LockBit ransomware recruiting insiders to breach corporate networks

bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

Lawrence Abrams

By
Lawrence Abrams

- August 4, 2021
- 12:19 PM
- 0

The LockBit 2.0 ransomware gang is actively recruiting corporate insiders to help them breach and encrypt networks. In return, the insider is promised million-dollar payouts.

Many ransomware gangs operate as a Ransomware-as-a-Service, which consists of a core group of developers, who maintain the ransomware and payment sites, and recruited affiliates who breach victims' networks and encrypt devices.

Any ransom payments that victims make are then split between the core group and the affiliate, with the affiliate usually receiving 70-80% of the total amount.

However, in many cases, the affiliates purchase access to networks from other third-party pentesters rather than breaching the company themselves.

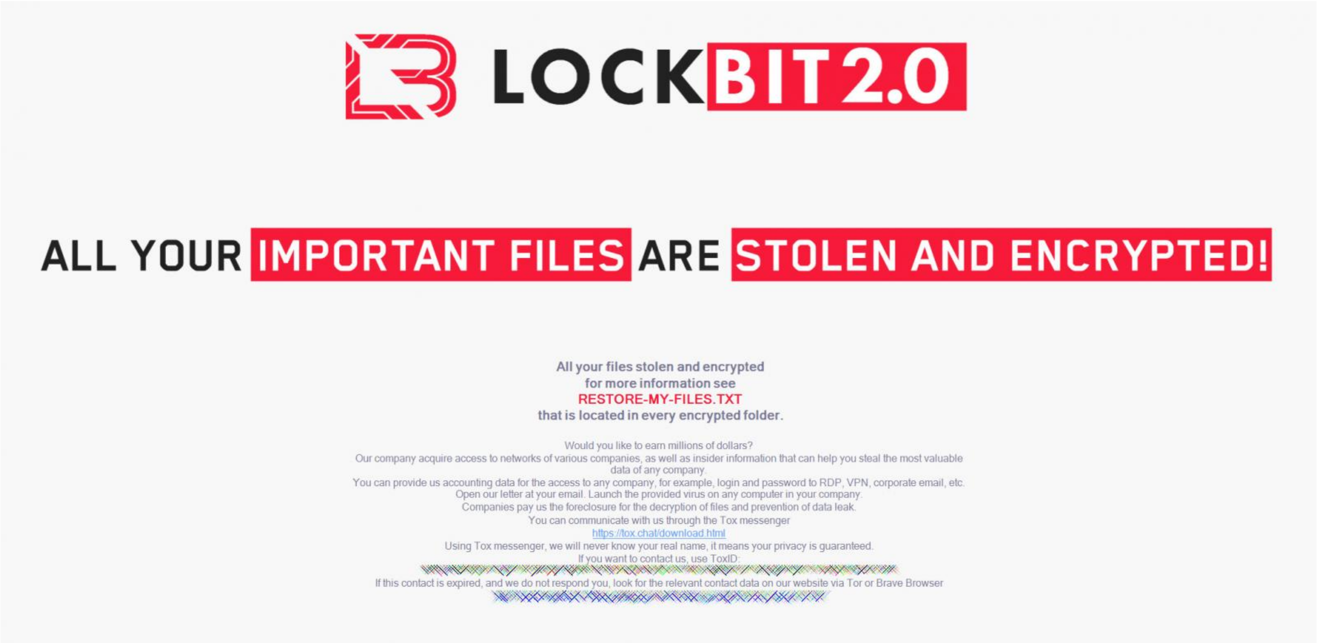
With LockBit 2.0, the ransomware gang is trying to remove the middle-man and instead recruit insiders to provide them access to a corporate network.

LockBit 2.0 promises millions of dollars to insiders

In June, the LockBit ransomware operation announced the launch of their new LockBit 2.0 ransomware-as-a-service.

This relaunch included redesigned Tor sites and numerous advanced features, including automatically encrypting devices on a network via group policies.

With this relaunch, LockBit has also changed the Windows wallpaper placed on encrypted devices to offer "millions of dollars" for corporate insiders who provide access to networks where they have an account.



LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
[redacted]
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
[redacted]

New LockBit 2.0 wallpaper recruiting insiders

The full text, with the contact information redacted, explains that LockBit is looking for RDP, VPN, corporate email credentials that they can then use to gain access to the network.

The ransomware gang also says they will send the insider a "virus" that should be executed on a computer, likely to give the ransomware gang remote access to the network.

> "Would you like to earn millions of dollars?
> Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
> You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc. Open our letter at your email.
> Launch the provided virus on any computer in your company.
> Companies pay us the foreclosure for the decryption of files and prevention of data leak.
> You can communicate with us through the Tox messenger
> https://tox.chat/download.html
> Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
> If you want to contact us, use ToxID: xxxx"

When we first saw this message, it seemed counterintuitive to recruit an insider for a network already been breached.

However, this message is likely targeting external IT consultants who may see the message while responding to an attack.

While this tactic may sound far-fetched, it is not the first time threat actors attempted to recruit an employee to encrypt their company's network.

In August 2020, the FBI arrested a Russian national for attempting to recruit a Tesla employee to plant malware on the network of Tesla's Nevada Gigafactory.

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

Online library app Onleihe faces issues after cyberattack on provider

New Black Basta ransomware springs into action with a dozen breaches

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.