16898: A Forensic Analysis of Security Events on System z, Without the Use of SMF Data

Brian Marshall
Vice President, Research and Development
Vanguard Integrity Professionals

Monday March 2, 2015
Well, today it’s all about data!
So, where is your data today?

Wherever you are........

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
Your data on the move with tablets....

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
...and oh so many devices!

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
Is your data in the cloud?

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
In the hands of criminals?

Knowledge is free.
We are anonymous.
We are legion.
We do not forgive.
We do not forget.
Expect us.
In the hands of other nations?
In the hands of some government agency?

I STOLE YOUR FACEBOOK LOGIN, CELLPHONE RECORDS & EMAIL PASSWORD

BUT IT'S COOL, YOU HAVE NOTHING TO HIDE, RIGHT?

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
We hear it every day!
Because the truth is….

You are about to be compromised

OR

You have already been compromised
Maybe you have better security......

The web became significantly more malicious, both as an attack vector and as the primary support element of other trajectories (i.e. social, mobile, e-mail, etc.).
Attack Statistics

Sampling of 2013 security incidents by attack type, time and impact

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
Biggest IT Myths

- Hey, it won’t happen to us!
- Buy this tool <insert tool here> and it will solve all of your problems.
- Let’s get the policy in place and we are good to go.
- I passed my IT audit, I must be secure.
Their M.O.

The cyber spies typically enter targeted computer networks through “spearfishing” attaches, in which company official receives a creatively disguised email and it tricked into clicking on a link or attachment that then opens a secret door for hackers.
They can’t get to me, I’m secure.

- Hackers go after suppliers to get into larger companies.
- Smaller companies tend not to have the funding, staff, or knowledge need to formalize – let alone maintain – more secure policies and procedures all combining to make them the path of least resistance….and the bad guys have discovered this.
But I run a mainframe. I’m not vulnerable.
While most IT security teams tend to lump mainframe systems into the category of legacy systems unnecessary or impossible to scrutinize during regular audits, that couldn't be farther from the truth, says a researcher at Black Hat USA.

On Mainframes.. I see them described as legacy all the time: 'Oh, we don't need to implement this policy because it's a legacy system.' Calling a mainframe legacy is like calling Windows 2012 Server legacy because parts of the Window NT kernel are still in the code. Or it's like calling my car legacy because it's still got tires," said Philip "Soldier of Fortran" Young, explaining that most enterprise mainframes today run off the IBM z/OS platform.

As part of the Black Hat presentation on Mainframe Vulnerabilities to being breached, a website with a number of tools to aid with the hacking of a mainframe was released including VERY SPECIFIC mainframe vulnerabilities (ACEE zapper, USS elevated permission code, TN3270 sniffers)

https://github.com/mainframed
In Response to Black Hat 2013 Mainframe “Hackable” Presentation

Excerpt from his response:

The person responsible for mainframe database security, don’t have a lot to worry about. And if you were worried about these attacks, you can disable FTP to thwart malicious code uploads. Or firewall off the mainframe from Web access, as seems common.

Any one want to guess why Adrian Lane is JUST WRONG???
In Response to Black Hat 2013

Adrian Lane states in the article:

• The reason we don’t hear about DB2 hacks is that, “Because Nobody uses it”.
  – Wow
• Mainframes come with “a Supplementary UNIX environment”. - How many of us run a z/OS system without UNIX? Does this negate or even mitigate the vulnerability?
• About the mainframe: “Mainframes do not attract attackers.” - I guess security by obscurity is alive and well.
• If you are worried about security, you need only wall off the mainframe from all internet access.
  - I guess all those applications (Airline Reservations, ACH transfers, Inventory Management Systems, Banking, Financial and Government applications) DO NOT NEED to run with connectivity to the world.
Logica and Nordea Bank Mainframe Breach 2013

Pirate Bay co-founder charged with hacking IBM mainframes, stealing money

IDG News Service >

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
Lessons Learned

Bill for date breach was expensive…Investigations aren't cheap!

Findings:
• Pirate Bay co-founder Gottfrid Svartholm Warg was charged with hacking the IBM mainframe of Logica, a Swedish IT firm that provided tax services to the Swedish government, and the IBM mainframe of the Swedish Nordea Bank, according to the Swedish public prosecutor.
• “This is the biggest investigation into data intrusion ever performed in Sweden”, said the public prosecutor Henrik Olin.
• It is not really clear why Logica was hacked said Olin. But the intruders stole expensive personal and vehicle data, including security numbers.
• They attempted to steal over $900K from Nordea customer accounts.
But Wait!!!

In September of 2013, Gottfrid Svartholm was cleared of hacking into the Swedish bank Nordea because it was impossible to prove that he had illegally gained access to their mainframe even though $990,000 was stolen and even though his conviction for hacking into the Banks IT provider Logica was upheld.
So what now???

- I have SMF running.
- I track my privileged users right?
- I don’t have unnecessary libraries in APF list.
- I follow the NIST security guidelines for securing my system.
- I pass all of my audits.

I must be secure!!!!!
So what now???

Are you sure???
So what now???

Of course not, but you can be more sure.
How?

With Vanguard Offline and Correlog.
What is Vanguard Offline?

Vanguard Offline is a product that captures all access requests passed to RACF, saves each unique access in a VSAM file, which then allows customers to execute RACF commands against a test copy of the RACF database and thereby evaluate the impact of those commands given historical authorization information.
What is Vanguard Offline?

- Vanguard Offline also provides reporting against all of the historical data and allows you to essentially data mine the access requests to RACF database.
- Reporting can be done against the raw access records, or can be replayed against a copy of the racf database for real time (batch or online) reporting of changes to access.
- Data capture is achieved through the use of RACF exits.
A RACROUTE REQUEST=AUTH determines whether a user is authorized to obtain use of a resource.
RACROUTE REQUEST=FASTAUTH examines the auditing and global options in effect for the resource while determining the access authority of the caller. There are two types of these exits: ICHRFX02 and ICHRFX04.
A RACROUTE REQUEST=VERIFY or RACROUTE REQUEST=VERIFYX request is used to determine whether a user ID is defined to RACF® and whether the user has supplied a valid password or password phrase and group name.
So what can we get from these exits?

Who – Userid
What – resource
Where – Terminal ID
When – Date and Time of access
How – Covering Profile (or other method that allowed access)
Access Requested
Access Allowed
Access History Reports

Access History reports are available organized in several ways:

- Access Summary by Access
- Access Summary by User
- Access Summary by Group
- Access Summary by Class
- Access Summary by System
- Access Detail by Masking
- Access Detail (Complete List)
- Access Detail (Denied Access)

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
Access History Reports

- Summarize all access data in the VOF history master file
- “Drill down” to view specific access records
- Direct mode – from VOF history master file
- Extract mode – from flat file created with the VOF history master file
What is the value?

• Provides a safe offline environment for testing changes in access
• Lowers the risk of making changes to access to production systems
• Provides reports to view details of individual access records
• Allows for complete reporting of who accessed what or attempted to access what, w/o having to peruse days/weeks/months or years of SMF data
• Can be used as a forensic tool or as a method to ensure that access is/is not granted any longer.

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
How It Works

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
CorreLog Agent for z/OS

Bridging the z/OS Gap in Your SIEM
Mainframe in the Network Security World

- Routers
- Firewalls
- Linux
- Windows
- Unix
- Web Server
- Security Operations Center

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
**SIEM Integration**

- Flexible enough to integrate with any SIEM or MSSP
- Customers running with LogRhythm, ArcSight, IBM QRadar, Dell SecureWorks, CorreLog SIEM, NTT Solutionary, Splunk and more
- SIEMs provide correlation, forensic archive, real-time alerts, reporting, etc.
- Very flexible configuration – out of the box compatibility
z/OS Events in ArcSight ESM

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
z/OS Events in Splunk

Complete your session evaluations online at www.SHARE.org/Seattle-Eval
Thank You

Stop by and visit us at Booth 607!