
DARK
HALO
AXIAL

A SURVEY ON DARK HALO: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

Dark Halo is also known as SolarStorm and UNC2452 is a relatively new threat group emerging from Russia. They have been seen being active since late 2019 and are motivated by Information Theft and Cyber-Espionage. Volexity tracked this threat actor since 2019 when it was found with few tools but in December 2020 it was revealed that they were the ones behind the Solar Winds supply chain hack.

II. TARGET SECTORS

The primary goal of the Dark Halo was to obtain the e-mails of specific individuals at the think tank. This included a handful of select executives, policy experts, and the IT staff at the organization.

III. METHODS USED

In most cases, the actor aimed to live off the land, primarily focusing on operations to extract e-mails from the organization. Dark Halo did use malware and red-teaming tools but largely only for specific one-time tasks as a fallback mechanism when other avenues of access were cut off.

IV. OPERATIONS

- In late 2019, Volexity found multiple tools, backdoors, and malware implants that had allowed the attacker to remain undetected for several years in the Think Tanks network.
- Early 2020, Dark Halo exploited a vulnerability in the Think Tank's Microsoft Exchange Control Panel. Near the end of this incident, Volexity observed the threat actor using a novel technique to bypass Duo multi-factor authentication (MFA) to access the mailbox of a user via the organization's Outlook Web App (OWA) service.
- December 2020, FireEye released a statement saying that they had been breached. Subsequent Investigations by FireEye and Microsoft revealed the threat actor breached the organization through its SolarWinds Orion software in June 2020 and has been actively exploiting it since March 2020 in other organizations. This led to the largest supply chain hack of 2020 affecting Solar Winds 18k of 300k Customer Base.

AX1AL

V. IOC

SHA256

- 019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134 (Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll))
- 292327e5c94afa352cc5a02ca273df543f2020d0e76368ff96c84f4e90778712 (Mal/Generic-S(OrionImprovementBusinessLayer.2.cs))
- 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77 (Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll))
- 53f8dfc65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7 (Mal/Generic-S(Solarwinds Worldwide LLC))
- ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6 (Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll))
- d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600 (Troj/SunBurst-A(Installer|CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp))
- a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc (SolarWinds.Orion.Core.BusinessLayer.dll)
- d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af (SolarWinds.Orion.Core.BusinessLayer.dll)
- ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
- c09040d35630d75dfef0f804f320f8b3d16a4810710769l8e9b236a321c1ea77
- dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
- eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
- b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07
- 1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
- 118189f90da3788362fe85eafa555298423e21ec37f147f3bf88c61d4cd46c51
- 6e4050c6a2d2e5e49606d96dd2922da480f2e0c70082cc7e54449a7dc0d20f8d
- c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71 (Mal/Sunburst-B(app_web_logoimagehandler.ashx.b6031896.dll).SuperNova webshell backdoor)

DOMAINS

1. avsvmcloud[.]com
2. deftsecurity[.]com
3. digitalcollege[.]com
4. digitalcollege[.]org
5. freescanonline[.]com
6. globalnetworkissues[.]com
7. seobundlekit[.]com
8. solartrackingsystem[.]net
9. thedoccloud[.]com
10. virtualwebdata[.]com
11. websitetheme[.]com

1. highdatabase[.]com
2. panhardware[.]com
3. zupertech[.]com
4. |computers[.]com
5. webcodez[.]com
6. kubecloud[.]com
7. incomeupdate[.]com
8. databasegalore[.]com

VII. REFERENCES

- https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/
- https://github.com/fireeye/sunburst_countermeasures
- https://blog.cyberint.com/solarwinds-supply-chain-attack