Sep 02 2023

NETMANAGEIT

Intelligence Report

Novel RAT discovered “SuperBear” targeting journalist covering geopolitics of Asia

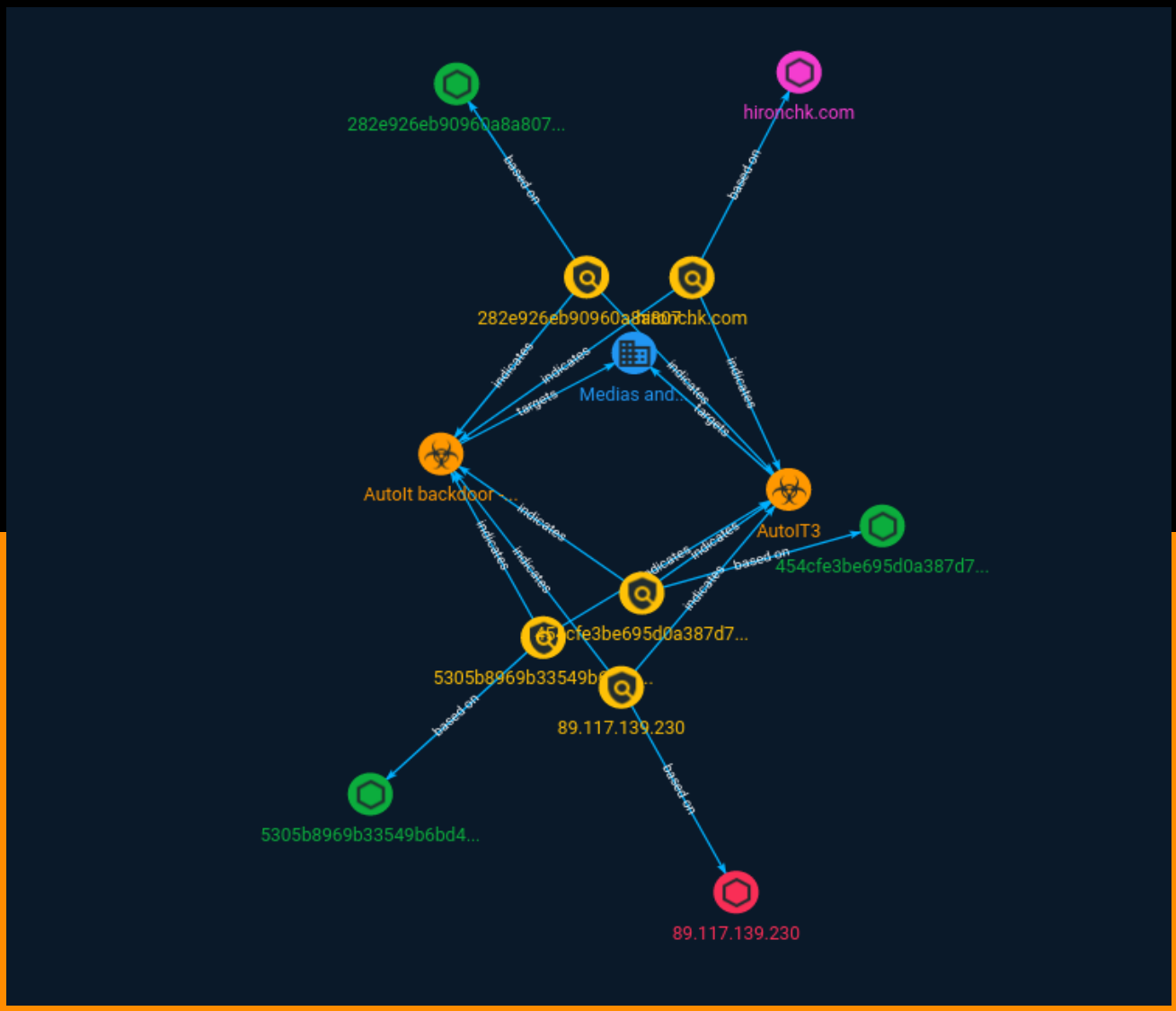

Table of contents

Overview

Entities

Observables

External References

Overview

Description

After initial compromise, the execution of an AutoIT script that was used to perform process injection using a process hollowing technique. The injected process contained a novel RAT, which we dubbed “SuperBear” due to naming conventions in the code. We believe this to be a new campaign targeting civil society groups.

Confidence

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

15 / 100

Indicator

Name

5305b8969b33549b6bd4b68a3f9a2db1e3b21c5497a5d82cec9beaeca007630e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5305b8969b33549b6bd4b68a3f9a2db1e3b21c5497a5d82cec9beaeca007630e']

Name

89.117.139.230

Description

ISP: Hostinger International Limited **OS:** None ---------- Hostnames: - hstgr.io ---------- Domains: - hstgr.io ---------- Services: **443:** ``` HTTP/1.1 403 Forbidden Connection: Keep-Alive Keep-Alive: timeout=5, max=100 cache-control: private, no-cache, no-store, must-revalidate, max-age=0 pragma: no-cache content-type: text/html content-length: 699 date: Wed, 30 Aug 2023 04:17:01 GMT server: LiteSpeed platform: hostinger alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46" ``` HEARTBLEED: 2023/08/30 04:17:12 89.117.139.230:443 - SAFE ----------

Pattern Type
stix
Pattern
[ipv4-addr:value = '89.117.139.230']
Name
hironchk.com
Pattern Type
stix
Pattern
[domain-name:value = 'hironchk.com']
Name
454cfe3be695d0a387d7877c11d3b224b3e2c7d22fc2f31f349b5c23799967ec
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '454cfe3be695d0a387d7877c11d3b224b3e2c7d22fc2f31f349b5c23799967ec']
Name

282e926eb90960a8a807dd0b9e8668e39b38e6961b0023b09f8b56d287ae11cb

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '282e926eb90960a8a807dd0b9e8668e39b38e6961b0023b09f8b56d287ae11cb']

Malware

Name
AutoIT3

Name
AutoIt backdoor - S0129

Sector

Name
Medias and audiovisual
Description
Communication outlets used to deliver information by print, broadcast or Internet and people working in these outlets.

Domain-Name

Value
hironchk.com

StixFile

Value
454cfe3be695d0a387d7877c11d3b224b3e2c7d22fc2f31f349b5c23799967ec
5305b8969b33549b6bd4b68a3f9a2db1e3b21c5497a5d82cec9beaeca007630e
282e926eb90960a8a807dd0b9e8668e39b38e6961b0023b09f8b56d287ae11cb

IPv4-Addr

Value
89.117.139.230

External References

- https://otx.alienvault.com/pulse/64f1ee46cf6a9ed65128fa75
- https://interlab.or.kr/archives/19416