IUG 2020
MINNEAPOLIS

Surviving Ransomware

Presented By - Nathan James

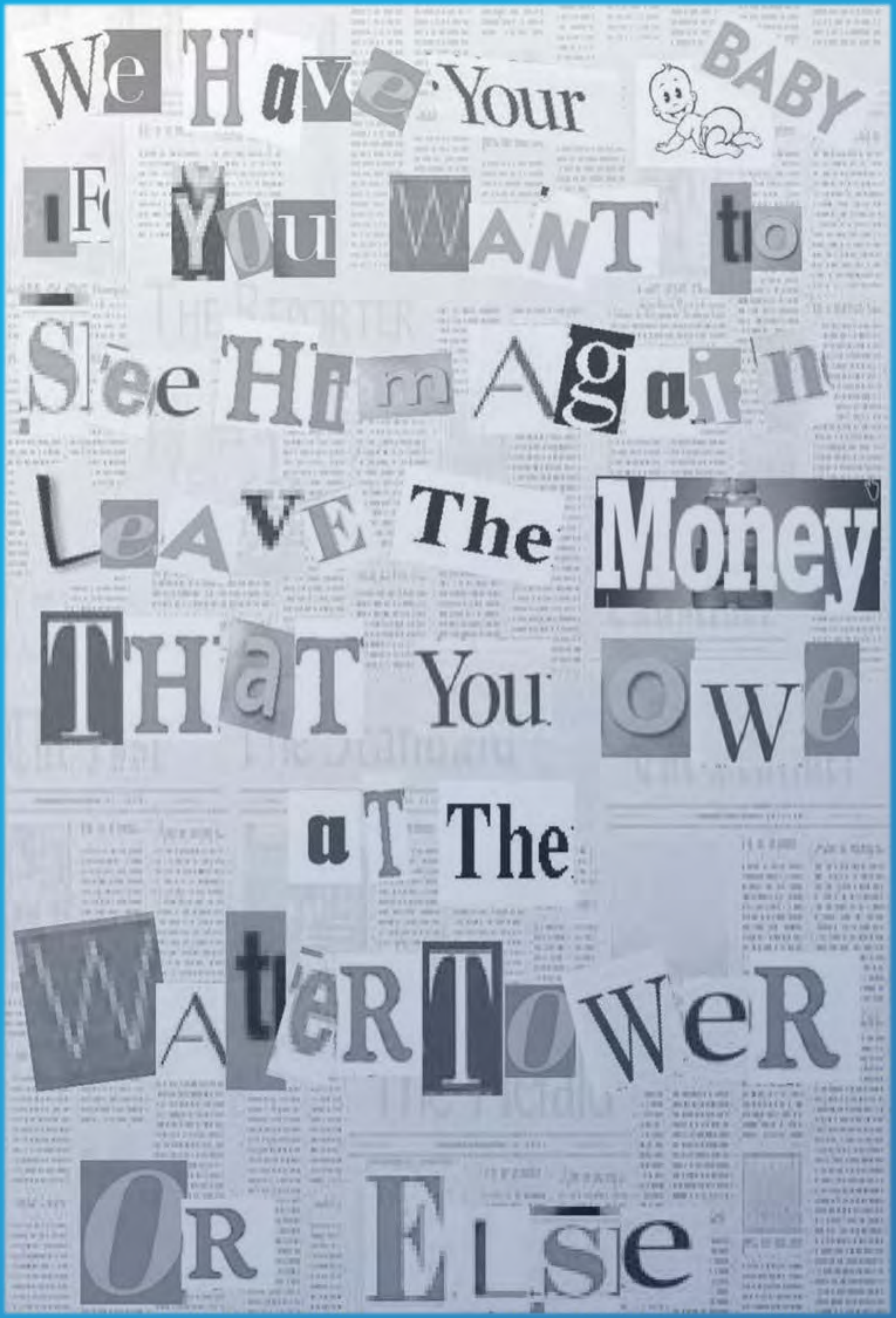
Pre-Conference • Wednesday, April 15th
Main Conference • Thursday, April 16th – Saturday, April 18th

AGENDA

- Ransomware 101
- Decisions: easy & difficult
- Protect yourself
- No more ransoms?

Chapter 1

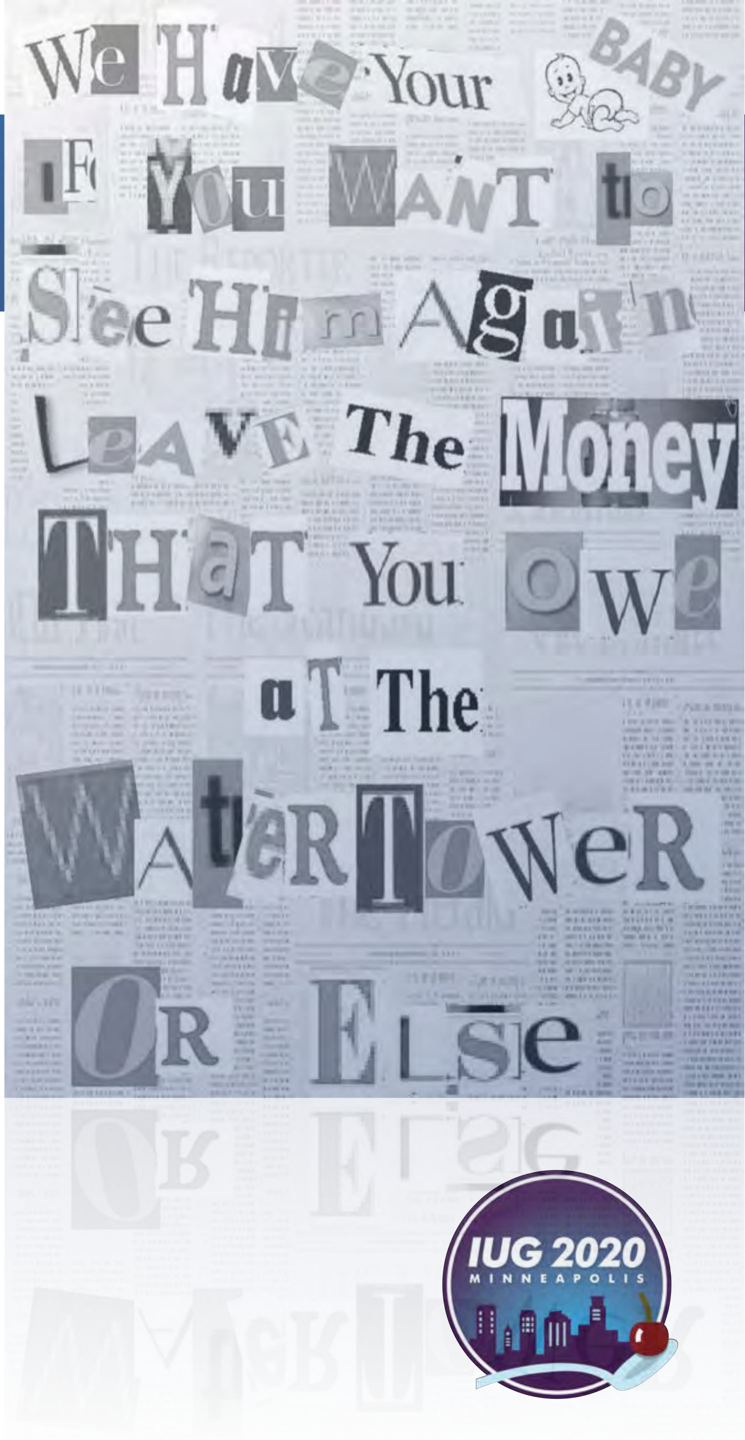
IT BEGAN AT BRUNCH



Ransomware 101

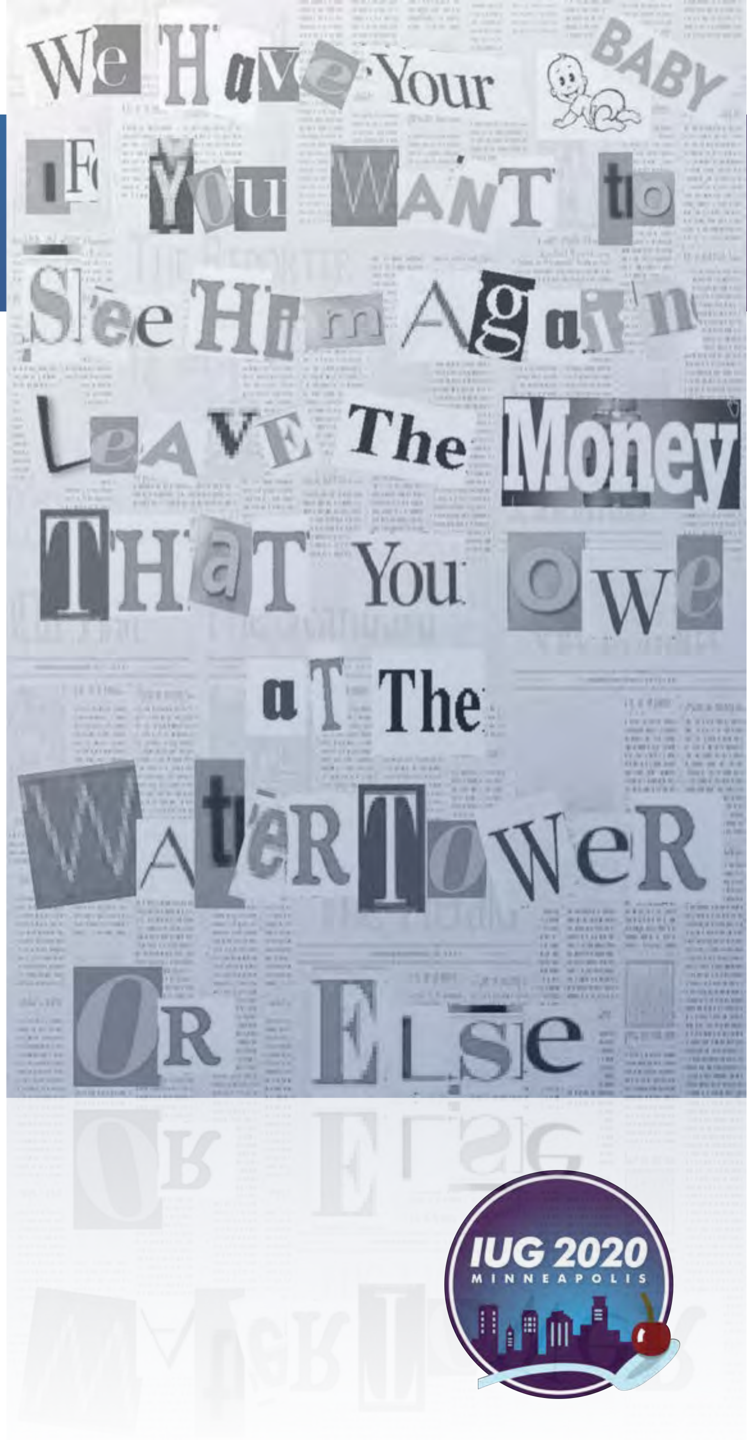
WHAT IS RANSOMWARE?

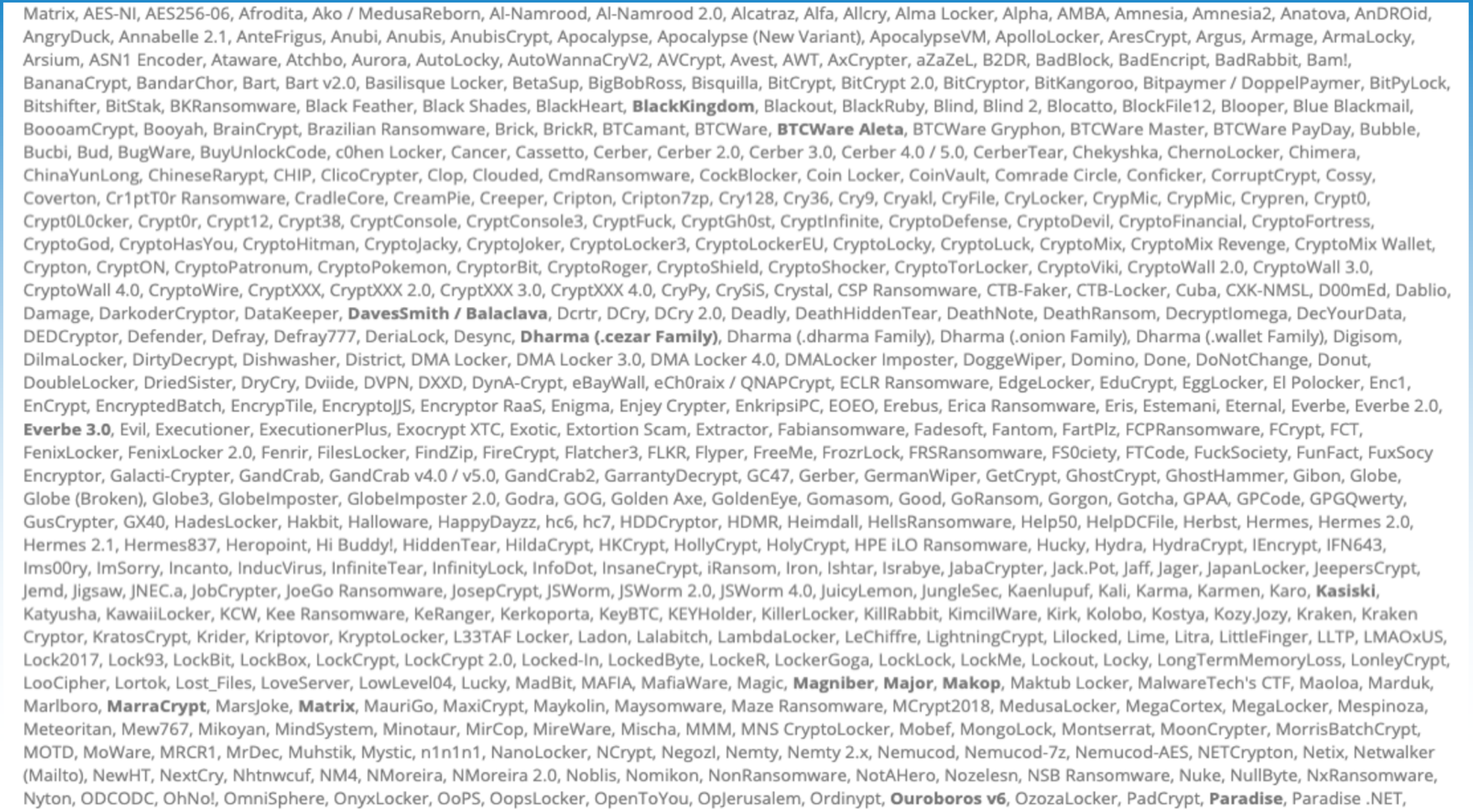
- Cyber attack where there is a demand for payment
- Attacker leaves a ransom note
- Typically the attack prevents access to files or systems
- Most common type of attack encrypts files on affected systems
- Your computer may still work, but apps may fail and data may be inaccessible



HOW COMMON IS IT?

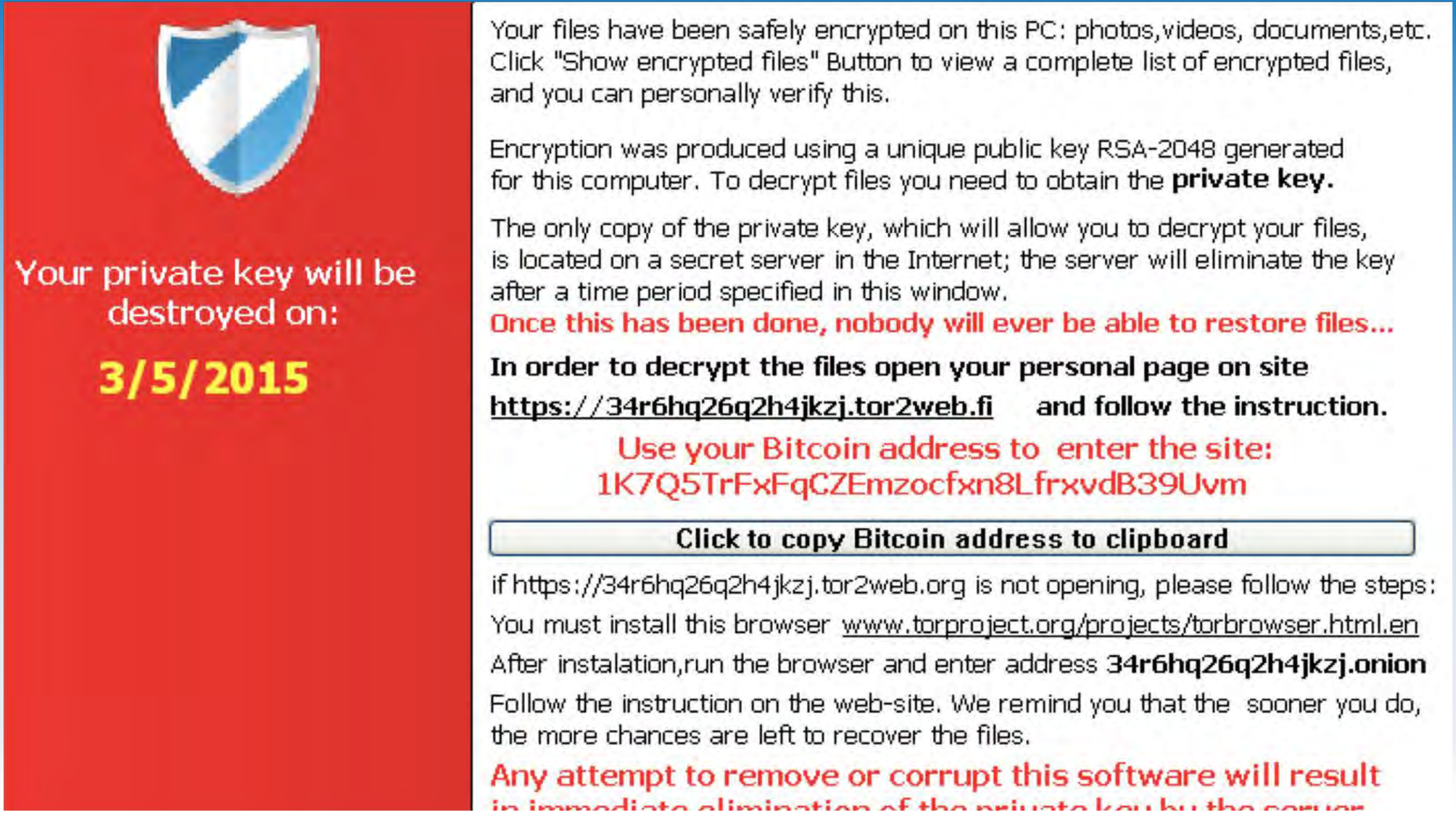
- Symantec reports ransomware attacks declined in 2019
- Reliable statistics are difficult to find





Matrix, AES-NI, AES256-06, Afrodita, Ako / MedusaReborn, Al-Namrood, Al-Namrood 2.0, Alcatraz, Alfa, Allcry, Alma Locker, Alpha, AMBA, Amnesia, Amnesia2, Anatova, AnDROid, AngryDuck, Annabelle 2.1, AnteFrigus, Anubi, Anubis, AnubisCrypt, Apocalypse, Apocalypse (New Variant), ApocalypseVM, ApolloLocker, AresCrypt, Argus, Armage, ArmaLocky, Arsium, ASN1 Encoder, Ataware, Atchbo, Aurora, AutoLocky, AutoWannaCryV2, AVCrypt, Avest, AWT, AxCrypter, aZaZeL, B2DR, BadBlock, BadEncript, BadRabbit, Bam!, BananaCrypt, BandarChor, Bart, Bart v2.0, Basilisque Locker, BetaSup, BigBobRoss, Bisquilla, BitCrypt, BitCrypt 2.0, BitCryptor, BitKangoroo, Bitpaymer / DoppelPaymer, BitPyLock, Bitshifter, BitStak, BKRansomware, Black Feather, Black Shades, BlackHeart, **BlackKingdom**, Blackout, BlackRuby, Blind, Blind 2, Blocatto, BlockFile12, Blooper, Blue Blackmail, BoooamCrypt, Booyah, BrainCrypt, Brazilian Ransomware, Brick, BrickR, BTCamant, BTCWare, **BTCWare Aleta**, BTCWare Gryphon, BTCWare Master, BTCWare PayDay, Bubble, Bucbi, Bud, BugWare, BuyUnlockCode, c0hen Locker, Cancer, Cassetto, Cerber, Cerber 2.0, Cerber 3.0, Cerber 4.0 / 5.0, CerberTear, Chekyshka, ChernoLocker, Chimera, ChinaYunLong, ChineseRarypt, CHIP, ClicoCrypter, Clop, Clouded, CmdRansomware, CockBlocker, Coin Locker, CoinVault, Comrade Circle, Conficker, CorruptCrypt, Cossy, Coverton, Cr1ptT0r Ransomware, CradleCore, CreamPie, Creeper, Cripton, Cripton7zp, Cry128, Cry36, Cry9, Cryakl, CryFile, CryLocker, CrypMic, CrypMic, Crypren, Crypt0, Crypt0L0cker, Crypt0r, Crypt12, Crypt38, CryptConsole, CryptConsole3, CryptFuck, CryptGh0st, CryptInfinite, CryptoDefense, CryptoDevil, CryptoFinancial, CryptoFortress, CryptoGod, CryptoHasYou, CryptoHitman, CryptoJacky, CryptoJoker, CryptoLocker3, CryptoLockerEU, CryptoLocky, CryptoLuck, CryptoMix, CryptoMix Revenge, CryptoMix Wallet, Crypton, CryptON, CryptoPatronum, CryptoPokemon, CryptorBit, CryptoRoger, CryptoShield, CryptoShocker, CryptoTorLocker, CryptoViki, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, CryptoWire, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, CryptXXX 4.0, CryPy, CrySiS, Crystal, CSP Ransomware, CTB-Faker, CTB-Locker, Cuba, CXK-NMSL, D00mEd, Dablio, Damage, DarkoderCryptor, DataKeeper, **DavesSmith / Balaclava**, Dcrtr, DCry, DCry 2.0, Deadly, DeathHiddenTear, DeathNote, DeathRansom, DecryptIomega, DecYourData, DEDCryptor, Defender, Defray, Defray777, DeriaLock, Desync, **Dharma (.cezar Family)**, Dharma (.dharma Family), Dharma (.onion Family), Dharma (.wallet Family), Digisom, DilmaLocker, DirtyDecrypt, Dishwasher, District, DMA Locker, DMA Locker 3.0, DMA Locker 4.0, DMALocker Imposter, DoggeWiper, Domino, Done, DoNotChange, Donut, DoubleLocker, DriedSister, DryCry, Dviide, DVPN, DXXD, DynA-Crypt, eBayWall, eCh0raix / QNAPCrypt, ECLR Ransomware, EdgeLocker, EduCrypt, EggLocker, El Polocker, Enc1, EnCrypt, EncryptedBatch, EncrypTile, EncryptoJJS, Encryptor RaaS, Enigma, Enjey Crypter, EnkripsiPC, EOEO, Erebus, Erica Ransomware, Eris, Estemani, Eternal, Everbe, Everbe 2.0, **Everbe 3.0**, Evil, Executioner, ExecutionerPlus, Exocrypt XTC, Exotic, Extortion Scam, Extractor, Fabiansomware, Fadesoft, Fantom, FartPlz, FCPRansomware, FCrypt, FCT, FenixLocker, FenixLocker 2.0, Fenrir, FilesLocker, FindZip, FireCrypt, Flatcher3, FLKR, Flyper, FreeMe, FrozrLock, FRSRansomware, FS0ciety, FTCode, FuckSociety, FunFact, FuxSocy Encryptor, Galacti-Crypter, GandCrab, GandCrab v4.0 / v5.0, GandCrab2, GarrantyDecrypt, GC47, Gerber, GermanWiper, GetCrypt, GhostCrypt, GhostHammer, Gibon, Globe, Globe (Broken), Globe3, GlobeImposter, GlobeImposter 2.0, Godra, GOG, Golden Axe, GoldenEye, Gomasom, Good, GoRansom, Gorgon, Gotcha, GPAA, GPCode, GPGQwerty, GusCrypter, GX40, HadesLocker, Hakbit, Halloware, HappyDayzz, hc6, hc7, HDDCryptor, HDMR, Heimdall, HellsRansomware, Help50, HelpDCFile, Herbst, Hermes, Hermes 2.0, Hermes 2.1, Hermes837, Heropoint, Hi Buddy!, HiddenTear, HildaCrypt, HKCrypt, HollyCrypt, HolyCrypt, HPE iLO Ransomware, Hucky, Hydra, HydraCrypt, IEncrypt, IFN643, Ims00ry, ImSorry, Incanto, InducVirus, InfiniteTear, InfinityLock, InfoDot, InsaneCrypt, iRansom, Iron, Ishtar, Israbye, JabaCrypter, Jack.Pot, Jaff, Jager, JapanLocker, JeepersCrypt, Jemd, Jigsaw, JNEC.a, JobCrypter, JoeGo Ransomware, JosepCrypt, JSWorm, JSWorm 2.0, JSWorm 4.0, JuicyLemon, JungleSec, Kaenlupuf, Kali, Karma, Karmen, Karo, **Kasiski**, Katyusha, KawaiiLocker, KCW, Kee Ransomware, KeRanger, Kerkoporta, KeyBTC, KEYHolder, KillerLocker, KillRabbit, KimcilWare, Kirk, Kolobo, Kostya, Kozy.Jozy, Kraken, Kraken Cryptor, KratosCrypt, Krider, Kriptovor, KryptoLocker, L33TAF Locker, Ladon, Lalabitch, LambdaLocker, LeChiffre, LightningCrypt, Lilocked, Lime, Litra, LittleFinger, LLTP, LMAOxUS, Lock2017, Lock93, LockBit, LockBox, LockCrypt, LockCrypt 2.0, Locked-In, LockedByte, LockeR, LockerGoga, LockLock, LockMe, Lockout, Locky, LongTermMemoryLoss, LonleyCrypt, LooCipher, Lortok, Lost_Files, LoveServer, LowLevel04, Lucky, MadBit, MAFIA, MafiaWare, Magic, **Magniber**, **Major**, **Makop**, Maktub Locker, MalwareTech's CTF, Maoloa, Marduk, Marlboro, **MarraCrypt**, MarsJoke, **Matrix**, MauriGo, MaxiCrypt, Maykolin, Maysomware, Maze Ransomware, MCrypt2018, MedusaLocker, MegaCortex, MegaLocker, Mespinoza, Meteoritan, Mew767, Mikoyan, MindSystem, Minotaur, MirCop, MireWare, Mischa, MMM, MNS CryptoLocker, Mobef, MongoLock, Montserrat, MoonCrypter, MorrisBatchCrypt, MOTD, MoWare, MRCR1, MrDec, Muhstik, Mystic, n1n1n1, NanoLocker, NCrypt, Negozl, Nemty, Nemty 2.x, Nemucod, Nemucod-7z, Nemucod-AES, NETCrypton, Netix, Netwalker (Mailto), NewHT, NextCry, Nhtnwcuf, NM4, NMoreira, NMoreira 2.0, Noblis, Nomikon, NonRansomware, NotAHero, Nozelesn, NSB Ransomware, Nuke, NullByte, NxRansomware, Nyton, ODCODC, OhNo!, OmniSphere, OnyxLocker, OoPS, OopsLocker, OpenToYou, OpJerusalem, Ordinypt, **Ouroboros v6**, OzozaLocker, PadCrypt, **Paradise**, Paradise .NET,

Source: https://id-ransomware.malwarehunterteam.com/index.php#faq



Your private key will be destroyed on:

3/5/2015

Your files have been safely encrypted on this PC: photos,videos, documents,etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files open your personal page on site https://34r6hq26q2h4jkzj.tor2web.fi and follow the instruction.

Use your Bitcoin address to enter the site:
1K7Q5TrFxFqCZEmzocfxn8LfrxvdB39Uvm

if https://34r6hq26q2h4jkzj.tor2web.org is not opening, please follow the steps:

You must install this browser www.torproject.org/projects/torbrowser.html.en

After instalation,run the browser and enter address **34r6hq26q2h4jkzj.onion**

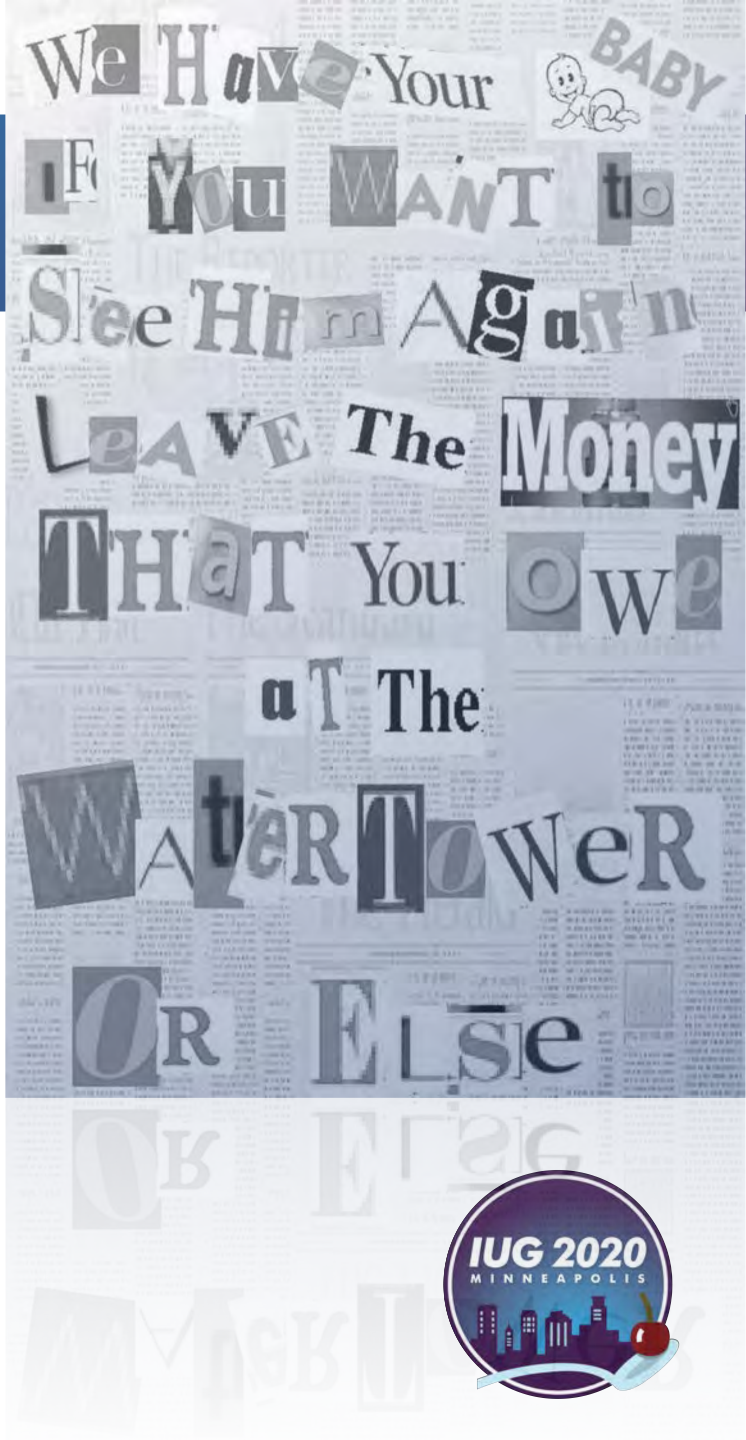
Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server

Source: Kaspersky Lab

INFECTION MECHANISMS

- Email
- Malicious web sites
- Vulnerable servers



Chapter 2

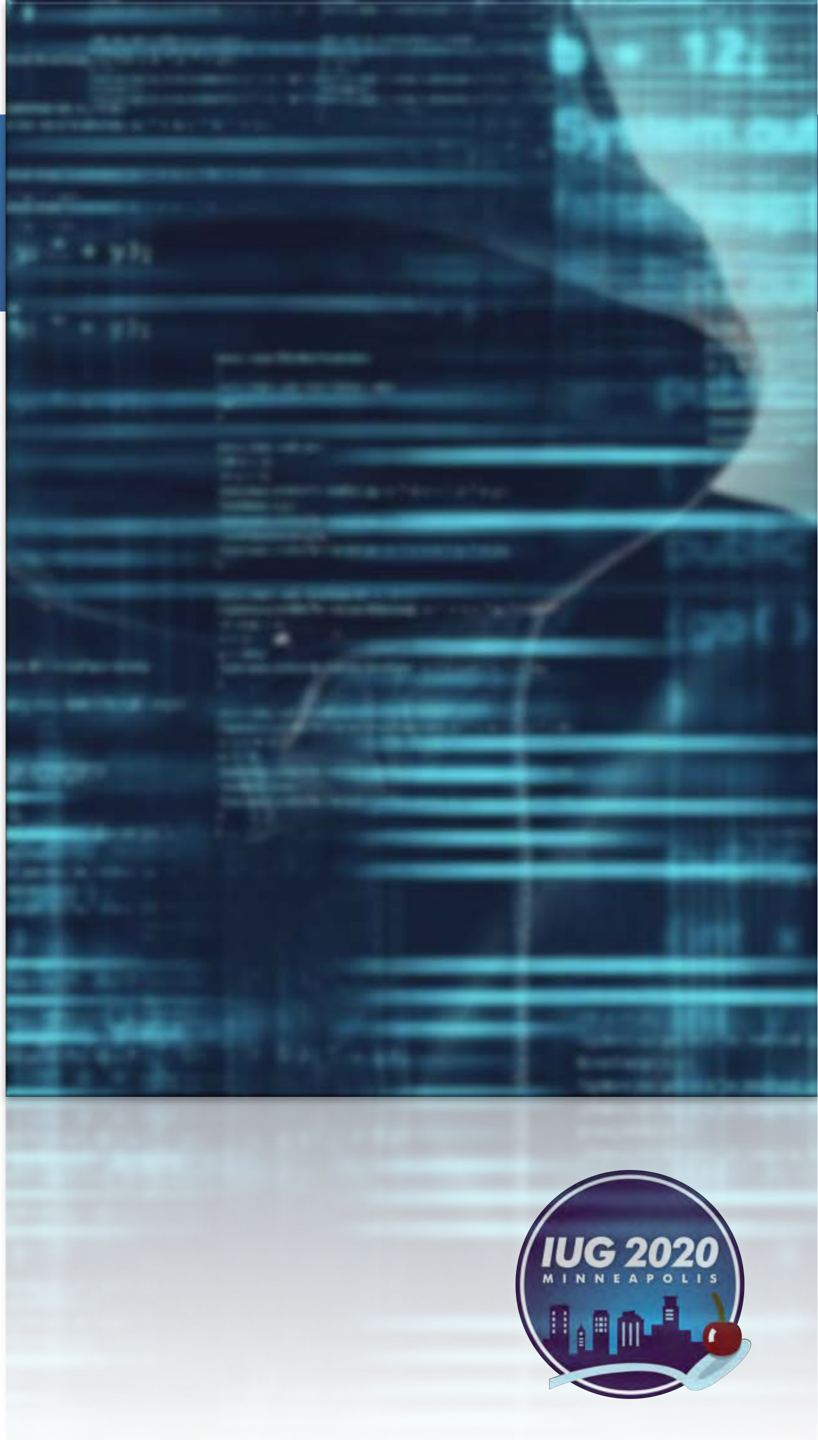
WHISKY TANGO FOXTROT

DECISIONS:

EASY & DIFFICULT

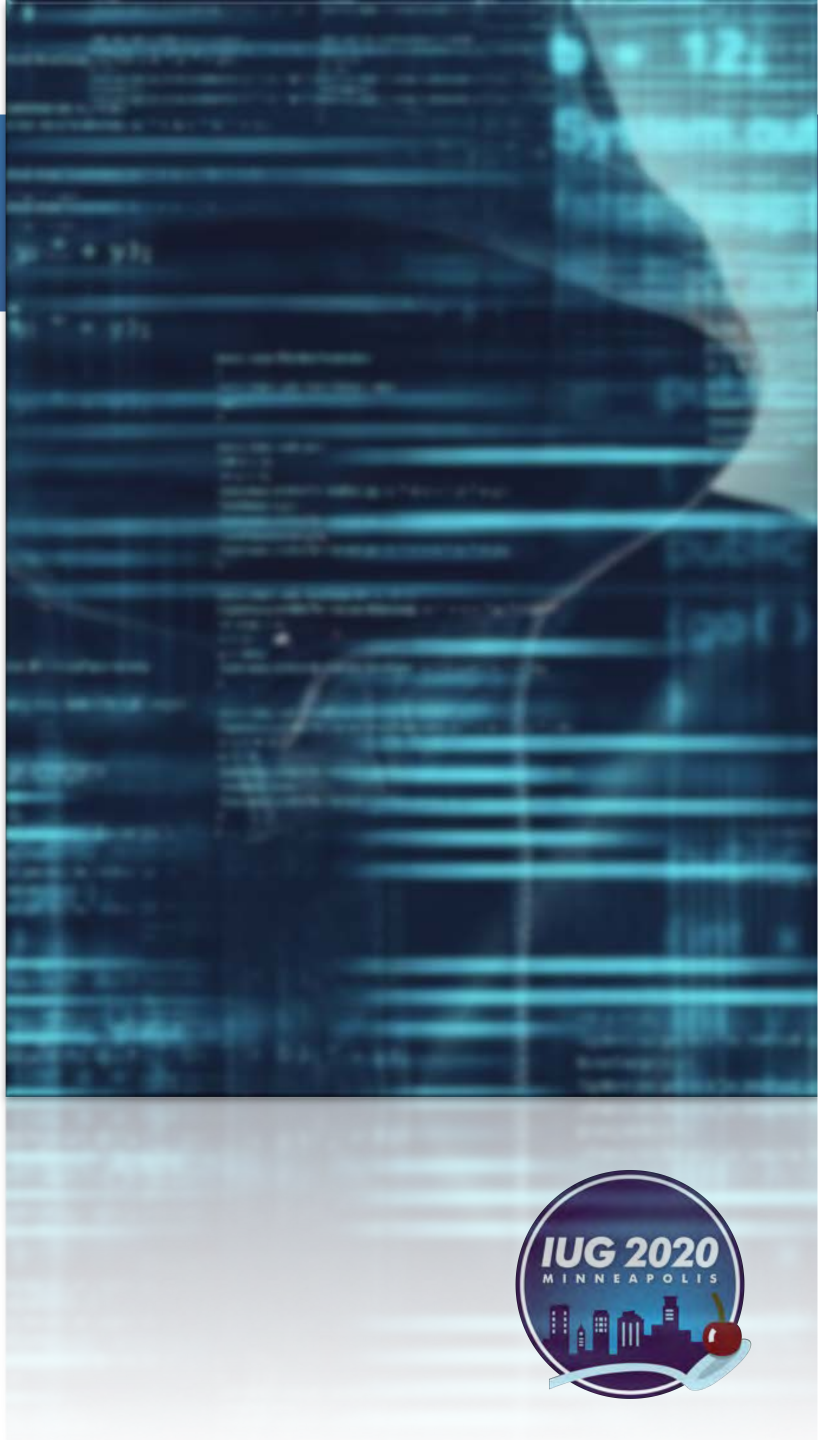
SHUT OFF THE WATER!

- You must stop the software which is encrypting your files
- Know how to disconnect the network (including wi-fi)
- If in doubt, pull the plug
- Stop and disconnect all backup systems



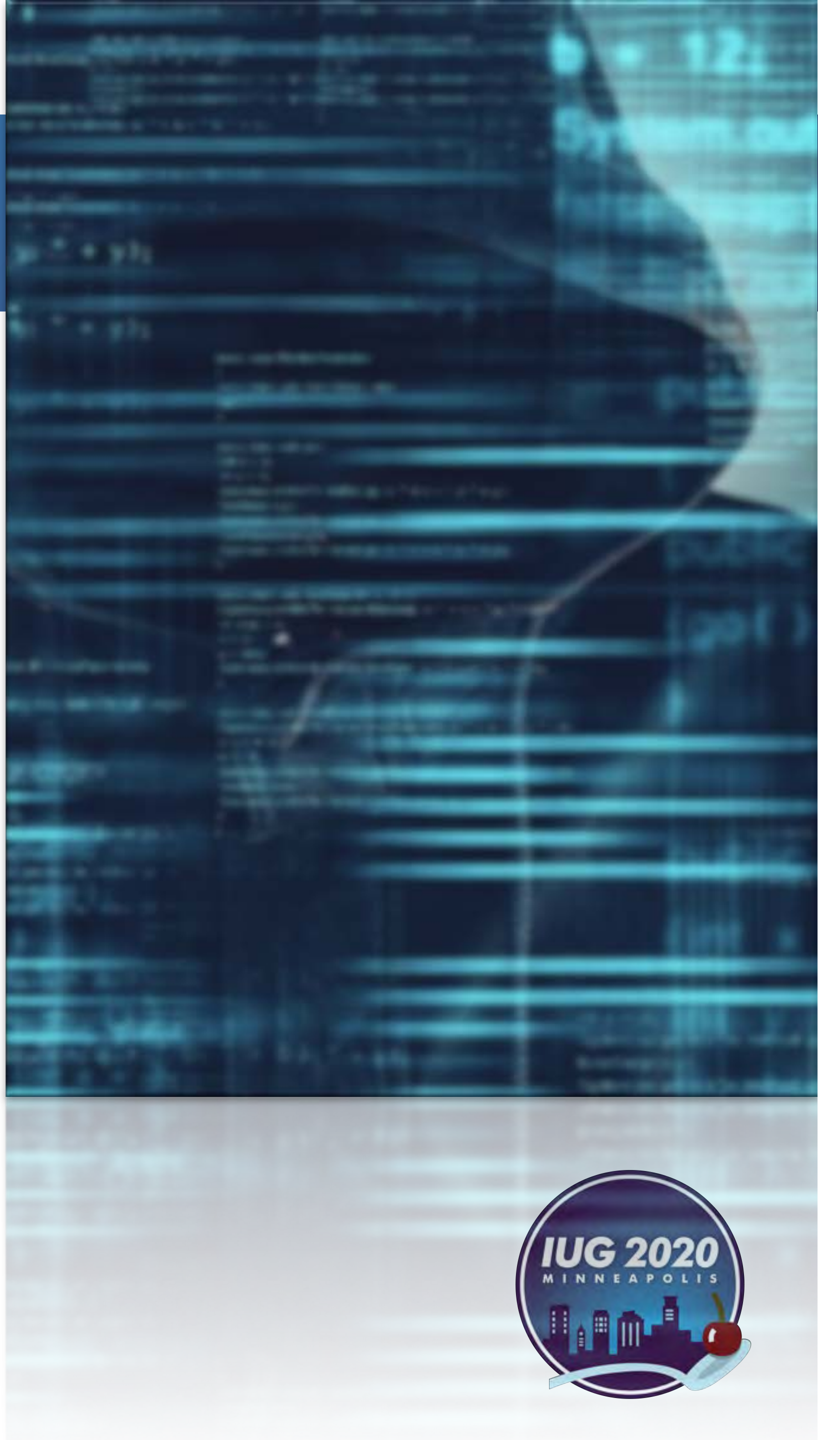
MAKE CALLS

- Call your ILS vendor
- Call your insurance provider (if you have cyber insurance)
- Call the authorities
- Contact the hacker?
  - Use a burner, non-work email account
  - Let your insurance team handle (if you have cyber insurance)
  - Expect aggressive threats



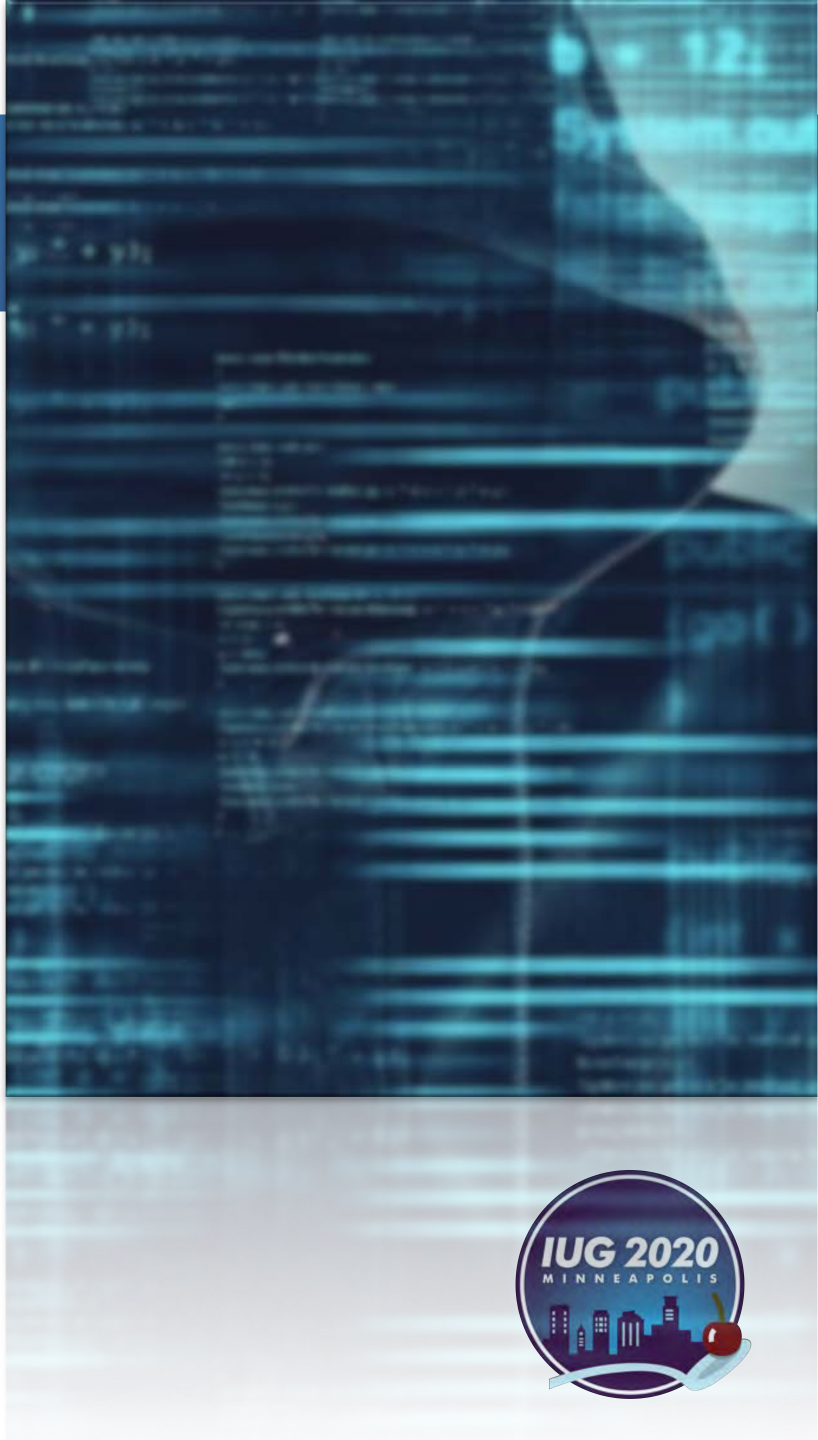
DAMAGE ASSESSMENT

- Determine type of ransomware
  - Google file extension of encrypted files
  - ID Ransomware
  - No More Ransom Project
- Has the attack stopped?
- How many systems are affected?
- Do any systems contain personal/sensitive information?
- May require expert help



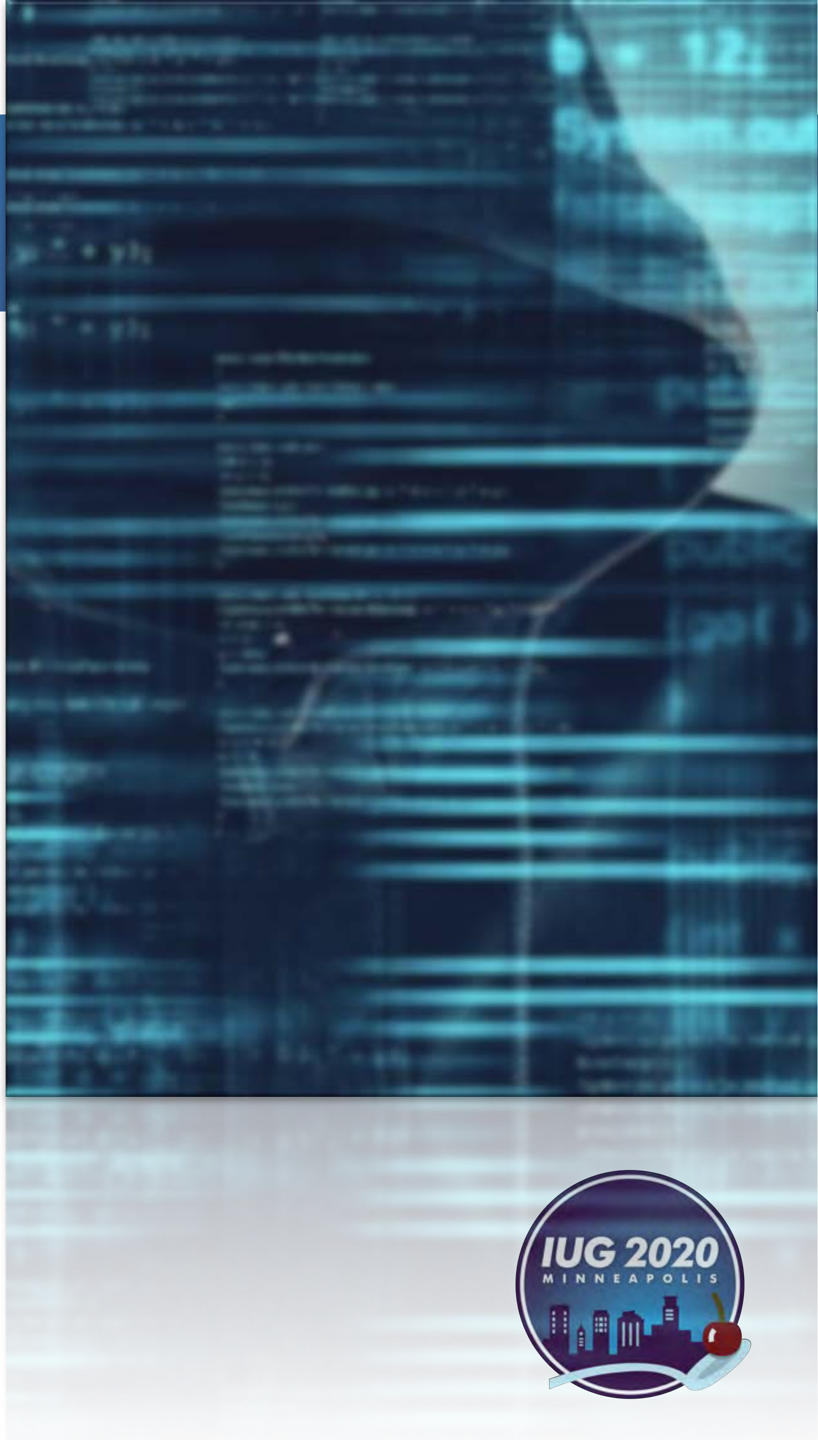
ONGOING COMMUNICATION

- Retain all communication related to the incident
- Document everything you do
- Prepare a statement on the current situation
- Determine who needs to know
    - Board
    - Staff
    - Public



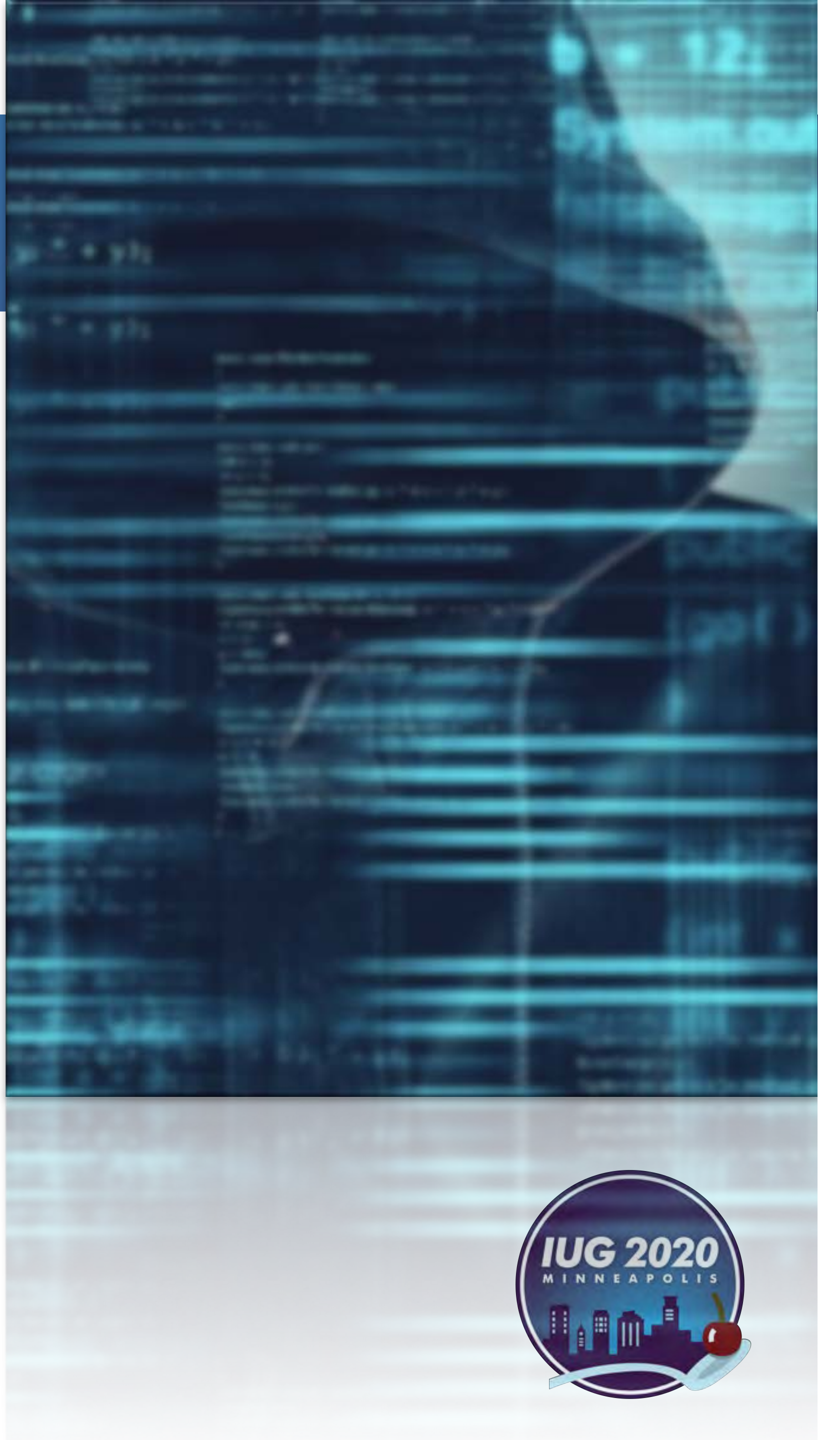
TO PAY OR NOT TO PAY

- Insurers may advise you to pay
- General advice is to not pay
- Assess the cost of paying vs not paying
- Decision depends on the situation
  - How much is the demand?
  - Are you able to pay in crypto-currency?
  - Can you continue business-critical processes without the affected systems?



IF YOU PAY

- Call for expert help
- Experts should review the decryption software provided
- It may or may not work
- Expect the decision to be questioned
- Prepare talking points



Chapter 3

THE ROAD TO RECOVERY

PROTECT YOURSELF

DO YOU?

- Backup your data?
- Update your operating system automatically?
- Update all applications automatically?
- Use anti-virus/anti-malware on all systems?
- Use strong passwords?
- Never use the same password twice?

PASSWORD MANAGEMENT

- Require strong passwords
  - Use an easy-to-remember formula
  - <word><punctuation><Word><punctuation><number>
- Require regular changes
- Use two-factor authentication if available
- Use a password manager
  - LastPass
  - 1Password

BACKUPS

- Use automatic backup systems
- Use a disconnected backup
  - A continuous or online system may backup encrypted/infected files
  - Backup systems can also be infected
- Alternate processes
  - Offline circulation
  - Bill payment
  - Payroll

RESTRICTING ACCESS

- Segment your network and services
  - Move system-critical services to the cloud
- Remove admin rights for users
- Switch port security
  - Our network is segmented into multiple VLANs
  - Prevented attacking app from seeing PCs on other VLANs
  - Work with a Cisco Certified Engineer for your network security

CYBER INSURANCE

- Contact your insurance carrier
- Provides expert help
  - Assessing scope of the problem
  - Assistance diagnosing and determining cause
- Protection should personal data be comprised

Chapter 4

SLEEPING EASIER

NO MORE RANSOMS?

ID RANSOMWARE

- id-ransomware.malwarehunterteam.com
- Tries to identify the type of ransomware
- Upload ransom note and/or an encrypted file

NO MORE RANSOM PROJECT

- Public-private partnership
  - Netherlands National High-Tech Crime Unit
  - Europol European Cybercrime Centre
  - Kaspersky
  - McAfee
- Provides identification tools
- Provides decryption tools for some types of ransomware

THANK YOU

QUESTIONS?