REVE™
antivirus
Secured Digital Experience

Best Practices to Prevent Ransomware

REVE
antivirus

EndpOint SECURITY

Giving you complete control
of your office network &
DIGITAL SECURITY

REVE Antivirus

Ransomware

Ransomware is a type of malware that prevents the access of system or files and demands ransom in order to access system or files.

It is a malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Data Encryption/Decryption Process

1. **Attacker** → **Victim**

   The attacker generates a key pair and places the corresponding public key in the malware. The malware is released.

2. **Victim** → **Attacker**

   To carry out the cryptoviral extortion attack, the malware generates a random symmetric key and encrypts the victim's data with it. It uses the public key in the malware to encrypt the symmetric key. This is known as hybrid encryption and it results in a small asymmetric ciphertext as well as the symmetric ciphertext of the victim's data. It zeroizes the symmetric key and the original plaintext data to prevent recovery. It puts up a message to the user that includes the asymmetric ciphertext and how to pay the ransom. The victim sends the asymmetric ciphertext and e-money to the attacker.

3. **Attacker** → **Victim**

   The attacker receives the payment, deciphers the asymmetric ciphertext with the attacker's private key, and sends the symmetric key to the victim. The victim deciphers the encrypted data with the needed symmetric key thereby completing the cryptovirology attack.

The symmetric key is randomly generated and will not assist other victims. At no point is the attacker's private key is exposed to victims and the victim need only to send a very small ciphertext (the encrypted symmetric-cipher key) to the attacker.

Prevention Steps

(i) Do not open and download any suspicious attachments through email.
(ii) Keep Antivirus software up to date.
(iii) Make sure all protection of Antivirus is turned ON and system is in "Secure mode".
(iv) Avoid pop-ups and fake notifications which offers eye-catching deals etc.
(v) In network, use password protected sharing rather than using simple file sharing.
(vi) If it is not highly required, avoid using network shared drive and keep disable Remote Desktop Protocol (RDP).
(vii) Keep backup of your important data and backup it on regular basis.
(viii) Disable Macros from MS Office application if not required.
(ix) Keep all your operating system and software patched up with latest available patches.
(x) Do not uses pirated software as they become source of infection.
(xi) Microsoft vulnerability patch (ms010-17) must be installed on operating systems.
https://docs.microsoft.com/enus/securityupdates/securitybulletins/2017/ms17-010

REVE Antivirus Configuration

(i) Check REVE Antivirus validity and signature update with priority.
(ii) Configure REVE AV firewall to block below ports
135 - RPC Endpoint Mapper
137 - (CIFS) Common Internet File Service
139 - NetBIOS
445 - SMB
(iii) Run complete system scan with REVE AV.
(iv) Control/Block the fraud web site, using REVE web security
(v) Turn on REVE Anti Ransomware feature to increase the protection level.
(vi) Configure REVE E-mail blacklisting policy for unknown email Ids.
(vii) Enable IPS/IDS from REVE Endpoint Security.
(viii) Take backup of Organization important data with REVE AV solution.

Special Note:

As Ransomware is, known for data encryption. Despite security software installed, lots of users/customers are affected with this malware due to open vulnerabilities and lack of user awareness, hence we strongly suggest to keep your important data backed-up, so that at the time of crises it can be restored for use.

REVE Endpoint security offers Network and Local Data backup solution in Antivirus. It has now become easy for an administrator to take the backup of his organization's important data by using REVE Endpoint security solution.