potential value to an adversary and may also be found on an information repository: * Policies, procedures, and standards * Physical / logical network diagrams * System architecture diagrams * Technical system documentation * Testing / development credentials * Work / project schedules * Source code snippets * Links to network shares and other internal resources Information stored in a repository may vary based on the specific instance or environment. Specific common information repositories include web-based platforms such as [Sharepoint](https://attack.mitre.org/techniques/T1213/002) and [Confluence](https://attack.mitre.org/techniques/T1213/001), specific services such as Code Repositories, IaaS databases, enterprise databases, and other storage infrastructure such as SQL Server.

Name

T1056

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

T1083

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A) Some files and directories may require elevated or specific user permissions to access.

Name

Data from Local System

ID

T1005

Description

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration. Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

Malware

Name
infostealer

StixFile

Value
21e871b4b19be6a25d9674194bd0411a4374ca8693bd7f6af9ba1c34f57d18ab

External References

- https://asec.ahnlab.com/en/64445/
- https://otx.alienvault.com/pulse/663105b7aa3c9f64f4b6f653