RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M03

HOW TO BREAK UP WITH YOUR EXTORTIONIST: TALES FROM THE RANSOM FRONT LINES

Eben Kaplan

Principal Consultant
CrowdStrike

Siobhan Gorman

Partner
Brunswick Group

Ransom attacks come in many flavors

Non-targeted ransomware

Targeted ransomware

"Data-napping"

False flag ransom attacks

Tales from the ransom frontlines

HBO

- $5.5 million ransom demand for supposed 1.5 TB of stolen material
- Direct hacker outreach to media and employees, and high-degree of public interest
- Quick, transparent response focused on employees, as well as creative and business partners

HBO

Uber

- $100K ransom demand for 57 million accounts breached
- Direct hacker outreach to senior security official, who paid the ransom.
- Once public, payment of ransom resulted in senior security and legal personnel changes and loss of trust

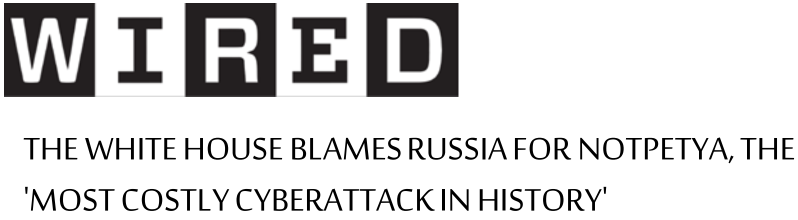
UBER

The Dark Overlord

- Previous demands range $50 – 75K
- Responsible for 15+ major breaches, including of Netflix and Columbia Falls School District
- Aggressive, pressure-building techniques including media outreach, harassment, and threats

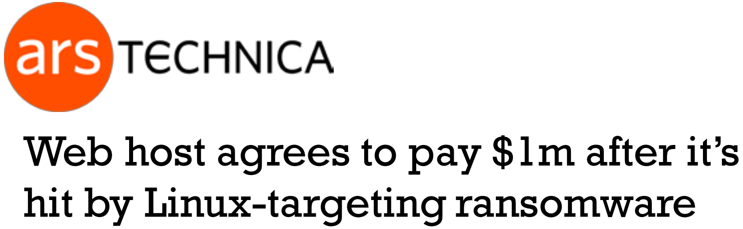
thedarkoverlord
@tdohacker

Tales from the ransom frontlines



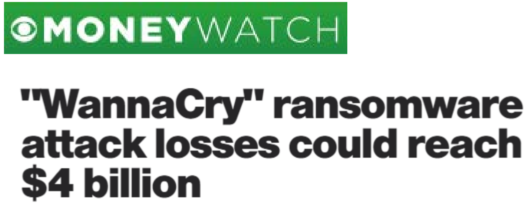
WIRED

THE WHITE HOUSE BLAMES RUSSIA FOR NOTPETYA, THE 'MOST COSTLY CYBERATTACK IN HISTORY'



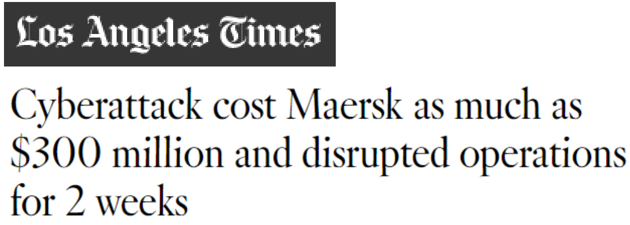
ars TECHNICA

Web host agrees to pay $1m after it's hit by Linux-targeting ransomware



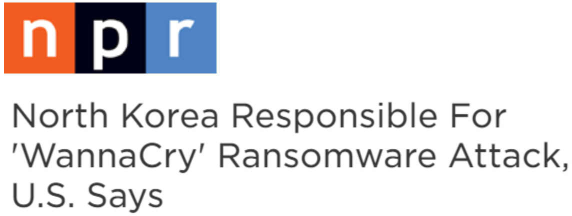
MONEYWATCH

"WannaCry" ransomware attack losses could reach $4 billion



Los Angeles Times

Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks



npr

North Korea Responsible For 'WannaCry' Ransomware Attack, U.S. Says

Game theory illustrates your options

First, define each “player’s” potential moves

Victim

- PAY
- DON’T PAY

Attacker

Availability Attack

- DECRYPT
- DON’T DECRYPT
- ASK FOR MORE MONEY

Confidentiality Attack

- DESTROY DATA
- PUBLISH DATA
- SELL DATA
- STORE/USE DATA
- ASK FOR MORE MONEY

Consider possible outcomes

Availability

	PAY	DON'T PAY
DECRYPT	RECOVER DATA GET PAID	RECOVER DATA DON'T GET PAID
DON'T DECRYPT	LOSE DATA GET PAID	LOSE DATA DON'T GET PAID
ASK FOR MORE MONEY	RECOVER FOR MORE $? GET PAID MORE	LOSE DATA DON'T GET PAID

Confidentiality

	PAY	DON'T PAY
DESTROY DATA	STOP LEAKAGE GET PAID	STOP LEAKAGE DON'T GET PAID
PUBLISH DATA	DATA LEAKAGE GET PAID	DATA LEAKAGE DON'T GET PAID
SELL DATA	RISK OF LEAKAGE GET PAID MORE	RISK OF LEAKAGE DON'T GET PAID
STORE/USE DATA	RISK OF LEAKAGE GET PAID MORE	RISK OF LEAKAGE DON'T GET PAID
ASK FOR MORE MONEY	STOP LEAKAGE/ MORE $ GET PAID MORE	RISK OF LEAKAGE DON'T GET PAID

An ounce of prevention is worth a pound of cure

- Benjamin Franklin

Questions for the business

How valuable is the information in question?

What is the potential impact to your business?

Are your backups sufficient, and can you recover if you don’t pay?

What recourse do you have if you don’t pay the ransom?

Do you have insurance that will cover the ransom payment?

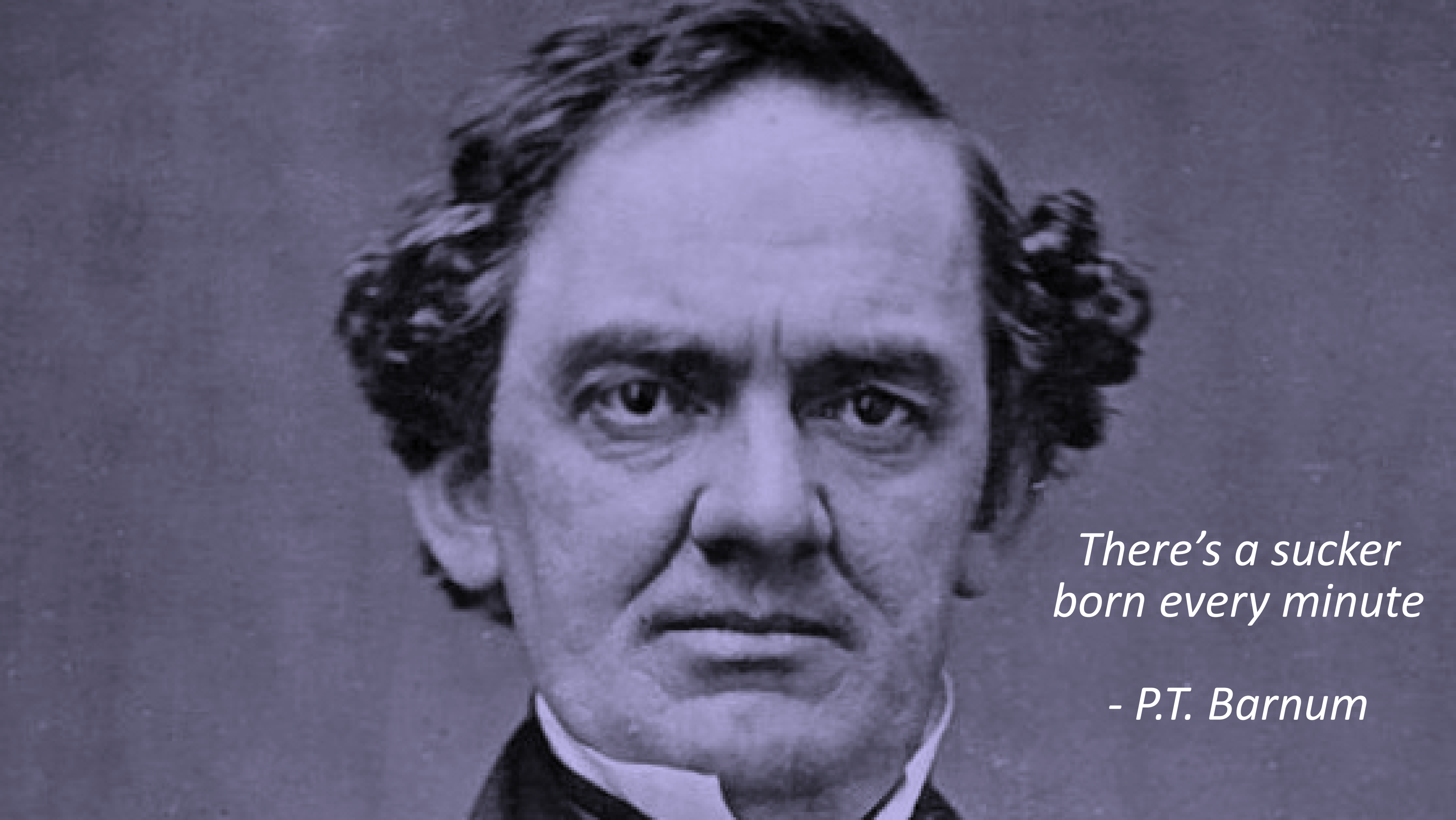
Could you pay if you wanted to?

How do you get enough bitcoins quickly enough?

Do you know who you are paying, and is doing so legal?

What is your mechanism for payment, and can you work with law enforcement to track the funds?

Has company leadership been educated on the pros and cons of paying?



There’s a sucker born every minute

- P.T. Barnum

What can you learn about your attacker?

Can cyber intelligence firms or law enforcement tell you about the attacker's profile?

- Is there evidence to suggest that you will get what you want if you pay the ransom?
- Is there evidence to suggest the attacker won't ask you for more money later?
- Can you find any information that could help law enforcement identify and apprehend the attacker?

Can you learn anything about the attacker by corresponding with him/her?

You may need to negotiate

Ransoms are often **negotiable** and some attackers even invite it.

Negotiation may be **prudent.**

Negotiating may **buy you time.**

Negotiation is also **uncomfortable** and potentially risky. Law enforcement and intel services can offer guidance on how, when, and tactics.

It could get ugly

Attackers have become their own PR agents.

Harassment of employees and their families.

Trashing the network.

Protect your reputation in a ransom attack

Be the first to reach your employees, customers, and key stakeholders, and focus your communications on supporting them.

Focus your message on the company’s response efforts, not the ransom demand or breach.

Get credit for transparency by communicating with customers in a clear, accurate, and consistent fashion.

Consider engaging law enforcement and forensics experts early.

Assume any correspondence with the attacker will become public.

Respond promptly to media and stakeholder inquiries.

Recap: How to deal with ransom demands

Avoid them

- Implement strong controls that limit the likelihood you'll be affected—and limit the damage if you are.

Prepare for them

- Develop an organizational playbook for managing cybersecurity incidents, including ransomware.
- Ensure corporate leadership understands what to expect.
- Map out the decisions and resources you'll need in advance.

Know what game you're playing

- Recognize your options and the attacker's options by planning for specific scenarios.
- Engage expert legal, forensic, and reputational advice for support in preparation and during an incident.