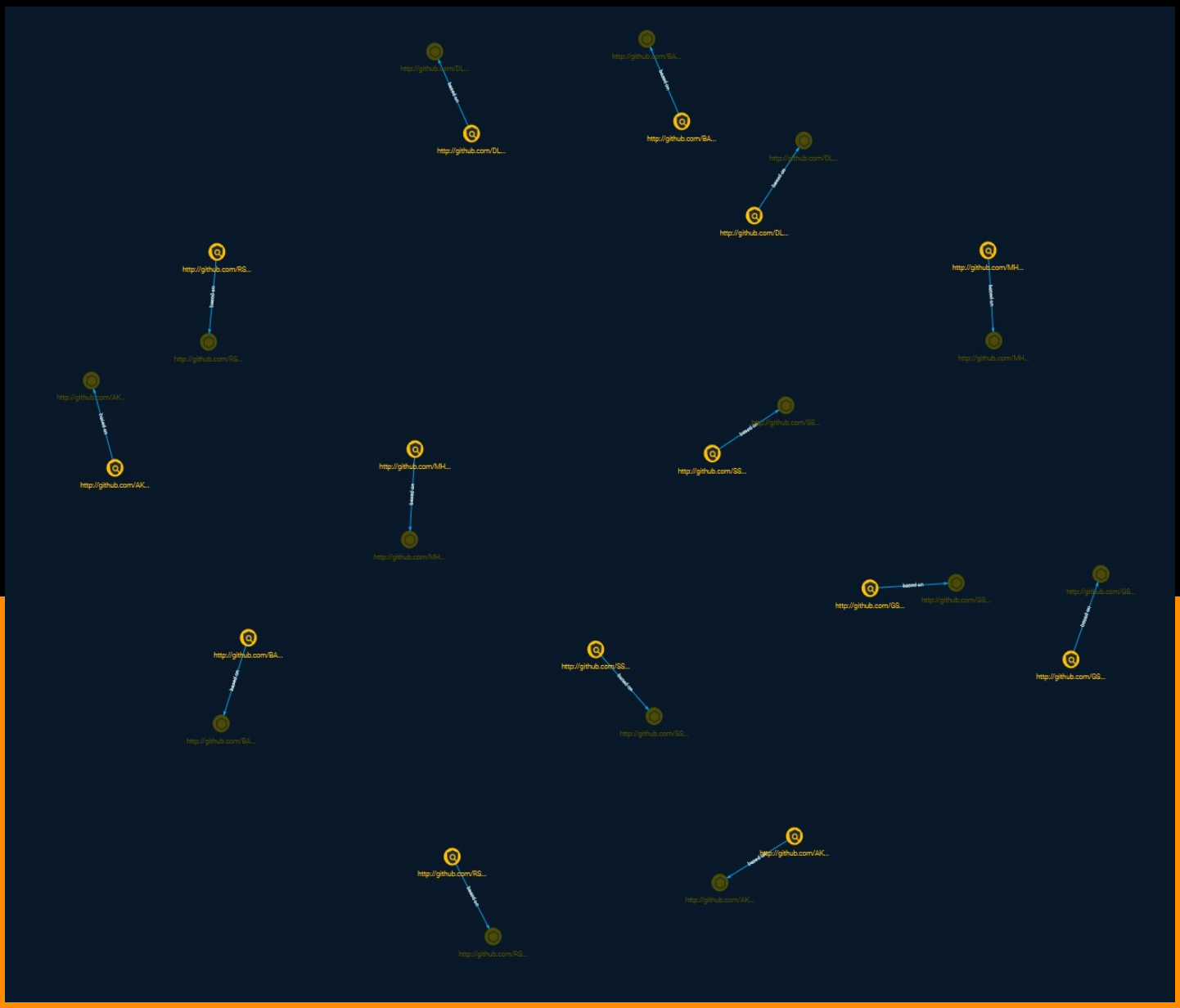
Jun 19 2023

NETMANAGEIT

# Intelligence Report

# Fake security researchers push malware files on GitHub



# Table of contents

# Overview

## Description

Researchers have observed a campaign using real security researchers as bait for malware. The campaign goes to some lengths to appear genuine, using fake profiles, downloads, websites, and bogus GitHub profiles, to paint a convincing picture of security professionals offering up exploit code for popular programs.

## Confidence

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

15 / 100

# Indicator

| Name |
| --- |
| http://github.com/GSandersonHSCS |
| **Pattern Type** |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/GSandersonHSCS'] |
| **Name** |
| http://github.com/RShahHSCS |
| **Pattern Type** |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/RShahHSCS'] |
| **Name** |
| http://github.com/SSankkarHSCS/Chromium-0-Day |

| Pattern Type |
| --- |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/SSankkarHSCS/Chromium-0-Day'] |
| **Name** |
| http://github.com/DLandonHSCS/Discord-RCE |
| **Pattern Type** |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/DLandonHSCS/Discord-RCE'] |
| **Name** |
| http://github.com/BAdithyaHSCS |
| **Pattern Type** |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/BAdithyaHSCS'] |
| **Name** |
| http://github.com/DLandonHSCS |

| Pattern Type |
| --- |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/DLandonHSCS'] |
| **Name** |
| http://github.com/SSankkarHSCS |
| **Pattern Type** |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/SSankkarHSCS'] |
| **Name** |
| http://github.com/MHadzicHSCS/Chrome-0-day |
| **Pattern Type** |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/MHadzicHSCS/Chrome-0-day'] |
| **Name** |
| http://github.com/BAdithyaHSCS/Exchange-0-Day |

| Pattern Type |
| --- |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/BAdithyaHSCS/Exchange-0-Day'] |
| **Name** |
| http://github.com/AKuzmanHSCS/Microsoft-Exchange-RCE |
| **Pattern Type** |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/AKuzmanHSCS/Microsoft-Exchange-RCE'] |
| **Name** |
| http://github.com/MHadzicHSCS |
| **Pattern Type** |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/MHadzicHSCS'] |
| **Name** |
| http://github.com/GSandersonHSCS/discord-0-day-fix |

| Pattern Type |
| --- |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/GSandersonHSCS/discord-0-day-fix'] |
| **Name** |
| http://github.com/RShahHSCS/Discord-0-Day-Exploit |
| **Pattern Type** |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/RShahHSCS/Discord-0-Day-Exploit'] |
| **Name** |
| http://github.com/AKuzmanHSCS |
| **Pattern Type** |
| stix |
| **Pattern** |
| [url:value = 'http://github.com/AKuzmanHSCS'] |

# Url

| Value |
| --- |
| http://github.com/MHadzicHSCS/Chrome-0-day |
| http://github.com/BAdithyaHSCS/Exchange-0-Day |
| http://github.com/MHadzicHSCS |
| http://github.com/RShahHSCS/Discord-0-Day-Exploit |
| http://github.com/SSankkarHSCS |
| http://github.com/RShahHSCS |
| http://github.com/DLandonHSCS |
| http://github.com/GSandersonHSCS |
| http://github.com/BAdithyaHSCS |
| http://github.com/DLandonHSCS/Discord-RCE |
| http://github.com/SSankkarHSCS/Chromium-0-Day |
| http://github.com/AKuzmanHSCS/Microsoft-Exchange-RCE |
| http://github.com/GSandersonHSCS/discord-0-day-fix |

http://github.com/AKuzmanHSCS

# External References

- https://www.malwarebytes.com/blog/news/2023/06/fake-security-researchers-push-malware-files-on-github
- https://otx.alienvault.com/pulse/6490651b05174d738c105128