Oct 28 2023

NETMANAGEIT

Intelligence Report

Void Rabisu Targets Female Political Leaders with New Slimmed-Down ROMCOM Variant

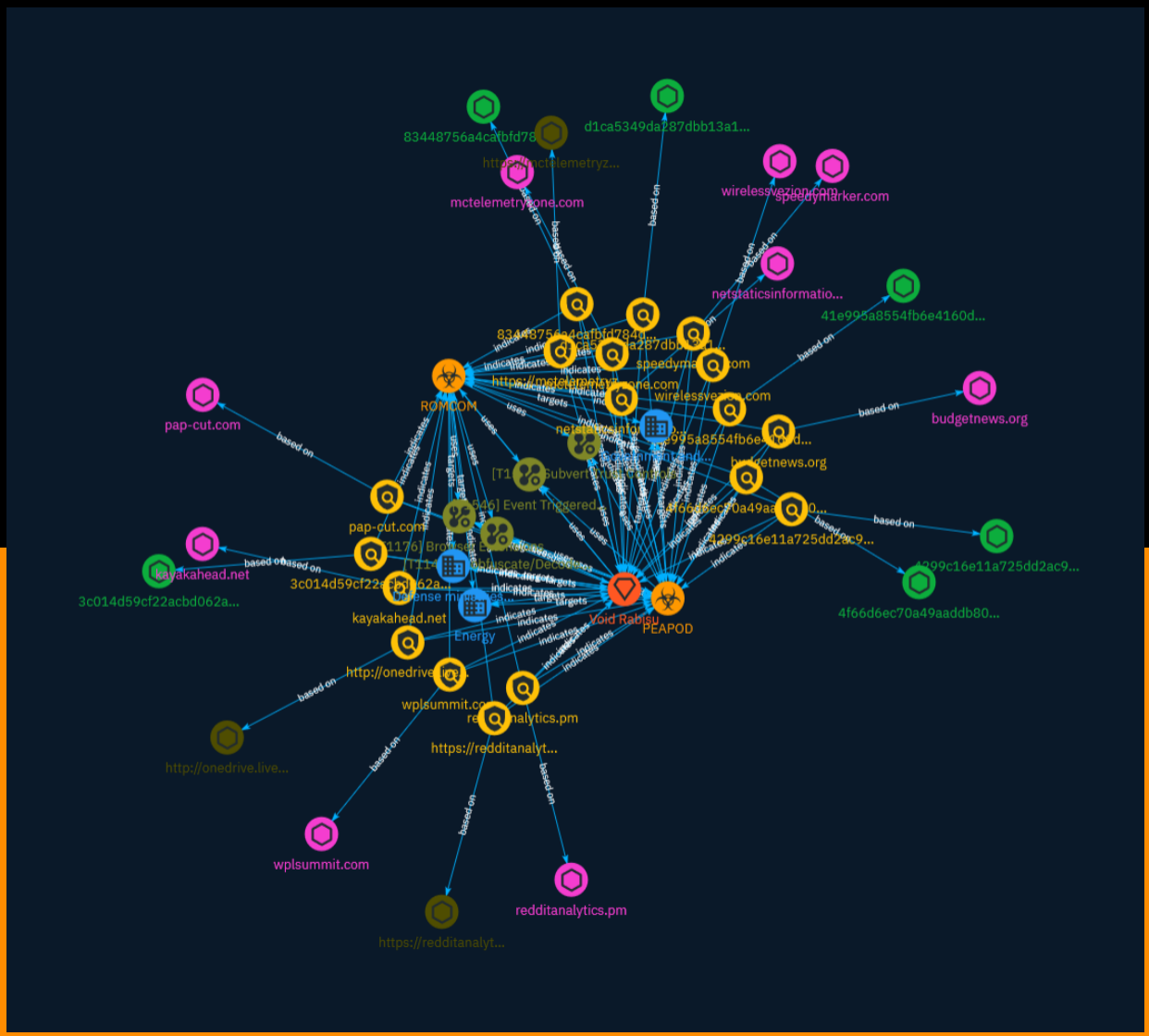

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6
- Sector 10
- Indicator 11
- Intrusion-Set 18
- Malware 19

Observables

- Domain-Name 20
- StixFile 21

- Url 22

External References

- External References 23

Overview

Description

Void Rabisu is an intrusion set associated with financially motivated ransomware attacks and targeted campaigns on Ukraine and its supporters. They've targeted various entities, including the Ukrainian government, military, energy sectors, EU politicians, and security conference participants. Void Rabisu uses the ROMCOM backdoor and combines tactics from both cybercriminals and nation-state-sponsored actors, exploiting vulnerabilities like CVE-2023-36884.

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)
Name
Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Name

Event Triggered Execution

ID

T1546

Description

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events. (Citation: Backdooring an AWS account)(Citation: Varonis Power Automate Data Exfiltration) (Citation: Microsoft DART Case Report 001) Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked. (Citation: FireEye WMI 2015)(Citation: Malware Persistence on OS X)(Citation: amnesia malware) Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/

encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Sector

Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.
Name
Defense ministries (including the military)
Description
Includes the military and all defense related-space activities.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Indicator

Name
speedymarker.com
Pattern Type
stix
Pattern
[domain-name:value = 'speedymarker.com']
Name
wplsummit.com
Pattern Type
stix
Pattern
[domain-name:value = 'wplsummit.com']
Name
https://mctelemetryzone.com/favicon.ico

Pattern Type
stix
Pattern
[url:value = 'https://mctelemetryzone.com/favicon.ico']
Name
budgetnews.org
Pattern Type
stix
Pattern
[domain-name:value = 'budgetnews.org']
Name
kayakahead.net
Pattern Type
stix
Pattern
[domain-name:value = 'kayakahead.net']
Name
41e995a8554fb6e4160d0e445856221ece2117a2b030012ead9efe76611bdc14

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '41e995a8554fb6e4160d0e445856221ece2117a2b030012ead9efe76611bdc14']

Name

redditanalytics.pm

Pattern Type

stix

Pattern

[domain-name:value = 'redditanalytics.pm']

Name

netstaticsinformation.com

Pattern Type

stix

Pattern

[domain-name:value = 'netstaticsinformation.com']

Name

wirelessvezion.com

Pattern Type

stix

Pattern

[domain-name:value = 'wirelessvezion.com']

Name

https://redditanalytics.pm/Mi8xMzI0NTY3ODk=

Pattern Type

stix

Pattern

[url:value = 'https://redditanalytics.pm/Mi8xMzI0NTY3ODk=']

Name

83448756a4cafbfd784d36add719cffa65b912e550d3a5fd63d407201c6ff94c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '83448756a4cafbfd784d36add719cffa65b912e550d3a5fd63d407201c6ff94c']

Name

4f66d6ec70a49aaddb8018af1bf859284a6a4a27eb2615c80a32d5c7c156e476

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4f66d6ec70a49aaddb8018af1bf859284a6a4a27eb2615c80a32d5c7c156e476']

Name

3c014d59cf22acbd062a4e2cab8cb8ede7127b6a69af9db45a7dcefde866369a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c014d59cf22acbd062a4e2cab8cb8ede7127b6a69af9db45a7dcefde866369a']

Name

d1ca5349da287dbb13a1ea2a2982d23e6ce34ed822baee7468ce1980a4179d42

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd1ca5349da287dbb13a1ea2a2982d23e6ce34ed822baee7468ce1980a4179d42']

Name

4299c16e11a725dd2ac9468c5c0aabf94ea5a90d2232810c19ba13b35b3708f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4299c16e11a725dd2ac9468c5c0aabf94ea5a90d2232810c19ba13b35b3708f9']

Name

pap-cut.com

Pattern Type

stix

Pattern

[domain-name:value = 'pap-cut.com']

Name

mctelemetryzone.com

Pattern Type

stix

Pattern

[domain-name:value = 'mctelemetryzone.com']

Name

http://onedrive.live.com/?authkey=%21AAdO%2Di5%2DikrnuaA&id=79E2A760F4732317%21106&cid=79E2A760F4732317

Pattern Type

stix

Pattern

[url:value = 'http://onedrive.live.com/?authkey=%21AAdO%2Di5%2DikrnuaA&id=79E2A760F4732317%21106&cid=79E2A760F4732317']

Intrusion-Set

Name
Void Rabisu

Malware

Name
ROMCOM

Name
PEAPOD

Domain-Name

Value
wirelessvezion.com
budgetnews.org
mctelemetryzone.com
kayakahead.net
redditanalytics.pm
pap-cut.com
netstaticsinformation.com
wplsummit.com
speedymarker.com

StixFile

Value
3c014d59cf22acbd062a4e2cab8cb8ede7127b6a69af9db45a7dcefde866369a
4299c16e11a725dd2ac9468c5c0aabf94ea5a90d2232810c19ba13b35b3708f9
4f66d6ec70a49aaddb8018af1bf859284a6a4a27eb2615c80a32d5c7c156e476
83448756a4cafbfd784d36add719cffa65b912e550d3a5fd63d407201c6ff94c
41e995a8554fb6e4160d0e445856221ece2117a2b030012ead9efe76611bdc14
d1ca5349da287dbb13a1ea2a2982d23e6ce34ed822baee7468ce1980a4179d42

Url

Value
http://onedrive.live.com/?authkey=%21AAdO%2Di5%2DikrnuaA&id=79E2A760F4732317%21106&cid=79E2A760F4732317
https://mctelemetryzone.com/favicon.ico
https://redditanalytics.pm/Mi8xMzI0NTY3ODk=

External References

- https://otx.alienvault.com/pulse/652ea034b4a8762d380d7dfc
- https://www.trendmicro.com/en_us/research/23/j/void-rabisu-targets-female-leaders-with-new-romcom-variant.html
- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/j/void-rabisu-targets-female-political-leaders/ioc-void-rabisu-targets-female-political-leaders-with-new-slimmed-down-ROMCOM-variant.txt