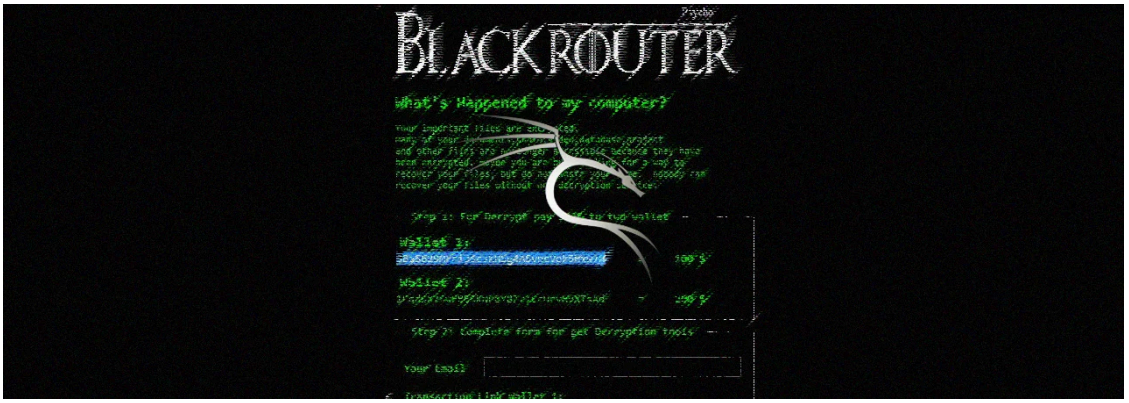
BlackRouter Ransomware Promoted as a RaaS by Iranian Developer

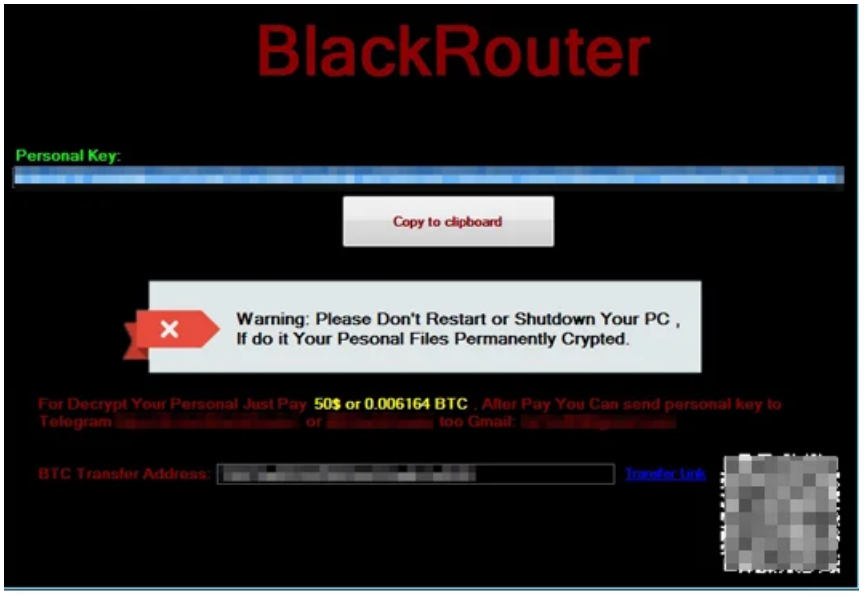
By Lawrence Abrams

Published: 2019-01-17 · Archived: 2026-04-05 21:49:17 UTC



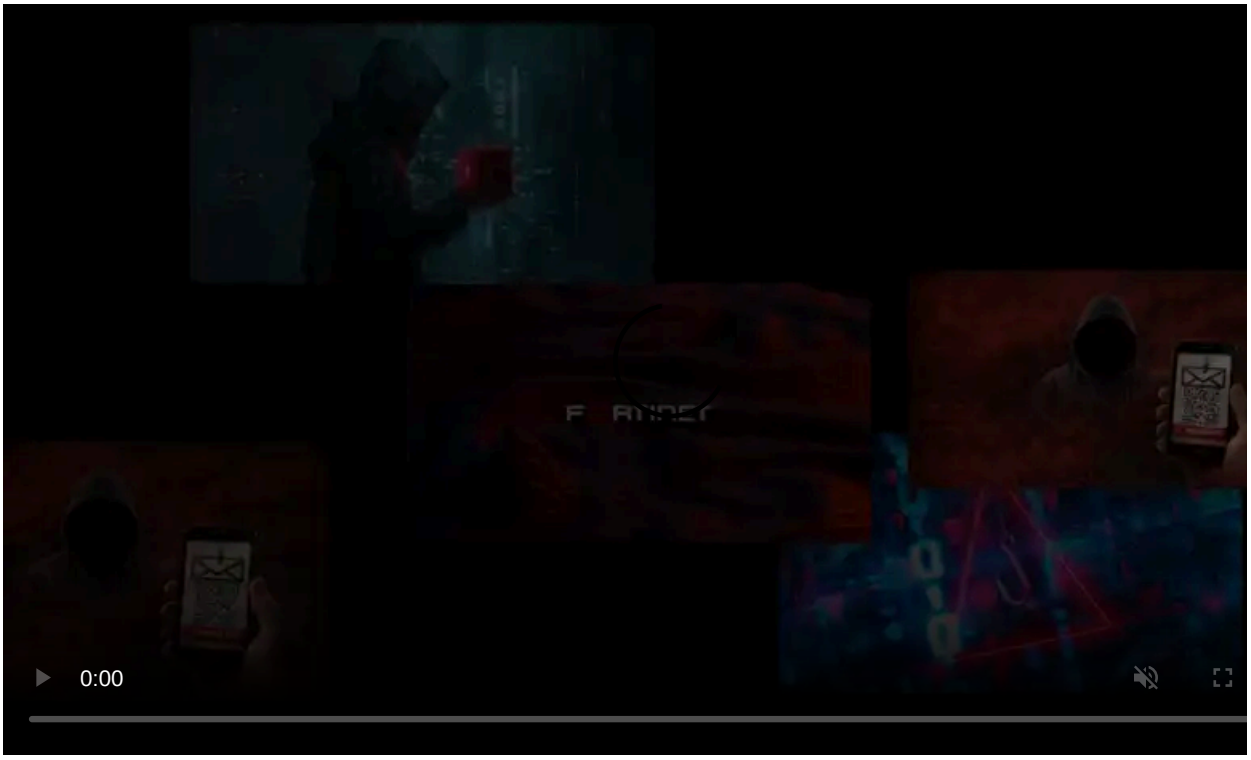
A ransomware called BlackRouter has been discovered being promoted as a Ransomware-as-a-Service on Telegram by an Iranian developer. This same actor previousl distributed another ransomware called Blackheart and promotes other infections such as a RAT.

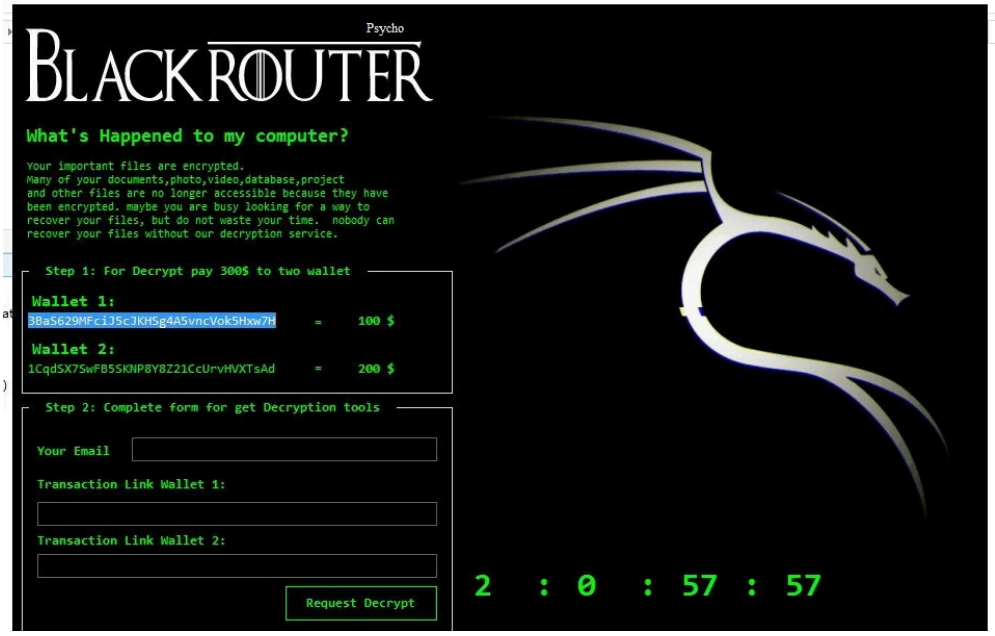
BlackRouter was originally spotted in May 2018 and had its moment of fame when TrendMicro discovered it being dropped along with the AnyDesk remote access program and keyloggers on victim's computers.



Original BlackRouter/Blackheart Ransomware

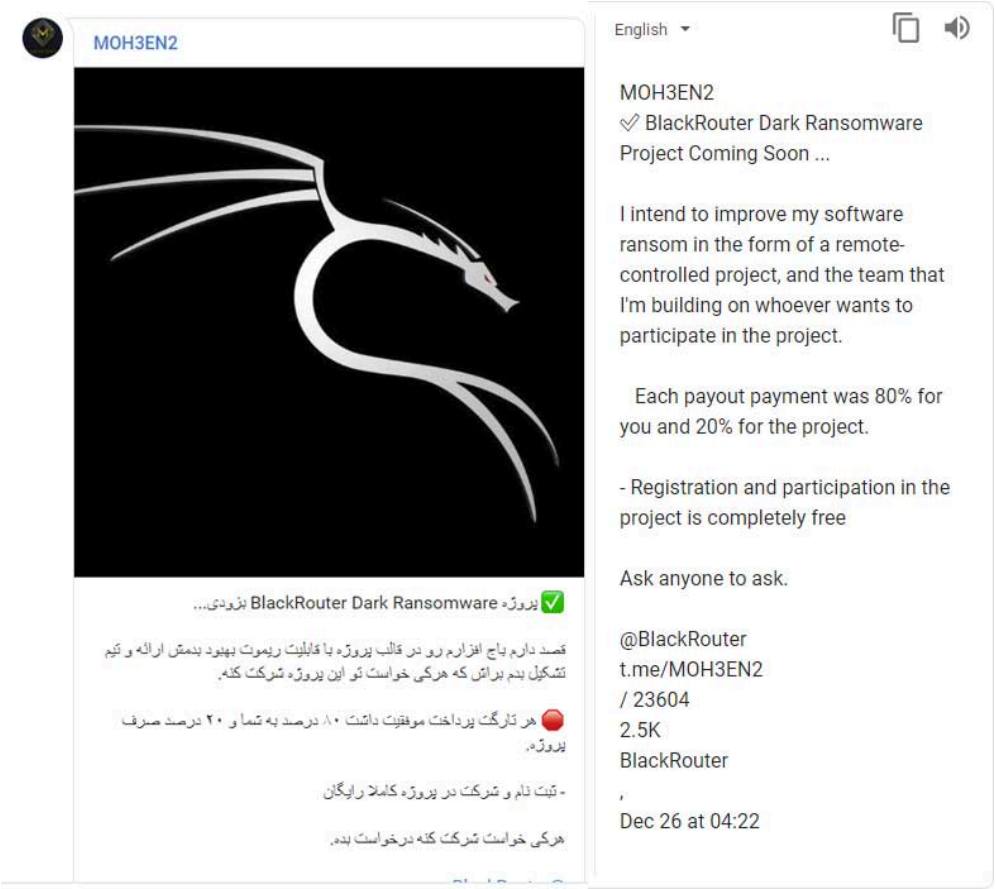
In early January, a new version of the BlackRouter Ransomware was discovered by a security researcher named Petrovic, who shared the sample on Twitter. Furthermore, MalwareHunterTeam stated that this was basically the same as the previous variant, but with a better looking GUI and the addition of a timer.


0:00



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.



BlackRouter Promotion on Telegram

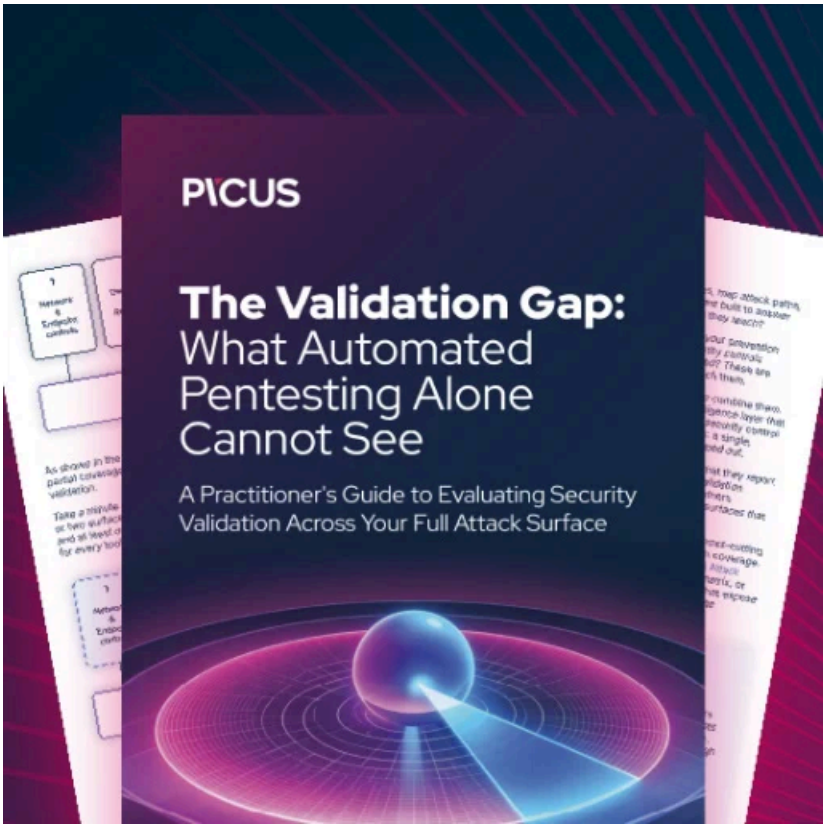
Affiliates who join this RaaS and distribute the BlackRouter ransomware will earn 80% of any paid ransom payments, with the other 20% going to the BlackRouter developer.

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.

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.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/blackrouter-ransomware-promoted-as-a-raas-by-iranian-developer/