Jul 03 2023

NETMANAGEIT

Intelligence Report

Manic Menagerie 2.0: The Evolution of a Highly Motivated Threat Actor

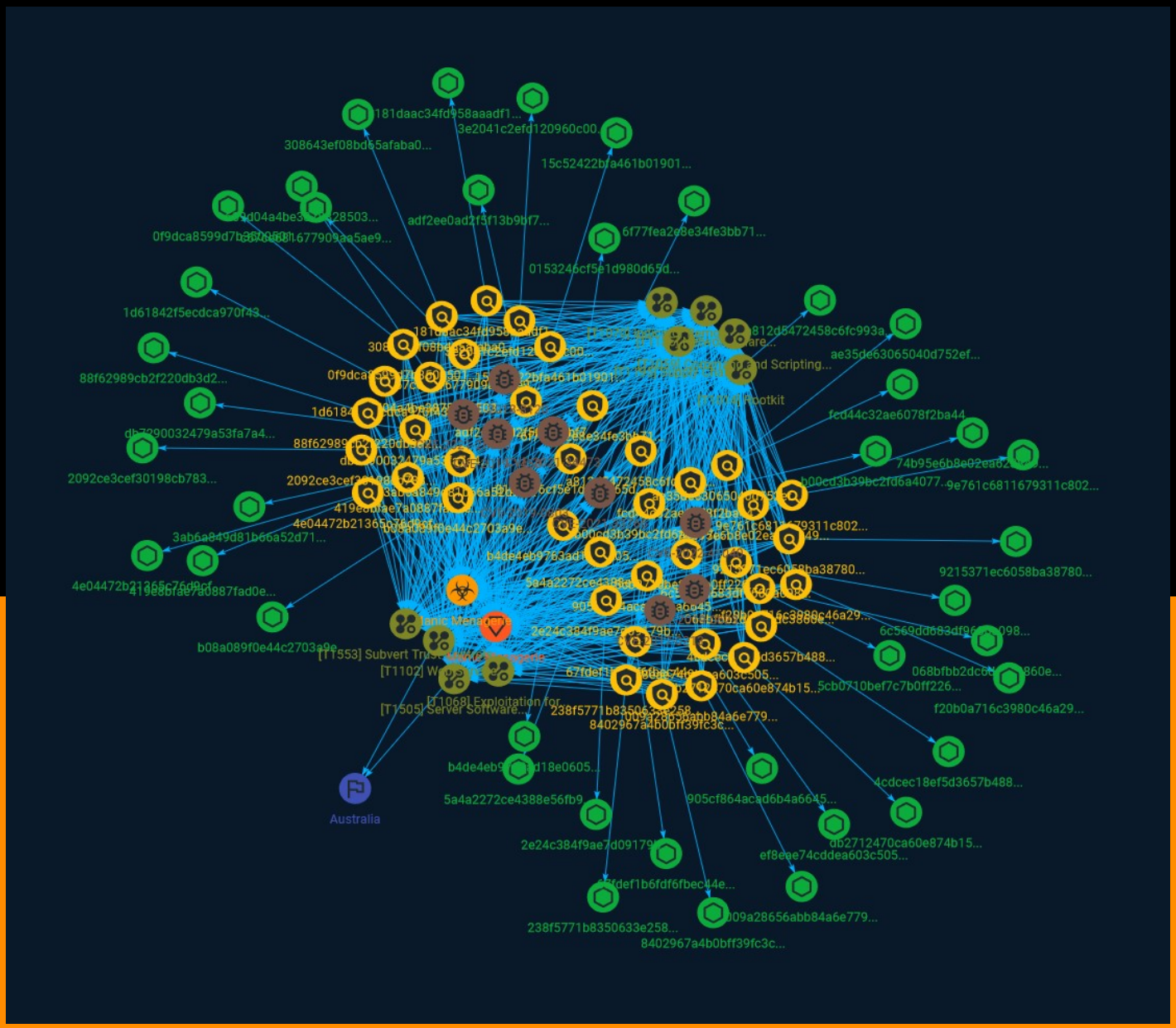

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Manic Menagerie 2.0 campaign was first observed in late 2020 and is believed to be linked to the same threat actor, according to a study by Palo Alto Networks Unit 42.

Confidence

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

15 / 100

Indicator

Name
a812d5472458c6fc993ae1e9e8b9f04e31d176e2ec9f5ce5ac48e32ed72fb414
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a812d5472458c6fc993ae1e9e8b9f04e31d176e2ec9f5ce5ac48e32ed72fb414']
Name
b4de4eb9763ad18e060513048eed4ac39481cfe62127345d0bb058eb26a18528
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b4de4eb9763ad18e060513048eed4ac39481cfe62127345d0bb058eb26a18528']
Name

419e8bfae7a0887fad0eb273791cf0d03c0ed01d1957c7dc796c6e0d1a43f3d6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '419e8bfae7a0887fad0eb273791cf0d03c0ed01d1957c7dc796c6e0d1a43f3d6']

Name

74b95e6b8e02ea623849b6bcbf702922dd064ae06238b27cbb20504e38d85756

Description

Win64:Trojan-gen

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '74b95e6b8e02ea623849b6bcbf702922dd064ae06238b27cbb20504e38d85756']

Name

ef8eae74cddea603c5051de7808f402943d674c6bb557db1eff6a50d25114b6b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ef8eae74cddea603c5051de7808f402943d674c6bb557db1eff6a50d25114b6b']

Name

c67ce681677909aa5ae9abcf42c35faffee08cd73b5cee8d975fa07159f76c87

Description

DT_VMP_32

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c67ce681677909aa5ae9abcf42c35faffee08cd73b5cee8d975fa07159f76c87']

Name

f20b0a716c3980c46a2996ae21e3566c0151202557417d171566b82e97057f2f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f20b0a716c3980c46a2996ae21e3566c0151202557417d171566b82e97057f2f']

Name

b08a089f0e44c2703a9e0dc4f6ef8d9285a08241499ad21dbf7f1fbc262d22bd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b08a089f0e44c2703a9e0dc4f6ef8d9285a08241499ad21dbf7f1fbc262d22bd']

Name

6f77fea2e8e34fe3bb7134e110036e44e30a6d5144794669a6de21a30f3b7247

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f77fea2e8e34fe3bb7134e110036e44e30a6d5144794669a6de21a30f3b7247']

Name

5a4a2272ce4388e56fb9d33255ac8c584d41c7099588ef9f39e4bee54be92992

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5a4a2272ce4388e56fb9d33255ac8c584d41c7099588ef9f39e4bee54be92992']

Name

3ab6a849d81b66a52d717cc1b0178882e30d44c39b1089604c5746a187b2e4ce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3ab6a849d81b66a52d717cc1b0178882e30d44c39b1089604c5746a187b2e4ce']

Name

0153246cf5e1d980d65d4920bdc5b2ac4c9aba6d5b6676f0e9bbde794dd04314

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0153246cf5e1d980d65d4920bdc5b2ac4c9aba6d5b6676f0e9bbde794dd04314']

Name

905cf864acad6b4a664582eb9fc6e0afab87198274a29e5f7d7863fee29f37cd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '905cf864acad6b4a664582eb9fc6e0afab87198274a29e5f7d7863fee29f37cd']

Name

adf2ee0ad2f5f13b9bf72741c75910f786d2cfee84b5ae78ea3e5464f46addde

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'adf2ee0ad2f5f13b9bf72741c75910f786d2cfee84b5ae78ea3e5464f46addde']

Name

b00cd3b39bc2fd6a4077c679f050d97ed26ef20a1fe80ad3525ea0dbbd131f74

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b00cd3b39bc2fd6a4077c679f050d97ed26ef20a1fe80ad3525ea0dbbd131f74']

Name

db7290032479a53fa7a43262188132d572fab63d00d6d64d39f9256df6c10f55

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'db7290032479a53fa7a43262188132d572fab63d00d6d64d39f9256df6c10f55']

Name

9e761c6811679311c80291b7d65f23cdd53865f72af64b5a72ae1a86d9ef27d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9e761c6811679311c80291b7d65f23cdd53865f72af64b5a72ae1a86d9ef27d0']

Name

67fdef1b6fdf6fbec44e4df1608fb46dfbcfa3363bf62872ec132d000092a18f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '67fdef1b6fdf6fbec44e4df1608fb46dfbcfa3363bf62872ec132d000092a18f']

Name

308643ef08bd65afaba0831582698597551584 5fb5d6235db80a9bc5bdbb00f3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '308643ef08bd65afaba0831582698597551584 5fb5d6235db80a9bc5bdbb00f3']

Name

068bfbb2dc6dadc3860eb16cc7ece97d935948f9b64ec66d5afda08e682be790

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '068bfbb2dc6dadc3860eb16cc7ece97d935948f9b64ec66d5afda08e682be790']

Name

4e04472b21365c76d9cf0a324f889f723621fc42433a2f211a23dce728fa4a8a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4e04472b21365c76d9cf0a324f889f723621fc42433a2f211a23dce728fa4a8a']

Name

3e2041c2efd120960c00bf794b5db4c967fc862e2d536ed5f7b5d5d1cf9bfda0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3e2041c2efd120960c00bf794b5db4c967fc862e2d536ed5f7b5d5d1cf9bfda0']

Name

6c569dd683df9600a098a93c9200d44778d535f58f5a82f4a58aeed3855fb9ca

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c569dd683df9600a098a93c9200d44778d535f58f5a82f4a58aeed3855fb9ca']

Name

609d04a4be3878328503c342f0d73c9ba5ff1c6c62f4c894516e50721207ef83

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '609d04a4be3878328503c342f0d73c9ba5ff1c6c62f4c894516e50721207ef83']

Name

9215371ec6058ba38780a5d336eb3201a47c77bb97bb00a60f1bec0386185c77

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9215371ec6058ba38780a5d336eb3201a47c77bb97bb00a60f1bec0386185c77']

Name

2e24c384f9ae7d09179bd41e51c4a9bb43102d170990e8e1576e79362b049ed6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2e24c384f9ae7d09179bd41e51c4a9bb43102d170990e8e1576e79362b049ed6']

Name

181daac34fd958aaadf1c9de1414cc3b331ef394ba47d5d2c77d30e9ac89ef17

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '181daac34fd958aaadf1c9de1414cc3b331ef394ba47d5d2c77d30e9ac89ef17']

Name

4cdcec18ef5d3657b488f32912a8ccf4541891e4e4c8518afbc1e1b0e147e96b

Description

Win.Trojan.CryptocoinMiner-6448864-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4cdcec18ef5d3657b488f32912a8ccf4541891e4e4c8518afbc1e1b0e147e96b']

Name

2092ce3cef30198cb7833851a1b1805bbfe71474152c1357ecd27f71ce807527

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2092ce3cef30198cb7833851a1b1805bbfe71474152c1357ecd27f71ce807527']

Name

fcd44c32ae6078f2ba44c8c5e2efa3f9b788d4c6470a5ee9bd4944699fb8357a

Description

Win.Trojan.Generic-9910725-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fcd44c32ae6078f2ba44c8c5e2efa3f9b788d4c6470a5ee9bd4944699fb8357a']

Name

009a28656abb84a6e7794fdd721565a2e2ca2565870597962d67a8e2c3707241

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '009a28656abb84a6e7794fdd721565a2e2ca2565870597962d67a8e2c3707241']

Name

1d61842f5ecdca970f43246ce93f51fa4c85c00b93b6b9e37db17325077497eb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1d61842f5ecdca970f43246ce93f51fa4c85c00b93b6b9e37db17325077497eb']

Name

5cb0710bef7c7b0ff226bf5ca12f499859505547696f22fa06ce1f47ea312d82

Description

Win64:Trojan-gen

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5cb0710bef7c7b0ff226bf5ca12f499859505547696f22fa06ce1f47ea312d82']

Name
238f5771b8350633e258221e25223e52545709b74cbe2c9361e2b730f9dbfa00
Description
Win64:Trojan-gen
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '238f5771b8350633e258221e25223e52545709b74cbe2c9361e2b730f9dbfa00']
Name
15c52422bfa461b01901953f5e0d9c77aa0f898c8de4841303a572c59a269674
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '15c52422bfa461b01901953f5e0d9c77aa0f898c8de4841303a572c59a269674']
Name
db2712470ca60e874b15fa1e5ef667dbf6b755223ee5eb20843843115537e1c4
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'db2712470ca60e874b15fa1e5ef667dbf6b755223ee5eb20843843115537e1c4']

Name

88f62989cb2f220db3d289ffea924423487b180fabe37711d2ef5c7f2e306f13

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '88f62989cb2f220db3d289ffea924423487b180fabe37711d2ef5c7f2e306f13']

Name

ae35de63065040d752ef9fa76c553c0fa5c3cc5c8d67cf6981c66d3c8d86a6a6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ae35de63065040d752ef9fa76c553c0fa5c3cc5c8d67cf6981c66d3c8d86a6a6']

Name

8402967a4b0bff39fc3ccc7a5b613734135551e9f6f32cf8c14fd6541a85d4d5

Description

Win.Malware.Vmprotect-6824127-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8402967a4b0bff39fc3ccc7a5b613734135551e9f6f32cf8c14fd6541a85d4d5']

Name

0f9dca8599d7b350050149e63a6a977f1d157d5967ba6da534919530063cdcde

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f9dca8599d7b350050149e63a6a977f1d157d5967ba6da534919530063cdcde']

Intrusion-Set

Name
Manic Menagerie

Malware

Name
Manic Menagerie

Vulnerability

Name
CVE-2018-8120
Name
CVE-2019-0623
Name
CVE-2019-0803
Name
CVE-2021-33766
Name
CVE-2017-0213
Name
CVE-2019-1458
Name
CVE-2022-41040

Name
CVE-2021-26855

Name
CVE-2021-34473

StixFile

Value
238f5771b8350633e258221e25223e52545709b74cbe2c9361e2b730f9dbfa00
5cb0710bef7c7b0ff226bf5ca12f499859505547696f22fa06ce1f47ea312d82
068bfbb2dc6dadc3860eb16cc7ece97d935948f9b64ec66d5afda08e682be790
0f9dca8599d7b350050149e63a6a977f1d157d5967ba6da534919530063cdcde
4e04472b21365c76d9cf0a324f889f723621fc42433a2f211a23dce728fa4a8a
6f77fea2e8e34fe3bb7134e110036e44e30a6d5144794669a6de21a30f3b7247
b08a089f0e44c2703a9e0dc4f6ef8d9285a08241499ad21dbf7f1fbc262d22bd
6c569dd683df9600a098a93c9200d44778d535f58f5a82f4a58aeed3855fb9ca
9e761c6811679311c80291b7d65f23cdd53865f72af64b5a72ae1a86d9ef27d0
308643ef08bd65afaba0831582698597551584 5fb5d6235db80a9bc5bdbb00f3
ae35de63065040d752ef9fa76c553c0fa5c3cc5c8d67cf6981c66d3c8d86a6a6
fcd44c32ae6078f2ba44c8c5e2efa3f9b788d4c6470a5ee9bd4944699fb8357a
5a4a2272ce4388e56fb9d33255ac8c584d41c7099588ef9f39e4bee54be92992

adf2ee0ad2f5f13b9bf72741c75910f786d2cfee84b5ae78ea3e5464f46addde

db7290032479a53fa7a43262188132d572fab63d00d6d64d39f9256df6c10f55

15c52422bfa461b01901953f5e0d9c77aa0f898c8de4841303a572c59a269674

ef8eae74cddea603c5051de7808f402943d674c6bb557db1eff6a50d25114b6b

2092ce3cef30198cb7833851a1b1805bbfe71474152c1357ecd27f71ce807527

74b95e6b8e02ea623849b6bcbf702922dd064ae06238b27cbb20504e38d85756

419e8bfae7a0887fad0eb273791cf0d03c0ed01d1957c7dc796c6e0d1a43f3d6

b00cd3b39bc2fd6a4077c679f050d97ed26ef20a1fe80ad3525ea0dbbd131f74

f20b0a716c3980c46a2996ae21e3566c0151202557417d171566b82e97057f2f

67fdef1b6fdf6fbec44e4df1608fb46dfbcfa3363bf62872ec132d000092a18f

3e2041c2efd120960c00bf794b5db4c967fc862e2d536ed5f7b5d5d1cf9bfda0

9215371ec6058ba38780a5d336eb3201a47c77bb97bb00a60f1bec0386185c77

b4de4eb9763ad18e060513048eed4ac39481cfe62127345d0bb058eb26a18528

905cf864acad6b4a664582eb9fc6e0afab87198274a29e5f7d7863fee29f37cd

c67ce681677909aa5ae9abcf42c35faffee08cd73b5cee8d975fa07159f76c87

181daac34fd958aaadf1c9de1414cc3b331ef394ba47d5d2c77d30e9ac89ef17

a812d5472458c6fc993ae1e9e8b9f04e31d176e2ec9f5ce5ac48e32ed72fb414

0153246cf5e1d980d65d4920bdc5b2ac4c9aba6d5b6676f0e9bbde794dd04314

db2712470ca60e874b15fa1e5ef667dbf6b755223ee5eb20843843115537e1c4

8402967a4b0bff39fc3ccc7a5b613734135551e9f6f32cf8c14fd6541a85d4d5

88f62989cb2f220db3d289ffea924423487b180fabe37711d2ef5c7f2e306f13

4cdcec18ef5d3657b488f32912a8ccf4541891e4e4c8518afbc1e1b0e147e96b

009a28656abb84a6e7794fdd721565a2e2ca2565870597962d67a8e2c3707241

609d04a4be3878328503c342f0d73c9ba5ff1c6c62f4c894516e50721207ef83

3ab6a849d81b66a52d717cc1b0178882e30d44c39b1089604c5746a187b2e4ce

1d61842f5ecdca970f43246ce93f51fa4c85c00b93b6b9e37db17325077497eb

2e24c384f9ae7d09179bd41e51c4a9bb43102d170990e8e1576e79362b049ed6

External References

- https://otx.alienvault.com/pulse/64a2fbb3456bca41d63e4011
- https://unit42.paloaltonetworks.com/manic-menagerie-targets-web-hosting-and-it/