Black Basta Ransomware Emerging From Underground to Attack Corporate Networks

gbhackers.com/black-basta-ransomware/

June 28, 2022

Two months have passed since the Black Basta Ransomware first surfaced. Nearly 50 victims have already been reported from the following countries:-

- The U.S.
- Canada
- The U.K.
- Australia
- New Zealand

This ransomware is a ransomware-as-a-service, which means that you can contract the malware and use it for a fee.

Industries Targeted

The Cybereason security experts claimed that Black Basta ransomware is observed to target industries across a wide range, and here they are mentioned below:-

- Manufacturing
- Construction
- Transportation

- Telcos
- Pharmaceuticals
- Cosmetics
- Plumbing
- Heating
- Automobile dealers
- Undergarments manufacturers

The threat actors who are behind Black Basta ransomware are known for extorting sensitive information from their victims in order to run their operations.

The operators of the ransomware start blackmailing people with threats of publishing stolen information online, and then it demands a digital payment to free up their data.

Key highlights of Black Basta

Ransomware attacks are a rapidly evolving problem worldwide due to advancing technology and the digitalization of society. While the very first ransomware attack occurred back in 1989.

The Black Basta exploits Qakbot to gain access to devices and move from one device to another collecting information from them.

Here below we have mentioned all the key highlights of Black Basta:-

- Prominent Threat
- Targets VMware ESXi
- High Severity
- Targeting English-speaking countries
- Targeting a Wide Range of Industries
- Human Operated Attack
- Detected and Prevented

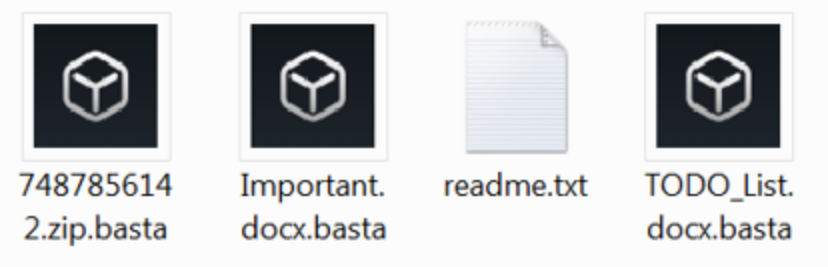
There have been some theories regarding the origins of this ransomware, considering the speed at which it has risen to prominence. In some cases, people have speculated that this ransomware may be related to Conti; however, that has not been confirmed yet.

Attack flow

After infecting the target network the ransomware performs the following actions:-

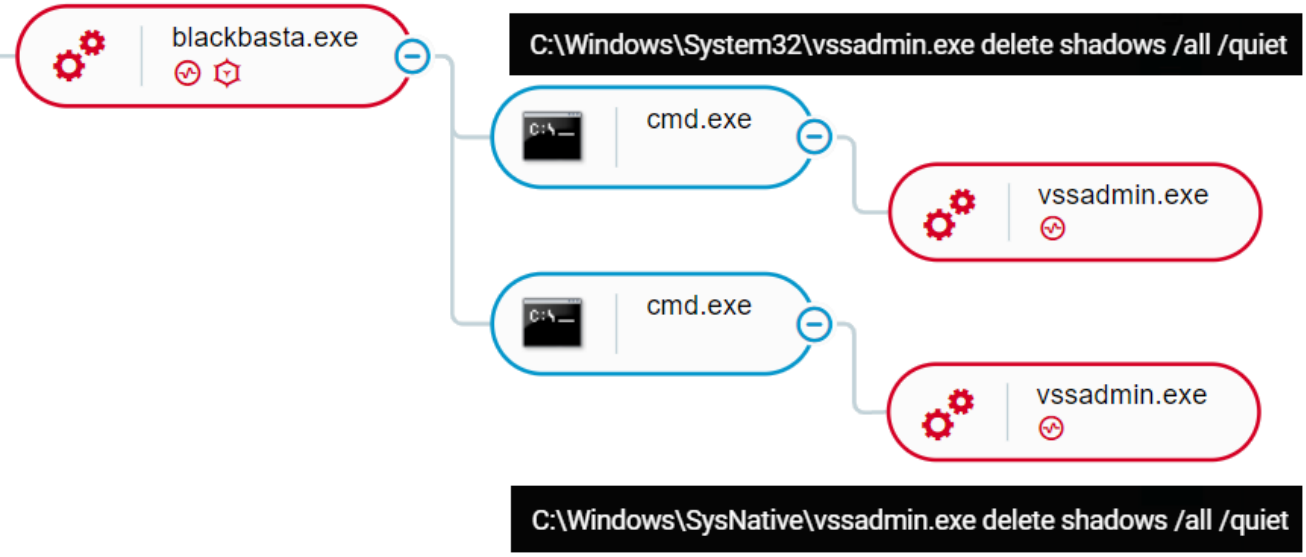
- Reconnaissance
- Collect data
- Credentials
- Move laterally
- Download payloads
- Execute payloads

In order to gain access to the Domain Controller, the attacker needs to harvest the credentials as well as understand the network structure and then using PsExec traverse to the next computer.



In the case of a successful breach, the attacker will perform a final procedure aimed at avoiding detection in order to hide their illicit activities.

Moreover, before encrypting files themselves, ransomware typically deletes shadow copies of files and other backups using VSSadmin.exe. At the end of the attack, the ransomware is deployed to the targeted endpoints, and this completes the final stage of the attack.



Recommendations

Here below we have mentioned all the security recommendations:-

- Enable the Anti-Ransomware Feature on AV tools that you have installed.
- Enable Anti-Malware Feature on AV tools that you have installed.
- Update your systems regularly to keep them in good working order
- Make sure your systems are fully patched
- Maintain regular backups of your files on a remote server
- Implement robust security solutions to stay secure.

Leave a Reply