© 2026 Roberto Dillon (https://adsumsoft.nicepage.io) - V. 2.0

CYBER CHAIN - *Real Hackers Don't Guess. Neither Will You.*

Introduction

Cyber Chain challenges you to build realistic cyber-attack chains representative of well-known cybersecurity incidents. Each chain is a set of 3 cards: a **Target**, a **Vector**, and a **Threat Actor**.

Playable solo or head-to-head, the game emphasizes hand management over luck. Aim of the game is to build logical chains where a particular threat actor uses a relevant vector to compromise a target matching their goals. Build an actual historical attack, and you will earn bonus points.

Games may last from 5 minutes (solo) to 10 minutes (two-player) for a quick and enjoyable experience. And you will also learn about real cybersecurity events and threats along the way!

Game Contents

The game includes 18 different cards, divided into 3 groups (**Targets, Attack Vectors, Threat Actors**) plus a special card. Specifically:

Targets (5 blue cards)



Each target card identifies a broad category (top) as well as a specific target that was breached in a famous cyber-attack (bottom).

Specific Target	Category
Colonial Pipeline	Infrastructure
Sony Pictures Entertainment	Media
Iranian Nuclear Program	Nation State
SolarWinds	Industry/Global Disruption
Ukrainian Power Grid	Energy

Attack Vectors (6 red cards)

Each card represents a common approach hackers use to attack specific targets. Each one has a specific purpose and was used in many famous and historical hacks, including the ones referenced in the cards themselves.













Vector	Purpose	Historical Hack
Ransomware	Lock PCs and Encrypt data till ransom is paid. Common in cybercrime.	Colonial Pipeline
Wiper malware	Destroy data. Common in cybercrime and also in cyberwarfare operations to damage targets.	Sony Pictures
Zero-day exploit	Exploit a new vulnerability. Common in Espionage and Cyberwarfare.	Ukraine Power Grid
Spear Phishing	Targeted email attacks. Very common in cybercrime to cheat employees in sharing sensitive information.	*Too many to list!*
Supply Chain Attack	Common in cybercrime to attack a target by exploiting vulnerabilities in related software applications, libraries, and services.	SolarWinds
USB worm	Used in espionage and cyberwarfare to attack computers not connected to the Internet (“air-gapped”)	Iranian Nuclear Program

Threat Actors (6 green cards)

These cards identify specific hacking groups, each with their modus operandi and goals.



Threat Actors are broadly divided into two main categories: Cybercriminal Hacking Groups, mainly interested in financial gain, and Intelligence Units, mainly interested in espionage and disruption of opposing parties.

Threat Actor	**Category**	**Famous Hacks they were involved in**
DarkSide	Cybercriminal Hacking Group	Colonial Pipeline
Lazarus Group	Cybercriminal Hacking Group	Sony Pictures
Unit 8200	Intelligence unit	Iranian Nuclear Program
Sandworm	Intelligence unit	Ukrainian Power Grid
Scattered Spider	Cybercriminal Hacking Group	*Lots of retail and gaming industry hacks*
Cozy Bear	Intelligence Unit	SolarWinds

Reconfigurator Wild card (1 card)



Remove one Vector or Threat Actor card in a chain of your choice.

GAME SETUP (Solo or 2-Player)

1. Separate the 5 Target cards. Shuffle them, draw 3 face-up in the center of the playing area. Return the other 2 to the box.
2. Shuffle the remaining 13 cards (6 Vectors + 6 Actors + Wild card) into the **Draw Deck** (face down).
3. Deal **2 cards** to each player's hand.
4. **2-Player mode: Players share the Targets and alternate turns trying to complete each attack chain**. Players can decide who goes first in any way the prefer (e.g. toss a coin, play a round of rock-paper-scissors, alternate each other across multiple rounds etc.)

GAME OBJECTIVE and HOW TO PLAY

The game ends when all 3 Target sequences are completed (matching one suitable Vector + Actor per Target) or when the Draw Deck runs out and **no further cards can be played**.

Each Target chain can have **only one Vector and one Actor** total.

Points are awarded to the player who completes a chain:

- A generic but realistic chain sequence scores **1 point**. This is any combination where:

  Target category matches the Vector plausibility (e.g.: Energy target + Ransomware by a cybercriminal to extort money, or + USB worm to gain access

to specific air-gapped resources by an intelligence unit). Note how the choice of Vector defines possible Actors accordingly.

Most Vectors can be played on most targets (in a head-to-head game, a player should be able to justify his choice if questioned by the other player) but there are exceptions:

- the USB Worm is **not** suitable for Media related attacks as this technique implies offline targets more common in nation state or highly sensitive energy/infrastructure attack scenarios.
- Ransomware is **not** suitable for espionage and cyberwarfare operations as this is a tool for financial extorsion and not for intelligence gathering.

Hence, to correctly complete a chain, the **Threat Actor must be chosen to match the specific Vector intent**:

- Ransomware → Cybercriminal actors
- Wiper/Zero-day → Any actor
- Phishing → Any actor
- Supply chain → Any actor
- USB worm → Intelligence units

Sequences that mismatch elements in the chain (e.g. an Intelligence Unit threat actor using Ransomware) are illegal and cannot be played.

In other words:

A “Plausible” sequence means that:

  - Media can only be attacked by financially motivated actors, i.e. hacking groups.
  - Nation State can only be attacked by Intelligence units.
  - Energy, Infrastructure, and Global Disruption can be targeted by either hacking groups or intelligence units.
  - Ransomware can only be used by hacking groups
  - USB worm can only be used by intelligence units.

- A completed historical sequence among the following scores **3 points**:

Target	Vector	Actor	Historical Significance
Colonial Pipeline	Ransomware	DarkSide	In 2021, a ransomware attack forced the largest fuel pipeline in the United States to shut down for nearly a week. The criminal group DarkSide broke into Colonial's billing system through a compromised password, then deployed ransomware that paralyzed the company's computers. Colonial paid roughly $4.4 million to restore operations, though authorities later recovered part of the payment. The incident revealed how a single weak password could threaten a nation's fuel supply.
Sony Pictures	Wiper malware	Lazarus Group	In 2014, a cyberattack linked to North Korea's Lazarus Group (aka Guardians of peace) destroyed thousands of Sony's computers and leaked unreleased films, embarrassing emails, and employee data. The attackers used a wiper malware called Shamoon to erase hard drives, then demanded Sony cancel the comedy film *The Interview*, which depicted the fictional assassination of North Korea's leader. Sony suffered over $100 million in damages.
Iranian Nuclear Program	USB worm	Unit 8200	Between 2009 and 2010, Stuxnet, a sophisticated digital weapon later attributed to Unit 8200 (an Israeli intelligence unit) working with the United States, sabotaged Iran's uranium enrichment centrifuges. The Stuxnet worm spread via infected USB drives, then quietly reprogrammed the centrifuges to spin out of control and destroy themselves while displaying normal readings to Iranian operators. It was the first known cyberweapon designed to cause physical destruction.
SolarWinds	Supply chain attack	Cozy Bear	In 2020, Cozy Bear, a Russian state-linked group, infiltrated thousands of organizations worldwide by hiding malicious code inside a routine software update for SolarWinds' Orion platform. The backdoored update affected over 18,000 customers, including nine US federal agencies (Treasury, Homeland Security, Commerce, etc.) and top cybersecurity firms like FireEye. For nine months, the attackers quietly spied on emails, source code, and internal systems before being discovered. The incident highlighted the devastating power of a supply chain attack, where a single trusted vendor becomes an unwitting weapon against its own customers.
Ukrainian Power Grid	Zero-day exploit	Sandworm	In 2015 and 2016 Russian-linked hackers from Sandworm and Fancy Bear hacking groups caused blackouts by remotely breaching Ukraine's electricity distribution centers. Using zero-day exploits (i.e. previously unknown vulnerabilities) they gained access to control systems and switched them off. This was the world's first known cyberattack on a power grid to cause a blackout, proving that critical infrastructure could be targeted remotely to support warfare operations.

- Incomplete sequences **score 0**.

TURN STRUCTURE (Solo or 2-Player)

On your turn, do **only one** among these actions:

A. Play a card matching an empty Target Vector slot

- Play a Vector from hand onto a Target with no Vector yet.
- Must be historically accurate (exact match) or plausible.
- Then draw 1 card from Deck.

B. Play an Actor card onto a Target that already has a Vector

- Play a Threat Actor from hand onto a Target that has a Vector but no Actor yet to compete a chain.
- Check match:
    - If [Target + Vector + Actor] matches a Historical Sequence → 3 points..
    - Else if plausible → 1 point when completed.
    - If not plausible → illegal play (cannot do it).
- Then draw 1 card.

C. If you have the Reconfigurator card (wild card), you can:

- Play it to remove one Vector or Actor of your choice.
- If disrupting a completed chain, previously awarded points remain, and a new chain can be created awarding additional points in the following rounds.
- Discard the wild card and draw 1 new card.

D. Discard up to 2 cards from your hand

- Place them face-down in a Discard Pile.
- Draw back a corresponding number of cards, if available.
- **Cards cannot be discarded in two consecutive turns**. I.e.: if you discarded card(s) in this turn, in the next turn you cannot discard cards again and must play a card instead. If no legal card can be played, your turn is over, and you have to wait for the following turn to discard your current cards. **In a solitaire game, the game is over.**

Then the turn passes to the other player (or in solo, continue).

ENDING THE GAME

The game ends when no more cards can be played. I.e.:

- All Target chains are completed (Vector + Actor on all 3 Targets), and players have no wild card in their hands that can be played.
- The Draw Deck is empty, and players cannot play any card,

Players count points from their **completed sequences only**. Higher score wins. Ties are possible.

In Solo/Solitaire mode: try to score the highest number of points and complete all the historical matches.

SCORING EXAMPLE

Targets in play: Colonial Pipeline, Sony Pictures, Ukrainian Power Grid.

Player 1 builds:

- Colonial + Ransomware + DarkSide → **3 pts** (historical)
- Sony + Wiper + Lazarus → **3 pts** (historical)

Player 2 builds:

- Ukraine Power Grid + Zero-day + Sandworm → **3 pts** (historical)

Total = 9 points awarded, Player 1 wins 6 points to 3.

Generic example:

- Colonial Pipeline + Phishing + Lazarus (not historical, but plausible: Infrastructure target + phishing to gain access and exfiltrate data + cybercriminal) → **1 pt**
- Sony + Supply chain + Scattered Spider (not what happened historically, but still plausible as a cybercriminal actor may compromise a supply chain element to compromise a more valuable target → **1 pt**

Credits:

Game Design & Rulebook: Roberto Dillon