A VIEW FROM THE FRONT LINES WITH M-TRENDS 2016

Presented by:

Charles Carmakal, Vice President, Mandiant

FireEye
SECURITY REIMAGINED

About the Presenter

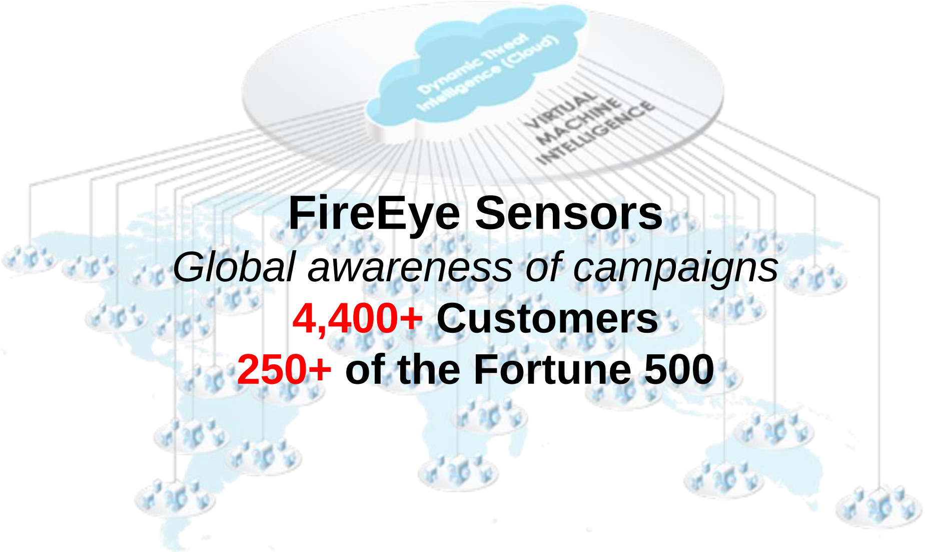
Charles Carmakal

- Vice President
- Based in Washington DC
- Leads a team of incident responders in North America
- 15+ years of experience with incident response and red teaming
- Previously led the security consulting business at a Big 4 consulting firm

Agenda

- The rise of business disruption attacks
- Theft of PII by China-based threat actors
- Attacks on enterprise networking devices
- Industry leading practices to combat these threats

Data is our Differentiator

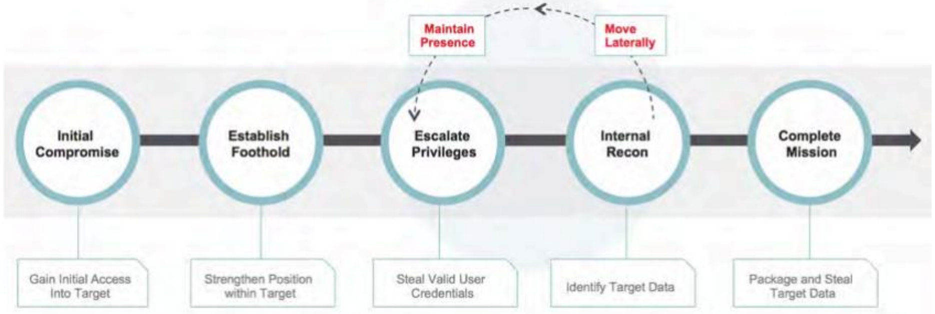

Dynamic Threat Intelligence (Cloud)
VIRTUAL MACHINE INTELLIGENCE

FireEye Sensors

Global awareness of campaigns

4,400+ Customers

250+ of the Fortune 500



Mandiant Incident Response

Understand the most devastating attacks

1,200+ customers

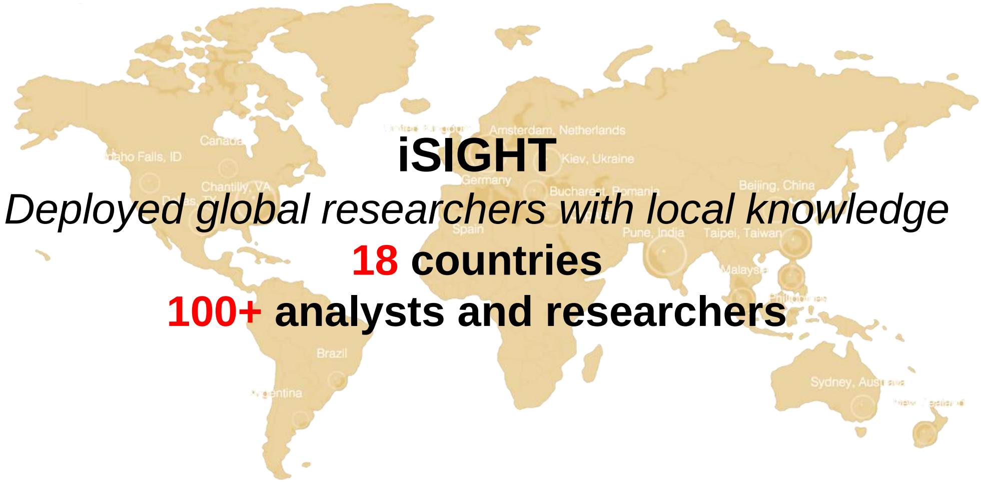
200+ of the Fortune 500

FireEye as a Service

Know active events for managed defense

6 Security Operations Centers

200+ Clients



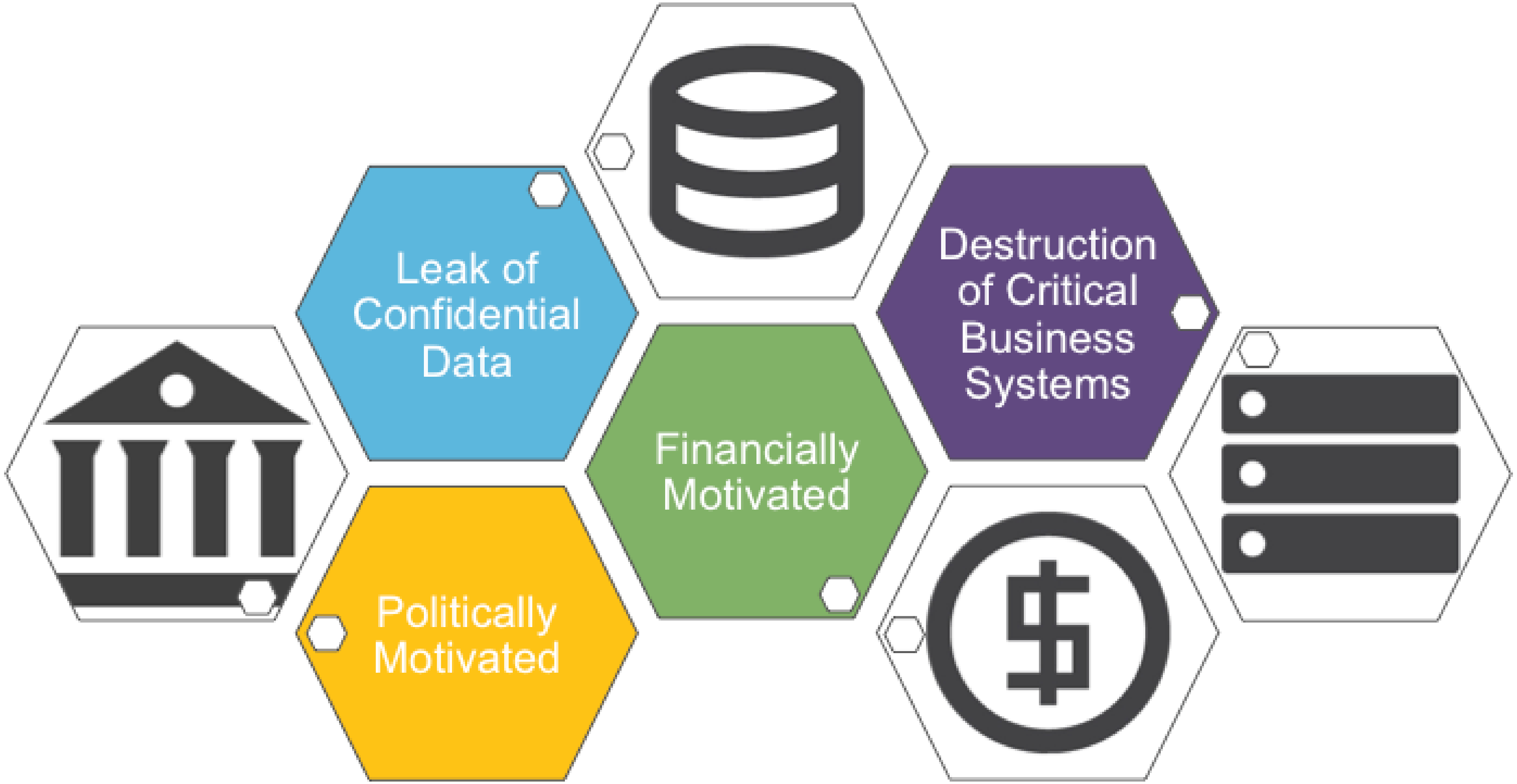
iSIGHT

Deployed global researchers with local knowledge

18 countries

100+ analysts and researchers

Trend 1: The rise of business disruption attacks



Leak of Confidential Data

Destruction of Critical Business Systems

Financially Motivated

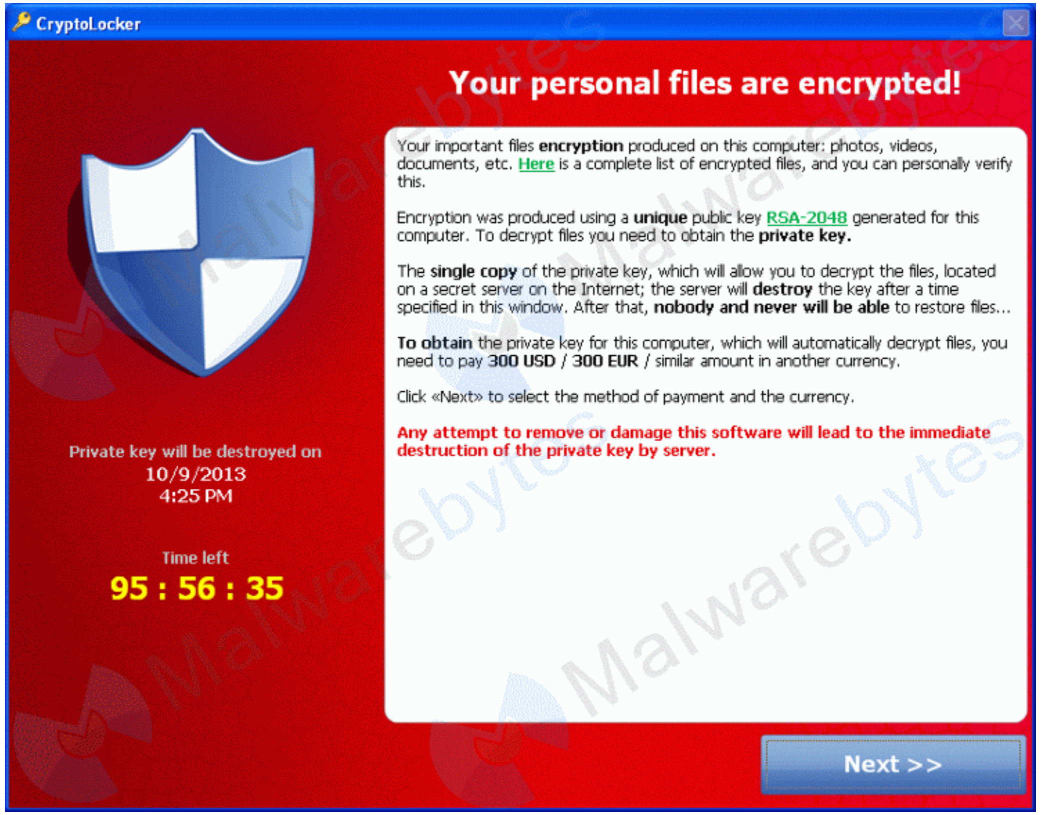
Politically Motivated

Extortion and Ransom

- Attacker contacts victim organization and notifies them that they have their materially sensitive data
- Attacker demands ransom payment, often in Bitcoins, in exchange for not releasing the data
- Attacker sets short timeframed deadline
- Victim organizations need to determine whether the attacker is real
- Victim organizations need to determine whether to pay the attacker
- Victim organizations often work with law enforcement to trace payments in hopes of catching the attacker

Ransomware

- A commodity threat that’s incredibly disruptive
- Many variants including CryptoLocker, CryptoWall, and TeslaCrypt
- Ransom values are usually around $500 (1 bitcoin)
- Mostly spread through automated means – emails and web exploit kits
- Starting to see threat actors manually deploying ransomware



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is 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 **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

Destroying Critical Systems and Data – Case Study 1

- Relatively unsophisticated threat actor taunted a victim organization for years
- Stole several gigabytes of materially sensitive data and published it on the Internet
- Created a scheduled task across the enterprise to destroy production systems

```
mkdir "C:\emptydir"
robocopy "C:\emptydir" "C:\windows\system32" /MIR | shutdown /s /t
1800
```

- Took the company’s production systems offline for several days

Destroying Critical Systems and Data – Case Study 2

- Multiple variants of malware designed to wipe Windows systems based on the function of the system
- Malware was manually deployed by the attacker, but designed to automatically spread across the network.
- The Domain Controller variant delayed destruction for a period of time so that the server could continue to provide Windows authentication services allowing the malware to spread.
- The attacker created a wiping script that differed for each Linux or Mac system in the environment
- Another script to wipe virtual machines on ESX servers
- The company’s backups were also erased

Lesson Learned – ensure the backup environment is segmented from corporate network

NORTH KOREA

Widespread DDoS Extortion Scam

From: LZ Security <sec@lzqsec.com>

Subject: DDoS Attack Imminent - Important information

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We are the Lizard Squad and we have chosen your website/network as target for our next DDoS attack. Please perform a google search for "Lizard Squad DDoS" to have a look at some of our previous "work". All of your servers will be subject to a DDoS attack starting at Tuesday the 3rd of May.

How do I stop this? We are willing to refrain from attacking your servers for a small fee. The current fee is 5 Bitcoins (BTC). The fee will increase by 5 Bitcoins for each day that has passed without payment.

Please send the bitcoin to the following Bitcoin address: 18QXdP9LUATBTisHJeA2jYRXJfQ1xoYET6

Once you have paid we will automatically get informed that it was your payment.

How do I get Bitcoins? You can easily buy bitcoins via several websites or even offline from a Bitcoin-ATM. We suggest you to start with localbitcoins.com or do a google search.

This is not a hoax, do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again!

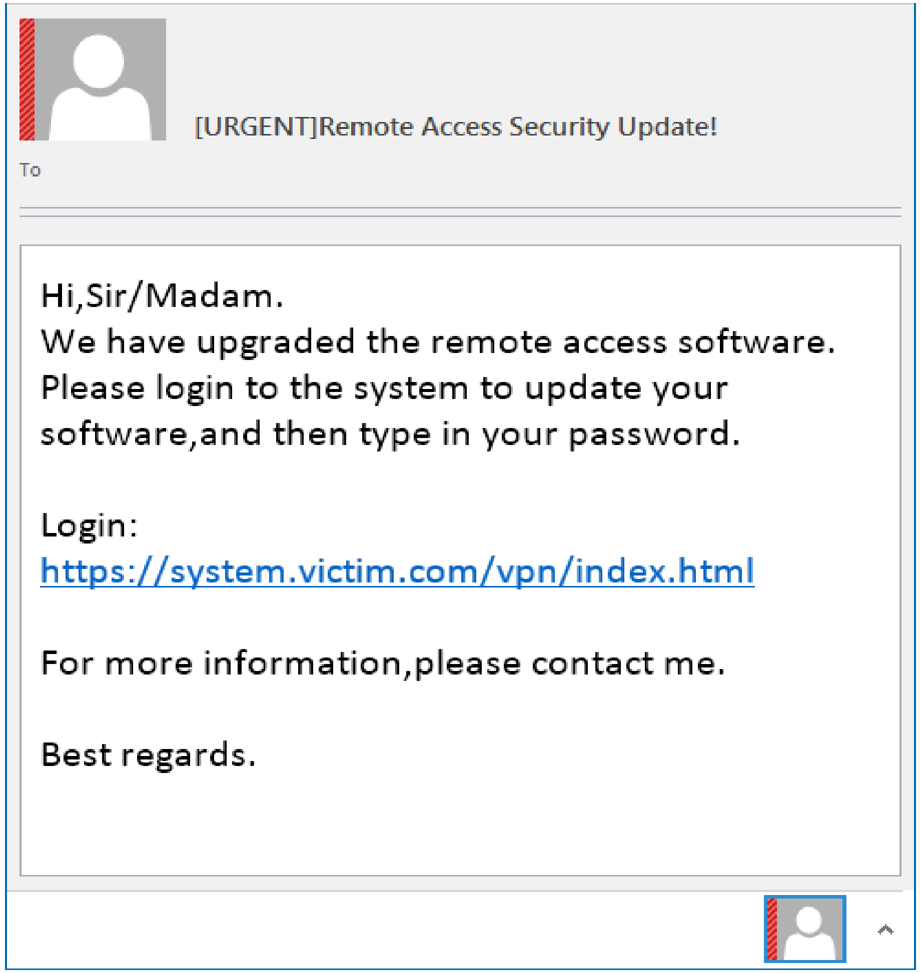
Lessons Learned from Disruptive Breaches

1. Confirm there is actually a breach or an imminent attack is credible
2. Remember that you’re dealing with a human adversary
3. Timing is critical
4. Stay focused
5. Evaluate whether to engage the attacker
6. Engage the experts before a breach
7. Consider all options when asked to pay a ransom
8. Ensure strong segmentation and controls over your backups
9. After the incident has been handled, immediately focus on broader security improvements
10. If you kick them out, they may try to come back in a different way

FireEye

Trend 2: Theft of PII by China-based threat actors

- Bulk theft of Personally Identifiable Information (PII)
- Industries affected: Government and contractors, healthcare payers, travel organizations, and others
- Stolen data: Social Security numbers, mothers' maiden names, birthdates, dependents, employment history, and challenge/response questions and answers
- Theories for the deviation in targeting:
  - Bypassing identify verification and access management Schemes
  - Facilitating "traditional" espionage operations & identifying and recruiting insider threats and subject matter experts
  - Targeting specific populations



[URGENT]Remote Access Security Update!

To

Hi,Sir/Madam.
We have upgraded the remote access software.
Please login to the system to update your software,and then type in your password.

Login:
https://system.victim.com/vpn/index.html

For more information,please contact me.

Best regards.

Case Study: Recent PII Theft By China-based Threat Actors

- Over the past year, Chinese threat actors have stolen personal information in bulk from global healthcare, travel, and government organizations
- Some organizations were hacked by multiple threat actors at the same time
- One threat actor breached multiple healthcare companies within a few days of each other
- The attackers continuously accessed the victims networks using a combination of backdoors and the victims' VPN solutions
- Very few systems with backdoors, yet hundreds of systems accessed by the attacker
- Some systems with evidence of data theft were not infected with malware
- Many of the victims didn't know about the breach for several months until they were notified of the compromise by Mandiant

Trend 3: Attacks on Networking Devices

There are numerous reasons why threat actors may target network infrastructure, given the critical role these devices play in a network. Some examples are:

- Traffic Monitoring
- Reconnaissance
- Subversion of Security Controls
- Persistence
- Disruption

Trend 3: Attacks on Networking Devices

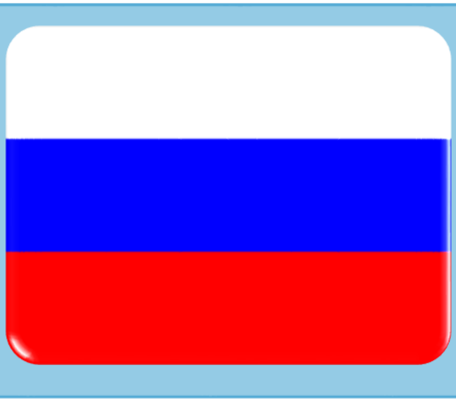
Modification of Cisco Router Images

Cross-Site Scripting a Cisco ASA VPN Concentrator

Cisco IOS Router Backdoors: SYNFUL Knock

Examples of significant attacks against networking infrastructure that Mandiant has observed recently

Key State Cyber Actors: Overview of Objectives



CHINA

Data theft to benefit Chinese companies

Advance Chinese military technologies

Protect the Chinese Communist Party

IRAN

Disrupt symbolic targets

Steal data to benefit military and energy decisions

RUSSIA

Intelligence collection against governments, militaries, and perceived opposition threats

Support military operations

NORTH KOREA

Information theft and disruption to protect the government’s image

Maintain military security

Considerations for Executives and the Board of Directors

Do we have the right strategy?

- How good do we want to be? How do we **define the win**?
- How often are cyber risks discussed by the **full board vs. the audit/risk committee**?

Do we have the right people and structure to be successful?

- Do we have **effective leadership** in place to manage our cyber risk? Do we have enough resources? Is the team empowered?
- Do we have the optimal **reporting structure** for our security organization?

Considerations for Executives and the Board of Directors

Do we have the right security capabilities?

- How well do we share, receive, and leverage **threat intelligence**? Are we able to learn from other security breaches?
- Do we have the capability to **know if we're compromised** without needing to be told by a third party?
- Do we have **pre-existing arrangements** with legal, technical, and public relations experts that we could leverage in the event of a major incident?

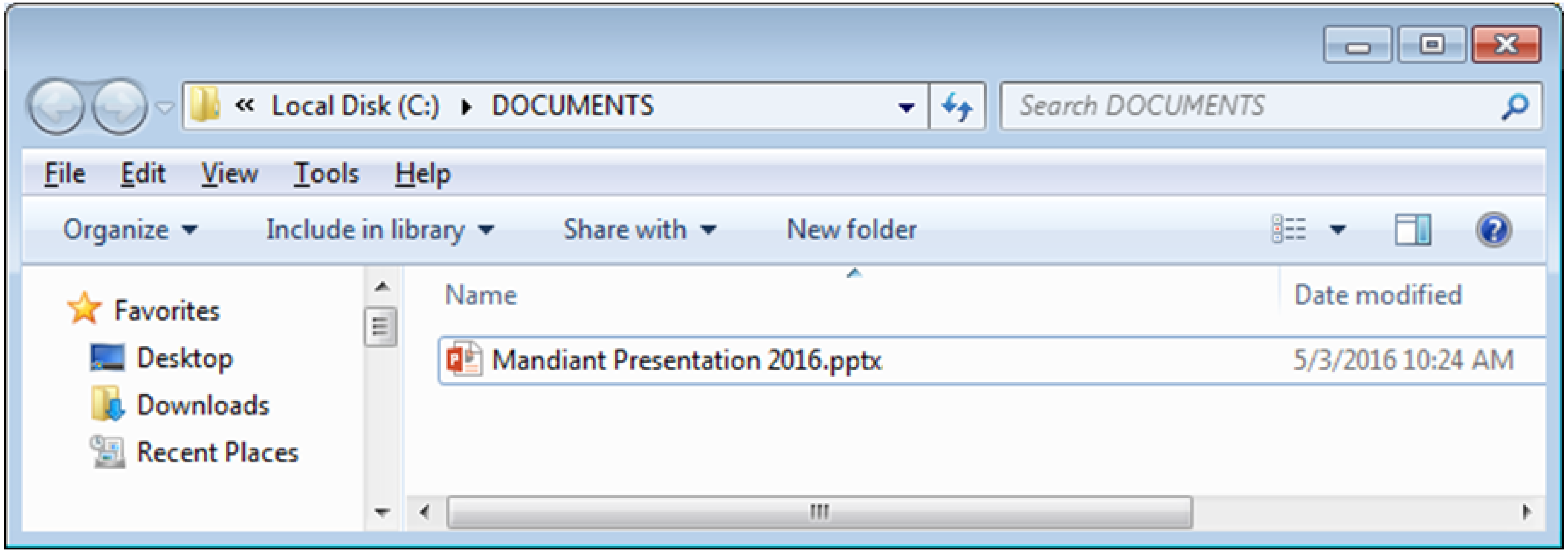
Do we have the right visibility?

- How mature are our processes to **detect and remediate security vulnerabilities**? Where are our blind spots?
- How effectively do we **monitor the environment** for attacks? Where are our blind spots?
- Are our **business partners** increasing our risk exposure? How do we embrace the **cloud** without increasing risk?

Industry Leading Practices

- Identification and protection of our most **critical assets**
- Annual "**red teaming"** of environments (internal and external networks, social engineering, and web applications)
- Requiring **dual factor authentication** on all remote access (VPN, Citrix, Terminal Services, and webmail)
- Deployment of **application whitelisting technology** to critical assets (domain controllers, mail servers, file servers, etc.)
- **Network compartmentalization** of critical assets and data
- Limit access to **system backups** to prevent intentional destruction
- Deployment of **advanced malware detection/prevention** technology at the perimeter (web and email)
- Searching for host and network-based **indicators of compromise** on a periodic basis
- Inventorying **service accounts** and resetting passwords on a periodic basis

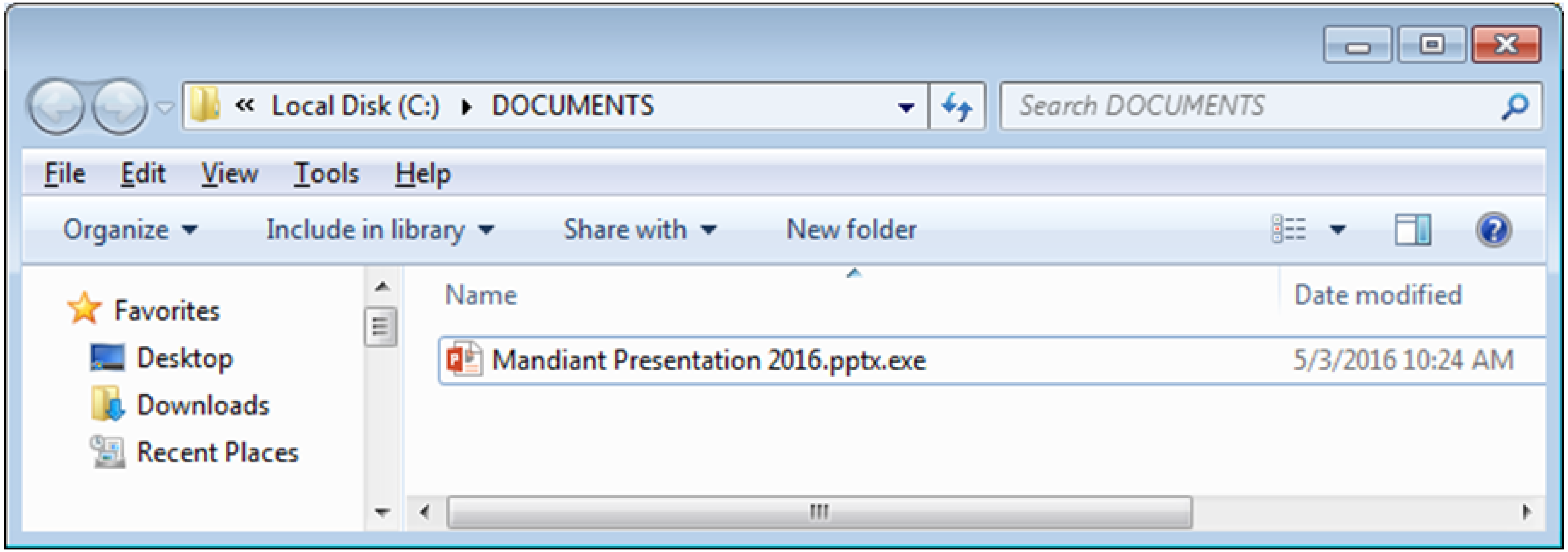
Pop Quiz - What type of file is this?



Mandiant Presentation 2016.pptx 5/3/2016 10:24 AM

1. Microsoft Word
2. Microsoft Excel
3. Microsoft PowerPoint
4. Adobe Acrobat

Pop Quiz - What type of file is this?


« Local Disk (C:) ▸ DOCUMENTS
Search DOCUMENTS
File Edit View Tools Help
Organize ▾ Include in library ▾ Share with ▾ New folder
Favorites
Desktop
Downloads
Recent Places
Name
Date modified

Mandiant Presentation 2016.pptx.exe 5/3/2016 10:24 AM

1. Microsoft Word
2. Microsoft Excel
3. Microsoft PowerPoint
4. Adobe Acrobat
5. **Executable File**

Reminder: Windows hides known file types by default

QUESTIONS?

Charles Carmakal
Vice President
charles.carmakal@mandiant.com
864-735-7242