Jun 21 2023

NETMANAGEIT

Intelligence Report

Cadet Blizzard emerges as a novel and distinct Russian threat actor | Microsoft Security Blog

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Cadet Blizzard operations are associated with the Russian General Staff Main Intelligence Directorate (GRU) but are separate from other known and more established GRU-affiliated groups such as Forest Blizzard (STRONTIUM) and Seashell Blizzard (IRIDIUM). The emergence of a novel GRU affiliated actor, particularly one which has conducted destructive cyber operations likely supporting broader military objectives in Ukraine, is a notable development in the Russian cyber threat landscape.

Confidence

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

15 / 100

Indicator

Name

3e4bb8089657fef9b8e84d9e17fd0d7740853c4c0487081dacc4f22359bade5c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3e4bb8089657fef9b8e84d9e17fd0d7740853c4c0487081dacc4f22359bade5c']

Name

7fedaf0dec060e40cbdf4ec6d0fbfc427593ad5503ad0abaf6b943405863c897

Description

Trojan:PHP/WebShell

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7fedaf0dec060e40cbdf4ec6d0fbfc427593ad5503ad0abaf6b943405863c897']

Name

3fe9214b33ead5c7d1f80af469593638b9e1e5f5730a7d3ba2f96b6b555514d4

Description

PHP.Shell-38

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3fe9214b33ead5c7d1f80af469593638b9e1e5f5730a7d3ba2f96b6b555514d4']

Name

179.43.187.33

Description

CC=CH ASN=AS51852 Private Layer INC

Pattern Type

stix

Pattern

[ipv4-addr:value = '179.43.187.33']

Name

23d6611a730bed886cc3b4ce6780a7b5439b01ddf6706ba120ed3ebeb3b1c478

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23d6611a730bed886cc3b4ce6780a7b5439b01ddf6706ba120ed3ebeb3b1c478']

Name

volodimir_azov@justiceua.org

Pattern Type

stix

Pattern

[email-addr:value = 'volodimir_azov@justiceua.org']

Name

justiceua.org

Pattern Type

stix

Pattern

[domain-name:value = 'justiceua.org']

Name

20215acd064c02e5aa6ae3996b53f5313c3f13625a63da1d3795c992ea730191

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '20215acd064c02e5aa6ae3996b53f5313c3f13625a63da1d3795c992ea730191']

Intrusion-Set

Name
Cadet Blizzard

Country

Name
Ukraine

Vulnerability

Name
CVE-2022-41040
Name
CVE-2021-26084
Name
CVE-2020-1472
Name
CVE-2021-4034

Domain-Name

Value
justiceua.org

Email-Addr

Value
volodimir_azov@justiceua.org

StixFile

Value
7fedaf0dec060e40cbdf4ec6d0fbfc427593ad5503ad0abaf6b943405863c897
3e4bb8089657fef9b8e84d9e17fd0d7740853c4c0487081dacc4f22359bade5c
3fe9214b33ead5c7d1f80af469593638b9e1e5f5730a7d3ba2f96b6b555514d4
23d6611a730bed886cc3b4ce6780a7b5439b01ddf6706ba120ed3ebeb3b1c478
20215acd064c02e5aa6ae3996b53f5313c3f13625a63da1d3795c992ea730191

IPv4-Addr

Value
179.43.187.33

External References

- https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/
- https://otx.alienvault.com/pulse/6492fb19bffd961021714870