Changing Battleground

Security Against Targeted Low Profile Attacks

By Abhilash V. Sonwane
Cyberoam

Presentation Sketch

Changing Battleground

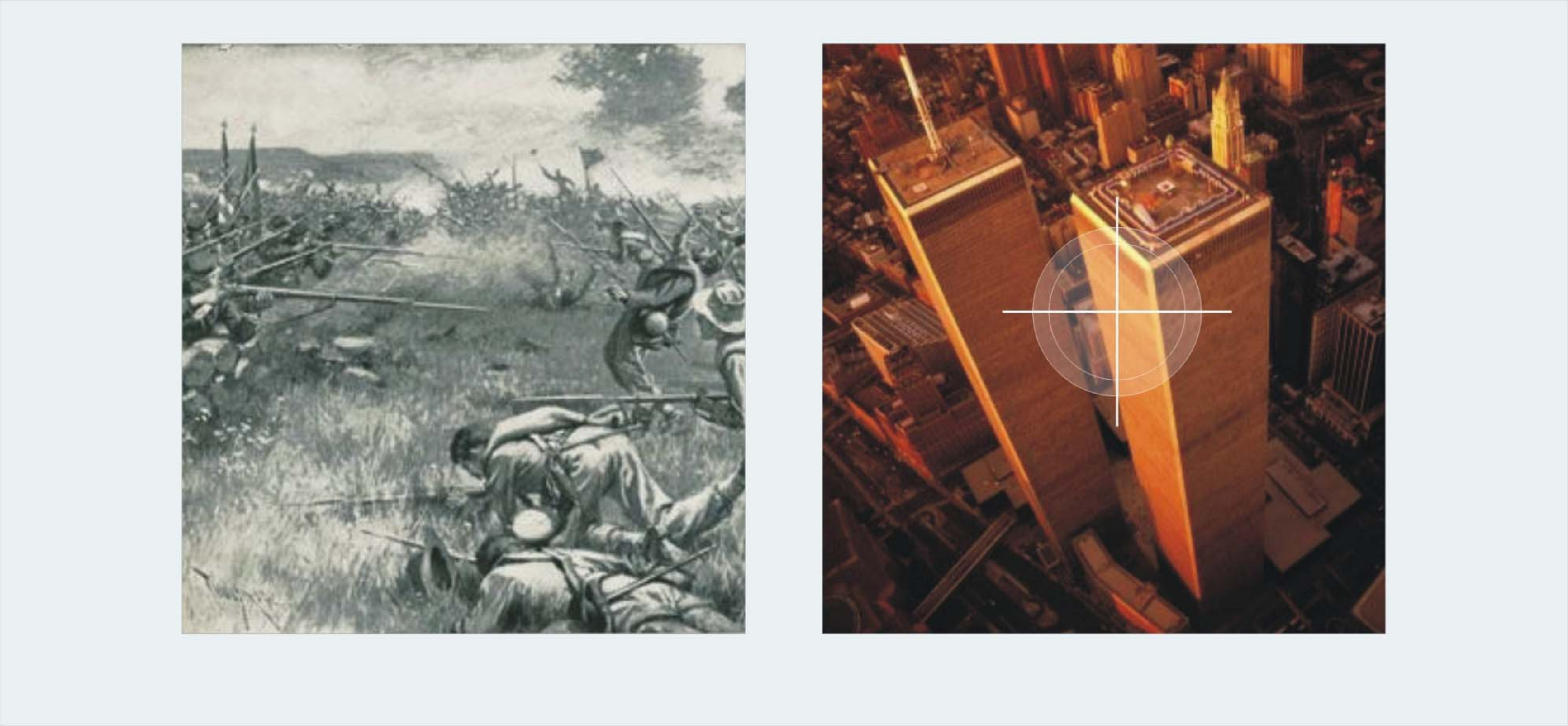
Shift Towards Targeted Attacks

Identity-based Heuristics – The Suggested Solution

Conclusion

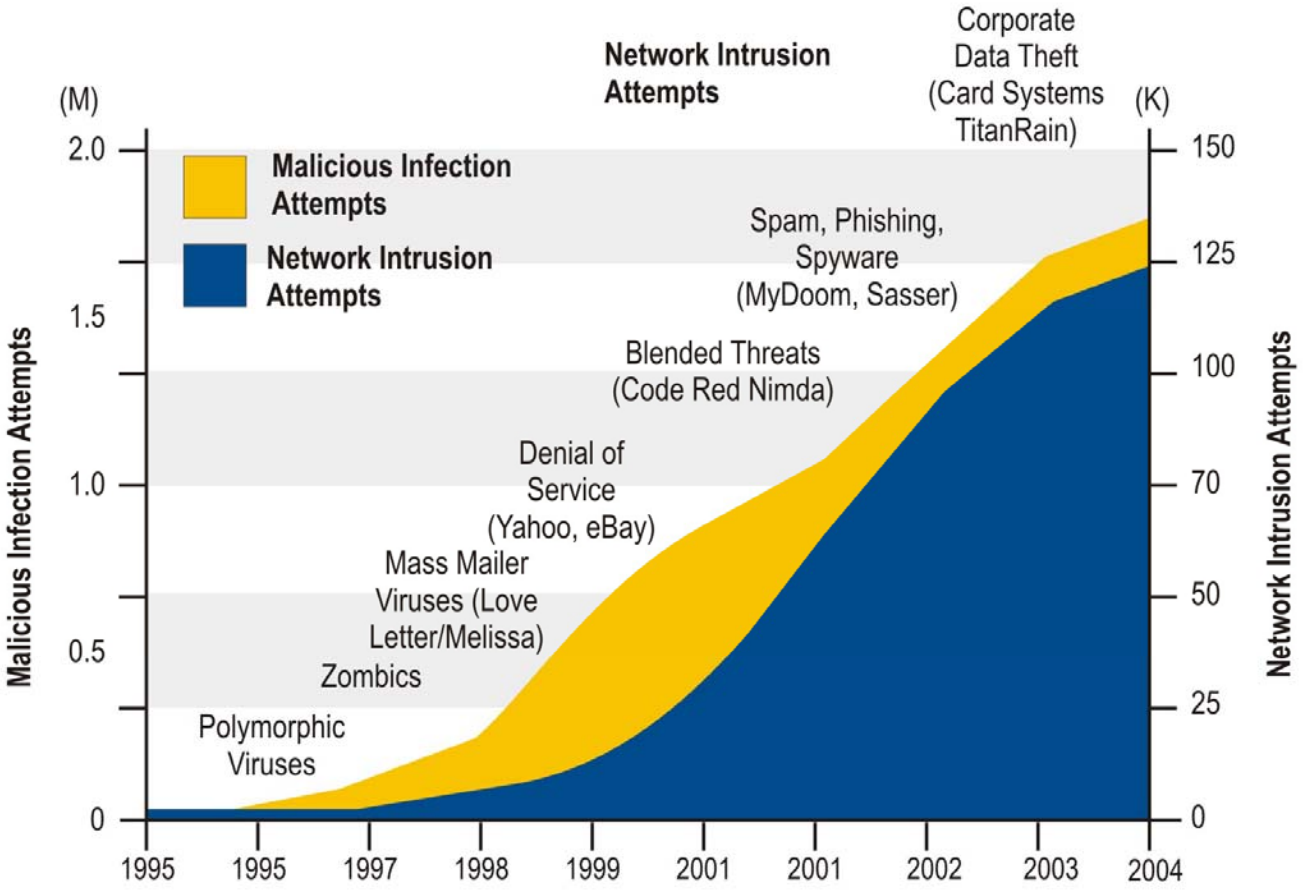
Changing Battleground

Evolution of the Real Battleground



- Evolving Trends in war and the evolution to today’s tactical battle
- A shift from Mass Attacks to Targeted Attacks

Evolution of the Virtual Battleground



Source: IDC, ICSA, CERT, CSVFBI, McAfee

Targeting the Masses – Everything and Everyone

When? 1980s

Attacker Profile

- Written by young programmers
- Kids who just had learned to program – script kiddies
- Young people – usually the students

Motive of the attack

- Out of Curiosity to test their skills

Targeting the Masses – Everything and Everyone

What was the target?

- Operating Systems

Who were the victims?

- Every user of the OS

What were the attack vectors?

- Simple programs with extremely primitive code

Example

- Brain

Targeting the Applications – The advent of macro viruses

When? Mid nineties

Attacker Profile

- Professional virus writers
- Exploited new infection vectors and used ever more complex technologies

Motive of the attack

- Publicity
- Showcasing their skills

What was the target?

- Applications like Microsoft Office
- MS Word and eventually in other MS Office applications

Targeting the Applications – The advent of macro viruses

Who were the victims?

- The Application users

What were the attack vectors?

- Payload was based on macros, mini-programs written in the Visual Basic programming language

Example

- Laroux – Excel Virus

Global Internet Attacks – The Blended ERA

When? Early 2000 (Year 2000-2003)

Attacker Profile

- Professional writers
- Virus Writer Groups

Motive of the attack

- Publicity
- Willful harm

What was the target?

- Still the masses
- Moving towards specific targets
  - Websites: SCO, Microsoft, Google
  - Network Applications: MS SQL

Global Internet Attacks – The Blended ERA

Who were the victims?

- Every Internet User
- Users who used mails
- Network applications

What were the attack vectors?

- Email and the Internet - primary sources of such new threats
- Virus writers and spammers united
- Milestone in Blended Attacks – Slammer –Jan 2003

Hitting the Financial Targets

When? 2003 - 2005

Attacker Profile

- Professional writers and crime rings who got down to business
- Designed attacks to commit financial fraud

Motive of the attack

- To hit large organizations – impacting their business and crippling their customers
- To Sniff out personal information, such as a SSN or bank account number
- To generate thousands of dollars from the harvested data

Hitting the Financial Targets

Who were the victims?

- Users, Employees of Large Organizations and Financial Institutions

What were the attack vectors?

- Blending of email and web threats
- Social engineering – Phishing emails
- Weak Web and email applications

Example

- Paypal, Ebay, Authorize.net

Narrowing the targets: Attackers Working Smart

When? 2005 onwards

Attacker Profile

- No longer mere individuals
- Attacks executed as joint ventures among professional programmers with access to greater pooled resources
- Consortiums dedicated to the creation and distribution of malicious software intended to steal money from individuals

Narrowing the targets: Attackers Working Smart

Motive of the attack

- To target Regional players and individuals – to escape attention
- Attacks driven by financial motives
- To steal confidential information from specific companies - Identity theft

Who are the victims?

- Small corporations, Key Individuals

What are the attack vectors?

- Spear phishing – exploiting individuals’ trust
- New hybrid combinations - spy phishing

Narrowing the targets: Attackers Working Smart

Examples

- Bank Of India
- ICICI Bank
- ABC, XYZ…

Do you know about them?

Have you heard about such small regional attacks?

- Such Attacks Fly under the radar
- Have a prolonged Lifespan
- Cause significantly high financial damage to Victims

Targeted Attacks Examples

Targeted Attacker Profile

- **Insiders**
- **External attackers**

Targeted Attacker Profile - Insiders

Insiders

Role

- Initiators
- Victims
- Conduits

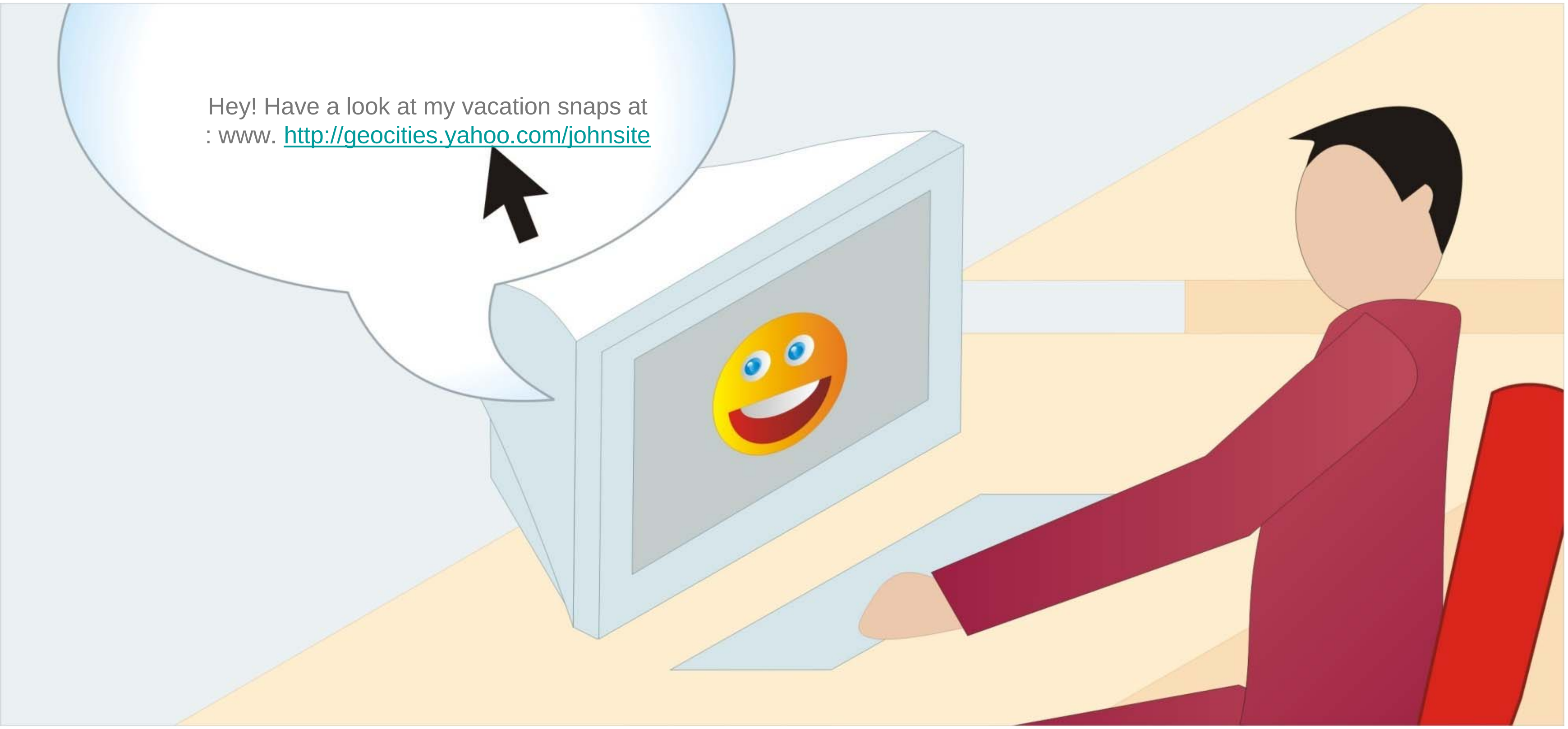
- Reasons
  - Malicious Intent - Greed
  - Disgruntled employees – Vengeance
  - User Ignorance

Targeted Attacker Profile – Insiders – An example

Hey! Have a look at my vacation snaps at : www. http://geocities.yahoo.com/johnsite

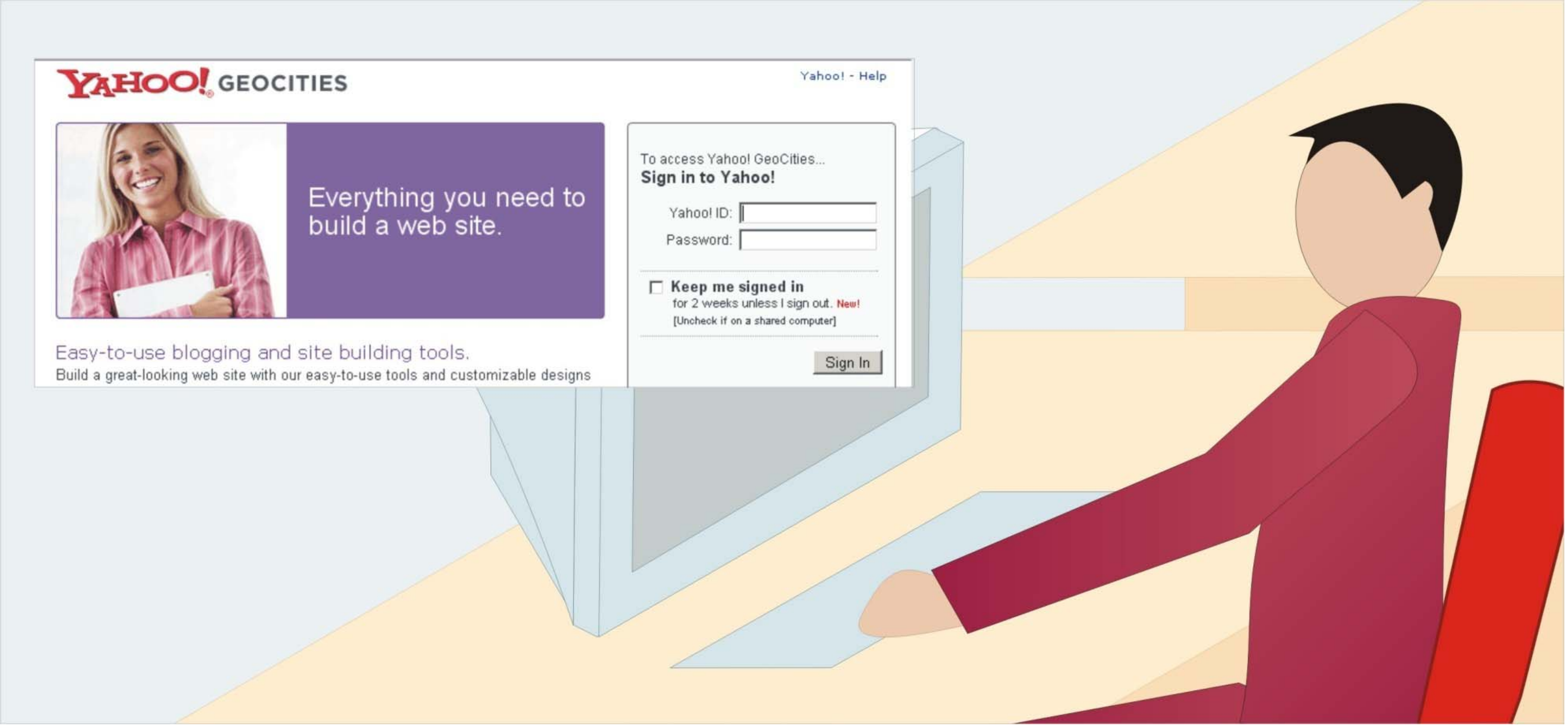
A former employee sends a chat message on Yahoo! casually asking his ex-colleague to look at his new photos on his Geocities Website

Targeted Attacker Profile – Insiders – An example


Hey! Have a look at my vacation snaps at
: www. http://geocities.yahoo.com/johnsite

His ex-colleague clicks on the link to look at the photos on his Geocities Website

Targeted Attacker Profile – Insiders – An example



YAHOO! GEOCITIES

Yahoo! - Help

Everything you need to build a web site.

Easy-to-use blogging and site building tools.

Build a great-looking web site with our easy-to-use tools and customizable designs

To access Yahoo! GeoCities...

Sign in to Yahoo!

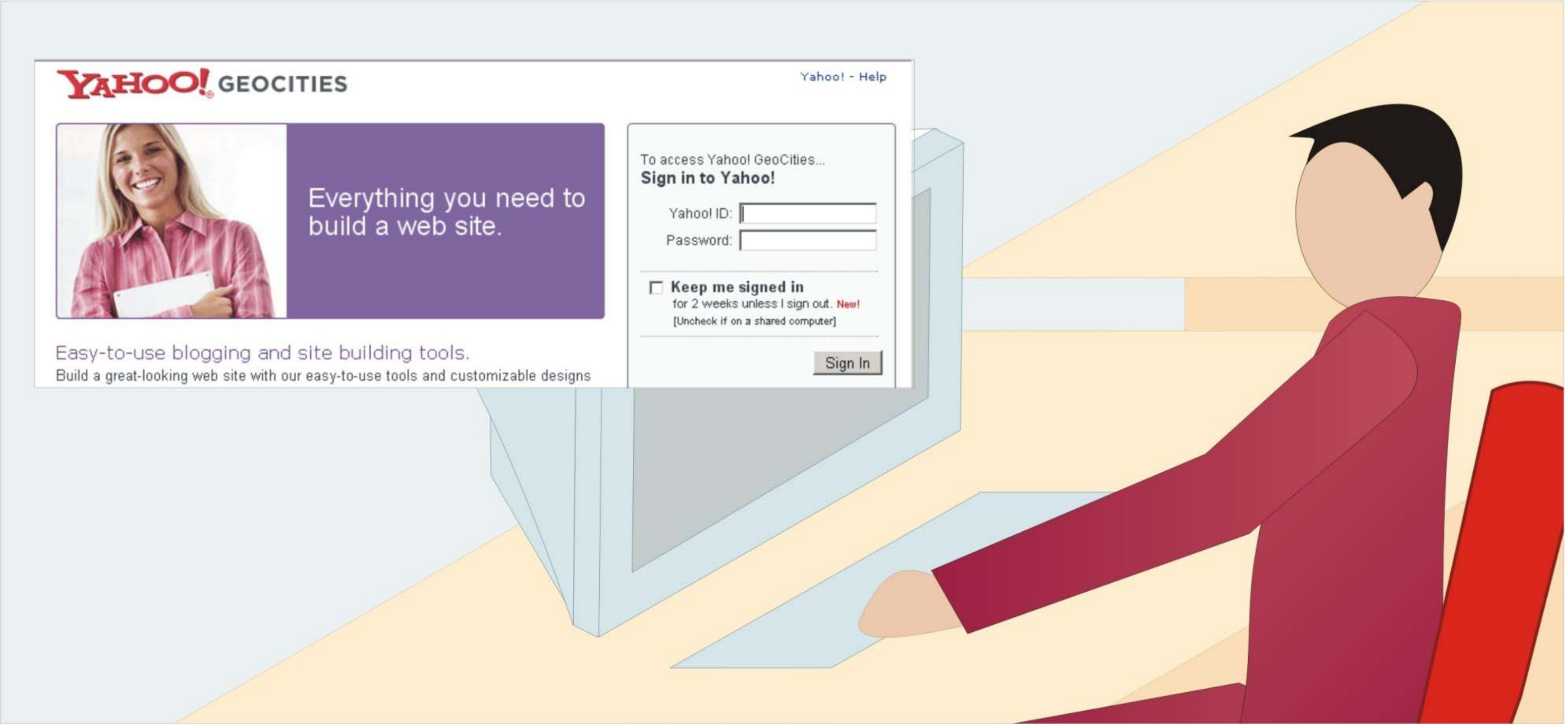
Yahoo! ID:

Password:

□ **Keep me signed in**
for 2 weeks unless I sign out. New!
[Uncheck if on a shared computer]

- The website asks for a Yahoo! Username and password
- The employee didn’t find anything suspicious and provided his information

Targeted Attacker Profile – Insiders – An example



YAHOO! GEOCITIES

Yahoo! - Help

Everything you need to build a web site.

Easy-to-use blogging and site building tools.

Build a great-looking web site with our easy-to-use tools and customizable designs

To access Yahoo! GeoCities...

Sign in to Yahoo!

Yahoo! ID:

Password:

□ **Keep me signed in**
for 2 weeks unless I sign out. New!
[Uncheck if on a shared computer]

Sign In

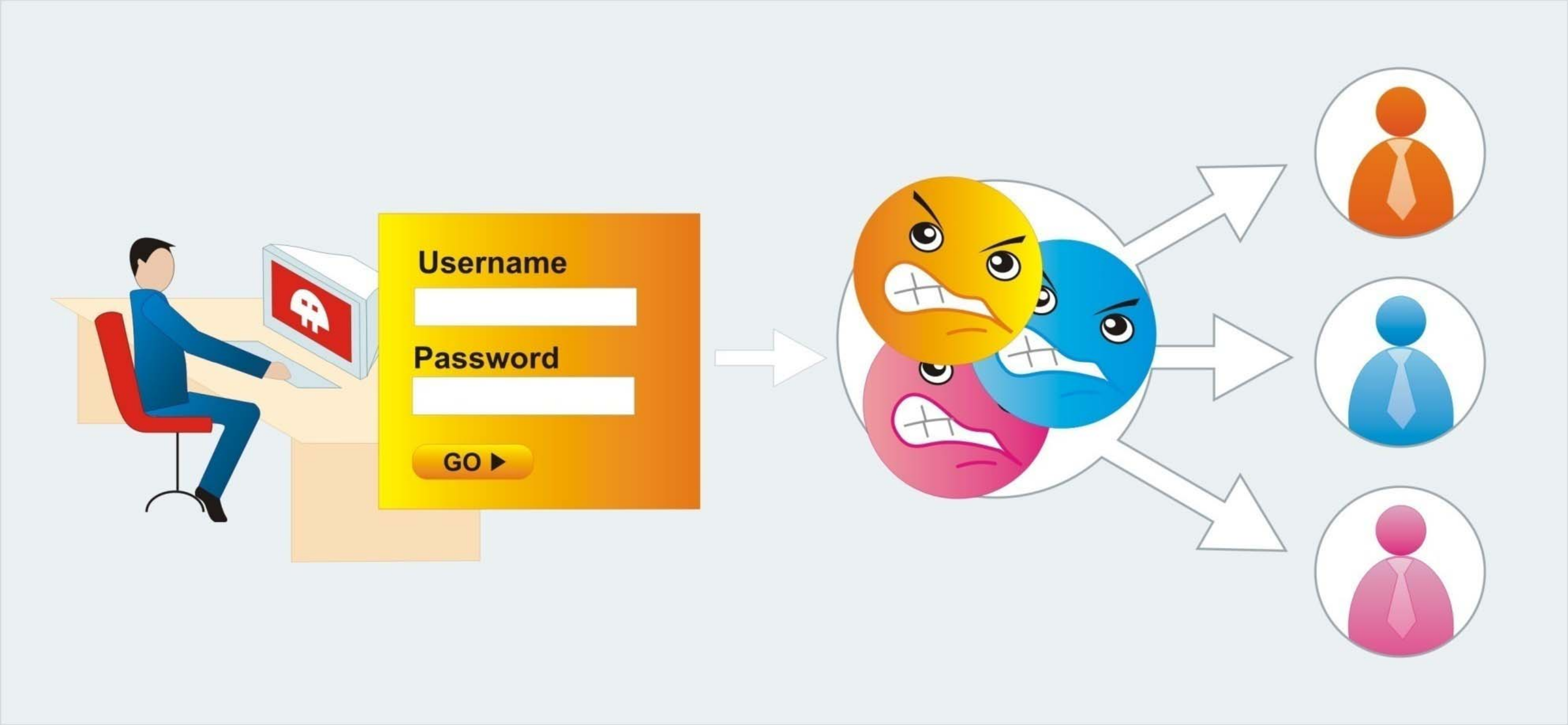
- What the ex-colleague didn't know was that the page was a fake
- His login information was now captured by his ex-colleague
- He was then redirected to the Geocities page with the photographs

Targeted Attacker Profile – Insiders – An example

YAHOO! GEOCITIES
To access Yahoo! GeoCities...
Sign in to Yahoo!
Yahoo! ID:
Password:

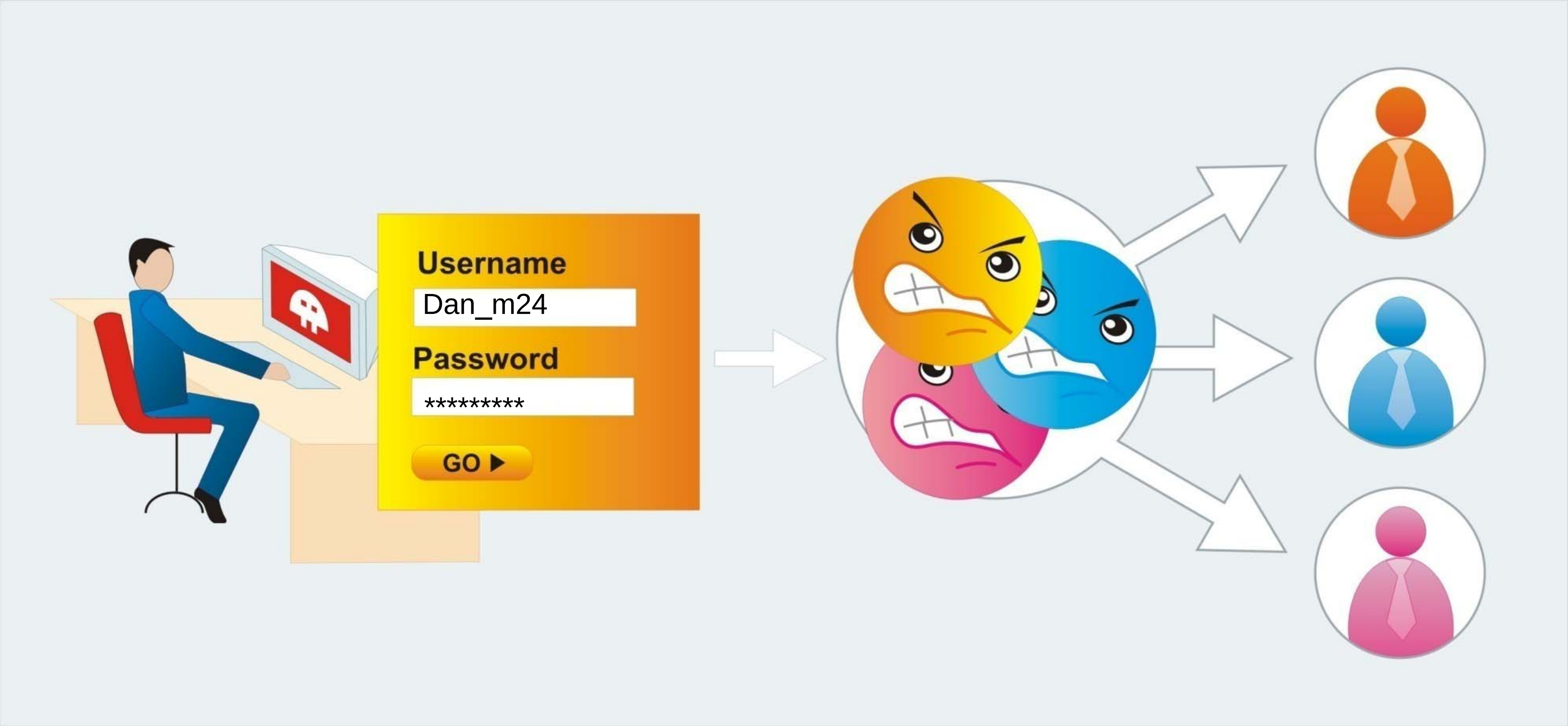
The same trick was applied to all former colleagues providing the disgruntled former employee with a good repository of username and passwords

Targeted Attacker Profile – Insiders – An example The Twist in the Tale



- Yahoo! Messenger is a standard mode of support communication for the corporation

Targeted Attacker Profile – Insiders – An example



- The attacker now had the ability to log on at will under the guise of his former colleagues
- Misguides customers and put the organization at risk

Targeted Attacks by External Attackers

- External Attackers getting insider information
- Targeting insider victims
- Targeting insiders as conduits

Targeted Attacks by External Attackers – A Recent Event

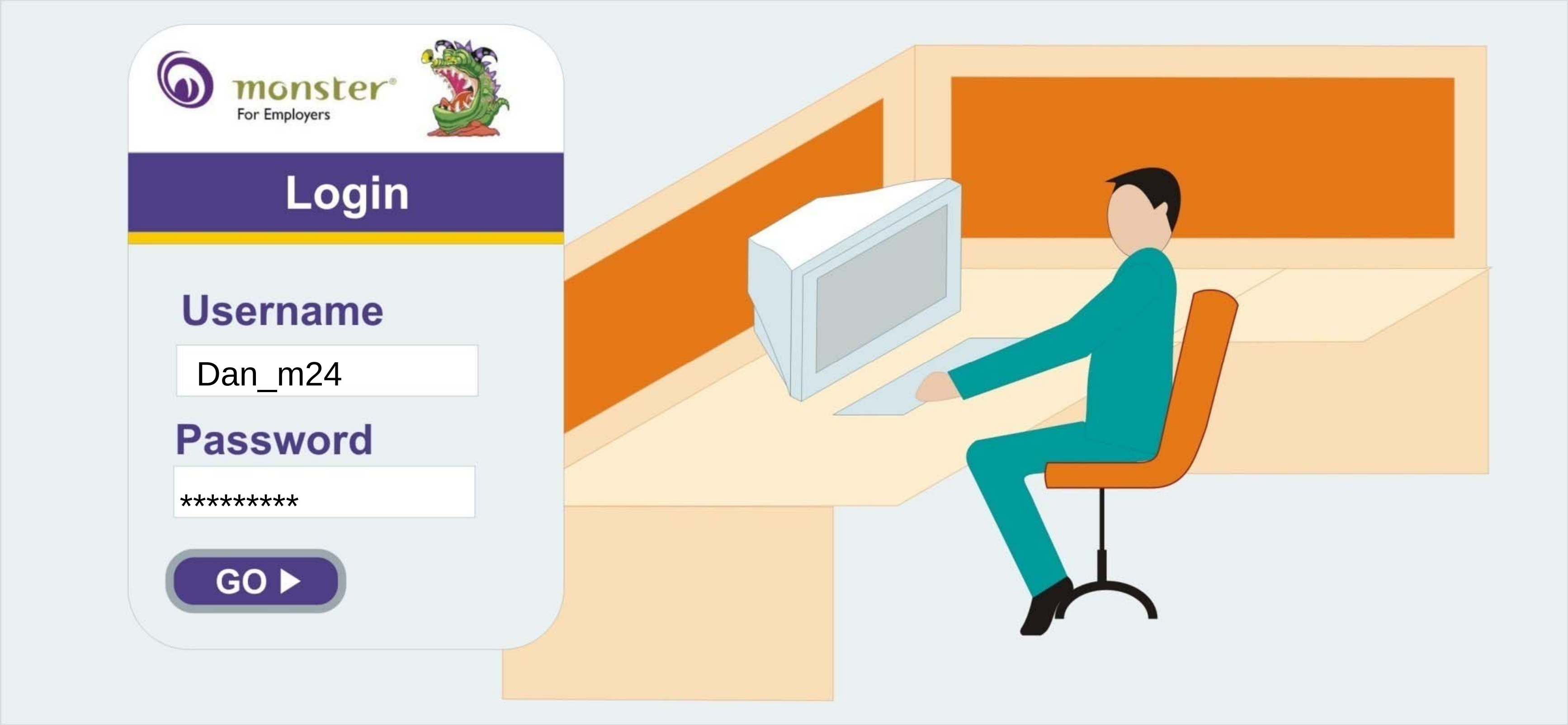
Employer/Recruiter

Monster.com

Hacker

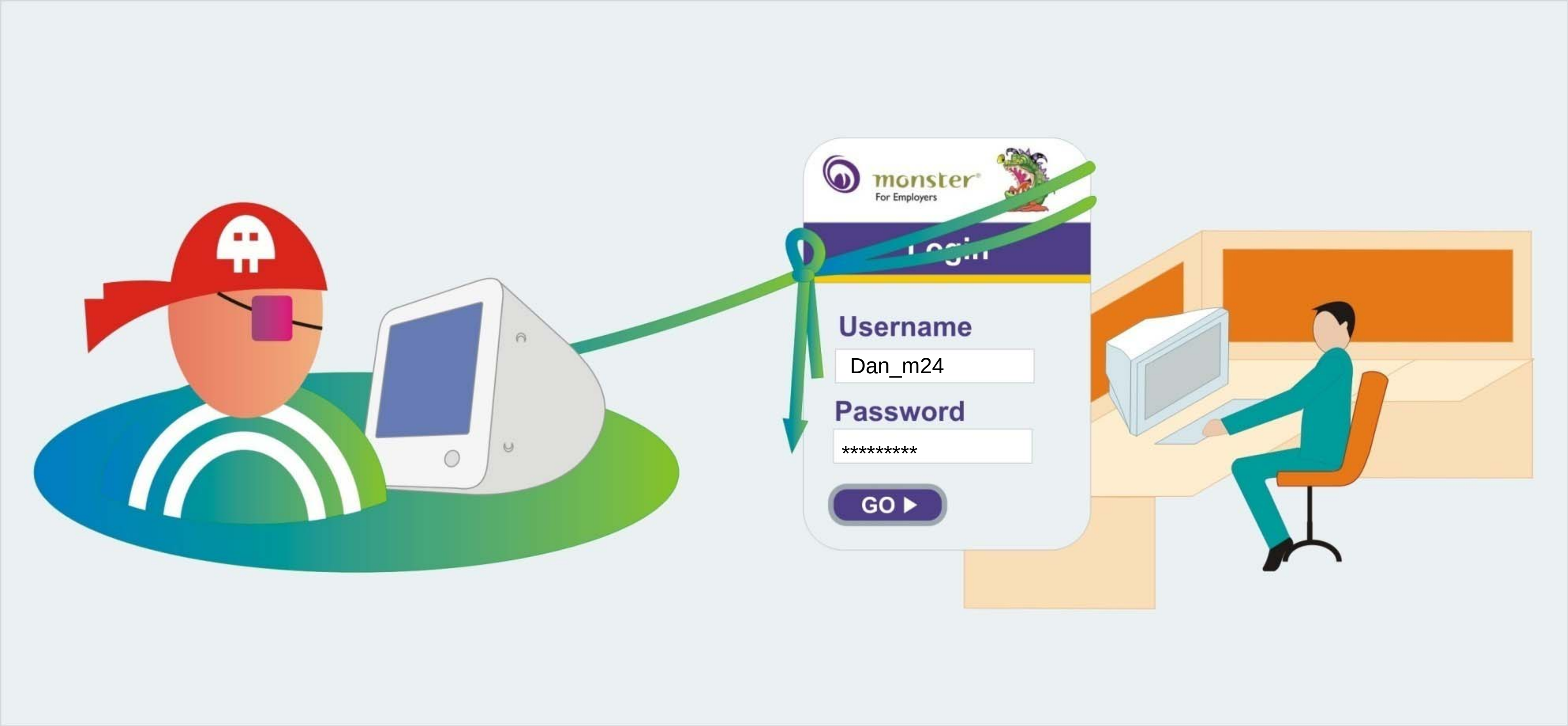
Monster.com - 1.6M records stolen from Monster.com

Targeted Attacks by External Attackers – A Recent Event



HR Personnel accessing monster’s online recruitment website hiring.monster.com and recruiter.monster.com

Targeted Attacks by External Attackers – A Recent Event



Trojan – Infostealer.Monstres stealing credentials of a number of recruiters

Targeted Attacks by External Attackers – A Recent Event

Username

Dan_m24

Password

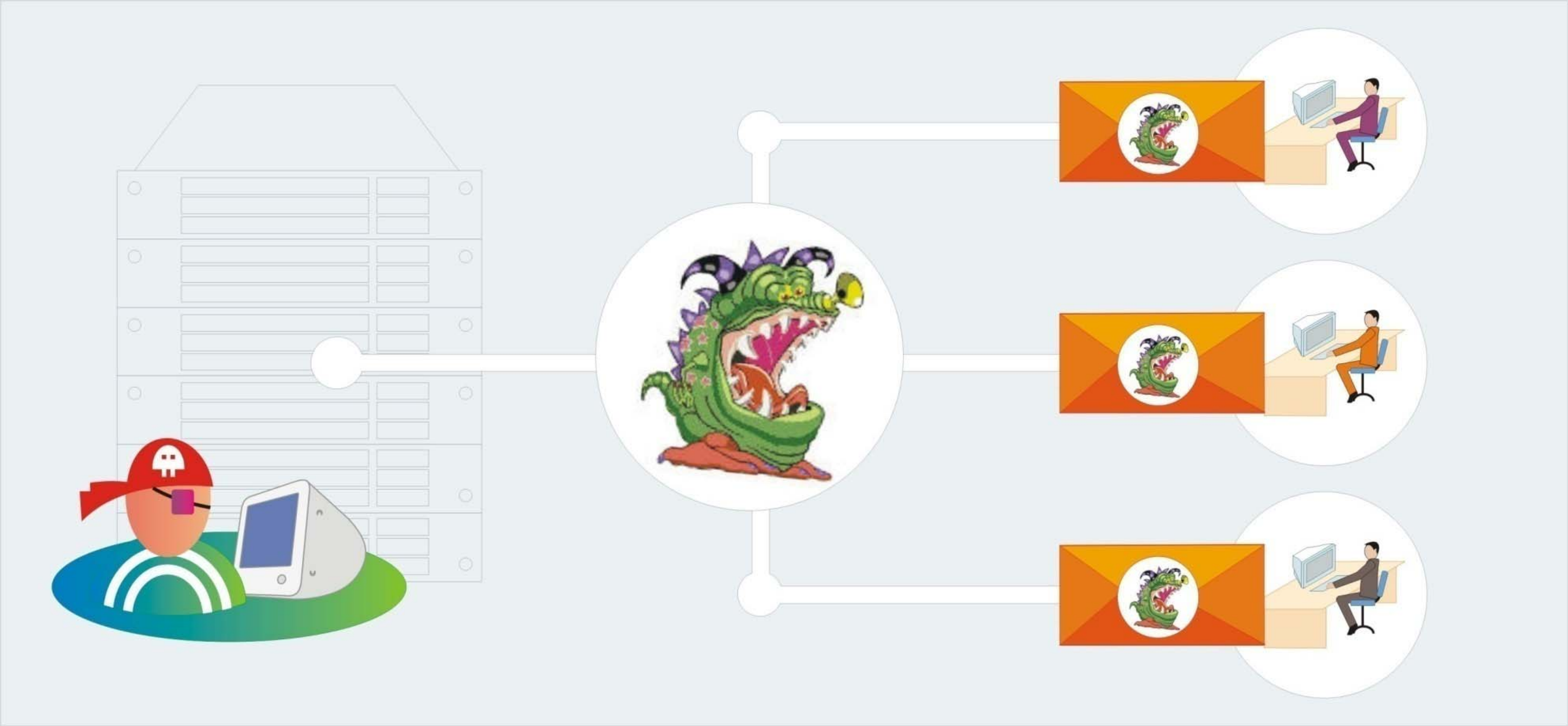
****

Trojan using stolen credentials of a number of recruiters to login to the Web site and perform searches for resumes of candidates located in certain countries or working in certain fields

Targeted Attacks by External Attackers – A Recent Event

The personal details of 1.6 million candidates, mainly based in the US, are then uploaded to a remote server under the control of the attackers

Targeted Attacks by External Attackers – A Recent Event

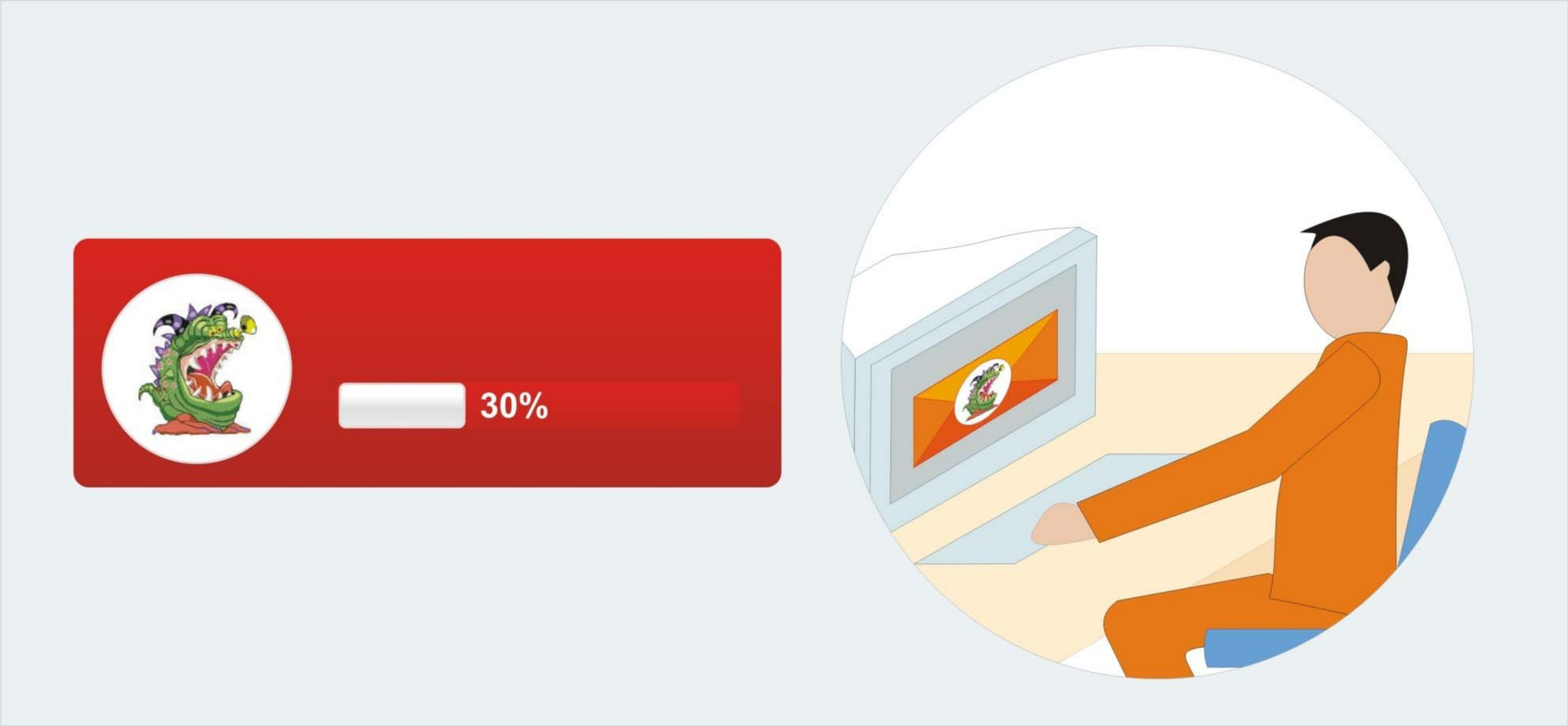


Targeted Monster.com Phishing emails which appeared very realistic, containing personal information of the victims were spammed at the victims

Targeted Attacks by External Attackers – A Recent Event

Emails requested that the recipient download a Monster Job Seeker Tool, which in fact was a copy of Trojan.Gpcoder.E.

Targeted Attacks by External Attackers – A Recent Event



Trojan.Gpcoder.E getting downloaded to the victims’ PC

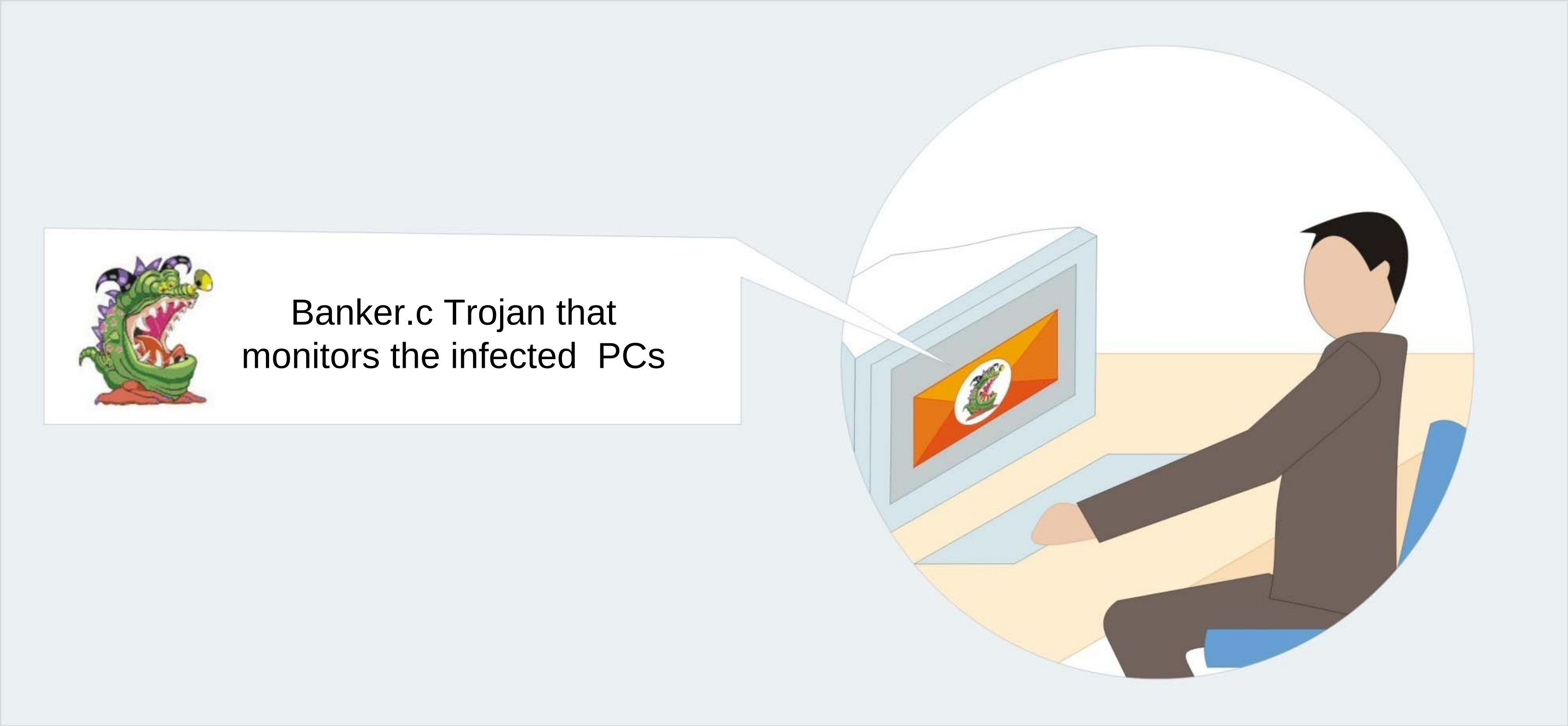
Targeted Attacks by External Attackers – A Recent Event

The Use of the Harvested Candidate data

Trojan encrypts files in the affected computer and leaves a text file requesting money to be paid to the attackers in order to decrypt the files

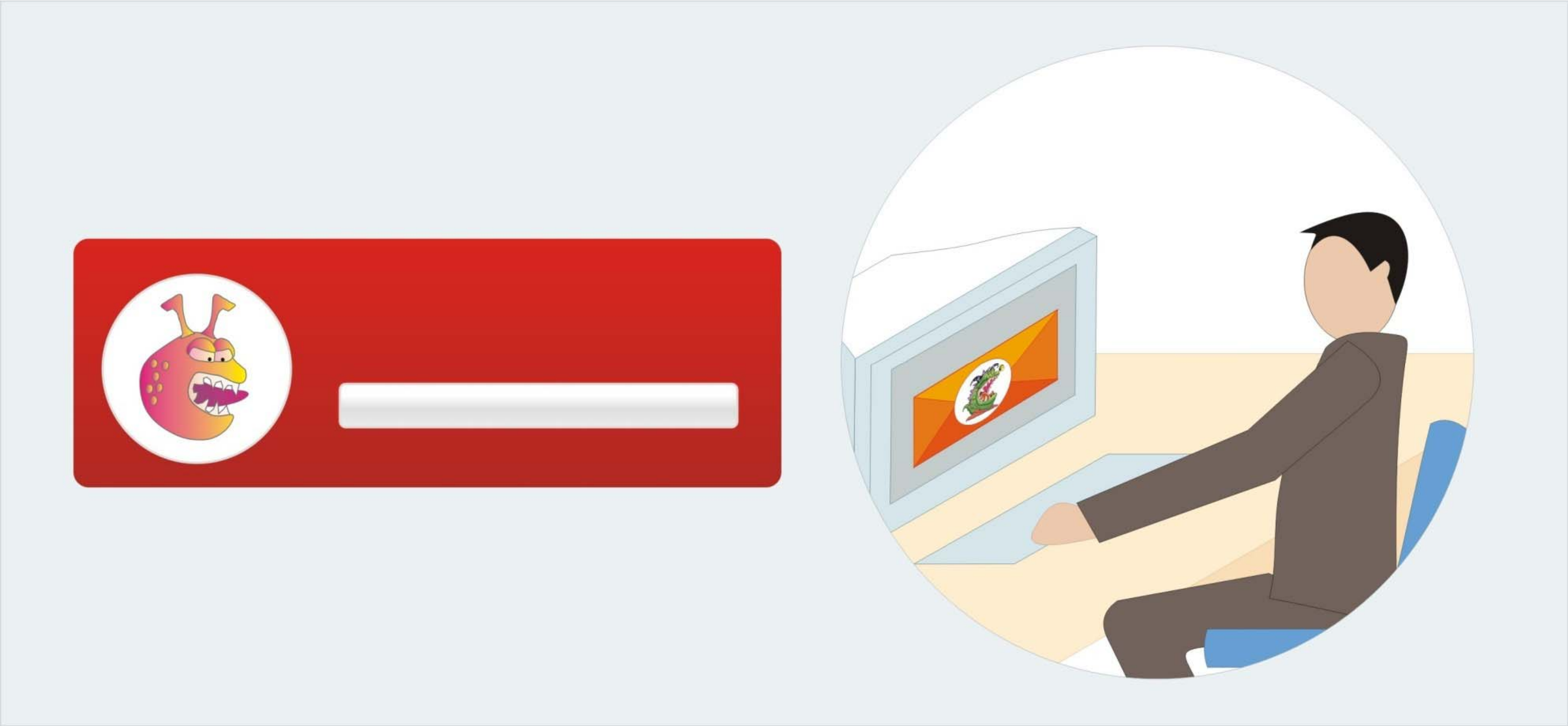
Targeted Attacks by External Attackers – A Recent Event

The Use of the Harvested Candidate data



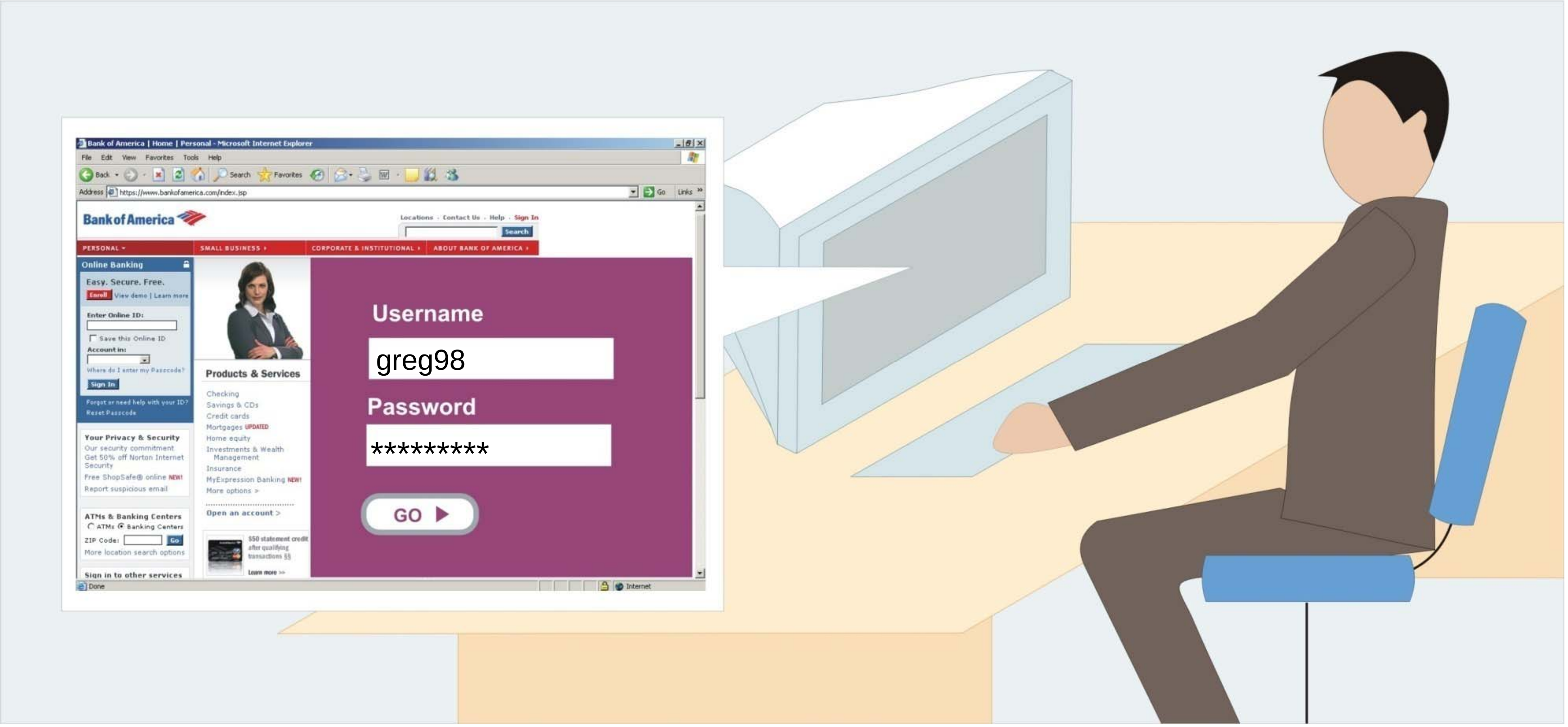
Targeted Monster.com Banking Fraud with Banker.c Trojan infecting the victim’s PC

Targeted Attacks by External Attackers – A Recent Event



Banker.c Trojan that monitors the infected PC for log-ons to online banking accounts. Records, the username and password, are then transmitted to hacker

Targeted Attacks by External Attackers – A Recent Event



Bank of America | Home | Personal - Microsoft Internet Explorer

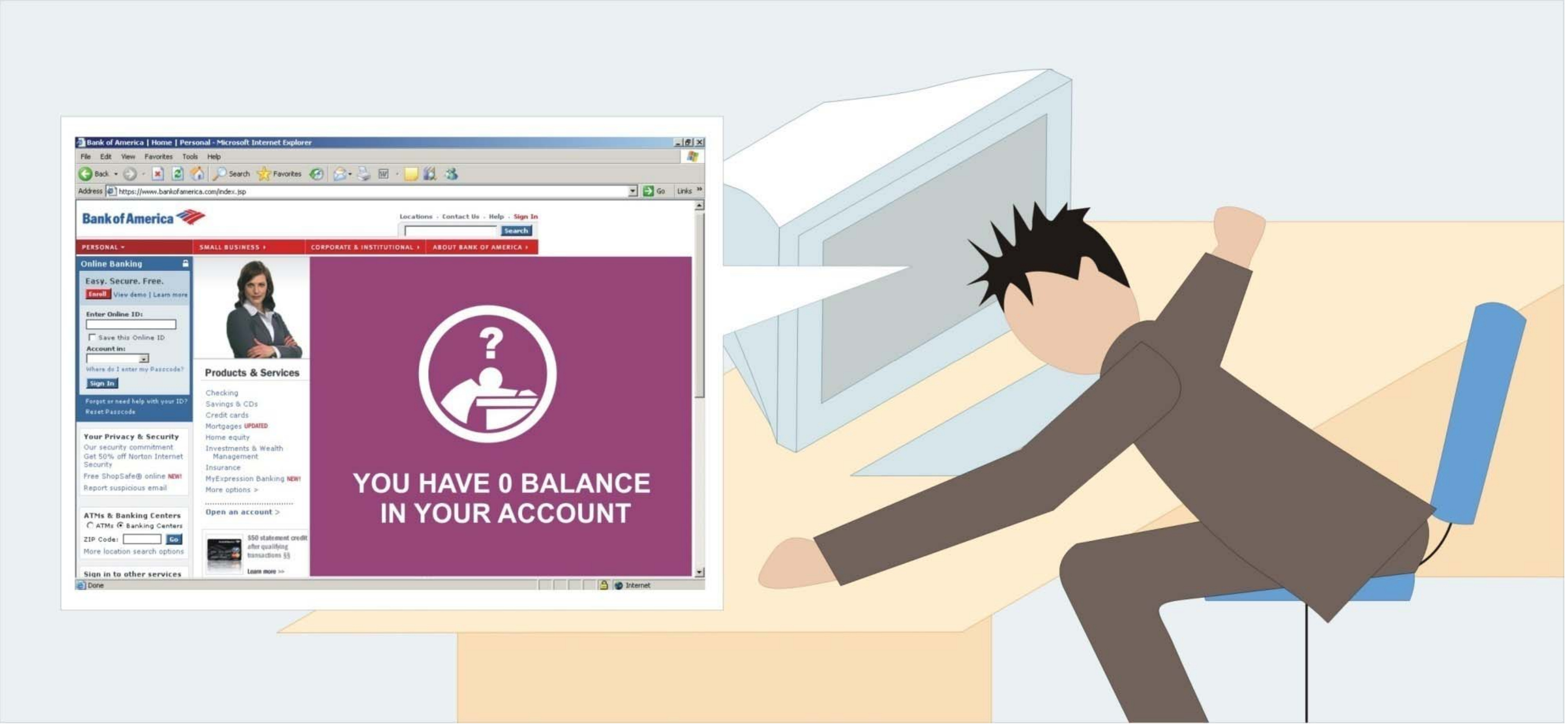
Address https://www.bankofamerica.com/index.jsp

Username greg98

Password *********

Hackers using banking account info for financial fraud

Targeted Attacks by External Attackers – A Recent Event



Bank of America | Home | Personal - Microsoft Internet Explorer

Address https://www.bankofamerica.com/index.jsp

YOU HAVE 0 BALANCE IN YOUR ACCOUNT

Victim suffers as a result of such financial fraud

Why are Targeted Attacks Succeeding?

Hackers on easy street

- Publicly available vulnerability information
- The Toolkit business
- Research – Easy access to information from public and internal resources

Today’s network scenario

- Fluidity of the network perimeter which opens it to partners, customers and more
- Employees have access to business critical information
- One cannot help not being (i)n the “Net”

Why are Targeted Attacks Succeeding?

Traditional products’ inability to detect the threat

- Detection of only massive or reported attacks
- Small scale attacks can’t grab media attention, go unnoticed, thus expanding attack life span
- Signature-based solutions
- Well-planned, pre-defined selected small target group – unlike the mass attacks

Why are Targeted Attacks Succeeding?

Unable to Identify the Human Role – User as a

- Victim – User Ignorance, Surfing Pattern, Loose Security Policy, Trust, Lack of Education

- Attacker – Malicious Intent, Vengeance, Greed

Stopping the attackers - Identity-Based Heuristics

First things first
A Multi Layered Security Approach:

- Security at the Desktop
  - Desktop Firewall
  - Host IPS
  - Anti Malware
  - Application Whitelisting
- Do not Forget the Network
  - Firewall
  - Network Anti Malware
  - Network IPS
  - Traffic Whitelisting

Evolving Towards Identity-Based Heuristics

User identity – An additional parameter to aid decision making

- Who is doing what?
- Who is the attacker?
- Who are the likely targets?
- Which applications are prone to attack – who accesses them?
- Who inside the organization is opening up the network? How?

Building patterns of activity profiles – User Threat Quotient

User Threat Quotient - UTQ

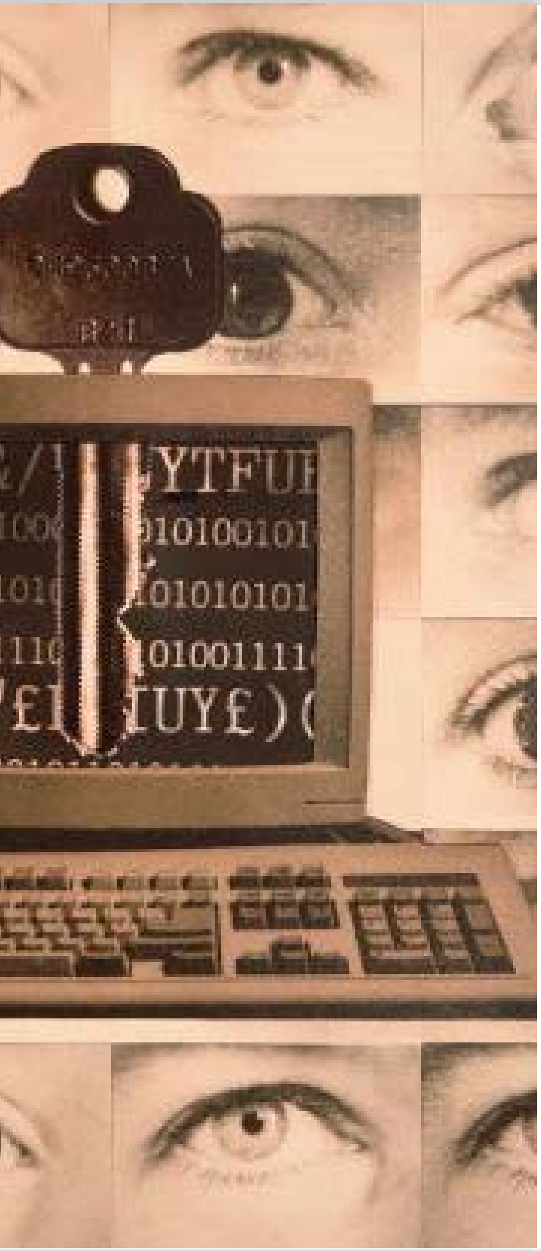
Calculating the UTQ

- Rating users on susceptibility to attack
- Nature of user activity
- History of activity – normal record access – number and type (customer data / research reports/..)
- Current status – new employee, terminated , etc.
- Analyze Who is doing What and When
  - Use of anonymous proxy
  - Downloading Hacker Tools
  - Accessing data off-hours
  - Amount of data accessed

Technical Preventive Measures

Use Network Activity coupled with user identity information to:

- Identify deviations from the normal acceptable user behavior
- Red flag malicious activity based on UTQ
- Context of activity – repeated wrong password attempts by new vs. old employee
- Get Intrusion alerts with user identity information
- Correlate data, e.g. using Bayesian inference network
- Use Identity as a decision parameter in security rules and policies



Use UTQ information for Soft Measures

- Individualized education based on UTQ information
- Educating to Key persons – having access to business critical information
- Educating the employees as their role evolves – joiner, moving up, quitter

Conclusion

- Threat landscape is shifting
- Current solutions need to change
- Need to leverage user Identity information for proactive control

Thank You

To Know more about Cyberoam : Visit www.cyberoam.com