

INFORMATION TECHNOLOGY SERVICES



METROPOLITAN STATE UNIVERSITY™
OF DENVER

EMOTET Incident Response

- Introductions
- Events leading up to incident
- Events of June 18
- Scope and impacts
- Mitigating factors
- Lessons learned
- Continuing efforts and future plans

Introductions

- Ben LeDoux
- Mike Hart
- IT Services

My First Real Job



Incident Summary

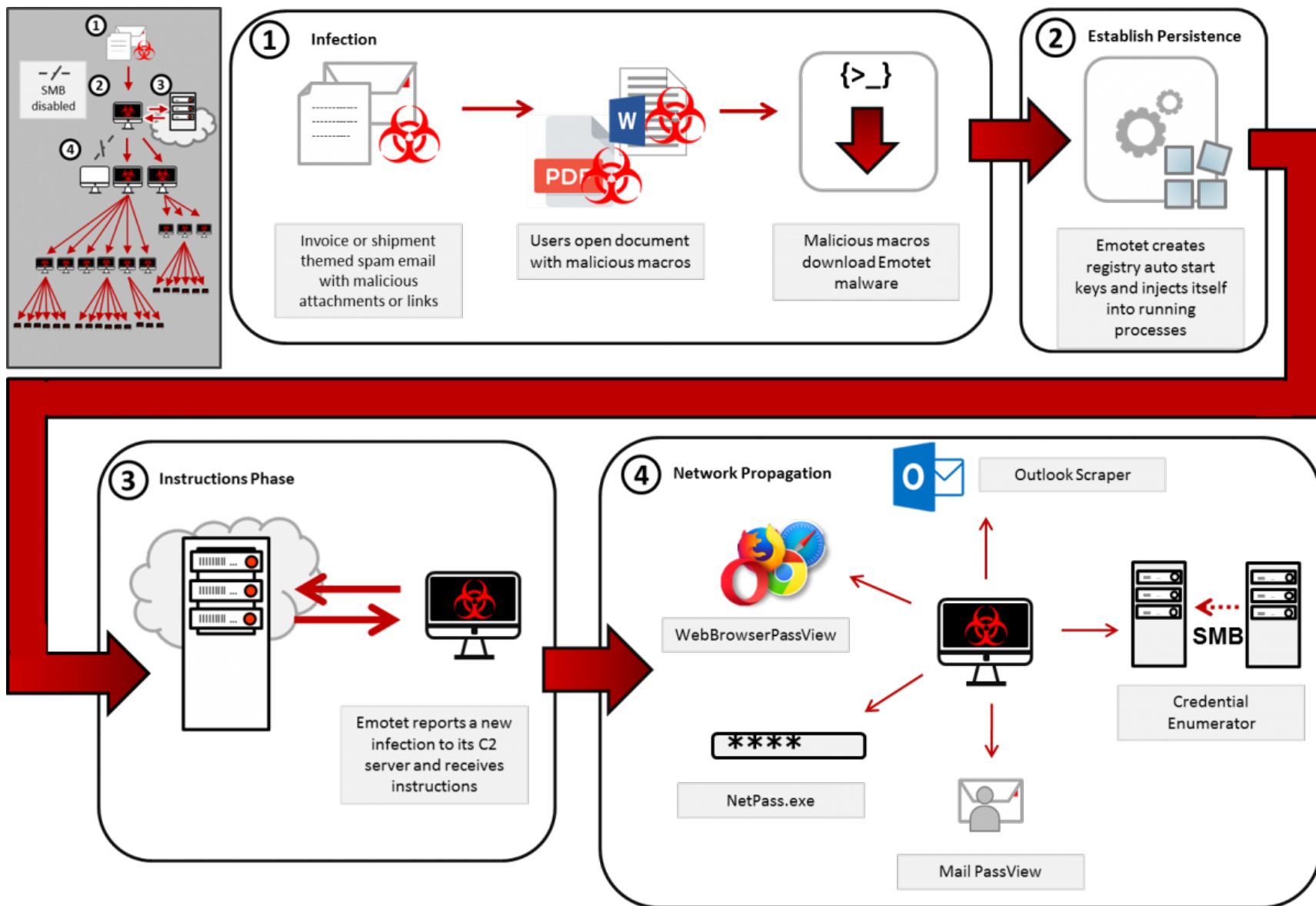
- June 18th, 2018 – Emotet Incident
- Scope of Incident
- Overall Impact

Events Leading Up to Incident

- Seasonal uptick in phishing
- Phishing was better targeted
- OSINT was used for targeting

EMOTET Lifecycle

<https://www.cisecurity.org/white-papers/ms-isac-security-primer-emotet/>



Examples of Artifacts

<https://www.cisecurity.org/white-papers/ms-isac-security-primer-emotet/>

- **Example Filenames and Paths:**

- C:\Users\<username>\AppData \Local\Microsoft\Windows\shedaudio.exe
- C:\Users\<username>\AppData\Roaming\Macromedia\Flash Player\macromedia\bin\flashplayer.exe

- **Typical Registry Keys:**

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

- **System Root Directories:**

- C:\Windows\11987416.exe
- C:\Windows\System32\46615275.exe
- C:\Windows\System32\shedaudio.exe
- C:\Windows\SysWOW64\f9jwqSbS.exe

Initial Indicators of Compromise

```

"action": "ACCOUNT_LOCKED", "source_account":
  nsudnver.edu", "action": "ACCOUNT_LOCKED",
denver.edu", "action": "ACCOUNT_LOCKED", "source_account":
er.edu", "action": "ACCOUNT_LOCKED", "source_account": "
  nsudnver.edu", "action": "ACCOUNT_LOCKED",
  nsudnver.edu", "action": "ACCOUNT_LOCKED", "source
", "action": "ACCOUNT_LOCKED", "source_account":
  nsudnver.edu", "action": "ACCOUNT_LOCKED", "source
du", "action": "ACCOUNT_LOCKED", "source_account":
", "action": "ACCOUNT_LOCKED", "source_account":
er.edu", "action": "ACCOUNT_LOCKED", "source_account": "
er.edu", "action": "ACCOUNT_LOCKED", "source_account": "
.edu", "action": "ACCOUNT_LOCKED", "source_account":
denver.edu", "action": "ACCOUNT_LOCKED", "source_account
.edu", "action": "ACCOUNT_LOCKED", "source_account":
.edu", "action": "ACCOUNT_LOCKED", "source_account":
"action": "ACCOUNT_LOCKED", "source_account":
du", "action": "ACCOUNT_LOCKED", "source_account":

```

Lateral Movement - Domain Credentials | LATERAL MOVEMENT

User attempted to remotely access 4 new assets

Lateral Movement - Domain Credentials | LATERAL MOVEMENT











User attempted to remotely access 5 new assets

Lateral Movement - Domain Credentials | LATERAL MOVEMENT

User attempted to remotely access 5 new assets

Lateral Movement - Domain Credentials | LATERAL MOVEMENT

User attempted to remotely access 28 new assets

<input type="checkbox"/>  High	TACTIC & TECHNIQUE Defense Evasion via Process... 
<input type="checkbox"/>  Medium	TACTIC & TECHNIQUE Execution via Command-Lin... 
<input type="checkbox"/>  High	TACTIC & TECHNIQUE Defense Evasion via Process... 
<input type="checkbox"/>  Low	TACTIC & TECHNIQUE Machine Learning via Adwar... 
<input type="checkbox"/>  High	TACTIC & TECHNIQUE Exploit via Exploit Mitigation 

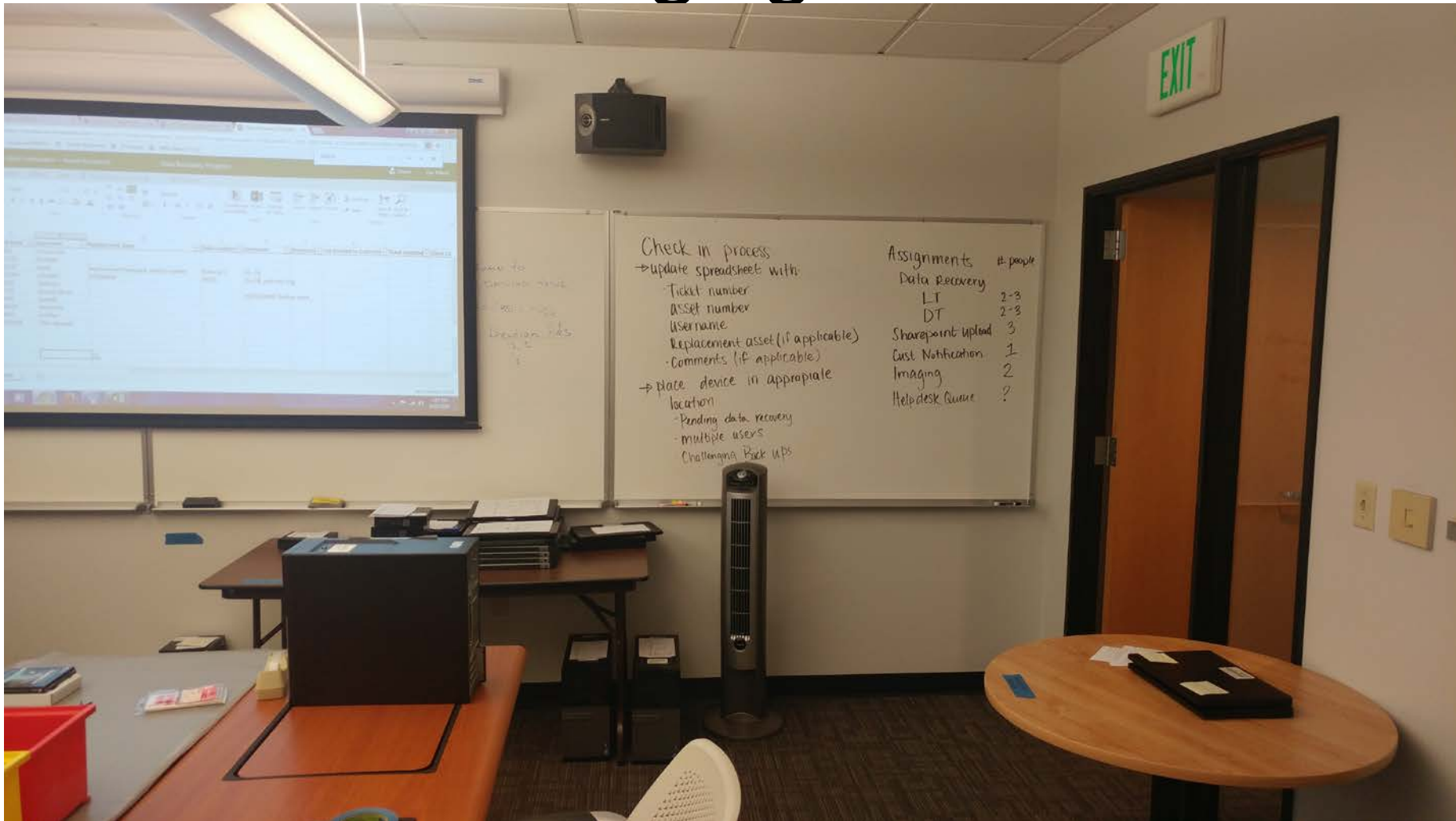
Timeline of Events

- Monday June 18th
 - Initial infection 11:04am
 - Symptoms detected 11:15am
 - Malware confirmed 11:20am
 - Administration building isolated 11:30am
 - Engaged with incident response partner 1pm
 - Removed administrative privileges 1:10pm
 - Updated malware signatures released 3pm
 - Advance endpoint protection pushed to ITS 7pm

Timeline of Events – Continued

- IT Services begins re-imaging 6/19
- Wireless network isolation 6/19
- Incident response partner meeting 6/19
- Administration building networks normalized at 12:15pm 6/20
- Majority of re-imaging work completed Saturday, 6/23

Re-imaging Room



Re-imaging Room



Re-imaging Room



Assessment

- Impacts
- Lessons learned
- We got *lucky*?

What has ITS Been Doing?

- Next Generation tools for threat mitigation
- Vulnerability scanning and assessments
- Device protection and encryption
- Regular patching of devices and software
- Backups and testing of restores
- REN-ISAC, MS-ISAC, Educause, and other peer groups
- Security awareness messaging – early bird, newsletters, spring fling and fall fest

Ongoing and Future Activities

- Implementation of new tools and services
- Cyber Security Insurance
- New security awareness training videos
- Changing our public facing posture
- Network Architecture Changes
- Systems Operations Center

THANK YOU

- Questions?