2 CASE STUDIES

by
Rodney Barnes
Computer Janitor
925-819-1895

CASE #1

A CLIENT HAD THEIR LAPTOP TAKEN

CASE#2

AN INDIVIDUAL ALLOWED REMOTE ACCESS INTO THEIR MACHINE

1

WHAT TO DO IN BOTH CASES

- CHANGE YOUR PASSWORDS ON ACCOUNTS
  - THIS INCLUDES, BANK ACCOUNTS, INVESTMENT ACCOUNTS, AMAZON, LINKEDIN, ETC.
- CHANGE YOUR PASSWORDS ON E-MAIL ACCOUNTS
  - THIS IS ON ALL EMAIL ACCOUNTS.
- TELL SOMEONE YOU TRUST WHAT HAPPENED
  - MAYBE IT'S THE POLICE
  - MAYBE IT'S THE COMPANY YOU ARE WORKING FOR
  - MAYBE A FAMILY MEMBER
  - MAYBE YOUR CREDIT CARD COMPANIES

2

WHAT DO THE CASES HAVE IN COMMON?

- USER PLACING BLAME ON THEMSELVES
  - I SHOULD OF, COULD OF, MIGHT OF DONE SOMETHING.
- DISBELIEF IN WHAT HAPPENED
  - HOW COULD THIS HAPPEN TO ME?
  - IS IT OUT OF MY CONTROL?
- RELYING ON SELF TO FIND A SOLUTION
  - ASKING WHAT DO I DO NOW?
  - HOW FAST SHOULD I ACT?
  - DO I NEED TO TALK WITH SOMEONE TO HELP?
  - WHO DO I TRUST?

3

FACING THE FACTS

- IF THE COMPUTER WAS COMPROMISED THEN IT WAS COMPROMISED.
  - YOU HAVE TO FORGIVE YOURSELF.
- GETTING THE INFORMATION BACK IS REMOTE.
  - YOU HAVE TO ACCEPT THAT FACT.
- YOU HAVE TO ACT IN A TIMELY FASHION.
  - DON'T WAIT FOR DAYS TO RESPOND TO THE SITUATION.
  - IT TAKES ABOUT 15 MINUTES TO BREAK INTO A MACHINE.

4

CASE #1

- THE PERSON LEFT THEIR LAPTOP IN THEIR CAR UNATTENDED.
- THE DOOR TO THE CAR WAS UNLOCKED.
- IT WAS PARKED IN THE GARAGE.
- WHEN THE OWNER WENT TO THE CAR TO GET THE LAPTOP IT WAS GONE.

5

CASE #1

- WHAT TO DO BEFORE THIS HAPPENS
- WHAT TO DO ONCE YOU DISCOVER IT
- WHAT TO DO GOING FORWARD

6

WHAT TO DO BEFORE THIS HAPPENS

- ANY COMPUTER THAT HAS EITHER BUSINESS OR PERSONAL INFORMATION ON IT SHOULD BE BACKED UP.
- SECURE YOUR COMPUTER EQUIPMENT BY NOT LEAVING IT WHERE PEOPLE CAN SEE IT.
- DON'T PUT IT IN THE TRUNK WHEN YOU ARRIVE AT YOUR DESTINATION.
- DON'T RETRIEVE YOUR EQUIPMENT FROM THE TRUNK TILL AFTER YOU HAVE LEFT YOUR DESTINATION.
- THINK ABOUT DATA ENCRYPTION

7

WHAT TO DO ONCE YOU DISCOVER IT

- MAKE SURE YOU REALLY DID LOOSE IT
  - CHECK WHERE YOU LAST WERE WHEN YOU HAD THE COMPUTER.
  - CHECK IN THE TRUNK OR UNDER THE SEAT OF THE AUTOMOBILE
- CHANGE YOUR PASSWORDS
  - IF YOU KEPT YOUR PASSWORDS IN A PASSWORD FILE ON YOUR LAPTOP THOSE SHOULD BE CHANGED
- NOTIFY YOUR BANK(S)
  - ANY ACCOUNTS THAT WERE ON YOUR COMPUTER MIGHT BE COMPROMISED.

8

WHAT DO YOU DO ONCE YOU DISCOVER IT

- GET YOURSELF COMPOSED
- FOLLOW A PLAN YOU HAVE DEVELOPED
- RELAX, WHAT IS DONE IS DONE

9

WHAT TO DO GOING FORWARD

- CREATE A CHECK LIST THAT YOU USE WHEN YOU TAKE YOUR COMPUTER OUT OF THE HOME.
  - REMOVED COMPUTER FROM CAR
  - PICKED UP COMPUTER AND PLACED IN COMPUTER BAG
  - LAST USED COMPUTER AT
  - LAST KNOWN PLACE OF THE COMPUTER
- IF YOU KEEP YOUR PASSWORDS ON THE COMPUTER IN A FILE, DON'T HAVE THE FILE NAME AS "PASSWORDS", ENCRYPT IT.

10

CASE #1 NORMAL EMOTIONAL RESPONSE

- PANIC
- CONFUSION
- DISBELEF
- PUTTING BLAME ON SOMEONE OR THING
- AFRAID TO TELL ANYONE
- EMBARSEMENT

11

CASE #1 – RECAP BASIC FACTS TO FACE

THE DATA ON THE MACHINE WAS LOST

THERE IS LITTLE CHANCE OF ANY RECOVERY

COMPANY NEEDS TO BE CONTACTED

ACCOUNTS NEED TO BE UPDATED

PASSWORDS NEED TO BE CHANGED

12

CASE #2

- THE PERSON WAS HAVING PROBLEMS WITH THEIR MACHINE.
  - THEY WENT TO A WEB SITE AND AN AUDIO MESSAGE CAME ON SAYING THEY WERE INFECTED AND TO CALL THIS NUMBER AND NOT TURN OFF THEIR MACHINE.
- THEY HAD A PHONE NUMBER ON THE SCREEN TO CALL FOR ASSISTANCE.
- THEY CALLED THE NUMBER FOR HELP.
- THEY TALKED WITH SUPPORT PEOPLE OVER THE PHONE AND THE TROUBLED USER DISCRIBED THE PROBLEM.

13

CASE #2

- WHAT TO DO BEFORE THIS HAPPENS
- WHAT TO DO ONCE YOU DISCOVER IT
- WHAT TO DO GOING FORWARD

14

CASE #2 WHAT TO DO BEFORE THIS HAPPENS

- HAVE A BACKUP OF YOUR DATA
- DO A SYSTEM RESTORE POINT ON A REGULAR BASIS
- DON'T HAVE YOUR PASSWORDS IN A "PASSWORD FILE" ON YOUR DESKTOP OR THE MY DOCUMENT FOLDER
- IF YOU NEED A PASSWORD FILE HAVE IT ENCRYPTED OR ON A THUMB DRIVE
- KNOW THAT MICROSOFT WILL NOT CALL YOU UNLESS YOU HAVE AN OPEN TICKET

15

CASE #2 WHAT TO DO ONCE IT'S DISCOVER

- MOST TIMES, IF A TELEPHONE NUMBER FLASHES ON THE SCREEN FOR SUPPORT IT'S AS A RESULT OF THE BROWSER GETTING HIJACKED.
- CLOSE THE BROWSER YOUR IN AND TRY A DIFFERENT BROWSER TO SEE IF THE SAME MESSAGE COMES UP ON THE SCREEN.
- USE <CTRL> <ALT> <DEL> TO END THE BROWSER TASK TO EXIT IF NECESSARY.
- YOU CAN ALWAYS SHUT DOWN THE MACHINE.

16

CASE #2 WHAT TO DO ONCE IT'S DISCOVER

- RUN A FULL SCAN USING YOUR ANTI-VIRUS PROGRAM.
- RUN MALWARE REMOVAL PROGRAM ON THE SYSTEM.
- RESET YOUR BROWSER THAT HAD THE MESSAGE.
- CLEAR BROWSING DATA.
- CHROME CAN FIND HARMFUL SOFTWARE ON YOUR COMPUTER AND REMOVE IT. IT'S UNDER SETTINGS AND ADVANCE.

17

CASE #2 WHAT TO DO ONCE IT'S DISCOVER

- CONTACT MICROSOFT TECHNICAL SUPPORT FOR THEM TO CHECK OUT YOUR MACHINE.
  - THEIR PHONE NUMBER IS: 866-234-6020
  - THEY WILL REMOTE INTO YOUR MACHINE FOR A FEE
- CALL YOUR FRIENDLY PROFESSIONAL TO CHECK OUT YOUR MACHINE.
  - IN CASE YOU DON'T HAVE MY NUMBER: 925-819-1895
  - I WILL COME TO YOUR HOME OR OFFICE FOR A FEE

18

WHAT TO DO GOING FORWARD

- PROTECT YOUR ACCOUNTS AND PASSWORD(S)
- THINK TWICE ABOUT HAVING A PASSWORD PROGRAM KEEPING TRACK OF PASSWORDS.
- THINK TWICE ABOUT HAVING YOUR BROWSER PROGRAM KEEPING TRACK OF PASSWORDS.
- THINK BEFORE YOU HAND OVER YOUR CREDIT CARD INFORMATION.
- BACKUP YOUR SYSTEM
  - IF YOU GET A NASTY PROGRAM THAT ENCRYPTS EVERTHING IN YOUR DATA FILES IT COMES IN HANDY

19

CASE #2 - NORMAL RESPONSE

- THE USER CALLS THE PHONE NUMBER
- THE SUPPORT PERSON GAIN'S THE CONFIDENCE OF THE USER.
- REMOTE ACCESS IS GRANTED.
- SUPPORT PERSON GIVES PROOF OF PROBLEMS RUNNING.
- SUPPORT PERSON TELLS OF PRICES RANGING FROM $150 TO $800, I HAVE EXPERIENCED.
- THE USER PASSES THE PAYMENT INFORMATION.
- THE SUPORT PERSON DOES THEIR WORK, WHICH CAN TAKE HOURS. SOME PARTNER WITH SOMEONE LOCAL TO CLEAN THE SYSTEM.

20

CASE #2 PAYMENT METHODS

- ONCE THE PAYMENT TERMS HAVE BEEN DISCUSSED AND AGREED UPON, PAYMENT IS TO BE MADE.
- IT'S BEEN MY EXPERIENCE THAT THERE IS USUALLY A ONE TIME FEE OR SEVERAL YEARS OF SERVICE AVAILABLE FOR DIFFERENT FEES.
  - ONE ELDERLY CLIENT SUBMITTED ONE CREDIT CARD AND THE SERVICE COMPANY SAID IT DIDN'T GO THRU. THEY THEN ASKED FOR ANOTHER CREDIT CARD.
  - THE NEXT CREDIT CARD WAS GIVEN AND THEY SAID IT DIDN'T GO THRU. THEY THEN ASKED FOR A CHECK TO BE FAXED TO THEM, FRONT AND BACK. THEN THEY ASKED TO HAVE IT E-MAILED TO THEM AFTER BEING SCANED.

21

WHAT HAPPENS IF YOU TERMINATE

- IT'S BEEN MY EXPERIENCE THAT IF THE USER TERMINATES THE SUPPORT THAT SEVERAL THINGS USUALLY HAPPENS.
  1. THEY WILL GET MANY CALL BACKS OVER SEVERAL DAYS
     - ONE CLIENT GOT SO MANY SHE REFUSED TO ANSWER HER PHONE. THEY WENT AS FAR AS TEXTING HER MANY TIMES
  2. THEY WILL BE CHARGED FOR THE SUPPORT CALL
     - SOMETIMES THE BANK CAN BLOCK THE CHARGES
  3. THREATS HAVE BEEN ISSUED
     - THEY SAID THEY HAD ALREADY DISPATCHED SOMEONE TO COME OVER
  4. THE MACHINE MIGHT BE LEFT IN WORSE SHAPE
  5. PROGRAMS HAVE BEEN DEPOSITED ON THE MACHINE

22

CASE 2 – BASIC EXPERIENCES

CLIENT CALLED THE NUMBER ON THE SCREEN

CLIENT GAVE OVER THEIR MACHINE TO ANOTHER

CREDIT CARD(S) INFORMATION GIVEN

COPY OF SIGNED CHECK FAXED TO SERVICE ORGANIZATION

ONE EXPERIENCE THE SERVICE COMPANY WAS REMOTED IN FOR OVER 3 HOURS

ONE INCIDENT THE SERVICE COMPANY TRIED TO MAKE A DIRECTORY LISTING OF EVERY FILE ON THE MACHINE IN A DOS WINDOW

A LEVEL OF ANXIETY INCREASES AS TIME PASSES

23

RECAP - WHAT TO CONSIDER TO DO

- NOTIFY THE CREDIT BUREAUS
  - THEY MIGHT FLAG YOUR ACCOUNTS
  - YOU MIGHT BE ABLE TO SETUP SECURITY ON THE SSAN FOR UNUSUAL ACTIVITY REPORTING
- CONTACT THE BANK AND NOTIFY THEM OF THE SITUATION
  - THEY MIGHT MONITOR YOUR ACCOUNTS
  - THEY MIGHT CLOSE OLD ACCOUNTS AND OPEN NEW ACCOUNTS
  - THEY MIGHT PUT A HOLD ON YOUR ACCOUNTS

24

RECAP - WHAT TO CONSIDER TO DO

- IF IT WAS A COMPANY COMPUTER, NOTIFY THE COMPANY SO THAT THEY CAN TAKE STEPS TO PROTECT THEIR DATA.
- IF IT WAS A GOVERNMENT COMPUTER THEN BE PREPAIRED TO FILE A POLICE REPORT ONCE YOU REPORT IT TO THE GOVERNMENT.
- NOTIFY CREDIT CARD COMPANIES.
- NOTIFY ONLINE DATA STORAGE COMPANIES YOU MIGHT SUBSCRIBE TO.

25