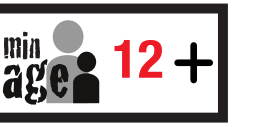


[d0x3d!]

a network security game

v2

[welcome]

Wow. I don't know what you did to make them angry. But they are angry. Your enemies have targeted you and your friends, and stolen your stuff. We aren't talking about candy or coupons; we are talking **stuff that matters**. Digital stuff. Private stuff. Valuable stuff. Possibly, embarrassing, personal stuff.

They took your **[digital assets]**.

They've locked them away in their network using keys and split those keys up into little pieces, and scattered those pieces across different servers.

Your job is to work as a group to **infiltrate** the network, **search for asset shares** (pieces of keys), reassemble the shares to **recover your stuff**, and then **escape**. You've learned some mad skillz, and now you are ready for the job: you and your friends are a **1337 cadre of hackers**, ready to attack the network and get your stuff back.

The only problem is: the admins are watching. As you invade their network, they are analyzing traffic, patching servers, and—once they figure out what you are up to—they will retaliate by taking all your personal data and posting it all over the the Internet. In other words:

You'll get **[d0x3d!]**

[d0x3d!], \doks'd\
Verb (past tense). Hacker slang.
To have one's personal data posted publically to a website, often leading to damage, humiliation, or worse. A form of bullying.

[objective]

[d0x3d!] is a cooperative game, for 1–4 players. Players assume the role of hackers, infiltrating a network. Together, you need to collect **[shares]** of digital assets and use each to **[recover]** each **[digital asset]**. Once you get all four digital assets, you and the other players need to escape the network, without getting caught. Each round, the admins will **[patch]** the network and they may detect your intrusions. If the admins begin to suspect you are in their network: machines may get **[decommissioned]** for forensic investigation, the network threat level increases, and you or your friends might get caught.

You all win or lose together. If someone gets caught, if the threat level reaches INFOCON Level 1, if you can no longer move around the network, or if it becomes impossible to win, you all lose.

[what's it all about?]

[d0x3d!] creates a context for thinking about and discussing issues in network security. It is a game, designed for informal learning. Teachers can find ideas for lessons that use this game in the classroom at our website, **www.d0x3d.com**.

[inventory]

A full game of **[d0x3d!]** consists of:

network **[node]** tiles
: Twenty-four (24) hex tiles, depicting servers and other parts of the network. Each tile has two states: uncompromised (solid border) and compromised (broken border). Some nodes are *hardened* and require extra work to compromise them.

the **[digital asset]** tokens
: Four (4) green tokens, each representing a digital asset. You recover these, to win.

the **[lo0t!]** deck
: Twenty-eight (28) cards make up the deck. Deck back is blue and marked **[lo0t!]**.

the **[patch!]** deck
: Twenty-four (24) cards make up the deck. Deck back is orange and marked **[patch!]**.

the **[hacker]** roles and pawns
: Eight (8) cards with yellow backs, each describes a hacker role.

an **[infocon]** threat meter and admin token
: A game mat and one (1) black token that, together, track the network threat level perceived by the network admins.

the **[digital asset drives]**
: A game mat used to store recovered **[digital asset]** tokens. The game also includes several (two-sided) customizable **[digital asset drives]**, you may use to re-name and customize the assets in the game.

stickers and **[order of play]** cards
: A page of stickers used to decorate game tokens, and four (4) cards that summarize rules and order of play.

[assembly]

Tokens. Use the stickers to assemble the (black) admin token and (green) digital asset tokens, so they appear like the tokens shown to the right. Only one token face needs a sticker. Enjoy the extra stickers! Use them as prizes or gifts.

Customized [digital asset drives]. Use the customizable drive mats to pick fun names for the specific digital assets stolen from you, in the game. If you customize your assets, tweet us a pic **@d0x3d**. Don't forget to let us know if you won them all back in the end!

[digital assets]

The object of the game is to reclaim your stuff and escape from the network, without a trace. There are four digital assets to recover in the game:

[authentication credentials]

Authentication credentials are data you use to prove your identity. They can be something you have (like a driver's license), something you know (like a password), or something you are (like a fingerprint). When stolen, someone could use these credentials to impersonate you.

[financial data]

If it's worth money or about money, it's financial data: credit card numbers, bank account numbers, tax data, electronic gift certificates, e-cash, quarterly earnings reports, etc.

[intellectual property]

Intellectual property is data that came out of your head or your hands, like inventions and creative works: an essay for school, an original photo, a piece of software, a secret recipe, your band's demo tracks, your YouTube videos, etc.

[personally identifiable information]

Personally identifiable information is data, about you or someone else: your home phone number, your address, photos of you and your friends, your grades, your medical records, etc.

[1337], \leet\
Adjective. Hacker slang.
" Elite. "

Each player takes on the role of a hacker. The game comes with eight (8) **[hacker]** role cards, each with its own l337 skill set. The role card describes these special abilities.

the [hacker] roles

[the social engineer] A master of manipulation, the social engineer attacks the human factor of security. Why pick a lock when they'll open the door for anyone dressed like a delivery person? Why crack a login screen, when the dumpster has crumpled-up passwords in it? Humans are part of the system, and you know how to hack them *to get just about anywhere*.

[the war driver] You use wireless to your advantage, gaining access from remote places. War driving is the act of methodically probing for wireless access points, and you've mapped the whole city. Did you know that, from your favorite coffee shop, a radio antenna at the right angle gets you network access to the office at the top of the neighboring skyscraper? You do your mobile magic, *long distance*.

[the insider] If you want to beat 'em, then join 'em! The malicious insider tears it apart from the inside, taking advantage of *free access to the surrounding machines*. Welcome to the company! The server room is down the hall.

[the botmaster] As a botmaster, you control hundreds—no, thousands—of machines across the world, and you know how to use them all to *dish it out, at scale*. Your "zombies" share files, fire out spam, and launch denial of service attacks ... all controlled by you.

[the cryptanalyst] Crypto is hard to get right. You've picked a much easier game: recognizing when its done wrong. Weak keys, unsafe primes, corrupt certificate authorities: an expert of finesse, the cryptanalyst is adept at tackling hard problems *from a slightly different angle*.

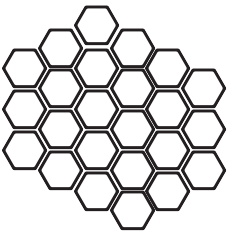
[the malware writer] When it comes to viruses, trojan horses, and worms you're the best of the best. An artist, a maestro, a poet ... that is, if poems could stop a car or explode a pacemaker. Like a nasty cold, your malware *spreads quickly across the network*.

[the forensics ninja] This forensics expert images the memory of a running process and scrapes the bits off drives, *to access data from the recent past*. You laugh at an empty trash can.

[the traffic spoofer] The traffic spoofer knows how to hand craft IP packets and make the routing table dance. Smurf attacks, ping of death, DNS spoofing, ARP poisoning: the spoofer shapes the traffic on the network, *changing its logical topology and opening new paths* between machines.

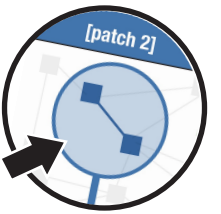
[setup]

1. Create the Network.
Shuffle and lay out the **[node]** tiles, each tile with its uncompromised side face up. You may choose any layout for the network. A topology that is good for first-time players is pictured, below.



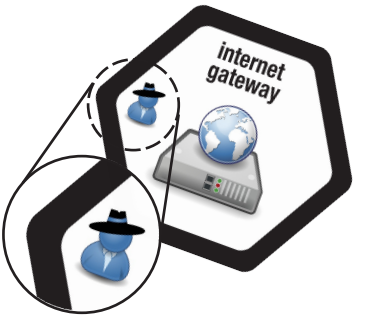
2. Shuffle the Decks.
Divide and shuffle the **[lo0t!]** and **[patch!]** decks. Set aside the **[digital asset]** tokens.

3. Set the INFOCON level.
Set the initial **[infocon]** level by placing the admin token on the meter. For an easier game, place the token on the lowest position (pictured, right).



4. Choose Characters.
Each player chooses a **[hacker]** role and a pawn of the corresponding color. Put unused pawns and **[hacker]** cards aside.

5. Infiltrate the Network.
Each **[hacker]** has a unique starting position on the board, marked in the left corner. For the starting position of your **[hacker]**, flip its tile to the compromised side and place your pawn on it.



6. Deal [lo0t!] Cards.
Deal two (2) cards to each player from the **[lo0t!]** deck. If an **[intrusion detected]** or **[honeypot audit]** card is dealt, then shuffle it back into the deck and deal out a different card. Lay your cards face up in front of you: since play is collaborative, it's useful for others to see them.

7. Start Play.
The player who most recently changed a password in real life goes first. Play proceeds counter-clockwise. In each round, follow the **[order of play]**. If there is ambiguity in any rules, decide as group how to interpret them.

Most importantly: have fun!

[order of play]

1. **[action]**
   Take up to three actions.
2. **[loot]**
   Draw two **[lo0t!]** cards.
3. **[patch]**
   Draw and resolve **[patch!]** cards, as indicated by the **[infocon]** level.
4. **[check]**
   Discard, to obey the hand limit.

[winning]

If all players occupy the Internet Gateway tile, all four **[digital asset]** tokens have been recovered, and anyone plays a **[zero-day exploit]** card, you win. This is the only way to win: re-capture your stuff, escape to the Internet.

[losing]

You lose when either (1) the threat level reaches **[infocon]** level one, or (2) it becomes impossible for all players to win, including:

- The Internet Gateway tile is decommissioned;
- A **[hacker]** is ejected from the network, for any reason;
- A **[capture point]** is decommissioned, such that it becomes impossible to **[recover]** some **[digital asset]**.

[check]

At the end of your turn, you may hold at most five **[lo0t!]** cards when a hand limit check is performed. Discard any cards in excess of the hand limit to the **[lo0t!]** discard pile. You can play **[zero-day exploit]** cards before discarding them.

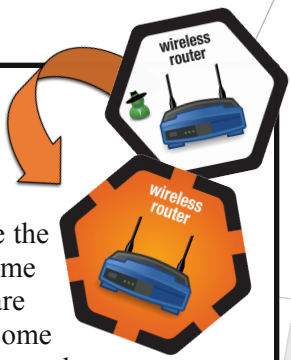
[layout]

You may layout the game pieces however you like. One possible layout is pictured on the back of this booklet.

[actions]

You may perform anywhere between 0 and 3 actions. **Actions are listed below**. An action must be completed before another action can be taken. A **[node]** tile is **adjacent** to another tile if both tiles share an edge.

[compromise]

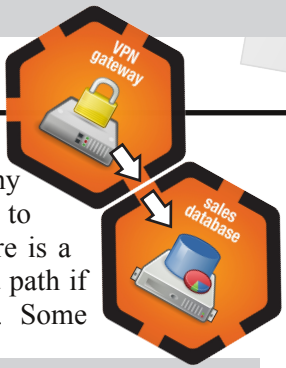


You may, as one action, compromise any adjacent node tile, flipping it so that its compromised face is showing. When a tile is flipped, you may choose the orientation of the compromised tile. Some nodes are hardened—two actions are required to compromise these. Some players have special compromise abilities.

[the insider] can compromise two adjacent nodes or one hardened node, as one action.
[the traffic spoofer] can reorient an already compromised tile, anywhere on the board, as one action.

[the forensic ninja] may search the **[lo0t!]** discard, to swap a card from her hand with one from the discard pile, as an action. She may do this at most once per turn.

[move]



You may, as one action, move to any compromised tile that is adjacent to your current position, to which there is a path. Two nodes are connected by a path if their broken borders are adjacent. Some players have special movement abilities.

[the social engineer] can move directly to a compromised tile, anywhere on the board.
[the malware writer] can move along a path across any number of compromised tiles.
[the cryptanalyst] can move to any adjacent compromised tile, even if there is no path.

[exchange] or [give]

As one action, you may trade one **[loOt!]** card with any player on the same tile as you. Or, as one action, you may give one **[loOt!]** card to any player on the same tile as you. You cannot take a card from a player without giving a card to that player. Some players have special give and exchange abilities.

[the botmaster] may give or exchange two cards, as one action.
[the war driver] may give or exchange a card, no matter where she is located.

[recover]

If you occupy a **[capture point]**, you may, as one action, discard four **[digital asset share]** cards of one type from your hand, to recover the **[digital asset]** token of that type, if the type matches the icon shown on the capture point. Store the token in your **[digital asset drive]**.

[capture point]

Some **[node]** tiles are special: they are where your digital assets are stored, and they are where you perform the **[recover]** action to reclaim them. These nodes are marked with the icon of a **[digital asset]** on them. There is one capture point for each **[digital asset]**.

[loot]

The **[lo0t!]** deck contains good stuff—like **[digital asset share]** and **[zero-day exploit]** cards—and bad stuff—like **[intrusion detected]** and **[honeypot audit]** cards. Bad stuff must be resolved immediately, and then discarded. If you run out of cards in the **[lo0t!]** deck, reshuffle the **[lo0t!]** discard pile.

[intrusion detected]
You've been spotted: raise the **[infocon]** level (see below) and then discard this card.

[honeypot audit]
If you draw this card, immediately draw a **[patch!]** card. The pictured **[node]** was a machine left intentionally unsecured as bait, to detect attacks. If this tile is currently compromised, you've been spotted: raise the **[infocon]** level and then discard this card.

[digital asset share]
Collect any four of the same type of this card, to **[recover]** the pictured **[digital asset]**.

[zero-day exploit]
Network admins cannot prevent these exploits, since they have never seen them before and no preventions have been invented. They can be played at any time by any player (even on someone else's turn), by discarding them from your hand. These can be played on already compromised nodes to reorient them, or played to interrupt and avoid **[patch]** effects. Zero-days compromise a hardened **[node]** as if it were a regular **[node]**.

Secret sharing is a way to protect data, similar to encryption. Simple sharing schemes require all shares to recover the original data. Complex schemes may require two (of three) shares to recover data. In **[d0x3d!]**, the admins use a scheme where any four shares can be used to recover the data locked away at a **[capture point]**.

[infocon]

To raise the **[infocon]** level, advance the **[admin]** token up the **[infocon]** threat meter, following the path connecting the circular token positions (highlighted to the right, with arrows). The network's current INFOCON threat level is determined by the color of the zone the admin token occupies. For example, if the token currently rests on a green circle, the **[infocon]** meter is at INFOCON threat level four; thus, during the **[patch]** round, the network admins will **[patch 3]** nodes.

[patch]

Draw the number of **[patch!]** cards indicated by the **[infocon]** meter. Resolve and discard each **[patch!]** card, one at a time, in the order drawn. If you run out of cards in the **[patch!]** deck, reshuffle the **[patch!]** discard pile.

For the tile of the node pictured on the card:

(1) If there is a pawn on the tile: the **[hacker]** must move to another tile, obeying her **[move]** rules; then, the tile gets **[decommissioned]**.

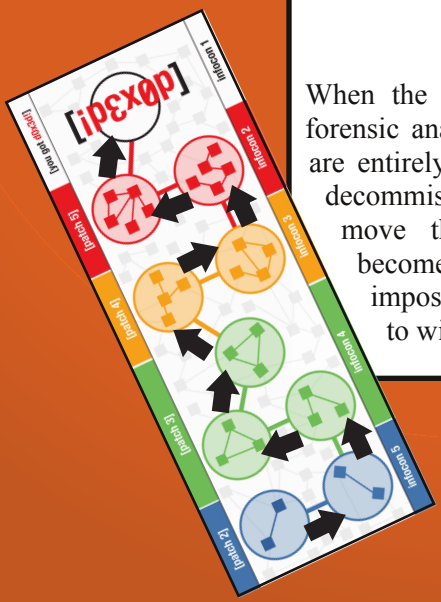
(2) If the tile was not decommissioned in Step 1, then flip the tile so its uncompromised side faces up.

If a player is forced to move in Step 1 but no nodes are reachable using her movement rules, then she is **ejected** from the network, and the team loses the game.

All the above **[patch]** effects may be prevented by using a **[zero-day exploit]** card.

[decommissioned]

When the admins decommission a machine for forensic analysis, its **[node]** tile and **[patch!]** card are entirely removed from the game. Be careful: decommissioned machines make it harder to move through the network, as the board becomes less connected and may cause it to be impossible to win.



Computer forensics is a branch of criminal investigation and computer security research. It develops methods of investigating digital evidence, to recover data, to investigate incidents, and to preserve evidence of cyber crime.

[cr3dits]

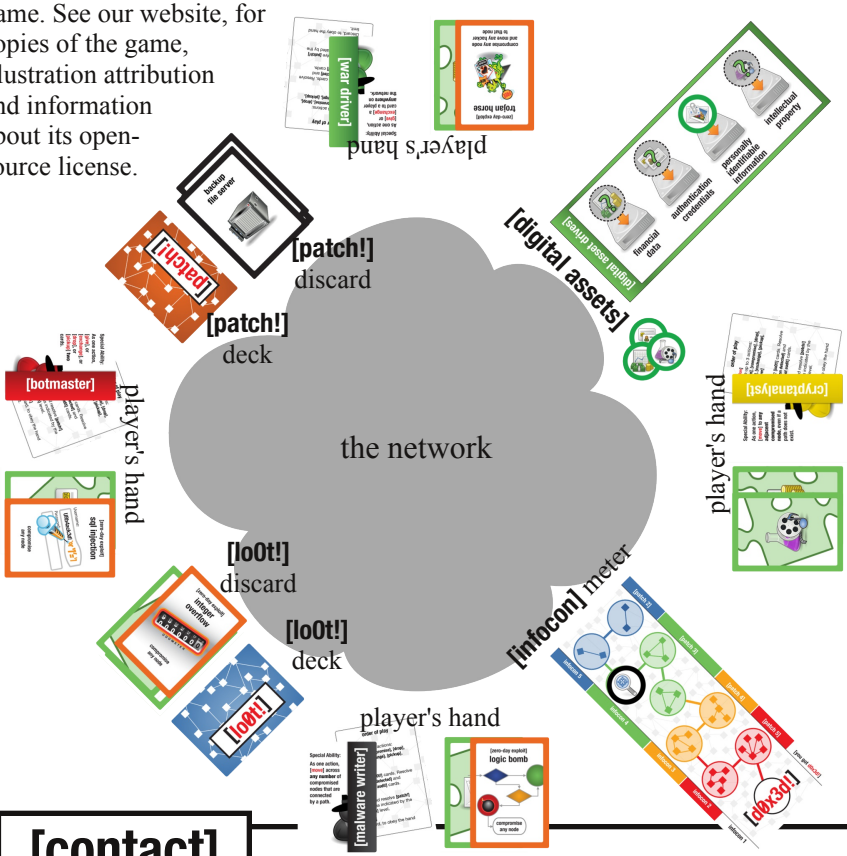
Game Design: Zachary N.J. Peterson
Mark Gondree
Print Design: Ann Gallenson
Illustrations: M. Sherwood Design,
Various FLOSS icons

[d0x3d!] is an open-source game. See our website, for copies of the game, illustration attribution and information about its open-source license.

[printing]

If you download and print the game from our website, the following are suggestions for how to assemble it:

- Print in color (it's worth it).
- Find fun substitutes for pawns from another game, like Monopoly.
- For tokens, use quarters or large buttons.



[contact]

Stay in touch, and learn about our other great games!

d0x3d.com **@d0x3d**

tabletopsecurity.com **@TableTopSecurity**