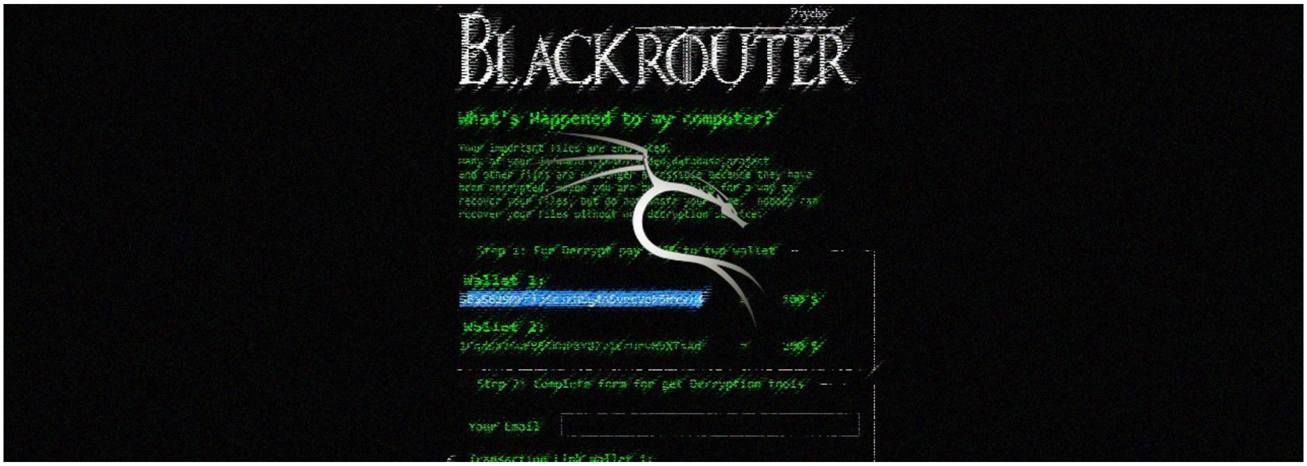
BlackRouter Ransomware Promoted as a RaaS by Iranian Developer

Lawrence Abrams

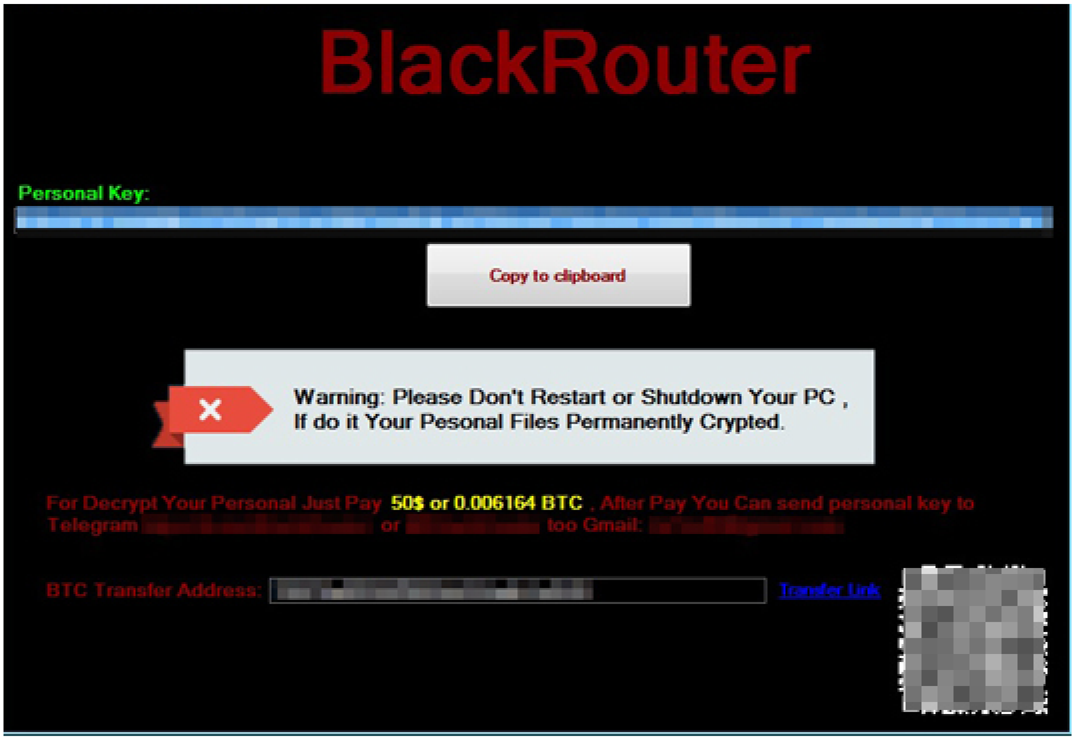
By
Lawrence Abrams

- January 17, 2019
- 05:48 PM
- 2



A ransomware called BlackRouter has been discovered being promoted as a Ransomware-as-a-Service on Telegram by an Iranian developer. This same actor previousl distributed another ransomware called Blackheart and promotes other infections such as a RAT.

BlackRouter was originally spotted in May 2018 and had its moment of fame when TrendMicro discovered it being dropped along with the AnyDesk remote access program and keyloggers on victim's computers.



BlackRouter

Personal Key:

[redacted]

Warning: Please Don't Restart or Shutdown Your PC ,
If do it Your Pesonal Files Permanently Crypted.

For Decrypt Your Personal Just Pay 50$ or 0.006164 BTC . After Pay You Can send personal key to
Telegram [redacted] or [redacted] too Gmail: [redacted]

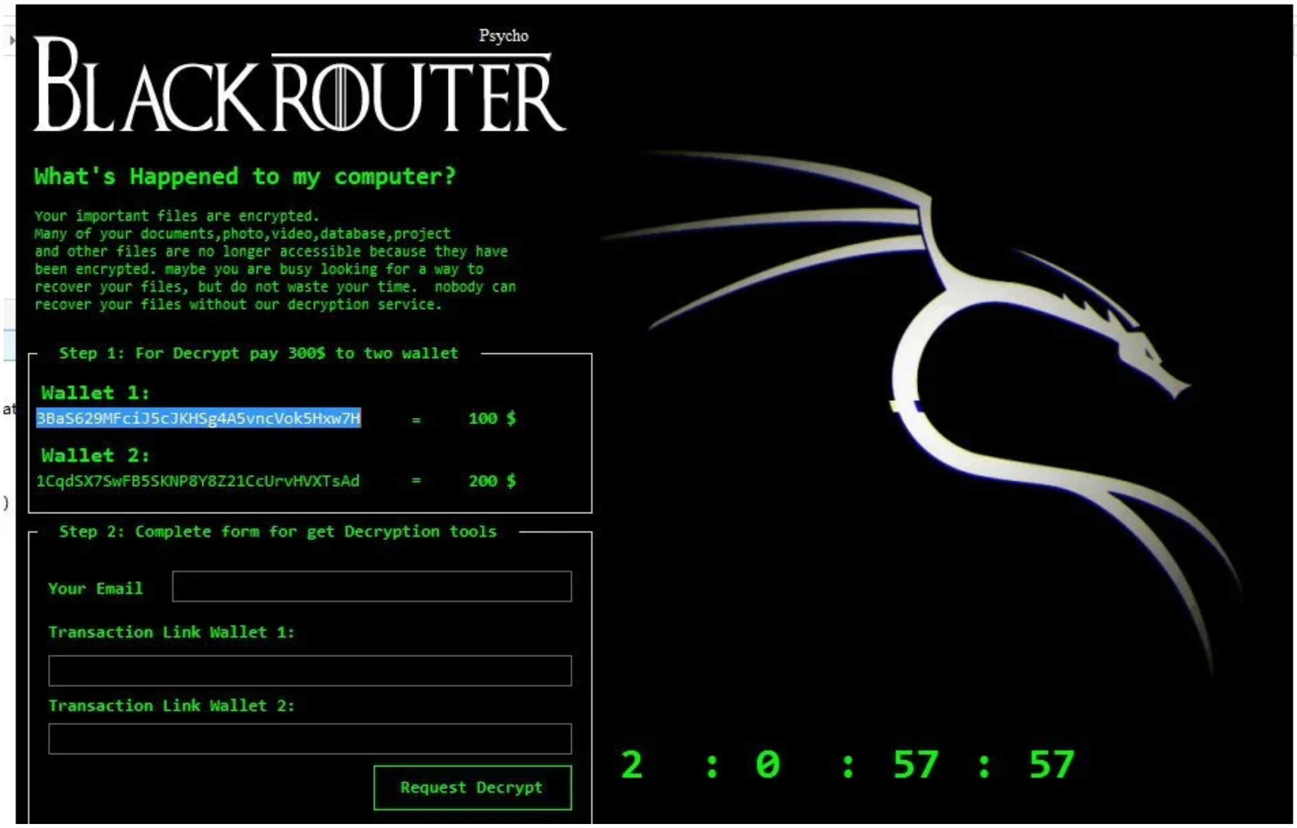
BTC Transfer Address: [redacted]

[redacted]

Original

BlackRouter/Blackheart Ransomware

In early January, a new version of the BlackRouter Ransomware was discovered by a security researcher named Petrovic, who shared the sample on Twitter. Furthermore, MalwareHunterTeam stated that this was basically the same as the previous variant, but with a better looking GUI and the addition of a timer.



Psycho

BLACKROUTER

What's Happened to my computer?

```
Your important files are encrypted.
Many of your documents,photo,video,database,project
and other files are no longer accessible because they have
been encrypted. maybe you are busy looking for a way to
recover your files, but do not waste your time.  nobody can
recover your files without our decryption service.
```

Step 1: For Decrypt pay 300$ to two wallet

Wallet 1:
3BaS629MFciJ5cJKHSg4A5vncVok5Hxw7H = 100 $

Wallet 2:
1CqdSX7SwFB5SKNP8Y8Z21CcUrvHVXTsAd = 200 $

Step 2: Complete form for get Decryption tools

Your Email

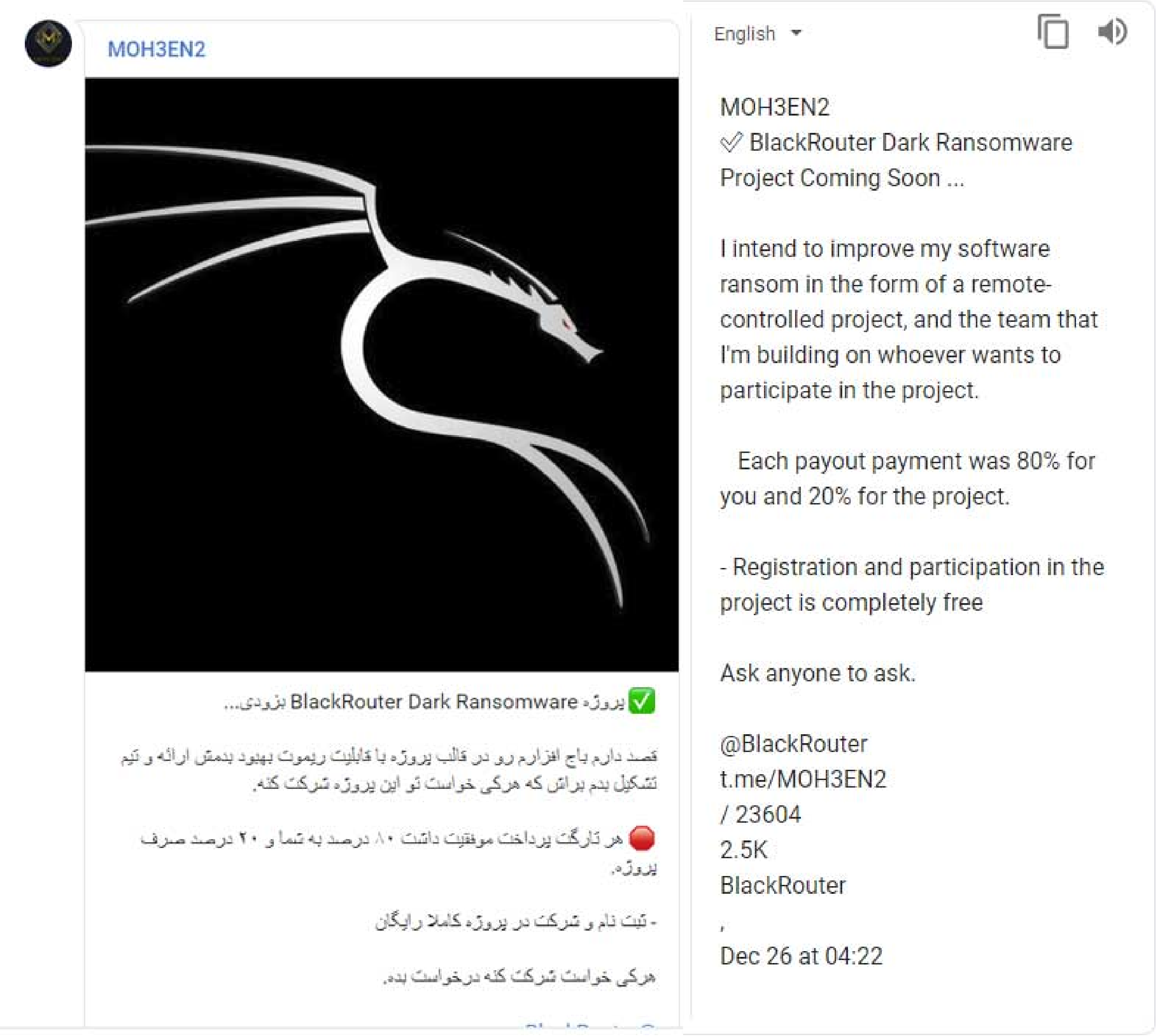
Transaction Link Wallet 1:

Transaction Link Wallet 2:

2 : 0 : 57 : 57

BlackRouter Ransomware GUI

Soon after BlackRouter was discovered, another security researcher named A Shadow told BleepingComputer that this ransomware was being promoted as a RaaS in a hacking channel on Telegram by an Iranian developer.



MOH3EN2

✅ پروژه BlackRouter Dark Ransomware بزودی...

قصد دارم باج افزارم رو در قالب پروژه با قابلیت ریموت بهبود بدمش ارائه و تیم تشکیل بدم براش که هرکی خواست تو این پروژه شرکت کنه.

🛑 هر تارگت پرداخت موفقیت داشت ۸۰ درصد به تما و ۲۰ درصد صرف پروژه.

- ثبت نام و شرکت در پروژه کاملا رایگان

هرکی خواست شرکت کنه درخواست بده.

MOH3EN2
✅ BlackRouter Dark Ransomware Project Coming Soon ...

I intend to improve my software ransom in the form of a remote-controlled project, and the team that I'm building on whoever wants to participate in the project.

Each payout payment was 80% for you and 20% for the project.

- Registration and participation in the project is completely free

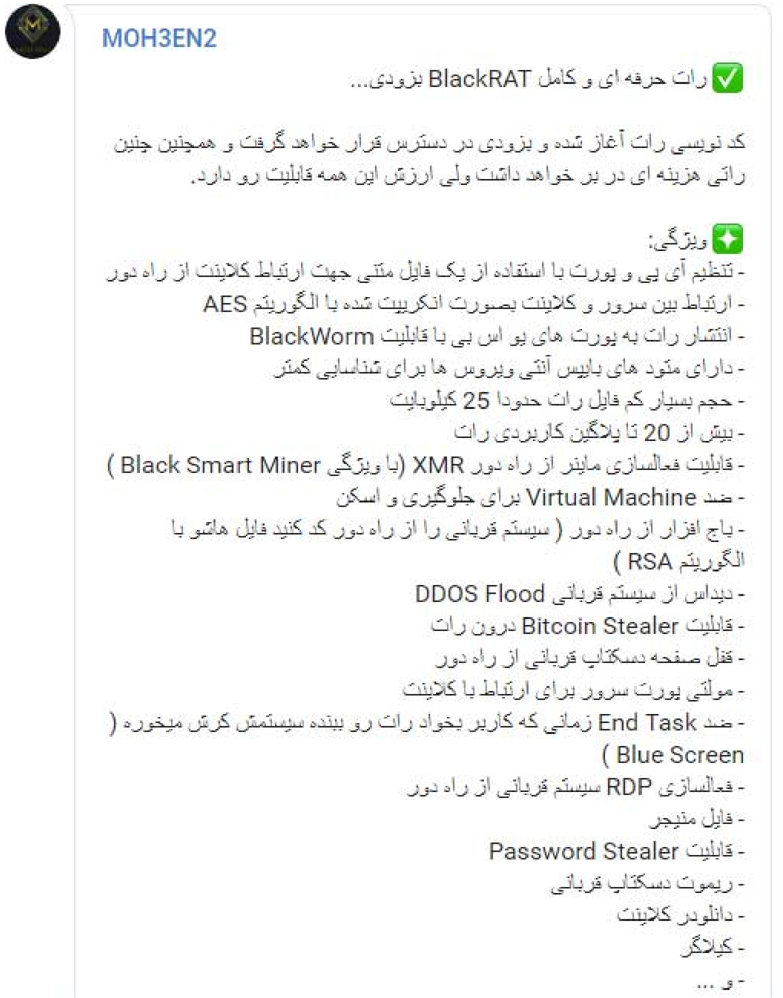
Ask anyone to ask.

@BlackRouter
t.me/MOH3EN2
/ 23604
2.5K
BlackRouter
,
Dec 26 at 04:22

BlackRouter Promotion on Telegram

Affiliates who join this RaaS and distribute the BlackRouter ransomware will earn 80% of any paid ransom payments, with the other 20% going to the BlackRouter developer.

In addition, this actor is promoting a remote access Trojan called BlackRat that allegedly includes features such as encrypted communications, AV evasion, small size, plugins, the ability to enable RDP, configure a miner, steal cryptocurrency wallets, keylogger, password-stealer, and more.



MOH3EN2

✅ رات حرفه ای و کامل BlackRAT بزودی...

کد نویسی رات آغاز شده و بزودی در دسترس قرار خواهد گرفت و همچنین چنین راتی هزینه ای در بر خواهد داشت ولی ارزش این همه قابلیت رو دارد.

✦ ویژگی:
- تنظیم آی پی و پورت با استفاده از یک فایل متنی جهت ارتباط کلاینت از راه دور
- ارتباط بین سرور و کلاینت بصورت انکریپت شده با الگوریتم AES
- انتشار رات به پورت های یو اس بی با قابلیت BlackWorm
- دارای متود های بایپس آنتی ویروس ها برای شناسایی کمتر
- حجم بسیار کم فایل رات حدودا 25 کیلوبایت
- بیش از 20 تا پلاگین کاربردی رات
- قابلیت فعالسازی ماینر از راه دور XMR (با ویژگی Black Smart Miner)
- ضد Virtual Machine برای جلوگیری و اسکن
- باج افزار از راه دور (سیستم قربانی را از راه دور کد کنید فایل هاشو با الگوریتم RSA)
- دیداس از سیستم قربانی DDOS Flood
- قابلیت Bitcoin Stealer درون رات
- قفل صفحه دسکتاپ قربانی از راه دور
- مولتی پورت سرور برای ارتباط با کلاینت
- ضد End Task زمانی که کاربر بخواد رات رو ببنده سیستمش کرش میخوره (Blue Screen
- فعالسازی RDP سیستم قربانی از راه دور
- فایل منیجر
- قابلیت Password Stealer
- ریموت دسکتاپ قربانی
- دانلودر کلاینت
- کیلاگر
- و ...

BlackRat Promotion

BlackRouter does not seem to be heavily distributed, with only one submission to ID Ransomware since December 31.

With that said, ransomware like BlackRouter is commonly distributed via hacking into Remote Desktop Services or through fake cracks and downloads. Therefore, make sure to not allow RDP to connect directly to the Internet and be sure to scan anything you download from an untrusted source.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

- BlackHeart
- BlackRouter

- Iran
- RaaS
- Ransomware
- Ransomware-as-a-Service

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

Comments

-
  achzone - 3 years ago
  -
  -

  I found this very interesting and enlightening. Thanks much for writing and sharing it!

  Regards, Andrew
-
  NoneRain - 3 years ago
  -
  -

  I agree! The articles here are always very well written and with contextual information that really adds to us.

You may also like: