SHARE San Jose 2017

Ransomware on the Mainframe Checkmate!

Chad Rikansrud

#SHAREsjc

SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.

SHARE
EDUCATE · NETWORK · INFLUENCE

About me

- Speaker at conferences
  - DEF CON, Derbycon, SHARE, RSA 2017, others
- Mainframe security consultant
- Reverse engineering, networking, forensics, development
- Mainframe (z/OS) researcher
- Doer of other stuff that probably isn't interesting

What is ransomware?

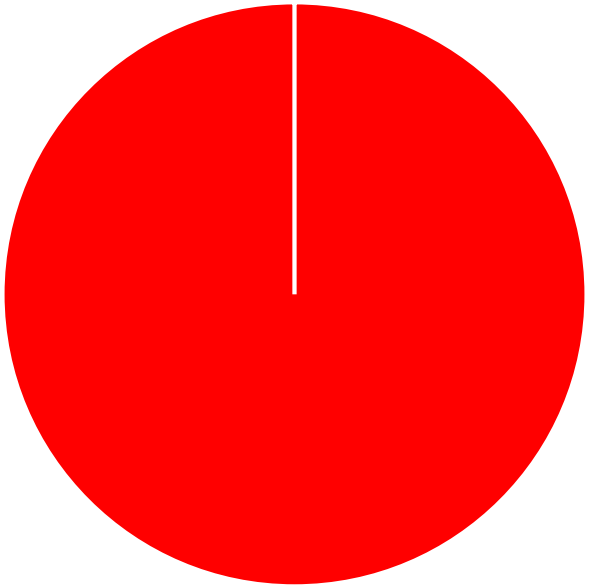
- Ransomware comprised of three major parts:
- Infection vector (phishing, web drive by, SE, other)
- Payload - generate key, enumerates and encrypts files
- Command and Control (optional)
  - Communicates with victims
  - Stores keys
  - Other items as required (e.g. customer service)

Why are we here?

SHARE
EDUCATE • NETWORK • INFLUENCE

- Was asked this question by some C-Levels:
  - “Do you think a mainframe could ever be infected by ransomware?”
- Me – after about 17.3 seconds of thought:
  - “Yes. And it would work really well!”
- Them:
  - ”You can’t just open an email on a mainframe.”
- Me – after shaking head:
  - “Right. But there’s still at least 3-4 ways I can imagine this working.”
  - “This is a misconception, other ways of introduction of malware.”

Percent of Systems Susceptible to Malware



- All of them.

About this presentation

- Did not build a fully working copy of ransomware for the mainframe
  - Liberties were taken for security's sake
  - But, if I can do it ....
  - This can be done
  - Do not rely on the obscurity of a system as a measure of prevention
- Just another computer

So, why would it “work really well?”

SHARE
EDUCATE • NETWORK • INFLUENCE

- Mainframe designed for batch workloads
- Superfast I/O to disk + massive caching
- Centralized catalog structure makes finding files a breeze
- Most of all

BLISTERINGLY FAST HARDWARE ENCRYPTION

Ok, so how would this work?

SHARE
EDUCATE • NETWORK • INFLUENCE

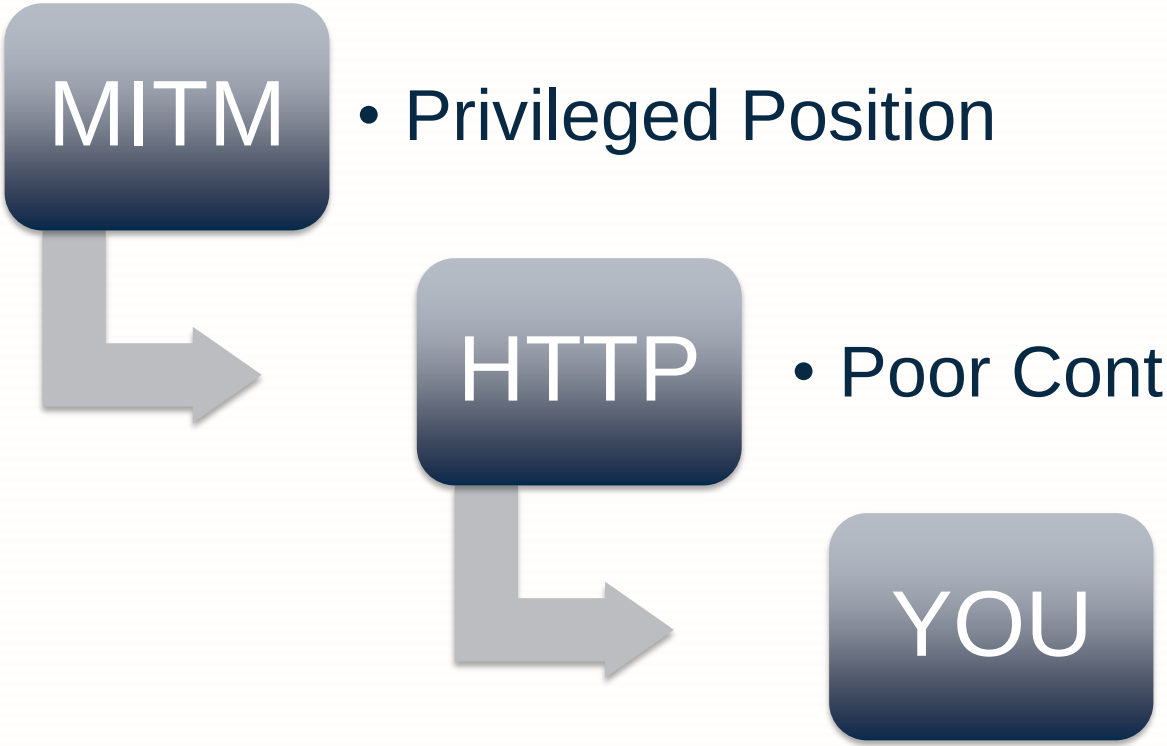
- Here is one idea:
  - System administrator is infected by malicious email / webpage
  - Malware deploys stage1 – keylogging & network sniffing
    - Captures tn3270 traffic, records hosts / ports
    - Captures User IDs / passwords relative to them
  - Malware deploys stage2 – upload, compile & run code
    - Use tn3270 host / port to upload code (using creds captured)
    - Multiple upload protocols (FTP, NJE, tn3270, SSH)
  - Victim system compiles & runs code

DEMOS

Ransomware Process

Infection

Drive-by Infection (one example)



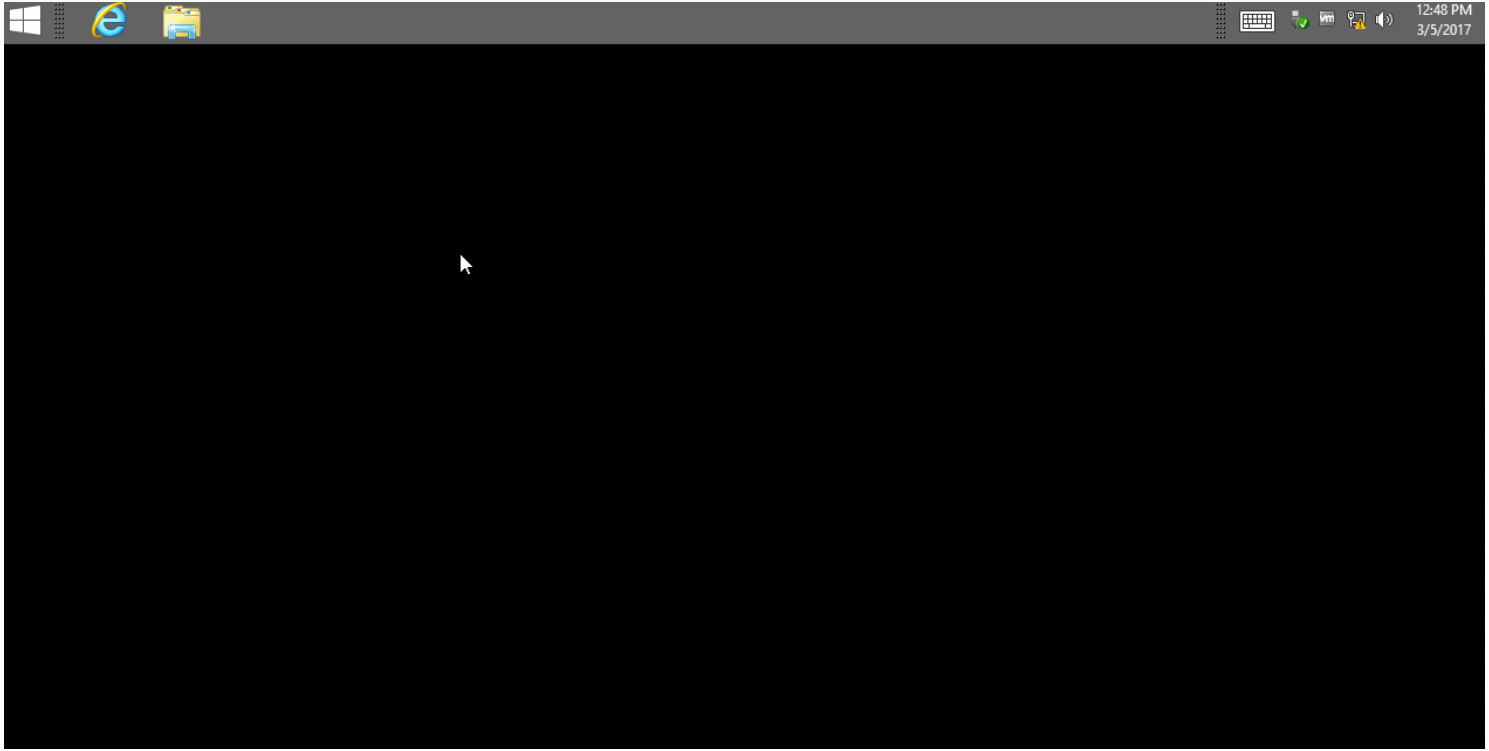
- Privileged Position
- Poor Controls
- Browse

Other types

- Malicious attachment
- URL Redirect to similar looking site
- Image processor
- Plug-in vulnerability (Flash anyone?)
- Myriads more. Some require interaction, some do not

Reconnaissance

Key Logger



Connection Getter

```
96          perror("Error allocating memory\n");
97          return 1;
98        }
99      }
100
101     // populate table
102     if ((dwRetVal = GetTcpTable(pTcpTable, &dwSize, TRUE)) == NO_ERROR) {
103
104       for (i = 0; i < (int) pTcpTable->dwNumEntries; i++) {
105         tsta = htonl(pTcpTable->table[i].dwRemoteAddr);
106
107         // make sure EST state first
108         if (pTcpTable->table[i].dwState == MIB_TCP_STATE_ESTAB) {
109
110           // are we looking at a local rfc1918 adr? if so carry on, if not move on
111           if ((tsta >= n10s && tsta <= n10e) ||
112               (tsta >= n172s && tsta <= n172e) ||
113               (tsta >= n192s && tsta <= n192e)) {
114             IpAddr.S_un.S_addr = (u_long) pTcpTable->table[i].dwRemoteAddr;
115             strcpy_s(szRemoteAddr, sizeof (szRemoteAddr), inet_ntoa(IpAddr));
116
                                                                                96,9
```

This PC | C:\WINDOWS\sys... | Google - Internet ... | tn3270 - offline | tn3270 - offline

1:31 PM
3/3/2017

C:\WINDOWS\system32\cmd.exe

```
C:\Users\chad\Downloads\ftpclient>tcp_check.exe
```

Google

Gmail Images Sign in

Google works better with Chrome. Try it?

NO THANKS YES, GET CHROME

Privacy Terms Settings

Deliver Payload & Enumerate Files

Payload Uploader

- For this example, wrote a simple FTP Client in C
- Hard-coded commands to upload malicious binary
- Uses JES/FTP commands to execute binary
- Checks for completion and cleans up
- Works on Win/Mac/Linux
- Uses input from key logger & connection getter

Payload Uploader

```
#include <stdio.h>

#ifdef WINDOWS            // windows
#include <winsock2.h>
#include <windows.h>
#include <ws2ipdef.h>
#else
#include <sys/socket.h>
#include <netinet/in.h>
#include <netinet/tcp.h>
#include <arpa/inet.h>
#endif //WINDOWS

// should be system agnostic
#include <sys/stat.h>
#include <fcntl.h>
#include <stdlib.h>
#include <string.h>
                                                    1,1           Top
```

Enumerate Datasets

- Using program from CBTTAPE
- Modified for our purposes
- Pass Master Catalog – lists all datasets
- Added RACROUTE function to test for write access
- This would be the input to the encryption function

Enumerate Datasets

```
Command ===>                                                    Scroll ===> CSR
****** ***************************** Top of Data ******************************
000001 *
000002 *  WORKS FOR VSAM / NONVSAM CATALOG ENTRIES ONLY
000003 *
000004 MYLC CSECT
000005 MYLC AMODE 24
000006 MYLC RMODE 24
000007          STM   14,12,12(13)
000008          BALR  12,0
000009          USING *,12
000010          ST    13,SAVE+4
000011          LA    13,SAVE
000012          OPEN  (PUTDCB,OUTPUT)
```

Enumerate Datasets

```
COMMAND INPUT ===>                                                SCROLL ===> CSR
******************************** TOP OF DATA ********************************
NONVSAM ------ ADCD.DYNISPF.ISPPLIB
NONVSAM ------ ADCD.LIB.JCL
NONVSAM ------ ADCD.S0W1.HZSPDATA
NONVSAM ------ ADCD.Z21F.CLIST
NONVSAM ------ ADCD.Z21F.DBA.ISPPLIB
NONVSAM ------ ADCD.Z21F.DBB.ISPPLIB
NONVSAM ------ ADCD.Z21F.ISPPLIB
NONVSAM ------ ADCD.Z21F.LINKLIB
NONVSAM ------ ADCD.Z21F.LPALIB
NONVSAM ------ ADCD.Z21F.PARMLIB
NONVSAM ------ ADCD.Z21F.PROCLIB
NONVSAM ------ ADCD.Z21F.SAXREXEC
```

Encrypt Files

Encrypt Datasets - flow

- Attacker has privileged position
- Injects Javascript to a common website
- User browses this site
- Unknowingly runs malicious code in browser
  - Keylogger
  - GetConnection
  - UploadPayload
  - ExecutePayload

Encrypt Datasets

```
Menu  Options  View  Utilities  Compilers  Help
--------------------------------------------------------------------------------
LEELA - Data Sets Matching BADGUY.FIXED*                    Data Set - Browsed
Command ===> _____________________________________________ Scroll ===> CSR

Command - Enter "/" to select action                 Message          Volume
--------------------------------------------------------------------------------
        BADGUY.FIXED.BLOCK                           Browsed          TEMP00
        BADGUY.FIXED.BLOCK2                          Browsed          TEMP00
        BADGUY.FIXED.BLOCK3                          Browsed          TEMP00
****************************** End of Data Set list ******************************

*DSLIST
```

Finally .. Demand

Demands

- Typically looking for Bitcoin
  - Mostly untraceable
- Does your company have a policy?
- What if there aren't demands?
  - Just cause mayhem
- Often files left behind with demands

Demand Notification

```
Menu  Options  View  Utilities  Compilers  Help
------------------------------------------------------------------------------
LEELA - Data Sets Matching BADGUY.FIXED*                          Row 1 of 3
Command ===> _____________________________________________ Scroll ===> CSR

Command - Enter "/" to select action                 Message          Volume
------------------------------------------------------------------------------
         BADGUY.FIXED.BLOCK                                           TEMP00
         BADGUY.FIXED.BLOCK2                                          TEMP00
         BADGUY.FIXED.BLOCK3                                          TEMP00
****************************** End of Data Set list ******************************

*DSLIST
```

Notify / Alerting

- How will you know about the attack?
- Do you realize something's happened?
- Likely jobs are crashing
- But what if they don't?
- The ransom screen?
- Once you figure it out, then what?

Incident response

Recovery

- This is happening, but slowly
- Need solutions similar to Time Machine (Think Mac)
  - Also needs intelligence for restarting jobs, etc.
  - Some solutions exist for this already
- Any solution must preserve forensic evidence
- Adjustable RPOs
- Reasonable RTO (hours? minutes? seconds?)

What to do?

- Multi-Factor Authentication
- Egress Filtering!
- Training
- Endpoint Protection
- Lock Down Crypto APIs
- Logging, Monitoring, Integration, Correlation

What to do – part 2

- Behavioral analysis
- Start penetration testing
- Partner with vendors
- Think like an adversary
- Phishing / social engineering

SHARE
EDUCATE • NETWORK • INFLUENCE

Thank You for Attending!

Complete your session evaluations online at SHARE.org/Evaluation

SHARE San Jose 2017

Appendix A

Encryption everywhere scenario

Phew, thank god that's over

- But ….
- It gets worse. That was the hard way.
- And it's not just "big iron."
- What about:
  - "**Encryption Everywhere**"

Encryption everywhere ..

- What is it?
  - All data files / disks are encrypted
  - Excellent for compliance / data protection
- Excellent idea for data privacy – but ….
- Focuses the risk now concentrated on key management
- Doing the attacker's work for them
- Key management centralized
- What would this attack look like?

Encryption Everywhere Takeover

- Attacker compromises key management system
- Attacker rotates/changes master keys (key encrypting keys)
- Wait for x days, weeks – then delete original keys
- What happens next?
  - Victim machine is eventually rebooted, needs to load keys
  - And then . . .

GAME OVER