January 13th, 2020

Industry Security Bulletin

Shining Light on “SolarLeaks”

Cyberint

INTRODUCTION

In the aftermath of the notorious SolarWinds breach, occurring in mid-December 2020, a nefarious website was observed on 12 January 2021 and, presumably linked to the threat actors involved in the original supply chain attacks, purports to offer stolen data from four victim companies for sale:

- Cisco - Source code for multiple products and an alleged 'bug tracker' dump;
- FireEye - Red Team tools, source code, binaries and documentation;
- Microsoft - Proprietary source code;
- SolarWinds - Product source code (including Orion) and a customer portal dump.

Other than the above, no file listings, screenshots or detailed 'proof' have been provided although links to four encrypted archive files, one for each potential victim organization, were uploaded to the popular filesharing service 'Mega', since taken down, as well as being hosted on the 'leak' domain itself.

Given that the files appear to be encoded with asymmetric encryption, it is not possible to validate the authenticity of the alleged leaks. In addition, the price requested by the attackers, a total of $1,000,000, adds to suspicion and speculation by numerous researchers to suggest that these files are in fact not valid and an attempt to defraud any would-be purchaser.

Furthermore, the email contact email address provided on the leak domain does not appear to exist at this time, potentially due to the webmail host ProtonMail taking it down, further adding to speculation about the mystery.

Notably, Cyberint Research were able to acquire the 'encrypted' files in question and will continue to monitor the situation to determine if a true data theft/leak threat is present.

LEAK WEBSITE

Seemingly first announced on Reddit at 1716hrs GMT on 12 January 2021 within the SolarWinds subreddit, `r/Solarwinds`, a user named `u/solarleaks` posted a message, since removed, claiming to have SolarWinds' data for sale along with a link to the `solarleaks[.]net` website (Figure 1).

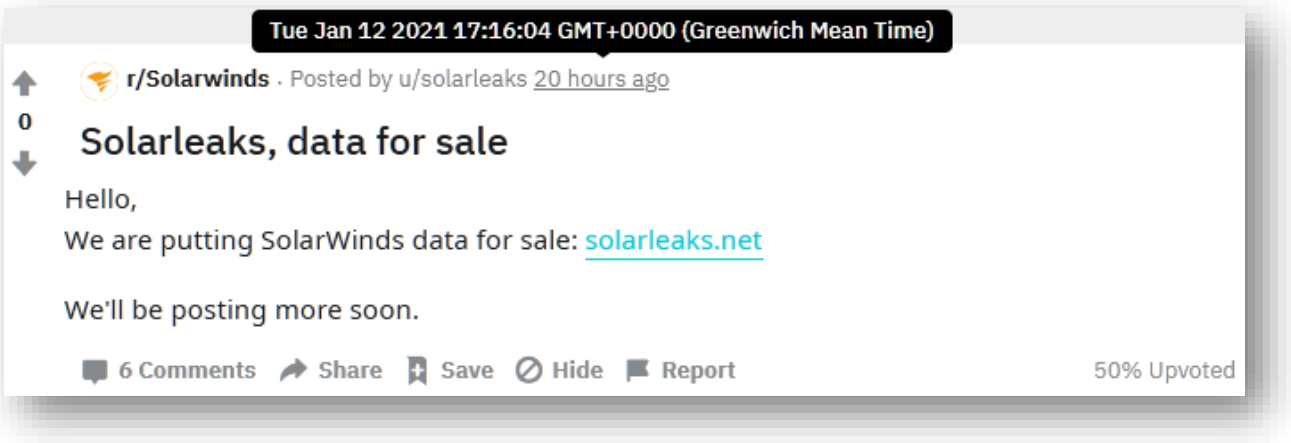


Figure 1 - *SolarWinds leak announcement on Reddit*

This Reddit post appears to have been made one hour after the conclusion of the leak website being configured, as determined by the last modified timestamps of the site content being between `1316hrs` and `1616hrs` on `12 January 2021.`

For reference, a full copy of the text, including download links, is provided in Appendix A.

Based on the location of this post, and the identifiers used, such as username and domain name, it is implied that access to this data was as a result of the recent SolarWinds critical vulnerability [1] and subsequent supply chain attack [2].

In order to protect the identity of those behind this supposed leak, the domain appears to be registered through `'Njalla'`, a privacy-aware service that accepts payment using common cryptocurrencies and has previously been favored by Russian-nexus threat actors.

In addition to making use of their domain registration service, the website appeared to be hosted on a Njalla VPS resolving to the IP address `185.193.126[.]236`

Somewhat amusingly, the use of this service, and their privacy mantra, can be seen when reviewing the name servers that include the 'you can get no info' message within their host names:

- `1-you.njalla[.]no`
- `2-can.njalla[.]in`
- `3-get.njalla[.]fo`

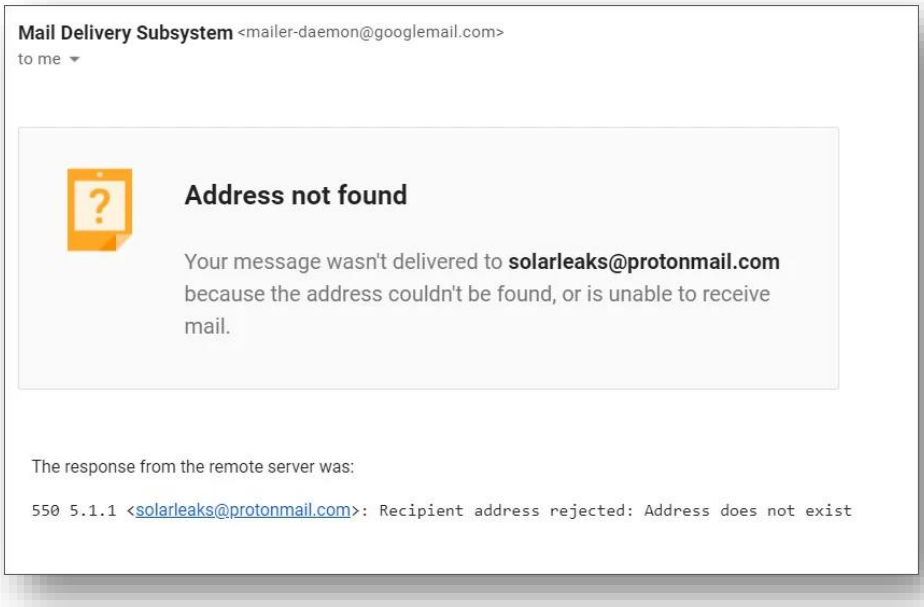
THREAT ACTOR EMAIL

Parties interested in purchasing these alleged data leaks are encouraged to contact the threat actor via email, `solarleaks[@]protonmail.com`, and a PGP public key has been provided to facilitate the use of encryption in these communications.

CONCLUSIONS

Whilst many have speculated that this may be the work of a Russian-nexus threat actor, others have suggested that the timing, following a recent US law enforcement statement [3], may simply be an attempt to take advantage of interest in this incident, either for fraudulent financial gain or to imply further responsibility on a foreign nation-state.

As such, Cyberint Research will continue to monitor the situation to determine if the content is indeed valid and what, if any, threat it poses to the victim organizations and others.



INDICATORS OF COMPROMISE

Whilst not strictly indicators of compromise (IOC), the following network and file artefacts relate to this bulletin.

DOMAINS:

- Solarleaks[.]net

IP'S:

- 185.193.126.236

FILES:

- 4289A4E60B97CFBA370838E68A06B7FAABC45BC8960C990B8AF63606F7C419DF
- FEE8AFA1081FFFE6543CF0E82DE05FDC4ECA4E148AAC98D074BC4AA1532D47BF
- FBFCE5FD66DDE0AA94D39BA5F271E0B52B618EDC63328B0CFCBF6709CAF185DB
- 9AA822193900D67FCF240E6AF8A8B7C296EF006C0386766AEBD7DE4D72F243CF

EMAIL ADDRESSES:

- Solarleaks[@]protonmail.com

CERTIFICATES:

- Digital message signature:

```
1. -----BEGIN PGP SIGNATURE-----
   iQEzBAEBCAAdFiEEJFFsLhzHiQgydxF44sc7xTuRGKAFAl/9yCsACgkQ4sc7xTuR
   GKC/NwgAk/KZ9id9++Fi68M10rzd9uiC2DKTEX+qgJ9kEIASIvB/vh1uaS/mRZnj
   GHf7I8D69zyI6FYlbndDN3DH6VUA21gD2dYxj7q79RpERQwV4PAO0iYRFBp0e3ho
   nezYmVMMxB1GSsd+6AcdybLRJ1dmeIDB/mWnNa4S0jf45IkIw8/6j5965QxKlXBb
   QlUShGTNom60BgpUOq7ud1ocH8c+HXbQdZpJ2LCq+CrQ+KuktMCsKUc1uydvTfDH
   9zyjUtb3H9TC+zVugN3ANhtjDq0cIdOJQQ4vaGhnvLnXIDMvNQ1B4wxK+Ij50M8u
   HD6LF0GUszJaNBdKylQaPV78sGqu3Q== =HjXU -----END PGP SIGNATURE-----
```

- E2C73BC53B9118A0

- ProtonMail Public Key for 'solarleaks@protonmail.com':

```
1. -----BEGIN PGP PUBLIC KEY BLOCK-----
   Version: ProtonMail

   xsBNBF/8svcBCADDHEB5KheF4UAJjbnTYyXRPC6C9Ozg8ToM0v3VgyDMrE/w
   F1Ifce0vyeC3OPIJsxfAoUzTZeBtFs5+DgbwqokG74il64wiMdlZdGFb2O2j
   T1OP+u/dxlWovZ7WxW/qXRC9eIyoR7g4a4DkJdS7H4g7Ik/dw/AgpIoJo5PS
   psizo1jVQrZMiO3kUQ2ARe4z1rB9TmL1LTrnEuWTPSBUMge7Xs579e51zciq
   iUZGGH5mJ7bgI42TYN8YCBk14lAgbSGrBc72NJ/GVjyLm+VwRUsXNEwnXW+p
   1pXFXpLbQ0x1OOer2xKQmg2LF61QZ5idBfyKc7nDffAsRXvAXMmz05+VABEB
   AAHNNXNvbGFybGVha3NAcHJvdG9ubWFpbC5jb20gPHNvbGFybGVha3NAcHJv
   dG9ubWFpbC5jb20+wsCNBBABCAAgBQJf/LL3BgsJBwgDAgQVCAoCBBYCAQAC
   GQECGwMCHgEAIQkQI3hckdtLCoUWIQQQtBK9rWvlMkxyYL4jeFyR20sKhUxu
   B/4zd094KDSU76pIxuM3WBob/CV1j3lyxWGDuy1PzJMx6PUC4GUH24CUMzqX
   gZy9e2bvGHPDmX4JEeHlsqXRIBZvMPfTydcEuJ6x0UmLBVQzFInGRX6m3RP6
   RoPMyAEEqul6+iwf/AedSxDceYVac01jFPv1I7c1EN6sWFoQeuY1VrjD++wT
   dwsJot3s2FYQniihXGCPND1tP6XkdHf3TdVASUV6Ymb3l42366LEq1vgEv0A
   qRgA6rREAA1jdyN6p23udiys7DvAgnaeqSowPQGvXFa+acDGzFLAmlMRQovR
   srh1h3yQr5UyFVjHkP87LQCksCIBsJ4i6bAe9u3V0i+1zsBNBF/8svcBCAC0
   +CBi4ddBmQSQALF1g29p14OJZyNCOEJdznU6DNuevLu6AR4zAX/uF93gIs2T
   AbH5Y7vhDG3mr89x1d6jzsS1HKV7mPMjv2mohbg2nrKhrSLLZD87+bhfp81Y
   KrzJxWm1Lip1XOWfr7tY3NboK3uSu13DrDhBgbHSy4QRYjQhy80UX7Jg2osk
   y3yvnfzW38+SED26H4Hlt80XZB5Ju1qVRpDpdEvAApjtszH1jOVi7O1pkwX9
   seHy7W1uc+fsJt9IS3HdIMMlErAhuQ6SVt6hJHGcBppNxppaaVH8UP0/V3RS
   k/NL1xh5LR92wW2pjBXZZfHVGOP7bhVU8ylGgRvVABEBAAHCwHYEGAEIAAkF
   Al/8svcCGwwAIQkQI3hckdtLCoUWIQQQtBK9rWvlMkxyYL4jeFyR20sKhUWv
   B/wL3NJhznm7tQG+50AyLGc9b2fVQoMFba9j+6X4rpomlFTGnaI8nMR3cYr4
   qW62mQ0s7S2Ah8TjKJIJTzhRz5DTMbyQo3deSfSk2Airazdt+0WcsFzTZBUu
   5UVtVLDXA+t5NztYM/EK9+Gny90pmcVIcJ0+uCtxDUMrwOZ/reuSU+44C0FN
   NVl/QMpx3Qlh67NTz2kurL+MdQdZam14B9M96LQT+zICK8oM4CdI5ENOkqoC
   MDKjX0/pKDgGzFDRnn3WvqXCw6QPY6pbO8nrghUXX5WH3k01v8oRFBWPZFMY
   UHRLYILrz9o/l3SkNQfY1gkaaCsTpCk0j26u2kZN33dK =SXk0

   -----END PGP PUBLIC KEY BLOCK-----
```

APPENDIX A: WEBSITE CONTENT

The following text is as it appeared on the 'leak' website as of 12 January 2020:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Happy new year!
Welcome to solarleaks.net (mirror:
5bpasg2kotxllmzsv6swwydbojnfuvfb7d6363pwe5wrzhjyn2ptvdqd.onion)

We are putting data found during our recent adventure for sale.

[Microsoft Windows (partial) source code and various Microsoft
repositories]
 price: 600,000 USD
 data: msft.tgz.enc (2.6G)
 link: https://mega.nz/file/1ehgSSpD#nrtzQwh-
qyCaUHBXo2qQ1dNbWiyVHCvg8J0As8VjrX0

 [Cisco multiple products source code + internal bugtracker dump]
 price: 500,000 USD
 data: csco.tgz.enc (1.7G)
 link: https://mega.nz/file/sSgQmJLT#NqaaYXsFkASwAc51lcjBnWjP4zrbqiN-
XQ7GVZGbL_o

 [SolarWinds products source code (all including Orion) + customer portal
dump]
 price: 250,000 USD
 data: swi.tgz.enc (612M)
 link: https://mega.nz/file/xawhBQgJ#f3X6lPORF16wh-
O9GiNVMVDZ6rxRKX64_XVR5y9KpFM

 [FireEye private redteam tools, source code, binaries and documentation]
 price: 50,000 USD
 data: feye.tgz.enc (39M)
 link:
https://mega.nz/file/hOBnVYjL#l3qojAvaFWtYtcB3vX4ZABG3tBLGyhJarBBbYaHnM-0

 [More to come in the next weeks]

 ALL LEAKED DATA FOR 1,000,000 USD (+ bonus)

 Data is encrypted with strong key.
 Serious buyers only: solarleaks@protonmail.com

 - -
 Q: Is this really happening? Can you provide proof?
 A: Yes and yes.

 Q: Why no more details?
 A: We aren't fully done yet and we want to preserve the most of our
current access. Consider this a first batch.

 Q: I'm [vendor] and want my data back?
 A: Talk to us.

 Q: Why not leak it for free?
```

```
A: Nothing comes free in this world.

Q: How to buy?
A: Contact us for more information.
-----BEGIN PGP SIGNATURE-----

iQEzBAEBCAAdFiEEJFFsLhzHiQgydxF44sc7xTuRGKAFAl/9yCsACgkQ4sc7xTuR
GKC/NwgAk/KZ9id9++Fi68M10rzd9uiC2DKTEX+qgJ9kEIASIvB/vh1uaS/mRZnj
GHf7I8D69zyI6FYlbndDN3DH6VUA21gD2dYxj7q79RpERQwV4PAO0iYRFBp0e3ho
nezYmVMMxB1GSsd+6AcdybLRJ1dmeIDB/mWnNa4S0jf45IkIw8/6j5965QxKlXBb
QlUShGTNom60BgpUOq7ud1ocH8c+HXbQdZpJ2LCq+CrQ+KuktMCsKUc1uydvTfDH
9zyjUtb3H9TC+zVugN3ANhtjDq0cIdOJQQ4vaGhnvLnXIDMvNQ1B4wxK+Ij50M8u
HD6LF0GUszJaNBdKylQaPV78sGqu3Q==
=HjXU
-----END PGP SIGNATURE-----
```

REFERENCES

[1] https://blog.cyberint.com/solarwinds-orion-api-lfi

[2] https://blog.cyberint.com/solarwinds-supply-chain-attack

[3] https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure