



[intrusion detected]: Raise the [infocon] level.

[honeypot audit]: Immediately draw a [patch!] card. If the pictured [node] is compromised, raise the [infocon] level.

[check]: The hand limit is five cards. Every card in excess of the hand limit must be discarded. You may play [zero-day exploits] before discarding them.

[patch] situations:

- Any [loot!] cards left on a [node] being patched are discarded.
- If a player is on a node being patched, she must [move] to a compromised node (obeying normal movement rules), then [decommission] the node and its [patch!] card.
- [zero-day exploits] can be used to prevent all [patch] effects.

order of play

1. [action]

Take up to 3 actions:

[move], [compromise], [drop],
[give], [exchange], [pickup],
[recover]

2. [loot]

Draw 2 [loot!] cards. Resolve [intrusion detected] and [honeypot audit] cards.

3. [patch]

Draw and resolve [patch!] cards, as indicated by the [infocon] level.

4. [check]

Discard, to obey the hand limit.

[intrusion detected]: Raise the [infocon] level.

[honeypot audit]: Immediately draw a [patch!] card. If the pictured [node] is compromised, raise the [infocon] level.

[check]: The hand limit is five cards. Every card in excess of the hand limit must be discarded. You may play [zero-day exploits] before discarding them.

[patch] situations:

- Any [loot!] cards left on a [node] being patched are discarded.
- If a player is on a node being patched, she must [move] to a compromised node (obeying normal movement rules), then [decommission] the node and its [patch!] card.
- [zero-day exploits] can be used to prevent all [patch] effects.

Special Ability:

As one action,
[move] to any
compromised
tile.



[social engineer]

Special Ability:

As one action,
[give] or
[exchange]
two cards.



[botmaster]

Special Ability:

As one action,
[move] across
two
compromised
tiles.



[malware writer]

Special Ability:

As one action,
[move] or
[compromise]
diagonally.



[cryptanalyst]

Special Ability:

As one action,
[compromise]
two adjacent
tiles.



[the insider]

Special Ability:

As one action,
[give] or
[exchange] a
card to a player
anywhere on
the network.



[war driver]

order of play

1. **[action]**
Take up to 3 actions:
[move], [compromise], [drop],
[give], [exchange], [pickup],
[recover]
2. **[loot]**
Draw 2 [loot!] cards. Resolve
[intrusion detected] and
[honeypot audit] cards.
3. **[patch]**
Draw and resolve [patch!] cards, as indicated by the
[infocon] level.
4. **[check]**
Discard, to obey the hand limit.

[intrusion detected]: Raise the [infocon] level.

[honeypot audit]: Immediately draw a [patch!] card. If the pictured [node] is compromised, raise the [infocon] level.

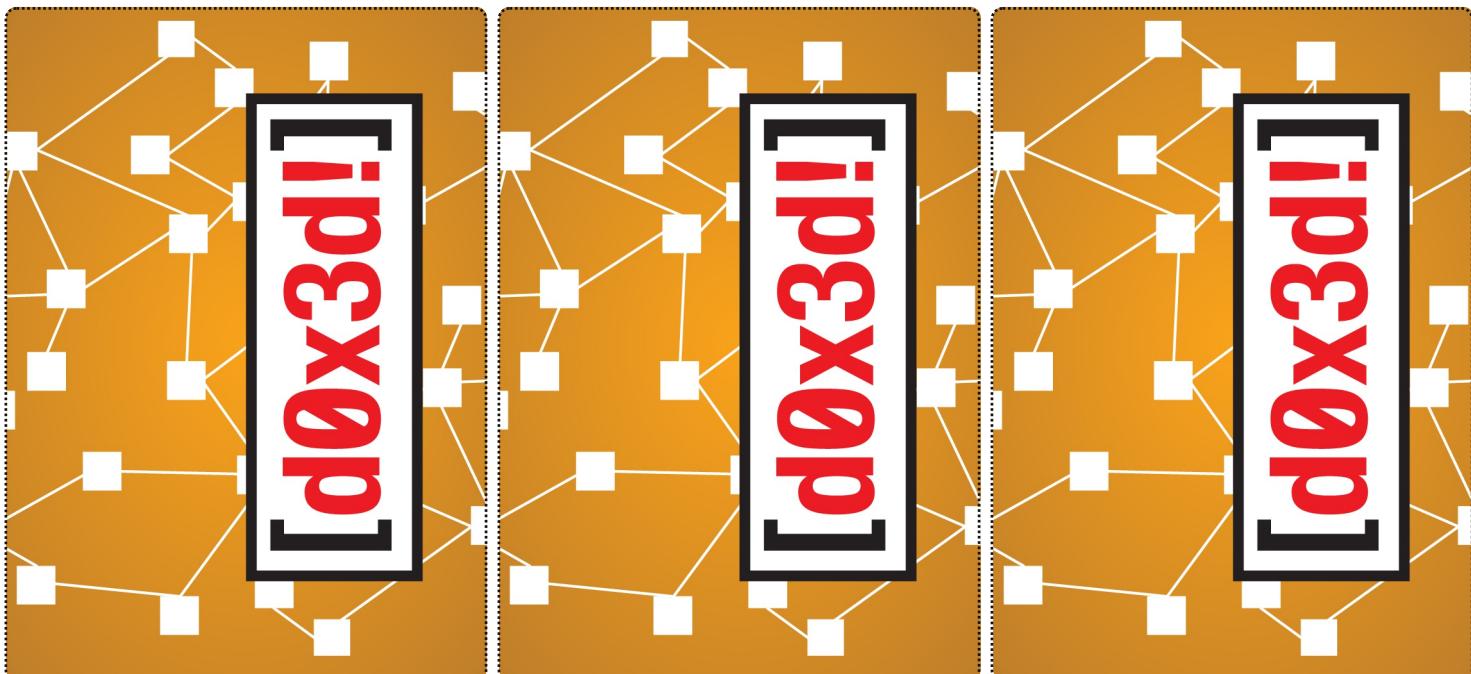
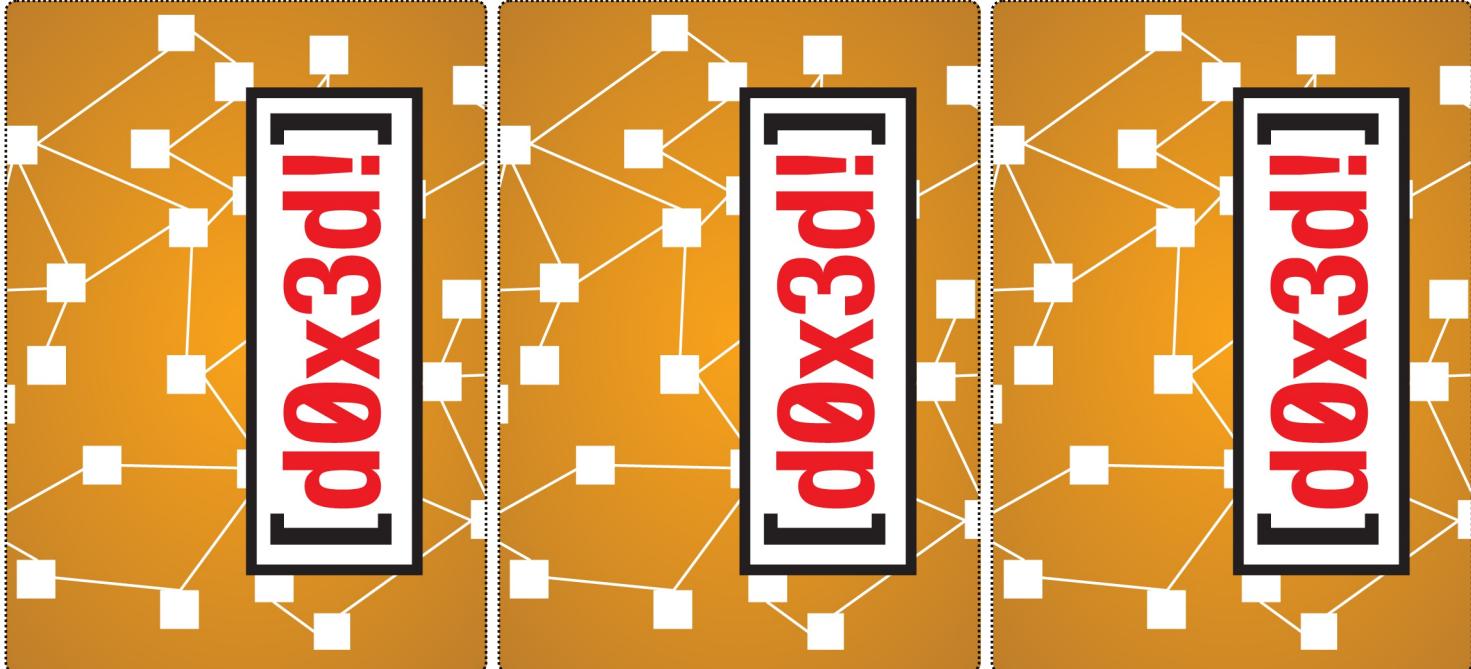
[check]: The hand limit is five cards. Every card in excess of the hand limit must be discarded. You may play [zero-day exploits] before discarding them.

[patch] situations:

- Any [loot!] cards left on a [node] being patched are discarded.
- If a player is on a node being patched, she must [move] to a compromised node (obeying normal movement rules), then [decommission] the node and its [patch!] card.
- [zero-day exploits] can be used to prevent all [patch] effects.

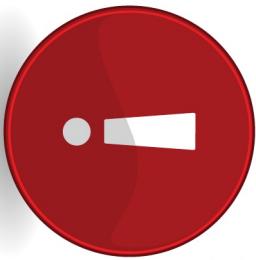
order of play

1. **[action]**
Take up to 3 actions:
[move], [compromise], [drop],
[give], [exchange], [pickup],
[recover]
2. **[loot]**
Draw 2 [loot!] cards. Resolve
[intrusion detected] and
[honeypot audit] cards.
3. **[patch]**
Draw and resolve [patch!] cards, as indicated by the
[infocon] level.
4. **[check]**
Discard, to obey the hand limit.

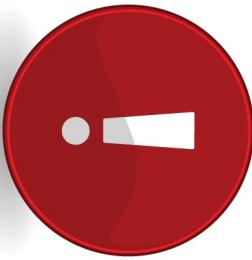




**honeypot
audit**



[intrusion detected]
**network
anomaly
observed**



[intrusion detected]
**virus
signature
matched**

[zero-day exploit]

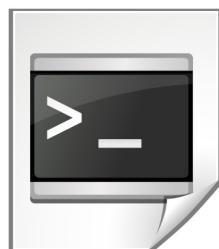
buffer overflow

EB F6
52 00
90 80
4E Ff

compromise any node
and move any hacker
to that node

[zero-day exploit]

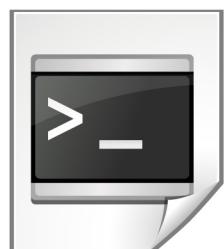
**format string
vulnerability**



compromise
any node

[zero-day exploit]

**integer
overflow**



compromise
any node

[zero-day exploit]

logic bomb



compromise
any node

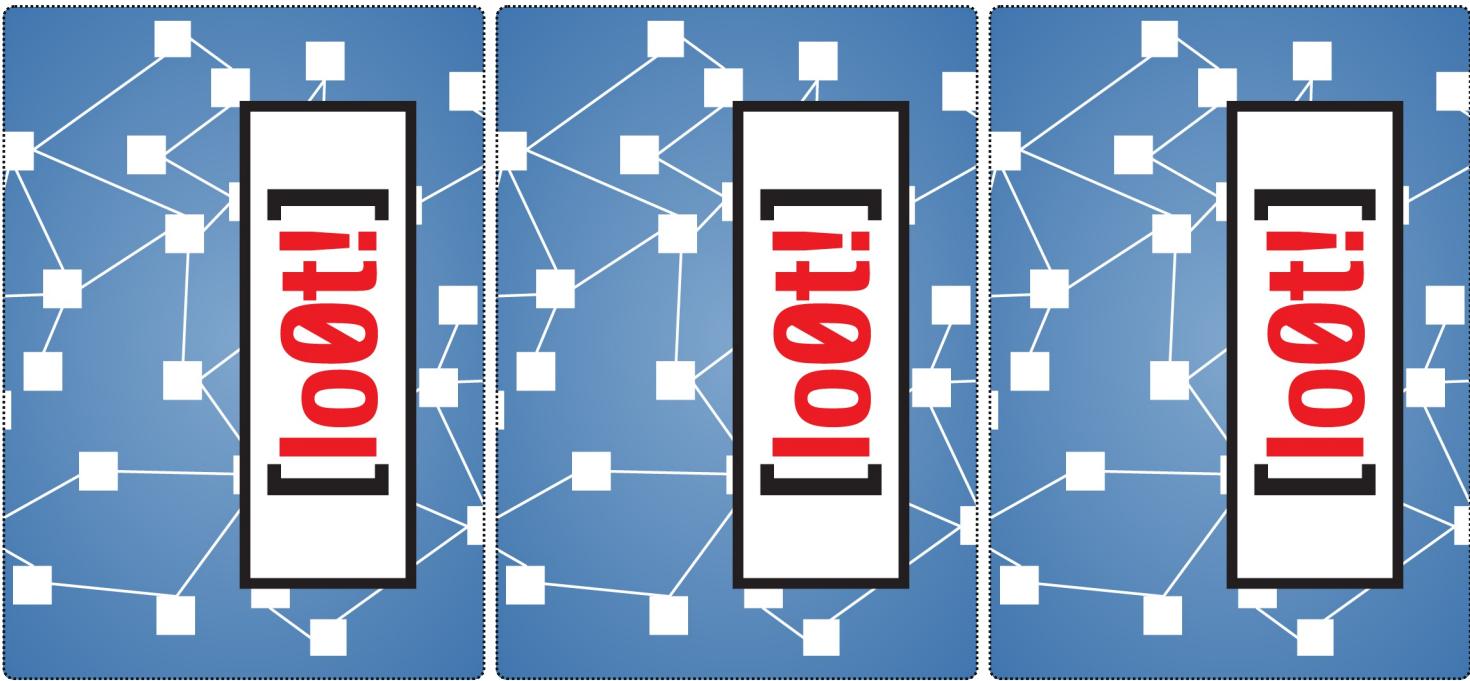
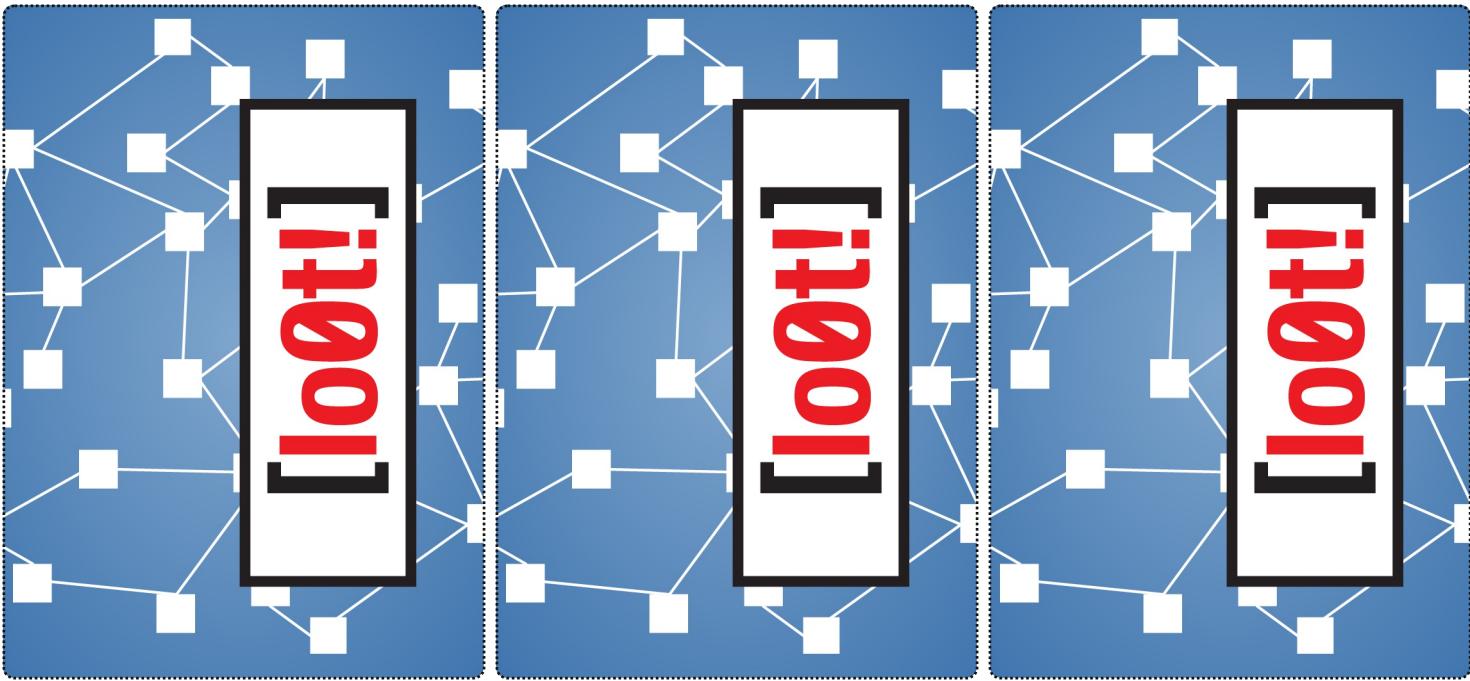
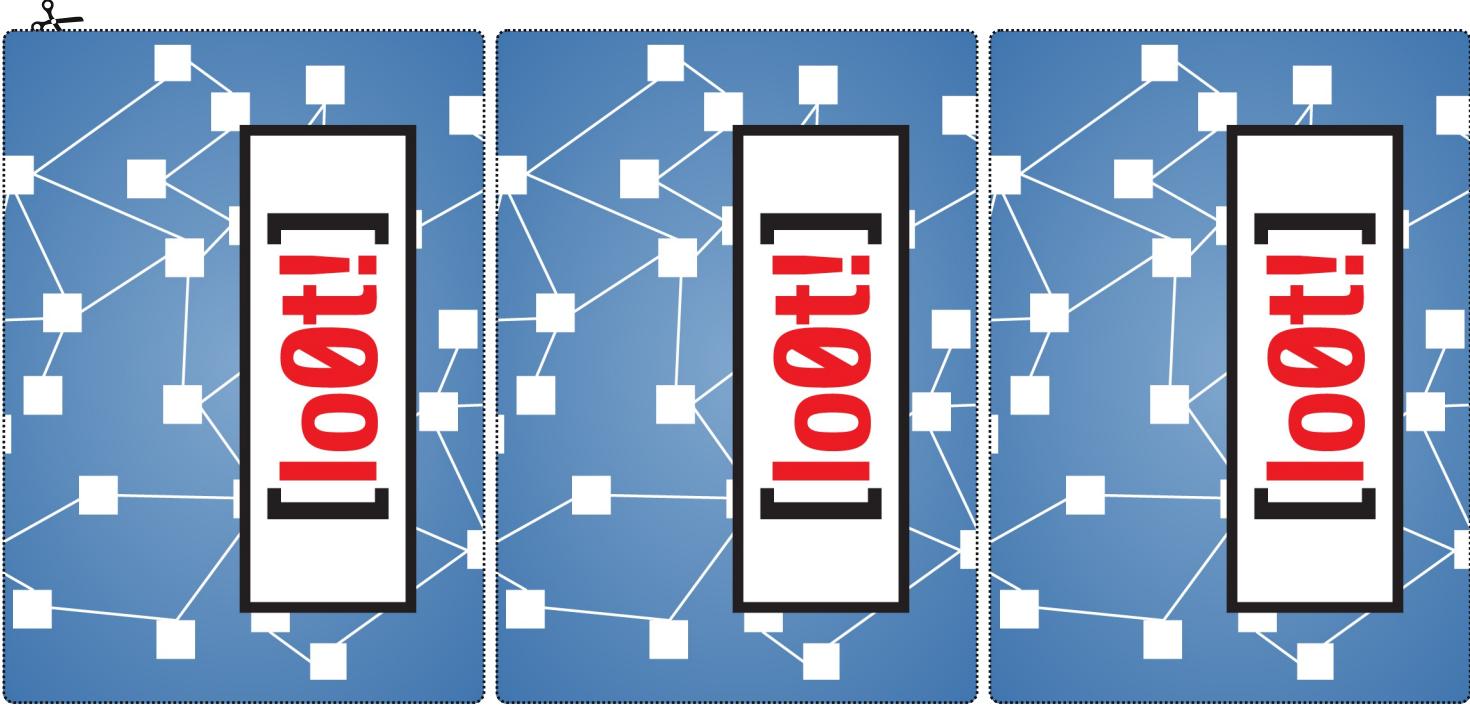
[zero-day exploit]

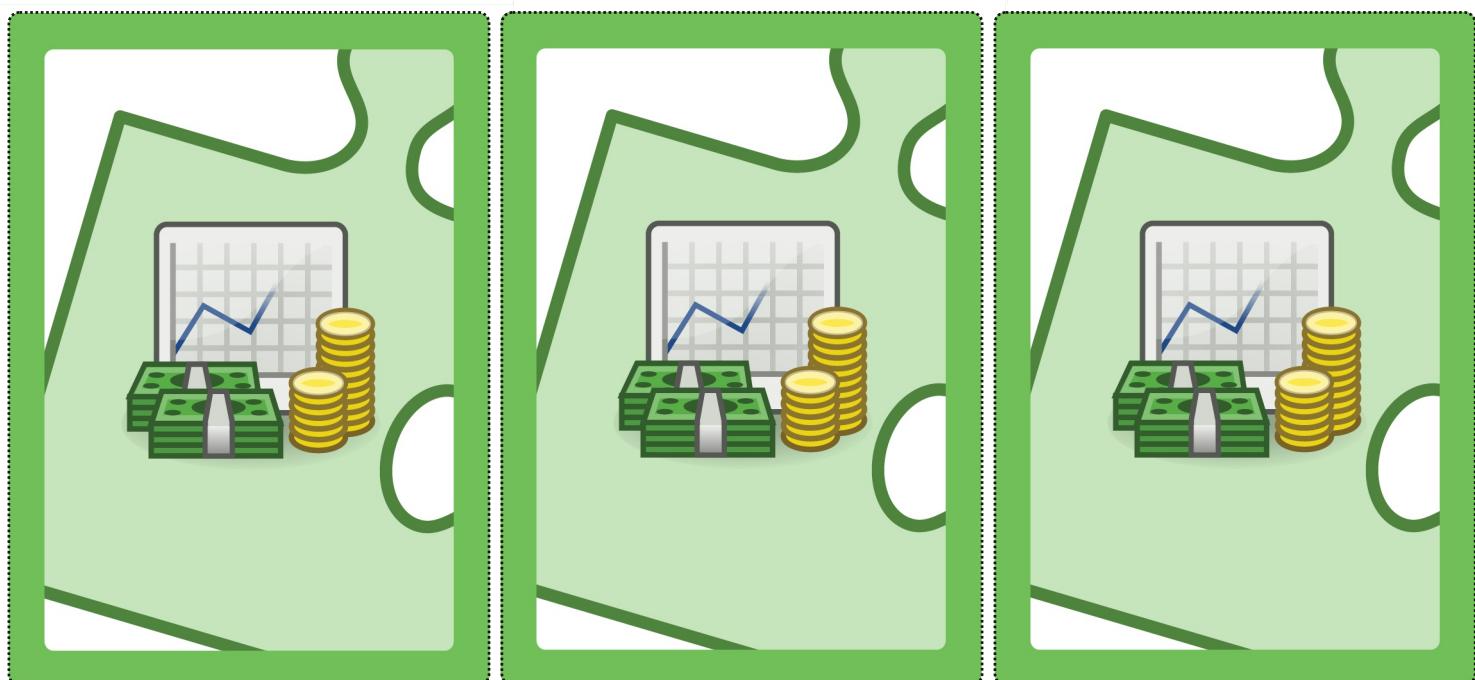
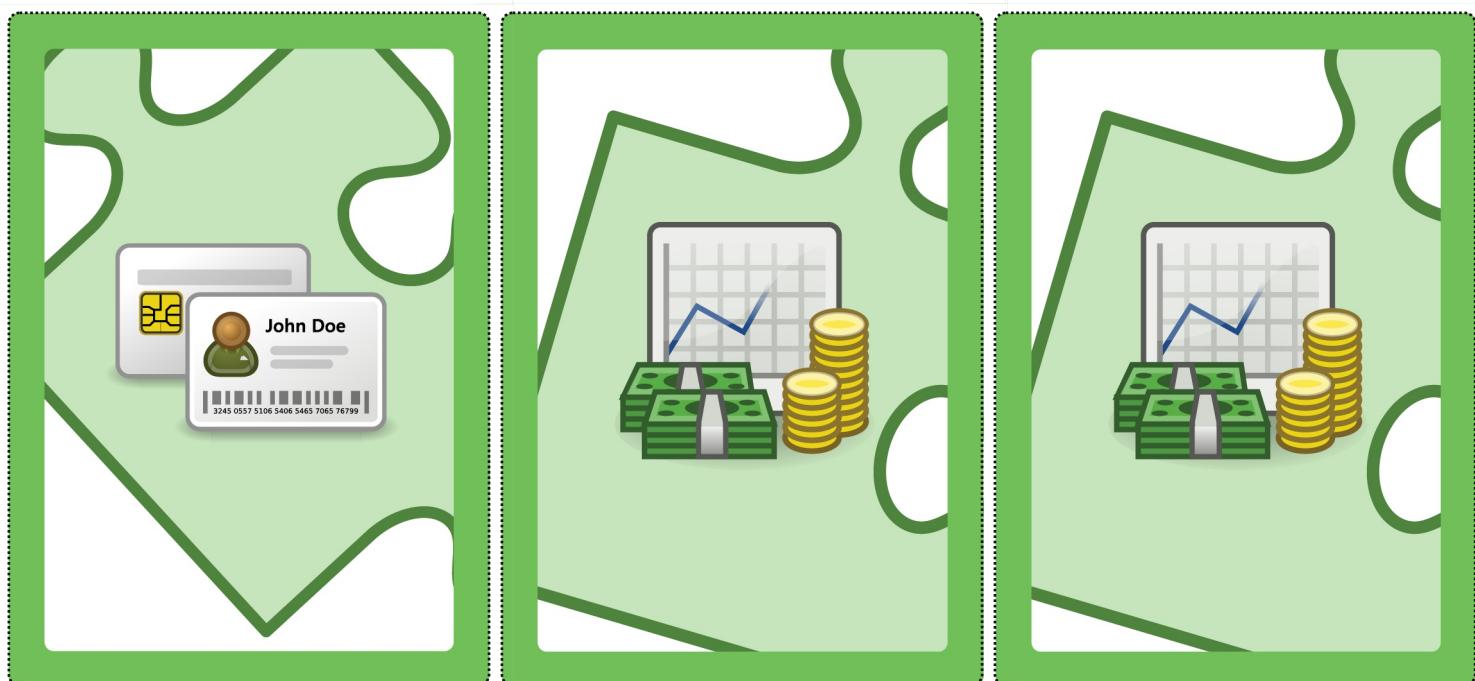
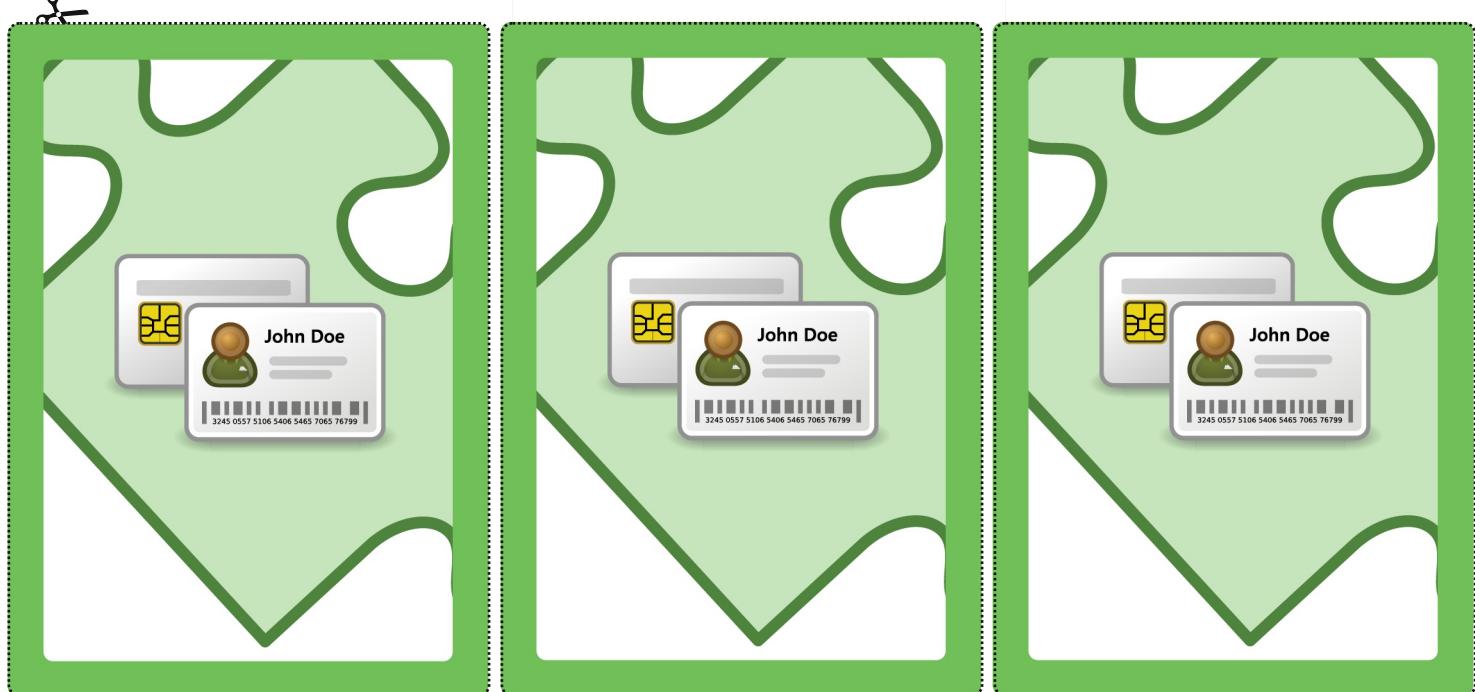
trojan horse

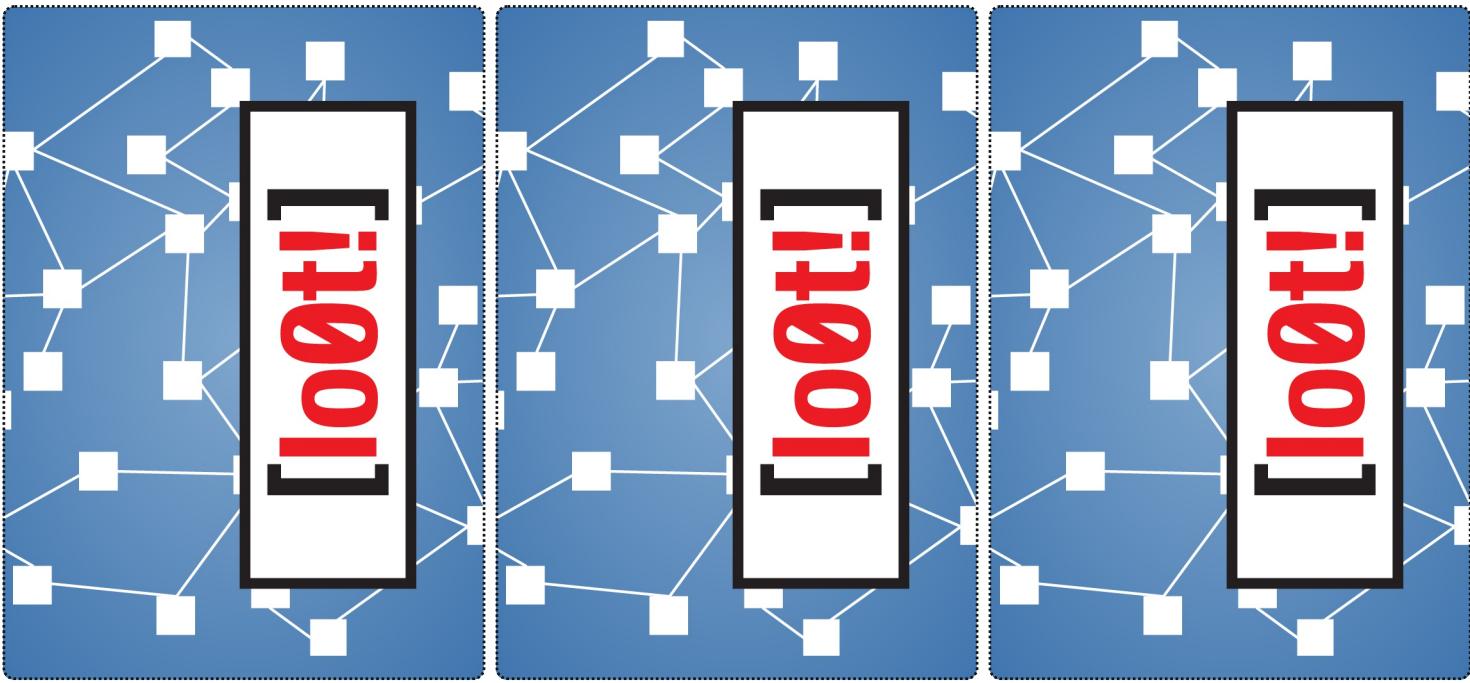
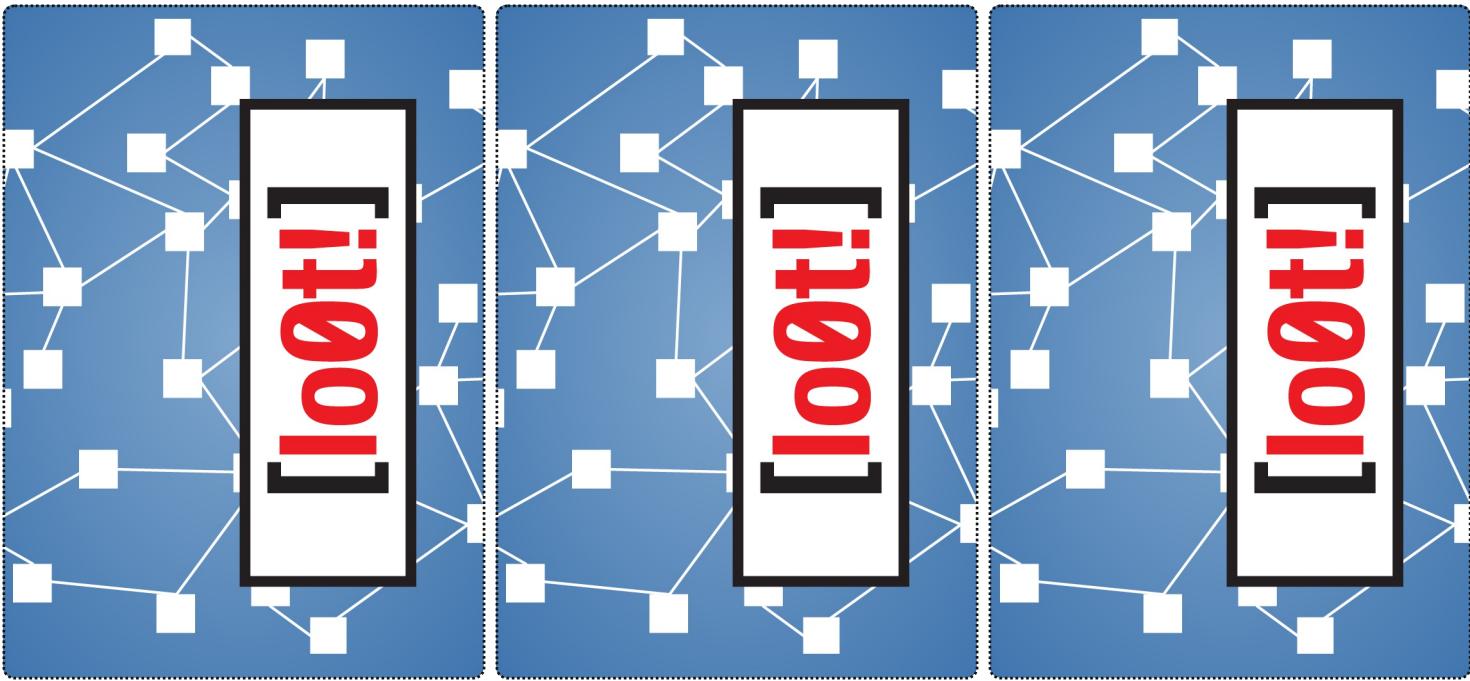
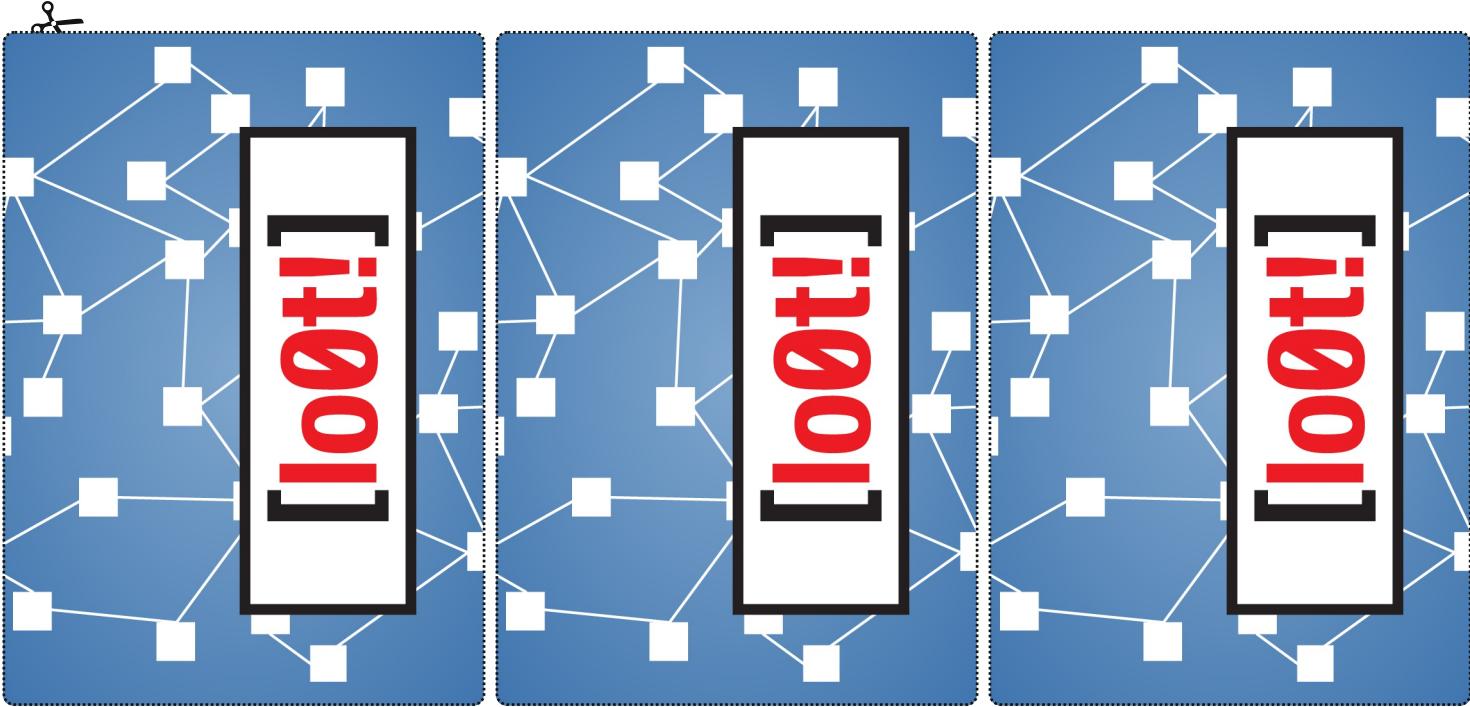
EB F6
52 00
90 80
4E Ff

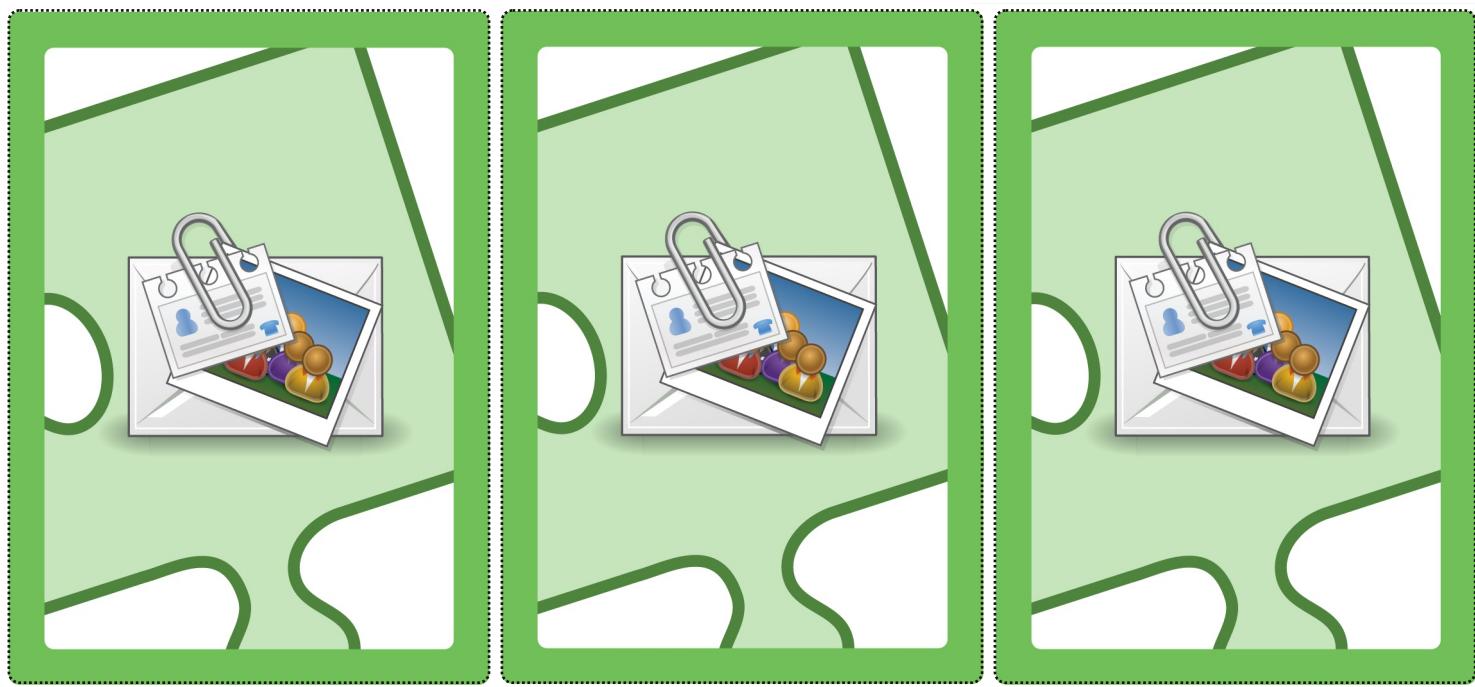
compromise any node
and move any hacker
to that node

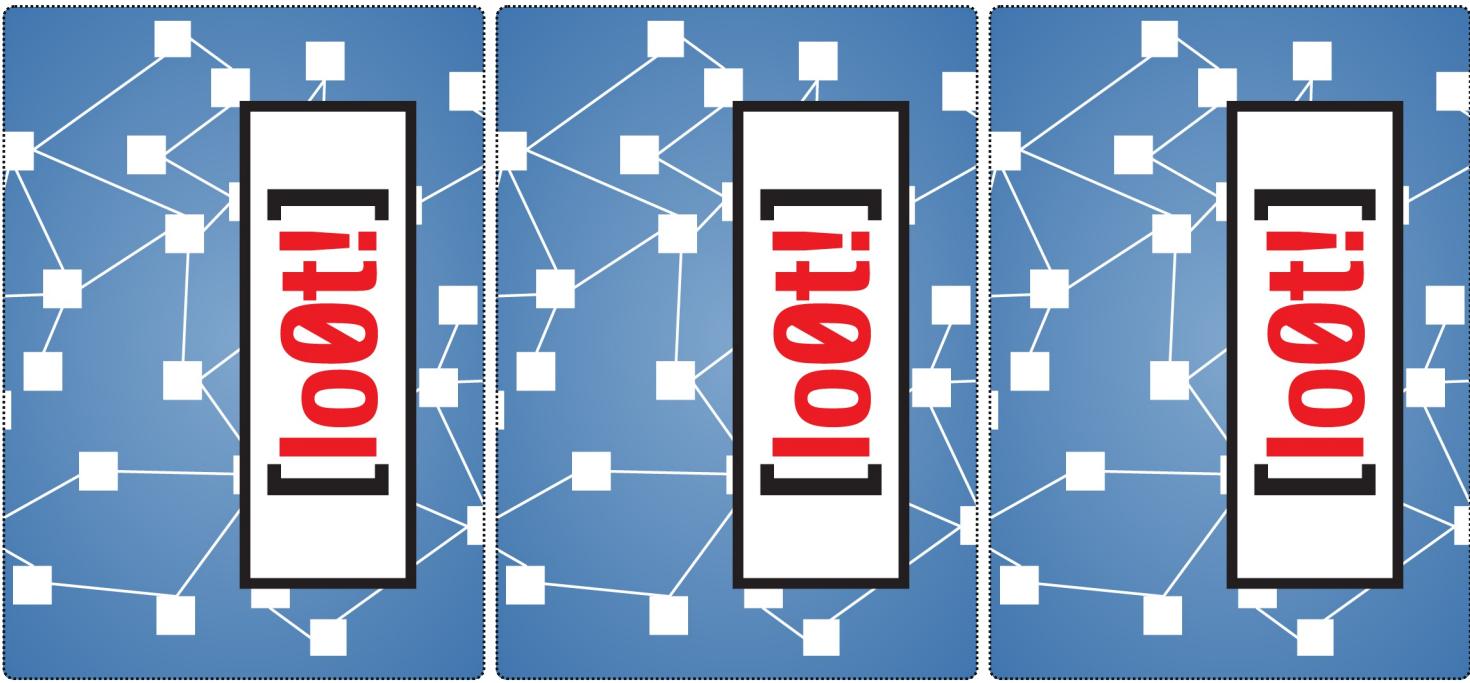
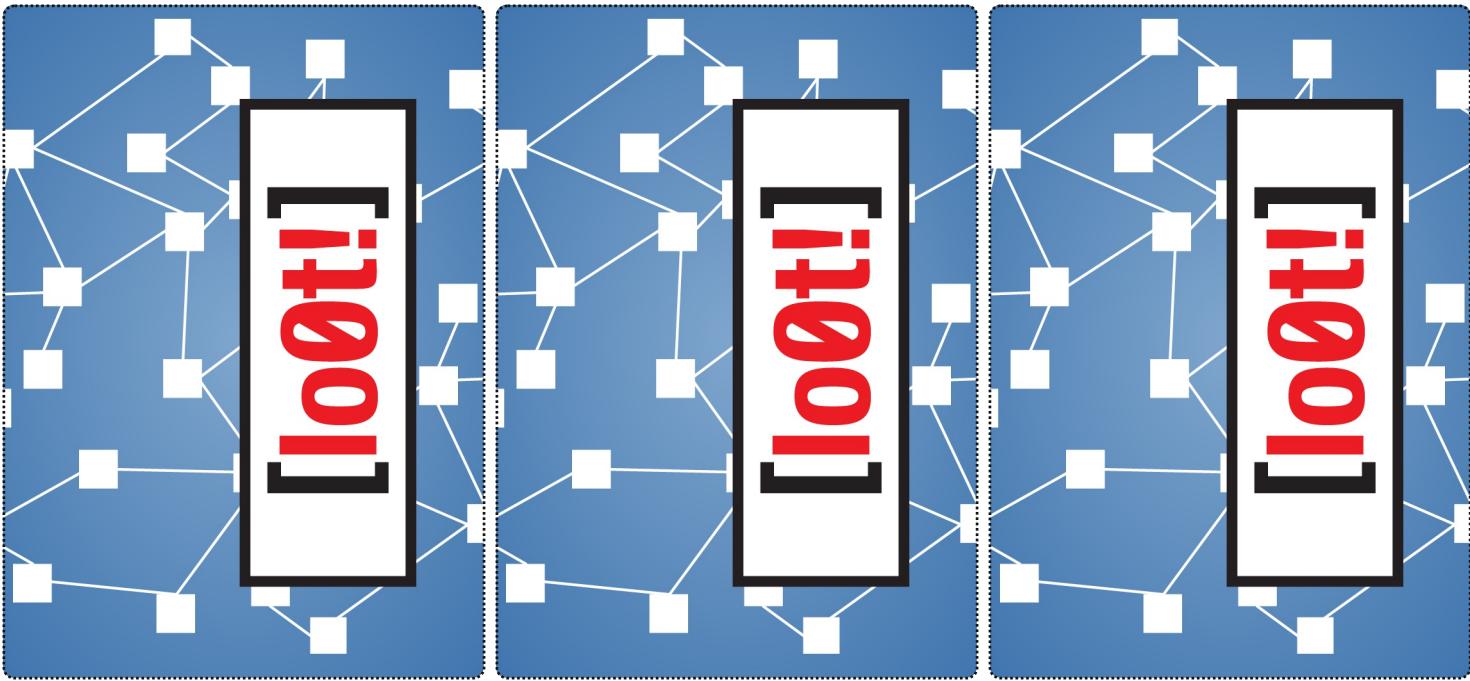
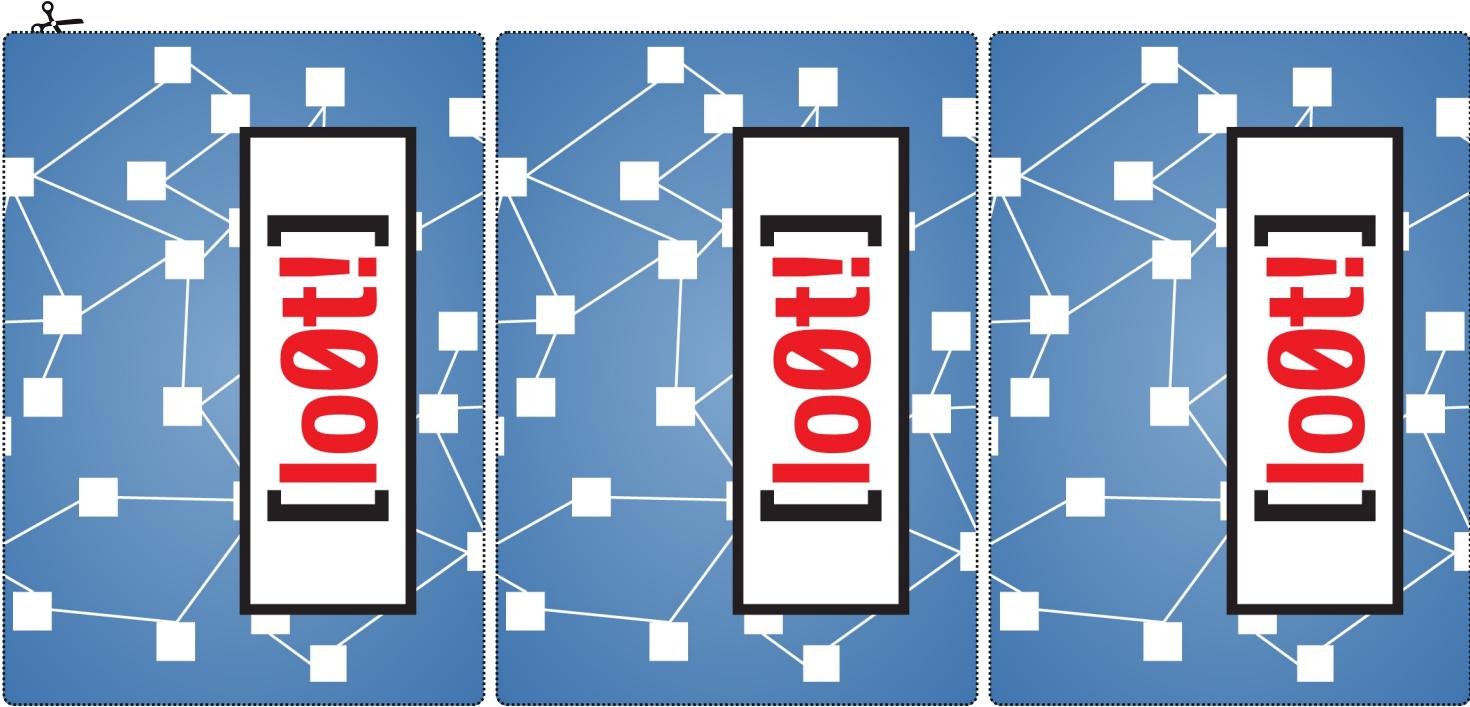














**backup
file server**



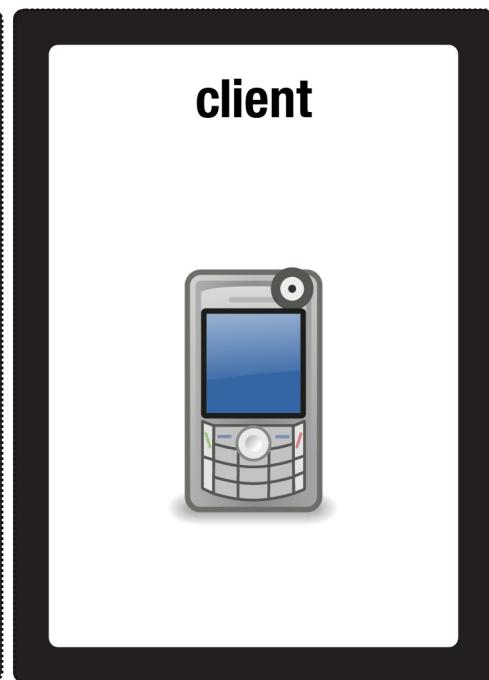
**certificate
services**



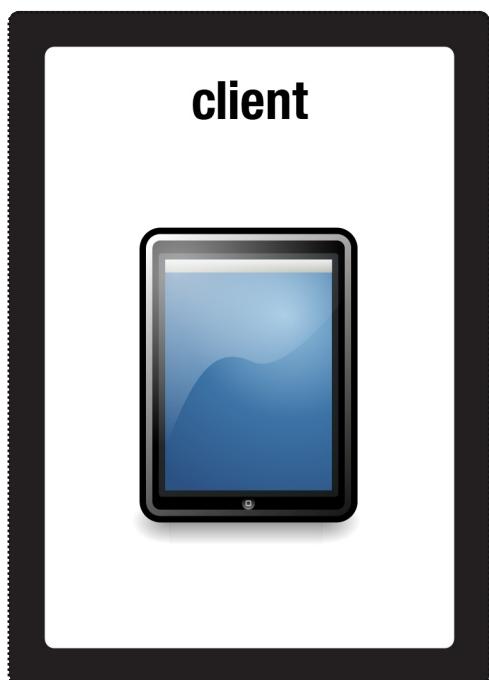
**chat
server**



client



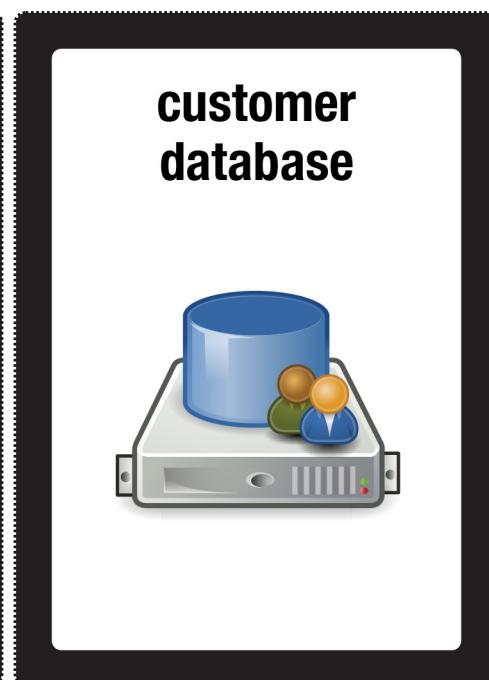
client



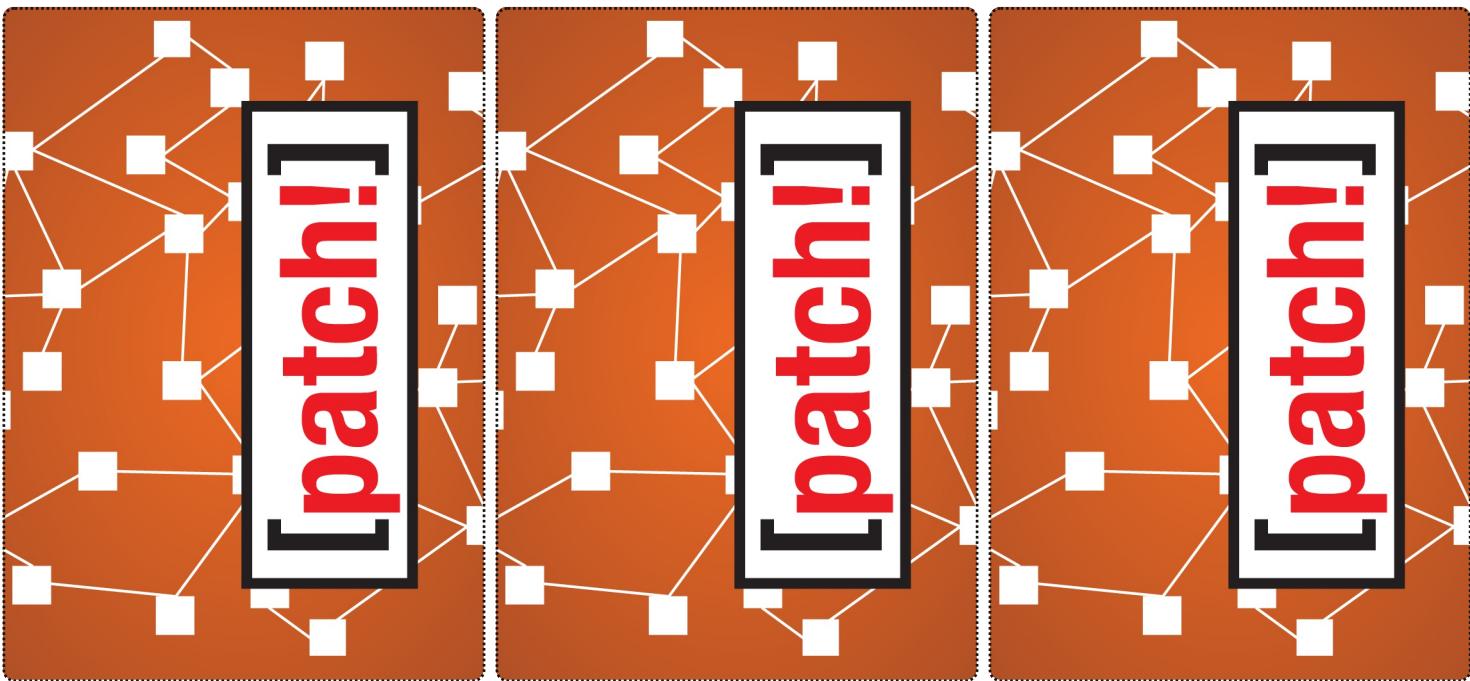
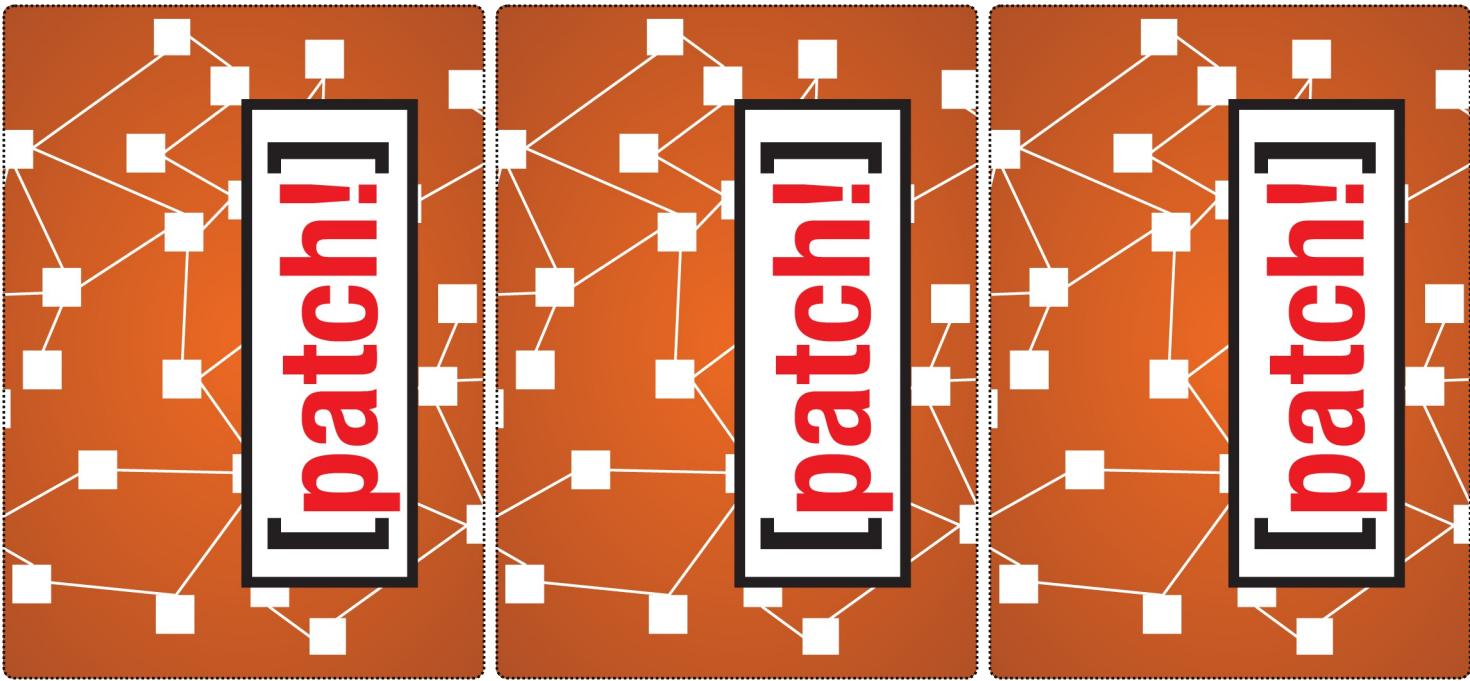
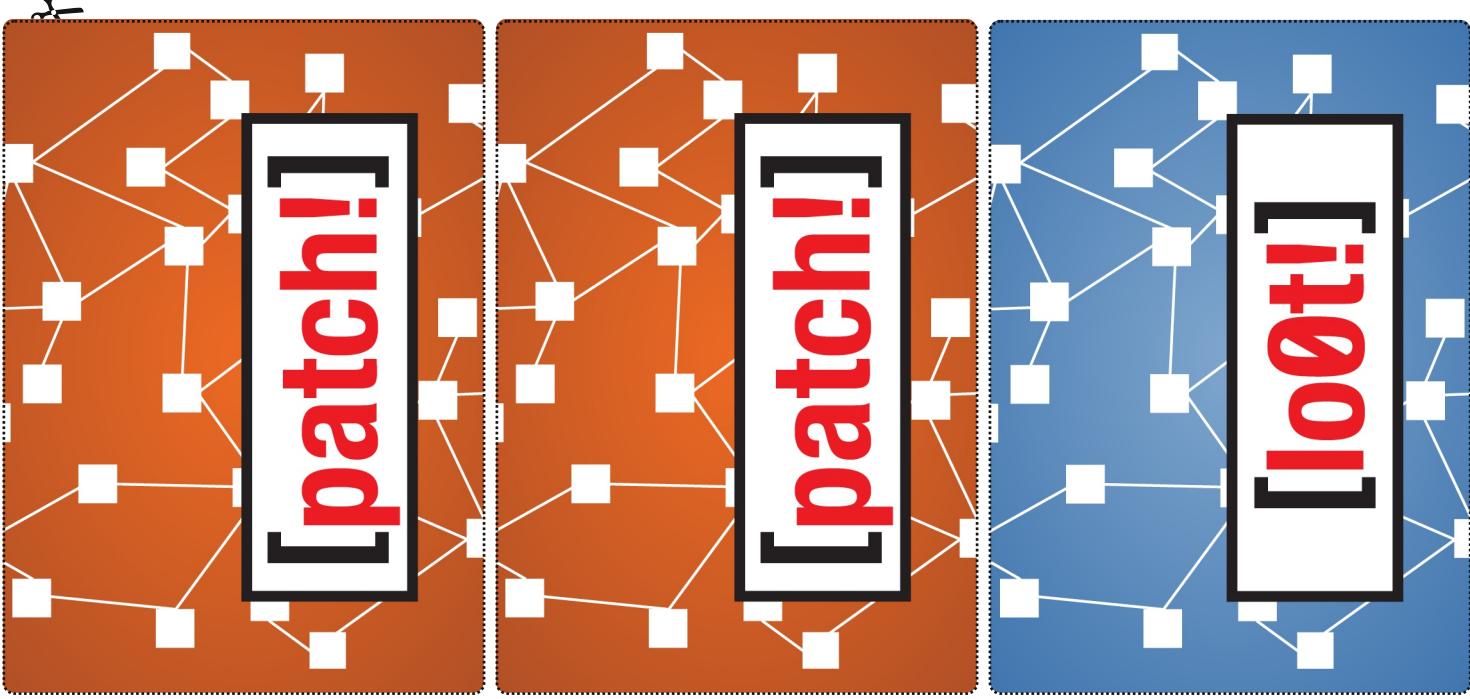
client



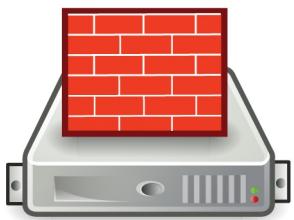
client



**customer
database**



firewall



IMAP server



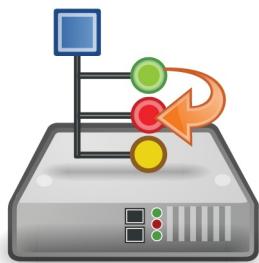
internet gateway



**intrusion
detection
system**



NAT device



**network
file server**



**primary
DNS server**

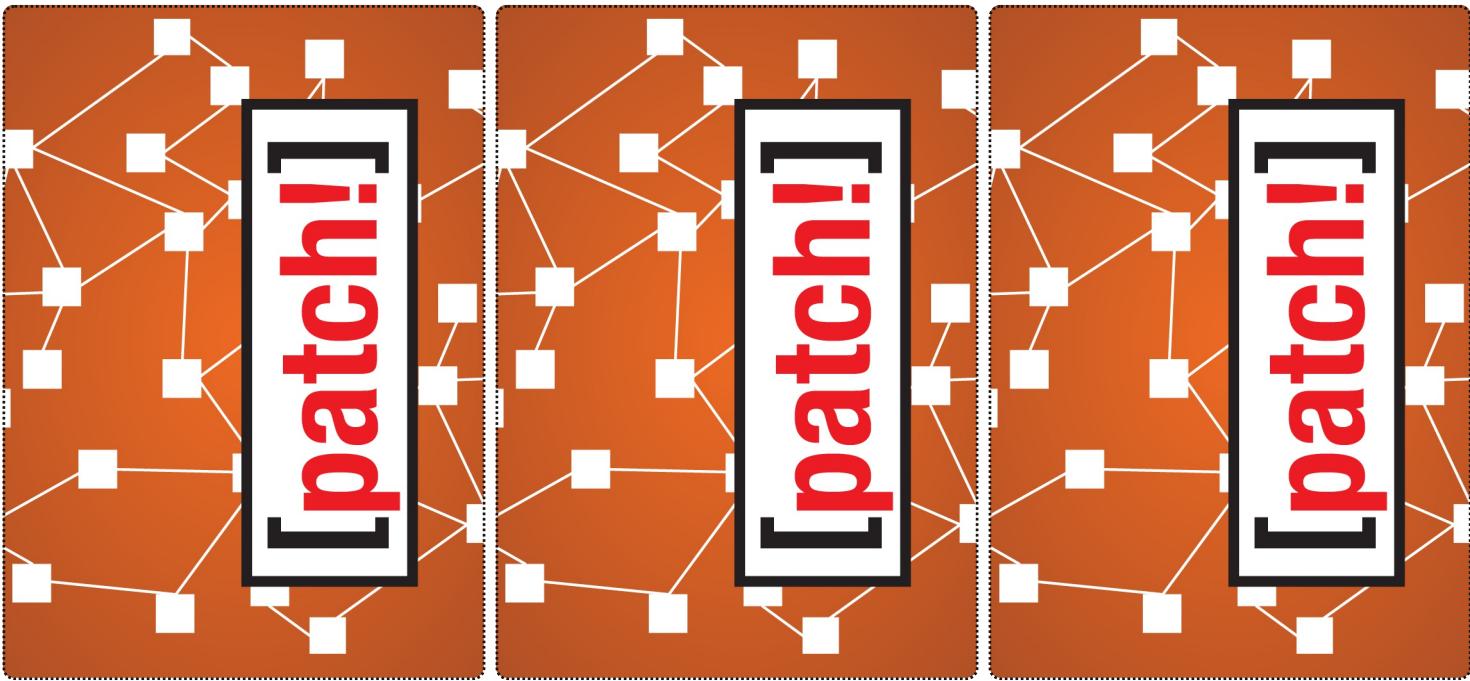
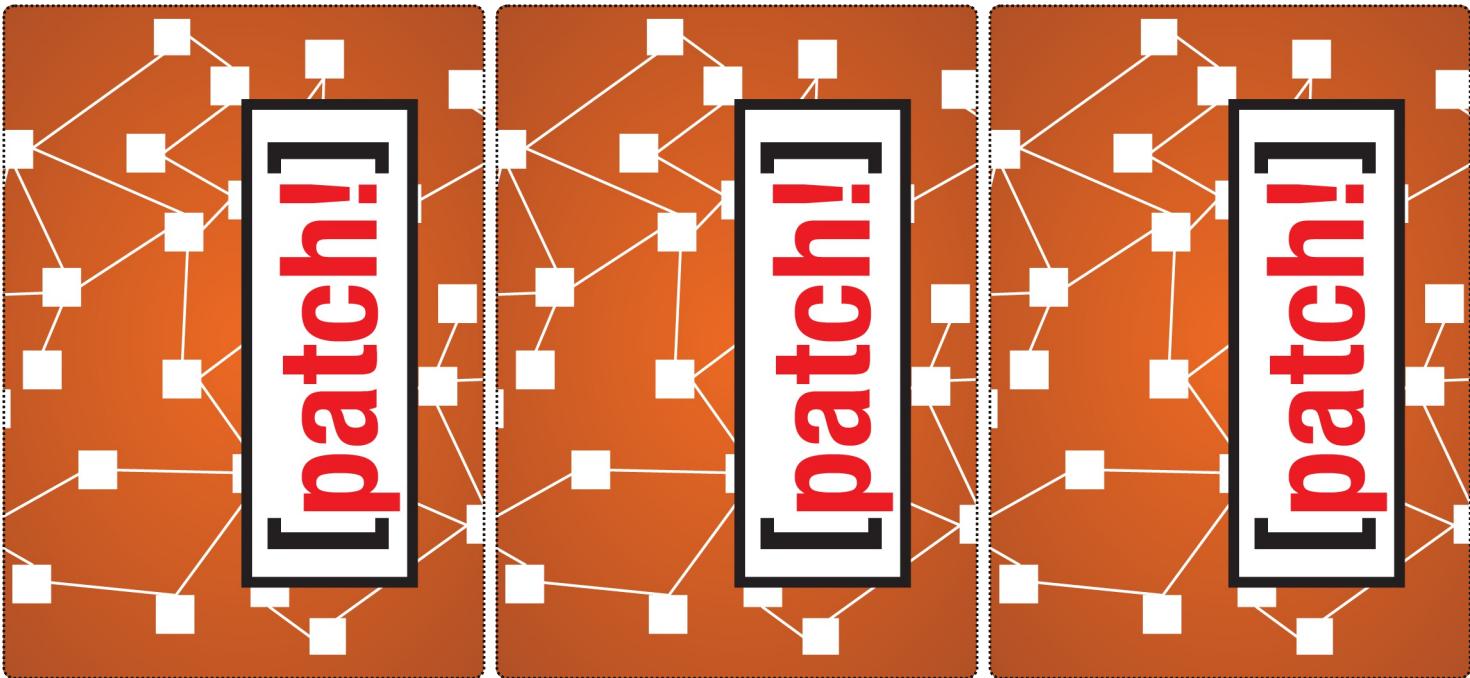
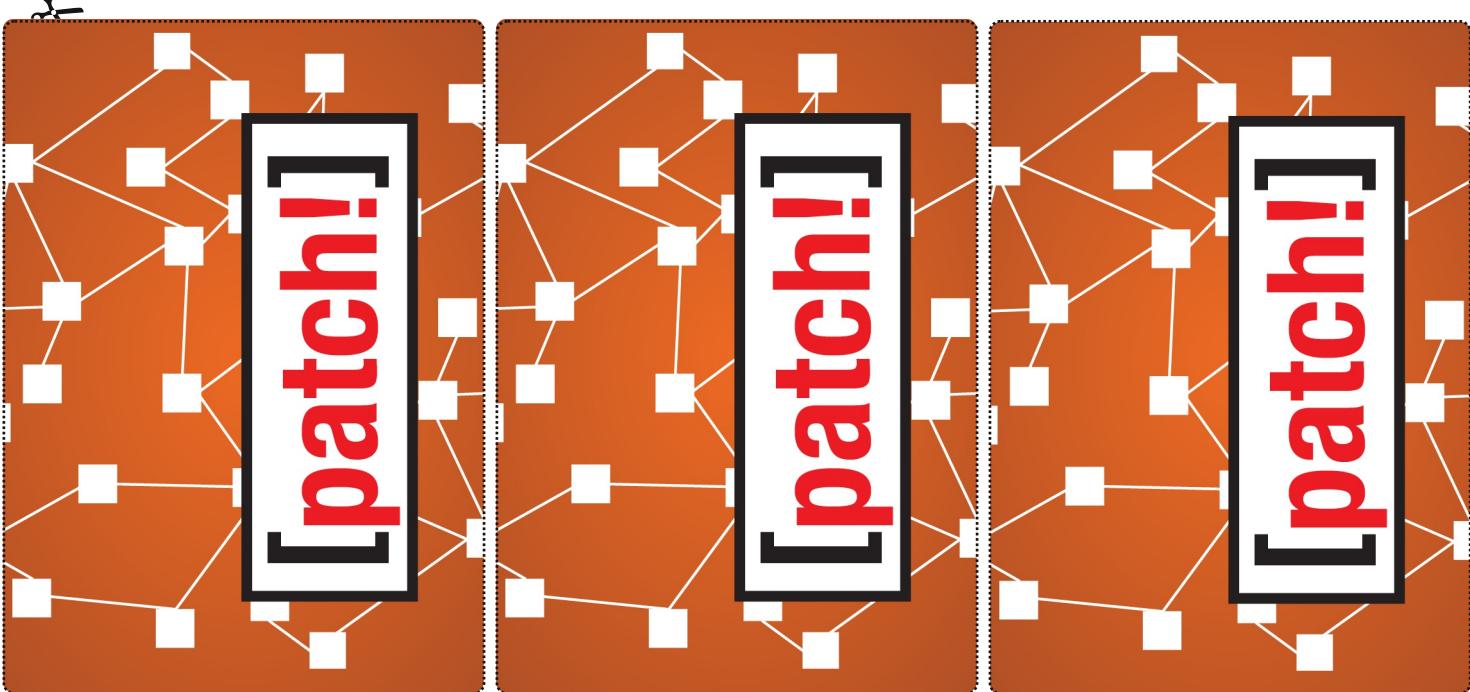


**sales
database**



**secondary
DNS server**





SMTP server



single sign-on service



single sign-on service



VLAN switch



VoIP server



VPN gateway



web server

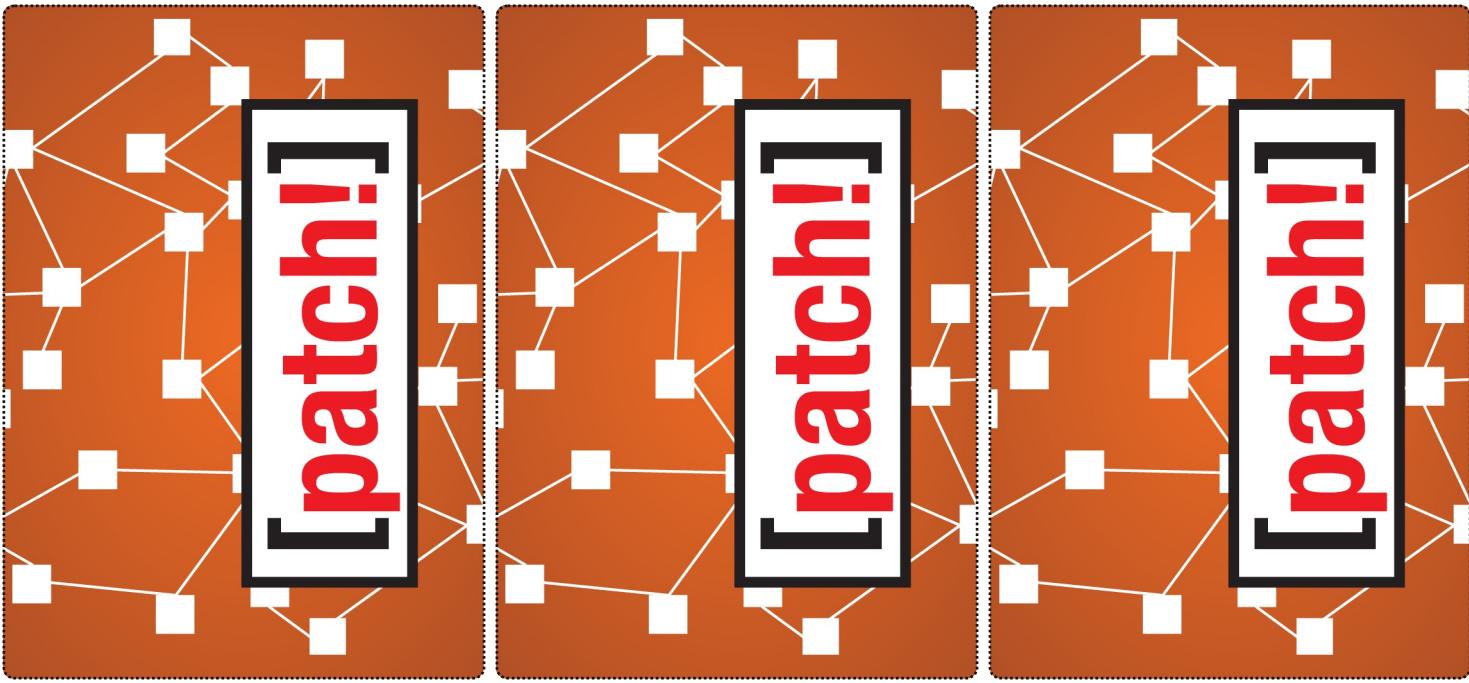
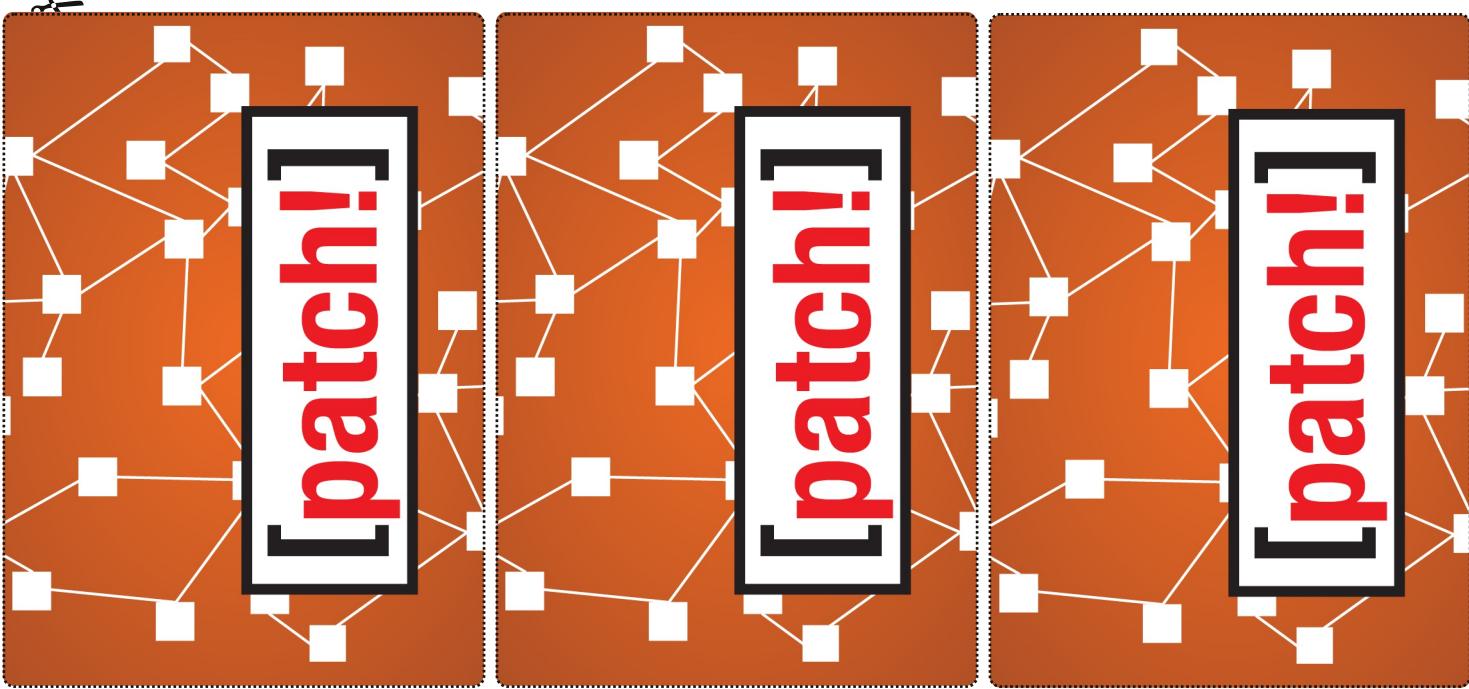


wireless router



order of play

1. **[action]**
Take up to 3 actions:
[move], [compromise], [drop],
[give], [exchange], [pickup],
[recover]
2. **[loot]**
Draw 2 [IoT!] cards. Resolve
[intrusion detected] and
[honeypot audit] cards.
3. **[patch]**
Draw and resolve [patch!] cards,
as indicated by the
[infocon] level.
4. **[check]**
Discard, to obey the hand
limit.



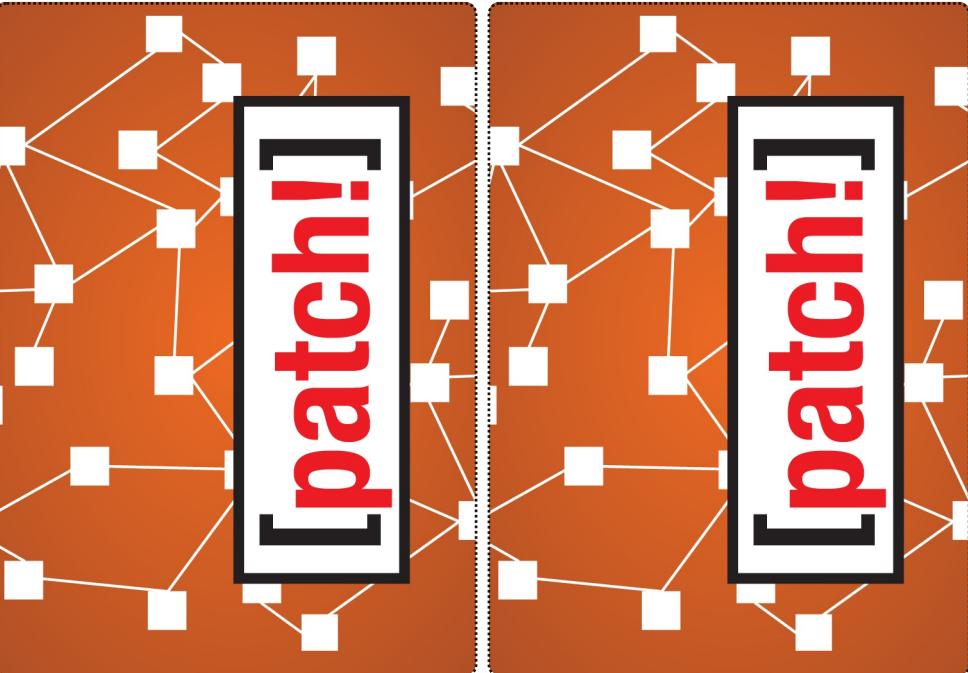
[intrusion detected]: Raise the **[infocon]** level.

[honeypot audit]: Immediately draw a **[patch!]** card. If the pictured **[node]** is compromised, raise the **[infocon]** level.

[check]: The hand limit is five cards. Every card in excess of the hand limit must be discarded. You may play **[zero-day exploits]** before discarding them.

[patch] situations:

- Any **[IoT!]** cards left on a **[node]** being patched are discarded.
- If a player is on a node being patched, she must **[move]** to a compromised node (obeying normal movement rules), then **[decommission]** the node and its **[patch!]** card.
- **[zero-day exploits]** can be used to prevent all **[patch]** effects.



backup file server



certificate services



chat server



client



client



client



certificate services



backup file server



client



chat server



client



client



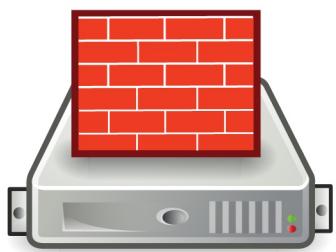
client



customer database



firewall



requires two actions
to compromise

IMAP server



internet gateway



intrusion detection system



requires two actions
to compromise

customer database



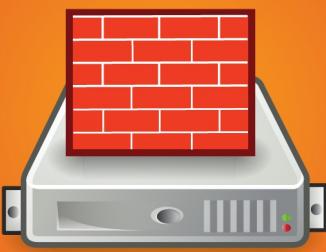
client



IMAP server



firewall



requires two actions
to compromise

intrusion detection system

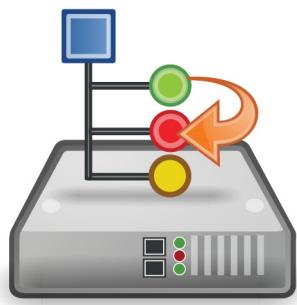


requires two actions
to compromise

internet gateway



NAT device



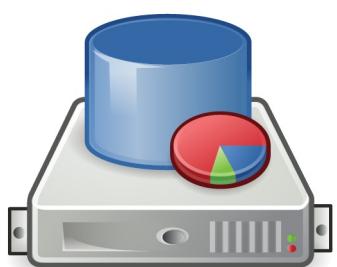
network file server



primary DNS server



sales database



secondary DNS server



SMTP server



network file server



NAT device



sales database



primary DNS server



SMTP server



secondary DNS server



single sign-on service



VLAN switch



VoIP server



VPN gateway



requires two actions
to compromise

web server



wireless router



VLAN switch



single sign-on service



VPN gateway



requires two actions
to compromise

VoIP server

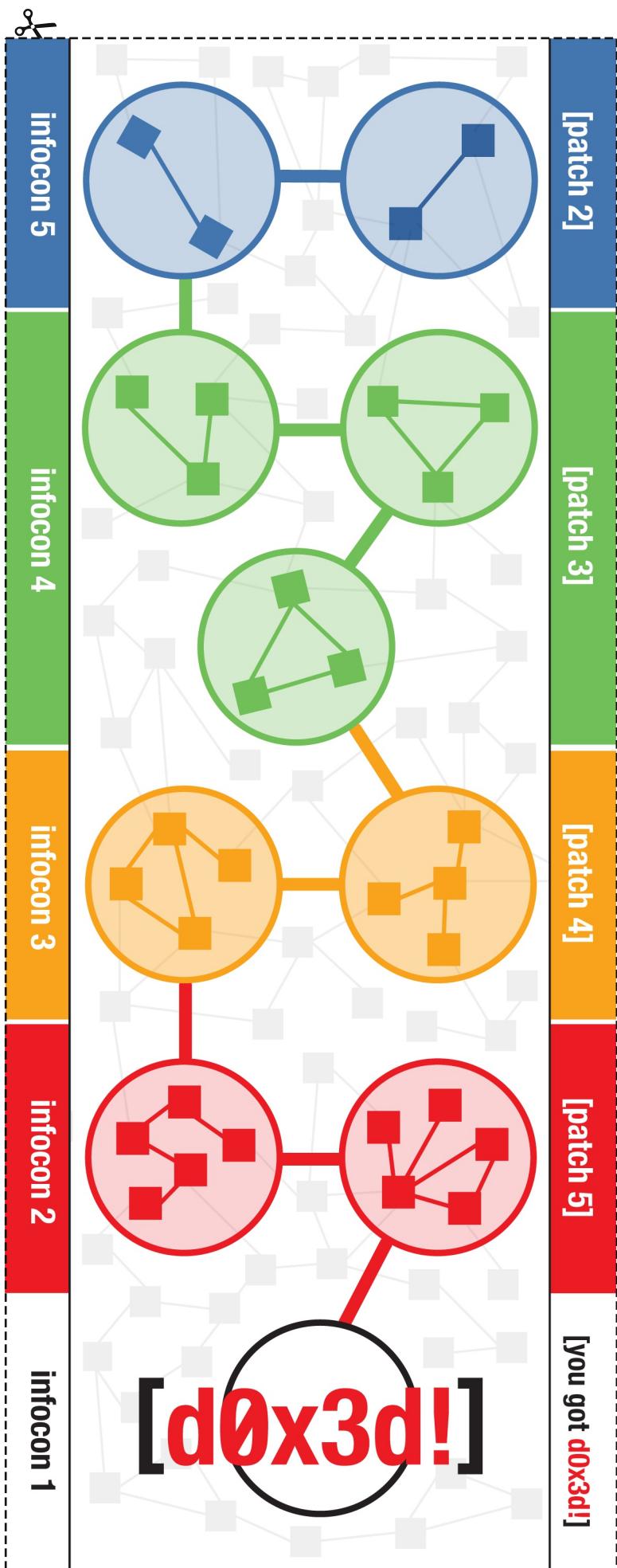


wireless router



web server





infocon 5

infocon 4

infocon 3

infocon 2

infocon 1

[patch 2]

[patch 3]

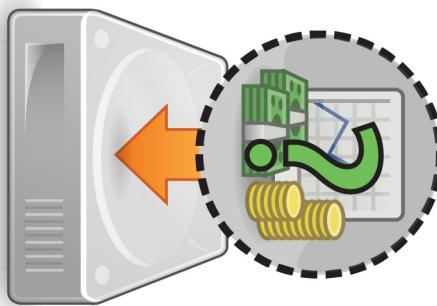
[patch 4]

[patch 5]

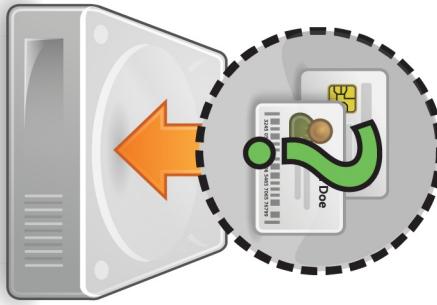
[you got d0x3d!]

[digital asset drives]

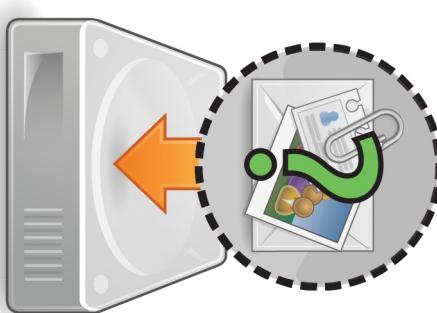
financial
data



authentication
credentials



personally
identifiable
information



intellectual
property

