

Identifying UNC2452-Related Techniques for ATT&CK

 medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714

Matt Malone

April 27, 2022



Matt Malone

Dec 22, 2020

.

4 min read

By Matt Malone (MITRE), Jamie Williams (MITRE), Jen Burns (MITRE), and Adam Pennington (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.

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 , , and) as well others that are less often disclosed in public reporting (ex:). 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](#).

The image shows a grid of ATT&CK techniques mapped to the UNC2452 threat actor. The grid is organized into columns representing ATT&CK categories: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. Each cell in the grid contains one or more technique names, some of which are highlighted in red to indicate they are mapped to the threat actor's behavior. For example, in the 'Initial Access' column, techniques like 'Valid Accounts' and 'Valid Accounts' are highlighted. In the 'Persistence' column, 'Valid Accounts' and 'Valid Accounts' are also highlighted. The grid is a comprehensive mapping of the threat actor's activities to the ATT&CK framework.

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:

- , such as including UNC2452 and including them
- , such as the description being amended to include in Azure AD
- , such as those necessary to describe UNC2452 forging () and () via stolen secret keys and compromised signing certificates () and making ()

New Group/Software Entries

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

- , added as with associated group names of Solorigate, StellarParticle and Dark Halo.
- , including , , , and .
- , .

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.



©2020-2021 The MITRE Corporation. ALL RIGHTS RESERVED Approved for public release. Distribution unlimited 20-00841-22.