UT LAW CLE

TEXAS
The University of Texas at Austin
School of Law

Ransomware Response and Recovery Efforts

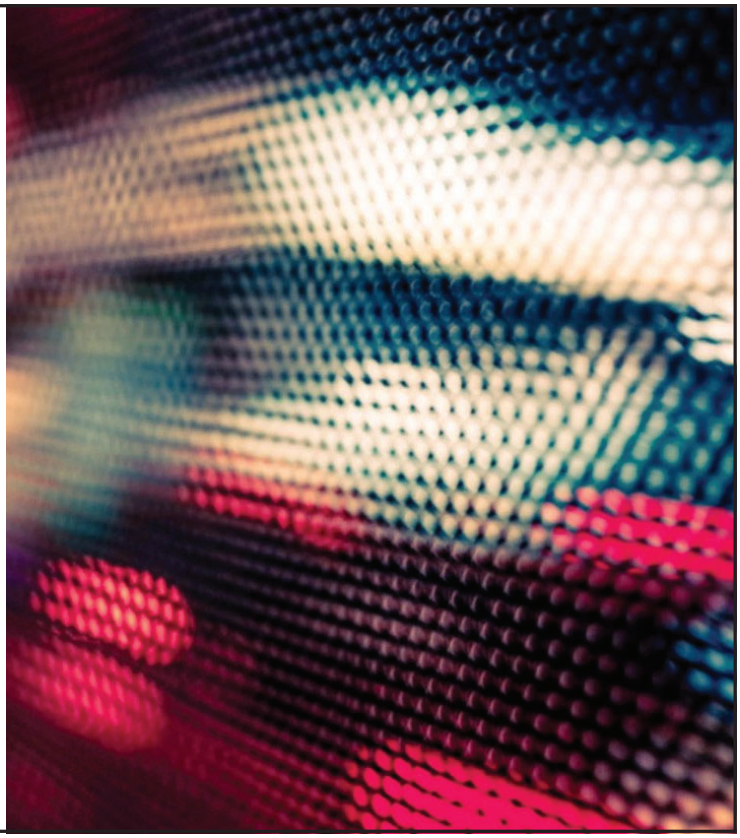
Essential Cybersecurity law

Will Daugherty
Norton Rose Fulbright
Houston, TX

Tim Newman
Haynes and Boone, LLP
Dallas, TX

Shawn E. Tuma
Spencer Fane
Plano, TX

July 21, 2021
Norton Rose Fulbright US LLP



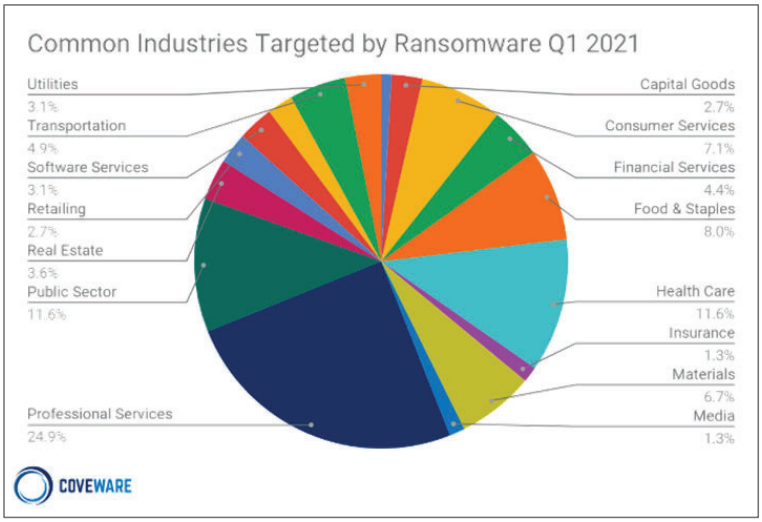
1

Ransomware → Multifaceted Extortion

- Deployment of ransomware encryptors
- Theft of sensitive data
- Publication of stolen data on a "name-and shame" website
- Additional coercive tactics
- Disruption and brand damage

Source: Mandiant M-Trends 2021

77%
of ransomware incidents now include data exfiltration



Source: Coveware Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound April 21, 2021

2

NRF

2

Introduction to the exercise

This presentation will provide an abbreviated example of ransomware attack with a hypothetical company (ACME) to highlight the unique challenges and legal nuances organizations face when responding to these attacks.

ACME in a multi-national, publicly traded company, based in Texas. ACME has operations in the UK, EU, and Brazil. The company employees 20,000 individuals, has a self-insured health plan, and directs sales to both businesses and individuals. ACME is also contractor with the US Department of Defense.

Throughout the exercise, Will Daugherty, Tim Newman and Shawn Tuma will serve as counsel for ACME and respond to factual scenarios presented.

Participants can use the Chat function to pose questions for the panel.

NRF

Initial Awareness

July 26, 2021, 6:30 a.m.

- On Monday morning, an ACME plant manager in the US reports that she is unable to access email, file-share, and other applications. While looking into the issue, the IT help desk receives several calls from other employees in Texas and EU with similar issues.
- IT discovers that files on numerous files shares are encrypted and sees active encryption taken place on other servers. They locate a ransom note and immediately escalate to the CISO.
- Initial analysis by the CISO and InfoSec team shows that domain controllers, file share servers, Exchange servers, and virtual server environment are actively being encrypted. The team is unable to gain access to the back-up environment to determine impact.

NRF

Ransom Note

```
---------- [ Welcome to DarkSide ] ------------->

 What happend?
 ---------------------------------------------
 Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
 But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
 Follow our instructions below and you will recover all your data.

 Data leak
 ---------------------------------------------
 First of all we have uploaded more then 2 TB data.

 Full dump network by our filters.

 Your personal leak page: http://darksidedxcftmqa.onion/ACME/YiUOk0S4v1j5XfdulmOPupA_ZUJZ-gu31nEfogNw-_-TM1q87Bm
 On the page you will find examples of files that have been downloaded.
 The data is preloaded and will be automatically published if you do not pay.
 After publication, your data will be available for at least 6 months on our tor cdn servers.

 We are ready:
 - To provide you the evidence of stolen data
 - To delete all the stolen data.


 What guarantees?
 ---------------------------------------------
 We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
 All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
 We guarantee to decrypt one file for free. Go to the site and contact us.

 How to get access on website?
 ---------------------------------------------
 Using a TOR browser:
 1) Download and install TOR browser from this site: https://torproject.org/
 2) Open our website: http://darksidfqzcuhtk2.onion/7UGEKLM57UIIZSBIWPN6QZNWZ7S6M3PNG55M7DLVZMKEL32204

 When you open our website, put the following data in the input form:
 Key:


7YwijMGOdQJiU7SDWwpJxH1KjA49x12BkszebPfYvNcIEFW5c4itG2fVI8tdo9taB3OI61V0WL69ezYsrGTG4UCJ1NfUBlZZHHGMJHuxk6N9sHmi33HfMIVwjXhKIzr3sAwaqOASLGL1i22DVriVrGXYHvwX
MtIumOpCmBm9AmRna9vbD41S9REK3DpOVLpvrmrf68zYM1KynhuZpSB7rm5d2f5ZNwsaQXnQ9Wk16PQOKAsgOmNKzgYBg8MrNDvqq6OmFG2607GyGRutR2We09U0Ia1KNmj7YWsw18w39P7q5teGcvA28VEh
A611PoR1Qx4SLdFuw383wDc9MVvmPpuhq3BRomS87hpn1vGNtePED155pqM7GOqrc5bOG8NA15rK5vUXyrNh4Yi1nD3bzXEZvaJXLONz2S1mkSKED385ubke12

5  !!! DANGER !!!
   DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
   !!! DANGER !!!
```

NRF

Incident Response Team Activation and Initial Steps

Containment

- Secure the network
- Preserve evidence for investigation
- How to minimize business impact from security measures

Restoration

- Identify available backups; prioritize systems to restore
- What options if backups destroyed?
- What costs to business if data must be recreated?

Business Continuity

- Identify critical systems impacted by the incident.
- What procedures can be implemented to minimize business operations?

6

NRF

Title search: Ransomware Response and Recovery Efforts

Also available as part of the eCourse
Hooked on CLE: October 2021

First appeared as part of the conference materials for the
2021 Essential Cybersecurity Law session
"Ransomware Response and Recovery Efforts"