SDT / Security Summit Files

FTA Technology Conference
July 31, 2017
Indianapolis, IN
Rod Sterling, IRS

Main Points

- Security Summit Overview
- Role of the Participants
- Security Summit Files for States
- SDT Customer Support
- SDT Connection & Authentication

Security Summit Overview

- Objective: to protect the American taxpayer by combating identity theft tax refund fraud through enhanced communication, information sharing and analysis among the parties involved:
  - IRS
  - States
  - Industry Partners
  - ISAC

Security Summit Overview

- Summit involves the exchange of information in the form of various files including:
  - Industry Lead Reports
  - PITRF files (Potential ID Theft & Refund Fraud)
  - Summit Miscellaneous Files
  - State leads, feedback, analysis reports, etc.
- File exchange methods include SDT, SES and other clients such as Accellion & MOVEit

Role of Industry

- Analyze and report indicators of potential ID theft/refund fraud using minimum standards and methodology developed for Summit
- Identify potentially suspicious activity after refund tax returns have been e-filed
- Provide lead reports that include authentication data elements and other relevant information to government and ISAC

Role of IRS

- Analyze industry return transmissions
- Identify overall trends and patterns
- Provide feedback to industry on lead reports
- Provide states with listings of taxpayers and preparers and other relevant info based on data from industry (via the PITRF files)

Role of States

- Send leads to IRS based on analysis of data received (SDT)
- Send lead report feedback to industry (SES)
- Request replacement lead reports by contacting the industry partner directly
- *Note*: states do not have the ability to send industry any data via SDT

Role of ISAC

- Information Sharing & Analysis Center
- Directed/administered by MITRE Corp.
- Forum for info sharing & ongoing collaboration
- Receives Lead Reports from Industry (conduit)
- Performs analysis and provides members with results directly using Accellion

What is the Conduit

- Industry sends Lead Reports to IRS via SDT
- A copy is sent to States and ISAC via SDT
- Copies are not opened by IRS and simply use SDT as a pass-thru
- Copies not considered FTI

Summit Files for States

- Industry Lead Reports
  - Suspicious Lead Files
  - From Industry to IRS, States and ISAC (conduit)
  - Weekly Jan-May, monthly June-Dec
  - Aggregated, anonymous reports (no PII); transmission ID number of e-filed refund returns
  - Patterns, trends, data elements that indicate suspicious activity

Summit Files for States

- Lead Report File Naming Convention
  - ######_STATE_LEADRPT_***_MMDDYYYY.txt *(1 file all)*
  - ####### = Industry Code assigned by IRS
  - STATE_LEADRPT = Lead Report (file description)
  - *** = sequence number (replacement, 2nd file same day)
  - *Variable prior to seq # indicates file type (C, E, X)*
  - If a specific file is sent to one agency only; the agency's SDT code replaces STATE in file name.
    - ######_SS###_LEADRPT_001_10152015.txt

Summit Files for States

- Lead Report File Name Examples
  - ######_STATE_LEADRPT_***_MMDDYYYY.txt
    - Same file all agencies
    - No variable before seq # indicates file format is text
  - ######_STATE_LEADRPT_E***_MMDDYYYY.txt
    - E=Excel format; also C=CSV, X=XML
  - Idaho Tax Comm asks Intuit for replacement file
    - INTUIT_ID182_LEADRPT_001_MMDDYYYY.txt

Summit Files for States

- PITRF files (Potential ID Theft & Refund Fraud)
  - From IRS to state agencies
  - Lists of *potential* ID Theft cases – daily & weekly
  - List of *confirmed* ID Theft cases – annual
  - Additional Information – distinguished by *sequence #* in file name

Summit Files for States

- PITRF File Names
  - PITRF***MMDDYYYY.txt *(same file all agencies)*
  - PITRF = file description
  - *** = sequence number
    - For PITRF files, the sequence # is used to provide a further description of the file content (see next slide)
  - If a specific file is sent to one agency only, the agency's SDT code is added after PITRF.
    - PITRFSS###***MMDDYYYY.txt

Summit Files for States

- PITRF Sequence Numbers (in file name)
  - 0** = daily file of potential ID theft (individual)
  - 1** = weekly file of potential ID theft (individual)
  - 2** = suspect email domains
  - 3** = annual individual/business confirmed ID theft
  - 4** = weekly file of potential ID theft (business)
  - 5** = likely compromised EFINs
  - 6** = miscellaneous (control file will further identify)
  - 7** = account verification (Green Dot pilot) – *New*

Summit Files for States

- PITRF 700 series – Pre-verification pilot with Green Dot Bank (GDB)
- Service allows for pre-verification of direct deposits to GDB accounts in real time
- Currently sharing info with 44 states and GDB
- Files going to states weekly since May 24
- Total of over 16,000 files thus far

Summit Files for States

- SUMMIT_MISCZ_XXXXXX_***_MMDDYYYY.zip
  - Miscellaneous Summit Information
  - Timing: Ad hoc
  - From IRS to Industry & States

What SDT is …

- A system that *moves files*
- A program used by IRS to exchange files with third parties electronically in a *secure*, automated environment over the Internet.
- The default method of file transfer used by IRS

** Analogy: SDT is the Delivery Service*

What SDT is *not* …

- A program that creates files
- A system that determines what data elements are included in a file
- The program that determines “where and when” files are delivered
- The system that determines a customer’s eligibility for a specific file

** Analogy: SDT is not the Retailer*

The UPS-SDT Analogy

- *UPS* delivers *JC Penney* merchandise to the correct address timely. But UPS doesn't look inside the package to make sure the contents are correct. JC Penney packs the order and determines where and when it gets delivered
- SDT delivers *IRS* merchandise (data) to the correct address timely. But SDT doesn't look inside the package (file) to make sure the contents are correct. The programmer packs the order and determines where and when it's delivered.

SDT Customer Support

- Primary: SDT Enterprise Help Desk
  - Issues related to actual transfer of file
  - Issues with system access & operation
  - Copy GL when sending email request
- Secondary: Local GL
  - File content
  - Spec book questions
  - Scheduling

Customer Support

Step 1: Create email w/subject line:
SDT Customer Support Request from SS###

Step 2: Include the following in the email:

- SDT Agency Code (SS###):
- State the question or describe the issue:
- IRS File Name (if applicable):
- Requestor's Name, phone number and email address:

Note to IRS ESD: Please attach this email to the KISAM ticket and assign to "EOPS-ECC-OSB-FTS-SDT"

Step 3: Send email to: **it-uns.enterprise.service.desk@irs.gov**
(copy your local GL)

SDT Connection Options

- There are a variety of client-protocol options available to connect to SDT
- Each customer's OS and configuration is unique and requires a unique solution
- IRS recommends Axway's SecureClient and provides it free of charge
- Need help? Submit a customer support request

User Authentication

- SDT uses digital certificates
  - Not transferrable
  - Two-year renewal requirement
- Two choices:
  - ACES certificate issued by Identrust
  - Self-generated certificate (SSH key pair)

User Authentication

ACES

- Cost: $119 for 2 years
- Download cert onto your device
- Export public key to IRS
- HTTPS protocol
- Faster download
- Renew key every 2 yrs.

Self-gen SSH key pair

- Cost: no cost
- Download cert onto your device
- Export public key to IRS
- SFTP protocol
- Slower download
- Renew key every 2 yrs.

- *Axway SecureClient uses both*

Questions

Rod Sterling
IRS Privacy, Gov't Liaison & Disclosure
Robert.J.Sterling@irs.gov