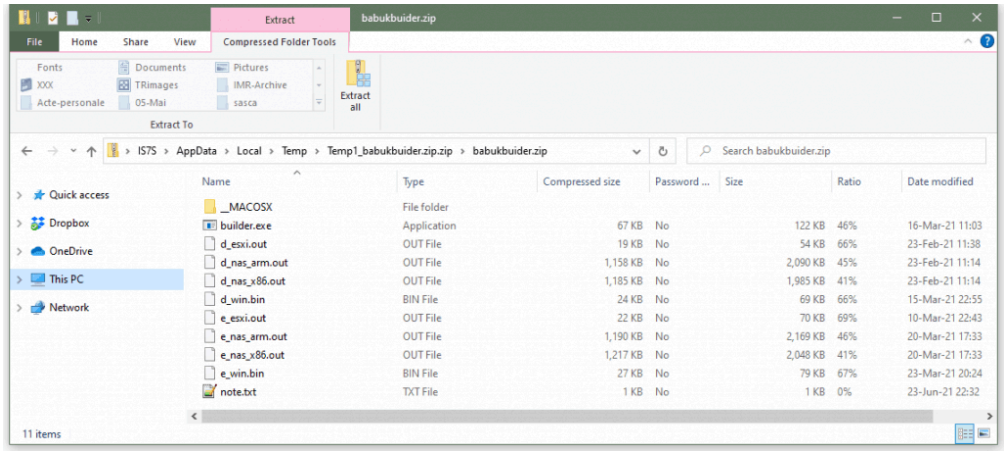
Builder for Babuk Locker ransomware leaked online

By Catalin Cimpanu

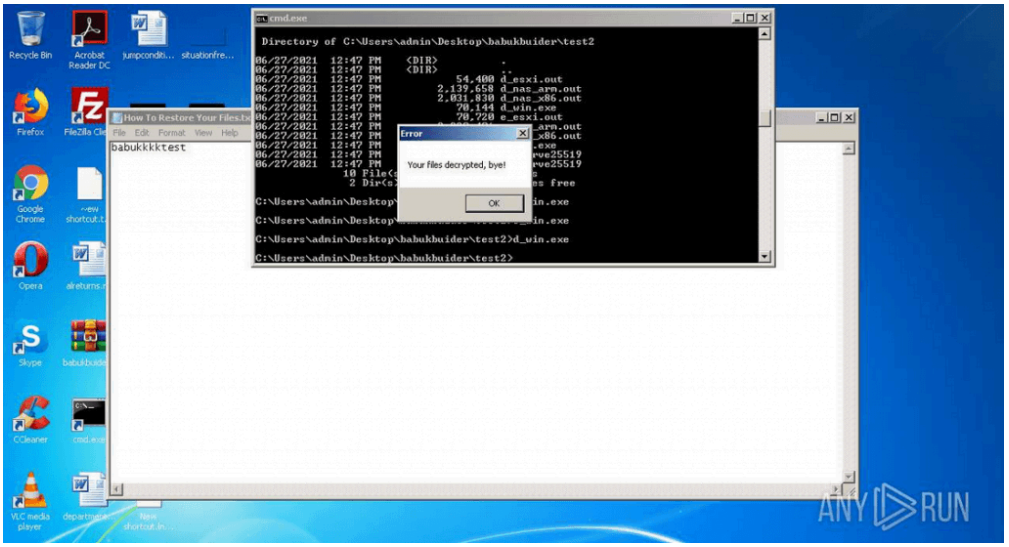
Published: 2022-12-17 · Archived: 2026-04-05 17:14:06 UTC

The builder for the Babuk Locker ransomware was leaked online this week, allowing easy access to an advanced ransomware strain to any would-be criminal group looking to get into the ransomware scene with little to no development effort.

According to a copy of the leak, obtained and tested by *The Record*, the Babuk Locker "builder" can be used to create custom versions of the Babuk Locker ransomware that can be used to encrypt files hosted on Windows systems, ARM-based network storage attached (NAS) devices, and VMWare ESXi servers.



Further, for every Babuk encrypter generated through the app, the builder also generates decrypters that can be used to recover the encrypted files from each victim.



The leak of the Babuk Locker builder comes two months after the Babuk Locker ransomware gang announced that it was retiring from ransomware operations after a high-profile attack on the Washington, DC police

department in late April.

The gang is believed to have followed through on its retirement plans in late May when it rebranded its ransomware leak site into **Payload.bin** and started operating as a third-patry host for other ransomware gangs that wanted to leak files from victims but did not want to operate their own leak site.

At the time of writing, it is unclear if the Babuk gang tried to sell their ransomware builder to a third party in a transaction that went bad, or if the builder was leaked by a rival or a white-hat security researcher.

But whatever happened behind the scenes, the gang's builder leaked online earlier this week when it was uploaded on the VirusTotal malware scanning portal.

The file was discovered earlier today by British security researcher Kevin Beaumont, who shared a copy with *The Record* for reporting purposes.

The Babuk builder leak also comes two weeks after the source code of the Paradise ransomware builder was also shared on a public hacking forum.

While the two incidents are believed to be unrelated, both are a cause of concern for cybersecurity experts, who believe low-effort cybercrime gangs will now adopt the two tools for future, and potentially very clumsy (destructive) attacks.

"Hopefully this can be used to drive research on detection and decryption," Beaumont said earlier today in a tweet.

A good starting point to improving detection would be to understand how the Babuk strain works, a process that was detailed in great technical depth in this 73-page Capgemini report [PDF].

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
