Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool

us-cert.cisa.gov/ncas/alerts/aa21-077a

Summary

Updated April 15, 2021: The U.S. Government attributes this activity to the Russian Foreign Intelligence Service (SVR). Additional information may be found in a statement from the White House. For more information on SolarWinds-related activity, go to https://us-cert.cisa.gov/remediating-apt-compromised-networks and https://www.cisa.gov/supply-chain-compromise.

This Alert announces the CISA Hunt and Incident Response Program (CHIRP) tool. CHIRP is a forensics collection tool that CISA developed to help network defenders find indicators of compromise (IOCs) associated with activity detailed in the following CISA Alerts:

> AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, which primarily focuses on an advanced persistent threat (APT) actor's compromise of SolarWinds Orion products affecting U.S. government agencies, critical infrastructure entities, and private network organizations.
>
> AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments, which 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 Azure/M365 environment.

Similar to Sparrow—which scans for signs of APT compromise within an M365 or Azure environment—CHIRP scans for signs of APT compromise within an on-premises environment.

In this release, CHIRP, by default, searches for IOCs associated with malicious activity detailed in AA20-352A and AA21-008A that has spilled into an on-premises enterprise environment.

CHIRP is freely available on the CISA GitHub Repository. For additional guidance watch CISA's CHIRP Overview video. **Note:** CISA will continue to release plugins and IOC packages for new threats via the CISA GitHub Repository.

CISA advises organizations to use CHIRP to:

- Examine Windows event logs for artifacts associated with this activity;

- Examine Windows Registry for evidence of intrusion;
- Query Windows network artifacts; and
- Apply YARA rules to detect malware, backdoors, or implants.

Network defenders should review and confirm any post-compromise threat activity detected by the tool. CISA has provided confidence scores for each IOC and YARA rule included with CHIRP's release. For confirmed positive hits, CISA recommends collecting a forensic image of the relevant system(s) and conducting a forensic analysis on the system(s).

If an organization does not have the capability to follow the guidance in this Alert, consider soliciting third-party IT security support. **Note**: Responding to confirmed positive hits is essential to evict an adversary from a compromised network.

Click here for a PDF version of this report.

Technical Details

How CHIRP Works

CHIRP is a command-line executable with a dynamic plugin and indicator system to search for signs of compromise. CHIRP has plugins to search through event logs and registry keys and run YARA rules to scan for signs of APT tactics, techniques, and procedures. CHIRP also has a YAML file that contains a list of IOCs that CISA associates with the malware and APT activity detailed in CISA Alerts AA20-352A and AA21-008A.

Currently, the tool looks 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.

Network defenders can follow step-by-step instructions on the CISA CHIRP GitHub repository to add additional IOCs, YARA rules, or plugins to CHIRP to search for post-compromise threat activity related to the SolarWinds Orion supply chain compromise or new threat activity.

Compatibility

CHIRP currently only scans Windows operating systems.

Instructions

CHIRP is available on CISA's GitHub repository in two forms:

1. A compiled executable
2. A python script

CISA recommends using the compiled version to easily scan a system for APT activity. For instructions to run, read the README.md in the CHIRP GitHub repository.

If you choose to use the native Python version, see the detailed instructions on the CHIRP GitHub repository.

Mitigations

Interpreting the Results

CHIRP provides results of its scan in JSON format. CISA encourages uploading the results into a security information and event management (SIEM) system, if available. If no SIEM system is available, results can be viewed in a compatible web browser or text editor. If CHIRP detects any post-compromise threat activity, those detections should be reviewed and confirmed. CISA has provided confidence scores for each IOC and YARA rule included with CHIRP's release. For confirmed positive hits, CISA recommends collecting a forensic image of the relevant system(s) and conducting a forensic analysis on the system(s).

If you do not have the capability to follow the guidance in this Alert, consider soliciting third-party IT security support. **Note:** Responding to confirmed positive hits is essential to evict an adversary from a compromised network.

Frequently Asked Questions

1. **What systems should CHIRP run on?**
   Systems running SolarWinds Orion or believed to be involved in any resulting lateral movement.
2. **What should I do with results?**
   Ingest the JSON results into a SIEM system, web browser, or text editor.
3. **Are there existing tools that CHIRP complements and/or provide the same benefit as CHIRP?**
    1. Antivirus software developers may have begun to roll out detections for the SolarWinds post-compromise activity. However, those products can miss historical signs of compromise. CHIRP can provide a complementary benefit to antivirus when run.
    2. CISA previously released the Sparrow tool that scans for APT activity within M365 and Azure environments related to activity detailed in CISA Alerts AA20-352A and AA21-008A. CHIRP provides a complementary capability to Sparrow by scanning for on-premises systems for similar activity.

4. **How often should I run CHIRP?**
   CHIRP can be run once or routinely. Currently, CHIRP does not provide a mechanism to run repeatedly in its native format.

5. **Do I need to configure the tool before I run it?**
   No.

6. **Will CHIRP change or affect anything on the system(s) it runs on?**
   No, CHIRP only scans the system(s) it runs on and makes no active changes.

7. **How long will it take to run CHIRP?**
   CHIRP will complete its scan in approximately 1 to 2 hours. Duration will be dependent on the level of activity, the system, and the size of the resident data sets. CHIRP will provide periodic progress updates as it runs.

8. **If I have questions, who do I contact?**
   For general questions regarding CHIRP, please contact CISA via email at central@cisa.dhs.gov or by phone at 1-888-282-0870. For reporting indicators of potential compromise, contact us by submitting a report through our website at https://us-cert.cisa.gov/report. For all technical issues or support for CHIRP, please submit issues at the CISA CHIRP GitHub Repository.

Revisions

March 18, 2021: Initial Publication

April 9, 2021: Fixed PDF (not related to content)

April 15, 2021: Updated with Attribution Statement

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.