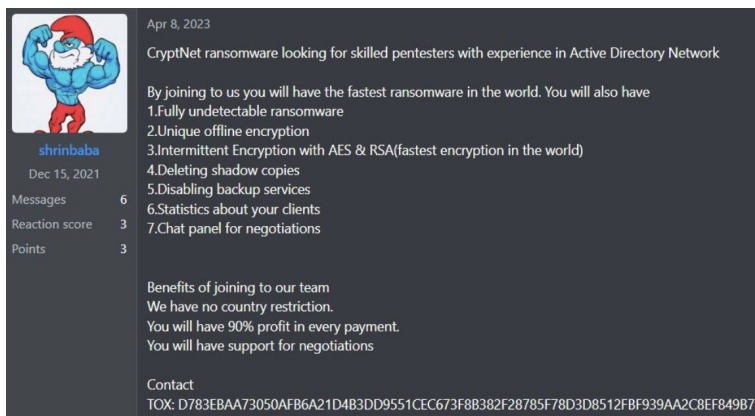


May 10, 2023

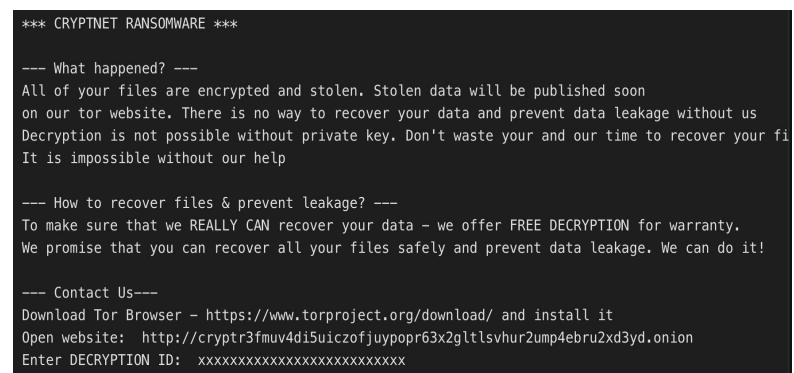
F-2023-05-10a

New CryptNet Ransomware-as-a-Service Announced on RAMP

- ZeroFox Intelligence has observed a new ransomware-as-a-service (RaaS) on Russian language deep and dark web (DDW) forum RAMP. On April 8, 2023, threat actor “shrinbaba” posted an advertisement seeking pentesters to work for their new RaaS, dubbed “CryptNet.”
- CryptNet is marketed as fast and fully undetectable with various capabilities and features, such as the ability to delete shadow copies and disable backup services, offline encryption, and a chat panel for negotiations.
- The advertisement states that CryptNet will offer its affiliates a 90 percent profit share from each successful attack. This represents one of the highest shares seen within the RaaS market, with affiliates typically receiving between 60 to 80 percent from most groups. CryptNet will allegedly provide support during ransom negotiations.
- While the original post states there are no restrictions on countries that can be targeted, after questioning from another forum member, this claim was subsequently deleted from the original post. This is very likely due to the original implication that Russia could be targeted, which is typically prohibited on Russian DDW forums.
- **ZeroFox Intelligence assesses that CryptNet is likely to become a notable player within the RaaS ecosystem. “Shrinbaba” is assessed to be credible threat actor, and the strain’s alleged advanced capabilities and attractive profit share offering will likely swiftly attract affiliates. CryptNet has become operational, with two victims identified to date—both in late April 2023.**



Source: ZeroFox Intelligence



Source:

[hXXps://research.openanalysis\[.\]net/dotnet/cryptnet/ransomw
are/2023/04/20/cryptnet.html](https://research.openanalysis[.]net/dotnet/cryptnet/ransomware/2023/04/20/cryptnet.html)

Recommendations

- Regularly back up critical data, including password-protected backup copies kept offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, or the cloud).
- Ensure proper network segmentation.
- Enable multi-factor authentication wherever possible.
- Disable PowerShell wherever possible to limit the possibility of operators employing lateral movement modules.

SCOPE NOTE ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 9:00 AM (EDT) on May 10, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.