RSH CONSULTING

Examining A Mainframe Internet Hack

KOIRUG – October 2018

RSH Consulting – Robyn E. Gilchrist

RSH Consulting, Inc. is an IT security professional services firm established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050

Robyn E. Gilchrist is a Senior RACF and CA ACF2 Consultant. She assists clients with conducting penetration and vulnerability tests to evaluate z/OS controls and with enhancing access controls. As a systems programmer and network engineer, Ms. Gilchrist has installed, configured, and maintained the z/OS Communications Server and WebSphere Application Server (WAS) for z/OS in Network Deployment (ND) mode with associated ACF2 and RACF controls. She has converted CPF-connected ACF2 databases to RRSF-connected RACF databases.

- 617-977-9090
- R.Gilchrist@rshconsulting.com
- www.linkedin.com/in/robyn-e-gilchrist/

SÄPO Police Report of Events on March 19, 2012

FTP data egress and telnet are seen on systems where normally that activity is very rare

Approximately 1.7TB of data has been illegally downloaded to an IP address in Cambodia

The CEO describes the situation at Logica as "panicky"

Logica Hack Overview

- Logica operates many z/OS datacenter locations including Bromölla, Sweden
- Beginning in January 2010, Applicate, a user of Logica mainframes and host of the Infotorg application data portal, began receiving reports of intermittent lock outs of FTP and CA-TPX USERIDs. At least one of the FTP connections downloaded data.
- In March 2012, hackers stole Logica's RACF database and cracked passwords for over 30,000 USERIDs using tools freely available on the internet.
- The hackers created multiple backdoors and used them to steal information including the identities of Swedish citizens in witness protection, Swedish national taxing authority records and the SPAR database, a Swedish government database.

Research Information Sources

- The Logica hack is so well known because there are lots documents on WikiLeaks - https://wikileaks.org/gottfrid-docs/
  - "These documents have been obtained by FOIA except for the correspondence with the prison relating to GSW's requests to access distance education and to use a graphing calculator. The letters are translated into English."
- A trial transcript translation is located at: http://qnrq.se/anakata-translated-hearings/
- Some English translations were provided, but for the most part, RSH used Microsoft Translator and Google Translate to translate and review the original documents
- The security report is heavily redacted seemingly to exclude information on the vulnerabilities that enabled the hackers to succeed

Research Information Sources

- Reviewing the Logica documentation is not for the faint of heart. Aside from the language barrier to non-Swedish speakers, the volume of material is substantial.
  - Each review of the documents unmasks another tidbit of knowledge
  - The language barrier was thought to be a control for the unsecured TPX sessions in 2010. They did not anticipate Bing Translate and Google Translate.
    - säkerhet genom dunkel

- This presentation provides RSH's observations and conclusions regarding the z/OS attack and suggested actions to mitigate attack vectors

Victims and Interesting Software

Organization	Involvement
Bisnode	Corporate owner of Applicate and Logica
Logica	A UK-based IT service provider and owner of the attacked z/OS systems
Applicate	Users of dedicated LPAR (SY19) and shared LPAR (SYS3), developer of Infotorg
Volvo IT	Co-tenants of LPAR SYS3 with Applicate

Software	Description
Infotorg	An information portal to government systems, including the Statens Person-och AdressRegister (SPAR), a Swedish government database.
aptcli	A *nix based program used to provide the hackers with a shell to z/OS Unix System Services

Attackers and Enablers

Name	Involvement
Gottfrid Svartholm Warg (a.k.a. GSW, anakata, lLT)	A very talented technician believed to be the mastermind behind the Logica attack. A co-founder of The Pirate Bay file sharing website, he fled to Cambodia where he became the subject of an Interpol warrant. He was extradited back to Sweden to stand trial for the Logica attack and was sentenced in 2013.
DiROX	An associate of GSW, DiROX used Internet Relay Chat (IRC) on the Swedish hacker website hack.se. Arrested in Sweden with a 3000m range antennae used for breaking into WiFi, Logica's logs show FTP downloads to and InfoTorg searches from DiROX's IP address in Sweden. DiROX led the police to GSW.
~~XXXXXXXXXXX~~	A user on a mailing list who had extensive discussions with the hackers about how to gain access to z/OS systems. The approach discussed was "very similar" to the actual hack.
~~¥¥¥¥¥¥¥¥¥¥¥~~s	Other suspected hackers downloaded or received copies of programs from SY19. Their exact involvement is unknown. The unrealized backdoors are written with German comments.

Goals and Objectives

- Hacker goals and objectives in the Logica hack:
  - Establish as many entry points into the system as possible to ensure connectivity if any one of several backdoors is closed
  - Acquire as many USERIDs and their passwords as possible
  - Obtain IDs with UID(0), Unix SUPERUSER, and RACF SPECIAL
  - Look around to see what is interesting
  - Steal data to be used for criminal purposes

Notable Events – FTP downloads in 2010

- "On 1/29 at 23.00, SEMA290 logs on via FTP and starts downloading a number of Files."
  - "Goes through FTP and downloads a large amount of datasets/files. See Appendix. Attempted retrieval of datasets stopped: see Appendix"
  - FTP logons are failing due to USERIDs being revoked on SYS3

Notable Events – Suspicious activity in 2010

- Two years prior to realization of the attack, Applicate called Logica Help Desk to report Applicate users being revoked without corresponding logons.
- Volvo IT and Applicate were co-tenants on LPAR SYS3
- “Logica contacts Volvo IT to ask for their assistance with troubleshooting Case is opened by Applicate. Troubleshooting starts, lose sessions in TPX” and that userid becomes revoked without the user being logged on.”

Notable Events – Volvo IT and the 2010 Security Report

- "The IP address from Cambodia blocked from SYS19 (and SYS3) by Volvo IT."
- "Due to a mistake from the current operating supplier, Volvo IT, there was an opportunity for the attacker to logon via TPX. At the time of the attack, the assessment was made that the intruder via TPX did not make any changes to data or copy additional data. The attacker made some changes to RACF which were backed up." – quote from Logica 2010 Security Incident Report
- "Developed list from Volvo IT shows that logging on via TPX without password is possible"

Stolen USERIDs that copied data with FTP

- AVIY356
  - USERID associated with Riksdag (Parliament)
  - First indicated USERID to be used in the attack
  - Access to z/OS USS
  - USERID that stole the RACF database
- SPRBI01, SPRBI08
  - RACF USERIDs described as “sales partner USERIDs”
- DAF1682 and SEMA290
  - CICS/TSO USERIDs
- BSN0058
  - An early use Infotorg USERID with mainframe access
- NUS
  - An admin USERID on LPAR SYS3 (SPAR location)
- WAHS006
  - A late use Infotorg USERID owned by the attorney who represented Hollywood in The Pirate Bay trial that convicted GSW

Attack Vectors

- FTP accessible from internet
  - Used an unprivileged CICS user's ID to gain early access
    - ID obtained Unix credentials via FACILITY class profile BPX.DEFAULT.USER
  - JESINTERFACELEVEL allows “SITE FILETYPE=JES” command
    - Issue JES2 and MVS OPERATOR commands
    - SUBMIT batch jobs including IRXJCL, BPXBATCH and IKJEFT01
- TSO commands from USS
  - tsocmd did not exist in Logica systems prior to hack
  - Believed to be installed by hackers
  - Not evident from FTP logs how tsocmd was uploaded
- CICS enumeration of valid USERIDs
  - Tested USERIDs sequentially to determine users with elevated authority
  - Tested different transactions
  - 1600 transactions per hour = scripted attack

Attack Vectors

- Zero-day Exploits
  - CNMEUNIX is the IBM Netview Unix command processor.
  - A design flaw allowed unauthorized users to gain access to UID(0).
- Compromising Services
  - Modifying inetd to add rogue entry
  - Stealing ssh private keys or modifying ssh public keystore
- USS file systems
  - /tmp

….. Fast forward to 2012

Notable Events – High CPU noted in 2012

- Wednesday March 7, 2012

- Applicate calls Logica Help Desk and asks to confirm high CPU utilization on SY19

- Logica asks Applicate to contact the owner of BSN0058 (an Infotorg search USERID) and determine why the user has a high CPU utilization socket open on z/OS

- Applicate revokes BSN0058 at 12:35

- Applicate and Logica escalate the issue from a performance problem to a security incident

Backdoors Installed – Reverse Shell

- C and REXX programs created by the hackers
- Reverse shell is when z/OS communicates back to local machine and local machine starts a program to listen
  - BPXAS starts a service on port 443 outbound
  - On local machine, issue c:\BadActor**aptcli**.exe which listens for a connection from z/OS
  - Works like VTAM terminals

Backdoors Installed – a.env (renamed CSQXDISP)

- The hackers renamed /tmp/a.env to CSQXDISP to disguise its presence in OMVS list process (ps) command output
- The hackers tried (and failed) to set the APF and Program Control bits.
  - No evidence they did not manage to eventually set
- CSQXDISP used reverse shell to aptcli on the perpetrator's machine

Backdoors Installed – REXX program

- "go.rx" (kurwa on SYS3) uses SETUID/SETGID to elevate authority and then calls USS shell
  - A "trampoline" hack
- Speculation – likely had access to SURROGAT BPX.SRV.*

Backdoors Installed – inetd.conf

- Attackers added an entry to inetd.conf to listen on port 443

443 stream tcp nowait SUPERUSR /bin/sh sh

- This allows any user that connects to port 443 to acquire a USS shell with SUPERUSR USERID. No password required.

- There is no evidence provided on when the change to inetd.conf was made or how it was implemented

Backdoors Developed But Not Installed

- Evidence was recovered from the hacker's computers that indicated other backdoors were developed on Hercules, a PC/*nix based software implementation of the 370/390/z architecture instruction set.

- SVC242 returns to the caller with elevated program authorization and then program TFY.BACKDOOR sets KEY=0, Supervisor state and flips the ACEE bits for SPECIAL, AUDITOR, OPERATIONS

- No evidence of these programs was recovered from Logica LPARs.

Notable Events - RACF Database Theft

- Saturday March 10, 2012 @ 03:27:23
- The RACF database was copied into /tmp and “tarred” into an archive file for ease of transport.
- The RACF database was exfiltrated to an IP address in Cambodia using FTP by AVIY356, a Swedish Riksdag USERID with improper access
- At this point the hackers started to work on the RACF database offline with “John the Ripper,” an open source password cracking tool.
  - Logica tests performed during the post mortem reveal around 30,000 passwords were easily cracked for SY19 in a few days using a reasonably powered standalone PC. Over 10,000 passwords were common to SY19 and SYS3.
  - Many of these passwords were easily guessed from common dictionary words, simple patterns and default passwords.
  - RACF extensions to John the Ripper appeared in the toolkit on the internet a short time after the hack.

Notable Events – Access is blocked

- Friday March 16, 2012
- All day long the volume of activity increases with hundreds of TSO logons and thousands of FTP downloads proceeding until …
- SY19 port 443 was blocked at the firewall
- The rogue entry in inetd.conf is removed
- SERVAUTH to deny FTP access to the HFS is implemented

EZB.FTP.SY19.FTPD1.ACCESS.HFS

- SYS3 was blocked for all internet FTP activity
  - An extended filtering whitelist was applied to SYS3 and connectivity to the internet was re-established
- The Logica research team went back four months including year end 2011 to make sure no backdoors had been placed with year end processing.
  - No additional evidence of backdoors was found

Hacking Defense – RACF Best Practices

- Restrict access to the RACF databases, both live and off-line copies
- Ensure sensitive data is properly protected
  - Good profile definitions
  - Pervasive encryption
- Strengthen user authentication
  - Mixed-case passwords
  - Passphrases
  - KDFAES
  - Multi-Factor Authentication (MFA)
- Monitor and/or secure RACF list commands like LISTUSER and RLIST

Hacking Defense – RACF Best Practices

- Strengthen Unix controls
  - Limit UID(0) on OMVS segments to server/daemon USERIDs only, as documented
  - Restrict access to BPX.DAEMON to server/daemon USERIDs only, as documented
  - Replace UID(0) with BPX.SUPERUSER access where ever feasible
  - Restrict access to SURROGAT BPX.SRV.userid profiles for privileged IDs
  - Use UNIXPRIV and FSACCESS classes to restrict privileges to UNIX resources, like the chmod command, and filesystems
  - Use FSEXEC to block the execution of programs and scripts from the /tmp directory
  - Give careful consideration to the implementation of BPX.UNIQUE.USER and the auto assignment of OMVS segments with UIDs

Hacking Defense – FTP and TN3270

- Restrict inbound access to mainframe FTP
  - White list trusted hosts at the firewall
  - Implement APPL class to restrict access to the FTP server
  - Use SERVAUTH to restrict FTP access to Unix File System
- Protect TCP/IP Ports
  - TCP parameter RESTRICTLOWPORTS
  - Use TCP PORT parameter and SERVAUTH to restrict access
- Deny access to FILETYPE=JES operand on the SITE command
  - FTP user exit FTCHKCMD
  - Heavy handed, but as a user exit, it can be refined and customized
  - Downside is that as a user exit is must be refined and customized (and maintained)
    - A challenge if you do not have much experience with z/OS exits or Assembler programming
- Use FTPS/SFTP and TN3270E
  - Encrypt traffic to reduce risk from WiFi snooping of clear text passwords
  - Use ICSF to store keys
  - Segregate SSH keys into unique FILESYSTEM with FSACCESS protection

IBM Request For Enhancement

- An IBM Request For Enhancement (RFE) has been created by RSH Consulting to improve the FTP to JES interface security

- RFE 125660 – Increasing Security and Control for FTP JES Interface
  - Requests JESINTERFACELEVEL=0 parameter in FTP.DATA to disable the FTP to JES interface
  - Requests a SAF resource to restrict job submission and sysout retrieval via FTP for installations that require the FTP to JES interface

- See RSH RACF Tips article on entering, examining, and voting on RFEs
  - https://www.rshconsulting.com/racftips/RSH_Consulting__RACF_Tips__January_2016.pdf

- Be sure to vote!

Quote From Logica Security Incident Report

"If the system resources are well protected and the hijacked user had a limited access right, then the security will hold."

- Report on the IT security incident of 2012 – External Version 1.3, page 36