Hackers use Conti's leaked ransomware to attack Russian companies

bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/

Lawrence Abrams

By
Lawrence Abrams

- April 9, 2022
- 02:30 PM
- 0

A hacking group used the Conti's leaked ransomware source code to create their own ransomware to use in cyberattacks against Russian organizations.

While it is common to hear of ransomware attacks targeting companies and encrypting data, we rarely hear about Russian organizations getting attacked similarly.

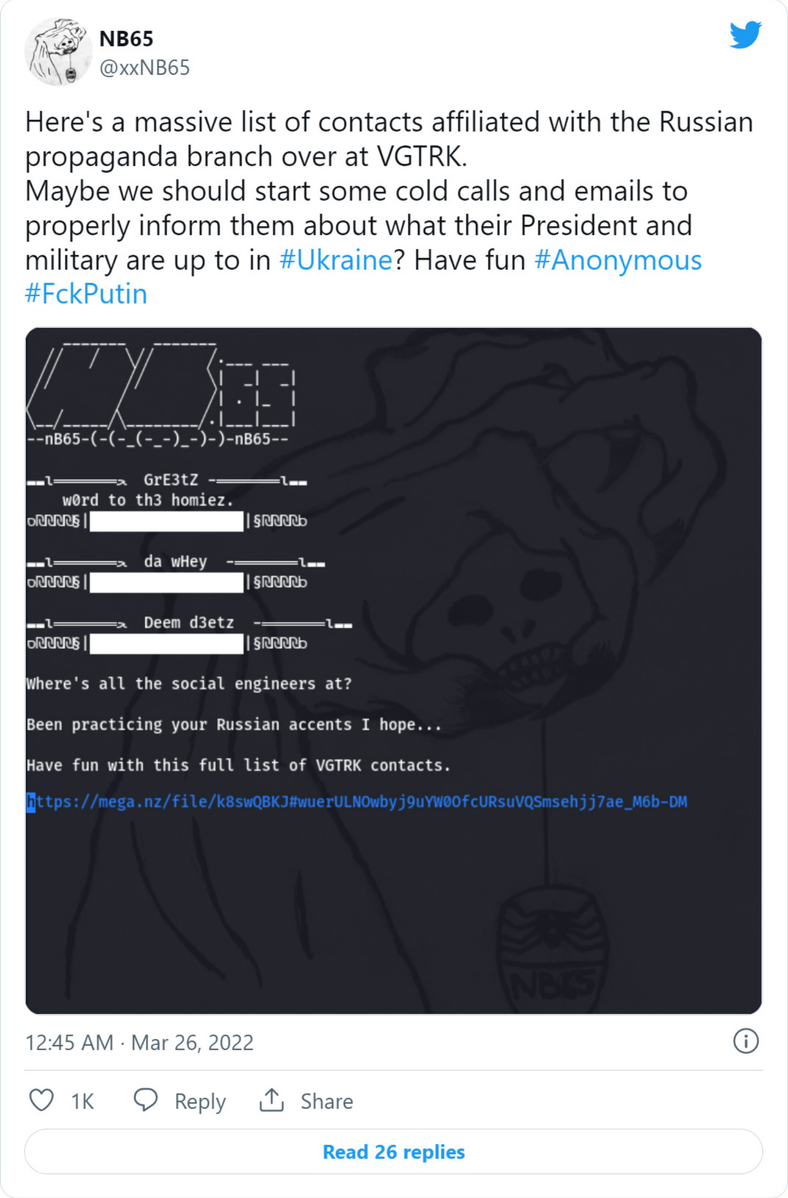
This lack of attacks is due to the general belief by Russian hackers that if they do not attack Russian interests, then the country's law enforcement would turn a blind eye toward attacks on other countries.

However, the tables have now turned, with a hacking group known as NB65 now targeting Russian organizations with ransomware attacks.

Ransomware targets Russia

For the past month, a hacking group known as NB65 has been breaching Russian entities, stealing their data, and leaking it online, warning that the attacks are due to Russia's invasion of Ukraine.

The Russian entities claimed to have been attacked by the hacking group include document management operator Tensor, Russian space agency Roscosmos, and VGTRK, the state-owned Russian Television and Radio broadcaster.



NB65
@xxNB65

Here's a massive list of contacts affiliated with the Russian propaganda branch over at VGTRK.
Maybe we should start some cold calls and emails to properly inform them about what their President and military are up to in #Ukraine? Have fun #Anonymous #FckPutin

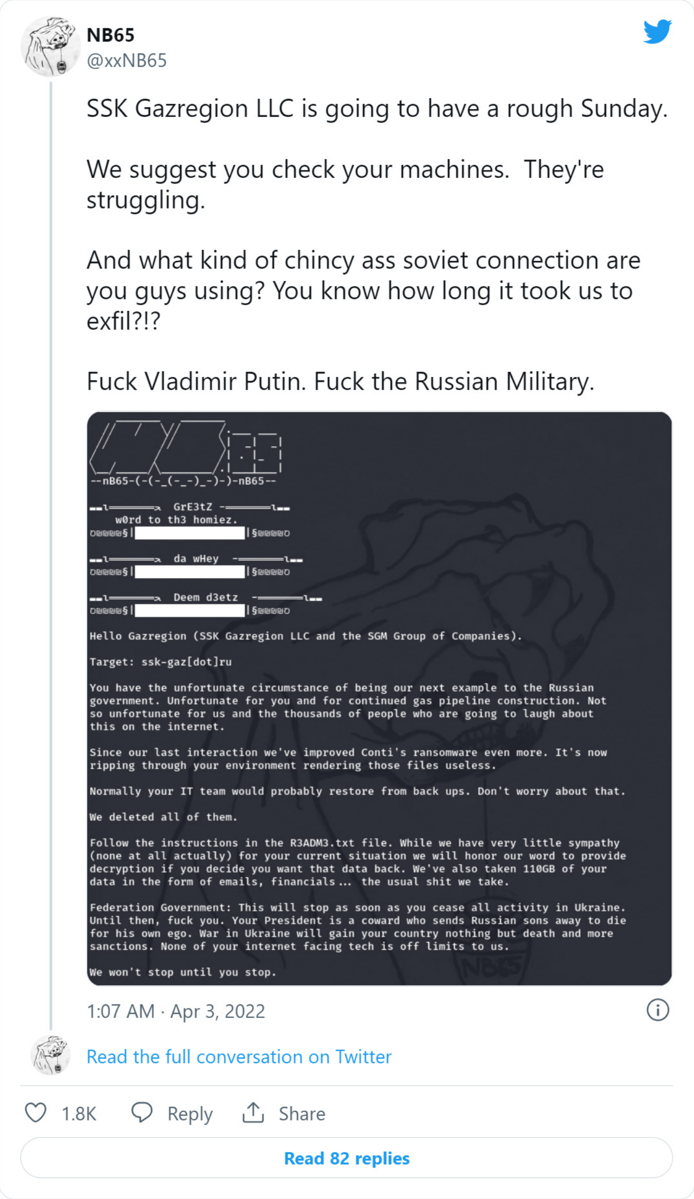
```
   _______   _______
 //  '  \Y/'        \.___ ___
/ /    /  /          |  _|  _|
\  /   / /           | . |_  |
 \__/_____/\________/.|___|___|
--nB65-(-(-_(-_-)_-)-)-nB65--

▬▬l═══════➢ GrE3tZ -═══════l▬▬
    w0rd to th3 homiez.
ᴏꝚꝚꝚꝚ§|[redacted]|§ꝚꝚꝚꝚb

▬▬l═══════➢ da wHey  -═══════l▬▬
ᴏꝚꝚꝚꝚ§|[redacted]|§ꝚꝚꝚꝚb

▬▬l═══════➢ Deem d3etz  -═══════l▬▬
ᴏꝚꝚꝚꝚ§|[redacted]|§ꝚꝚꝚꝚb

Where's all the social engineers at?

Been practicing your Russian accents I hope...

Have fun with this full list of VGTRK contacts.

https://mega.nz/file/k8swQBKJ#wuerULNOwbyj9uYW0OfcURsuVQSmsehjj7ae_M6b-DM
```

12:45 AM · Mar 26, 2022

The attack on VGTRK was particularly significant as it led to the alleged theft of 786.2 GB of data, including 900,000 emails and 4,000 files, which were published on the DDoS Secrets website.

More recently, the NB65 hackers have turned to a new tactic — targeting Russian organizations with ransomware attacks since the end of March.

What makes this more interesting, is that the hacking group created their ransomware using the leaked source code for the Conti Ransomware operation, which are Russian threat actors who prohibit their members from attacking entities in Russia.



NB65
@xxNB65

SSK Gazregion LLC is going to have a rough Sunday.

We suggest you check your machines. They're struggling.

And what kind of chincy ass soviet connection are you guys using? You know how long it took us to exfil?!?

Fuck Vladimir Putin. Fuck the Russian Military.

```
--nB65-(-(-_(-_-)_-)-)-nB65--

▬▬l═══════> GrE3tZ -═══════l▬▬
    w0rd to th3 homiez.
ʊɐɐɐɐ§|[redacted]|§ɐɐɐɐʊ

▬▬l═══════> da wHey  -═══════l▬▬
ʊɐɐɐɐ§|[redacted]|§ɐɐɐɐʊ

▬▬l═══════> Deem d3etz  -═══════l▬▬
ʊɐɐɐɐ§|[redacted]|§ɐɐɐɐʊ

Hello Gazregion (SSK Gazregion LLC and the SGM Group of Companies).

Target: ssk-gaz[dot]ru

You have the unfortunate circumstance of being our next example to the Russian
government. Unfortunate for you and for continued gas pipeline construction. Not
so unfortunate for us and the thousands of people who are going to laugh about
this on the internet.

Since our last interaction we've improved Conti's ransomware even more. It's now
ripping through your environment rendering those files useless.

Normally your IT team would probably restore from back ups. Don't worry about that.

We deleted all of them.

Follow the instructions in the R3ADM3.txt file. While we have very little sympathy
(none at all actually) for your current situation we will honor our word to provide
decryption if you decide you want that data back. We've also taken 110GB of your
data in the form of emails, financials... the usual shit we take.

Federation Government: This will stop as soon as you cease all activity in Ukraine.
Until then, fuck you. Your President is a coward who sends Russian sons away to die
for his own ego. War in Ukraine will gain your country nothing but death and more
sanctions. None of your internet facing tech is off limits to us.

We won't stop until you stop.
```

1:07 AM · Apr 3, 2022

Read the full conversation on Twitter

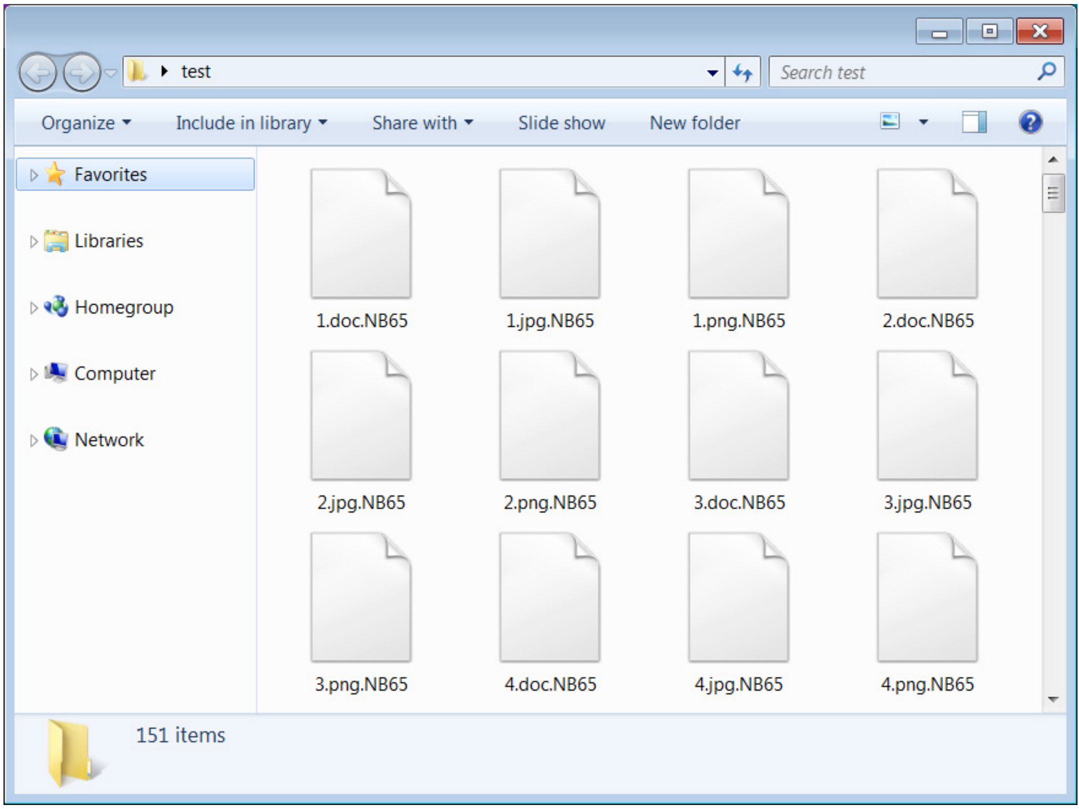
Conti's source code was leaked after they sided with Russia over the attack on Ukraine, and a security researcher leaked 170,000 internal chat messages and source code for their operation.

BleepingComputer first learned of NB65's attacks by threat analyst Tom Malka, but we could not find a ransomware sample, and the hacking group was not willing to share it.

However, this changed yesterday when a sample of the NB65's modified Conti ransomware executable was uploaded to VirusTotal, allowing us to get a glimpse of how it works.

Almost all antivirus vendors detect this sample on VirusTotal as Conti, and Intezer Analyze also determined it uses 66% of the same code as the usual Conti ransomware samples.

BleepingComputer gave NB65's ransomware a run, and when encrypting files, it will append the **.NB65** extension to the encrypted file's names.

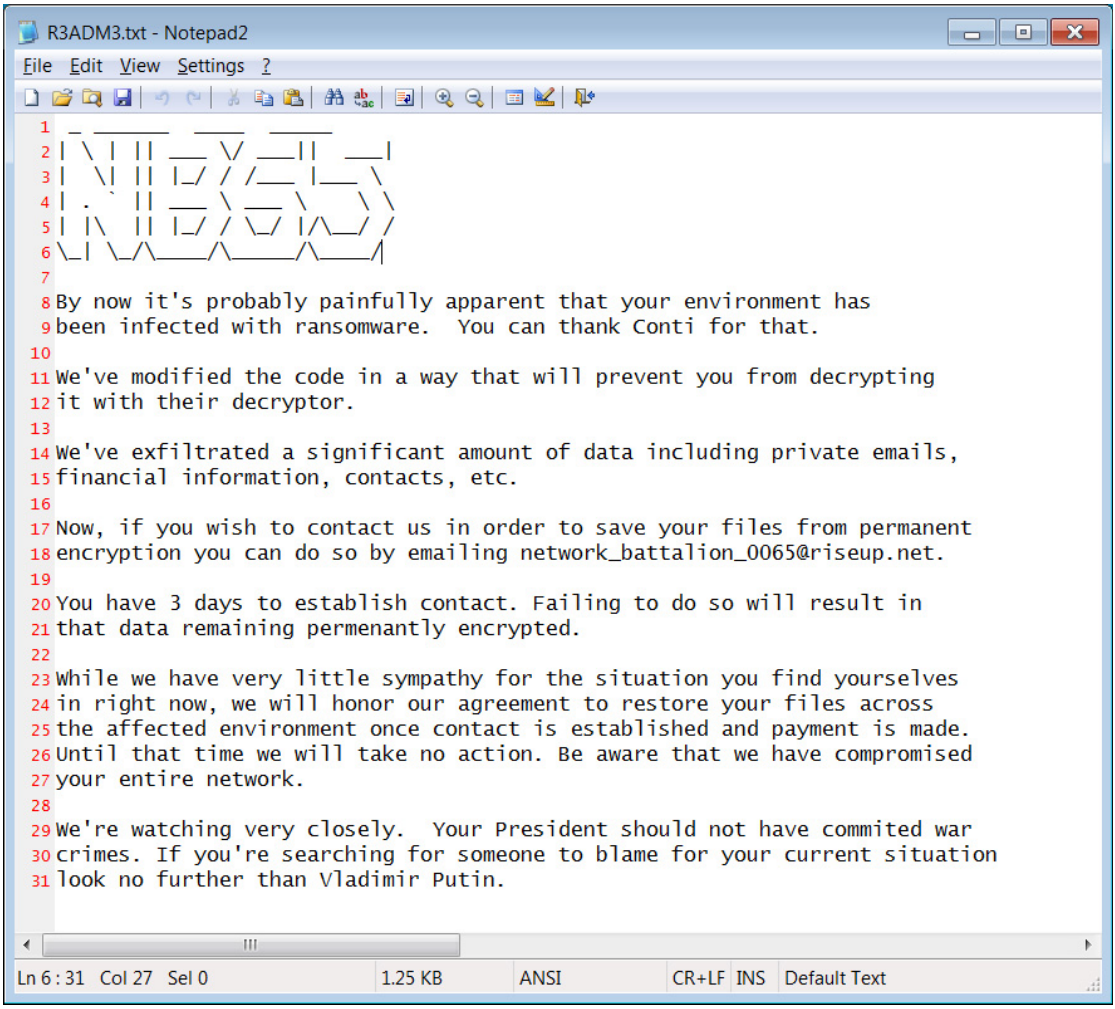


Files encrypted by NB65's ransomware

Source: BleepingComputer

The ransomware will also create ransom notes named **R3ADM3.txt** throughout the encrypted device, with the threat actors blaming the cyberattack on President Vladimir Putin for invading Ukraine.

"We're watching very closely. Your President should not have commited war crimes. If you're searching for someone to blame for your current situation look no further than Vladimir Putin," reads the NB65 ransomware note displayed below.



```
 _   _ ______  ____  _____ 
| \ | || ___ \/ ___||  ___|
|  \| || |_/ / /___ |___ \ 
| . ` || ___ \ ___ \    \ \
| |\  || |_/ / \_/ |/\__/ /
\_| \_/\____/\_____/\____/ 

By now it's probably painfully apparent that your environment has
been infected with ransomware.  You can thank Conti for that.

We've modified the code in a way that will prevent you from decrypting
it with their decryptor.

We've exfiltrated a significant amount of data including private emails,
financial information, contacts, etc.

Now, if you wish to contact us in order to save your files from permanent
encryption you can do so by emailing network_battalion_0065@riseup.net.

You have 3 days to establish contact. Failing to do so will result in
that data remaining permenantly encrypted.

While we have very little sympathy for the situation you find yourselves
in right now, we will honor our agreement to restore your files across
the affected environment once contact is established and payment is made.
Until that time we will take no action. Be aware that we have compromised
your entire network.

We're watching very closely.  Your President should not have commited war
crimes. If you're searching for someone to blame for your current situation
look no further than Vladimir Putin.
```

Ransom note for NB65 ransomware

Source: BleepingComputer

A representative for the NB65 hacking group told BleepingComputer that they based their encryptor on the first Conti source code leak but modified it for each victim so that existing decryptors would not work.

"It's been modified in a way that all versions of Conti's decryptor won't work. Each deployment generates a randomized key based off of a couple variables that we change for each target," NB65 told BleepingComputer.

"There's really no way to decrypt without making contact with us."

At this time, NB65 has not received any communications from their victims and told us that they were not expecting any.

As for NB65's reasons for attacking Russian organizations, we will let them speak for themselves.

> "After Bucha we elected to target certain companies, that may be civilian owned, but still would have an impact on Russias ability to operate normally. The Russian popular support for Putin's war crimes is overwhelming. From the very beginning we made it clear. We're supporting Ukraine. We will honor our word. When Russia ceases all hostilities in Ukraine and ends this ridiculous war NB65 will stop attacking Russian internet facing assets and companies.
>
> Until then, fuck em.
>
> We will not be hitting any targets outside of Russia. Groups like Conti and Sandworm, along with other Russian APTs have been hitting the west for years with ransomware, supply chain hits (Solarwinds or defense contractors)... We figured it was time for them to deal with that themselves."

NB65 further stated on Monday that they will never target organizations outside of Russia, and any ransom payments will be donated to Ukraine.

Update 4/11/22: Added updated about how ransoms would be used

Related Articles:

The Week in Ransomware - April 15th 2022 - Encrypting Russia

Conti ransomware shuts down operation, rebrands into smaller units

Costa Rica declares national emergency after Conti ransomware attacks

Hackers display “blood is on your hands" on Russian TV, take down RuTube

Microsoft says Russia hit Ukraine with hundreds of cyberattacks

- Conti
- Cyberattack
- NB65
- Ransomware
- Russia
- Source Code
- Ukraine

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.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: