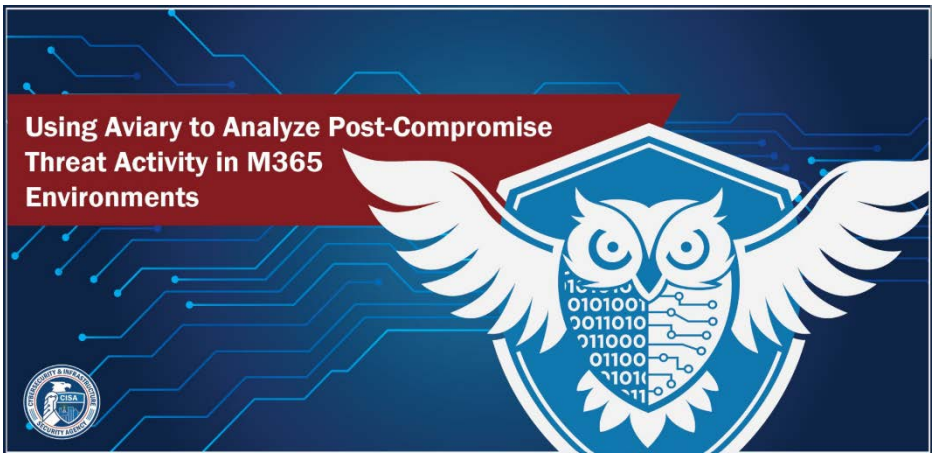
Railway Alert Network (RAN) Cybersecurity Advisory: CISA Releases Complement to Tool for Detecting Possible Compromised Accounts and Applications – Azure/M365 Environment

April 14, 2021

Executive Summary:

As of Thursday, April 8, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) announced **release of a new tool to complement the Sparrow detection capability issued in December 2020**.

The new tool, designated "**Aviary**," is intended **for use by information technology and cybersecurity staffs for more effective visualization and analysis of data produced by Sparrow**.



CISA developed to support hunting for threat activity in the **wake of widespread exploitation by a highly sophisticated illicit cyber actor of vulnerabilities in the SolarWinds Orion software supply chain**.

A third tool, made available as of March 21, 2021 – the **CISA Hunt and Incident Response Program (CHIRP) tool – scans for signs of advanced persistent threat (APT) compromise**.

- CHIRP searches specifically for indicators of compromise associated with malicious activity detailed in
  - CISA Activity Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations; and
  - CISA Activity Alert AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments. This Alert also addresses activity—irrespective of the initial access vector leveraged—that CISA attributes to an APT actor.
  - Watch the CISA video for using CHIRP: https://www.youtube.com/watch?v=UGYSNiNOpds

Please note: This message is intended to provide awareness of these tools developed by DHS/CISA, their purpose, and their intended usage. For troubleshooting, technical questions, and reporting of issues and concerns regarding performance, CISA has established a GitHub site at Sparrow GitHub.

Detailed Discussion:

Via a public announcement originally issued on Thursday April 8, the **Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) "released 'Aviary, a new companion resource to its existing Sparrow detection tool"** intended to help organizations – in government and industry – to **detect possible compromised accounts and applications in the Microsoft Azure Active Directory (AD), Office 365 (O365), and Microsoft 365 (M365) environments**.

Per an **accompanying notification issued by the United States Computer Emergency Response Team (US-CERT)**:

- "**Aviary** is a new dashboard that CISA and partners developed to **help visualize and analyze outputs from its Sparrow detection tool** released in December 2020."
- "Sparrow helps network defenders detect possible compromised accounts and applications in Azure/Microsoft O365 environments. **CISA created Sparrow to support hunts for threat activity following the SolarWinds compromise**."
- "Aviary – a Splunk-based dashboard – facilitates analysis of Sparrow data outputs."

The **Sparrow tool**:

- Checks and installs the required PowerShell modules on the machine to analyze;
- Then checks the unified audit log in Azure/M365 for certain indicators of compromise; and
- Lists Azure active directory (AD) domains and checks Azure service principals and their Microsoft Graph application programming interface (API) permissions to identify potential malicious activity.

Sparrow outputs the data into multiple CSV files that are located in the user's default home directory in a folder called 'ExportDir' (ie: Desktop/ExportDir). Informed by customer feedback on experience using Sparrow, **CISA has developed Aviary for use by information technology and cybersecurity staffs for more effective visualization and analysis of data produced by Sparrow**.

CISA encourages network defenders interested in using Aviary to facilitate analysis of output from Sparrow to review CISA Activity Alert: **AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments**.

- Please note that CISA has updated the Sparrow tool section in Activity Alert AA21-008A with instructions on using the Aviary tool. Key extracts follow:

Aviary is able to analyze the following sources from Sparrow:

- AppUpdate_Operations_Export.csv
- AppRoleAssignment_Operations_Export.csv
- Consent_Operations_Export.csv
- Domain_List.csv

- Domain_Operations_Export.csv
- FileItems_Operations_Export.csv
- MailItems_Operations_Export.csv
- PSLogin_Operations_Export.csv
- PSMailbox_Operations_Export.csv
- SAMLToken_Operations_Export.csv
- ServicePrincipal_Operations_Export.csv

Directions:

i. Ingest Sparrow logs (sourcetype=csv)
ii. Import Aviary .xml code into new Dashboard
iii. Point Aviary to Sparrow data using the index and host selection
iv. Review the output.

Alert (AA21-008A) Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments:

(Updated April 8, 2021): CISA has created "Aviary," which is a companion Splunk dashboard that can assist in visualizing and reviewing the output of Sparrow. Network defenders can find Aviary on **CISA's Sparrow GitHub page**. CISA advises network defenders to perform the following actions to use Sparrow: **Technical Details**.

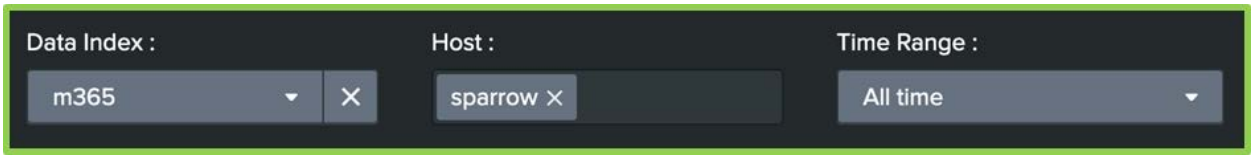
1. Use Sparrow to detect any recent domain authentication or federation modifications.
2. Examine logs for new and modified credentials applied to applications and service principals; delineate for the credential type. Sparrow can be used to detect the modification of service principals and application credentials.
3. Use Sparrow to detect privilege escalation, such as adding a service principal, user, or group to a privileged role.
4. Use Sparrow to detect **OAuth** consent and users' consent to applications, which is useful for interpreting changes in adversary tactics, techniques, and procedures (TTPs).
5. Use Sparrow to identify anomalous Security Assertion Markup Language (SAML) token sign-ins by pivoting on the unified audit log UserAuthenticationValue of 16457, which is an indicator of how a SAML token was built and a potential indicator for forged SAML tokens.
6. Review the PowerShell logs that Sparrow exports.
7. Use Sparrow to check the Graph API application permissions of all service principals and applications in M365/Azure AD.
8. Review Sparrow's listed tenant's Azure AD domains, to see if the domains have been modified.
9. For customers with G5 or E5 licensing levels, review MailItemsAccessed for insight into what application identification (ID) was used for accessing users' mailboxes. Use Sparrow to query for a specific application ID using the application identification (app id) investigation capability, which will check to see if it is accessing mail or file items.

(Updated April 8, 2021): Aviary can be used to assist with performing the above tasks. To install Aviary, after running Sparrow:

1. Ingest comma separated values (CSV) output from the Sparrow PowerShell script into Splunk.
    a. Sparrow output will have the following default filenames, which should not be modified:

       AppUpdate_Operations_Export.csv, AppRoleAssignment_Operations_Export.csv, Consent_Operations_Export.csv, Domain_List.csv, Domain_Operations_Export.csv, FileItems_Operations_Export.csv, MailItems_Operations_Export.csv, PSLogin_Operations_Export.csv, PSMailbox_Operations_Export.csv, SAMLToken_Operations_Export.csv, and ServicePrincipal_Operations_Export.csv

2. Copy and paste the contents of the .xml file (aviary.xml in the root directory) into a new dashboard.
3. Use the data selection filters to point to the indexed Sparrow data (see figure 1)



Data Selection Filters

A **third capability developed and issued by CISA** that merits attention is the **CISA Hunt and Incident Response Program (CHIRP) tool**, which the agency **released as of March 21, 2021**.

- This **Python-based tool** enables **detection of malicious activity associated with the SolarWinds hackers in compromised on-premises enterprise Microsoft Windows environments**.

CHIRP scans for signs of advanced persistent threat (APT) compromise – which are commonly associated with active involvement or sponsorship and support by nation-state actors – **within an on-premises environment**. By default, the CHIRP tool searches for **indicators of compromise associated with malicious activity detailed in CISA Activity Alerts AA20-352A and AA21-008A**.

- **AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations**: Focuses primarily on an APT actor's compromise of SolarWinds Orion products and exploitation affecting federal government agencies, critical infrastructure entities, and private network organizations.
- **AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments**: Addresses APT activity within Microsoft 365/Azure environments and

offers an overview of, and guidance on, available open-source tools. The Alert includes the CISA-developed Sparrow tool that helps network defenders detect possible compromised accounts and applications in the Microsoft Azure Active Directory (AD), Office 365 (O365), and Microsoft 365 (M365) environments.

Further, **CHIRP**:

- **Examines Microsoft Windows event logs** for artifacts associated with this illicit activity;
- **Scans Windows Registry** for evidence of intrusion;
- **Queries Windows network artifacts**; and
- **Applies YARA rules** to **detect malware, backdoors, or implants**.

In its public statement issued on release of this capability, DHS emphasized, "The CISA Hunt and Incident Response Program (CHIRP) is a tool created to dynamically query Indicators of Compromise (IoCs) on hosts with a single package, outputting data in a JSON format for further analysis in a SIEM or other tool. CHIRP does not modify any system data."

Currently, **CHIRP scans for**:

- The **presence of malware** identified by security researchers as **TEARDROP** and **RAINDROP**;
- **Credential dumping certificate pulls**;
- **Certain persistence mechanisms** identified as associated with this campaign;
- **System, network, and M365 enumeration**; and
- **Known, observable indicators of lateral movement**.

As additional relevant references, CISA recommends:

- Remediating Networks Affected by the SolarWinds and Active Directory/M365
- Supply Chain Compromise

Updates will follow as additional information is provided by CISA, the Federal Bureau of Investigation (FBI), and other reliable sources.

Distribution:

Please feel free to disseminate this message, and to use all or portions of its content, widely to inform cyber security awareness throughout your respective railroads and industry organizations.

You may also share this information with contracted information technology and cyber security support, customers, colleagues in local and State law enforcement, State fusion centers, and Federal security and law enforcement agencies.

Association of American Railroads
Railway Alert Network (RAN)
425 3rd Street, SW
Washington, DC 20024
202-639-2910 Emergency
866-494-4353 "
202-639-2950 Non-Emergency