Apr 10 2024

NETMANAGEIT

Intelligence Report

Crypt888 ransomware: technical analysis of the malware

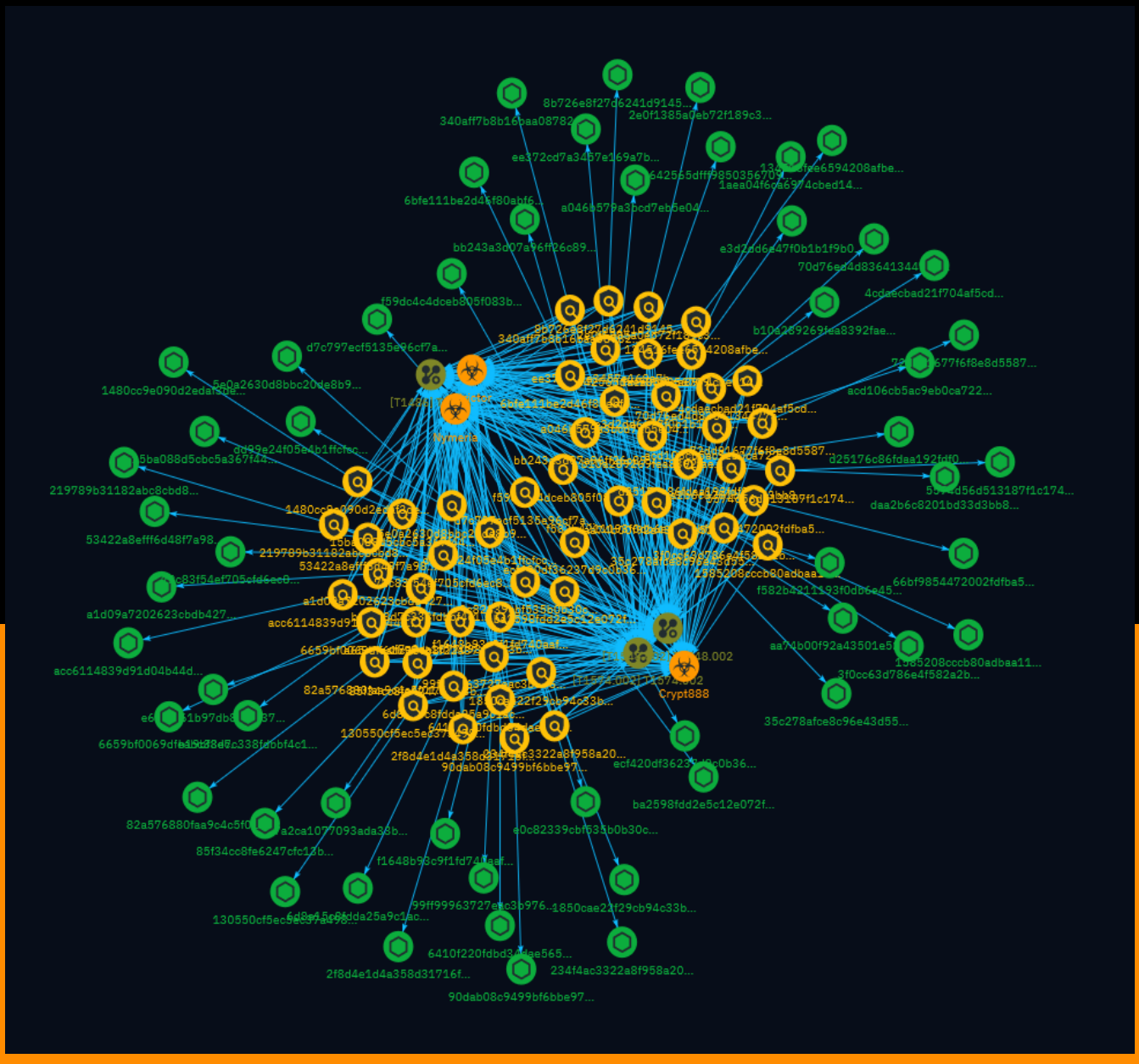

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report details the technical analysis conducted by Stormshield's Cyber Threat Intelligence team on the Crypt888 ransomware, a malware family also known as Strictor or Nymeria. It outlines the initial attack vectors, language and obfuscation techniques used, the chronology of the ransomware attack including UAC bypass, file encryption, and ransom note display. The report also provides a synthesis of the attack modeling using the MITRE ATT&CK framework, indicators of compromise (IOCs), and recommendations for protection against this threat.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
f59dc4c4dceb805f083b4aad13705e2a4dde67967e9dd29fa8bb6fce3e00b1f0
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f59dc4c4dceb805f083b4aad13705e2a4dde67967e9dd29fa8bb6fce3e00b1f0']
Name
f582b4211193f0db6e4519667794942561830 6d270e47ac720cfe58a537147ff
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f582b4211193f0db6e4519667794942561830 6d270e47ac720cfe58a537147ff']
Name

ee372cd7a3457e169a7b8ebaabce843531d67c6f0c72cf17ec2fb7b292f43b4a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ee372cd7a3457e169a7b8ebaabce843531d67c6f0c72cf17ec2fb7b292f43b4a']

Name

f1648b93c9f1fd740aaf2e367284c6e23ecebe8238b9dfd50c06c2a664184ee7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f1648b93c9f1fd740aaf2e367284c6e23ecebe8238b9dfd50c06c2a664184ee7']

Name

ecf420df36237d9c0b360bbde960ddf398759a128f56f4a0ff8717f107741c8b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ecf420df36237d9c0b360bbde960ddf398759a128f56f4a0ff8717f107741c8b']

Name

e3d2dd6e47f0b1b1f9b0816b83107c94d5fc46cc299e7dd9470610130bb8ce13

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e3d2dd6e47f0b1b1f9b0816b83107c94d5fc46cc299e7dd9470610130bb8ce13']

Name

e65d2f61b97db8f22a370b987ddc50fd26b1c95e1ec545c2777484796fbf942a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e65d2f61b97db8f22a370b987ddc50fd26b1c95e1ec545c2777484796fbf942a']

Name

e0c82339cbf535b0b30cef16dcb590cbdfe3898605776c6ca296070c5b11c9d9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e0c82339cbf535b0b30cef16dcb590cbdfe3898605776c6ca296070c5b11c9d9']

Name

daa2b6c8201bd33d3bb871e2b94ec3beb4b4de471104082b0eafece5bd68ccc3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'daa2b6c8201bd33d3bb871e2b94ec3beb4b4de471104082b0eafece5bd68ccc3']

Name

dd99e24f05e4b1ffcfcc8823826fb098db7a3793b0c798f8fc195351812330f7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dd99e24f05e4b1ffcfcc8823826fb098db7a3793b0c798f8fc195351812330f7']

Name

d7c797ecf5135e96cf7a6936ac5eb53d6cd39e019159789d6ba857f6285eaddb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd7c797ecf5135e96cf7a6936ac5eb53d6cd39e019159789d6ba857f6285eaddb']

Name

d25176c86fdaa192fdf02abc04842f05c40bb7c0f6bfce8864f166031bd0ba32

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd25176c86fdaa192fdf02abc04842f05c40bb7c0f6bfce8864f166031bd0ba32']

Name

cf7a2ca1077093ada33b15a0ed40067eee421e084d2fefb544d865352b1138d5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cf7a2ca1077093ada33b15a0ed40067eee421e084d2fefb544d865352b1138d5']

Name

bb243a3d07a96ff26c89496a9901c14772f235d0a678798f30faa389a25b1bb7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb243a3d07a96ff26c89496a9901c14772f235d0a678798f30faa389a25b1bb7']

Name

ba2598fdd2e5c12e072fbe4c10fcdc6742bace92c0edba42ca4ca7bc195cb813

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ba2598fdd2e5c12e072fbe4c10fcdc6742bace92c0edba42ca4ca7bc195cb813']

Name

b19bf8d7c338fdbbf4c15cf91749796ed7d9bd6ff2bd39c0d8a1b9a439db0bf7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b19bf8d7c338fdbbf4c15cf91749796ed7d9bd6ff2bd39c0d8a1b9a439db0bf7']

Name

b10a289269fea8392fae69aef57ed8fd7ed1faaec188bb4526927a37d99b22a8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b10a289269fea8392fae69aef57ed8fd7ed1faaec188bb4526927a37d99b22a8']

Name

acc6114839d91d04b44de3f4483abcbbaeadb16294ce058348046f089bc65283

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'acc6114839d91d04b44de3f4483abcbbaeadb16294ce058348046f089bc65283']

Name

acd106cb5ac9eb0ca722b3453c9641e536db573dbf5e6dc03591b5158b751a41

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'acd106cb5ac9eb0ca722b3453c9641e536db573dbf5e6dc03591b5158b751a41']

Name

aa74b00f92a43501e52e20a8c214dd2e9c3d86c14935b3cbb01e2a81fca2c9e3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa74b00f92a43501e52e20a8c214dd2e9c3d86c14935b3cbb01e2a81fca2c9e3']

Name

a1d09a7202623cbdb4278d980a522320be83ceb1f99d5f4ed87b4844fb8064a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a1d09a7202623cbdb4278d980a522320be83ceb1f99d5f4ed87b4844fb8064a9']

Name

a046b579a3bcd7eb5e044bfa10161ca5ae78dc3ebd395244d3f764b179f4a827

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a046b579a3bcd7eb5e044bfa10161ca5ae78dc3ebd395244d3f764b179f4a827']

Name

99ff99963727eac3b9766674faf1660348453c4509741be7d975f88a69a83331

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '99ff99963727eac3b9766674faf1660348453c4509741be7d975f88a69a83331']

Name

8b726e8f27d6241d914588a1bd39fb37cf4ba5b181ff013c083e71f0f1ee4ff9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8b726e8f27d6241d914588a1bd39fb37cf4ba5b181ff013c083e71f0f1ee4ff9']

Name

90dab08c9499bf6bbe9795116f9207d047283eccfee792894335b8ea1afbcac7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '90dab08c9499bf6bbe9795116f9207d047283eccfee792894335b8ea1afbcac7']

Name

85f34cc8fe6247cfc13b3521a4678030a120f623bfc85bca186a8291a926d0b0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '85f34cc8fe6247cfc13b3521a4678030a120f623bfc85bca186a8291a926d0b0']

Name

72dd91677f6f8e8d5587d4a9c684f46eda77ede9dfcf22c699af8651cb407d34

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '72dd91677f6f8e8d5587d4a9c684f46eda77ede9dfcf22c699af8651cb407d34']

Name

82a576880faa9c4c5f017688ea414f54e10d7db78a83def90eb8a98c88c078cb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '82a576880faa9c4c5f017688ea414f54e10d7db78a83def90eb8a98c88c078cb']

Name

72c83f54ef705cfd6ec86ac5e1a28810744670f6064c2b9a9501d5208b1d54b1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '72c83f54ef705cfd6ec86ac5e1a28810744670f6064c2b9a9501d5208b1d54b1']

Name

70d76ed4d836413447756b708875881f2afcf1bf7a00609e8cd37fa04fff354e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '70d76ed4d836413447756b708875881f2afcf1bf7a00609e8cd37fa04fff354e']

Name

6d8a15c8fdda25a9c1ac11028a93c0a6d95e1dd8327e7558a67bcf0ac39e2da6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d8a15c8fdda25a9c1ac11028a93c0a6d95e1dd8327e7558a67bcf0ac39e2da6']

Name

6bfe111be2d46f80abf6eea2371059d8e5dbaa3cecdf9aaf242f23ef894869f3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6bfe111be2d46f80abf6eea2371059d8e5dbaa3cecdf9aaf242f23ef894869f3']

Name

66bf9854472002fdfba5974f8fcba00b08b721c7241a1f0df06d18fd0858a387

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '66bf9854472002fdfba5974f8fcba00b08b721c7241a1f0df06d18fd0858a387']

Name

6659bf0069dfeabc33ec7ac5ec0c50e5a8cf70aa10f4201a83b870aa6c115627

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6659bf0069dfeabc33ec7ac5ec0c50e5a8cf70aa10f4201a83b870aa6c115627']

Name

642565dfff9850356709a6a094c169e1ee83cba56ac1bd92477e7de01e965ac3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '642565dfff9850356709a6a094c169e1ee83cba56ac1bd92477e7de01e965ac3']

Name

6410f220fdbd34dae565f5fba45e85107741c13d19a91b3126e735fbe0425606

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6410f220fdbd34dae565f5fba45e85107741c13d19a91b3126e735fbe0425606']

Name

5e0a2630d8bbc20de8b90ccd89389f8c01298b475fd8330738fe5519a6e01cfb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e0a2630d8bbc20de8b90ccd89389f8c01298b475fd8330738fe5519a6e01cfb']

Name

5574d56d513187f1c174c30f07c7d8b61d312cd0c303012e53a7877e0564bee8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5574d56d513187f1c174c30f07c7d8b61d312cd0c303012e53a7877e0564bee8']

Name

53422a8efff6d48f7a985a6cb48b26035ca1cda53c40b1aeea1864270c324831

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '53422a8efff6d48f7a985a6cb48b26035ca1cda53c40b1aeea1864270c324831']

Name

4cdaecbad21f704af5cdfb089a88c2947ebe3dc4c6965f5d273533c6810162ea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4cdaecbad21f704af5cdfb089a88c2947ebe3dc4c6965f5d273533c6810162ea']

Name

3f0cc63d786e4f582a2bf200ac2fde5f44a3e095b5cf40a1a8dedcbe4fb1aded

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3f0cc63d786e4f582a2bf200ac2fde5f44a3e095b5cf40a1a8dedcbe4fb1aded']

Name

340aff7b8b16baa0878296d974b3a3114fb84dde6dd891bfe64adc8c12bd2cb5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '340aff7b8b16baa0878296d974b3a3114fb84dde6dd891bfe64adc8c12bd2cb5']

Name

35c278afce8c96e43d556ed58e82108cbef6253e52e6ffcb04edac695d1bafbf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35c278afce8c96e43d556ed58e82108cbef6253e52e6ffcb04edac695d1bafbf']

Name

2f8d4e1d4a358d31716fcb5f7bc8d00913708ac47e5607265b33d47b201fa58b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f8d4e1d4a358d31716fcb5f7bc8d00913708ac47e5607265b33d47b201fa58b']

Name

2e0f1385a0eb72f189c3d3cffa38020d71370ab621139c5688647c5bab6bc7f2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2e0f1385a0eb72f189c3d3cffa38020d71370ab621139c5688647c5bab6bc7f2']

Name

234f4ac3322a8f958a20d7e68ea60a95732ede2d4b4050bb800d66a6b6c23636

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '234f4ac3322a8f958a20d7e68ea60a95732ede2d4b4050bb800d66a6b6c23636']

Name

219789b31182abc8cbd83b5fee52d72f9a1bf20a38557c2d5b9a2aa96281e5de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '219789b31182abc8cbd83b5fee52d72f9a1bf20a38557c2d5b9a2aa96281e5de']

Name

1aea04f6ca6974cbed14b9858dd6731b0d38d1313db23a38145dacdace725932

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1aea04f6ca6974cbed14b9858dd6731b0d38d1313db23a38145dacdace725932']

Name

1850cae22f29cb94c33b33a2361ed7de3c4a94c42cb3b3bda69b2b26dbec3259

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1850cae22f29cb94c33b33a2361ed7de3c4a94c42cb3b3bda69b2b26dbec3259']

Name

15ba088d5cbc5a367f44e2a36beccee4ba90fec855c20e2b18adc889bd3b1bff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '15ba088d5cbc5a367f44e2a36beccee4ba90fec855c20e2b18adc889bd3b1bff']

Name

1585208cccb80adbaa116c96f0efae1ccfdbc0fe7d9cff97c9c5ba714d18fd92

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1585208cccb80adbaa116c96f0efae1ccfdbc0fe7d9cff97c9c5ba714d18fd92']

Name

1480cc9e090d2edaf3de59b1b4e76a43c8f1fe40f66e73c5c6b9c91b69ba7a00

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1480cc9e090d2edaf3de59b1b4e76a43c8f1fe40f66e73c5c6b9c91b69ba7a00']

Name

134516fee6594208afbe6c4fe9dec0926130afecd9f46e26989f202176cea01e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '134516fee6594208afbe6c4fe9dec0926130afecd9f46e26989f202176cea01e']

Name

130550cf5ec5ec37a4985b0fd3c66582d941c80e35e804e98a842dc5bef38c27

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '130550cf5ec5ec37a4985b0fd3c66582d941c80e35e804e98a842dc5bef38c27']

Malware

Name
Nymeria
Name
Strictor
Name
Crypt888

Attack-Pattern

Name
T1574.002
ID
T1574.002
Description
Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001), side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s). Side-loading takes advantage of the DLL search order used by the loader by positioning both the victim application and malicious payload(s) alongside each other. Adversaries likely use side-loading as a means of masking actions they perform under a legitimate, trusted, and potentially elevated system or software process. Benign executables used to side-load payloads may not be flagged during delivery and/or execution. Adversary payloads may also be encrypted/packed or otherwise obfuscated until loaded into the memory of the trusted process.(Citation: FireEye DLL Side-Loading)
Name
T1486
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

T1548.002

ID

T1548.002

Description

Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action. (Citation: TechNet How UAC Works) If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs can elevate privileges or execute some elevated [Component Object Model](https://attack.mitre.org/techniques/T1559/001) objects without prompting the user through the UAC notification box.(Citation: TechNet Inside UAC)(Citation: MSDN COM Elevation) An example of this is use of [Rundll32](https://attack.mitre.org/techniques/T1218/011) to load a specifically crafted DLL which loads an auto-elevated [Component Object Model](https://attack.mitre.org/techniques/T1559/001) object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user.(Citation: Davidson Windows) Many methods have been discovered to bypass UAC. The Github readme page for UACME contains an extensive list of methods(Citation: Github UACMe) that have been discovered and implemented, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as: * `eventvwr.exe` can auto-elevate and execute a specified binary or script.(Citation: enigma0x3 Fileless UAC Bypass)(Citation: Fortinet Fareit) Another bypass is possible through some lateral movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on remote systems and default to high integrity.(Citation: SANS UAC Bypass)

StixFile

Value
f59dc4c4dceb805f083b4aad13705e2a4dde67967e9dd29fa8bb6fce3e00b1f0
f582b4211193f0db6e45196677949425618306d270e47ac720cfe58a537147ff
f1648b93c9f1fd740aaf2e367284c6e23ecebe8238b9dfd50c06c2a664184ee7
ee372cd7a3457e169a7b8ebaabce843531d67c6f0c72cf17ec2fb7b292f43b4a
ecf420df36237d9c0b360bbde960ddf398759a128f56f4a0ff8717f107741c8b
e65d2f61b97db8f22a370b987ddc50fd26b1c95e1ec545c2777484796fbf942a
e3d2dd6e47f0b1b1f9b0816b83107c94d5fc46cc299e7dd9470610130bb8ce13
e0c82339cbf535b0b30cef16dcb590cbdfe3898605776c6ca296070c5b11c9d9
dd99e24f05e4b1ffcfcc8823826fb098db7a3793b0c798f8fc195351812330f7
daa2b6c8201bd33d3bb871e2b94ec3beb4b4de471104082b0eafece5bd68ccc3
d7c797ecf5135e96cf7a6936ac5eb53d6cd39e019159789d6ba857f6285eaddb
d25176c86fdaa192fdf02abc04842f05c40bb7c0f6bfce8864f166031bd0ba32
cf7a2ca1077093ada33b15a0ed40067eee421e084d2fefb544d865352b1138d5

bb243a3d07a96ff26c89496a9901c14772f235d0a678798f30faa389a25b1bb7

ba2598fdd2e5c12e072fbe4c10fcdc6742bace92c0edba42ca4ca7bc195cb813

b19bf8d7c338fdbbf4c15cf91749796ed7d9bd6ff2bd39c0d8a1b9a439db0bf7

b10a289269fea8392fae69aef57ed8fd7ed1faaec188bb4526927a37d99b22a8

acd106cb5ac9eb0ca722b3453c9641e536db573dbf5e6dc03591b5158b751a41

acc6114839d91d04b44de3f4483abcbbaeadb16294ce058348046f089bc65283

aa74b00f92a43501e52e20a8c214dd2e9c3d86c14935b3cbb01e2a81fca2c9e3

a1d09a7202623cbdb4278d980a522320be83ceb1f99d5f4ed87b4844fb8064a9

a046b579a3bcd7eb5e044bfa10161ca5ae78dc3ebd395244d3f764b179f4a827

99ff99963727eac3b9766674faf1660348453c4509741be7d975f88a69a83331

90dab08c9499bf6bbe9795116f9207d047283eccfee792894335b8ea1afbcac7

8b726e8f27d6241d914588a1bd39fb37cf4ba5b181ff013c083e71f0f1ee4ff9

85f34cc8fe6247cfc13b3521a4678030a120f623bfc85bca186a8291a926d0b0

82a576880faa9c4c5f017688ea414f54e10d7db78a83def90eb8a98c88c078cb

72dd91677f6f8e8d5587d4a9c684f46eda77ede9dfcf22c699af8651cb407d34

72c83f54ef705cfd6ec86ac5e1a28810744670f6064c2b9a9501d5208b1d54b1

70d76ed4d836413447756b708875881f2afcf1bf7a00609e8cd37fa04fff354e

6d8a15c8fdda25a9c1ac11028a93c0a6d95e1dd8327e7558a67bcf0ac39e2da6

6bfe111be2d46f80abf6eea2371059d8e5dbaa3cecdf9aaf242f23ef894869f3

66bf9854472002fdfba5974f8fcba00b08b721c7241a1f0df06d18fd0858a387

6659bf0069dfeabc33ec7ac5ec0c50e5a8cf70aa10f4201a83b870aa6c115627

642565dfff9850356709a6a094c169e1ee83cba56ac1bd92477e7de01e965ac3

6410f220fdbd34dae565f5fba45e85107741c13d19a91b3126e735fbe0425606

5e0a2630d8bbc20de8b90ccd89389f8c01298b475fd8330738fe5519a6e01cfb

5574d56d513187f1c174c30f07c7d8b61d312cd0c303012e53a7877e0564bee8

4cdaecbad21f704af5cdfb089a88c2947ebe3dc4c6965f5d273533c6810162ea

53422a8efff6d48f7a985a6cb48b26035ca1cda53c40b1aeea1864270c324831

3f0cc63d786e4f582a2bf200ac2fde5f44a3e095b5cf40a1a8dedcbe4fb1aded

35c278afce8c96e43d556ed58e82108cbef6253e52e6ffcb04edac695d1bafbf

340aff7b8b16baa0878296d974b3a3114fb84dde6dd891bfe64adc8c12bd2cb5

2f8d4e1d4a358d31716fcb5f7bc8d00913708ac47e5607265b33d47b201fa58b

219789b31182abc8cbd83b5fee52d72f9a1bf20a38557c2d5b9a2aa96281e5de

2e0f1385a0eb72f189c3d3cffa38020d71370ab621139c5688647c5bab6bc7f2

234f4ac3322a8f958a20d7e68ea60a95732ede2d4b4050bb800d66a6b6c23636

1aea04f6ca6974cbed14b9858dd6731b0d38d1313db23a38145dacdace725932

1850cae22f29cb94c33b33a2361ed7de3c4a94c42cb3b3bda69b2b26dbec3259

15ba088d5cbc5a367f44e2a36beccee4ba90fec855c20e2b18adc889bd3b1bff

134516fee6594208afbe6c4fe9dec0926130afecd9f46e26989f202176cea01e

1585208cccb80adbaa116c96f0efae1ccfdbc0fe7d9cff97c9c5ba714d18fd92

130550cf5ec5ec37a4985b0fd3c66582d941c80e35e804e98a842dc5bef38c27

1480cc9e090d2edaf3de59b1b4e76a43c8f1fe40f66e73c5c6b9c91b69ba7a00

External References

- https://www.stormshield.com/news/technical-analysis-of-ransomware-crypt888
- https://otx.alienvault.com/pulse/66168f60eef1356560bf1388