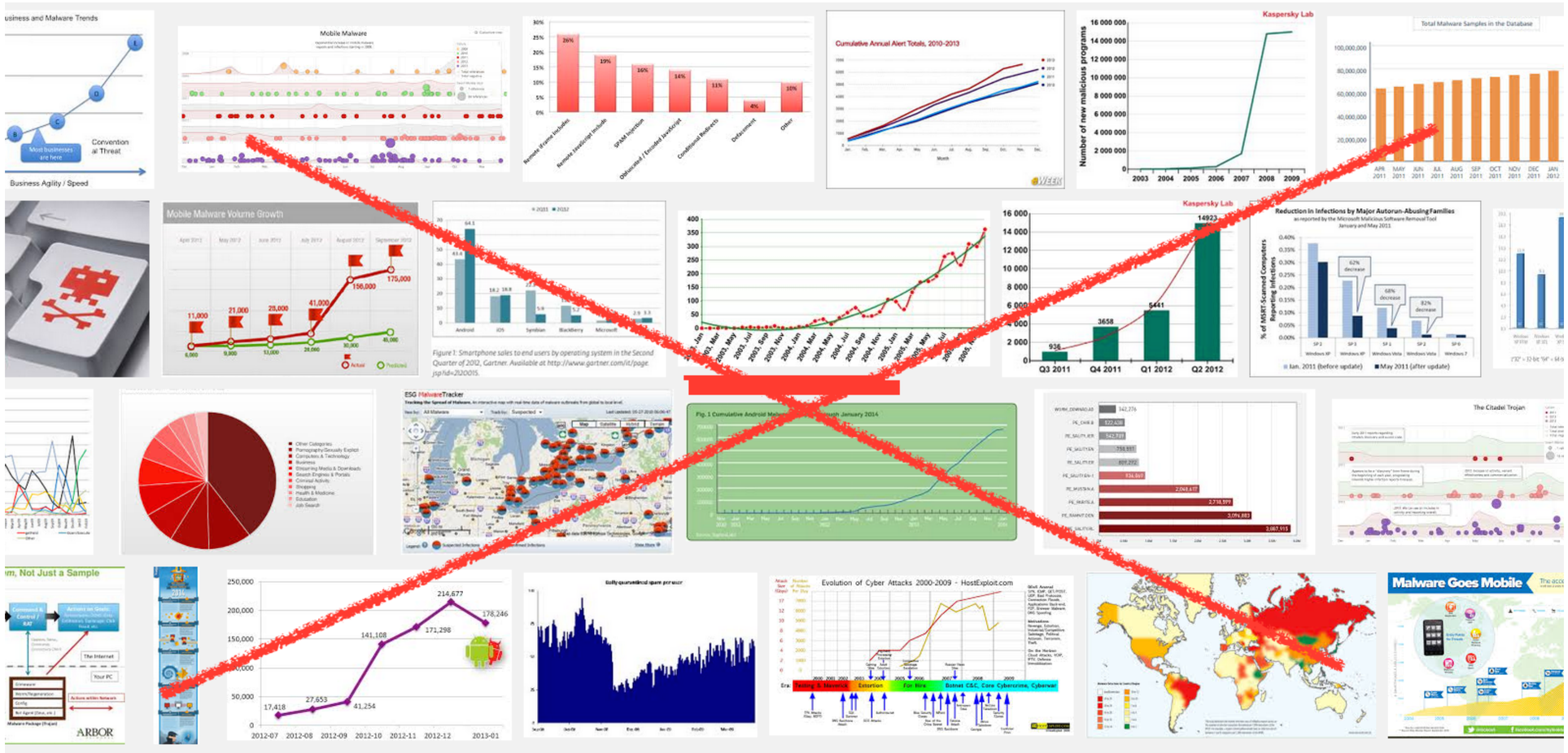
Cybercrime Trends –Things are Going to Get Interesting

Shmulik Regev, Head of Security Innovation | IBM Security



Trends ?

Let’s roll up our sleeves

A game, a spoiler, some good and some bad news

- Pacman anyone?
- Spoiler - the bad guy wins.
- The good news - we'll learn how to significantly reduce the risk.
- The bad news - it requires additional work.
- More good news - you are less likely to get fired.

Before we start

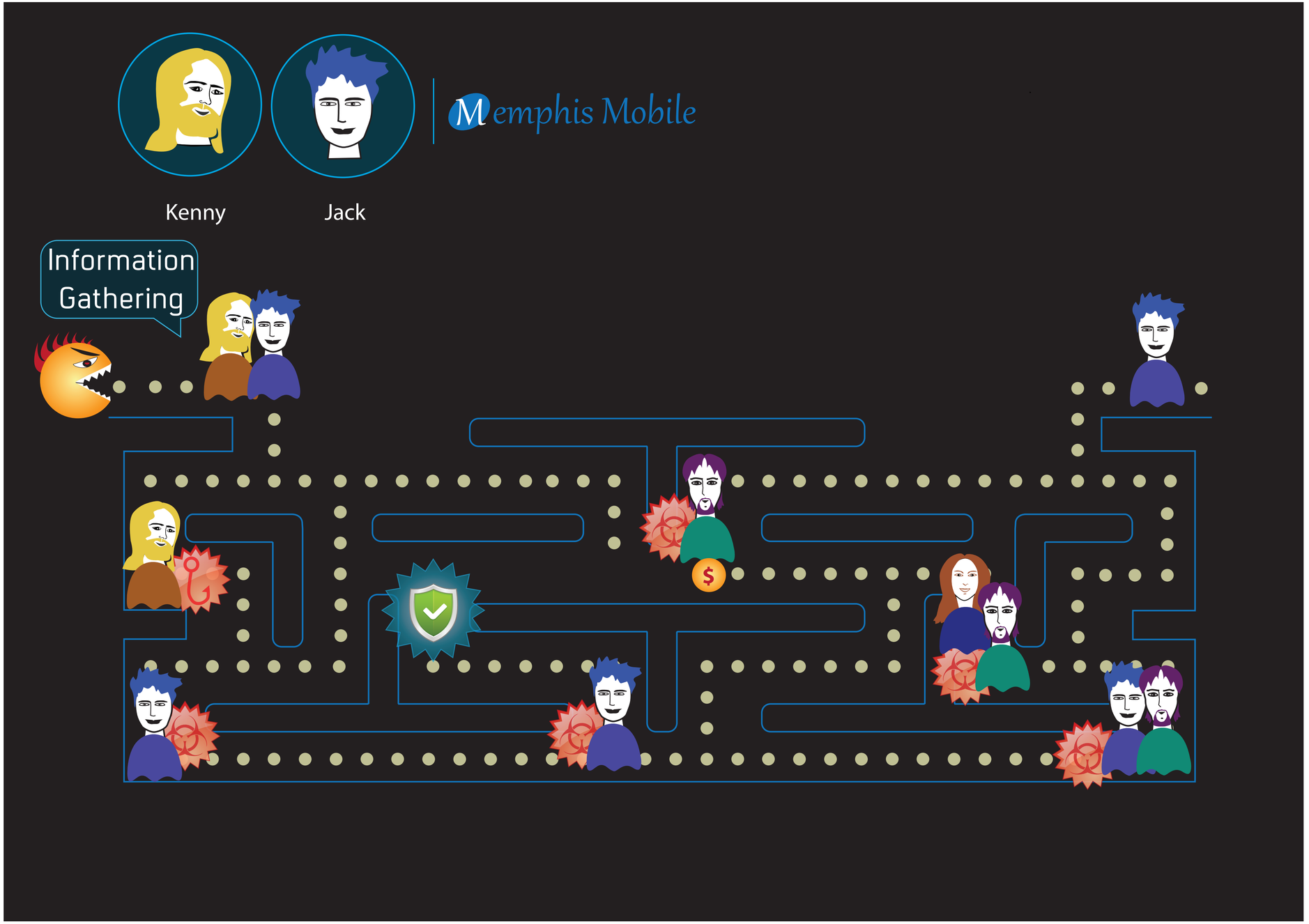
- We'll cover real world techniques used by real adversaries.
- However, this particular attack never happened (as far as we know).
- Note that such attacks can take several weeks to conduct and are rarely fully automatic.

The Playground

- Company:

  Memphis Mobile

- Employees:
  - Kenny - Procurement
  - Jack - System Administrator
  - Bob - DBA
  - Bill - Network Administrator
  - Dawn - application developer

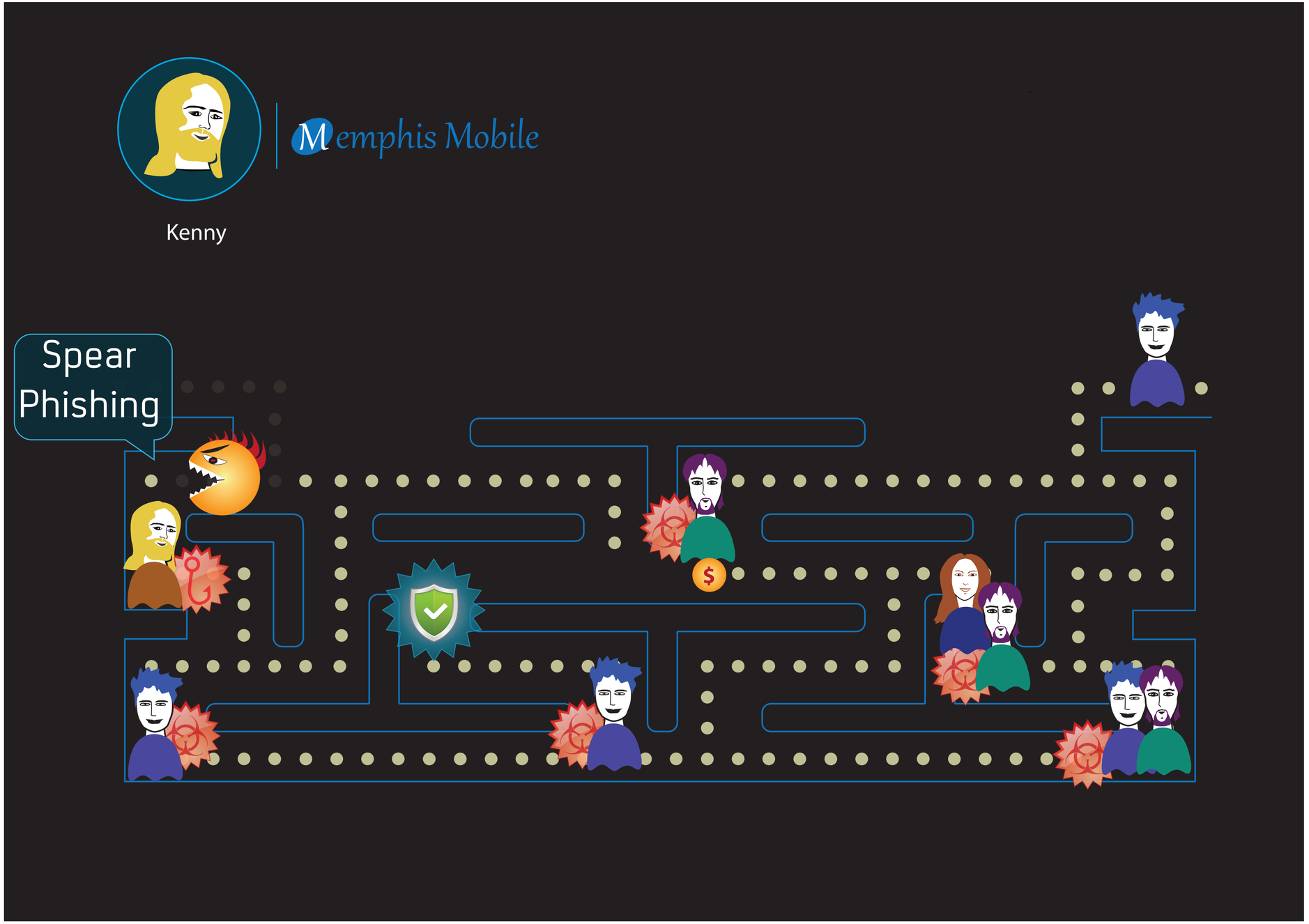


Information Gathering - it is out there

- Using Linkedin - locating employees working for Memphis Mobile.
- The profiles of Kenny and Jack were found.
- Turns out Kenny is from Procurement.
- And Jack is an avid banjo player (belongs to the Memphis banjo players club). It wasn't listed in his profile, but searching for his (company) email address revealed frequent posts at the club forum.

Information Gathering - it is out there

- There are perfectly legit tools to conduct such activities.
- LinkedIn is a great place to harvest data on employees and especially senior executives.
- 77% of employees use their work email to sign up for personal accounts on the Internet.



Spear Phishing attack

- Kenny gets an email with the title "Order information" and a pdf attachment.
- Kenny works with a lot of external parties so he opens this document. It is all Chinese to him, so he closes it.
- BUT - this was an infected document.
- It had an exploit making use of a known vulnerability.

Spear Phishing attack - how can we handle it

- Regular updates and monitoring of the computer hygiene.
- Run an exploit prevention tool.
- Very strict - open attachments only on highly secure virtual machines. Very hard to follow.

Phishing Trends

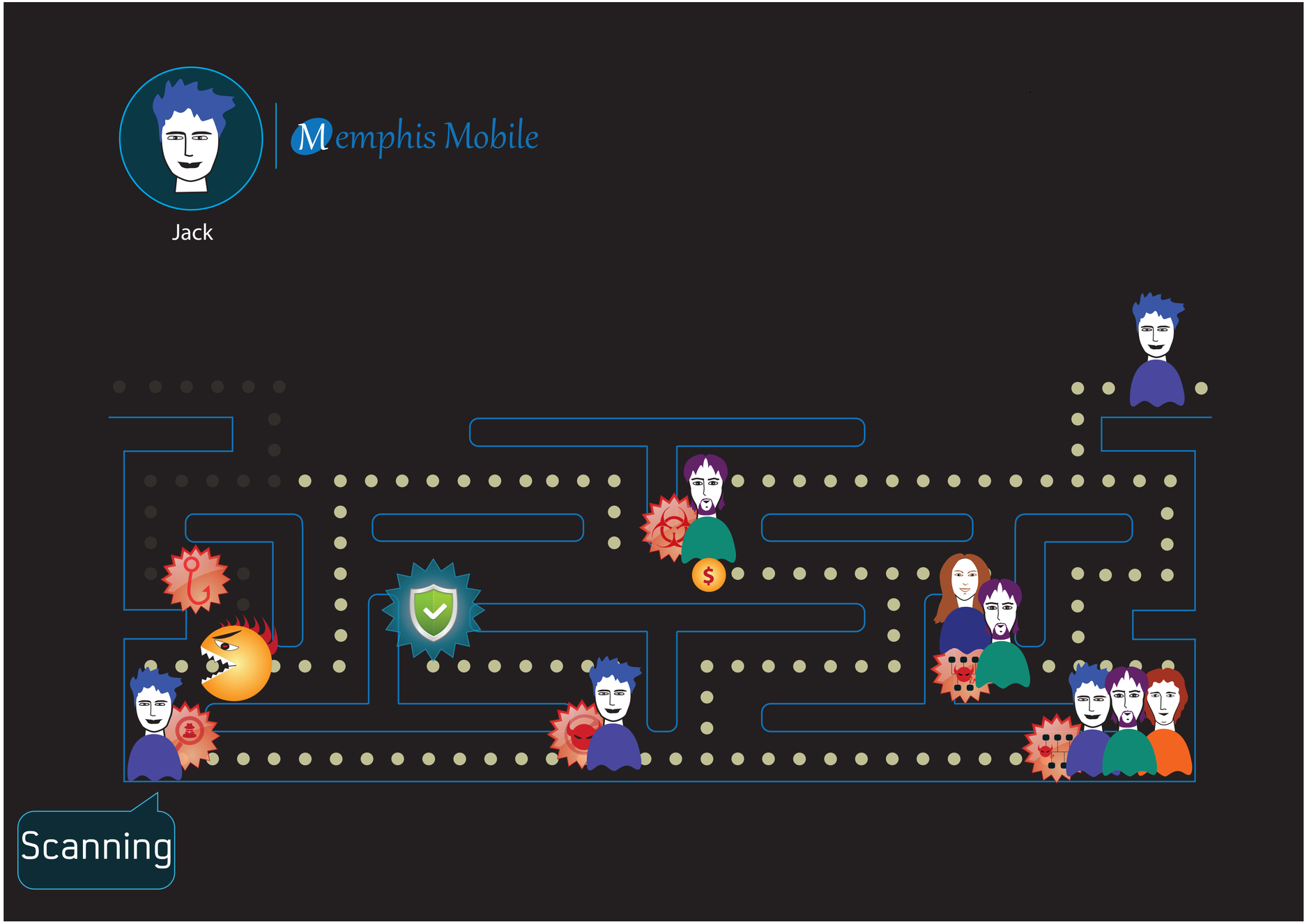
- Image based phishing
- PAC file usage
- Geography/Culture related, e.g. Japan & Brazil ask for ID, Passport scans.
- Social engineering makes the user enable macros to facilitate the exploit (including UAC bypass)

A bit more about the attack

- The exploit lets the attacker runs his code on the machine. He "owns" the machine.
- Frequently the actual payload is downloaded from the Internet. It can be from a compromised host, or from a legitimate cloud service etc.
- The payload is often polymorphic i.e. it will escape simplistic detection. If it is packed/encrypted (many are) it is hard to detect them on the network level also.
- The malware will try to gain persistency on the machine so it'll survive reboot. It may even generate a local user (in the RDP group for example) to retain access even if/when deleted!
- It will hide itself in some popular folder (system, temp), and deletes the dropper.
- A RAT (Remote Access Tool) is installed. It has a keylogging module, network scanner, VNC like interface, remote shell (command prompt). These tools aren't necessarily malicious, i.e. you can legitimately buy them.

Malware - Trends

- Sandbox based dynamic analysis is nowadays frequently bypassed.
- Agile malware development cycle. Dyre/Ramnit are updated weekly.
- Developed by gangs with startup mentality. Not an off-the-shelf malware.
- Analytics are used.
- Removal of other security tools.



Scanning

- Now the attacker has to map the network and move closer to the gold.
- Networking scanning reveals a domain called Servers. Sounds good.
- How do we get in? Let’s see if they have RDP access (port 3389)?
- Oh, they do. So we can try one of its known vulnerabilities. Sure it has been around for ages (August 2011) but not all servers are patched.
- Most of the servers are protected, but one, called "Win2k.hr" is vulnerable. Yoopee. we're in.

Scanning - What can be done

- Patch all systems. This particular one is a legacy system running an application no one knows how to maintain or update so it was left behind.
- Move legacy non upgradable servers to separate, risk reduced domain/ VLAN.
- Monitor **internal** network traffic and look for brute force scanning.

Bugs/Vulnerabilities - Trends

- Credentials grabbing, "redirect to SMB" - a 1997 bug discovered on April 2015! (https://securityledger.com/2015/04/windows-bug-from-1997-enables-credential-theft/) .

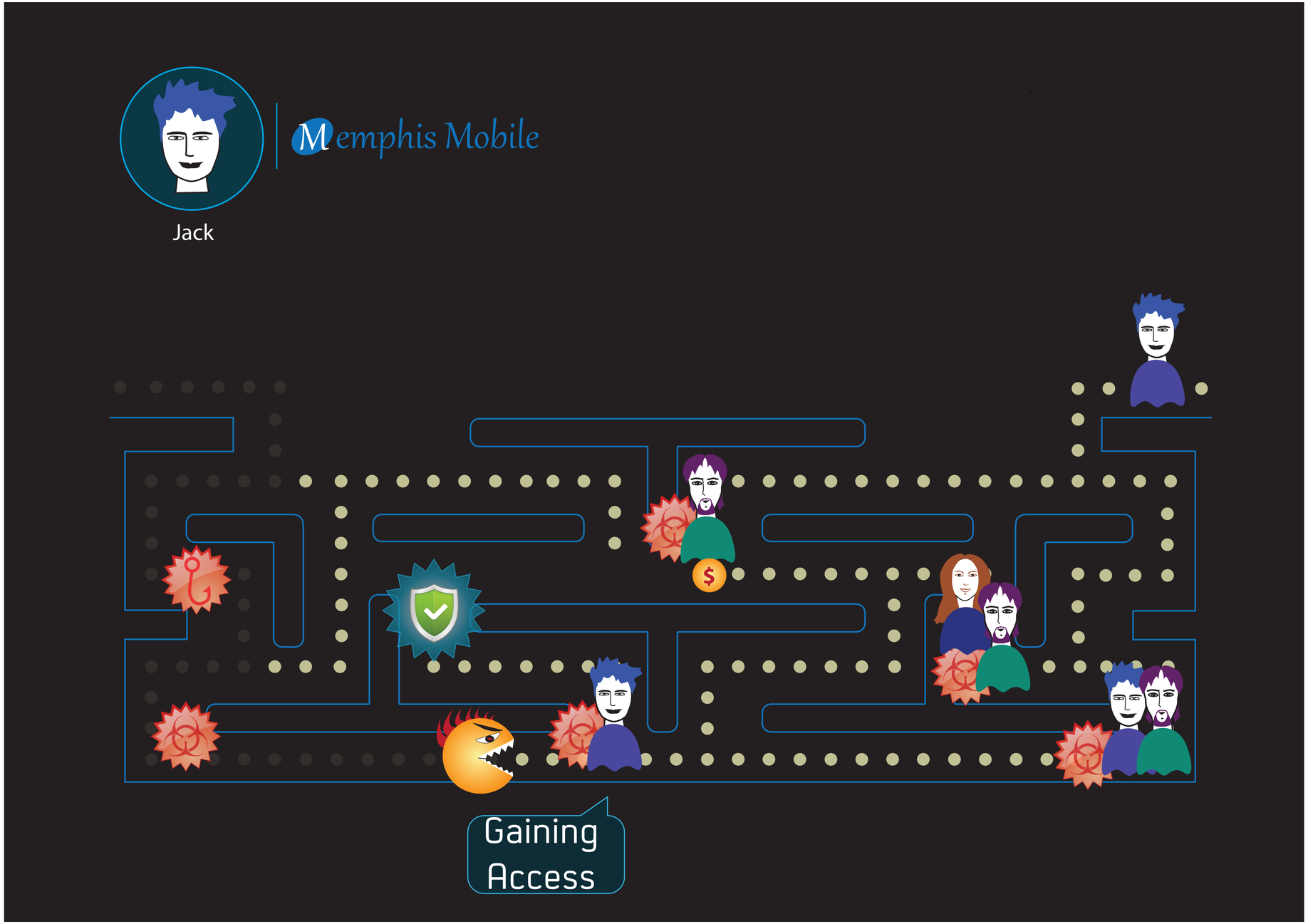
- The age of catchy names (*celebrity* bugs):

  - Heartbleed - allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software.

  - Shell-shock - remote code execution (bash) bug.

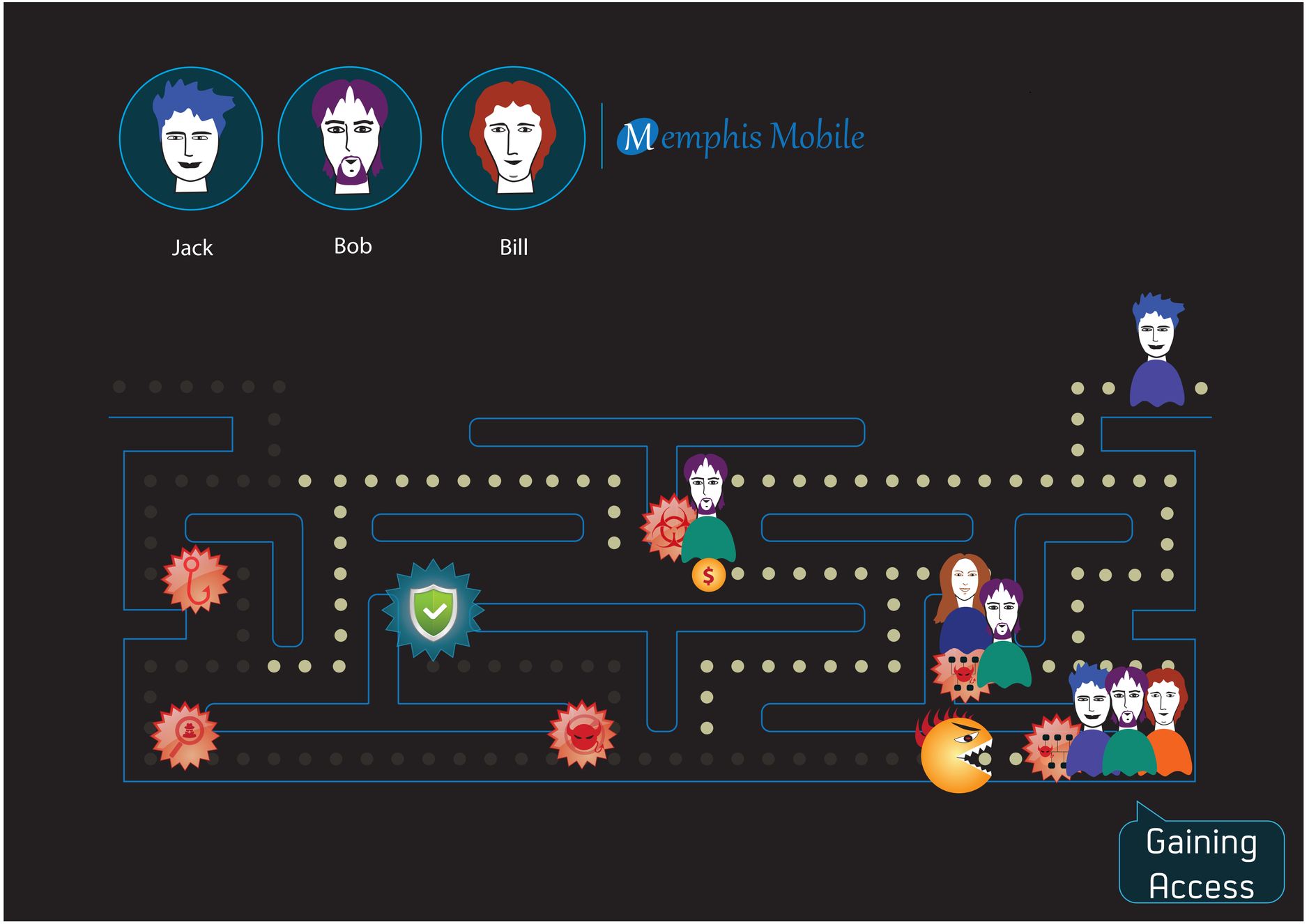
  - Poodle - a downgrade to SSL 3.0, an older protocol which the attacker can then exploit (cypher suite rollback attack).

  - Bar Mitzvah attack - (13 years old obviously) exploits the weak keys used by RC4.



Gaining access

- We are now in the servers network. Let’s look around.
- Look Ma - here is an ERP server (at least it is called so).
- Let’s try to log into it.
- Send a request to `http://erp.memphis-mobile.local`
- Got a "`401 Unauthorized`" response. Good thing it responds.
- Let’s capture Kenny's credentials (using the built in keylogger) and try to use them to login.
- That worked.
- But, it seems Kenny has low privileges. Bummers. (Note that we can see the browser using the VNC like tool from Kenny's machine).



Gaining access, one more try

- We need to find more users. Let’s look for a directory server.
- Using network capturing we can see the machine we're on, communicates with the domain controller. It is called "`elvis`".
- Let’s try sending LDAP queries to it.
- Wow. That was easy. We now have the directory structure of Memphis-Mobile. And we have everyone's phone numbers. This may become handy.
- And look, it says Bob is a DBA. Bob must have access to the ERP.
- We'll now try a brute force attack on the ERP server. We'll use a password cracking dictionary we can buy for $5. It has ~ 1,500,000,000 words.
- .... After 2 hours and 6,326,135 attempts Bob’s password was recovered. It was "`cass1dy`".
- Voila. We are in the ERP server.

Gaining access, what can we do

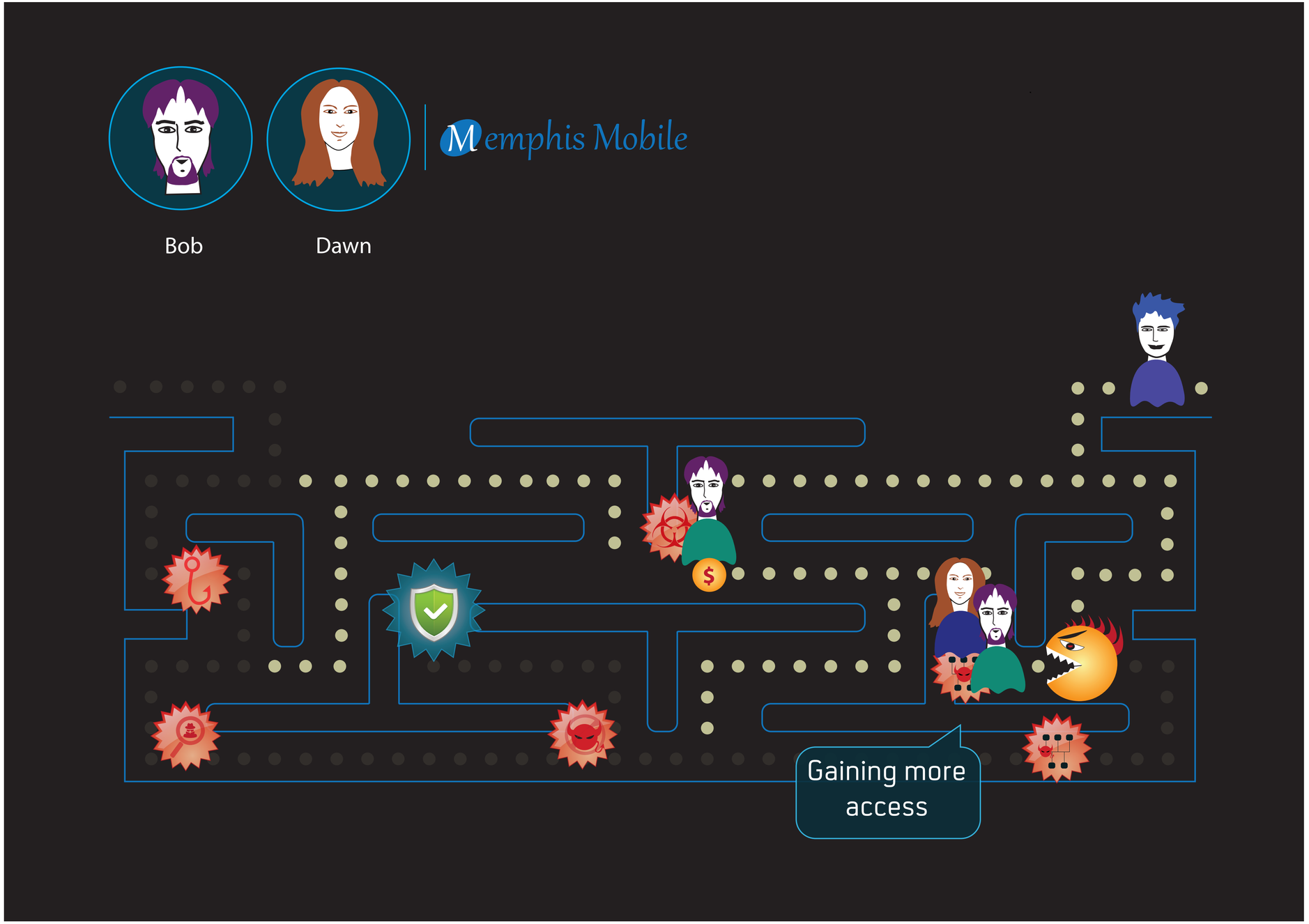
- Prevent traversal of directory structure - harden LDAP (active directory).
- Login throttling.
- Monitor logs - brute force attacks have high visibility.
- Passwords - prefer pass-phrases to passwords.
- Anomaly detection - did Bob (the DBA) ever logged in from Kenny's machine?

The convergence of Fraud and APTs

- Fraud is becoming more like APTs:
  - Higher profile victims.
  - The adversaries learn the behavior patiently.
  - Carbanak was dubbed “The greatest heist of the century”. $1B losses. Attacks took 2-4 months (!).

Underground shopping

- Spam lists for phishing (~50$ per 100k emails, depending on quality, country, etc..)
- Bulletproof hosting servers (~100-1000$ per month/two weeks rental of VPS)
- Anonymous mailing servers (~2000$ rent/month per 1 dedicated server, for use of heavy spam campaigns)
- Credit cards (1-4$ for one USA stolen credit card, 5-15$ for a european card)
- Trojan Logs (~10$ per 100mb of raw unparsed text logs)
- Bank Accounts (price is determined according to 5-10% of available balance on account)
- Mules for hire (~55-75% of transfer amount)
- Call "centers" for fraudsters (~10$ per call to bank/credit card issuer/online merchant/casino/wherever you want a call to be made)



Gaining more access

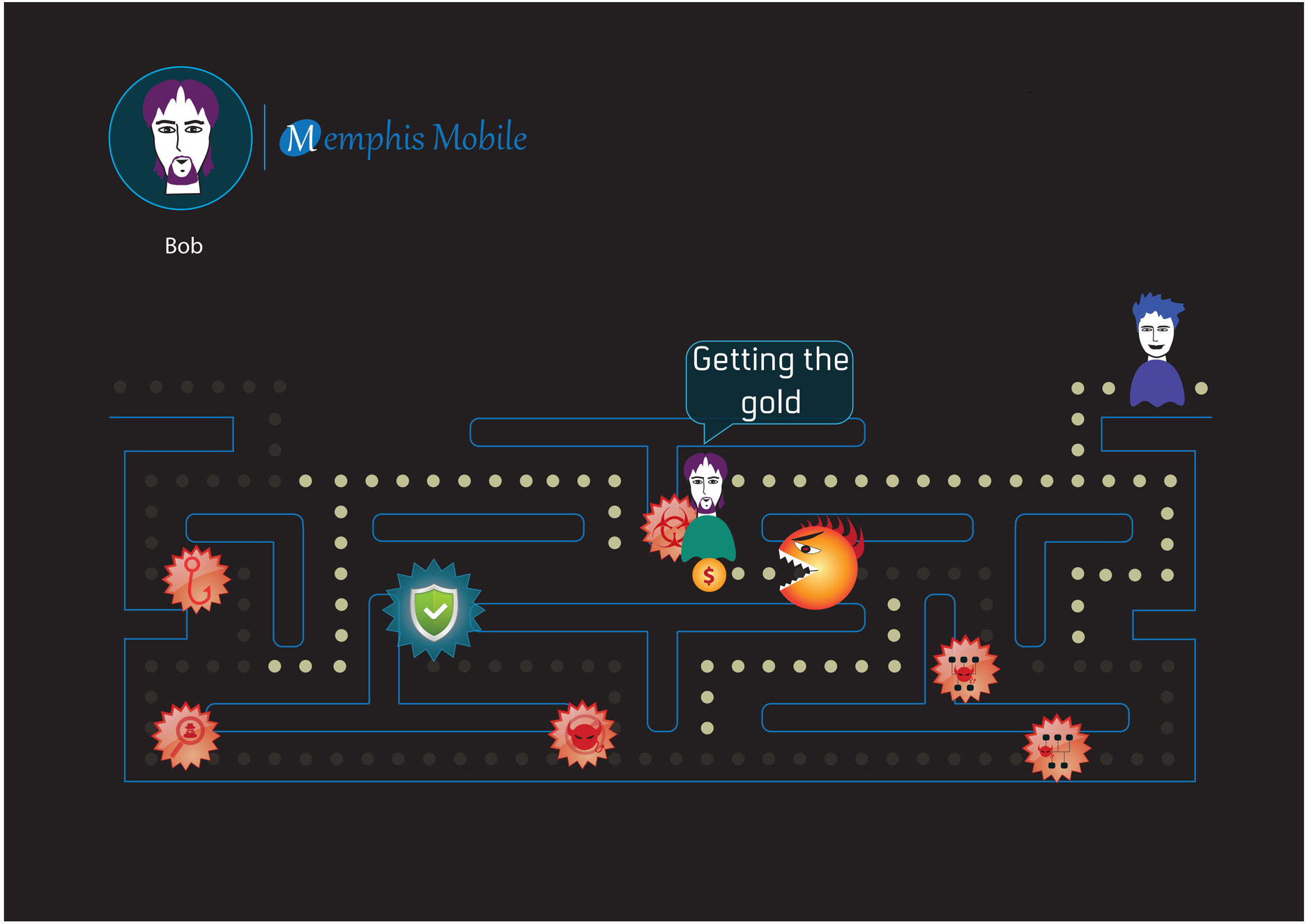
- The ERP is nice, but we really want the Billing server that holds the customer data, credit cards included (Memphis-Mobile is PCI certified...)
- Since Bob is an DBA, he has privileges to the admin part of the ERP. He can run all sorts of raw queries (Dawn wrote it for him so it will be easier for him to manage the system).
- Lets try some good-old SQL injection using "`EXEC xp_cmdshell`". We'll submit

```
 SELECT * FROM userinfo WHERE id =1; EXEC
master.dbo.xp_cmdshell 'dir c:\inetpub > c:\inetpub\wwwroot
\test.txt'--
```

- And voila, we have shell access on the ERP server!

Gaining more access, what can we do

- Protect yourself from SQL injections by properly verifying input, escaping input and/or parameterized statements.
- In fact, follow all of OWASP's top ten list.
- Disable functionality of services (here the DB) that you don't need.
- Use a server's protection application with application lock-down capabilities.



Getting the gold (1)

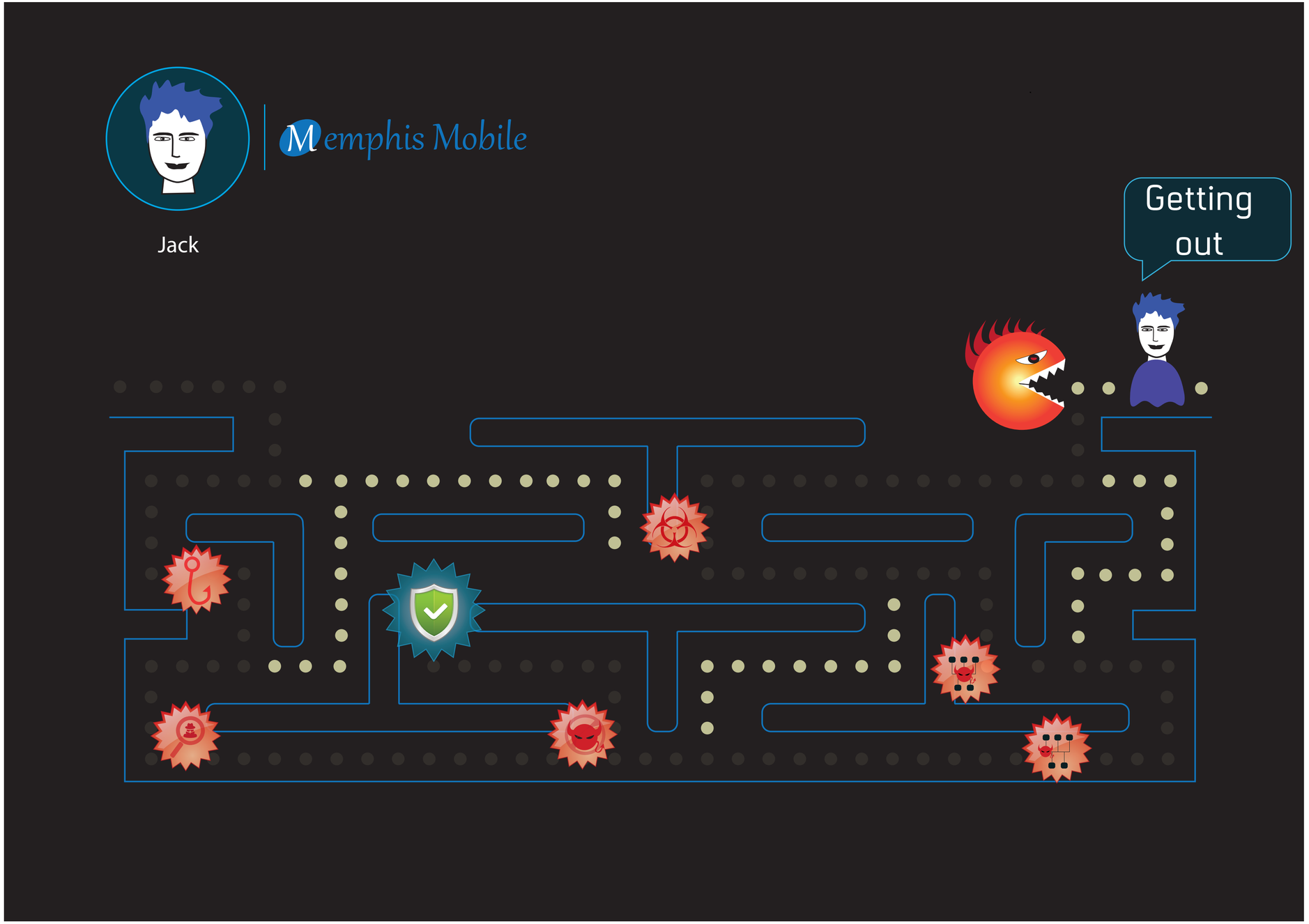
- Now that we have shell access on a privileged machine, (the ERP machine), everything is doable.
- Looking around we discover the Billing DB. It runs on a different server, but in the same servers' domain.
- Since Bob's password is used across all services (SSO is great) it can be used to get to this machine also and dump the data from the DB.
- Alas, it has two factor authentication built in (since this is such a sensitive DB).

Getting the gold (2)

- We'll send Bob an SMS with a malicious file URL (remember we have Bob's phone from the LDAP dump?).
- Boom. He clicked the link and his mobile phone (he had it rooted previously, good thing he is a power user) is now infected (a mobile exploit took care of that). We can divert messages and forward it to us.
- We're trying to login to the DB again. An SMS with a token is sent to Bob's phone. We hijack it and we're in the Billing DB.
- Now dump the file into a temp directory and we have the gold.

Getting the gold, what can be done

- Be very suspicious with links in SMS messages.
- Run a protection module on the phone.
- Disallow usage of rooted devices by employees for work related activities.



Getting out, under the radar

- We have the data in a file, but access to the Internet from the machine (the shell runs on the ERP machine) is blocked.
- We'll move it to the Procurement directory and try to get it out without being noticed.
- Recall that Jack posts to an online forum? We will wrap it in an image attachment to the mailing list, and it is out there. All we have to do is get it from download it from the forum.

Juicy trends - Cyber Gangs Fights

- Hellsing vs. Naikon - fights between cyber crime groups (http://securityaffairs.co/wordpress/36002/cyber-crime/hellsing-apt-on-apt-attack.html)

- What do you think they used? Spear phishing to get in. A backdoor with modular design was installed. The rest of the story? You can now imagine it.