Oct 03 2023

NETMANAGEIT

Intelligence Report

The art of manipulation: fraudsters steal money with remote administration software for mobile devices

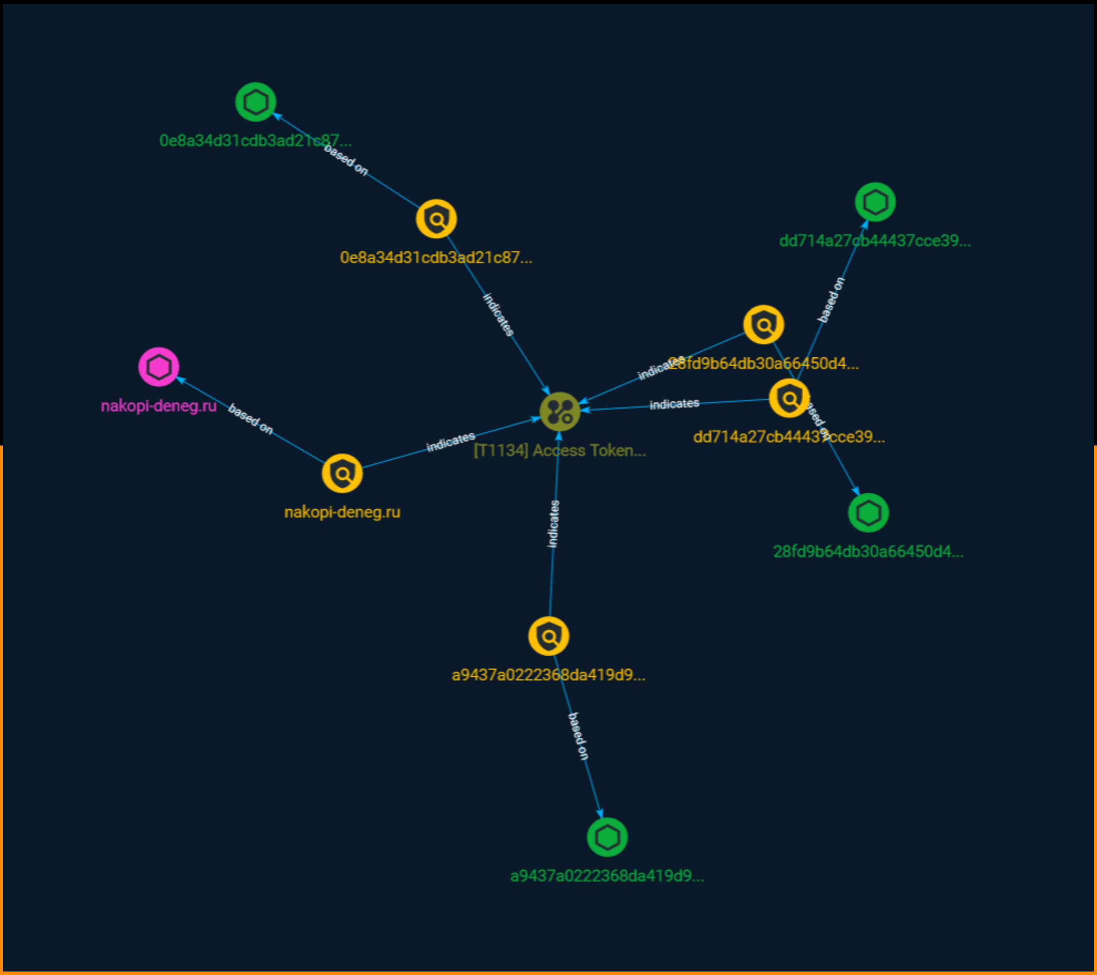

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Doctor Web is reporting on the growing number of fraud cases involving remote desktop access applications. RustDesk is the most popular among attackers.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Access Token Manipulation
ID
T1134
Description
Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the \`runas\` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

Indicator

Name

28fd9b64db30a66450d498994e6b5ab9772d398bf5d8abda15abd6e249d417c9

Description

SHA256 of ee406a21dcb4fe02feb514b9c17175ee95625213

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '28fd9b64db30a66450d498994e6b5ab9772d398bf5d8abda15abd6e249d417c9']

Name

a9437a0222368da419d9d05c60198c8763b3d5f46743a2c727089b7fbbdfee06

Description

SHA256 of f28cb04a56d645067815d91d079b060089dbe9fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a9437a0222368da419d9d05c60198c8763b3d5f46743a2c727089b7fbbdfee06']

Name

0e8a34d31cdb3ad21c87e7d113ffb0e65cff4469a0e02b199035ddd9d0dfe8fe

Description

SHA256 of 9a96782621c9f98e3b496a9592ad397ec9ffb162

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e8a34d31cdb3ad21c87e7d113ffb0e65cff4469a0e02b199035ddd9d0dfe8fe']

Name

dd714a27cb44437cce3932ae738cc5ef3c3e17f64159034ce882850401b14463

Description

SHA256 of 535ecea51c63d3184981db61b3c0f472cda10092

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dd714a27cb44437cce3932ae738cc5ef3c3e17f64159034ce882850401b14463']

Name

nakopi-deneg.ru

Pattern Type

stix

Pattern

[domain-name:value = 'nakopi-deneg.ru']

Domain-Name

Value
nakopi-deneg.ru

StixFile

Value
28fd9b64db30a66450d498994e6b5ab9772d398bf5d8abda15abd6e249d417c9
dd714a27cb44437cce3932ae738cc5ef3c3e17f64159034ce882850401b14463
a9437a0222368da419d9d05c60198c8763b3d5f46743a2c727089b7fbbdfee06
0e8a34d31cdb3ad21c87e7d113ffb0e65cff4469a0e02b199035ddd9d0dfe8fe

External References

- https://otx.alienvault.com/pulse/651c3d1b75ef4b67af8fd142
- https://news.drweb.com/show/?i=14755&lng=en&c=5