VSRC 安全周报（2021-09-07）

0x00 本周漏洞综述

本周需要关注漏洞共 5 个：Annke NVR 远程代码执行漏洞（CVE-2021-32941）；TeamViewer 任意代码执行漏洞(CVE-2021-34858)；Apache Dubbo 远程代码执行漏洞(CVE-2021-36162)；Cisco Enterprise NFVIS 身份验证绕过漏洞（CVE-2021-34746）；BrakTooth：蓝牙堆栈多个安全漏洞。

本周安全态势共 1 个：勒索软件 Hive 分析。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. Annke NVR 远程代码执行漏洞（CVE-2021-32941）

漏洞概况

CVE ID	CVE-2021-32941	时 间	2021-08-30
类 型	RCE	等 级	严重
远程利用	是	影响范围	
攻击复杂度	低	可用性	高
用户交互	无	所需权限	无
PoC/EXP		在野利用	

漏洞详情

Annke 是一家受欢迎的监控系统和解决方案制造商，其产品辐射全球 30 多个国家和地区，一跃成为北美、欧洲多国、澳洲等在线市场知名品牌。它改变了千万用户对家居安防的使用体验，全球活跃用户数量达 3000 万。

2021 年 8 月 26 日，CISA 发布安全公告，公开了在 Annke Network Video Recorder（NVR）中发现的一个远程代码执行漏洞（CVE-2021-32941），其 CVSSv3 评分为 9.4。

NVR 是任何联网安全摄像机系统的一个重要组成部分，它们被设计用来捕捉、存储和管理来自 IP 摄像头的传入视频源。该漏洞是 Annke N48PBB（NVR）中基于堆栈的缓冲区溢出漏洞，未经身份验证的远程攻击者可以利用此漏洞访问敏感信息并以 root 权限执行任意代码。攻击者可以利用此漏洞访问录制的视频、删除镜头、更改配置和关闭某些摄像机等。

影响范围

N48PBB (NVR) <= V3.4.106 build 200422

安全建议

目前此漏洞已经修复，建议及时升级更新到最新版本。

下载链接：

https://www.annke.com/pages/download-center

通用安全建议

- 尽量减少所有控制系统设备或系统的网络暴露情况，并确保它们不能从互联网访问。
- 将控制系统网络和远程设备置于防火墙之后，并将其与商业网络隔离。
- 当需要远程访问时使用安全的方法，如虚拟专用网络（VPN），并确保 VPN 是最

新版本。

参考链接：

https://us-cert.cisa.gov/ics/advisories/icsa-21-238-02

https://www.nozominetworks.com/blog/new-annke-vulnerability-shows-risks-of-iot-security-camera-systems/

https://www.infosecurity-magazine.com/news/critical-iot-camera-flaw-allows/

2. TeamViewer 任意代码执行漏洞(CVE-2021-34858)

漏洞概况

CVE ID	CVE-2021-34858	时 间	2021-08-24
类 型	代码执行	等 级	高危
远程利用	是	影响范围	
攻击复杂度		可用性	
用户交互	是	所需权限	
PoC/EXP		在野利用	否

漏洞详情

TeamViewer 是一个使用广泛的远程控制软件，它可以在任何防火墙和 NAT 代理的后台实现桌面共享和文件传输。

2021 年 8 月 24 日，TeamViewer 发布更新公告，修复了 TeamViewer 中的一个任意代码执行漏洞（CVE-2021-34858）和一个越界读取漏洞（CVE-2021-34859），攻击者可以利用这些漏洞执行任意代码、导致二进制文件崩溃或导致越界读取。

TeamViewer 任意代码执行漏洞（CVE-2021-34858）

由于 TeamViewer 在使用现有 TVS 进行安装时容易受到文件解析问题的影响，攻击者可以利用此漏洞执行任意代码并导致二进制文件崩溃。但远程利用此漏洞需要用户交互以及第三方漏洞。

TeamViewer 越界读取漏洞（CVE-2021-34859）

由于共享内存管理中存在安全问题，导致 TeamViewer 服务执行越界读取。

影响范围

TeamViewe [Linux] < v15.21.4

TeamViewe [Windows] < v15.21.4

TeamViewe [macOS] < v15.21.2

[仅限 Windows]：默认情况下，TeamViewer 安装在受保护的 Program Files 目录中。如果用户有意选择将其安装在其它位置，则攻击者将能够实现权限提升。

安全建议

目前此漏洞已经修复，建议及时升级更新到以下最新版本：

TeamViewe [Linux] v15.21.4

TeamViewe [Windows] v15.21.6

TeamViewe [macOS] v15.21.2

下载链接：

https://www.teamviewer.cn/cn/

参考链接：

https://community.teamviewer.com/English/discussion/117791/linux-v15-21-4

https://community.teamviewer.com/English/categories/change-logs

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34858

3. Apache Dubbo 远程代码执行漏洞（CVE-2021-36162）

漏洞概况

CVE ID	CVE-2021-36162	时 间	2021-08-30
类 型	RCE	等 级	高危
远程利用	是	影响范围	
攻击复杂度		可用性	
用户交互		所需权限	
PoC/EXP	已公开	在野利用	

漏洞详情

Apache Dubbo 是一款应用广泛的 Java RPC 分布式服务框架。

2021 年 8 月 30 日，Github SecurityLab 公开披露了 Apache Dubbo 中的多个高危漏洞（CVE-2021-36162 和 CVE-2021-36163），攻击者可以利用这些漏洞远程执行任意代码。

Apache Dubbo YAML 反序列化漏洞（CVE-2021-36162）

Apache Dubbo 中存在 YAML 反序列化漏洞，可以访问配置中心的攻击者可以利用此漏洞远程执行任意代码。

Apache Dubbo 远程代码执行漏洞（CVE-2021-36163）

Apache Dubbo 使用了不安全的 Hessian 协议（可选），导致不安全的反序列化，攻击者可以利用此漏洞远程执行任意代码。

此外，SecurityLab 还公开了 Apache Dubbo 中的另一个 RCE 漏洞（GHSL-2021-096，拒绝修复），由于 Apache Dubbo 使用了不安全的 RMI 协议，导致不安全的反序列化，攻击者能够发送任意类型的参数并远程执行任意代码。

影响范围

Apache Dubbo v2.7.10

安全建议

目前 CVE-2021-36162 和 CVE-2021-36163 已经修复，建议及时应用安全补丁。但 GHSL-2021-096 问题拒绝修复，建议用户启用 JEP 290 机制。

CVE-2021-36162 补丁链接：

https://github.com/apache/dubbo/pull/8350

CVE-2021-36163 补丁链接：

https://github.com/apache/dubbo/pull/8238

参考链接：

https://securitylab.github.com/advisories/GHSL-2021-094-096-apache-dubbo/

https://dubbo.apache.org/en/downloads/

http://openjdk.java.net/jeps/290

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36162

4. Cisco Enterprise NFVIS 身份验证绕过漏洞（CVE-2021-34746）

漏洞概况

CVE ID	CVE-2021-34746	时 间	2021-09-01
类 型	身份验证绕过	等 级	严重
远程利用	是	影响范围	
攻击复杂度	低	可用性	高
用户交互	无	所需权限	无

PoC/EXP	已公开	在野利用	否

漏洞详情

2021 年 9 月 1 日，Cisco 发布安全公告，修复了其企业 NFV 基础设施软件（NFVIS）的 TACACS+认证、授权和计费（AAA）功能中的一个身份验证绕过漏洞（CVE-2021-34746），该漏洞的 CVSSv3 评分为 9.8。

由于对传递给认证脚本的用户输入的验证不完整，远程攻击者可以通过在认证请求中注入参数来利用此漏洞。成功利用此漏洞的攻击者可以绕过认证，并以管理员身份登录受影响的设备。

思科产品安全事件响应团队表示，已有适用于此漏洞的 PoC/EXP，目前暂未发现恶意利用。

影响范围

如果配置了 TACACS 外部认证方法，此漏洞会影响 Cisco Enterprise NFVIS 版本 4.5.1。

注：仅使用 RADIUS 或本地认证的配置不受影响。

安全建议

目前 Cisco 已经修复了此漏洞，建议受影响用户及时升级更新到 Cisco Enterprise NFVIS 版本 4.6.1 或更高版本。

下载链接：

https://software.cisco.com/download/home

确定是否启用 TACACS 外部认证

1.要确定设备上是否启用了 TACACS 外部认证功能，请使用 show running-config tacacs-server 命令。以下示例显示了当 TACACS 外部认证被启用时，Cisco Enterprise NFVIS 上 show running-config tacacs-server 命令的输出：

```
nfvis# show running-config tacacs-server
tacacs-server host 192.168.1.1
 key                  0
 shared-secret "example!23"
 admin-priv       15
 oper-priv        1
!
nfvis#
```

如果 show running-config tacacs-server 命令的输出为 No entries found，则未启用 TACACS 外部认证功能。

2.通过 GUI 检查配置。选择配置 > 主机 > 安全 > 用户和角色。如果在外部认证下定义了 TACACS+主机，那么该设备容易受到此漏洞的影响。

参考链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-g2DMVVh

https://www.cisco.com/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34746

5. BrakTooth：蓝牙堆栈多个安全漏洞

漏洞概述

2021 年 9 月 2 日，研究人员公开披露了商业蓝牙堆栈中统称为 BrakTooth 的多个安全漏洞，这些漏洞涉及英特尔、高通、德州仪器和赛普拉斯在内的十多家 SoC 供应商的 13 款蓝牙芯片组，使得全球数十亿台设备容易受到拒绝服务和任意代码执行的攻击风险。

漏洞详情

研究人员发现，这些漏洞至少存在于 1,400 个嵌入式芯片组件使用的封闭商业 BT 堆栈中，甚至还可能影响了 BT 系统芯片（SoC）、BT 模块或其它 BT 终端产品。受影响的产品包括智能手机、信息娱乐系统、笔记本电脑和台式机系统、音频设备（扬声器、耳机）、家庭娱乐系统、键盘、玩具和工业设备（如可编程逻辑控制器 - PLC）等类型的设备。受影响的产品列表总数如下所示：

Vendor	SoC	QID(s)	Listing(s) Count
Intel	AX200	127398	17*
Texas Instruments	CC2564C	87924, 126789, 117855	14
Cypress	CYW20735B1	169362, 112768	1
Bluetrum Technology	AB32VG1	115952, 131655	201
Zhuhai Jieli Technology	AC6905X	91274	341
Zhuhai Jieli Technology	AC6925C	110839	376
Zhuhai Jieli Technology	AC6366C	136145	173
Actions Technology	ATS281X	124400, 124265	47
Qualcomm	WCN3990/8	96248, 116819	22
Qualcomm	CSR8811/CSR8510	30846, 58778, 70941	92
Espressif Systems	ESP32	**116661 (ESP32 Dual-Mode Stack)**	28
Harman International	JX25X	84803, 62232	63
Silabs	WT32i	49552	48
Total Listings			**1423**

图 1. 受影响的产品列表总数

到目前为止，已经有 20 个漏洞分配了 CVE 编号，有 4 个漏洞正在等待英特尔和高通为其分配 CVE。BrakTooth 漏洞列表如下：

Anomalies	CVE ID(s)	Device(s)	State(s)	Target Layer(s)	Impact Type	Compliance Violated
8.1 **V1** Feature Pages Execution	CVE-2021-28139	ESP-WROVER-KIT	*Feature Exchange*	LMP	ACE / Deadlock	[V.1] Part E, Sec. 2.7
8.2 **V2** Truncated SCO Link Request	CVE-2021-34144	AC6366C_DEMO_V1.0	***After Paging***	LMP	Deadlock	[V.2] Part E, Sec. 2.7
8.3 **V3** Duplicated IOCAP	CVE-2021-28136	ESP-WROVER-KIT	*Bounding*	LMP	Crash	[V.2] Part C, Sec. 4.2.7.1
8.4 **V4** Feature Resp. Flooding	CVE-2021-28135 CVE-2021-28155 CVE-2021-31717	ESP-WROVER-KIT JBL TUNE500BT Xiaomi MDZ-36-DB	***After Paging***	LMP	Crash	[V.1] Part E, Sec. 2.7
8.5 **V5** LMP Auto Rate Overflow	CVE-2021-31609 CVE-2021-31612	DKWT32I-A BT Audio Receiver	Data Rate Change	Baseband	Crash	[V.2] Part B, Sec. 6.6.2
8.6 **V6** LMP 2-DH1 Overflow	Pending	DVK-BT900-SA	After EDR Change	Baseband	Deadlock	[V.2] Part C, Sec. 2.3
8.7 **V7** LMP DM1 Overflow	CVE-2021-34150	AB32VG1	***Many***	Baseband	Deadlock	[V.2] Part B, Sec. 6.5.4.1
8.8 **V8** Truncated LMP Accepted	CVE-2021-31613	BT Audio Receiver XY-WRBT Module	***Many***	LMP	Crash	[V.2] Part C, Sec. 5.1
8.9 **V9** Invalid Setup Complete	CVE-2021-31611	BT Audio Receiver XY-WRBT Module	*Feature Exchange*	LMP	Deadlock	[V.1] Part E, Sec. 2.7
8.10 **V10** Host Conn. Flooding	CVE-2021-31785	Xiaomi MDZ-36-DB	*Host Connection*	LMP	Deadlock	[V.1] Part E, Sec. 2.7
8.11 **V11** Same Host Connection	CVE-2021-31786	Xiaomi MDZ-36-DB	*Host Connection*	LMP	Deadlock	[V.1] Part E, Sec. 2.7
8.12 **V12** AU Rand Flooding	CVE-2021-31610 CVE-2021-34149 CVE-2021-34146 CVE-2021-34143	AB32VG1 CC256XCQFN-EM CYW920735Q60EVB AC6366C_DEMO_V1.0	***After Paging***	LMP	Crash Deadlock	[V.1] Part E, Sec. 2.7
8.13 **V13** Invalid Max Slot Type	CVE-2021-34145	CYW920735Q60EVB	*After Setup Complete*	Baseband	Crash	[V.1] Part E, Sec. 2.7
8.14 **V14** Max Slot Length Overflow	CVE-2021-34148	CYW920735Q60EVB	*After Setup Complete*	Baseband	Crash	[V.1] Part E, Sec. 2.7
8.15 **V15** Invalid Timing Accuracy	CVE-2021-34147 Pending Pending	CYW920735Q60EVB Pocophone F1 (WCN3990) Intel AX200	*Timing Accuracy*	LMP, Baseband	Crash	[V.1] Part E, Sec. 2.7
8.16 **V16** Paging Scan Deadlock	Pending	Intel AX200	*After Host Connection*	LMP, Baseband	Deadlock	[V.1] Part E, Sec. 2.7
A1 Accepts Lower LMP Length	N.A	**All tested devices**	***Many***	Baseband	Non-Compliance	[V.2] Part C, Sec. 5.1
A2 Accepts Higher LMP Length	N.A	**All, except ESP32**	***Many***	Baseband	Non-Compliance	[V.2] Part C, Sec. 5.1
A3 Multiple Encryption Start	N.A	Xiaomi MDZ-36-DB	*After Encryption Start*	LMP	Non-Compliance	[V.2] Part C, Sec. 4.12
A4 Ignore Role Switch Reject	N.A	Pocophone F1 (WCN3990)	*Role Switch*	LMP	Non-Compliance	[V.2] Part C, Sec. 4.4.2
A5 Invalid Response	N.A	Intel AX200 DVK-BT900-SA	*Feature Exchange*	LMP	Non-Compliance	[V.2] Part C, Sec. 4.3.4
A6 Ignore Encryption Stop	N.A	CYW920735Q60EVB	*After Encryption Start*	LMP	Non-Compliance	[V.2] Part C, Sec. 4.2.5.4

图 2. BrakTooth 漏洞列表

研究人员发现了漏洞的三种主要攻击场景，其中最严重的漏洞会导致物联网（IoT）设备上的任意代码执行。

- 智能家居设备的任意代码执行

BrakTooth 漏洞中，最严重的漏洞为 CVE-2021-28139，影响了乐鑫 ESP32 SoC，这是一系列低成本、低功耗的 SoC 微控制器，集成了 Wi-Fi 和双模蓝牙，常用于工业自动化、智能家居设备、个人健身小工具等物联网设备中。由于 ESP32 BT 库中缺乏越界检查，导致攻击者可以在扩展功能页表的范围之外注入 8 个字节的任意数据。

- 笔记本电脑和智能手机中的 DoS

研究人员发现英特尔的 AX200 SoC 和高通的 WCN3990 SoC 上运行的设备在收到格式错误数据包时容易触发 DoS。

- BT 音频产品崩溃

各种 BT 音箱容易受到一系列漏洞的影响 (CVE-2021-31609 和 CVE-2021-31612-发送超大的 LMP 数据包时失败；CVE-2021-31613-截断的数据包；CVE-2021-31611-启动程序失败；以及 CVE-2021-28135、CVE-2021-28155 和 CVE-2021-31717-功能响应泛滥）。成功利用这些漏洞可导致程序崩溃，用户需手动打开无响应的设备。

目前 Espressif（乐鑫）、Infineon（Cypress）（英飞凌（赛普拉斯）和 Bluetrum Technology (蓝讯科技) 已发布补丁修复其产品中的漏洞，但 Intel (英特尔)、Qualcomm（高通）和 Zhuhai Jieli Technology（珠海杰利科技）正在调查漏洞或开发补丁。

SoC or Module Vendor	BT SoC	Firmware or SDK Ver.	Vuln. / Anomalies	Patch Status
Espressif Systems	ESP32	esp-idf-4.4	V1,V3-4 / A1	[10] **Available**
Intel	AX200	Linux - ibt-12-16.ddc Windows - 22.40.0	V15-16 / A1-2, A5	Patch in progress
Qualcomm	WCN3990/8	crbtfw21.tlv, patch 0x0002	V15 / A1-2,A4	Patch in progress
Qualcomm	CSR8811/CSR8510	v9.1.12.14	V6 / A1-2	No fix
Texas Instruments	CC2564C	cc256xc_bt_sp_v1.4	V12 / A1-2	No fix
Infineon (Cypress)	CYW20735B1	WICED SDK 2.9.0	V12-15 / A2,A6	**Available** *
Bluetrum Technology	AB5301A	V06X_S6645 (LMP Subver. 3)	V7,V12 / A1-2	**Available** *
Zhuhai Jieli Technology	AC6925C	*unspecified* (LMP Subver. 12576)	V8-9 / A1-2	Investigation in progress
Zhuhai Jieli Technology	AC6905X	*unspecified* (LMP Subver. 12576)	V5,V8-9 / A1-2	Investigation in progress
Zhuhai Jieli Technology	AC6366C	fw-AC63_BT_SDK 0.9.0	V2,V12 / A1-2	Patch in progress
Actions Technology	ATS281X	*unspecified* (LMP Subver. 5200)	V4,V10-11 / A1-2	Investigation in progress
Harman International	JX25X	*unspecified* (LMP Subver. 5063)	V4 / A1-2	Pending
Silabs	WT32i	iWRAP 6.3.0 build 1149	V5 / A1-2	Pending

图 3.受影响厂商及其产品补丁状态

此外，研究人员已经为生产 BT SoC、模块和产品的供应商发布了 BrakTooth 漏洞的 PoC ，以供其检查设备中的漏洞。

影响范围

受影响的厂商、芯片组和设备：

BT SoC Vendor	BT SoC	Dev. Kit / Product	Sample Code
Bluetooth 5.2			
Intel	AX200	Laptop Forge15-R	N.A
Qualcomm	WCN3990	Xioami Pocophone F1	N.A
Bluetooth 5.1			
Texas Instruments	CC2564C	CC256XCQFN-EM	SPPDMMultiDemo
Zhuhai Jieli Technology	AC6366C	AC6366C_DEMO_V1.0	app_keyboard
Bluetooth 5.0			
Cypress	CYW20735B1	CYW920735Q60EVB-01	rfcomm_serial_port
Bluetrum Technology	AB5301A	AB32VG1	Default
Zhuhai Jieli Technology	AC6925C	XY-WRBT Module	N.A
Actions Technology	ATS281X	Xiaomi MDZ-36-DB	N.A
Bluetooth 4.2			
Zhuhai Jieli Technology	AC6905X	BT Audio Receiver	N.A
Espressif Systems	ESP32	ESP-WROVER-KIT	bt_spp_acceptor
Bluetooth 4.1			
Harman International	JX25X	JBL TUNE500BT	N.A
Bluetooth 4.0			
Qualcomm	CSR 8811	Laird DVK-BT900-SA	vspspp.server.at
Bluetooth 3.0 + HS			
Silabs	WT32i	DKWT32I-A	ai-6.3.0-1149

安全建议

目前部分供应商已经修复了其产品中的漏洞，部分供应商正在开发补丁，但德州仪器（Texas Instruments）拒绝修复漏洞。建议受影响用户参考厂商发布的补丁及时更新。

BrakTooth PoC 下载链接：

https://docs.google.com/forms/d/e/1FAIpQLSdYGKfZrImQfGMM9JWUNldtsjTKfBDia8eg0bCJX__UPNsD4A/viewform

参考链接：

https://asset-group.github.io/disclosures/braktooth/disclosure.html#x1-150008.1

https://www.bleepingcomputer.com/news/security/bluetooth-braktooth-bugs-could-affect-billions-of-devices/

https://threatpost.com/bluetooth-bugs-dos-code-execution/169159/

https://thehackernews.com/2021/09/new-braktooth-flaws-leave-millions-of.html

0x02 本周安全态势

1. 勒索软件 Hive 分析

执行摘要

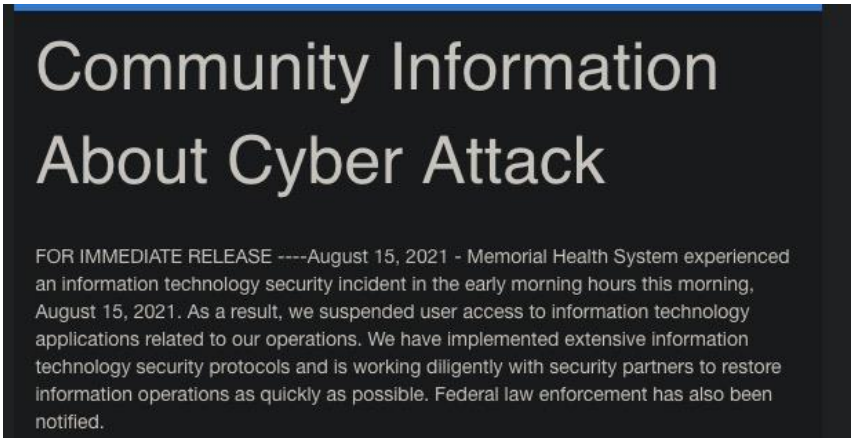
Hive 是 2021 年 6 月首次出现的使用双重勒索策略的勒索运营团伙。值得注意的是，该团伙选择目标时不会过多思考，尤其是在涉及医疗机构和医院时并不会加以限制，最近对俄亥俄州纪念卫生系统医院的攻击证明了这点。勒索软件 Hive 是用 Go 语言编写的，利用该语言的并发功能，可以更快地加密文件。本文讲述了勒索软件 Hive 的 TTP，并对其 Payload 进行了逆向工程深入研究。撰写本文时，Hive 仍然活跃，其 Hive Leaks 网站上列出了多达 30 家公司。

背景

虽然许多活跃的勒索运营团伙已经承诺放弃对医疗目标的攻击，以顺应当前的全球形势，但 Hive 并不是其中之一。2021 年 8 月 15 日，有消息称 Hive 对俄亥俄州的一家医疗机构 Memorial Health System 发起了攻击。结果，该医院被迫建议一些病人到其它机构寻求治

疗。

虽然一些针对公共卫生和关键基础设施目标的勒索软件攻击可能是采取了猎枪式攻击的结果，大规模的网络钓鱼活动在不了解受害者环境的情况下盲目地在受害者设备上执行恶意软件，但 Hive 的情况并非如此。这是一个人为操作的勒索软件攻击，旨在接受来自命令行的输入，表明攻击者既了解环境，又对其攻击进行调整以造成最大影响。



Memorial Health Systems 关于勒索软件攻击的公开声明

Hive

Hive 或 "HiveLeaks "是一个相对较新的勒索团伙，于 2021 年 6 月底首次出现。Hive 使用双重勒索策略，他们通过双管齐下的攻击来赚钱：在锁定受害者的系统之前渗出敏感数据。这使他们能够向受害者施压，使其支付比传统勒索软件攻击更大的金额，因为受害者还面临着敏感数据大规模泄漏的威胁。到目前为止，Hive 的计划被证明是成功的，因为在他们的受害者网站上发布了多个泄漏数据信息。撰写本文时，HiveLeaks 网站上有 30 家公司。

HiveLeaks 站点在发布受害者文件之前显示计时器

我们不能把泄露的数据放回其原来的系统里，但我们至少可以对 Hive 运营商的首选技术进行细分，并深入研究他们的勒索软件工具包，以帮助其他潜在受害者。

技术分析

初始访问方式可能会有所不同。Cobalt Strike 植入物通常是首选工具，它们通过网络钓鱼或电子邮件传递，以建立初始访问。这些 beacons 保持持久性，并使攻击者在受感染的环境中扩大其影响范围。它们还被用来启动 Hive Payload。

最近的活动选择使用 ConnectWise。ConnectWise 是一个合法的商业远程管理工具，近年来已被多个勒索软件运营商滥用。该工具使得他们能够在 Cobalt Strike 没有成功的环境中持久化和管理其恶意软件。

一旦进入，攻击者将试图通过 consvcs.dll（MinDump）的方式转储凭证 rundll32.exe。

```
\Windows\system32\cmd.exe /C rundll32.exe
\Windows\System32\comsvcs.dll MinDump 752 lsass.dmp full
```

此外，WDigest 可以被操作以允许缓存明文凭证数据。

```
\Windows\system32\cmd.exe /C reg add
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 && gpupdate /force
```

ADRecon 等其它工具可以用来进一步了解和遍历被感染的活动目录（AD）环境。ADRecon 是一个开源的工具，旨在映射、遍历和枚举 AD 环境。

Hive Payload

虽然上面提到的工具、技术和程序对于现在的勒索团伙来说是相当标准的，但 Hive 使用的是他们自己的闭源勒索软件。Payload 是用 Go 语言编写的，并用 UPX 打包。解压后，由于 Go 软件包静态链接所有的依赖关系以创建一个可靠的可移植可执行文件的方式，赎金软件本身的大小超过 2MB。

开发人员正在利用 Go 的一些原生优势，特别是实现简单和可靠的并发能力。另一方面，Go 以能够在不同的操作系统中轻松进行交叉编译而闻名，但 Hive 实现其功能的方式使其目前只针对 Windows。

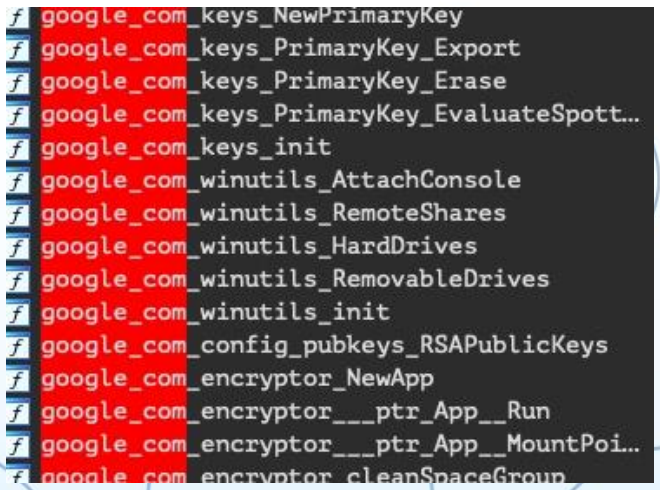
该勒索软件被设计为接受来自命令行的输入，表明它是要由操作人员或包含所需参数的脚本直接运行。可用的标志如下：

Flag	Type	Functionality
t	Int	Number of threads to run in parallel
stop	String	Regex for services to stop
kill	String	Regex for process to kill (case insensitive)
skip	String	Regex for filenames to skip (case insensitive)
no-cleanpollDesc	Bool	Skip clean disk space stage

Hive 勒索软件使用的标志

这些标志在很大程度上是易于理解的，除了最后一个选项 no-cleanpollDesc。这是勒索软件功能的最后阶段，即在所有逻辑驱动器中寻找一个名为 swap.tmp 的文件，并在勒索软件退出前将其删除。开发者将此称为 "cleaning space"。目前，我们不知道该文件的作用，不管它是在操作过程中生成的组件、本机 Windows 文件，还是对未来构建的不完整的跨平台功能的一个参考。

Go 恶意软件通常被认为是很难进行逆向工程的，主要原因是在每个可执行文件中都有大量与之相关的导入代码。隔离恶意软件开发者提供的代码非常重要。在这种情况下，Hive 开发者提供了由 main（）函数编排的四个包：encryptor、keys、winutils 和 config。



google.com 父目录下的自定义包

粗略检查可能会遗漏这些，因为它们位于一个名为 google.com 的父包下，或许是为了让人觉得这些是标准包。

在初始化 encryptor.NewApp（）下的勒索软件功能之前，主函数解析了操作者提供的标志。首先，它生成并导出加密密钥，并生成赎金票据。它将受害者引导到一个有密码保护的 Onion 域。

```
http://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd[.]onion/
```

它还警告受害者，他们即将在 Hive Leaks 站点上披露他们被盗的数据。

```
http://hiveleakdbtnp76ulyhi52eag6c6tyc<redacted>.onion/
```

主要功能位于 encryptor.(*App).Run()下，它的作用如下：

1.App.ExportKeys()环绕标准的 go crypto 函数，它用来生成 RSA 密钥。一个密钥文件被导出。

2.MountPoints()列举了不同类型的驱动器，并将它们附加到一个切片（Go 中动态大小的数组）。这包括本地逻辑驱动器、可移动驱动器和远程共享。

3.根据 kill 标志，恶意软件会杀死与提供的正则表达式匹配的进程。如果未提供自定义值，则使用以下默认值：

```
“bmr|sql|oracle|postgres|redis|vss|backup|sstp”
```

4.根据 stop 标志，恶意软件连接到 Windows 服务控制管理器，并停止符合所提供的搜索条件的服务。

5.恶意软件会创建一个批处理文件来自我删除，文件名为 hive.bat，通过一个新的进程从磁盘上删除自己的组件。

```
timeout 1 || sleep 1

del "C:\Users\admin1\Desktop\hmod4.exe"

if exist "C:\Users\admin1\Desktop\hmod4.exe" goto Repeat

del "hive.bat"
```

6. 它创建了一个批处理文件来删除文件名为 shadow.bat 的副本，并作为一个单独的进程执行。

```
vssadmin.exe delete shadows /all /quiet

del shadow.bat
```

7.为了利用 Go 的并发功能，Hive 的开发人员运行了一个 Notify()函数来观察跟踪并行线程的 WaitGroup。只要有线程挂起，这个函数就会保持程序的运行。

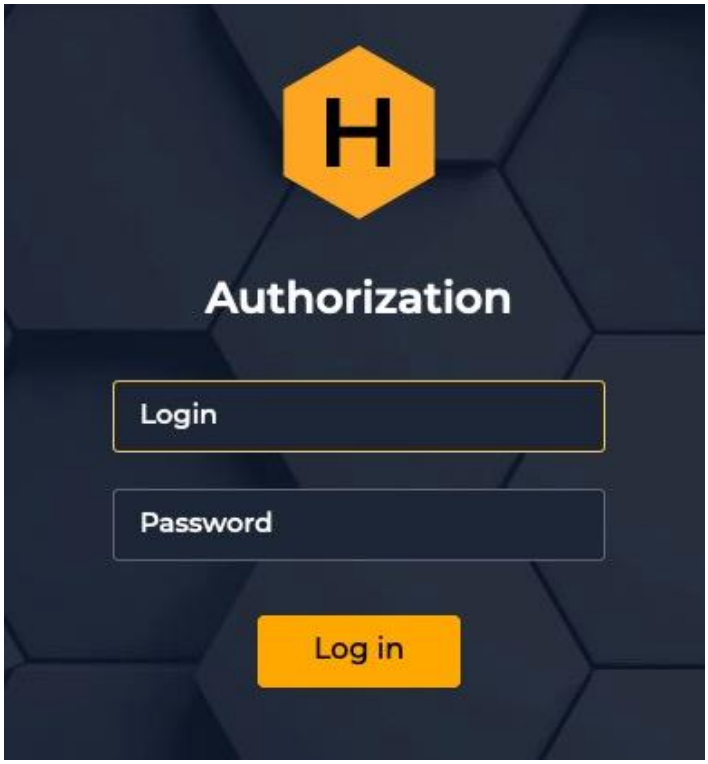
8.现在进入勒索软件的主要功能。ScanFiles()将填充一个文件绝对路径的列表，并将其输入通道（各种队列）。然后，EncryptFiles()将产生线程，每个线程从该队列中取出一个文件并进行加密。用 Go 编写实现了并发特性，这是这个勒索软件的主要优势，它能够更快的进行文件加密。

9.最后，设计人员确保从内存中删除加密密钥。

赎金票据被存放在包含加密文件的每个文件夹（跳过 C:\windows）中。

'HOW_TO_DECRYPT.TXT' 赎金票据

赎金通知指示受害者通过 TOR 访问 Hive 门户网站，并用他们指定的唯一 ID 登录，以进行支付。



Hive 受害者门户网站

每个感染活动都被分配了独特的凭证，可在赎金通知中找到。这个门户将受害者引向标准的勒索软件 "support "区，在那里他们可以上传免费的测试文件，与攻击者沟通，并在他们选择付款时收到解密器（理想情况下，受害者不应该付款）。

结论

随着这些攻击继续升级并变得更加恶劣，因此，预防攻击变得更加重要。虽然日常维护和备份策略是必须的，但在双重勒索攻击中，这些还不够。

一旦执行，大多数勒索软件会以相当聪明的方式去攻击备份和存储卷。许多勒索软件甚至已经发展到针对特定的 NAS 设备和平台，也有一些勒索软件将完全绕过加密阶段，选择偷窃数据来公开敲诈受害者。虽然后一种情况可能由于缺乏干扰而显得更易于实现，但对声誉的损害、潜在的责任和对企业生存能力的威胁仍然存在。因此，我们强调预防此类威胁。

我们建议所有企业和组织部署端点保护技术，这些技术超越了静态检查、基本签名和其它过时的组件。

IoC

文件哈希

SHA1

67f0c8d81aefcfc5943b31d695972194ac15e9f2

edba1b73ddd0e32784ae21844c940d7850531b82

2877b32518445c09418849eb8fb913ed73d7b8fb

cd8e4372620930876c71ba0a24e2b0e17dcd87c9

eaa2e1e2cb6c7b6ec405ffdf204999853ebbd54a

0f9484948fdd1b05bad387b14b27dc702c2c09ed

e3e8e28a70cdfa2164ece51ff377879a5151abdf

9d336b8911c8ffd7cc809e31d5b53796bb0cc7bb

1cc80ad88a022c429f8285d871f48529c6484734

3b40dbdc418d2d5de5f552a054a32bfbac18c5cc

2f3273e5b6739b844fe33f7310476afb971956dd

7777771aec887896be773c32200515a50e08112a

5dbe3713b309e6ecc208e2a6c038aeb1762340d4

480db5652124d4dd199bc8e775539684a19f1f24

Dc0ae41192272fda884a1a2589fe31d604d75af2

Hive.bat

C9471adc8db180a7da5a56966b156b440483856f

Shadow.bat

4714f1e6bb75a80a8faf69434726d176b70d7bd8

SHA256

a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749

50ad0e6e9dc72d10579c20bb436f09eeaa7bfdbcb5747a2590af667823e85609

5ae51e30817c0d08d03f120539aedc31d094b080eb70c0691bbfbaa4ec265ef3

77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618

e1a7ddbf735d5c1cb9097d7614840c00e5c4d5107fa687c0ab2a2ec8948ef84e

ed614cba30f26f90815c28e189340843fab0fe7ebe71bb9b4a3cb7c78ff8e3d2

c5fe23c626413a18cba8fb4ea93df81529c85f470577fb9c2336d6b692689d9d

88f7544a29a2ceb175a135d9fa221cbfd3e8c71f32dd6b09399717f85ea9afd1

2f7d37c22e6199d1496f307c676223dda999c136ece4f2748975169b4a48afe5

fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf

1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff

bf7bc94506eb72daec1d310ba038d9c3b115f145594fd271b80fbe911a8f3964

c04509c1b80c129a7486119436c9ada5b0505358e97c1508b2cfb5c2a177ed11

612e5ffd09ca30ca9488d802594efb5d41c360f7a439df4ae09b14bce45575ec

0df750bf15895d410c3f6ce45279ab0329c5c723af38b99aadc9a60bcdc9a71d

5954558d43884da2c7902ddf89c0cf7cd5bf162d6feefe5ce7d15b16767a27e5

Hive.bat

93852dbd3a977cf2662b0c4db26b627736ba51c0df627eb36b41fdbde093c3c3

Shadow.bat

D158f9d53e7c37eadd3b5cc1b82d095f61484e47eda2c36d9d35f31c0b4d3ff8

通信

Cobalt Beacon: 176.123.8.228

MITRE ATT&CK

T1574.001 -劫持执行流程为：DLL 搜索顺序劫持

https://attack.mitre.org/techniques/T1574/001/

TA0005 -防御规避

https://attack.mitre.org/tactics/TA0005/

TA0004 -特权提升

https://attack.mitre.org/tactics/TA0004/

T1486 -数据加密的影响

https://attack.mitre.org/techniques/T1486/

T1027.002 -混淆后的文件或信息：软件包装

https://attack.mitre.org/techniques/T1027/002/

T1003.001 - OS 凭证转储：LSASS 内存

https://attack.mitre.org/techniques/T1003/001/

T1007 -系统服务发现

https://attack.mitre.org/techniques/T1007/

T1059 -命令和脚本解释器

https://attack.mitre.org/techniques/T1059/

T1059.001 -命令和脚本解释器：PowerShell

https://attack.mitre.org/techniques/T1059/001/

T1059.003 -命令和脚本解释器：Windows Command Shell

https://attack.mitre.org/techniques/T1059/003/

T1490 -禁止系统恢复

https://attack.mitre.org/techniques/T1490/

原文链接：

https://labs.sentinelone.com/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/