REvil ransomware devs added a backdoor to cheat affiliates

bleepingcomputer.com/news/security/revil-ransomware-devs-added-a-backdoor-to-cheat-affiliates/

Ionut Ilascu

By
Ionut Ilascu

- September 23, 2021
- 02:26 AM
- 0

Cybercriminals are slowly realizing that the REvil ransomware operators may have been hijacking ransom negotiations, to cut affiliates out of payments.

By using a cryptographic scheme that allowed them to decrypt any systems locked by REvil ransomware, the operators left their partners out of the deal and stole the entire ransom.

Conversations about this practice started a while ago on underground forums, in posts from collaborators of the gang, and have been confirmed recently by security researchers and by malware developers.

REvil ransomware, also known as Sodinokibi, emerged in the first half of 2019 and built a reputation as a successor of the GandCrab ransomware-as-a-service (RaaS) operation.

The RaaS cybercriminal business model involves a developer, who creates the ransomware malware and sets up the infrastructure, and affiliates recruited to breach and encrypt victims. The proceedings are divided between the two parties with affiliates taking the larger cut (typically 70-80%).

Promoted by veterans of underground forums, the REvil gang developed a highly lucrative private operation that accepted only experienced network hackers.

REvil name goes down the drain

If the REvil operation started as an “honest” cybercriminal endeavor, it soon switched to scamming affiliates out of the promised 70% share of a ransom from paying victims.

Yelisey Boguslavskiy, head of research at Advanced Intel, told BleepingComputer that since at least 2020 various actors on underground forums claimed that the RaaS operators were taking over negotiations with victims in secret chats, unbeknownst to affiliates.

The rumor became more frequent after the sudden shut down of DarkSide ransomware and Avaddon’s exit by releasing the decryption keys for their victims.

The conversations involved individuals that played a role in REvil ransomware attacks, such as partners that provided network access, penetration-testing services, VPN specialists, and potential affiliates.

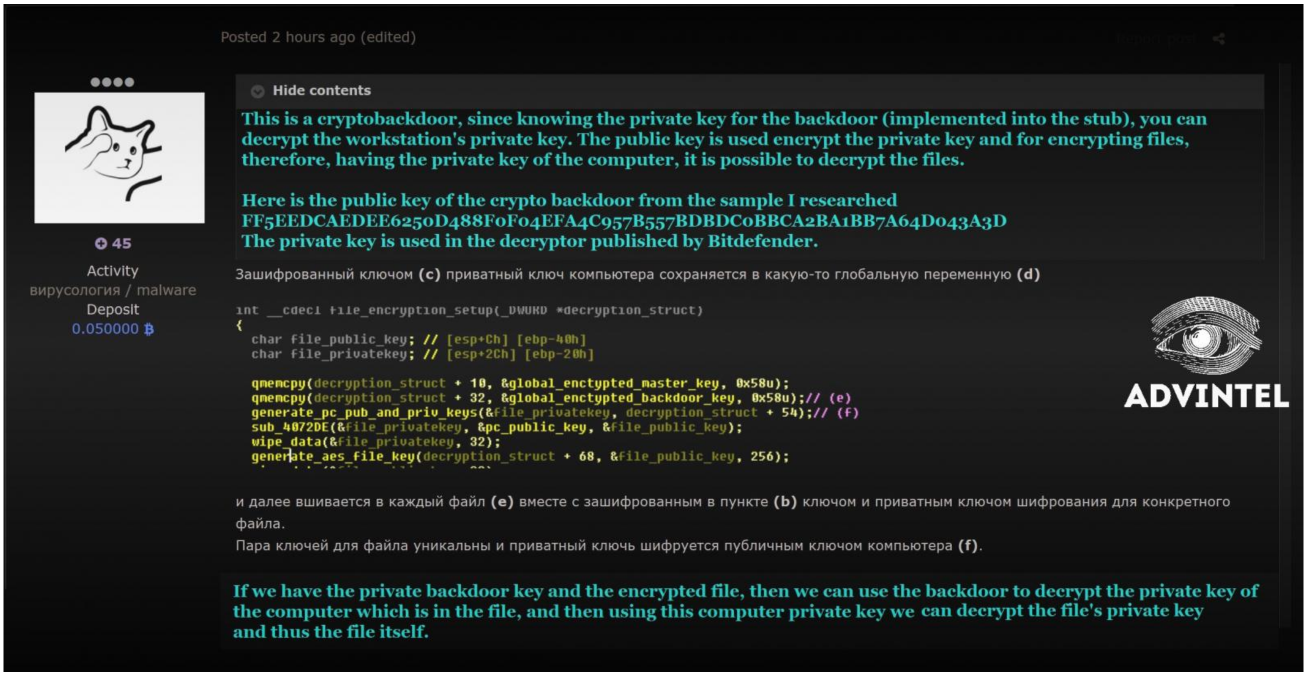
Boguslavskiy says that REvil admins reportedly opened a second chat, identical to the one used by their affiliate to negotiate a ransom with the victim.

When talks reached a critical point, REvil would take over by posing as the victim quitting the negotiations without paying the ransom, Boguslavskiy explained to BleepingComputer.

The gang would continue the talks with the victim and obtain the full ransom with the affiliate being none the wiser.

Recently, these claims got more substance as an underground malware reverse engineer provided evidence of REvil’s double-dipping practices. They talk of a “cryptobackdoor” in the REvil samples that RaaS operators gave affiliates to deploy on victim networks.

The author’s revelation comes after cybersecurity company Bitdefender released a universal REvil decryption tool that works for all victims encrypted up to July 13, 2021.


Posted 2 hours ago (edited)

This is a cryptobackdoor, since knowing the private key for the backdoor (implemented into the stub), you can decrypt the workstation's private key. The public key is used encrypt the private key and for encrypting files, therefore, having the private key of the computer, it is possible to decrypt the files.

Here is the public key of the crypto backdoor from the sample I researched
FF5EEDCAEDEE6250D488F0F04EFA4C957B557BDBDC0BBCA2BA1BB7A64D043A3D
The private key is used in the decryptor published by Bitdefender.

Зашифрованный ключом **(c)** приватный ключ компьютера сохраняется в какую-то глобальную переменную **(d)**

```
int __cdecl file_encryption_setup(_DWORD *decryption_struct)
{
  char file_public_key; // [esp+Ch] [ebp-40h]
  char file_privatekey; // [esp+2Ch] [ebp-20h]

  qmemcpy(decryption_struct + 10, &global_enctypted_master_key, 0x58u);
  qmemcpy(decryption_struct + 32, &global_enctypted_backdoor_key, 0x58u);// (e)
  generate_pc_pub_and_priv_keys(&file_privatekey, decryption_struct + 54);// (f)
  sub_4072DE(&file_privatekey, &pc_public_key, &file_public_key);
  wipe_data(&file_privatekey, 32);
  generate_aes_file_key(decryption_struct + 68, &file_public_key, 256);
```

и далее вшивается в каждый файл **(e)** вместе с зашифрованным в пункте **(b)** ключом и приватным ключом шифрования для конкретного файла.
Пара ключей для файла уникальны и приватный ключь шифруется публичным ключом компьютера **(f)**.

If we have the private backdoor key and the encrypted file, then we can use the backdoor to decrypt the private key of the computer which is in the file, and then using this computer private key we can decrypt the file's private key and thus the file itself.

source: Advanced Intel
Public key in the image above:

```
FF5EEDCAEDEE6250D488F0F04EFA4C957B557BDBDC0BBCA2BA1BB7A64D043A3D
```

What the author of the above post is saying is that affiliates were not the only ones that could decrypt the systems they locked with the REvil ransomware sample they received.

REvil operators had a master key they could use to restore encrypted files.

Researcher revealed the trick in July

Fabian Wosar, "ransomware slayer" par excellence and chief technology officer at Emsisoft, in early July provided a clear explanation for how REvil's cryptographic scheme worked.

GandCrab's successor uses in their malware four sets of public-private keys responsible for the encryption and decryption tasks:

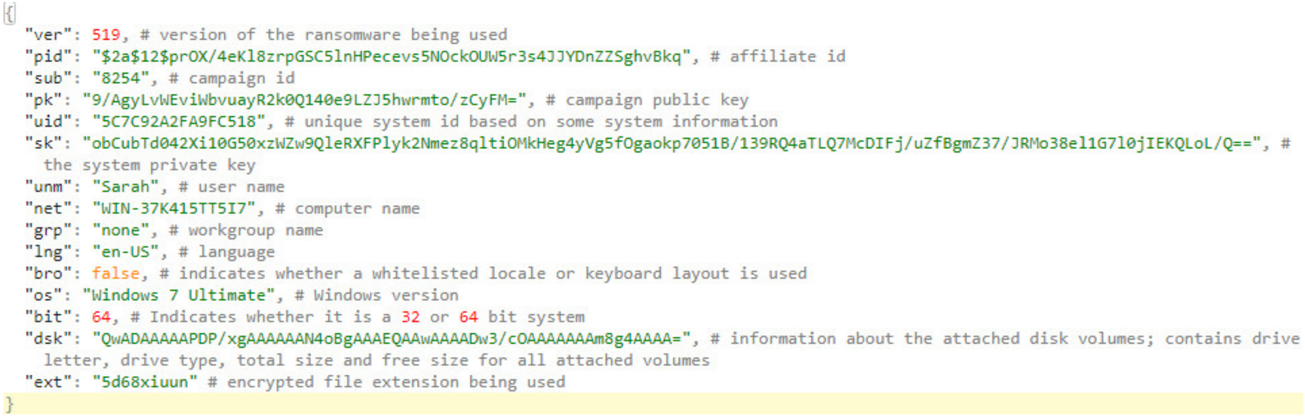
1. An operator/master pair that has the public part hardcoded in all REvil samples
2. A campaign pair, whose public part is stored in the configuration file of the malware as a PK value
3. A system-specific pair - generated upon encrypting the machine, with the private part encrypted using both the public master and campaign keys
4. A key pair generated for each encrypted file

"The private file key and public system key are then used as inputs for ECDH using Curve25519 in order to generate the Salsa20 key (called a shared secret) that is being used to actually encrypt the file content," Wosar explains.

The system private key is essential to unlocking a machine because it is the only one required to decrypt individual files. Recovering it is possible with either the master private key - available only to REvil operators, or the campaign key that affiliates have.

Wosar notes that the master private key is REvil's insurance against rogue affiliates, allowing them to decrypt any victim. This is also what Bitdefender used for their REvil decryption tool and likely what helped Kaseya victims recover files for free.

To access the REvil payment portal, the ransomware threat actor requires a blob of data present in the ransom note. That string of apparently nonsensical characters includes various data about the machine, campaign, version of the malware used, and the system private key.



```
{
  "ver": 519, # version of the ransomware being used
  "pid": "$2a$12$prOX/4eKl8zrpGSC5lnHPecevs5NOckOUW5r3s4JJYDnZZSghvBkq", # affiliate id
  "sub": "8254", # campaign id
  "pk": "9/AgyLvWEviWbvuayR2k0Q140e9LZJ5hwrmto/zCyFM=", # campaign public key
  "uid": "5C7C92A2FA9FC518", # unique system id based on some system information
  "sk": "obCubTd042Xi10G50xzWZw9QleRXFPlyk2Nmez8qltiOMkHeg4yVg5fOgaokp7051B/139RQ4aTLQ7McDIFj/uZfBgmZ37/JRMo38el1G7l0jIEKQLoL/Q==", #
    the system private key
  "unm": "Sarah", # user name
  "net": "WIN-37K415TT5I7", # computer name
  "grp": "none", # workgroup name
  "lng": "en-US", # language
  "bro": false, # indicates whether a whitelisted locale or keyboard layout is used
  "os": "Windows 7 Ultimate", # Windows version
  "bit": 64, # Indicates whether it is a 32 or 64 bit system
  "dsk": "QwADAAAAAPDP/xgAAAAAAN4oBgAAAEQAAwAAAADw3/cOAAAAAAAm8g4AAAA=", # information about the attached disk volumes; contains drive
    letter, drive type, total size and free size for all attached volumes
  "ext": "5d68xiuun" # encrypted file extension being used
}
```

source: Fabian Wosar

Keeping an ace up their sleeve that gives ransomware operators total control over decrypting any system locked by their malware is a practice seen with other, newer ransomware groups.

Boguslavskiy says that the DarkSide ransomware gang was rumored to run their operation in the same way.

After rebranding as BlackMatter, the actor was open about this practice, letting everybody know that they reserved their right to take over the negotiations at any point, without explaining.

Reverse engineer and Advanced Intelligence CEO Vitali Kremez told BleepingComputer that the latest REvil samples, which emerged when the gang restarted operations, no longer have the master key that enabled the decryption of any system locked with REvil ransomware.

Related Articles:

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

Conti, REvil, LockBit ransomware bugs exploited to block encryption

REvil ransomware returns: New malware sample confirms gang is back

REvil's TOR sites come alive to redirect to new ransomware operation

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

- Decryption Key
- Ransomware
- REvil
- Scam

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- 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: