Zero Day (v0.5 2019-10-27)

Adapted from Pandemic™ by Mat Leacock, Z-Man Games

Do you have what it takes to save the Internet? As skilled members of a technical team, you must keep malicious software programs from spreading while developing and deploying patches for four previously unknown software vulnerabilities on a world-wide network of data centers, server, and workstations.

You and your teammates will connect to data centers across the globe, cleaning malware from systems while finding the resources to develop patches that prevent further spread and system failures. You must work together, using your individual strengths, to succeed. The clock is ticking as hackers launch new attacks, viruses spread, and new *Zero Day* vulnerabilities are discovered that fuel the spread of malicious software across the Internet.

Can you find the vulnerabilities and develop patches in time? The fate of the Internet is in your hands!

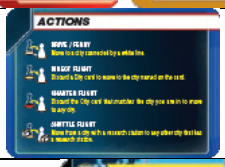
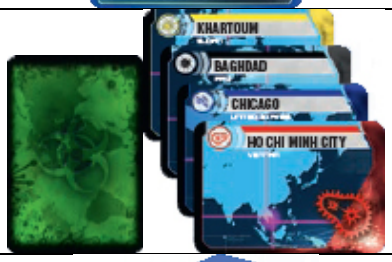
Pandemic™ Required

This game is based on Pandemic™ by Mat Leacock and at this time requires a copy of Pandemic™ to play. You will reuse most of the Pandemic components for this game with the following substitutions:

- 7 Role Cards: replace these with the Zero Day Role cards
- 59 Player cards (blue back cards)
  - 48 Data Center cards
  - 6 Epidemic cards: replace with the Zero Day Discovery cards
  - 5 Event cards: replace with the Zero Day Event cards
- 4 Reference cards: replace with Zero Day Reference cards
- 48 Infection cards (green back cards)
- 4 Cure markers: “Patch Markers” in Zero Day
- 1 Outbreaks marker: “Malware Outbreak” in Zero Day
- 6 Research Stations: “Secure Hosts” in Zero Day
- 96 Infection cubes (24 in 4 colors)
- 1 Infection rate marker
- 7 Pawns
- 1 Board

If you print the Zero Day components, it’s recommended to put the Pandemic™ cards in card sleeves, then slide the printed Zero Day cards into the sleeves in front of the cards they replace. Then, the cards are indistinguishable from the reverse side. Only Role cards and cards from the player deck have replacements. The Infection Deck is used as is from Pandemic™.

Contents (from Pandemic™)

7 Role Cards	
7 Pawns	
59 Player Cards (48 Data Center cards, 6 Zero Day Discovery cards, 5 Event cards)	
4 Reference Cards	
48 Infection Cards	
96 Malware Infection Cubes (24 in 4 colors)	
4 Patch markers (patched and eradicated side)	
1 Infection Rate marker	
1 Outbreaks marker	
6 Secure hosts	
1 Game Board	

Overview

In *Zero Day*, you and your fellow players are members of a technical team working to keep world-wide data centers online. You must work together to clean infected systems and develop patches for 4 previously unknown vulnerabilities (Blue, Yellow, Black, and Red) that computer malware (viruses, cryptocurrency miners, and crypto-malware) can use to infect and exploit systems and eventually take the entire Internet down

Zero Day is a cooperative game. The players all win or lose together.

The goal is to develop patches for all 4 vulnerabilities that allow the malicious software to spread. The players lose if:

- 8 Outbreaks occur (the Internet breaks down; all systems go offline).
- Not enough infection cubes are left when needed (malicious software spreads too much and is uncontrollable), or,
- Not enough player cards are left when needed (your team runs out of time).

Each player has a specific role with special abilities to improve the team's chances.

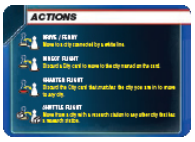
Setup

1. Set out the board and pieces
   Place the board within easy reach of all players. Put the 6 Secure Host and Infection Cubes nearby. Separate the cubes by color into 4 supply piles. Place 1 Secure Host in the Atlanta data center.

2. Place Outbreak and Patch Markers
   Place the Outbreak marker on the "0" space of the Outbreaks Track. Place the 4 Patch markers, "vial" side up, near the Patches Developed Indicators.

3. Place the Infection Rate marker and infect 9 cities
   Place the infection rate marker on the left-most "2" space of the Infection Rate Track. Shuffle the Infection Cards and flip over 3 of them. Put 3 Malware Infection cubes of the matching color on each of these data centers. Flip over 3 more cards; put 2 malware infection cubes on each of these data centers. Flip over 3 more cards; put 1 malware infection cube on each of these data centers. (You will place a total of 18 malware infection cubes, each matching the color of the data center). Place these 9 cards face up on the Infection Discard Pile. The other Infection cards form the Infection Deck.

4. Give each player cards and a pawn
   Give each player a reference card. Shuffle the Role cards and deal 1 face up in front of each player. Place the matching colored pawns for these roles in the Atlanta data center. Remove from the game the remaining Role cards and pawns.



   Take the Zero Day Discovery cards out of the Player Deck and set them aside until Step 5. Shuffle the other Player Cards (Data Center and Event Cards). Deal cards to the players to form their initial hands. Give cards according to the number of players:

Players	Cards
2	4
3	3
4	2

5. Prepare the Player Deck
   Set the game's difficulty level, by using either 4, 5, or 6 Zero Day Discovery cards, for an Introductory, Standard, or Heroic game. Remove any unused Zero Day Discovery cards from the game.

   Divide the remaining player cards into face down piles, as equal in size as you can, so that the number of piles matches the number of Zero Day Discovery cards you are using. Shuffle 1 Zero Day Discovery card into each pile, face down. Stack these piles to form the Player Deck, placing smaller piles on the bottom.

6. Begin Play
   The players look at the Data Center cards they have in their hand. The player with the most servers in their data center goes first (when using Pandemic cards, the number of servers is the population number).

Play

Each player turn is divided into 3 parts:

1. Do 4 actions.

2. Draw 2 Player Cards

3. Infect Data Centers

After a player is done infecting data centers, the player on their left goes next.

Players should freely give each other advice. Let everyone offer opinions and ideas. However, the player whose turn it is decides what to do.

Your hand can have Data Center and Event cards in it. Data Center cards are used in some actions and Event cards can be played at any time.

Actions

You may do up to 4 actions on each turn.

Select any combination of the actions listed below. You may do the same action several times, each time counting as 1 action. Your role's special abilities may change how an action is done. Some actions involve discarding a car from you hand; all these discards go to the Player Discard Pile.

Movement Actions

- Direct Connection -- (Drive / Ferry)
  Move to a data center connected by a white line to the one you are in.

- Secure Shell (SSH) Jump -- (Direct Flight)
  Discard a data center card to move to the data center named on the card.

- Reverse Connection -- (Charter Flight)
  Discard the data center card that matches the data center you are in to move to any data center.

- Secure Tunnel -- (Shuttle Flight)
  Move from a data center with a Secure Host to any other data center that has a Secure Host

Other Actions

- Install a Secure Host
  Discard the Data Center card that matches the data center you are in to place a secure host there. Take the secure host from the pile next to the board. If all 6 secure hosts have been installed, take a secure host from anywhere on the board.

  NOTE: If more than 6 secure hosts were supplied, set any extra aside during setup.

- Remove Malware

Remove 1 malware infection cube from the data center you are in, placing it in the cube supply next to the board. If this vulnerability color has been patched (see Develop a Patch below), remove all cubes of that color from the data center you are in.

If the last cube of a patched vulnerability is removed from the board, this vulnerability is *eradicated*. Flip its Patch marker from the "vial" side to the "not" side.

NOTE: If there are cubes from several patched vulnerabilities in a data center you must still Remove Malware once for each vulnerability color to remove those cubes.

NOTE: Eradicating malware is not needed to win. However, when data centers of an eradicated vulnerability are infected, no new malware infection cubes are placed there (see Zero Day Discovery and Infections). Removing the last cube of a vulnerability that has not been patched has no effect.

- Share Knowledge
  You can do this action in two ways:
  - Give the Data Center card that matches the data center you are in to another player, or
  - Take the Data Center card that matches the data center you are in from another player.

  The other player must also be in the data center with you. Both of you need to agree to this.
  If the player who gets the card now has more than 7 cards, that player must immediately discard a card or play an Event card (see Event Cards).

- Develop a Patch
  At any Secure Host, discard 5 Data Center cards of the same color from your and to patch the vulnerability of that color. Move the Patch Marker to the appropriate Patched Indicator.

  NOTE: When a patch is developed for a vulnerability, its cubes remain on the board and new cubes can still be placed during Zero Day Discovery (see Zero Day Discovery and Infections). However, removing malware for these vulnerabilities is now easier and you are closer to winning.

Draw Cards

After doing 4 actions, draw the top 2 cards together from the Player Deck.

If, as you are about to draw, there are fewer than 2 cards left in the Player Deck, the game ends and you team has lost! (Do not reshuffle the discards to form a new deck).

Zero Day Discovery Cards

If your draw includes any Zero Day Discovery cards, immediately do the following steps in order:

1. Increase: Move the infection rate marker forward 1 space on the Infection Rate Track.

2. Infect: Draw the bottom card from the Infection Deck. Unless its vulnerability color has been eradicated, put 3 malware infection cubes of that color on the named data center. If the data center already has cubes of this color, do not add 3 cubes to it. Instead, add just enough cubes so that it has 3 cubes of this color and then a Malware Outbreak of this color occurs in the data center (see Outbreaks below). Discard this card to the Infection Discard Pile.

ALERT: If you cannot place the number of cubes actually needed on the board, because there are not enough cubes of the needed color left in the supply, the game ends and your team has lost! This can occur during a Zero Day Discovery, an Outbreak, or Infections (see Outbreaks and Infections below).

3. Intensify: Reshuffle the just the cards in the Infection Discard Pile and place them on top of the Infection Deck.

ALERT: When doing these steps, remember to draw from the bottom of the Infection Deck and to then reshuffle only the Infection Discard Pile, placing it on top of the existing Infection Deck.

It is rare but possible to draw 2 Zero Day Discovery cards at once. In this case, do all three steps above once and then again.

NOTE: In this case in the second Zero Day Discovery's Infection card will be the only card to reshuffle, ending on top of the Infection Deck. A Malware Outbreak will then occur in this data center during Infections (see Infections below), unless an Event card is played to prevent this (see Event Cards).

After resolving any Zero Day Discovery cards, remove them from the game. Do not draw replacement cards for them.

Hand Limit

If you ever have more than 7 cards in hand (after first resolving and Zero Day Discovery cards you may have drawn), discard cards or play Event cards until you have 7 or less cards in hand (see Event Cards).

Malware Infections

Flip over as many Infection cards from the top of the Infection Deck as the current infection rate. This number is below the space of the Infection Rate Track that has the infection rate marker. Flop these cards over one at a time, infecting the data center named on each card.

To infection a data center place 1 malware infection cube matching its color onto the data center, unless this vulnerability has been patched and eradicated. If the data center already has 3 cubes of this color, do not place a 4th cube. Instead, a Malware Outbreak using this vulnerability occurs in the data center (see Malware Outbreaks below). Discard this card to the Infection Discard Pile.

Malware Outbreaks

When a malware outbreak occurs, move the outbreaks marker forward 1 space on the Malware Outbreaks track. Them, place 1 cube of the vulnerability color on every data center connected to the data center. If any of them already has 3 cubes of the vulnerability color, do not place a 4th cube in those data centers. Instead, in each of them, a *chain reaction* malware outbreak occurs after the current malware outbreak is done.

When a chain reaction outbreak occurs, first move the malware outbreaks marker forward 1 space. Then, place cubes as above, except do not add a cube to data centers that have already had an outbreak (or a chain reaction outbreak) as part of resolving the current Infection card.

As a result of malware outbreaks, a data center may have vulnerability cubes of multiple colors on it; up to 3 cubes of each color.

ALERT: If the malware outbreaks marker reaches the last space on the Malware Outbreaks Track, the game ends and your team has lost!

Turn End

After infection and discarding infection cards, your turn is over. The player on your left begins their turn.

Event Cards

During a turn, any player may play Event cards. Playing an Event card is not an action. The player who plays an Event cards decides how it is used.

Event Cards can be played at any time, except in between drawing and resolving a card.

NOTE: When 2 Zero Day Discovery cards are drawn together, events can be played after resolving the first Zero Day Discovery.

Example: During infections, the first Infection card drawn causes an outbreak. You may not play the VPN Event card to move the Network Specialist to prevent this. After this outbreak happens however, you may use the VPN to move the Network Specialist (to possibly protect other data centers) before flipping over the next Infection card.

After playing an Event card, discard it to the Player Discard Pile.

Player Cards

When playing the Introductory game (4 Zero Day Discovery cards), place your cards face up in front of you, for all players to see.

NOTE: Only Player cards count towards you hand limit. Your role and Reference cards are not part of your hand.

When playing the Standard (5 Zero Day Discovery cards) or Heroic (6 Zero Day Discovery cards) games, keep your cards private, so everyone has information to contribute to play discussions.

NOTE: Experience groups may decide to play with open hands, if desired, in these games.

Players may freely examine either discard pile at any time.

Game End

The players win as soon as Patches are developed for all 4 vulnerabilities.

NOTE: The players do not have to eradicate malware that exploits all 4 vulnerabilities to win; just develop patches for them. Once all vulnerabilities have patches developed, the game ends and players win immediately, no matter how many malware infection cubes are on the board.

There are 3 ways for the game to end and the players lose:

- If the Malware Outbreaks marker reaches the last space on the Malware Outbreaks Track.
- If you are unable to place the number of malware infection cubes actually needed on the board, or
- If a player cannot draw 2 Player cards after doing their actions.

Roles

Each player has a role with special abilities to improve your team's chances.

Project Manager

- The Project Manager may, as an action, take any discarded Event card from the Player Discard Pile and place it on their Role Card. Only 1 Event card can be on the role card at a time. It does not count against the player's hand limit.
- When the Project Manager plays the Event card on their role card, remove the Event card from the game (instead of discarding it).

Help Desk Manager

The Help Desk Manager may, as an action, either:

- Move any pawn, if its owner agrees, to any city containing another pawn.
- Move another player's pawn, if its owner agrees, as if it were the Help Desk Manager's own.
- When moving a player's pawn as if it were your own, discard cards for Direct and Charter Flights from your hand. A card discarded for a Charter Flight must match the city the pawn is moving from.
- The Help Desk Manager can only move other player's pawns; they may not direct them to do other actions, such as *Remove Malware*.

SysAdmin

- The SysAdmin removes *all* cubes, not 1, of the same color when doing the Remove Malware action.
- If a vulnerability has been *patched*, the SysAdmin automatically removes all cubes of that color from a data center, simply by entering it or being there. This does not take an action.
- The SysAdmin's automatic removal of cubes can occur on other players' turns, if he is moved by the Help Desk Manager or the VPN Event.
- The SysAdmin also prevents placing infection cubes (and outbreaks) of *patched* vulnerabilities in their location.

White Hat Hacker

The White Hat Hacker may, as an action, either:

- Install a secure host in the data center they are in without discarding (or using) a Data Center card.
- Once per turn, move from a secure host to any data center by discarding any Data Center card.

Network Specialist

- Prevents both outbreaks and the placement of malware infection cubes in the data center they are in and all data centers directly connected to that data center. They do not affect cubes placed during setup.

Security Researcher

- When doing the Share Knowledge action, the Security Researcher may give any Data Center card from their hand to another player in the same data center as them, without this card having to match their data center. The transfer must be from the Security Researcher's hand to the other player's hand, but it can occur on the other player's turn.

Software Developer

- The Software Developer needs only 4 (not 5) Data Center cards of the same vulnerability color to Develop a Patch for that vulnerability.

Commonly Overlooked Rules

- You do not draw a replacement card after drawing a Zero Day Discovery card.
- You may Develop a Patch at any Secure Host – the color of its data center does not need to match the vulnerability you are patching.
- On your turn, you may take a card from another player, if you are both in the data center that matches the card you are taking.
- On your turn, you may take any card from the Security Researcher (only), if you are in the same data center.
- You hand limit applies immediately after getting a card from another player.

Terms as related to Pandemic

Infection Deck = Infection Deck
Infection Discard Pile = Infection Discard Pile
Player Deck / Discard Pile = Player Deck / Discard Pile
City = Data Center (contains servers)
Epidemic = Zero Day Discovery – new malware exploits an unknown vulnerability
Infection = Malware Infection (exploits a vulnerability)
Outbreak = Malware Outbreak
Discover Cure = Develop Patch (which can be applied to servers in data centers)
Eradicate = Eradicate (after developing a patch, patching all systems, and cleaning all systems with malware that used the vulnerability)
Discovered Cure Indicators = Patches Developed indicators
Research Station = Secure Host (a secure system in a data center that your team can use)
Administer Cure = Remove Malware or Malicious Software

Old Intro… working
Can you keep a world-wide network of data centers, servers, and workstations running while computer criminals try to exploit unknown vulnerabilities in them? Your team is responsible for keeping all your data centers operational while simultaneously working to develop and deploy patches for four previously unknown computer viruses.

Your team is responsible not only keeping all your data centers operational but also developing software patches and counter-attacks to prevent downtime and private customer data from being stolen and sold on the black market. Your team will remotely connect to systems around the world using their unique skills and work together to succeed.

If you don't get patches for four major, zero day, vulnerabilities developed and deployed on time, your company, and the entire Internet is doomed.

Terms (to define and change)

* disease = virus/worm
* infection = virus infection
* outbreak = outbreak
* discover a cure = install/update virus software, update signatures, discover signature, collecte d enough for vendor to provide updated signatures
* treat = clean/disinfect/rebuild machine
* epidemic = new zero day exploit/vulnerability, zero-day
* city = workstation/server/data center in city
* drive/ferry = visit/ssh/telnet/connect
* research = research, researcher, honey pot (to collect data)

Ideas to play with

1. city = workstation

2. city = server

3. city = data center in a city
   * can re-use existing city cards
   * regions/availability zones in AWS/Azure/Google