ATT&CK™

TRAM:

An Easier Way to Map to ATT&CK

Jackie Lasky

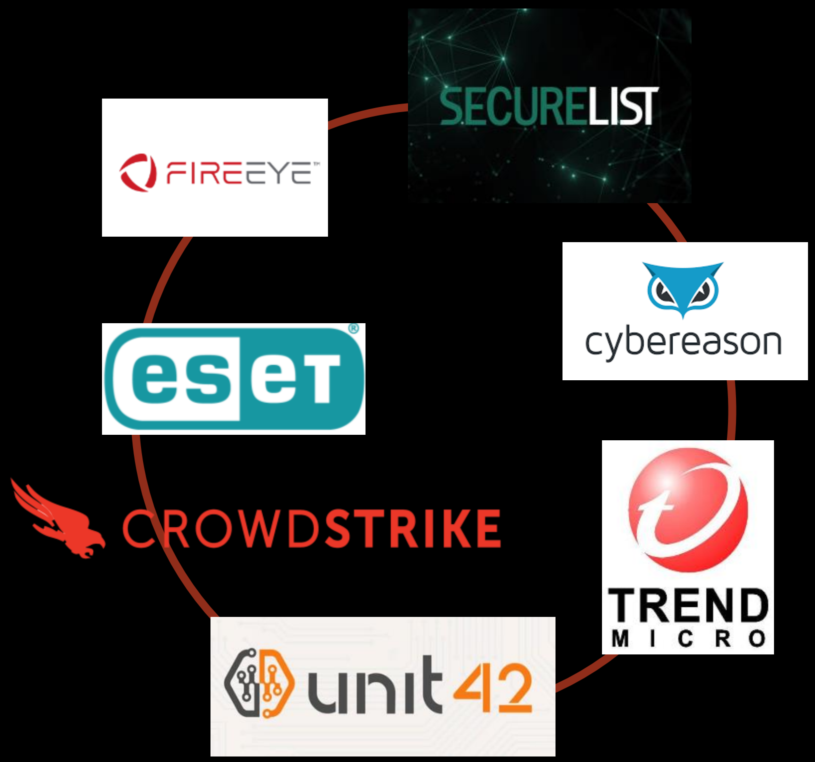
Sarah Yoder
@sarah__yoder

@MITREattack #ATTACKcon

MITRE

How Does Information Get into ATT&CK?

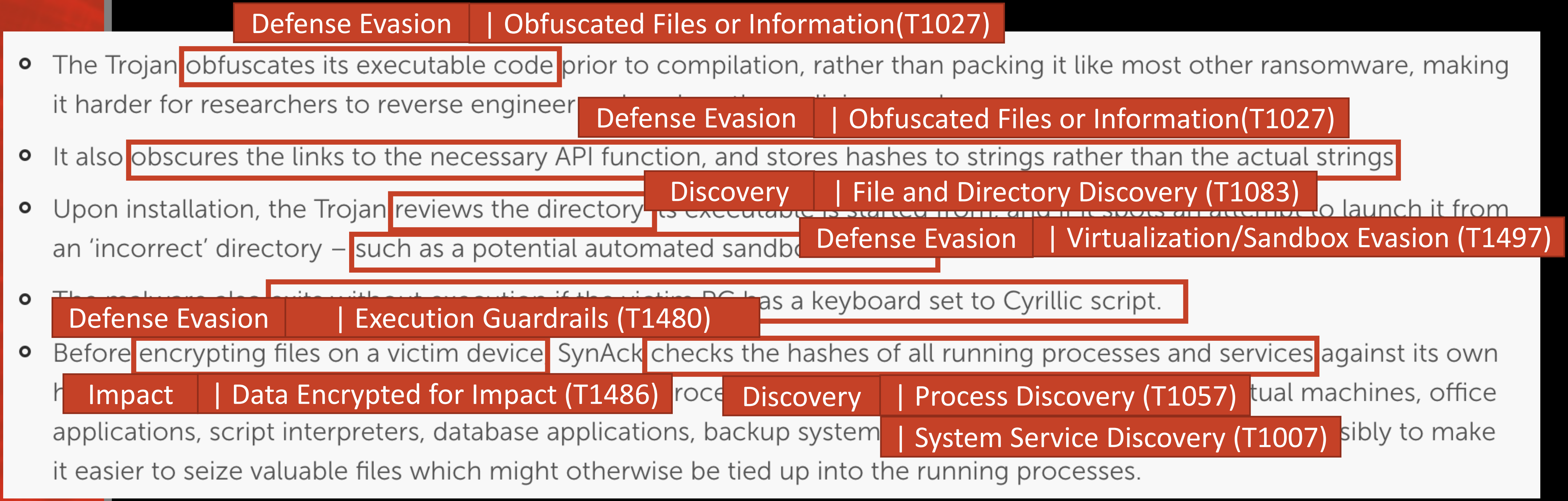
1. Find reliable open source reporting



2. Find behaviors in the report

- Think ATT&CK structure
  - Tactic (Why)
  - Technique (How)
  - Procedure (What)

Finding Behaviors in Finished Reporting



Defense Evasion | Obfuscated Files or Information(T1027)

- The Trojan obfuscates its executable code prior to compilation, rather than packing it like most other ransomware, making it harder for researchers to reverse engineer

Defense Evasion | Obfuscated Files or Information(T1027)

- It also obscures the links to the necessary API function, and stores hashes to strings rather than the actual strings

Discovery | File and Directory Discovery (T1083)

- Upon installation, the Trojan reviews the directory its executable is started from, and if it spots an attempt to launch it from an 'incorrect' directory – such as a potential automated sandb

Defense Evasion | Virtualization/Sandbox Evasion (T1497)

- The malware also quits without execution if the victim PC has a keyboard set to Cyrillic script.

Defense Evasion | Execution Guardrails (T1480)

- Before encrypting files on a victim device SynAck checks the hashes of all running processes and services against its own h roce tual machines, office applications, script interpreters, database applications, backup system sibly to make it easier to seize valuable files which might otherwise be tied up into the running processes.

Impact | Data Encrypted for Impact (T1486)

Discovery | Process Discovery (T1057)

| System Service Discovery (T1007)

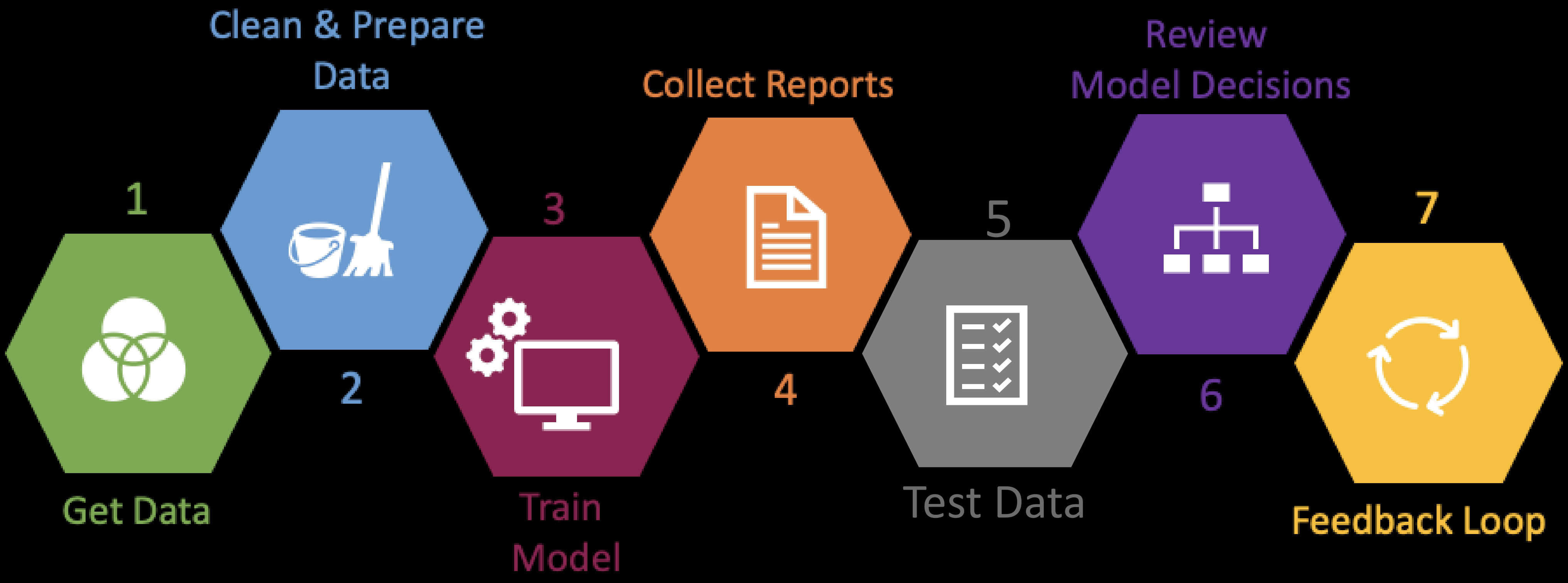
https://usa.kaspersky.com/about/press-releases/2018_synack-doppelganging

The Problem

- **Too many reports, not enough people!**
  - ATT&CK is updated manually
  - Backlog of unanalyzed reports
- **Human error**
  - Potential for inaccurate information
  - Availability bias
- **Training new team members**
  - Analysis process is complex
  - Takes time to learn ATT&CK

Our Solution: Threat Report ATT&CK Mapper (TRAM)

TRAM Under the Hood



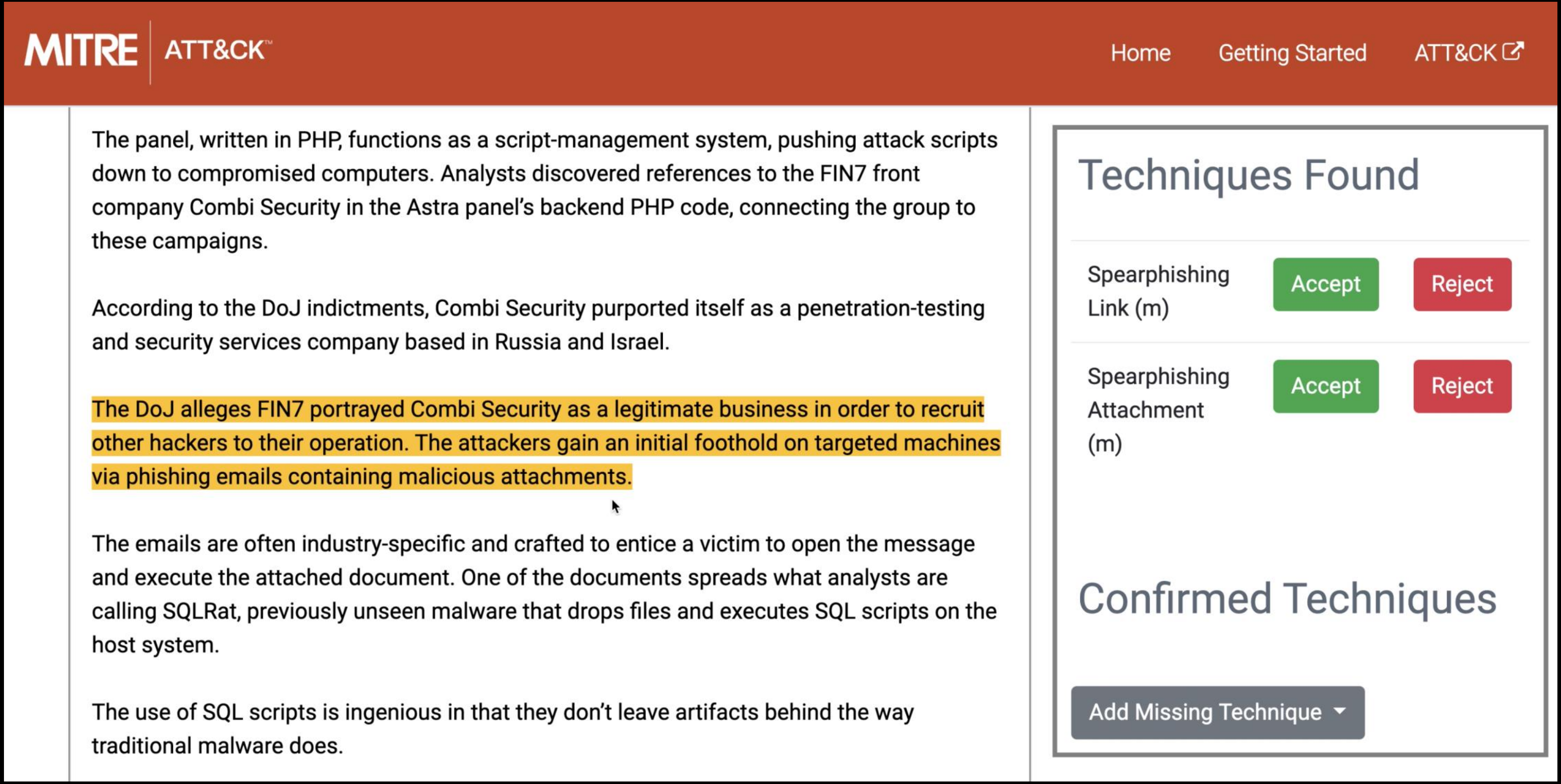
ATT&CK™

MITRE

Challenges

- **Extracting meaning from text is hard**
- **Handling prediction error**
  - Noise in data
  - Anomalies
  - Differentiating between similar techniques
- **Needing more data**
  - Imbalanced datasets
  - Lots of false positives
- **Creating a backup plan for techniques with no data**
  - Regular expressions
  - String matching

TRAM "Demo"



The panel, written in PHP, functions as a script-management system, pushing attack scripts down to compromised computers. Analysts discovered references to the FIN7 front company Combi Security in the Astra panel's backend PHP code, connecting the group to these campaigns.

According to the DoJ indictments, Combi Security purported itself as a penetration-testing and security services company based in Russia and Israel.

The DoJ alleges FIN7 portrayed Combi Security as a legitimate business in order to recruit other hackers to their operation. The attackers gain an initial foothold on targeted machines via phishing emails containing malicious attachments.

The emails are often industry-specific and crafted to entice a victim to open the message and execute the attached document. One of the documents spreads what analysts are calling SQLRat, previously unseen malware that drops files and executes SQL scripts on the host system.

The use of SQL scripts is ingenious in that they don't leave artifacts behind the way traditional malware does.

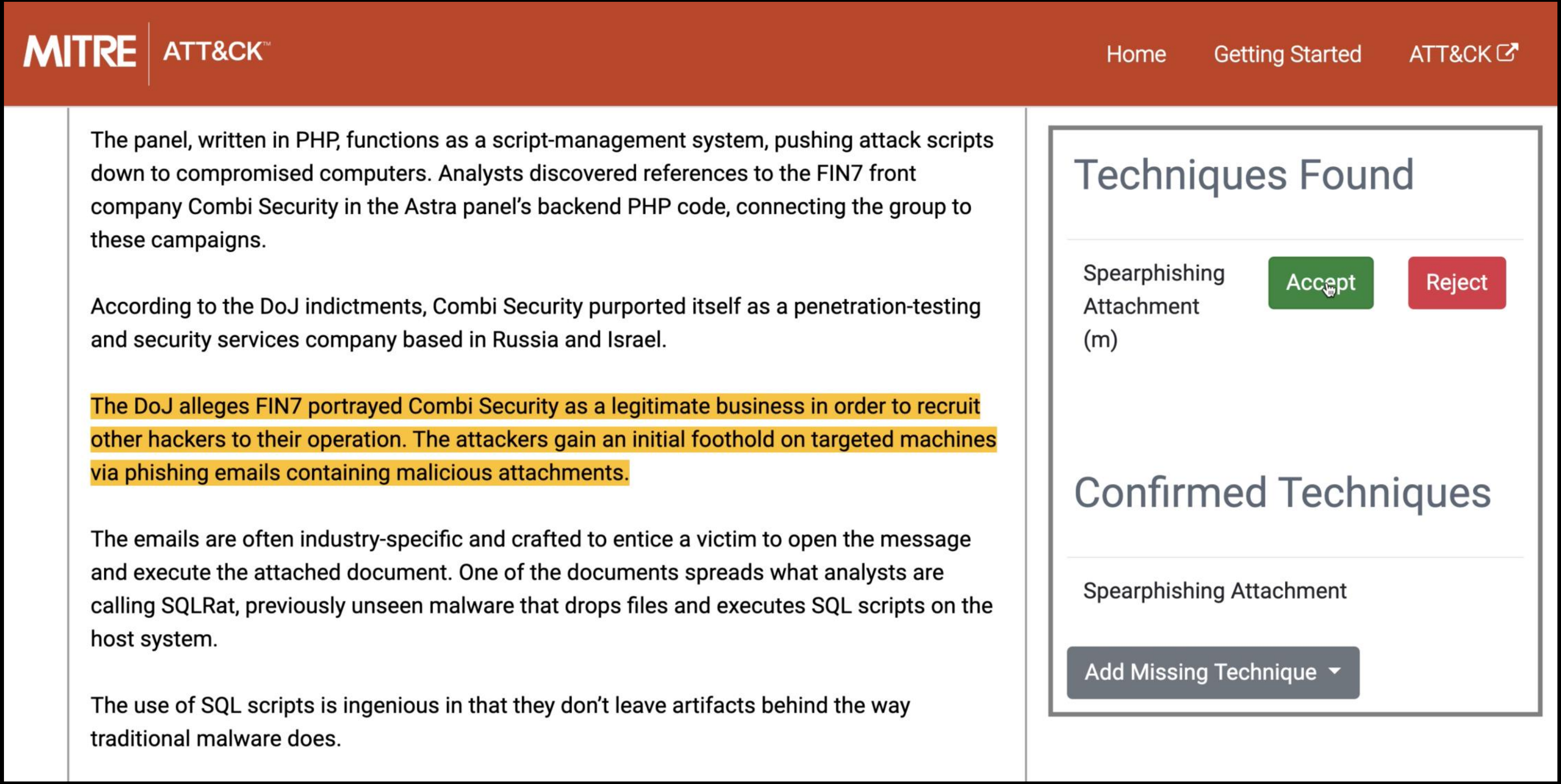
Techniques Found

Spearphishing Link (m) Accept Reject

Spearphishing Attachment (m) Accept Reject

Confirmed Techniques

TRAM "Demo"



The panel, written in PHP, functions as a script-management system, pushing attack scripts down to compromised computers. Analysts discovered references to the FIN7 front company Combi Security in the Astra panel's backend PHP code, connecting the group to these campaigns.

According to the DoJ indictments, Combi Security purported itself as a penetration-testing and security services company based in Russia and Israel.

The DoJ alleges FIN7 portrayed Combi Security as a legitimate business in order to recruit other hackers to their operation. The attackers gain an initial foothold on targeted machines via phishing emails containing malicious attachments.

The emails are often industry-specific and crafted to entice a victim to open the message and execute the attached document. One of the documents spreads what analysts are calling SQLRat, previously unseen malware that drops files and executes SQL scripts on the host system.

The use of SQL scripts is ingenious in that they don't leave artifacts behind the way traditional malware does.

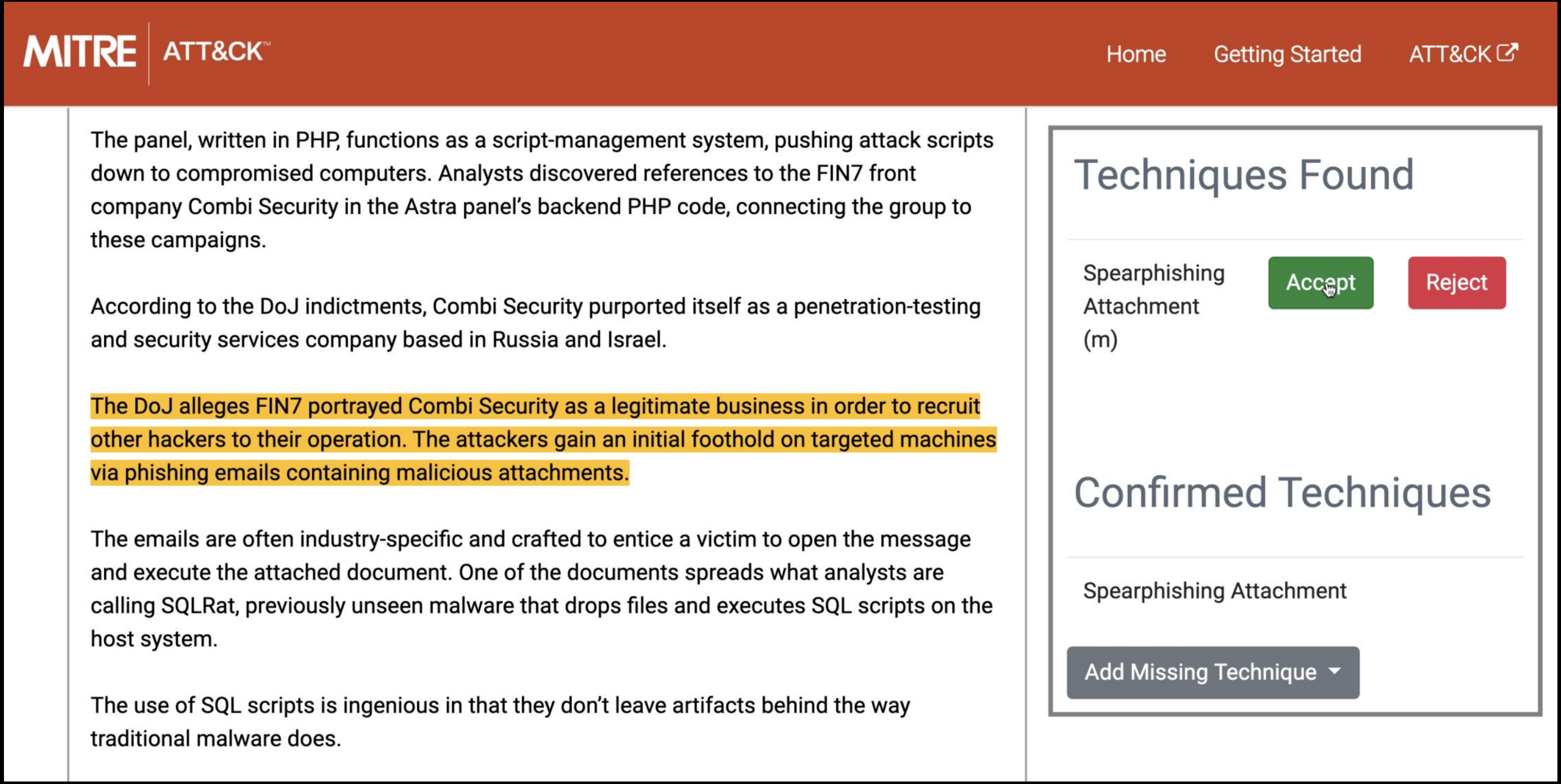
Techniques Found

Spearphishing Attachment (m)

Confirmed Techniques

Spearphishing Attachment

TRAM “Demo”



The panel, written in PHP, functions as a script-management system, pushing attack scripts down to compromised computers. Analysts discovered references to the FIN7 front company Combi Security in the Astra panel’s backend PHP code, connecting the group to these campaigns.

According to the DoJ indictments, Combi Security purported itself as a penetration-testing and security services company based in Russia and Israel.

The DoJ alleges FIN7 portrayed Combi Security as a legitimate business in order to recruit other hackers to their operation. The attackers gain an initial foothold on targeted machines via phishing emails containing malicious attachments.

The emails are often industry-specific and crafted to entice a victim to open the message and execute the attached document. One of the documents spreads what analysts are calling SQLRat, previously unseen malware that drops files and executes SQL scripts on the host system.

The use of SQL scripts is ingenious in that they don’t leave artifacts behind the way traditional malware does.

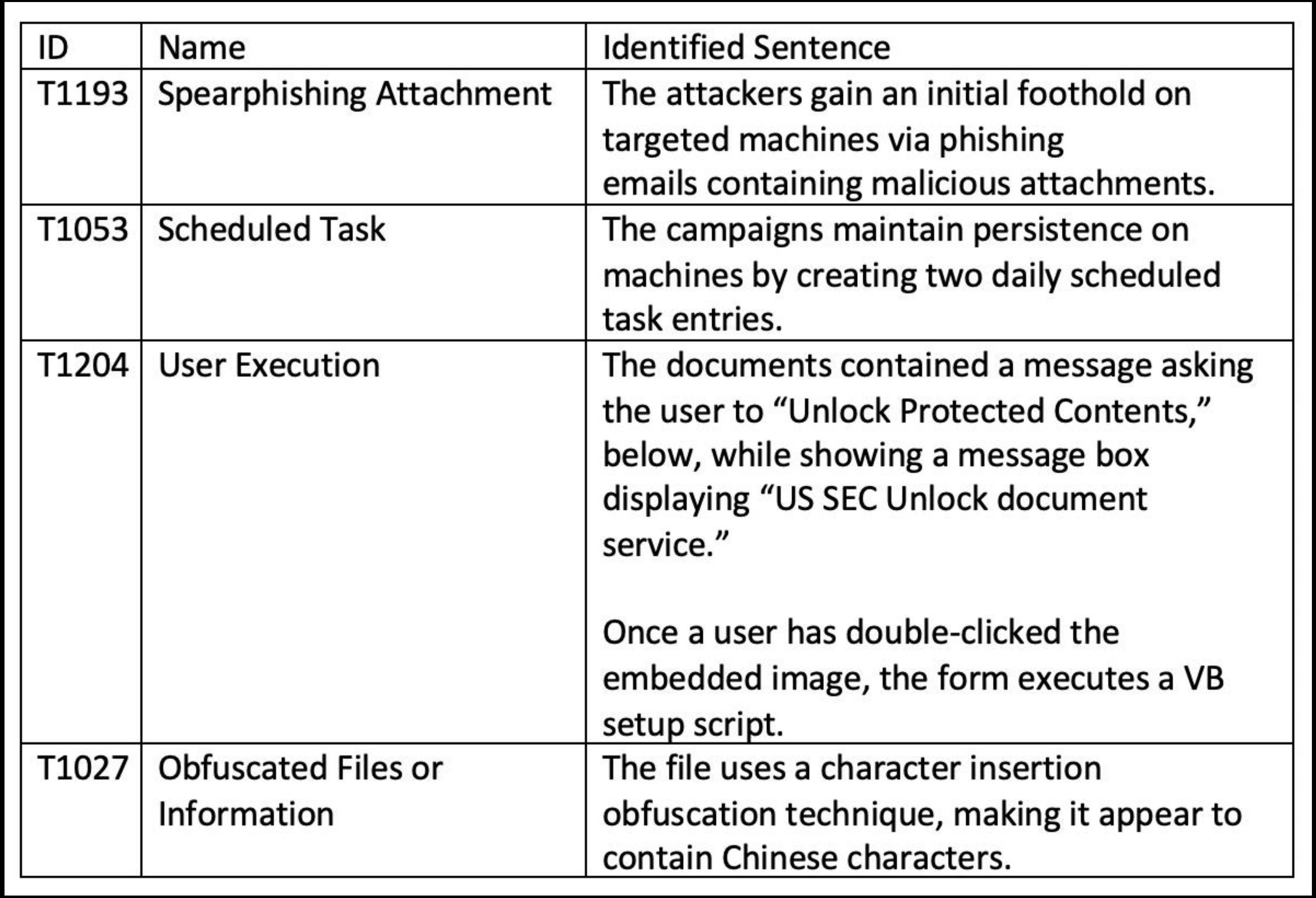
Techniques Found

Spearphishing Attachment (m)

Confirmed Techniques

Spearphishing Attachment

TRAM “Demo”



ID	Name	Identified Sentence
T1193	Spearphishing Attachment	The attackers gain an initial foothold on targeted machines via phishing emails containing malicious attachments.
T1053	Scheduled Task	The campaigns maintain persistence on machines by creating two daily scheduled task entries.
T1204	User Execution	The documents contained a message asking the user to “Unlock Protected Contents,” below, while showing a message box displaying “US SEC Unlock document service.” Once a user has double-clicked the embedded image, the form executes a VB setup script.
T1027	Obfuscated Files or Information	The file uses a character insertion obfuscation technique, making it appear to contain Chinese characters.

Why Does This Matter?

- **Make it easier to get started with ATT&CK**
  - We know mapping reports to ATT&CK can be overwhelming
- **Find techniques we forget about or have never heard of**
  - Remembering 266+ techniques is hard!
- **Use reporting that is important to you**
  - We try to stay up to date, but new information comes out faster than we can say ATT&CK

Takeaways

- **Understand adversary TTPs**
  - ATT&CK helps frame these behaviors
  - You can then write detections, assess where your gaps are, track adversaries you care about, and emulate those adversaries
- **Mapping data to ATT&CK is hard**
- **TRAM hopes to make that easier**
  - NLP + SQL + regex + ATT&CK = ☺
  - Available to the community soon!

Jackie Lasky

Sarah Yoder
@sarah__yoder

ATT&CK™

attack@mitre.org
@MITREattack
#ATTACKcon