redsense
INTELLIGENCE OPERATIONS

TLP:GREEN

OVERVIEW

Blackbasta is an active former-Conti staffed ransomware group that began organizing in late 2021 behind the dissolution of Conti's centralized operations. Active operations were first observed in spring and summer of 2022, and there are several TTP similarities that carry forward from Conti to blackbasta operations:

MALWARE

Post infection, the desktop background is changed, icons of encrypted files are replaced with black cube, and victims are presented with a ransom note.

T1566: Well-crafted phishing lures
T1219: Cobalt Strike beaconing (default base64 encoded ps1)
T1059: Recon, enumeration, and lateral movement via PowerShell
T1482: Kerberoasting
T1136: Domain admin account creation
T1003: Credential dumping
T1197: Background Intelligence Transfer Service (BITS) jobs

```
All of your files are currently encrypted by no_name_software.

These files cannot be recovered by any means without contacting our team directly.

DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additional recovery software) can damage your files.
However,
if you want to try - we recommend choosing the data of the lowest value.

DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond.
So it will be better for both sides if you contact us as soon as possible.

DON'T TRY TO CONTACT feds or any recovery companies.
We have our informants in these structures, so any of your complaints will be immediately directed to us.
So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will consider this as a hostile intent and
initiate the publication of whole compromised data immediately.

DON'T move or rename your files. These parameters can be used for encryption/decryption process.

To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

https://REDACTED.onion:80/

Your company id for log in: REDACTED
Your company key: 3 of any of your dc through comma. Example: "DC1, DC2, DC3". You can type less if you have no enough

YOU SHOULD BE AWARE!
We will speak only with an authorized person. It can be the CEO, top management, etc.
In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to your company!
Inform your supervisors and stay calm!
```

Both the .onion URL of the chat and the "company unique ID" are provided for the victim to use to access the negotiation chat.

TARGETING

Blackbasta is assessed as financial motivated and highly opportunistic, and initial victim verticals include construction, manufacturing, and healthcare fields. According to DarkFeed, blackbasta has published details relating to 79, mostly U.S. victims.

REFERENCES

https://northwave-security.com/black-basta-blog/
https://bazaar.abuse.ch/browse/signature/BlackBasta/
https://www.securityweek.com/black-basta-ransomware-becomes-major-threat-two-months
https://blog.malwarebytes.com/ransomware/2022/06/blackbasta-is-the-latest-ransomware-to-target-esxi-virtual-machines-on-linux/
https://intel471.com/blog/access-brokers-ransomware-relationship-growing
https://www.securityweek.com/access-brokers-and-ransomware-service-gangs-tighten-relationships
https://www.truesec.com/hub/blog/proxyshell-qbot-and-conti-ransomware-combined-in-a-series-of-cyber-attacks