Jun 10 2023

NETMANAGEIT

Intelligence Report

Buhti: New Ransomware Operation Relies on Repurposed Payloads

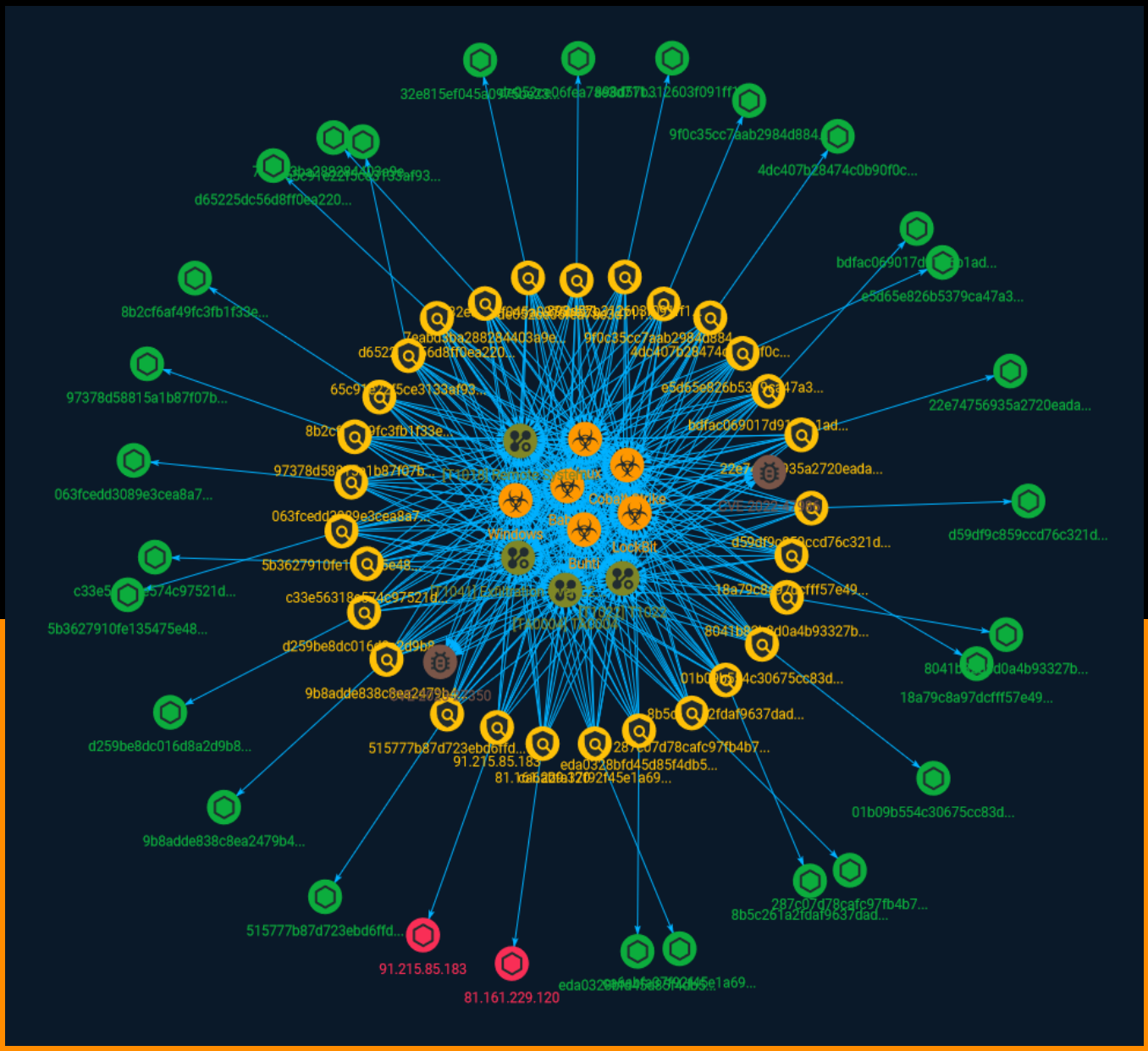

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A relatively new ransomware operation calling itself Buhti appears to be eschewing developing its own payload and is instead utilizing variants of the leaked LockBit and Babuk ransomware families to attack Windows and Linux systems.

Confidence

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

15 / 100

Attack-Pattern

Name
TA0004
ID
TA0004
Name
Remote System Discovery
ID
T1018
Description
Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097) or `net view` using [Net](https://attack.mitre.org/software/S0039). Adversaries may also analyze data from local host files (ex: `C:\Windows\System32\Drivers\etc\hosts` or `/etc/hosts`) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment. Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information

about systems within a network (e.g. `show cdp neighbors`, `show arp`).(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)

Name

T1022

ID

T1022

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.

Indicator

Name

8b5c261a2fdaf9637dada7472b1b5dd1d340a47a00fe7c39a79cf836ef77e441

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8b5c261a2fdaf9637dada7472b1b5dd1d340a47a00fe7c39a79cf836ef77e441']

Name

063fcedd3089e3cea8a7e07665ae033ba765b51a6dc1e7f54dde66a79c67e1e7

Description

Win.Ransomware.BlackMatter-9965914-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '063fcedd3089e3cea8a7e07665ae033ba765b51a6dc1e7f54dde66a79c67e1e7']

Name

bdfac069017d9126b1ad661febfab7eb1b8e70af1186a93cb4aff93911183f24

Description

Win.File.Sliver-9942542-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bdfac069017d9126b1ad661febfab7eb1b8e70af1186a93cb4aff93911183f24']

Name

81.161.229.120

Description

CC=US ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '81.161.229.120']

Name

d65225dc56d8ff0ea2205829c21b5803fcb03dc57a7e9da5062cbd74e1a6b7d6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd65225dc56d8ff0ea2205829c21b5803fcb03dc57a7e9da5062cbd74e1a6b7d6']

Name

8041b82b8d0a4b93327bc8f0b71672b0e8f300dc7849d78bb2d72e2e0f147334

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8041b82b8d0a4b93327bc8f0b71672b0e8f300dc7849d78bb2d72e2e0f147334']

Name

d259be8dc016d8a2d9b89dbd7106e22a1df2164d84f80986baba5e9a51ed4a65

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd259be8dc016d8a2d9b89dbd7106e22a1df2164d84f80986baba5e9a51ed4a65']

Name

9f0c35cc7aab2984d88490afdb515418306146ca72f49edbfbd85244e63cfabd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f0c35cc7aab2984d88490afdb515418306146ca72f49edbfbd85244e63cfabd']

Name

eda0328bfd45d85f4db5dbb4340f38692175a063b7321b49b2c8ebae3ab2868c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'eda0328bfd45d85f4db5dbb4340f38692175a063b7321b49b2c8ebae3ab2868c']

Name

8b2cf6af49fc3fb1f33e94ad02bd9e43c3c62ba2cfd25ff3dfc7a29dde2b20f2

Description

SLFPER:Win32/Meterpreter!ApiRetrieval

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8b2cf6af49fc3fb1f33e94ad02bd9e43c3c62ba2cfd25ff3dfc7a29dde2b20f2']

Name

22e74756935a2720eadacf03dc8fe5e7579f354a6494734e2183095804ef19fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '22e74756935a2720eadacf03dc8fe5e7579f354a6494734e2183095804ef19fe']

Name

91.215.85.183

Description

CC=RU ASN=AS200593 Prospero Ooo

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.215.85.183']

Name

32e815ef045a0975be2372b85449b25bd7a7c5a497c3facc2b54bcffcbb0041c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '32e815ef045a0975be2372b85449b25bd7a7c5a497c3facc2b54bcffcbb0041c']

Name

01b09b554c30675cc83d4b087b31f980ba14e9143d387954df484894115f82d4

Description

ELF:Filecoder-BP\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '01b09b554c30675cc83d4b087b31f980ba14e9143d387954df484894115f82d4']

Name

5b3627910fe135475e48fd9e0e89e5ad958d3d500a0b1b5917f592dc6503ee72

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5b3627910fe135475e48fd9e0e89e5ad958d3d500a0b1b5917f592dc6503ee72']

Name

4dc407b28474c0b90f0c5173de5c4f1082c827864f045c4571890d967eadd880

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4dc407b28474c0b90f0c5173de5c4f1082c827864f045c4571890d967eadd880']

Name

ca6abfa37f92f45e1a69161f5686f719aaa95d82ad953d6201b0531fb07f0937

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ca6abfa37f92f45e1a69161f5686f719aaa95d82ad953d6201b0531fb07f0937']

Name

65c91e22f5ce3133af93b69d8ce43de6b6ccac98fc8841fd485d74d30c2dbe7b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '65c91e22f5ce3133af93b69d8ce43de6b6ccac98fc8841fd485d74d30c2dbe7b']

Name

d59df9c859ccd76c321d03702f0914debbadc036e168e677c57b9dcc16e980cb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd59df9c859ccd76c321d03702f0914debbadc036e168e677c57b9dcc16e980cb']

Name

9b8adde838c8ea2479b444ed0bb8c53b7e01e7460934a6f2e797de58c3a6a8bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9b8adde838c8ea2479b444ed0bb8c53b7e01e7460934a6f2e797de58c3a6a8bf']

Name

de052ce06fea7ae3d711654bc182d765a3f440d2630e700e642811c89491df72

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de052ce06fea7ae3d711654bc182d765a3f440d2630e700e642811c89491df72']

Name

287c07d78cafc97fb4b7ef364a228b708d31e8fe8e9b144f7db7d986a1badd52

Description

ELF:Filecoder-BP\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '287c07d78cafc97fb4b7ef364a228b708d31e8fe8e9b144f7db7d986a1badd52']

Name

97378d58815a1b87f07beefb24b40c5fb57f8cce649136ff57990b957aa9d56a

Description

Trojan:Win64/Meterpreter.B

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '97378d58815a1b87f07beefb24b40c5fb57f8cce649136ff57990b957aa9d56a']

Name

e5d65e826b5379ca47a371505678bca6071f2538f98b5fef9e33b45da9c06206

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e5d65e826b5379ca47a371505678bca6071f2538f98b5fef9e33b45da9c06206']

Name

515777b87d723ebd6ffd5b755d848bb7d7eb50fc85b038cf25d69ca7733bd855

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '515777b87d723ebd6ffd5b755d848bb7d7eb50fc85b038cf25d69ca7733bd855']

Name

7eabd3ba288284403a9e041a82478d4b6490bc4b333d839cc73fa665b211982c

Description

ELF:Filecoder-BP\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7eabd3ba288284403a9e041a82478d4b6490bc4b333d839cc73fa665b211982c']

Name

18a79c8a97dcfff57e4984aa7e74aa6ded22af8e485e807b34b7654d6cf69eef

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '18a79c8a97dcfff57e4984aa7e74aa6ded22af8e485e807b34b7654d6cf69eef']

Name

c33e56318e574c97521d14d68d24b882ffb0ed65d96203970b482d8b2c332351

Description

Trojan:Win64/Meterpreter.B

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c33e56318e574c97521d14d68d24b882ffb0ed65d96203970b482d8b2c332351']

Name

898d57b312603f091ff1a28cb2514a05bd9f0eb55ace5d6158cc118d1e37070a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '898d57b312603f091ff1a28cb2514a05bd9f0eb55ace5d6158cc118d1e37070a']

Malware

Name
LockBit

Name
Babuk

Description
[Babuk](https://attack.mitre.org/software/S0638) is a Ransomware-as-a-service (RaaS) malware that has been used since at least 2021. The operators of [Babuk](https://attack.mitre.org/software/S0638) employ a "Big Game Hunting" approach to targeting major enterprises and operate a leak site to post stolen data as part of their extortion scheme.(Citation: Sogeti CERT ESEC Babuk March 2021)(Citation: McAfee Babuk February 2021)(Citation: CyberScoop Babuk February 2021)

Name
Linux

Name
Buhti

Name
Windows

Name
Cobalt Strike

Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

StixFile

Value
ca6abfa37f92f45e1a69161f5686f719aaa95d82ad953d6201b0531fb07f0937
eda0328bfd45d85f4db5dbb4340f38692175a063b7321b49b2c8ebae3ab2868c
898d57b312603f091ff1a28cb2514a05bd9f0eb55ace5d6158cc118d1e37070a
287c07d78cafc97fb4b7ef364a228b708d31e8fe8e9b144f7db7d986a1badd52
e5d65e826b5379ca47a371505678bca6071f2538f98b5fef9e33b45da9c06206
9b8adde838c8ea2479b444ed0bb8c53b7e01e7460934a6f2e797de58c3a6a8bf
32e815ef045a0975be2372b85449b25bd7a7c5a497c3facc2b54bcffcbb0041c
01b09b554c30675cc83d4b087b31f980ba14e9143d387954df484894115f82d4
18a79c8a97dcfff57e4984aa7e74aa6ded22af8e485e807b34b7654d6cf69eef
bdfac069017d9126b1ad661febfab7eb1b8e70af1186a93cb4aff93911183f24
22e74756935a2720eadacf03dc8fe5e7579f354a6494734e2183095804ef19fe
8041b82b8d0a4b93327bc8f0b71672b0e8f300dc7849d78bb2d72e2e0f147334
8b2cf6af49fc3fb1f33e94ad02bd9e43c3c62ba2cfd25ff3dfc7a29dde2b20f2

4dc407b28474c0b90f0c5173de5c4f1082c827864f045c4571890d967eadd880

de052ce06fea7ae3d711654bc182d765a3f440d2630e700e642811c89491df72

c33e56318e574c97521d14d68d24b882ffb0ed65d96203970b482d8b2c332351

65c91e22f5ce3133af93b69d8ce43de6b6ccac98fc8841fd485d74d30c2dbe7b

7eabd3ba288284403a9e041a82478d4b6490bc4b333d839cc73fa665b211982c

9f0c35cc7aab2984d88490afdb515418306146ca72f49edbfbd85244e63cfabd

063fcedd3089e3cea8a7e07665ae033ba765b51a6dc1e7f54dde66a79c67e1e7

515777b87d723ebd6ffd5b755d848bb7d7eb50fc85b038cf25d69ca7733bd855

d59df9c859ccd76c321d03702f0914debbadc036e168e677c57b9dcc16e980cb

8b5c261a2fdaf9637dada7472b1b5dd1d340a47a00fe7c39a79cf836ef77e441

d65225dc56d8ff0ea2205829c21b5803fcb03dc57a7e9da5062cbd74e1a6b7d6

97378d58815a1b87f07beefb24b40c5fb57f8cce649136ff57990b957aa9d56a

5b3627910fe135475e48fd9e0e89e5ad958d3d500a0b1b5917f592dc6503ee72

d259be8dc016d8a2d9b89dbd7106e22a1df2164d84f80986baba5e9a51ed4a65

IPv4-Addr

Value
91.215.85.183
81.161.229.120

External References

- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/buhti-ransomware
- https://otx.alienvault.com/pulse/6471109bec697a82895fc293