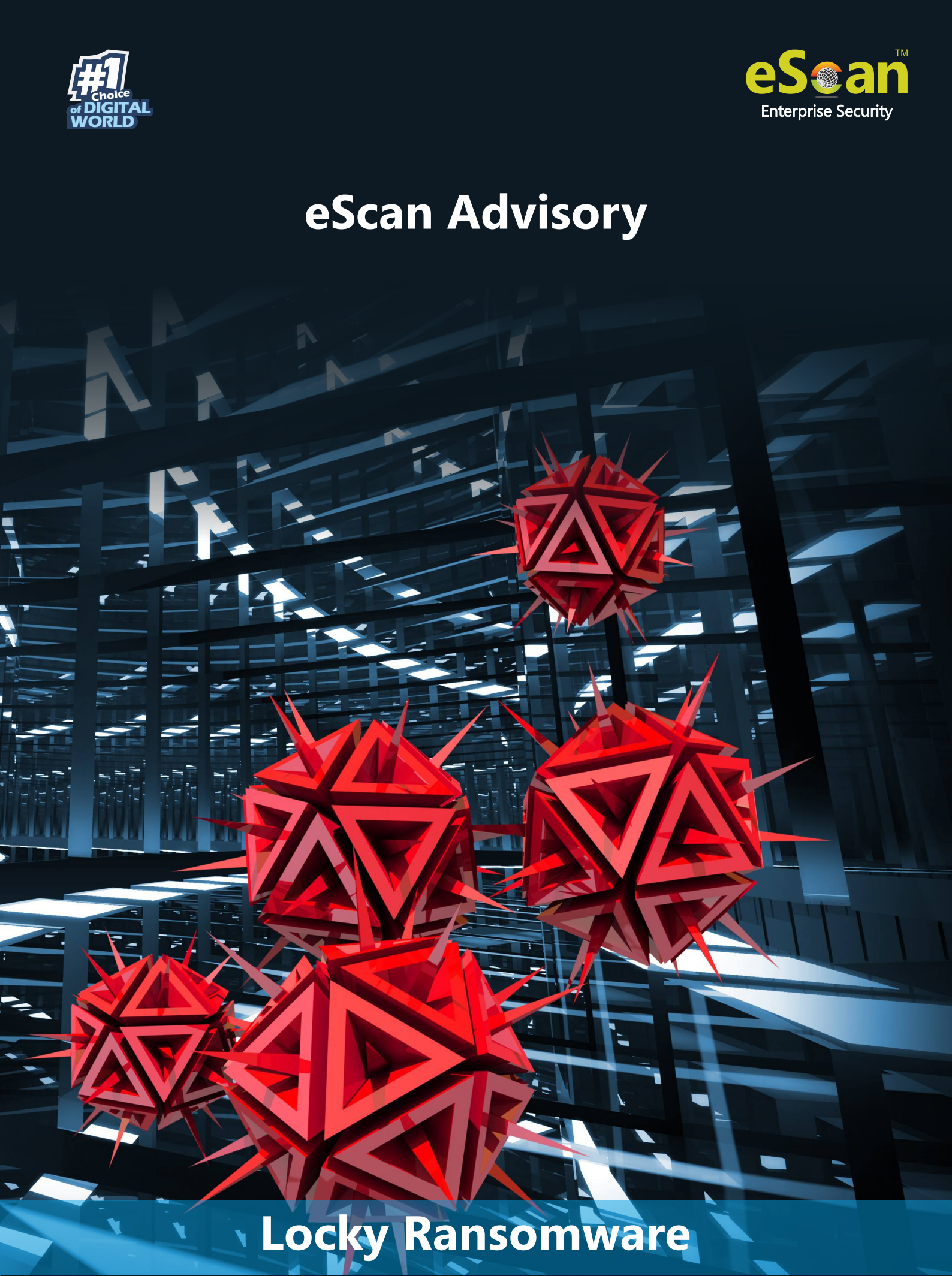
#1 Choice of DIGITAL WORLD

eScan™ Enterprise Security

eScan Advisory



Locky Ransomware

Version: eEA-1.0.0

www.escanav.com

This is a ransomware that comes to you via email. The purpose of these threats is to extort money from their victims with promises of restoring encrypted data. The ransomware encrypts files with the RSA-2048 algorithm and AES-128 ciphers and asks a ransom for decryption. This type of malware also comes as highly obfuscated JavaScript (file with .JS extension) inside an archive which is attached to a Spam Mail, usually pretending to be an official document. Opening of such an attachment is enough to get system compromised with Ransomware.

This virus can also spread via file sharing services and social networking sites, which may contain similar attachments and files which might be presented to you as useful or something required, like an update.

As the number of incidents of computer systems getting infected by this Ransomware is on the rise and almost all of the reported cases are from the Indian Sub-Continent, we at eScan are issuing an advisory so that further outbreak can be prevented.

The encrypted data **cannot** be decrypted or recovered, as the RSA keys are stored on a hidden server. Although, there are claims of paid alternatives but the success rate is minimal.

Do's and Dont's:

- If data's been encrypted by Ransomware, DO NOT PAY THE RANSOM!
- Isolate the affected system from your Network.
- Restore the encrypted files from the backup or from system restore point (if enabled).
- Install and Configure eScan with all security modules active.
    - eScan Real Time Monitoring.
    - eScan Proactive protection.
    - eScan Firewall IDS/IPS Intrusion prevention.
- Restrict user to access email only using Mail Client and block accessing of email via any browser.
- Don't enable macros in documents received as attachments via email.
- Do not open attachments if received from unsolicited source.
- Deploy and maintain a backup solution.
- And last, but most important, protection of Mail server at Gateway Level with Mailscan to prevent delivering of such suspicious emails

The information provided above will help you to protect your system from being victim of Ransomware.

How eScan protects your system from Ransomware:

Protection at Gateway Level:

MailScan at Gateway level scans all emails and detects attachments carrying Ransomware infection. This could be via suspicious executables, documents carrying suspicious macros or script files. All such attachments are blocked by MailScan before they are delivered to users Inbox.

Protection at Desktop/Server/Endpoint Level:

- If MailScan is not deployed on the gateway, eScan at desktop level also protects your system from getting compromised with Ransomware. If attachments related to Ransomware (MS Office files with Macros, MHTML files, ZIP/RAR with scripts, etc.) are opened via any email client, eScan Real Time Monitoring will block such access, thereby providing the first layer of protection.

- If a user is not using any email client, and accesses his emails via a browser, the second layer of protection is given by eScan Firewall. This monitors all incoming and outgoing traffic and blocks download of ransomware malware executable via scripting tools.

- If eScan Firewall is not available on the system, the malware downloaded from remote server gets blocked on execution by eScan Proactive Monitor, the third layer of protection. This detects the behavior of downloaded malware and blocks it before it can start damaging your system.

The above protection layers provided by eScan protect your system not only from Ransomware but from various similar threats trying to destroy critical data.

To make user data more secure, eScan will soon launch an endpoint backup feature (currently available in its eScan Total Security Suite SOHO product) which will keep a backup of user's data, and will help a user to get back to last best state in the worst case scenario of the system getting compromised.

In case of any assistance, do write to us at ransom@escanav.com.