# Identifying UNC2452-Related Techniques for ATT&CK

By Matt Malone

Published: 2022-04-27 · Archived: 2026-04-05 13:12:07 UTC

By

(MITRE), (MITRE), (MITRE), and (MITRE)

Last updated 27 April 2022 12:00pm EDT

Reporting regarding activity related to the SolarWinds supply chain injection has grown quickly since initial disclosure on 13 December 2020. A significant amount of press reporting has focused on the identification of the actor(s) involved, victim organizations, possible campaign timeline, and potential impact. The US Government and cyber community have also provided detailed information on how the campaign was likely conducted and some of the malware used.

MITRE's ATT&CK team — with the assistance of contributors — has been mapping techniques used by the actor group, referred to as UNC2452/Dark Halo by FireEye and Volexity respectively and more recently attributed to the existing APT29/Cozy Bear/The Dukes threat group by Mandiant, and members of the US Intelligence Community, as well as SUNBURST, SUNSPOT, Raindrop, and TEARDROP malware. We have now published a point release to ATT&CK, v8.2, with the information we've mapped and new techniques we've spotted so far.

It's also been difficult keeping up with all the reporting and updates while trying to track down descriptions of adversary behavior, particularly as we're looking for direct analysis of intrusion data rather than derivative reporting. We were originally listing reports we were tracking in this blog post itself, but have moved our tracking to a GitHub repository and are continuing to update that in partnership with MITRE Engenuity's Center for Threat-Informed Defense.

## Get Matt Malone's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

A key challenge mapping current reporting is that the actor used a number of behaviors not currently described by ATT&CK Enterprise or Cloud techniques. We have added new techniques, sub-techniques, and expansions of scope on existing content to improve this coverage and wanted to describe what's new in ATT&CK in v8.2.

## UNC2452 Technique Analysis

**First and foremost, we would like to thank the individuals and teams responsible for analyzing, publishing, and/or contributing invaluable information to help the community react and respond to this incident.** This wealth of publicly available intelligence has described many behaviors performed by the threat actor identified as *UNC2452/Dark Halo/SolarStorm*. Mapping these behaviors to ATT&CK, we see a combination of very commonly used techniques (such as *T1059 Command and Scripting Interpreter*, *T1105 Ingress Tool Transfer*, and *T1218 Signed Binary Proxy Execution*) as well others that are less often disclosed in public reporting (ex: *T1195 Supply Chain Compromise*). You can see the techniques we currently have mapped in the ATT&CK Navigator here, or grab the Navigator layer file from our repository here.

Press enter or click to view image in full size

Techniques used by UNC across multiple reports.

Several behaviors were identified that weren't previously explicitly captured within existing techniques. We have now released updates that include:

- **New procedural example variations of techniques**, such as *T1070 Indicator Removal on Host* including UNC2452 reverting changes to legitimate utilities and tasks after abuse and *T1098.002 Account Manipulation: Exchange Email Delegate Permissions* including them granting additional permissions to the target Application or Service Principal to read mail content from Exchange Online via Microsoft Graph or Outlook REST
- **Expansion of current technique scoping**, such as the *T1098.001 Account Manipulation: Additional Cloud Credentials* description being amended to include adding credentials to legitimate OAuth Applications as well as Service Principals in Azure AD
- **New (sub-)techniques not previously published within ATT&CK**, such as those necessary to describe UNC2452 forging web cookies (*T1606.001 Forge Web Credentials: Web Cookies*) and SAML tokens (*T1606.002 Forge Web Credentials: SAML Tokens*) via stolen secret keys and compromised signing certificates (*T1552.004 Unsecured Credentials: Private Keys*) and making malicious modifications to domain federation trust settings to include adversary owned objects (*T1484.002 Domain Policy Modification: Domain Trust Modification*)

## New Group/Software Entries

Along with new/updated techniques we have added several new group and software entries to ATT&CK including:

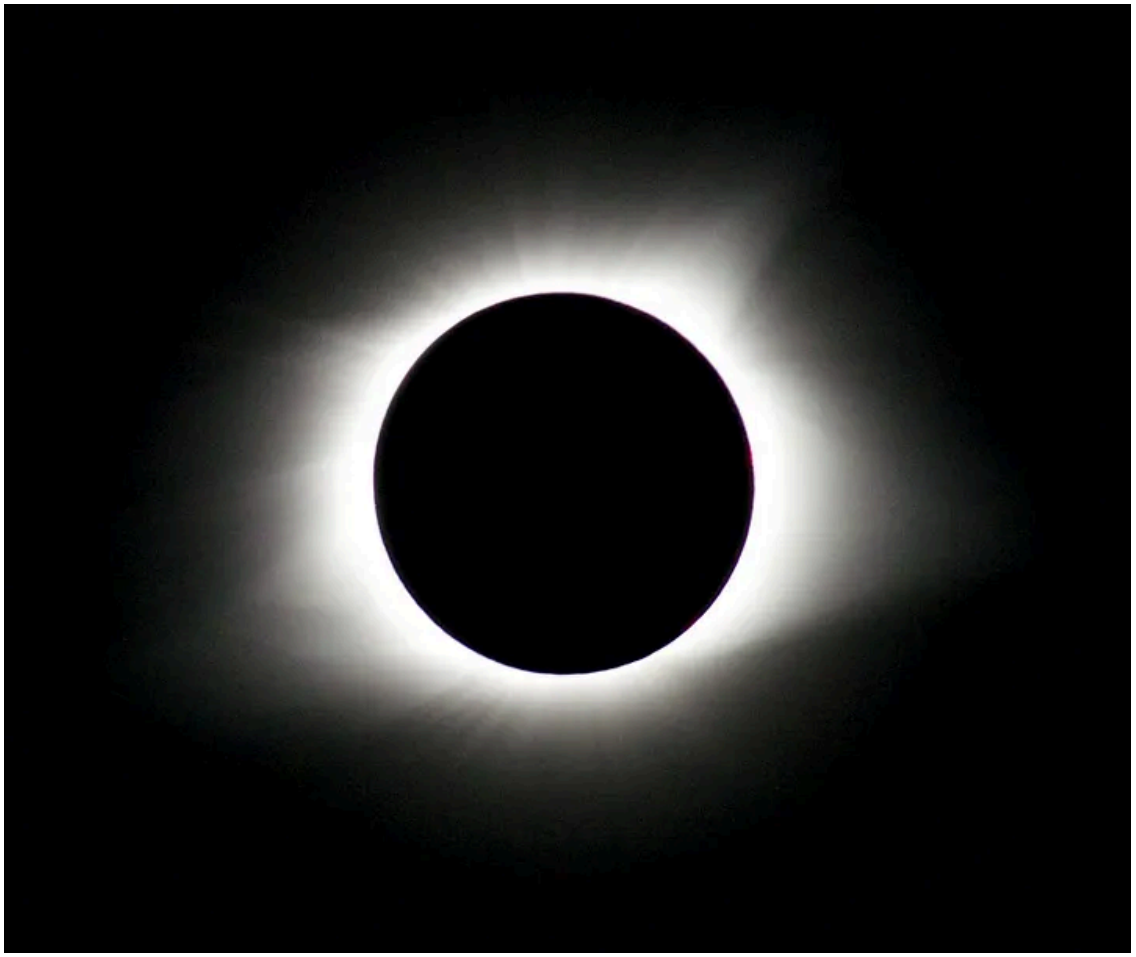
- **A new group representing the threat group responsible for the intrusions**, added as UNC2452 with associated group names of Solorigate, StellarParticle and Dark Halo.
- **New malware first spotted in this intrusion**, including Sunburst, Teardrop, Sunspot, and Raindrop.
- **An existing tool used in this intrusion**, AdFind.

## More to Come?

We don't expect to add more content to ATT&CK itself before our next major release (announced as planned for April 2021 in our recent State of the ATT&CK), but anticipate that more reporting on this intrusion will continue to be released. We will be continuing to watch and add reporting to our public report tracking, as well as any new techniques or software that appear to the next release of ATT&CK.

If you see a technique we're missing from existing reporting, a report with unique information that we're missing out on, or want to share a mapping of a new report you've done, please reach out to us at attack@mitre.org.

Press enter or click to view image in full size



---