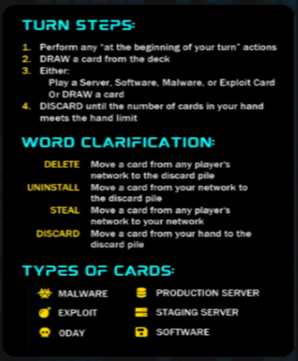
ADVANCED PERSISTENT THREAT

SPECTANT
SECURITY
3106 COMMERCE ST. DALLAS, TX 75226

WHATS IN THE BOX

138 Game Cards

14 Adversary Cards



TURN STEPS:

1. Perform any "at the beginning of your turn" actions
2. DRAW a card from the deck
3. Either:
   Play a Server, Software, Malware, or Exploit Card
   Or DRAW a card
4. DISCARD until the number of cards in your hand meets the hand limit

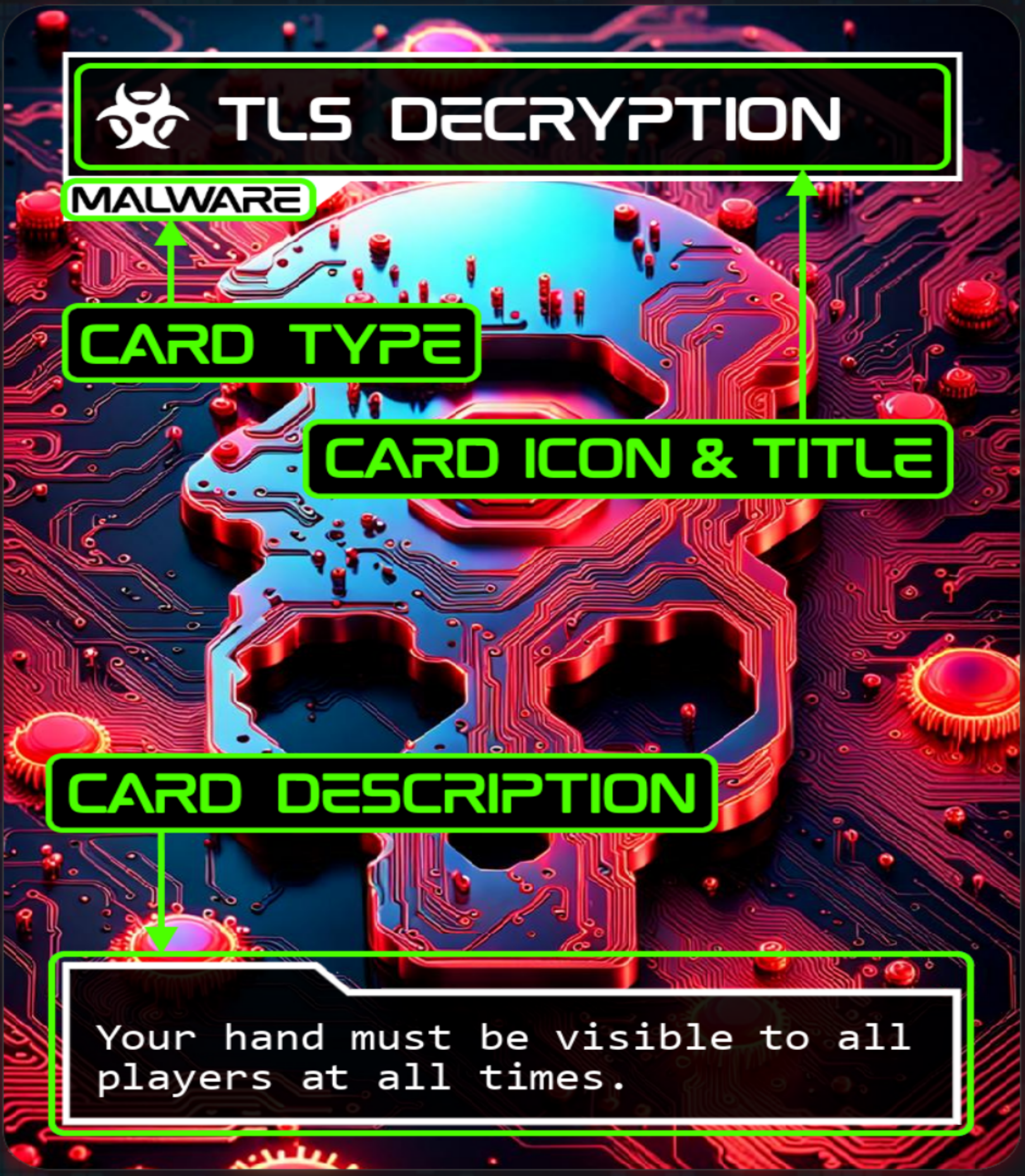
WORD CLARIFICATION:

DELETE	Move a card from any player's network to the discard pile
UNINSTALL	Move a card from your network to the discard pile
STEAL	Move a card from any player's network to your network
DISCARD	Move a card from your hand to the discard pile

TYPES OF CARDS:

- MALWARE
- EXPLOIT
- 0DAY
- PRODUCTION SERVER
- STAGING SERVER
- SOFTWARE

8 Reference Cards



TLS DECRYPTION

MALWARE

Your hand must be visible to all players at all times.

Card Layout

SETUP

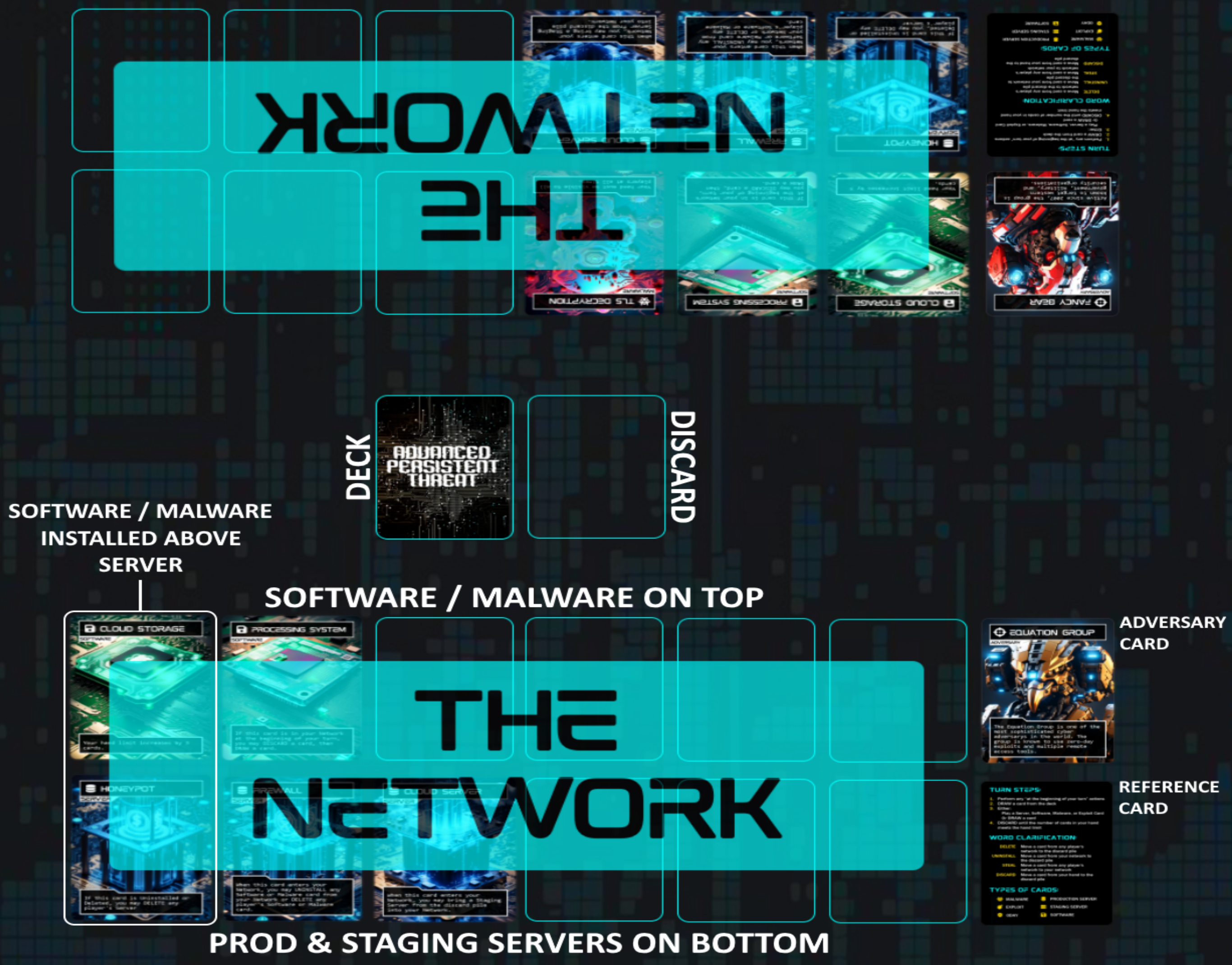
To Start, each player must choose an ADVERSARY card to represent them during the game. After each player has chosen an ADVERSARY card, separate the remaining white backed ADVERSARY cards from the deck and put them back in the box. Next, give each player:

1 STAGING SERVER CARD
1 SMALL DDOS CARD

Then, shuffle the remaining cards, and deal each player 5 cards. Place the remaining cards face down in the center of the table. This stack is the DECK. Leave a space next to the DECK for the DISCARD PILE. Cards that are UNINSTALLED, DELETED, or DISCARDED are placed here during the game.

Each player must take their STAGING SERVER and place it face up in the space in front of them. This space is called their NETWORK, as seen in the diagram below.

Each player may also take a REFERENCE CARD to quickly reference the rules. The following diagram represents an example 2 player table layout:


THE NETWORK
DECK
ADVANCED PERSISTENT THREAT
DISCARD
SOFTWARE / MALWARE INSTALLED ABOVE SERVER
SOFTWARE / MALWARE ON TOP
ADVERSARY CARD
REFERENCE CARD
THE NETWORK
PROD & STAGING SERVERS ON BOTTOM

IMPORTANT TERMS

Below are a few term definitions/clarifications:

NETWORK The play area in front of you where SERVER, SOFTWARE, and MALWARE cards are played

DECK The stack of cards that players DRAW from during the game

DISCARD PILE The stack of cards next to the DECK that have been DELETED, UNINSTALLED, or DISCARDED during the game

DELETE Move a card from any player's NETWORK to the discard pile

UNINSTALL Move a card from your NETWORK to the discard pile

STEAL Move a card from any player's NETWORK to your NETWORK

DISCARD Move a card from your hand to the discard pile

TYPE OF CARDS

There are 6 types of cards in the game:

PRODUCTION SERVER

This card has a database icon. Each production SERVER stays in a player's NETWORK until it is DELETED, UNINSTALLED, STOLEN, or MOVED. These have special effects when they enter and leave a NETWORK.

STAGING SERVER

This card has a stacked SERVER icon. These SERVERS do not have any special effects, but you can try to guess which hacker themed movie the quotes on them come from.

SOFTWARE

This card has a floppy disk/save file icon. These cards give you positive effects when installed in your NETWORK.

MALWARE

This card has a spikey biohazard icon. These cards give you negative effects when installed in your NETWORK. You can install MALWARE cards into any other player's NETWORK.

EXPLOIT

This card has a bomb icon. These cards are single-use. Once you play an EXPLOIT card you must move it to the discard pile.

0DAY

Pronounced: Zero Day or Oh Day. This card has a skull icon. This is the only type of card you can play at ANY time, even when another player is playing a card. Each player can play as many 0DAY cards as they want to, whenever they want to, so these cards can be played back-to-back.

HOW TO PLAY

Decide who goes first. After that, each player takes a turn going clockwise around the table after the first player. Each turn is made up of 4 steps:

1. Perform any "at the beginning of your turn" actions on any SERVER, SOFTWARE, or MALWARE cards in your NETWORK

   For this step, if you have a SERVER, SOFTWARE, or MALWARE card in your NETWORK with an effect that states “If this card is in your NETWORK at the beginning of your turn” its effect is triggered during this step.

2. DRAW a card from the DECK

   For this step, you DRAW a card from the DECK and place it into your hand.

3. Either: Play a SERVER, SOFTWARE, MALWARE, or EXPLOIT Card or DRAW a card

   For this step, you can EITHER play a SERVER, SOFTWARE, MALWARE, or EXPLOIT card from your hand OR you can DRAW a card, but not both. If you choose to play a card, you must read the card out loud for all players to hear.

4. DISCARD until the number of cards in your hand meets the 7 card hand limit

   For this step, if you have 8 or more cards at the end of your turn, you MUST DISCARD cards until you only have 7 cards in your hand, unless you have a card in your NETWORK that increases or reduces your hand limit. If so, you’re only allowed to keep as many cards as your new hand limit states.

NOTE: 0DAY Cards can be played at ANY time. See the card type descriptions for more details.

HOW TO WIN

The first person to have 6 SERVERS in their network wins!

For a longer game you can increase this number to 7 SERVERS. For a shorter game you can reduce this number to 5 SERVERS.

If the DECK runs out of cards before any player reaches the required number of SERVERS the player with the most SERVERS in their NETWORK wins.

If two or more players tie for the most number of SERVERS installed, then the player with the least amount of MALWARE in their NETWORK wins.

If there is still a tie, the player with the most amount of SOFTWARE installed in their NETWORK wins.

If there is still a tie after that, the winner will be decided by a single (best two out of three) game of ROCK, PAPER, SCISSORS.

EXAMPLE TURN WALKTHROUGH - PLAYER 1

For this example, we'll assume it's the very first turn of a 2 player game. Because of this, each player will have 1 STAGING SERVER installed in their network infront of them and 1 SMALL DDOS card, along with 5 other cards, for a total of 6 cards in their hand.

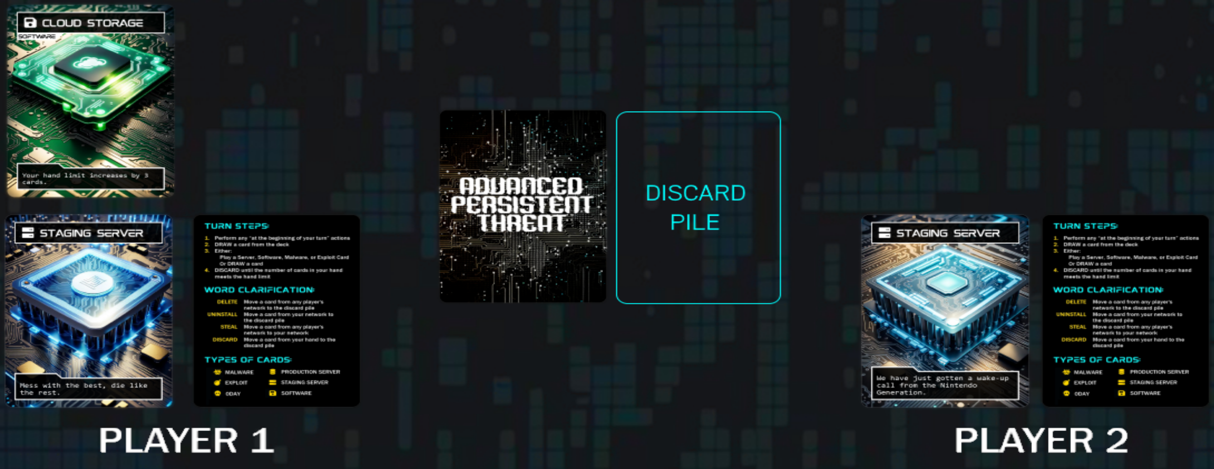
CLOU
SERVER
FIREV
SERVER
HONE
SERVER
PROCE
SOFTWARE
TLS D
MALWARE
SMALL DDOS
0DAY
Play this card when any other player tries to play a card. Stop that player's card from being played and sent it to the discard pile.

PLAYER 1 will start their turn and verify there are no "at the beginning of your turn" cards in their network. Since this is the first turn of the game, and there is only 1 STAGING SERVER in their network, they will move to the second step of their turn and DRAW a card.

For this example, we will assume that PLAYER 1 drew the CLOUD STORAGE SOFTWARE card which states "Your hand limit increases by 3 cards.":

PLAYER 1 then decides to INSTALL that SOFTWARE card above their STAGING SERVER in their NETWORK and reads the card outloud so PLAYER 2 knows which card has been played. As PLAYER 1 only has 6 cards remaining in their hand, their turn is now over.

After PLAYER 1's turns PLAYER 1 and PLAYER 2's NETWORKS look like:


CLOUD STORAGE
SOFTWARE
Your hand limit increases by 3 cards.
STAGING SERVER
Mess with the best, die like the rest.
ADVANCED PERSISTENT THREAT
DISCARD PILE
STAGING SERVER
We have just gotten a wake-up call from the Nintendo Generation.
PLAYER 1
PLAYER 2

TURN STEPS:

1. Perform any "at the beginning of your turn" actions
2. DRAW a card from the deck
3. Either:
   Play a Server, Software, Malware, or Exploit Card
   Or DRAW a card
4. DISCARD until the number of cards in your hand meets the hand limit

WORD CLARIFICATION:

DELETE	Move a card from any player's network to the discard pile
UNINSTALL	Move a card from your network to the discard pile
STEAL	Move a card from any player's network to your network
DISCARD	Move a card from your hand to the discard pile

TYPES OF CARDS:

MALWARE	PRODUCTION SERVER
EXPLOIT	STAGING SERVER
0DAY	SOFTWARE

EXAMPLE TURN WALKTHROUGH - PLAYER 2

PLAYER 2 will start their turn and verify there are no "at the beginning of your turn" cards in their network. Since this is their first turn of the game, and there is only 1 STAGING SERVER in their network, they will move to the second step of their turn and DRAW a card.

For this example, we will assume that PLAYER 2 drew the NETWORK WORM EXPLOIT card which states "Move a Software or Malware card from any player's Network to any other Player's Network.":

NETWORK WORM
EXPLOIT
Move a Software or Malware card from any player's Network to any other player's Network.

PLAYER 2 then decides to play the NETWORK WORM EXPLOIT card they just drew and STEAL PLAYER 1's CLOUD STORAGE SOFTWARE card by moving/INSTALLING it above their STAGING SERVER in their NETWORK.

PLAYER 1 immediately decides to play their SMALL DDOS 0DAY card in an attempt to stop the NETWORK WORM EXPLOIT card from being played.

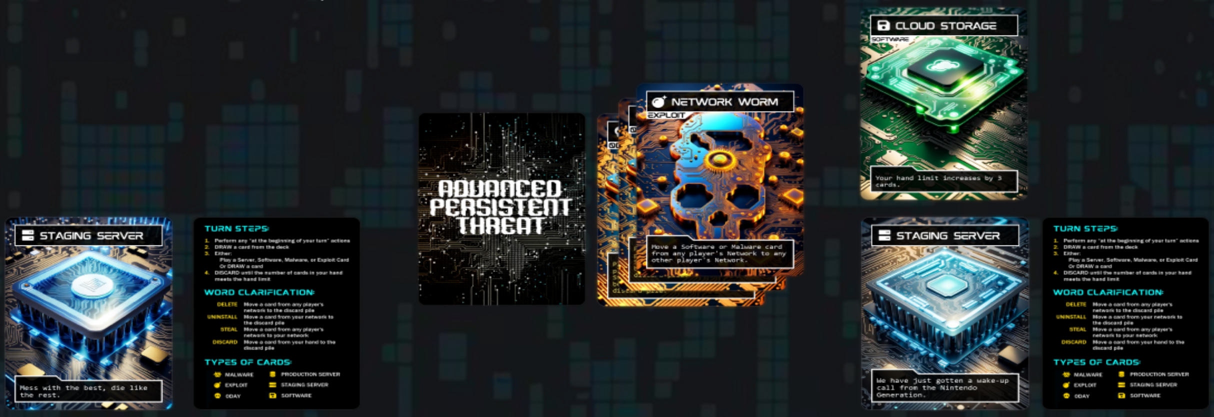
However, PLAYER 2 decides to counter PLAYER 1's SMALL DDOS 0DAY card with their own SMALL DDOS 0DAY card.

Assuming PLAYER 1 has no other DDOS cards (or PLAYER 1 chooses not to play any other DDOS/0DAY cards), PLAYER 2 wins the exchange.

Both SMALL DDOS 0DAY cards, as well as the NETWORK WORM EXPLOIT card are then sent to the DISCARD PILE and the CLOUD STORAGE SOFTWARE card is INSTALLED above PLAYER 2's STAGING SERVER in their NETWORK.

As PLAYER 2 only has 5 cards remaining in their hand, their turn is now over.

After PLAYER 2's turn, PLAYER 1 and PLAYER 2's NETWORKS look like:

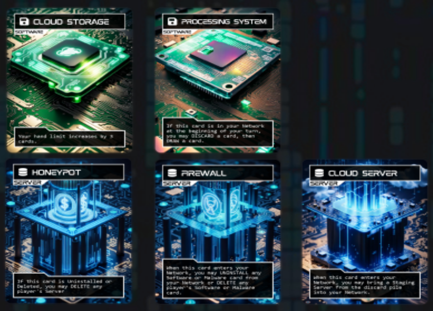

STAGING SERVER
Mess with the best, die like the rest.
TURN STEPS
WORD CLARIFICATION
TYPES OF CARDS
ADVANCED PERSISTENT THREAT
NETWORK WORM
EXPLOIT
Move a Software or Malware card from any player's Network to any other player's Network.
CLOUD STORAGE
SOFTWARE
Your hand limit increases by 3 cards.
STAGING SERVER
We have just gotten a wake-up call from the Nintendo Generation.

PLAYER 1 PLAYER 2

HOW TO INSTALL MALWARE & SOFTWARE

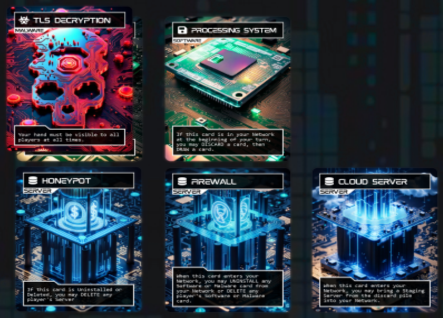
SOFTWARE & MALWARE cards can only be played on SERVER cards that are already in the NETWORK. You can only play 1 SOFTWARE card above a SERVER in your NETWORK.

In the example below there are 3 SERVER cards installed in the player's NETWORK:



Note, 2 SERVER cards already have SOFTWRAE installed on them. That means there is only 1 remaining SOFTWARE slot available for that player to use.

Similarly, you can only play 1 MALWARE card above a SERVER card in a NETWORK. MALWARE cards can be played ON TOP of already installed SOFTWARE cards. This cancels out the effect of the SOFTWARE card. Following the previous example, the played MALWARE card cancels out the effect of the SOFTWARE card on the first SERVER in the NETWORK:



Note, that SOFTWARE cards CAN NOT be played ON TOP of MALWARE cards. If a SERVER is infected with MALWARE, no SOFTWARE can be installed on it until the MALWARE card has been removed.

Even though SOFTWARE and MALWARE cards are bound to individual SERVER cards, their effects apply to the entire NETWORK.

When a SERVER is UNINSTALLED or DELETED, ANY SOFTWARE or MALWARE cards installed on that SERVER are also UNINSTALLED or DELETED.

If a SERVER card instructs you to "return this card to your hand", ONLY THE SERVER card is returned to your hand. ANY SOFTWARE or MALWARE installed on that SERVER gets placed in the DISCARD PILE.

Note, that some cards may allow you to return ANY card from your NETWORK into your hand. These cards can be used to remove MALWARE from SERVER cards allowing you to simultaneously obtain a MALWARE card to use against another player.

However, these cards DO NOT allow you to move any SOFTWARE cards that are UNDER a MALWARE card into your hand. In the example above, if the player had one of these cards, they could remove the MALWARE from the first SERVER and place it in their hand, however they would not be able to remove the SOFTWARE card under it.

FURTHER CLARIFICATION

CARD EFFECTS:

SERVER, SOFTWARE, and MALWARE cards have no effect while they are in your hand. They only become active when entering or leaving a NETWORK.

ENTERING and LEAVING a NETWORK:

Each time any card is STOLEN, any "leaves the NETWORK" effect is triggered as it leaves the victim's NETWORK before any "enters the NETWORK" effect is triggered as it enters its new NETWORK.

OPTIONAL vs. MANDATORY EFFECTS & FORGETTING EFFECTS:

Some card effects are mandatory (DISCARD a card), while others are optional (you may DISCARD a card). If a card does not use the word MAY, the effect is mandatory. If you forget to perform an optional effect AFTER you have already drawn a card for the ‘DRAW a card’ step of your turn, you CANNOT go back and use that effect. However, if you forget to perform a MANDATORY effect, you MUST STILL DO IT when you or any other player notices.

BEGINNING TURN EFFECTS:

If you have multiple cards that state "at the beginning of your turn", their effects occur simultaneously. Even if using one effect ends your turn, you still get to perform the other effects.

0DAY CARDS:

Pronounced: Zero Day or Oh Day

0DAY Cards can only be used to modify what a player does when playing a card. This means that you CANNOT use a 0DAY card to cancel out or modify an already played SERVER, SOFTWARE, or MALWARE card effect.

PLAYER SELECTION:

Any player means any single player, including you.

Another player means any single player, excluding you.

Each player refers to every player, including you.

MULTIPLE ACTION CARD EFFECTS:

Some cards have multiple actions e.g. "DISCARD a card, then DRAW a card." If, however, you cannot satisfy the first effect of the card, then you cannot perform the second effect. Given the stated example, if you do not have any cards to discard, then you CANNOT DRAW a card.

CARD SPECIFIC CLARIFICATION

EXPLOITS & MALWARE CARDS

These CAN be played on, or against, yourself.

REMOTE ROOT

This CAN block and/or reflect MULTIPLE deletions from a single card.

PROCESS KILL

This prevents SERVER card "Entering Network" effects too.

GR33TZ & TH4NK Y0UZ

The following people were instrumental in helping me finish this project, whether it be through kind words, inspiration, motivation, play testing, or all of the above.

THE ENTIRE DFW HACKING & INFOSEC COMMUNITY

LAN
MIKE
BELINDA
ELISE
LAFE
LOCKE
MOTUMBO
ANGELA
JOHN
R3X3R
BLAISEBITS
MICHAEL
XORT
MIKEP

VALERIE
MICHELLE
KONRAD
ERICK
IKIRUMATA
KALEB
SOPHIE
BRAIDEN
ALLISON

HOW TO PLAY

MORE GAMES

SPECTANT
SECURITY
3106 COMMERCE ST. DALLAS, TX 75226