Scientific Research Publishing

Journal of Information Security, 2021, 12, 224-231
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Hacked by Bits and Pieces: What Can We Learn from an Example of Corporate Espionage?

Jack Schafer[1], Marvin Karlins[2]

[1]Western Illinois University, Macomb, USA
[2]MUMA School of Busines, University of South Florida, Tampa, USA
Email: mkarlins@usf.edu

How to cite this paper: Schafer, J. and Karlins, M. (2021) Hacked by Bits and Pieces: What Can We Learn from an Example of Corporate Espionage? *Journal of Information Security*, **12**, 224-231.
https://doi.org/10.4236/jis.2021.123012

Received: April 19, 2021
Accepted: July 6, 2021
Published: July 9, 2021

Abstract

Information security often involves the development and application of sophisticated software to protect sensitive information stored in corporate computers. Yet, in this example of corporate espionage, a clever person, a cellphone and some readily available software were all it took to crack through one company's advanced security barriers. By reading this article it is hoped that employees at all levels of an organization's hierarchy will become more aware of—and recognize—how: 1) bits and pieces of seemingly harmless and easy-to-acquire information can be used for sinister purposes; 2) building rapport and trust with a person can make them more likely to become unknowing co-conspirators in a devious undertaking; and 3) how one must be constantly alert not to give out information without carefully considering the authenticity and justification of the source requesting it.

Keywords

Cyber Security, Hacking, Social Engineering, Scams, Corporate Espionage

1. Introduction

As it becomes standard business practice to store proprietary and confidential information on company computers, the need for cyber security becomes increasingly important [1] [2]. This need has been highlighted due to numerous security breaches involving organizations well-known to the public, including Adobe, eBay, Equifax, LinkedIn and Yahoo [3] [4].

When well-publicized cases of corporate espionage at major American companies are reported to the public, most people conjure up Hollywood inspired images of darknet super-techno-geeks with banks of computers and James Bond type hacking devices who use their superior knowledge and cutting-edge inven-

tions to blast through firewalls and extract the data they want.

Although this highly sophisticated means of espionage does occur, as was the case with the recent ransomware attack on the Colonial Pipeline (the largest gasoline pipeline in the United States), oftentimes the same results can be achieved through far simpler means. In fact, all it takes is a person, a cellphone, some readily available software and an action plan to crack through the most advanced corporate security barriers and gain proprietary business information. The purpose of this paper is to emphasize, through an actual example, 1) how important it is to realize and recognize that each individual in an organization can be a portal for cyber intrusion; and 2) the need to properly train individuals how to be vigilant for cyber-scams and be wary *whenever* requests for computer access are made.

2. Procedure

To demonstrate how simple it is for a clever hacker to gain access to computer information—even when that data is protected by advanced cyber security measures—we have provided an example of just one such data breach. The authors thank Nathan House, a cybersecurity expert, for supplying us with this eye-opening example of corporate espionage. His challenge—as the would-be hacker—is to break into a secured computer network using only his wits and a cellphone.

3. Results

Nathan's goal is to access a specific Company's computer so he will be able to extract information otherwise unavailable to him. Below, he explains, step by step, what he does and why he does it (what information he is trying to gain).

Call #1: To the Company's Main Switchboard

NATHAN: Hi, I'm having a problem with my desk phone. Can you put me through to someone who may be able to sort this out for me?

RECEPTIONIST: Connecting you.

PHONE SERVICES: Hi.

NATHAN: Hi. I'm having a problem with my desk phone. Sorry, I'm new here. Is there any way I can find out who is calling me when they call my desk phone? Is there a caller ID?

PHONE SERVICES: Not really, because we use hot desks here. [A hot desk is a desk shared by more than one person, sometimes several people over three separate shifts]. Because people usually use their mobile phones, the caller ID isn't often related to a name. Is this a problem for you?

NATHAN: No, it's fine now. I understand. Thanks. Bye.

I now know that the company uses hot-desks and that phone caller ID is not always expected. Therefore, it is not an issue if I call from outside the company. If it was expected, then I could work around it anyway.

Call #2: To the Company's Main Switchboard

NATHAN: Hi, could you put me through to building security?

RECEPTIONIST: Okay.

BUILDING SECURITY: Hello, how can I help you?

NATHAN: Hi, I don't know if you will be interested, but I found an access card outside the building which I think someone must have dropped.

BUILDING SECURITY: Just return it to us. We are in Building 3.

NATHAN: Okay, no problem. May I ask who I'm speaking to?

BUILDING SECURITY: My name's Eric Wood. If I'm not here, give it to Neil.

NATHAN: Okay, that's great. I will do. Are you the head of building security?

BUILDING SECURITY: It's actually called Facilities Security, and the head is Peter Reed.

NATHAN: Okay, thanks a lot. Bye.

This exchange told me the names of a few people in Security, the correct name of the department and the head of security, and that they are the ones who deal with physical access cards.

Call #3: To the Company's Main Switchboard

NATHAN: Hi, I'm calling from Agency Group Associates and I wonder if you could help me. I had a meeting about a month ago with some of your HR people, but unfortunately my computer crashed and I have totally lost their names.

RECEPTIONIST: Sure, no problem. Let me look up that department. Have you any idea at all of their names?

NATHAN: I know that one of them was the head of HR. There were a number of people at the meeting, though.

RECEPTIONIST: [Pause.] Okay, here we are. Head of HR is Mary Killmister. XXX-XXXX.

NATHAN: Yes, that rings a bell. What are the other names in HR?"

RECEPTIONIST: In HR, Jane Ross, Emma Jones…

NATHAN: Yes, definitely Jane and Emma. Could I have their numbers, please."

RECEPTIONIST: Sure. Jane Ross is XXX-XXXX and Emma Jones is XXX-XXXX. Would you like me to put you through to any of them?

NATHAN: Yes. Could you put me through to Emma, please?

I now know the names of the three people in HR, including the department head.

Call #4: To the Company's Human Resources Department

HUMAN RESOURCES: Hello, Emma Jones.

NATHAN: Hi, Emma. This is Eric from Facilities Security in Building 3. I wonder if you can help me. We have had a problem here with the access card database computer. It crashed last night, and some of the data for the new employees got lost. Do you know who would be able to tell us who the new employees were over the last two weeks, as their access cards will have stopped

working? We need to contact them and let them know ASAP.

EMMA: I can help you with this. I'll look up the names and email them to you if that's okay. For the last two weeks, did you say?

NATHAN: For the last two weeks, yes. That's great, thanks, but would it be possible to fax it, as we share one computer for email and that was affected by the computer crash, too.

EMMA: Yes, okay. What is your fax number? Oh, and what's your name again?

NATHAN: Mark it to the attention of Eric. I'll have to find out the fax number for you and call you back.

EMMA: Okay.

NATHAN: Do you know how long it will take you to find out the information?

EMMA: It shouldn't take me more than thirty minutes.

NATHAN: Will you be able to start working on it straightaway? It's quite urgent.

EMMA: I have a few things to do this morning, but I should have the names by this afternoon.

NATHAN: That's great, Emma. Thanks. When you're done, would you be able to call me straightaway so I can start reactivating their cards?

EMMA: Yes, sure. What is your number?

NATHAN: I'll give you my mobile number. That way you'll be guaranteed to get me. XXX-XXX-XXXX.

EMMA: Okay, sure. I'll call you when I have the list.

NATHAN: Excellent. Thanks. I really appreciate this.

Call #5: To the Company's Main Switchboard

NATHAN: Hello. Could you put me through to IT Support?

RECEPTIONIST: Connecting you… [Long wait in the queue].

IT SUPPORT: Hello, can I have your I S number or your case reference?

NATHAN: I've just got a quick question. Is that okay?

IT SUPPORT: What is it?

NATHAN: A guy from Reuters is trying to send me a presentation and is asking me what the maximum size is for attachments.

IT SUPPORT: It's 5 megabytes, sir.

NATHAN: That's great, thanks. Oh, one more thing. He said it's an .exe file and sometimes those get blocked or something.

IT SUPPORT: He won't be able to send an executable file, as the virus scanners will stop it. Why does it need to be an .exe file?

NATHAN: I don't know. How can he send it to me, then? Could he zip it or something?

IT SUPPORT: Zip files are allowed, sir.

NATHAN: Okay. Oh, one more thing: I can't seem to see my Norton Antivirus icon in my system tray. The last place I worked, there was a little icon.

IT SUPPORT: We run McAfee here. It's just a different icon—the blue one.

NATHAN: That explains it, then. Thanks. Bye.

I now know that to send an executable via email, it will have to be zipped first and less than 5 *MB. I also know that they are using McAfee antivirus.*

Call #6: A Few Hours Later, a Call from Emma in Human Resources

EMMA: Hi, is this Eric?

NATHAN: Yes, hi.

EMMA: I have the new employees list for you. Do you want me to fax it?

NATHAN: Yes, please. That would be great. How many are there?

EMMA: About ten people.

NATHAN: I'm not sure the fax is working properly here. Could you possibly read them out to me? I think it would be quicker.

EMMA: Okay. Do you have a pen?

NATHAN: Yes, go ahead.

EMMA: Sarah Jones, Sales. Manager is Roger Weaks… [Reads off the rest of the list].

NATHAN: Okay, thanks. You have been a real help. Bye.

I now have a list of the new employees over the last two weeks. I also have the departments they belong to and their managers' names. New employees are many times more susceptible to social engineering (*influence or control by an outside source*) *than long-term employees.*

Call #7: To the Company's Main Switchboard

NATHAN: Hi, I'm trying to email Sarah Jones but am not sure what the format of your email addresses are. Do you know?

RECEPTIONIST: Yes. It would be sarah.jones@targetcompany.com.

NATHAN: Thanks.

Social Engineering Email

Minutes later, a spoofed email [email message with a forged sender address] is sent.

From: itsecurity@targetcompany.com.

To: sar.jones@targetcompany.com.

Subject: IT Security.

Dear Sarah,

As a new employee with the company, you will need to be made aware of the company's IT security policies and procedures and, specifically, the employee's "Acceptable Use Policy".

The purpose of this policy is to outline the acceptable use of computer equipment at [target company]. These rules are in place to protect the employee and [target company]. Inappropriate use exposes risks, including virus attacks, compromise of network systems and services, and legal issues.

This policy applies to employees, contractors, consultants, temporaries, and other workers at [target company], including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by target company].

Someone will contact you shortly to discuss this with you.

Regards,

IT Security

Call #8: A Couple of Hours Later, a Call to the Company's Main Switchboard

NATHAN: Hi. Could you put me through to Sarah Jones, please?

RECEPTIONIST: Connecting you.

SARAH: Hello. Sales. How can I help you?

NATHAN: Hi, Sarah. I'm calling from IT Security to brief you on IT security best practices. You should have gotten an email about it.

SARAH: Yes, I got an email about it today.

NATHAN: Okay, excellent. It's just standard procedure for all new employees and only takes about five minutes. How are you finding things here? Everybody being helpful?

SARAH: Yes, thanks. It's been great. It's a bit daunting starting somewhere new, though.

NATHAN: Yes, and it's always difficult to remember everyone's name. Has Roger introduced you around? [The small talk is designed to build rapport interspersed with trust building.] Emma Jones is very nice in HR if you need any help with that side of things.

SARAH: Yes, Emma did my HR interview for the job.

NATHAN: Well, I better run through the security presentation with you. Do you have your email open? I'll send you the security presentation now and I can talk you through it.

SARAH: Okay, I see the email.

NATHAN: Okay, just double click on the Security Presentation.zip attachment.

SARAH: Okay….

The executable that she ran is, in fact, a cleverly packaged series of scripts and tools created by our wrapper program including within it the RAT (remote access Trojan malware program used to gain control of a computer), a rootkit (allows access to a computer while hiding its existence), a keylogger (keeps track of keystrokes on the computer keyboard), and anything else I may want to add.

When Sarah clicks on the file, the presentation immediately starts. This is just a series of PowerPoint slides telling her not to run executables that she is sent, etc., and other good security practices.

The presentation is branded with all the company logos that were conveniently copied from their public web server, just to add a little more trust. A few seconds later, as she is being taken through the presentation, scripts within the package start to try to disable McAfee and any other PC security that may be found that may help protect the user. Then the rootkit installs itself, hiding all future actions from the operating system or anybody doing a forensic investigation.

Next the RAT is hidden and installed. The RAT is made to start every time the

machine reboots, and these actions are all rootkitted and hidden.

The RAT then looks up any proxy settings and other useful information and tries to make its way out of the network and onto the Internet, ready to get its commands from its master. Obviously, all processes and TCP (Transmission Control Protocol) connections are hidden and even running things like netstar (network statistics) and task manager (procedures that can be bused to detect unsanctioned computer manipulation) will not reveal them.

The RAT connects to the master. I now own the PC and it's time to start looking around and really start hacking! Job is done.

4. Discussion

The authors hope that by reading the example just provided, describing the step-by-step calculated takeover of a target company's computer system, employees at all levels of an organization's hierarchy will become more aware (and recognize) how 1) bits and pieces of seemingly harmless and easy-to-acquire information can be used for sinister purposes; 2) building rapport and trust with a person can make them more likely to become unknowing co-conspirators in a devious undertaking; and 3) how one must be constantly alert not to give out information without carefully considering the authenticity and justification of the source requesting it.

When teaching our students—whether they be at the FBI Academy or the School of Business—we always present them with a quote that reminds them of the role they play in keeping national and/or corporate information safe: "Proprietary information can be protected in locked safes, behind a series of physical and electronic barriers. The weakest link in any security chain is humans. Once a lock is locked, it will not unlock itself ... but a tied tongue easily unties itself." That comment is followed by this observation: "Whenever someone involves you in a conversation—particularly when they are seeking information—don't go into 'automatic response' mode! Think about any possible hidden motive the person talking to you might have as the dialogue unfolds. Be cautious about giving up information, particularly the kinds of data that could be used in identify theft or corporate espionage, and remember that the one piece of information you give up might not seem significant, but, combined with other pieces, might just be the critical item that brings the entire jigsaw puzzle together" [5].

5. Conclusion

The information presented in this article illustrates how bits and pieces of information, carefully and cleverly collected, can lead to a major security breach in an organization's computer network. It is meant to give the reader an advance warning of just how such a process works so as to reduce the risk of it happening in the future.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Brooks, C.J., Grow, C., Craig, P. and Short, D.D. (2018) Cybersecurity Essentials. Sybex, Hoboken. https://doi.org/10.1002/9781119369141

[2] Sai, H. (2019) Next Level Cyber Security. Leader's Press, Santa Barbara.

[3] Swinhoe, D. (2021) The 15 Biggest Data Breaches of the 21st Century. https://www.csoonline.com/

[4] Daswani, N. and Elbayadi, M. (2021) Big Breaches: Cybersecurity Lessons for Everyone. Apress, New York, USA. https://doi.org/10.1007/978-1-4842-6655-7

[5] Schafer, J. and Karlins, M. (2020) The Truth Detector. Simon & Schuster, New York, USA.