Responding To Ransomware

X by Invincea

Ransomware Nightmares

Ransomware is getting more sophisticated, and shifting to an enterprise threat

Hello,

Thank you for your order. We'll be informing you once item(s) have dispatched.

You can check the invoice number [redacted] by downloading Your Order Invoice to this mail. Download Invoice.

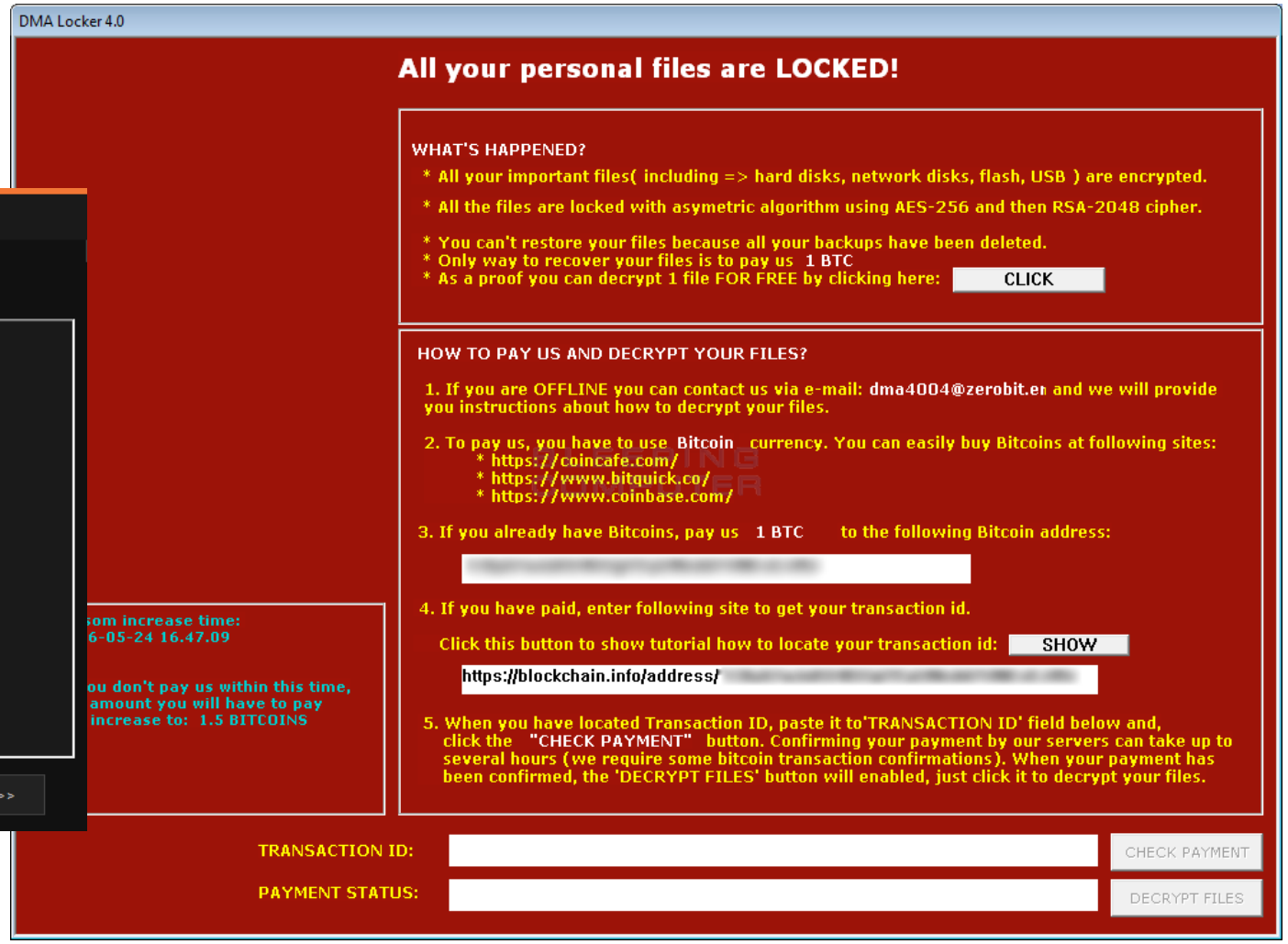
The City keeps a copy of all E-mails sent and received for a minimum of 2 years. All retained E-mails will be treated as a Public Record per the California Public Records Act, and may be subject to disclosure pursuant to the terms, and subject to the exemptions, of that Act.

This email invites you to download `invoice-order.zip`.
The ZIP file contains the ransomware as `invoice-order.exe`.

invincea

X by Invincea

Ransomware Nightmares



invincea

X by Invincea

To Pay Or Not To Pay?

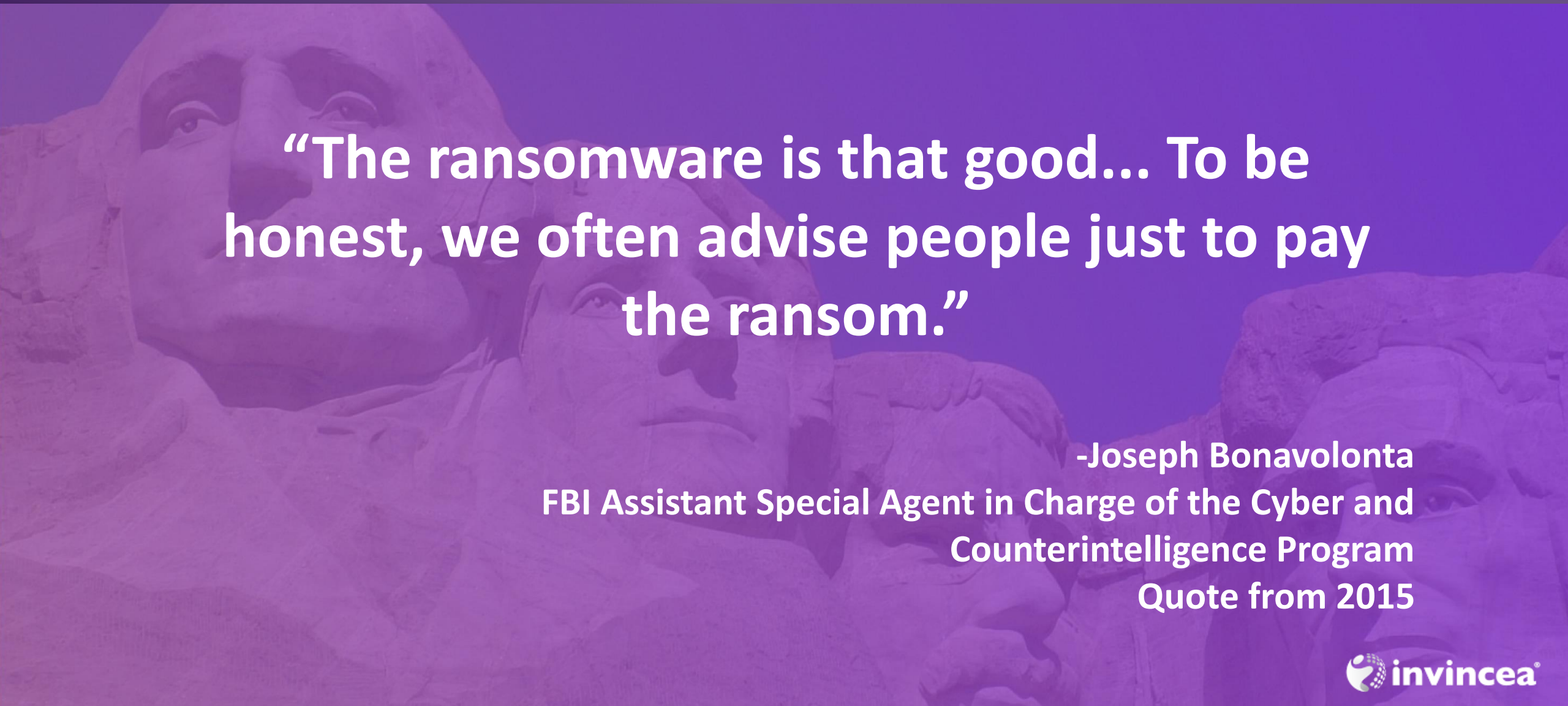
Your money or your files?

?

invincea

X by Invincea

Argument for paying



“The ransomware is that good… To be honest, we often advise people just to pay the ransom.”

-Joseph Bonavolonta
FBI Assistant Special Agent in Charge of the Cyber and Counterintelligence Program
Quote from 2015

invincea

X by Invincea

Money or Files?

50%

50% of ransomware victims have paid

40% said they would pay if they were hit with ransomware

Source: BitDefender

invincea

A RANSOMWARE ANECDOTE

X by Invincea

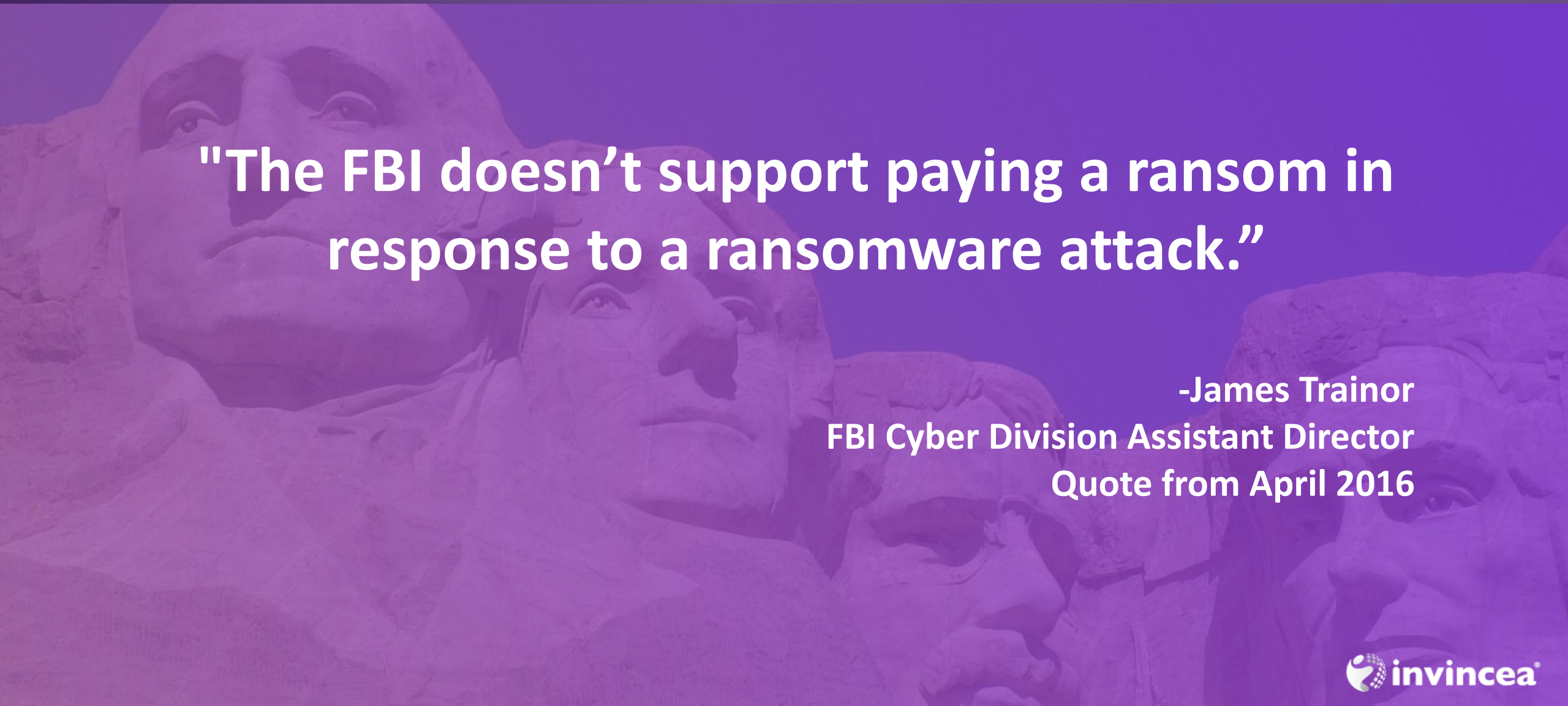
Argument against paying

- We don’t negotiate with terrorists
- Paying incents attackers to keep using ransomware

invincea

X by Invincea

Argument against paying



"The FBI doesn’t support paying a ransom in response to a ransomware attack.”

-James Trainor
FBI Cyber Division Assistant Director
Quote from April 2016

invincea

X by Invincea

Criminals Are Unreliable

"Paying a ransom doesn't guarantee an organization that it will get its data back—we've seen cases where organizations never got a decryption key after having paid the ransom."

-James Trainor
FBI Cyber Division Assistant Director
Quote from April 2016

invincea

X by Invincea

True Cost

$600 Average price of ransomware

$50K Some ransom demands are as high as $50K

$325M Amount extorted by CryptoWall since 2015

$1M+ True cost of a large ransomware attack

invincea®

Ransomware Trends

invincea

Targets

1 

2 

3 

Critical Infrastructure:

- Healthcare
- Government
- Law Enforcement
- Energy
- Financial

X by Invincea

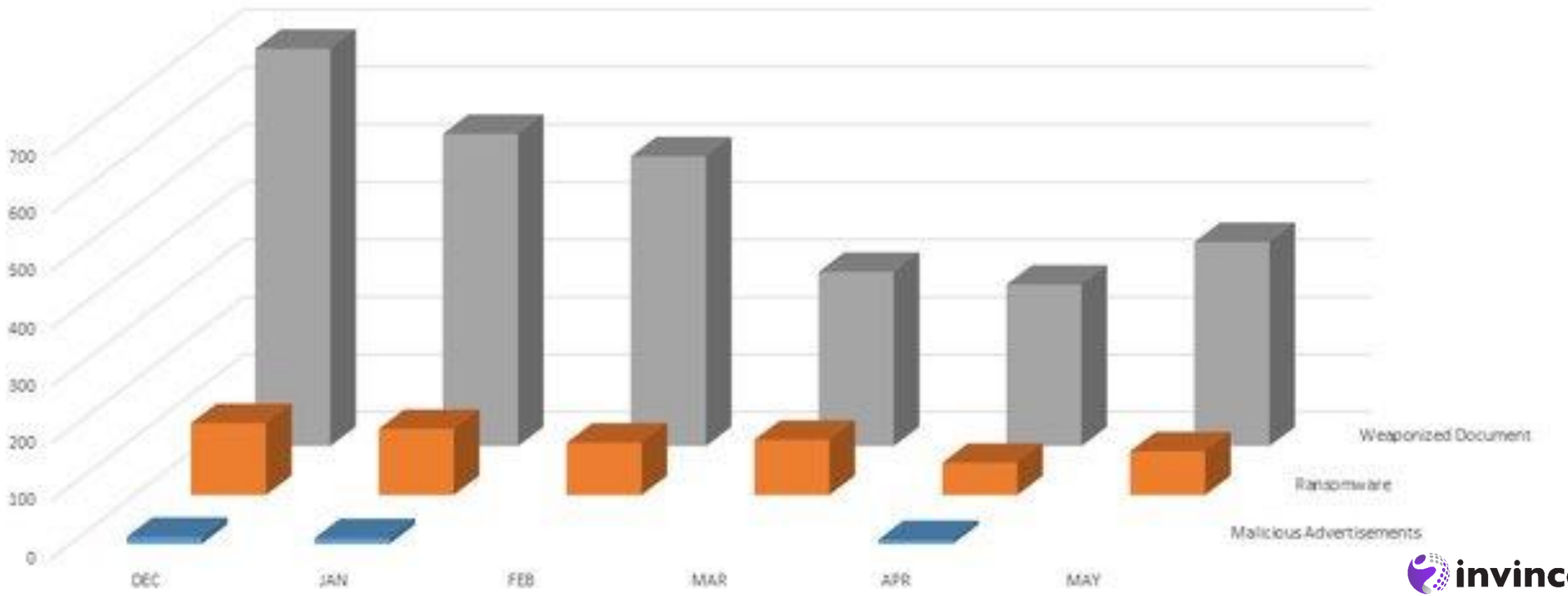
Top Infection Methods

1. Weaponized Office documents
2. Malicious email links
3. Malvertising
4. Unauthorized programs

invincea

Trends

Ransomware and Weaponized Docs (which can spread ransomware) increased in May



X by Invincea

Constant State of Innovation

- 2-for-the-price-of-1 Ransomware: Ransomware + DDOS
- Hash Factory: Ransomware changes hash every 15 seconds
- Server-side Ransomware: Beyond the desktop
- Viral Ransomware: Spreads like a virus

invincea®

Recommendations

invincea

X by Invincea

Limited Decryption Ability

- TeslaCrypt (v3.0-v4.2)
  - –ESET was able to get the decryption key by ASKING attackers for it. Seriously.
- Decryption tools are available for:
  - –777
  - –Xorist
  - –8Lock8
  - –GhostCrypt

invincea®

Common Advice Only Helps So Much

X by Invincea

- Keep Your AV up-to-date
- Filter your email
- Patch everything all the time
- Careful what you click

"Users will open attachments, they will visit sites that are infected, and when that happens, you just need to make sure that your security technology protects you."

-Anup Ghosh
CEO, Invincea
Wired Magazine, May 2016

KIM ZETTER SECURITY 05.13.16 1:00 PM

4 WAYS TO PROTECT AGAINST THE VERY REAL THREAT OF RANSOMWARE

X by Invincea

Our Recommendations

- Deploy anti-malware prevention
- Behavioral monitoring
- Isolation
- Back it up!!!!

"network shares are as at risk as your desktop system in a ransomware infection. If the backups are done offline, and the backup is not reachable from the machine that is infected, then you're fine."

-Anup Ghosh
CEO, Invincea
Wired Magazine, May 2016

KIM ZETTER SECURITY 05.13.16 1:00 PM

4 WAYS TO PROTECT AGAINST THE VERY REAL THREAT OF RANSOMWARE

X by Invincea

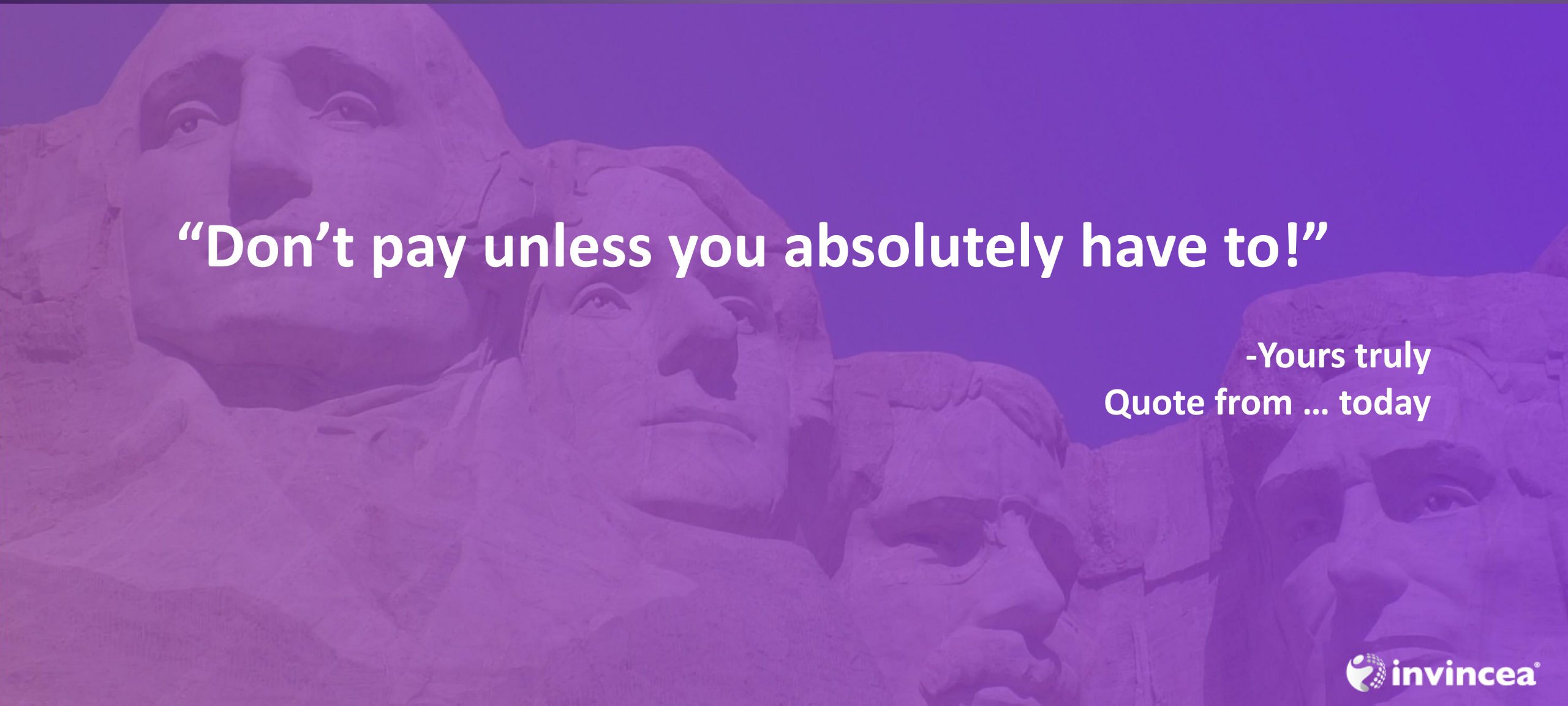
Business Continuity & Disaster Recovery

- Develop a business continuity plan for what happens if you loose access to your data or systems
- Backup your data and airgap it from your primary network
  - –Put controls in place that will allow you to rapidly your recover files
- Have an IR plan in place with access to 3rd parties that can assist

invincea

X by Invincea

Final Recommendation



“Don’t pay unless you absolutely have to!”

-Yours truly
Quote from … today

invincea

THANK YOU

www.invincea.com

invincea