Feb 28 2024

NETMANAGEIT

Intelligence Report

Unveiling UAC-0184: The Steganography Saga of the IDAT Loader Delivering Remcos RAT to a Ukraine Entity in Finland

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A recent discovery sheds light on the IDAT loader delivering the Remcos Remote Access Trojan to a Ukrainian entity in Finland. The attack used steganography to obfuscate malicious code within an image. Remcos allows attackers to control an infected computer and steal information without developing remote access capabilities. Proactive defense mechanisms prevented execution of the campaign before public disclosure, providing crucial time for response.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

https://aveclagare.org/wp-content/plugins/wpstream/public/js/youtube.min.js

Pattern Type

stix

Pattern

[url:value = 'https://aveclagare.org/wp-content/plugins/wpstream/public/js/youtube.min.js']

Name

194.87.31.181

Description

ISP: GLOBAL INTERNET SOLUTIONS LLC **OS:** Windows (build 10.0.19041) ---------- Hostnames: ---------- Domains: ---------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: DESKTOP-TCRDU4C NetBIOS Domain Name: DESKTOP-TCRDU4C NetBIOS Computer Name: DESKTOP-TCRDU4C DNS Domain Name: DESKTOP-TCRDU4C FQDN: DESKTOP-TCRDU4C ``` ----------

Pattern Type
stix
Pattern
[ipv4-addr:value = '194.87.31.181']
Name
4b36a82e1781ffa1936703971e2d94369e3059c8524d647613244c6f9a92690b
Description
Delphi
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4b36a82e1781ffa1936703971e2d94369e3059c8524d647613244c6f9a92690b']

Malware

Name
Remcos RAT

Intrusion-Set

Name
UAC-0184

Attack-Pattern

Name
Steganography
ID
T1001.002
Description
Adversaries may use steganographic techniques to hide command and control traffic to make detection efforts more difficult. Steganographic techniques can be used to hide data in digital messages that are transferred between systems. This hidden information can be used for command and control of compromised systems. In some cases, the passing of files embedded using steganography, such as image or document files, can be used for command and control.

Country

Name
Finland

Name
Ukraine

Region

Name
Northern Europe
Name
Eastern Europe
Name
Europe

Sector

Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Url

Value
https://aveclagare.org/wp-content/plugins/wpstream/public/js/youtube.min.js

IPv4-Addr

Value
194.87.31.181

StixFile

Value
4b36a82e1781ffa1936703971e2d94369e3059c8524d647613244c6f9a92690b

External References

- https://blog.morphisec.com/unveiling-uac-0184-the-remcos-rat-steganography-saga
- https://otx.alienvault.com/pulse/65dda518ce4e10650ab76250