Dec 05 2023

NETMANAGEIT

Intelligence Report

New BlueNoroff loader for macOS

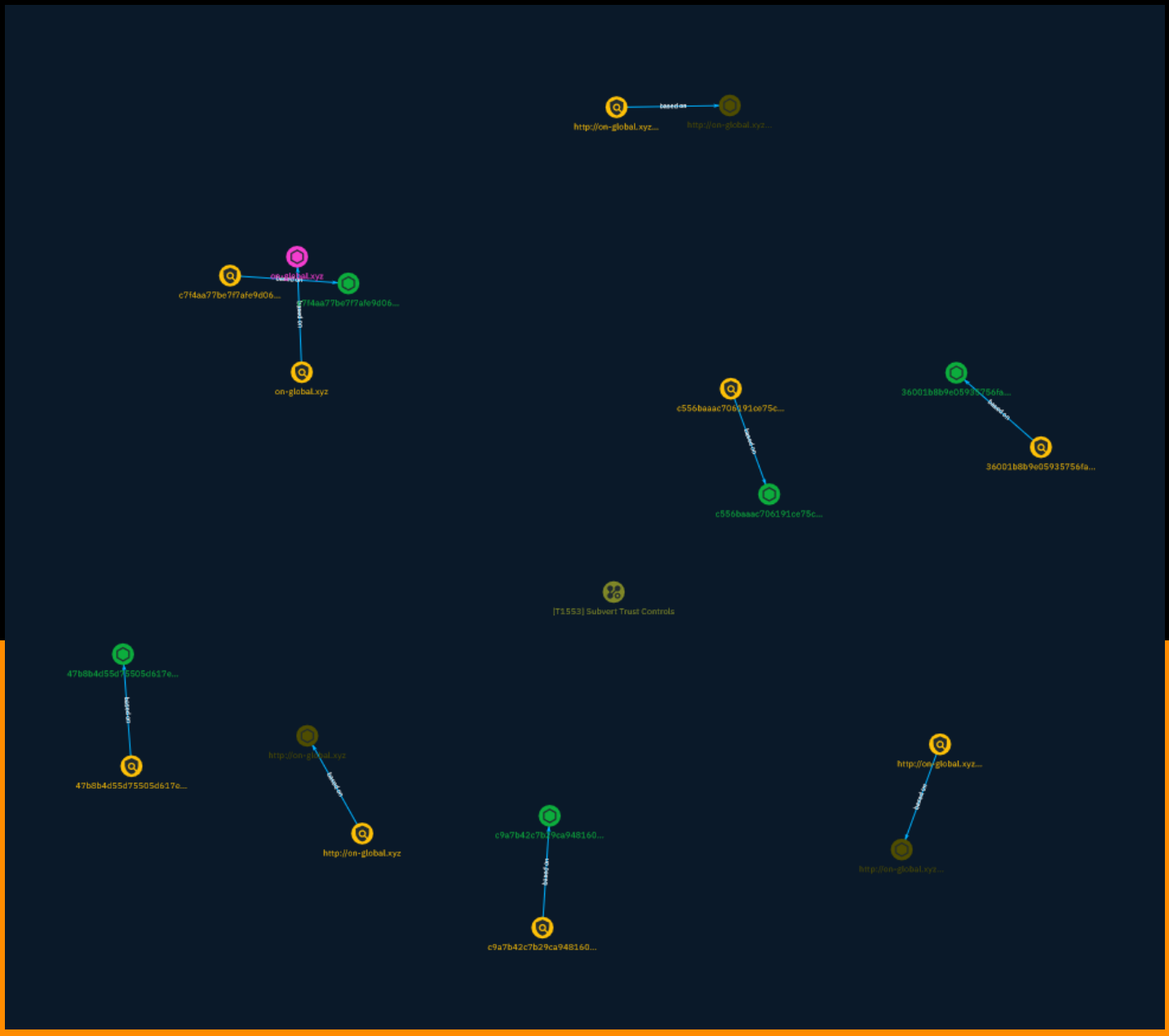

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new type of malicious loader that targets Apple's operating system BlueNoroff has been discovered and spread its malicious payload via a PDF file.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Subvert Trust Controls
ID
T1553
Description
Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Indicator

Name
c9a7b42c7b29ca948160f95f017e9e9ae781f3b981ecf6edbac943e52c63ffc8
Description
SHA256 of 1fddf14984c6b57358401a4587e7b950
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c9a7b42c7b29ca948160f95f017e9e9ae781f3b981ecf6edbac943e52c63ffc8']
Name
http://on-global.xyz/Ov56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A==
Pattern Type
stix
Pattern

[url:value = 'http://on-global.xyz/Ov56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A==']

Name

http://on-global.xyz/Of56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A==

Pattern Type

stix

Pattern

[url:value = 'http://on-global.xyz/Of56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A==']

Name

on-global.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'on-global.xyz']

Name

c556baaac706191ce75c9263b349242caa3d8efca7b5639896fa3e6570d7c76e

Description

SHA256 of 3b3b3b9f7c71fcd7239abe90c97751c0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c556baaac706191ce75c9263b349242caa3d8efca7b5639896fa3e6570d7c76e']

Name

http://on-global.xyz

Pattern Type

stix

Pattern

[url:value = 'http://on-global.xyz']

Name

c7f4aa77be7f7afe9d0665d3e705dbf7794bc479bb9c44488c7bf4169f8d14fe

Description

SHA256 of d8011dcca570689d72064b156647fa82

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7f4aa77be7f7afe9d0665d3e705dbf7794bc479bb9c44488c7bf4169f8d14fe']

Name
36001b8b9e05935756fa7525dd49d91b59ea882efe5a2d23ccec35fef96138d4
Description
SHA256 of b1e01ae0006f449781a05f4704546b34
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '36001b8b9e05935756fa7525dd49d91b59ea882efe5a2d23ccec35fef96138d4']
Name
47b8b4d55d75505d617e53afcb6c32dd817024be209116f98cbbc3d88e57b4d1
Description
SHA256 of 90385d612877e9d360196770d73d22d6
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '47b8b4d55d75505d617e53afcb6c32dd817024be209116f98cbbc3d88e57b4d1']

Domain-Name

Value
on-global.xyz

StixFile

Value
c9a7b42c7b29ca948160f95f017e9e9ae781f3b981ecf6edbac943e52c63ffc8
c7f4aa77be7f7afe9d0665d3e705dbf7794bc479bb9c44488c7bf4169f8d14fe
c556baaac706191ce75c9263b349242caa3d8efca7b5639896fa3e6570d7c76e
47b8b4d55d75505d617e53afcb6c32dd817024be209116f98cbbc3d88e57b4d1
36001b8b9e05935756fa7525dd49d91b59ea882efe5a2d23ccec35fef96138d4

Url

Value
http://on-global.xyz/Of56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A==
http://on-global.xyz
http://on-global.xyz/Ov56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A==

External References

- https://otx.alienvault.com/pulse/656f2fb83b7c921884ae28ad
- https://securelist.com/bluenoroff-new-macos-malware/111290/