Jun 10 2023

NETMANAGEIT

Intelligence Report

Investigating BlackSuit Ransomware's Similarities to Royal

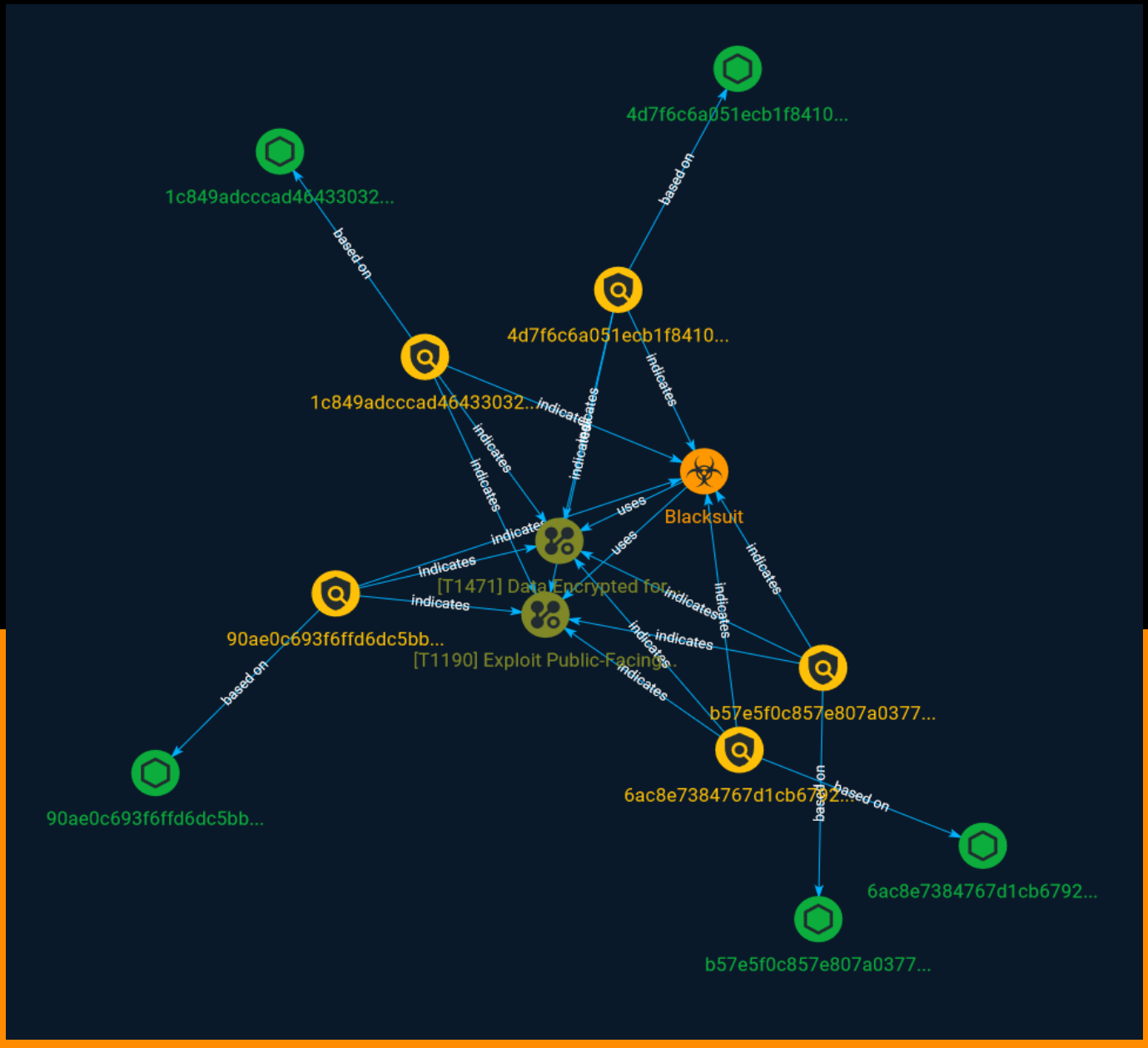

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The emergence of BlackSuit ransomware (with its similarities to Royal) indicates that it is either a new variant developed by the same authors, a copycat using similar code, or an affiliate of the Royal ransomware gang that has implemented modifications to the original family.

Confidence

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

15 / 100

Attack-Pattern

Name
Exploit Public-Facing Application
ID
T1190
Description
Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name
Data Encrypted for Impact
ID
T1471
Description
An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

Indicator

Name

b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08687796be30e2093286c

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08687796be30e2093286c']

Name

90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c

Description

case_4485_ekix4 SHA256 of 30cc7724be4a09d5bcd9254197af05e9fab76455

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c']

Name

4d7f6c6a051ecb1f8410243cd6941b339570165ebcfd3cc7db48d2a924874e99

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d7f6c6a051ecb1f8410243cd6941b339570165ebcfd3cc7db48d2a924874e99']

Name

6ac8e7384767d1cb6792e62e09efc31a07398ca2043652ab11c090e6a585b310

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6ac8e7384767d1cb6792e62e09efc31a07398ca2043652ab11c090e6a585b310']

Name

1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e

Description

is__elf SHA256 of 861793c4e0d4a92844994b640cc6bc3e20944a73

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e']

Malware

Name
Blacksuit

StixFile

Value
6ac8e7384767d1cb6792e62e09efc31a07398ca2043652ab11c090e6a585b310
b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08687796be30e2093286c
1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e
90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c
4d7f6c6a051ecb1f8410243cd6941b339570165ebcfd3cc7db48d2a924874e99

External References

- https://www.trendmicro.com/en_us/research/23/e/investigating-blacksuit-ransomwares-similarities-to-royal.html
- https://otx.alienvault.com/pulse/6478acb235b6b9b1e1726002