中招目标首次披露：SolarWinds供应链攻击相关域名生成算法可破解！

By 红雨滴团队

Archived: 2026-04-05 13:24:50 UTC

事件背景

近日，全球最著名的网络安全管理软件供应商SolarWinds遭遇国家级APT团伙高度复杂的供应链攻击并植入木马后门[1][2]。该攻击直接导致使用了SolarWinds Orion管理软件某些版本的企业客户全部受到影响：可任由攻击者完全操控。同时，SolarWinds在其官网发布安全通告称，受影响的产品为2020年3月至2020年6月间发布的2019.4到2020.2.1版本的SolarWinds Orion管理软件，并表示约有18000名客户下载使用了受影响的软件产品，但攻击者并未对所有使用者采取进一步的攻击行动，而仅选择感兴趣的目标开展后续攻击活动。

事件披露后的第一时间，奇安信红雨滴团队联合奇安信A-TEAM等安全团队，对该事件进行了持续分析与监测，并在第一时间对相关的报告、样本、域名和IP进行分析、扩展和验证，输出了目前比较全面的IOC列表[3]以及详细的排查方案和解决方案[4]。而在进一步的样本详细分析过程中我们发现，攻击者植入的恶意代码在生成DGA域名的时候，采用了受害者计算机域进行编码，所以可通过解码部分已知相关DGA域名，从而推导出部分受害者计算机域，我们通过对公开的DGA域名解码后发现大量中招的知名企业和机构，其中不乏Intel、Cisco等高科技企业和各类高校和政企单位。

奇安信威胁情报中心红雨滴团队第一时间向安全社区披露相关解码算法[5]，以帮助各用户在自己的数据视野内解码可见的数据以评估影响面。

事件时间线

时间	内容
2020年12月13日	火眼发布SolarWinds供应链攻击事件分析报告
2020年12月14日	微软发布SolarWinds供应链攻击事件分析报告
2020年12月14日	奇安信威胁情报中心发布事件分析以及国内视野补充报告
2020年12月15日	奇安信威胁情报中心破解SolarWinds供应链攻击域名编码算法

DGA域名编码-解码分析

因公开报告中已有多份相关恶意软件分析报告，故此处仅以DGA域名编码解码为分析展示。
恶意代码首先判断当前的ReportStatus状态，如果是New，则走第一个分支，会调用OrionImprovementBusinessLayer.CryptoHelper.GetPreviousString()。
同时如果上一次DNS解析的时候出现异常导致addressFamilyEx为Error，则会调用OrionImprovementBusinessLayer.CryptoHelper.GetCurrentString()

GetPreviousString()和GetCurrentString()生成的域名格式如下：

<encode_string_guid>+char+<substring(encode_string_domain) >.appsync-api.<domain2>. avsvmcloud.com

其中domain2的取值有eu-west-1、us-west-2、us-east-1、us-east-2。名的前缀部分，是一个三段式的字符串。

<encode_string_guid>+char+<substring(encode_string_domain) >

第一部分<encode_string_guid>是采用OrionImprovementBusinessLayer.CryptoHelper.guid经过CreateSecureString生成的一段15字节encode字符串。字符串构成为”ph2eifo3n5utg1j8d94qrvbmk0sal76c”

此处用于编码的OrionImprovementBusinessLayer.CryptoHelper.Base64Encode其实是自定义映射表的Base32算法，并不是常用的Base64Encode。

第二部分通过OrionImprovementBusinessLayer.CryptoHelper.CreateString生成一个字符。

第三部分<substring(encode_string_domain) >：由OrionImprovementBusinessLayer.CryptoHelper.dnStrLower组成

而dnStrlower是OrionImprovementBusinessLayer.CryptoHelper.dnStr的子串，dnStr在OrionImprovementBusinessLayer.CryptoHelper类的构造函数中被赋值，如下图所示，在构造函数中，传入的domain参数经DecryptShort encode后赋值给dnStr。

OrionImprovementBusinessLayer.CryptoHelper.DecryptShort中，首先对domain进行检查，如果domain的所有字符构成均在”0123456789abcdefghijklmnopqrstuvwxyz-_.”的范围内，则调用OrionImprovementBusinessLayer.CryptoHelper.Base64Decode将其encode（这里Base64Decode也只是作者起的方法名，并不是真正的base64decode）。否则调用OrionImprovementBusinessLayer.CryptoHelper.Base64Encode，并在前面拼接上”00”。

OrionImprovementBusinessLayer.CryptoHelper.Base64Decode的算法如下：

而OrionImprovementBusinessLayer.CryptoHelper在实例化的时候，传入的domain是OrionImprovementBusinessLayer.domain4，domain4在OrionImprovementBusinessLayer.Initialize中被赋值，其值是当前计算机所在域的名称。

故只需将OrionImprovementBusinessLayer.CryptoHelper.Base64Decode和OrionImprovementBusinessLayer.CryptoHelper.Base64Encode分析后，做逆运算，即可通过生成的域名 decode出感染主机的AD域名称（MAC地址无法解出，因为OrionImprovementBusinessLayer.userId会通过xor MD5生成）。

通过前面的分析，我们已经可以对SolarWinds供应链攻击的相关域名进行解码，以1fik67gkncg86q6daovthro0love0oe2.appsync-api.us-west-2.avsvmcloud.com为例：

1. 前15个字节是userId encode后的编码1fik67gkncg86q6
2. 中间一个字节是通过CreatString生成的“d”
3. 后面的aovthro0love0oe2则是AD域被编码后的字符串。
4. aovthro0love0oe2中只有”””0”而不是””00”，对应的编码是OrionImprovementBusinessLayer.CryptoHelper.Base64Decode，否则为OrionImprovementBusinessLayer.CryptoHelper.Base64Encode

5. 调用OrionImprovementBusinessLayer.CryptoHelper.Base64Decode对应的解码算法

解码后即是我们自己构造的域名称：qingmei-inc.co

解码算法

OrionImprovementBusinessLayer.CryptoHelper.Base64Decode的解码算法如下：

OrionImprovementBusinessLayer.CryptoHelper.Base64Encode的解码算法如下：

奇安信红雨滴团队DGA域名完整解码代码下载地址：

https://github.com/RedDrip7/SunBurst_DGA_Decode

疑似受害者域名分析

在分析的过程中，我们发现安全研究员@bambenek在其GitHub(https://github.com/bambenek/research/blob/main/sunburst/uniq-hostnames.txt)[6]上公布了多个疑似与此次攻击事件相关的DGA域名。

通过对这些域名进行解码分析我们发现，疑似包括思科，Intel在内的多家科技公司，以及美国多所大学，政府机构均疑似本次攻击的受害者。

解决方案

请装有SolarWinds Orion Platform软件的用户自查版本，若发现装有2019.4到2020.2.1版本的用户请立刻更新到2020.2.1HF 1或HF 2版本。

目前，奇安信已经提供了本次后门的专杀工具[7]，工具下载链接如下：
http://dl.qianxin.com/skylar6/SolarWinds_Focus_1.2.0.4000_1A13CB8CCD0BB68DC51A12882E478

专杀工具文件信息：

大小: 9.93 MB (10,417,262 字节)

MD5: 1A13CB8CCD0BB68DC51A12882E4783F1

SHA1: 8C77FAD5E13B1D1678A9FE00DF474014D13849AB

SHA256: 3BECC1CD192AD1AC11CAC1AABB237F4214837F7CDABDE8F39C27DAE1E1A2316A

也可通过杀毒软件（如奇安信天擎）进行全盘查杀，防止有攻击武器历史残留。更新链接：

https://documentation.solarwinds.com/en/success_center/orionplatform/content/install-prepare.htm

总结

通过修改软件下载源头的软件代码，无论是企业还是个人用户都非常难对软件检测出存在恶意代码，这也是供应链攻击的一种很强的属性。本次事件中的主角SolarWinds连续3年在网络管理软件市场中占有率第一，这也就意味着客户量巨大。

但即使是如此大体量，该供应链攻击过去了9个月才被发现，主要原因在于，攻击者会对感染了受影响版本的受害者进行筛选，并在后续仅对特定目标进行指令下发，以便进行后续的攻击，这可以看出供应链攻击的多变性和高精度性。另外，据外媒报道此次事件幕后可能归属于俄罗斯背景组织APT29，但未给出证据指向，目前该结论存疑。

目前，奇安信已经提供了本次后门的专杀工具，有需要的可以联系ti_support@qianxin.com。基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC等，都已经支持对此类攻击的精确检测。

IOCs

DOMAIN：

*.avsvmcloud.com

*.appsync-api.eu-west-1.avsvmcloud.com （DGA域名，*代表DGA的子域名）

*.appsync-api.us-west-2.avsvmcloud.com （DGA域名，*代表DGA的子域名）

*.appsync-api.us-east-1.avsvmcloud.com （DGA域名，*代表DGA的子域名）

*.appsync-api.us-east-2.avsvmcloud.com （DGA域名，*代表DGA的子域名）

######以下域名建议只用于检测2020-03之后的流量#######

databasegalore.com

deftsecurity.com

digitalcollege.org

freescanonline.com

globalnetworkissues.com

highdatabase.com

incomeupdate.com

kubecloud.com

lcomputers.com

panhardware.com

seobundlekit.com

solartrackingsystem.net

thedoccloud.com

virtualwebdata.com

webcodez.com

websitetheme.com

zupertech.com

URL：

http://websitetheme.com/swip/upd/Orion.Apollo.Xml

http://websitetheme.com/swip/upd/Orion.NPM-10.2.xml

文件HASH:

3e329a4c9030b26ba152fb602a1d5893

6ffe608a0a43054f850001d4ac31e76f

e18a6a21eb44e77ca8d739a72209c370

02af7cec58b9a5da1c542b5a32151ba1

2c4a910a1299cdae2a4e55988a2f102e

56ceb6d0011d87b6e4d7023d7ef85676

846e27a652a5e1bfbd0ddd38a16dc865

b91ce2fa41029f6955bff20079468448

参考链接

[1]https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[2]https://mp.weixin.qq.com/s/ms7u5PtvU36M3aYbTo2F5A

流行网管软件厂商SolarWinds供应链攻击事件通告

[3]https://mp.weixin.qq.com/s/q0IRgnZBHXoXoPS6BxAneA

SolarWinds供应链攻击事件最全IOC

[4]https://mp.weixin.qq.com/s/g6m4j7jZ9kSDHeZcLp-Xaw

【通告更新】内附详细排查方案和解决方案，SolarWinds供应链安全事件安全风险通告第二次更新

[5]https://github.com/RedDrip7/SunBurst_DGA_Decode

奇安信红雨滴团队DGA域名完整解码代码下载地址

[6]https://github.com/bambenek/research/blob/main/sunburst/uniq-hostnames.txt

[7]http://dl.qianxin.com/skylar6/SolarWinds_Focus_1.2.0.4000_1A13CB8CCD0BB68DC51A12882E4783F1.zip

[8]https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

[9]https://github.com/fireeye/sunburst_countermeasures

[10]https://www.solarwinds.com/securityadvisory
