<redacted>
Demo Script Part 2 of 2
Version: 2
9 April 2015

Original

Script Version 1

RSA demo script – data exfiltration using a temporary account

It never fails, does it? Right in the middle of REM sleep, 3 AM, that high priority text message crashes your dreams. In this case, the alert informs our intrepid Security Admin of an event with a risk rating of 100 out of 100. This is as serious as it gets.

1. Security Admin receives a high priority alarm via email and/or text message with a risk rating of 100 out of 100
2. Security Admin logs into <redacted> Web UI
3. Security Admin jumps to the Alarms tab
4. Security Admin (SA) clicks on 100 Risk alarm (AIE: Compromise: Corroborated Account Anomalies)
    a. Alarm appears in Inspector
    b. SA points out that the Alarm Description describes a highly suspicious combination of 3 different anomalous types of behavior by the same user have all taken place within a 3 hour period.
    c. SA points out that this increases the risk rating because each event is already suspicious, and 3 different suspicious activities tied to the same user in a short time period is an almost certain attack
    d. Time to dig into the details – SA clicks on the Alarm drilldown icon

Within a few moments after login to the <redacted> Web UI, our Admin already secures an initial review: the details of a system compromise corroborating account anomalies. Three different anomalous behaviors occurred, tied to the same user. Considering the brief time-frame, this activity almost certainly indicates an attack.

5. Alarm drilldown reveals 3 different anomalous events – all tied to user steven.jacobs
    a. AIE: Account Anomaly: Temporary Account
    b. AIE: Account Anomaly: Abnormal Origin Location
    c. AIE: Account Anomaly: Abnormal File Access
6. SA decides there is enough there to open a Case
    a. Clicks New Case Button
    b. Names Case something like “Account steven.jacobs behaving suspiciously”
    c. Escalates to a P2 priority due to high probability of attack
    d. Assigns today’s date for resolution
    e. Adds a note describing the potential scenario
    f. Case created
    g. SA adds logs from the first investigation to the case

Those three events emerge: temporary account creation, associated with an abnormal origin location, involving abnormal file access. With this information in hand, our Admin opens a case.

7. SA jumps back to Alarms tab
    a. Selects all alarms that appeared in the investigation
    b. Adds all selected alarms to Case with on click of the case icon
8. SA jumps back to the Analyze view
    a. SA highlights the AIE: Account Anomaly: Abnormal File Access
    b. This seems like the most likely activity tied to the eventual target because it involves suspicious access of actual, specific data
    c. SA points out the AIE Drill Down as a one click method of investigating specific attack behavior

9. SA clicks AIE Drilldown
    a. Analyze tab opens with multiple Common Events - File Monitoring Event – Access
    b. User (Origin) is all <redacted>
    c. Jump to Application tab in mega grid
    d. Scroll to Object field to show Object field
    e. Multiple Object entries indicating financial projections are being accessed
        i. F:\Finance\Projected Earnings\Q4-2014-EMEA-Bookings.xlsx
        ii. F:\Finance\Projected Earnings\Q4-2014-NA-Bookings.xlsx
        iii. F:\Finance\Projected Earnings\Q4-2014-WW-Bookings.xlsx
    f. Jump to Host confirms that the user has logged into us-finsvr001 * (restricted access finance department server)
    g. Add Logs to Case with note about financial projections being accessed in the finance department server

Now with certainty, our Admin can act, skipping time lost to indecision. From that vantage point, with the knowledge this new case involves suspicious behavior, our Admin escalates to priority P2.

It's time to start gathering evidence. The case builds as our Admin adds logfiles associated with the initial investigation.

10. SA decides to dig into activity on this user as well as additional activity on the Host containing the sensitive data
    a. Click Pivot button on any User (Origin) – <redacted>
        i. In Pivot menu select User (Login or Account) to investigate what was done both *WITH* and *TO* the account
        ii. Select +Add To Search
    b. Click on Pivot button on Host (Origin) and +Add To Search
    c. Click on Search at the top right to expose Advanced Search
        i. SA wants to see *ALL* activity tied to <redacted> and *ALL* activity on us-finsvr001 to see the entire threat
        ii. SA changes “All of the following” qualifier to “Any of the following”
    d. SA clicks Search to run the investigation

There is confidence in knowing the best toolkit is at our Admin's fingertips, providing a full range of information. The case builds with the added alarms, but most importantly, the target of the intrusion is now identified: the suspicious access to actual, specific data.

11. SA opens the new Investigation and walks through the entire attack
    a. SA re-sorts Log Date to display info from oldest to newest
    b. Incident starts with Common Event – User Account Created
        i. Account was created by <redacted>
    c. User (Origin) <redacted> then modifies and enables the account
        i. Common Event - User Account Attribute Modified and
        ii. Common Event - Account Enabled
    d. SA then sees that <redacted> adds <redacted> to a

It only takes a single click to investigate the specific attack behavior.

Our Admin navigates to fields indicating the objects being

new group
    i. SA clicks on Common Event - Account Added To Group
    ii. SA scrolls down on Event & Actions details to the right
    iii. SA points out that <redacted> has been added to Group – Finance Group (a restricted group with privileged access to sensitive data)

accessed entail sensitive financial projects data.

e. SA then shows that <redacted> then logs into the Finance Department server
    i. Common Event – Authentication Activity
    ii. Host (Impacted) –

There's no room for imprecise, nebulous speculation when identifying the list of affected servers. <redacted> leaves nothing to guesswork as it confirms the exact servers accessed. Already, our Admin ticks off some vital questions as answered.

f. SA then points out that right after logging in, <redacted> accesses multiple financial projection spreadsheets
    i. Common Event – File Monitoring Event – Access
    ii. Object - F:\Finance\Projected Earnings\Q4-2014-…

g. SA points out the most concerning activity – Dropbox was accessed from the Fiance Department server at the same time
    i. Common Event – General Web Access
    ii. Jump to Application and scroll to URL
    iii. URL –

But it's time to turn our attention to the perpetrator. Who are you?

h. The suspicious account, <redacted> , then logs off
    i. Common Event - User Logoff
    ii. User (Origin) - <redacted> the

i. SA then shows that <redacted> has deleted the account
    i. Common Event – User Account Deleted
    ii. User (Origin) – <redacted>
    iii. User (Impacted) – <redacted>

<redacted>'s powerful Advanced Search cuts through the chatter to see all activity tied to the intruder and all activity on the financial servers. Our Admin secures a view of the entire threat.

j. SA adds logs to the Case and points out that this is a likely example of data exfiltration and requires escalation

12. SA clicks on Case to open Case View
    a. Adds Note about <redacted> creating steven.jacobs account to exfiltrate financial projections using dropbox
    b. Clicks lightning bolt to escalate incident
    c. Clicks Add Collaborator and adds a collaborator (this is the CISO…)
    d. Jumps to Assign Ownership and click Owner button next to the new account (acting CISO for this use case)
13. Incident has been detected, quickly investigated and escalated for resolution by the appropriate resource

After opening a new Investigation, our Admin walks

through the entire attack as it transpired. With a slight time jog, setting virtual feet onto this electronic trail, our Admin paces out the intrusion.

Chronologically, this replay exposes the intruder's creation of the account, modified and enabled. The account is added to a restricted group with privileged access to sensitive data. With this omniscient view, our Admin observes the intruder logging into the finance department server. On the server, the intruder accesses a number of financial projection spreadsheets.

More disconcerting than simple access to the spreadsheet is that the intruder simultaneously accesses an outside web storage site. Undoubtedly, the intruder transfers a copy of the spreadsheets to the storage site. With the theft complete, the intruder logs out and deletes the temporary account in an attempt to cover any trace of the intrusion.

The verdict: this is a clear case of data exfiltration and requires escalation. Initial alert to final escalation has transpired over a relatively short amount of time.

<redacted>
Demo Script Part 2 of 2
Version: 2
9 April 2015

With the powerful tools provided by <redacted>, the incident has been detected, investigated, and escalated for resolution by the appropriate resource. When an intrusion turns time into your enemy, <redacted> cuts time down to size.