

Morgan Lewis

BITE-SIZED

BANKING BULLETIN

**PRACTICES FOR RESPONDING TO AND
PREVENTING RANSOMWARE ATTACKS**

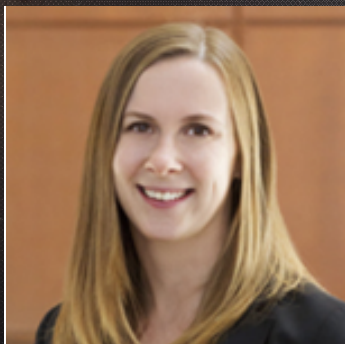
Kristin M. Hadgis

Terese M. Schireson

May 9, 2022



Presenters



Kristin M. Hadgis
Partner | Philadelphia



Terese M. Schireson
Associate | Philadelphia

Morgan Lewis



Agenda

- Background on Ransomware
- Incident-Response Considerations
- US Government Sanctions
- Best Practices for Preparedness

Ransomware in the News

Ransomware warning: Hackers see holidays and weekends as a great time to attack

Recent Cyber Attacks Target Asset Management Firms

Hacks, ransomware and data privacy dominated cybersecurity in 2021

Banking industry sees 1318% increase in ransomware attacks in 2021

FBI: Hackers Behind 'Cuba' Ransomware Have Earned at Least \$43.9 Million

Background

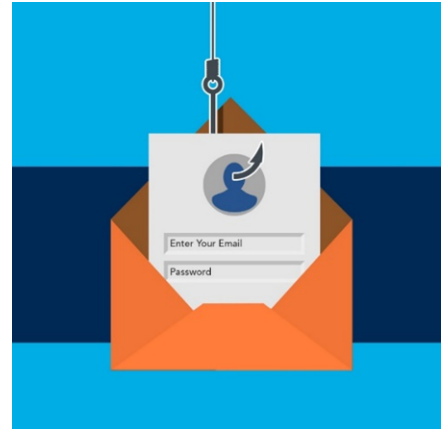
- **What is ransomware?**

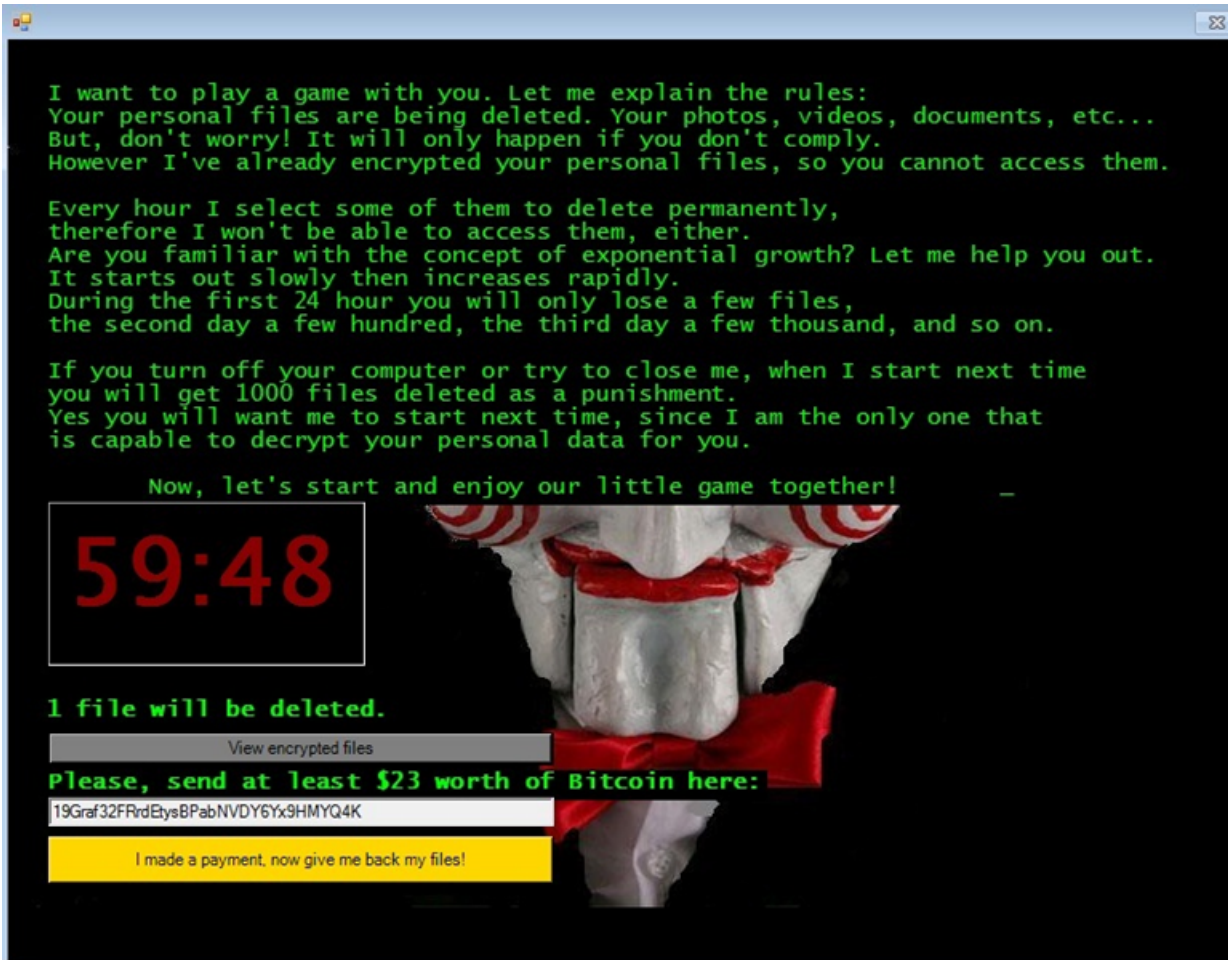
- Malicious software that infiltrates a network and restricts access to critical data by encrypting files until a ransom is paid
- Can spread through a network undetected for months
- Cryptocurrency obscures the money trail
- Can affect virtually any organization in any industry
- Increasing in severity and sophistication
- 105% increase in ransomware attacks in 2021
- Launched by organized criminal groups, typically located in Russia, China, or North Korea, with Darkside, Nightwalker, and Revil



Stages of a Ransomware Attack

- Enters system
 - Most commonly through phishing, faulty passwords, or software vulnerabilities
- Scans system to find files to encrypt
- Encrypts files, starting with local files and then moving to the shared network
- Ransom note is deposited throughout the files; may threaten to begin leaking or destroying data if ransom is not paid





I want to play a game with you. Let me explain the rules:
Your personal files are being deleted. Your photos, videos, documents, etc...
But, don't worry! It will only happen if you don't comply.
However I've already encrypted your personal files, so you cannot access them.

Every hour I select some of them to delete permanently,
therefore I won't be able to access them, either.
Are you familiar with the concept of exponential growth? Let me help you out.
It starts out slowly then increases rapidly.
During the first 24 hour you will only lose a few files,
the second day a few hundred, the third day a few thousand, and so on.

If you turn off your computer or try to close me, when I start next time
you will get 1000 files deleted as a punishment.
Yes you will want me to start next time, since I am the only one that
is capable to decrypt your personal data for you.

Now, let's start and enjoy our little game together!

59:48

1 file will be deleted.

[View encrypted files](#)

Please, send at least \$23 worth of Bitcoin here:

19Graf32FRrdElysBPabNVDY6Yx9HMYQ4K

[I made a payment, now give me back my files!](#)

Ransomware Attacks – What Is Causing Them?

- Change in business model-traditional attacks focused on exfiltration are more difficult to perpetrate and less lucrative
 - Companies are avoiding storing sensitive data and are using encryption, using multifactor
 - Payment network has evolved with chip technology and other changes
 - Your data is already out there!
- Fueled by the rise in remote work and distraction due to COVID-19 over the last year and a half, which has opened companies to more vulnerability.
 - Use of remote access tools such as outdated VPNs and equipment, personal devices, and unsecure Wi-Fi
 - Microsoft found that the level of overall cyber attacks reached an all-time high in the three months immediately after the WHO announced that COVID-19 was a global pandemic in May 2020

Data Incident Response

- Convene the incident-response team
- Outside counsel's role
- Outside cybersecurity expertise
- Insurance
- PR and crisis communications
- Contacting law enforcement
- Negotiating a ransom payment
- Data mining
- Notification obligations



US Government Sanctions



- The US Department of the Treasury's Office of Foreign Assets Control (OFAC) strongly discourages ransomware payments
- US persons are generally prohibited from engaging in transactions, directly or indirectly, with persons on OFAC's Specially Designated Nationals and Blocked Persons List
- Sanctions may be imposed on:
 - Perpetrators of ransomware
 - Those who provide financial, material, or technological support for ransomware activities
- "OFAC may impose civil penalties for sanctions violations based on **strict liability**, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC" (OFAC Ransomware Advisory, September 2021)

Ransomware and Other Attacks – How Can You Prevent Them?

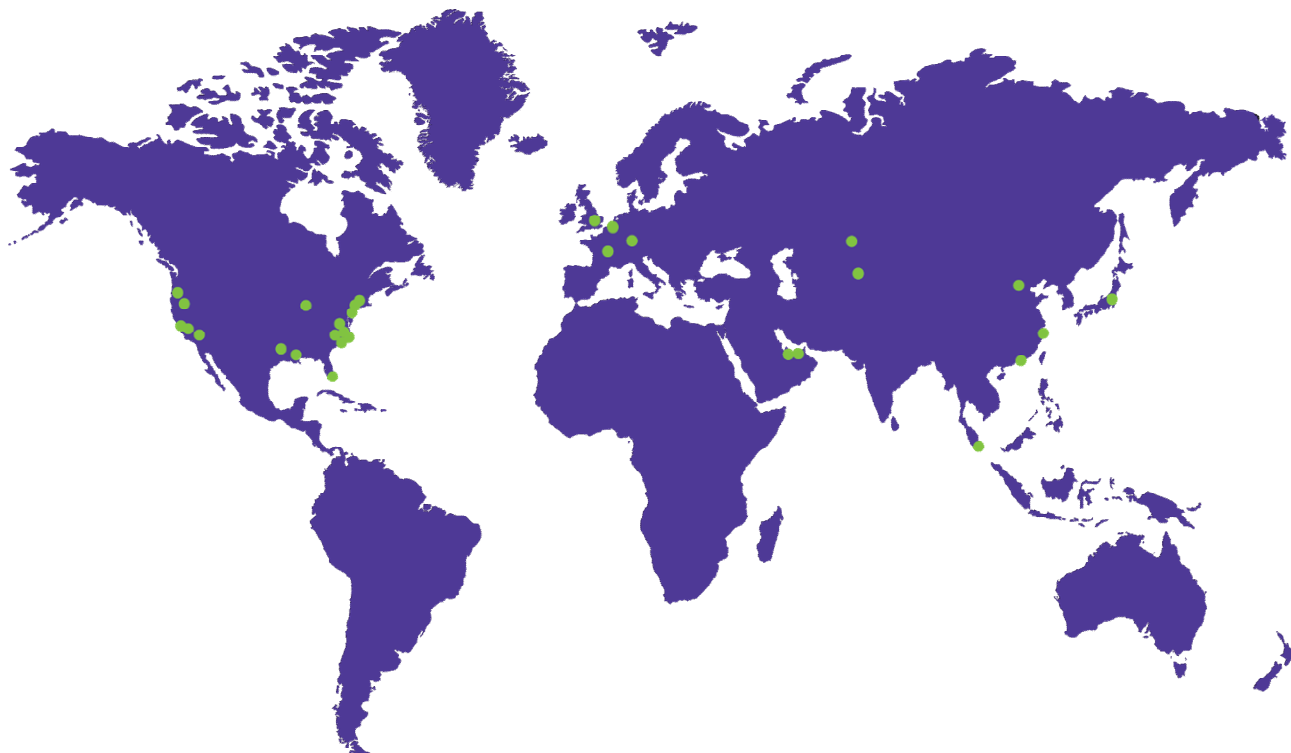
- Focus on backups-ensure regular, complete, and segregated.
- Know your system and endpoints-inventory and data map are critical.
- Consider vulnerabilities created in remote work environment.
- Maintain good, consistent cyber hygiene.
 - Regular patches
 - Updated antivirus
 - Authentication protocols (passwords and multifactor)
- The buck stops with your incident-response team and planning process.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

© 2022 Morgan, Lewis & Bockius LLP
© 2022 Morgan Lewis Stamford LLC
© 2022 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.