

Ransomware

ATTACK VECTORS, MITIGATION & KILL CHAIN OPPORTUNITIES

Sylint

What is Ransomware

Malicious software (malware) designed to encrypt local and network-based files and demand a ransom for decryption. Payment of the ransom is frequently requested in bitcoins (a relatively untraceable currency) via anonymous internet sites.

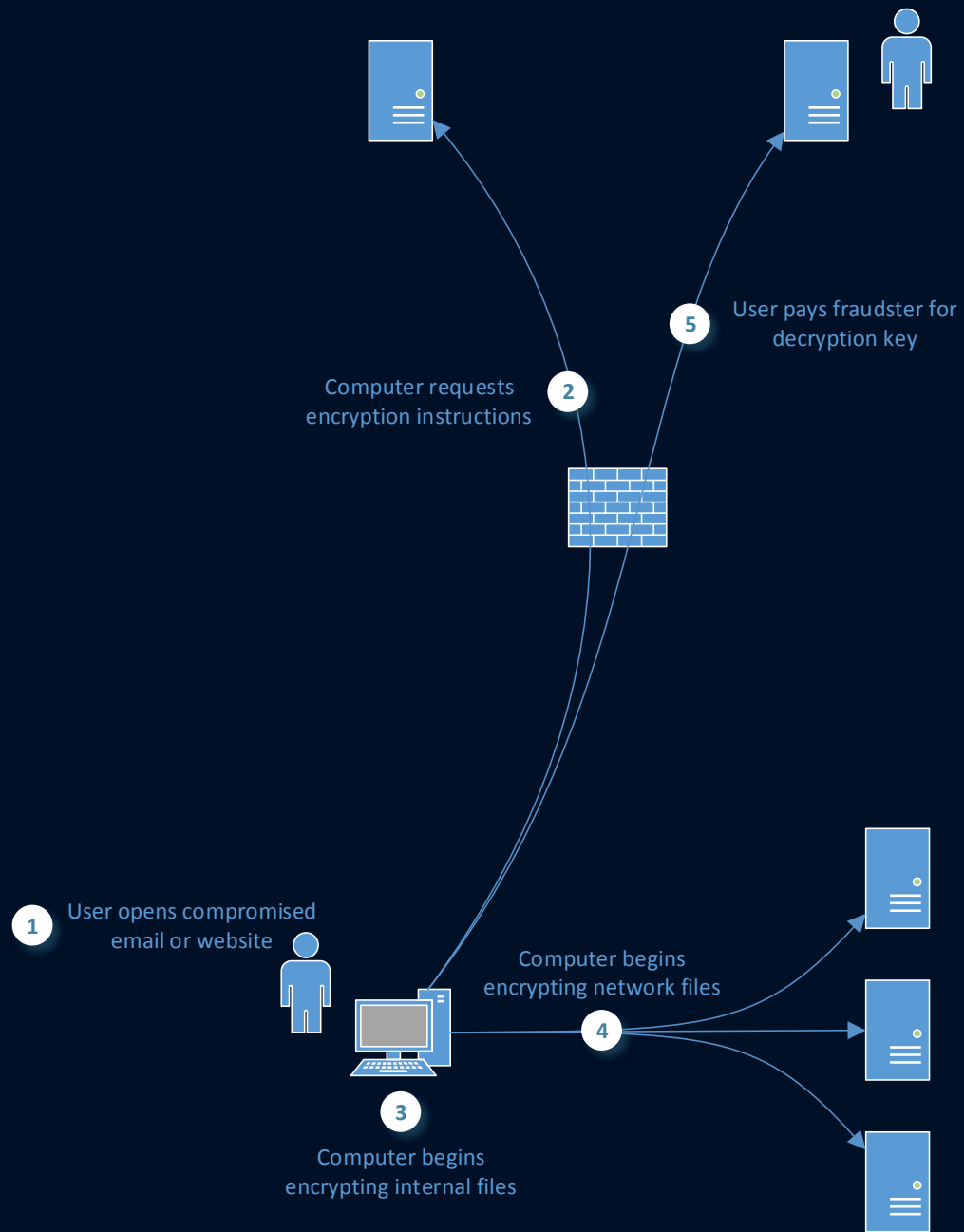
Encryption now commonly uses a public/private key pair to make brute-force decryption difficult or impossible.

Often only the first 2KB of the file is encrypted to increase speed

Attack Vectors

- Email
 - Attachments
 - Malicious links
- Web Browsing
 - Legitimate pages with Java-exploit in embedded advertisement
 - Malicious pages





Prepare

- Review mapped drives and file shares
 - Ensure only minimum network shares are made
 - Check folder permissions and avoid "Authorized User" and "Everyone" permissions
- Check backups of critical files
 - Confirm nightly backups (or more frequent) are running successfully
 - Ensure enough versions of backups exist to restore from more than "yesterday"



Prevent

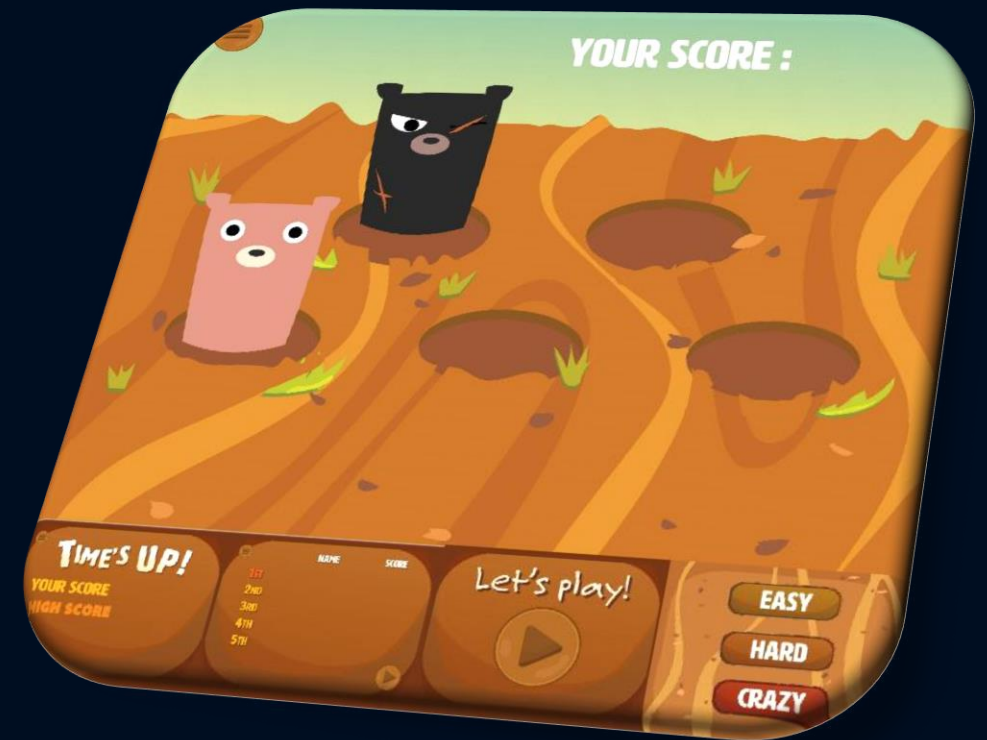
- Mail Gateways & Filters (e.g., ProofPoint)
 - Attachment controls
 - URL defense
- Web Proxies (e.g., Zscaler)
 - Malicious advertisements
 - Malicious pages
- Server Usage Habits
 - No web browsing
 - No mail checking



Disrupt

- Web Proxies (e.g., Zscaler)
 - Prevent exchange of encryption keys
- Application Whitelisting (e.g., Bit9)
 - Stop executable from running
- Process Monitoring (e.g., CarbonBlack)
 - Find new malicious processes
 - Identify suspiciously high network connections

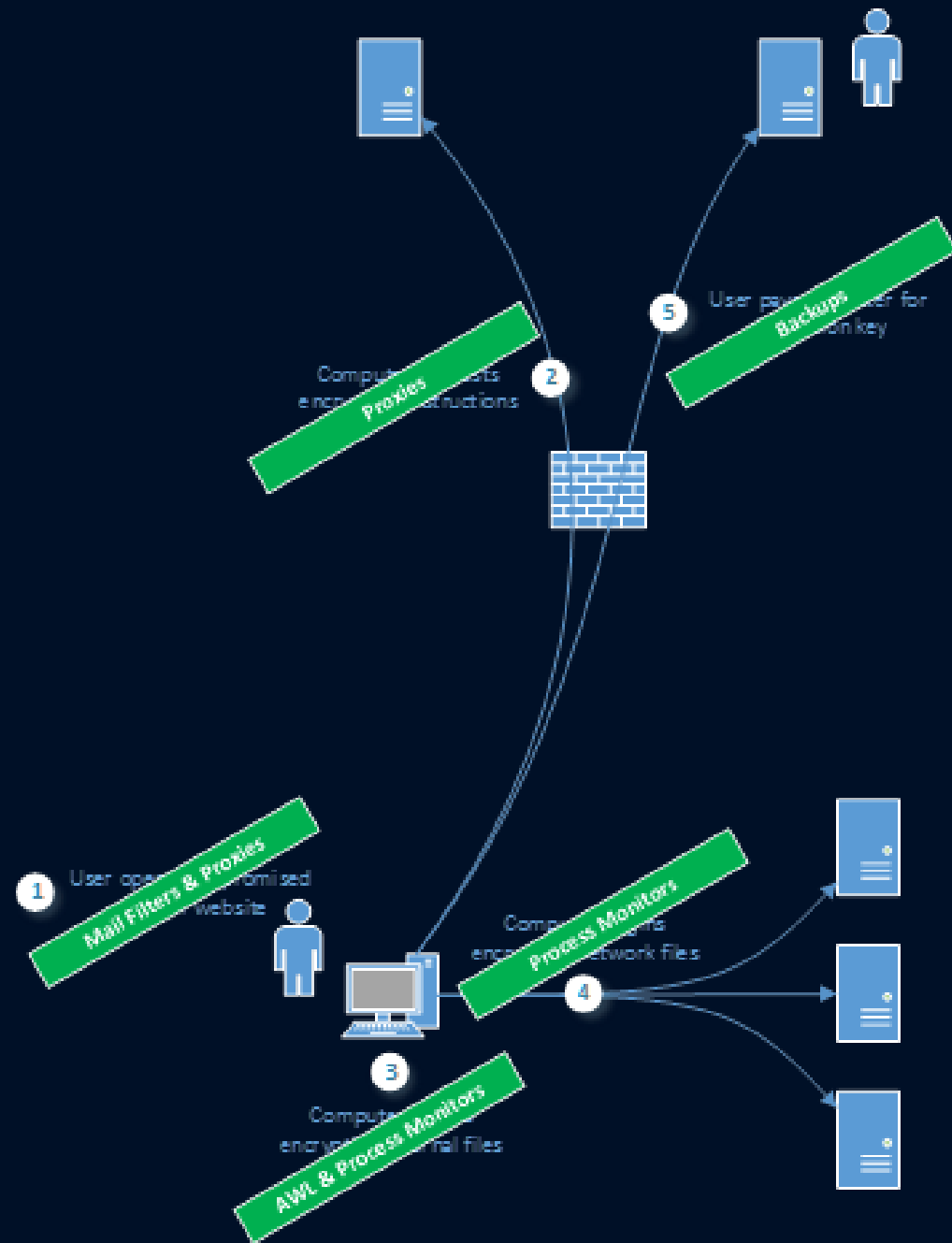
~~• Anti-Virus~~



Respond

- Active Attack
 - Unmount shared drives
 - Find the root cause
 - Check logs for users with high number of network connections
 - Check for ongoing, broad authentication/access requests
 - Confirm backups won't overwrite good data with bad
 - Engage Insurance, Legal and Cyber-Security teams
- Completed Attack
 - Find the root cause before bringing data back online
 - Determine if ransom payment will be necessary
 - Engage Insurance, Legal and Cyber-Security teams





Lauren Bicknese

RCM&D

lbicknese@rcmd.com

443.921.3811

Serge D. Jorgensen

Sylint Group, Inc.

sdj@usinfosec.com

941.951.6015

Sylint