Oct 05 2023

NETMANAGEIT

Intelligence Report

Exposing Infection Techniques Across Supply Chains and Codebases

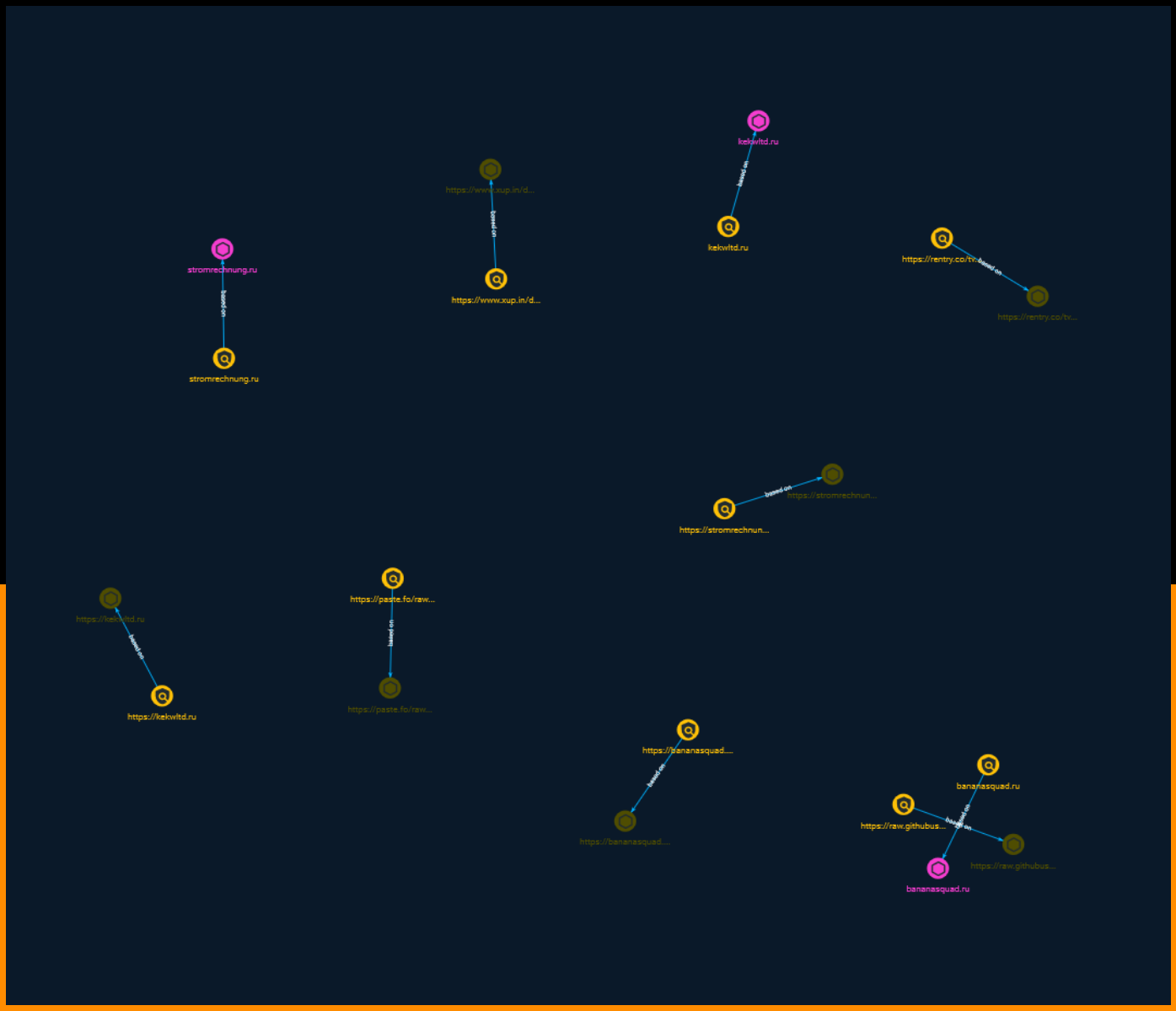

Table of contents

Overview

- Description 3
- Confidence 3
- Content 4

Entities

- Indicator 5

Observables

- Domain-Name 9
- Url 10

External References

- External References 11

Overview

Description

TrendMicro has published a new blog regarding a case study using a combination of techniques such as exec smuggling, employing platforms such as GitHub and repositories such as PyPi packages to infect individuals and organizations.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
kekwltd.ru
Pattern Type
stix
Pattern
[domain-name:value = 'kekwltd.ru']
Name
https://www.xup.in/dl,20029171/USDT_SWEEPER.PY
Pattern Type
stix
Pattern
[url:value = 'https://www.xup.in/dl,20029171/USDT_SWEEPER.PY']
Name
https://rentry.co/tvfwh/raw

Pattern Type
stix
Pattern
[url:value = 'https://rentry.co/tvfwh/raw']
Name
https://raw.githubusercontent.com/yusiqo/anonchat/main/lrdstl
Pattern Type
stix
Pattern
[url:value = 'https://raw.githubusercontent.com/yusiqo/anonchat/main/lrdstl']
Name
stromrechnung.ru
Pattern Type
stix
Pattern
[domain-name:value = 'stromrechnung.ru']
Name
https://bananasquad.ru/paste

Pattern Type
stix
Pattern
[url:value = 'https://bananasquad.ru/paste']
Name
https://stromrechnung.ru
Pattern Type
stix
Pattern
[url:value = 'https://stromrechnung.ru']
Name
https://paste.fo/raw/efda79f59c55
Pattern Type
stix
Pattern
[url:value = 'https://paste.fo/raw/efda79f59c55']
Name
bananasquad.ru

Pattern Type
stix
Pattern
[domain-name:value = 'bananasquad.ru']
Name
https://kekwltd.ru
Pattern Type
stix
Pattern
[url:value = 'https://kekwltd.ru']

Domain-Name

Value
kekwltd.ru
bananasquad.ru
stromrechnung.ru

Url

Value
https://rentry.co/tvfwh/raw
https://paste.fo/raw/efda79f59c55
https://www.xup.in/dl,20029171/USDT_SWEEPER.PY
https://raw.githubusercontent.com/yusiqo/anonchat/main/lrdstl
https://kekwltd.ru
https://stromrechnung.ru
https://bananasquad.ru/paste

External References

- https://otx.alienvault.com/pulse/651e969f7319e72bd78fd510
- https://www.trendmicro.com/en_us/research/23/j/infection-techniques-across-supply-chains-and-codebases.html