Jul 07 2023

NETMANAGEIT

Intelligence Report

The five-day job: A BlackByte ransomware intrusion case study

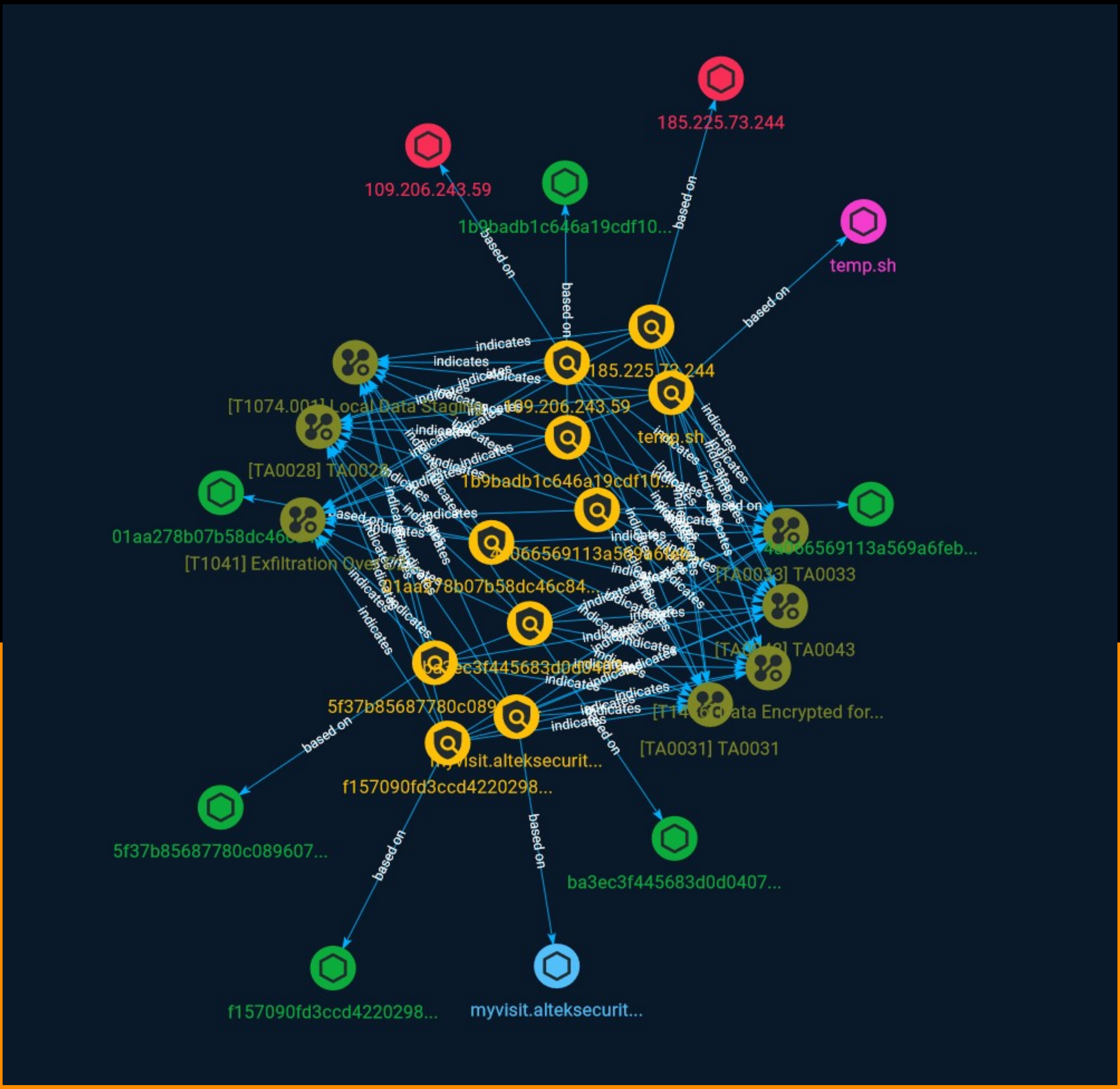

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In a recent investigation by Microsoft Incident Response of a BlackByte 2.0 ransomware attack, we found that the threat actor progressed through the full attack chain, from initial access to impact, in less than five days, causing significant business disruption for the victim organization.

Confidence

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

15 / 100

Indicator

Name

1b9badb1c646a19cdf101ac4f6fdd23bc61eaab8c9f925eb41848cea9fd0738e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1b9badb1c646a19cdf101ac4f6fdd23bc61eaab8c9f925eb41848cea9fd0738e']

Name

5f37b85687780c089607670040dbb3da2749b91b8adc0aa411fd6280b5fa7103

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f37b85687780c089607670040dbb3da2749b91b8adc0aa411fd6280b5fa7103']

Name

01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd']

Name

4a066569113a569a6feb8f44257ac8764ee8f2011765009fdfd82fe3f4b92d3e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4a066569113a569a6feb8f44257ac8764ee8f2011765009fdfd82fe3f4b92d3e']

Name

ba3ec3f445683d0d0407157fda0c26fd669c0b8cc03f21770285a20b3133098f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ba3ec3f445683d0d0407157fda0c26fd669c0b8cc03f21770285a20b3133098f']

Name

109.206.243.59

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.206.243.59']

Name

myvisit.alteksecurity.org

Pattern Type

stix

Pattern

[hostname:value = 'myvisit.alteksecurity.org']

Name

185.225.73.244

Pattern Type

stix

Pattern
[ipv4-addr:value = '185.225.73.244']
Name
temp.sh
Pattern Type
stix
Pattern
[domain-name:value = 'temp.sh']
Name
f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e
Description
TEL:Trojan:Win32/SuspLDAPQuery.A
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e']

Attack-Pattern

Name
TA0033
ID
TA0033
Name
TA0031
ID
TA0031
Name
TA0028
ID
TA0028
Name
TA0043

ID

TA0043

Name

Local Data Staging

ID

T1074.001

Description

Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location. Adversaries may also stage collected data in various available formats/locations of a system, including local storage databases/repositories or the Windows Registry. (Citation: Prevailion DarkWatchman 2021)

Name

Data Encrypted for Impact

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. 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.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Domain-Name

Value
temp.sh

StixFile

Value
5f37b85687780c089607670040dbb3da2749b91b8adc0aa411fd6280b5fa7103
1b9badb1c646a19cdf101ac4f6fdd23bc61eaab8c9f925eb41848cea9fd0738e
ba3ec3f445683d0d0407157fda0c26fd669c0b8cc03f21770285a20b3133098f
01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd
4a066569113a569a6feb8f44257ac8764ee8f2011765009fdfd82fe3f4b92d3e
f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e

Hostname

Value
myvisit.alteksecurity.org

IPv4-Addr

Value
109.206.243.59
185.225.73.244

External References

- https://otx.alienvault.com/pulse/64a8361b22c5c40074fd43cd
- https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/