FIN6 组织针对性勒索行动频发，安天智甲有效防护

安天 CERT

1 概述

自 2019 年 1 月起，安天 CERT 持续监测发现多起目标为大型企业或组织的针对性勒索软件攻击事件。攻击者所使用的勒索软件为 LockerGoga，而在 LockerGoga 之前，另一勒索软件 Ryuk 同样针对大型企业发起了多次定制攻击，安天对二者展开了关联分析，确定两勒索软件的运营者为同一攻击组织——FIN6 组织。

安天 CERT 通过多维度的关联分析，揭示了勒索软件 LockerGoga 与 Ryuk 之间的关联性与同源性，确定了两个勒索软件的运营者为同一组织。分析人员在相关威胁情报分析中发现，FIN6 组织针对 POS 系统攻击活动的相关 IP 与 LockerGoga 勒索活动部分重合，攻击活动中使用的 stager 为同一类型，据此确定 LockerGoga 与 Ryuk 勒索活动的运营者同为 FIN6 组织。同时，分析人员通过对 FIN6 组织针对性勒索活动展开关联分析，揭示了 FIN6 组织针对大型企业或组织的勒索行动的攻击链路。

经验证，安天智甲终端防御系统（英文简称 IEP，以下简称安天智甲）可实现对 FIN6 组织常用勒索软件 LockerGoga、Ryuk 的有效防护。

2 FIN6 组织系列针对性勒索事件回顾

2.1 针对法国亚创集团（Altran）的勒索事件

企业介绍：法国亚创集团成立于 1982 年，是一家提供创新和工程咨询服务的全球性公司，业务遍布全球 30 多个国家，涉及汽车、通信、生命科学、航空航天、国防、能源、金融和铁路等行业。

事件回顾：2019 年 1 月 24 日，攻击者利用 LockerGoga 勒索软件对亚创集团进行了勒索攻击。2019 年 1 月 28 日，亚创集团发布声明，称技术专家正在对此次勒索事件进行取证跟进。受此次勒索事件影响，亚创集团暂停了全球多项业务[3]。

Press release
28.01.2019

Information on a cyber attack

On the 24th of January 2019, Altran was the target of a cyber attack affecting operations in some European countries.

To protect our clients, employees and partners, we immediately shut down our IT network and all applications. The security of our clients and of data is and will always be our top priority. We have mobilized leading global third-party technical experts and forensics, and the investigation we have conducted with them has not identified any stolen data nor instances of a propagation of the incident to our clients.

图 2-1 亚创集团针对勒索事件发布的声明

此次勒索事件涉及到的样本标签如表 2-1 所示。

表 2-1 LockerGoga 样本信息

病毒名称	Trojan[Ransom]/Win32.Crypren
原始文件名	svch0st.Random.exe
MD5	52340664fe59e030790c48b66924b5bd
处理器架构	Intel 386 or later processors and compatible processors
文件大小	1.20 MB (1,267,728 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2019-01-23 22:42:50
数字签名	MIKL LIMITED
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2019-01-24 09:41:18
VT 检测结果	56 / 72

感染勒索软件后，LockerGoga 作者要求受害公司通过邮箱联系，支付比特币来解密文件。联系邮箱为 CottleAkela@protonmail.com 和 QyavauZehyco1994@o2.pl，被加密文件后缀为.lock。

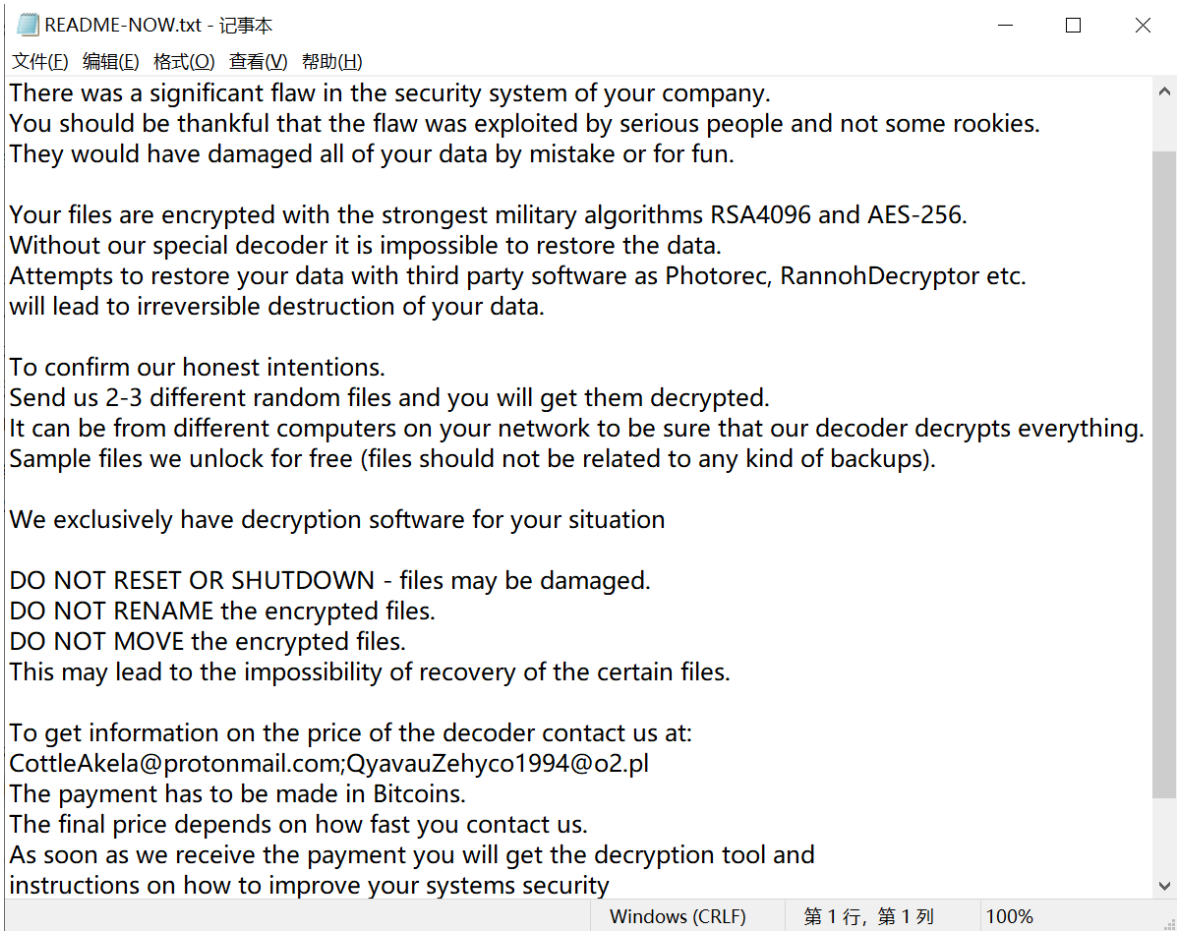


图 2-2 亚创集团勒索事件中的勒索信

2.2 针对挪威海德鲁公司（Norsk Hydro）的勒索事件

企业介绍：挪威海德鲁公司创建于 1905 年，主要经营石油、能源、轻金属（铝、镁）、石化产品、水电及设备、工业用化学品等，是世界最大的综合性铝业集团之一。

事件回顾:海德鲁公司于 2019 年 3 月 19 日举行新闻发布会，称 3 月 18 日午夜，公司遭到勒索软件攻击，致使主机死机，导致生产业务中断。参会的 NorCERT（挪威的国家应急响应中心）代表称此次攻击事件是由一个名为 LockerGoga 的勒索软件发起的，可能涉及到对海德鲁公司的 Active Directory 系统的攻击。

该事件所涉及到的样本标签如表 2-2 所示。

表 2-2 LockerGoga 样本信息

病毒名称	Trojan[Ransom]/Win32.Crypren
原始文件名	zzbdrimp2939.exe
MD5	7e3f8b6b7ac0565bfcbf0a1e3e6fcfbc
处理器架构	Intel 386 or later processors and compatible processors

文件大小	1.2 MB (1249144 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2019-03-09 17:50:30
数字签名	ALISA LTD
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2019-03-12 19:49:00
VT 检测结果	45 / 67

此次勒索事件中，攻击者使用了与亚创勒索事件中不同的联系邮箱 DharmaParrack@protonmail.com、wyattpettigrew8922555@mail.com。

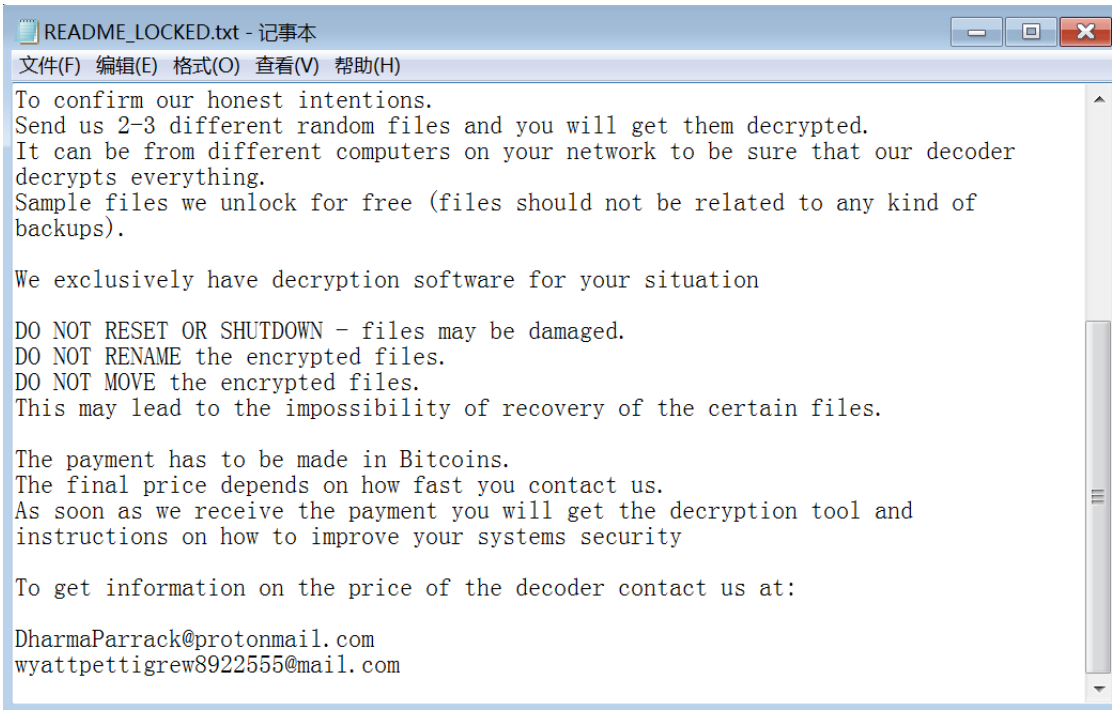


图 2-3 海德鲁公司勒索事件中的勒索信

2.3 针对英国警察联合会（Police Federation）的勒索事件

事件回顾：英国警察联合会于 2019 年 3 月 21 日在 Twitter 上发表声明，称其萨里总部的计算机在 3 月 9 日遭受到勒索软件的攻击，几个数据库和电子邮件系统被加密，备份数据也被删除，导致其服务中断[4]。

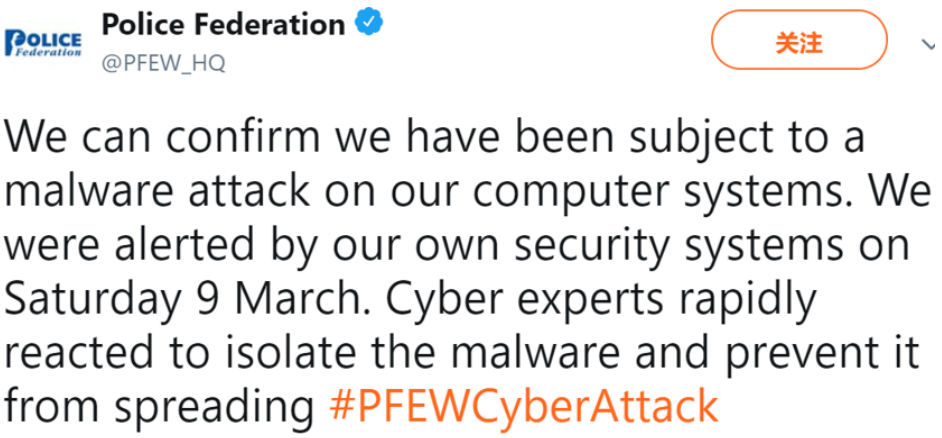


图 2-4 英国警察联合会的声明

根据英国国家网络安全中心发布的预警信息，可以得知此次攻击事件中的勒索软件为 LockerGoga。

2.4 针对美国化学公司瀚森（Hexion）和迈图（Momentive）的勒索事件

企业介绍：迈图高新材料集团是全球第二大的有机硅产品及其关联产品的生产商，瀚森化工是一家特种树脂和先进材料的全球领先企业，这两家企业于 2010 年 9 月 14 日宣布合并。

事件回顾：这两家化学公司 2019 年 3 月 12 日遭到 LockerGoga 勒索软件攻击，迈图称其公司的 Windows 计算机出现了蓝屏并且文件被加密，受勒索软件攻击的计算机上的数据可能已经丢失。瀚森员工拒绝提供更多关于攻击的信息[5]。

表 2-3 LockerGoga 和 Ryuk 勒索行动的相似之处

操作	Ryuk	LockerGoga
目标为大型企业，目的是勒索并获取高额赎金	是	是
运行 powershell 脚本，连接 IP 下载 payload	是	是
下载反向 shell 并运行	是	是
使用 windows 命令行工具以及外部上传工具进行网络侦查	是	是
使用 RDP 进行横向移动	是	是
使用 psexec 向局域网分发勒索软件	是	是
使用批处理脚本 kill.bat 结束服务/进程，删除备份	是	是

LockerGoga 和 Ryuk 勒索活动的详细对比内容如下：

1. 二者使用同名批处理文件 kill.bat 结束进程、停止反病毒引擎服务以及删除备份。

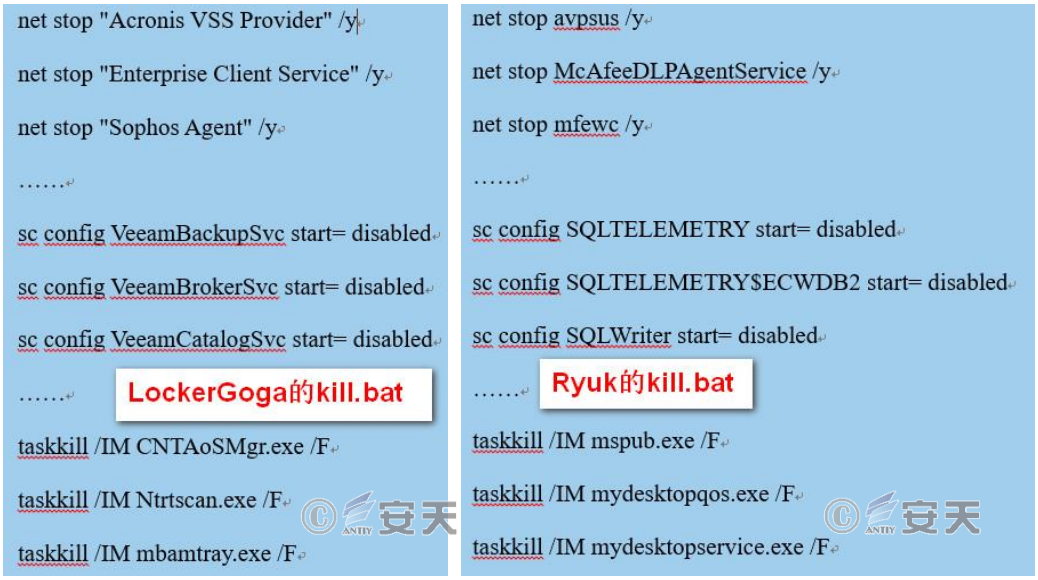


图 2-5 LockerGoga 和 Ryuk 的 kill.bat 对比

2. 根据所捕获的 IP 来看，二者在攻击过程中都使用了 Cobalt Strike/Powershell Empire/meterpreter。

3. 二者勒索信有多处相似之处。

(1). LockerGoga 勒索信中的联系邮箱多为***@protonmail.com 和***@oz.pl，Ryuk 在勒索信中的联系邮箱为***protonmail.com 和***@tutanota.com。

(2). 勒索信部分内容对比。

图中黄色部分为相似之处。

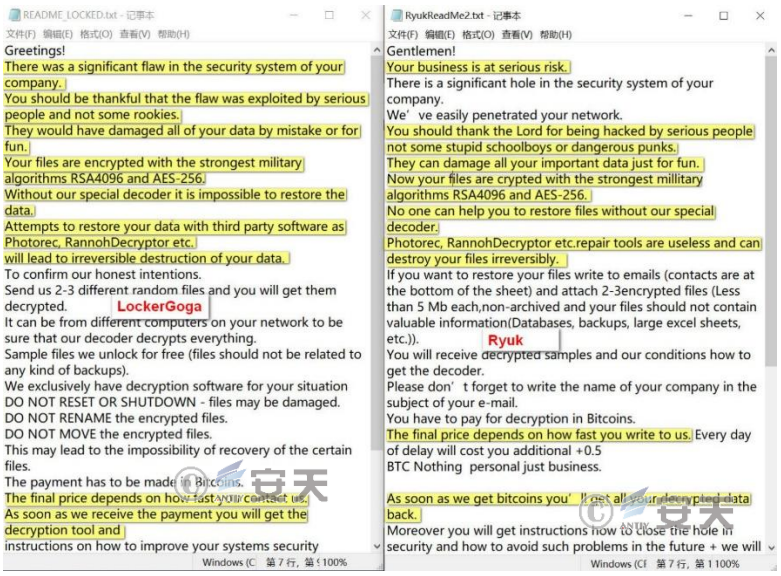


图 2-6 LockerGoga 和 Ryuk 勒索信部分对比

这里值得注意的一点是，尽管 FIN6 组织将目标转向定制化的勒索活动，但并没有放弃针对 POS 系统的攻击。在 2019 年 2 月 27 日 MORPHISEC 实验室发布的《针对 POS 系统的全球攻击》报告中[6]，涉及近期 FIN6 组织针对 POS 系统的攻击事件，而针对 POS 系统攻击活动中的相关 IP 与 FIN6 组织入侵工业产业并部署 LockerGoga 活动中的 IP 存在部分重合。

表 2-4 针对 POS 系统攻击活动相关 IP 与 LockerGoga 重合部分

状态	报告中提到的 C2	是否与 LockerGoga 相关 IP 重合	IP 信息最后一次修改时间
有效	http://89.105.194.*:443/Xaq2	是	2017-08-15
	http://46.166.173.*:443/Qq9a	是	2015-04-21
失活	http://185.202.174.*:443	是	2018-11-27
	http://185.202.174.*:443/c9Fz	是	2018-11-27
	http://93.115.26.*:443	是	2018-03-28

经过验证，这些 IP 的 whios 信息在近一年没有更改，因此，可以判定 IP 的所有者没有更改。同时报告中所展示的 poweshell stager 与 LockerGoga 事件中攻击者所使用的 stager 为同一类型，详见图 3-3。报告中也提到了这些特征属于 FIN6 组织（WMI/PowerShell、FrameworkPOS、横向移动和权限提升）。

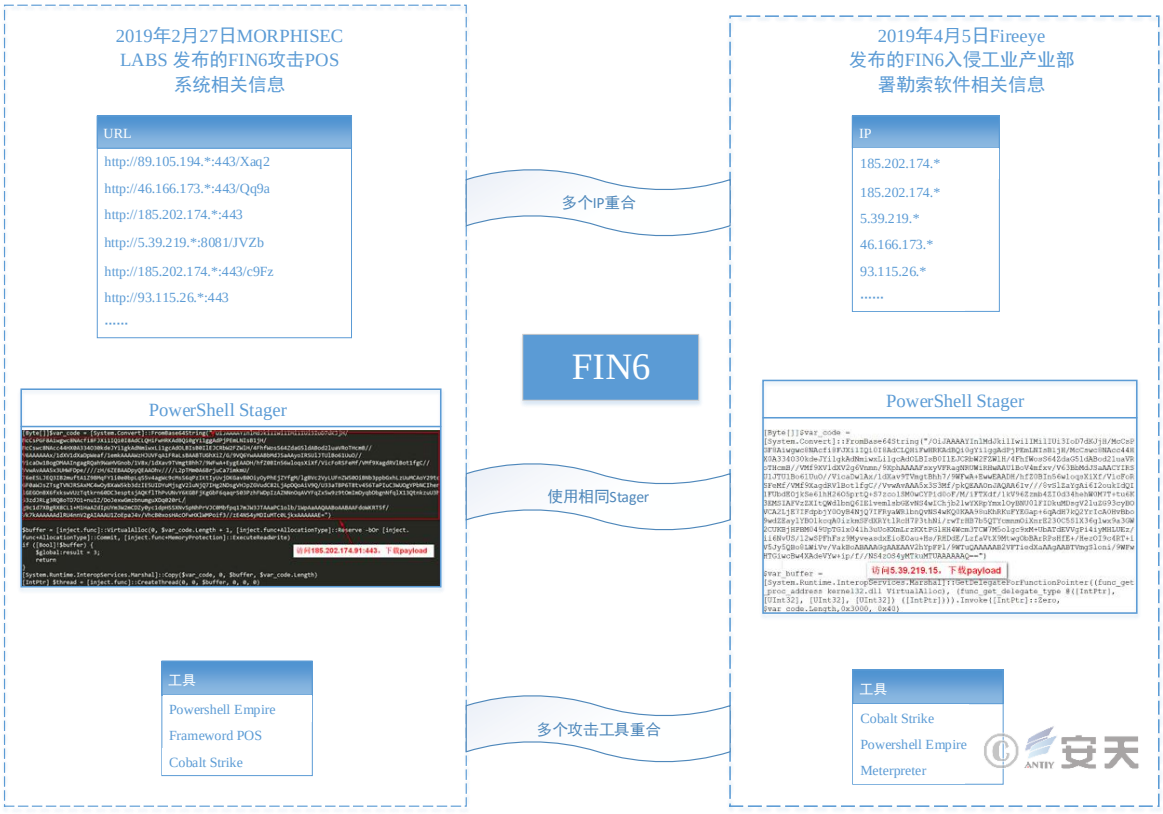


图 2-7 针对 POS 与勒索软件的关联分析

综上所述，攻击者运营 LockerGoga 的动机（向大型企业勒索比特币获利）、战术（防御规避、账户发现、横向移动）、技术（powershell 脚本下载 payload、使用 psexec 分发勒索软件并运行、使用 kill.bat 进行防御规避）、以及过程（详见图 3-4）都与 Ryuk 十分相似，因此安天 CERT 可以确定 LockerGoga 和 Ryuk 的运营者为同一组织，并将其归因于 APT 组织 FIN6。

2.5 FIN6 组织攻击流程/链路

随着 FIN6 组织勒索活动策略和技术的提升，目前已经无需借助其他装备进行勒索软件的传播。近期的活动中，攻击者利用暴露在互联网中的服务器作为攻击入口，利用外网服务器远程登录到内网服务器，借助开源渗透工具实现内网横移，向内网主机分发勒索软件，并使用有效签名规避反病毒监测和多进程技术规避沙箱检测。

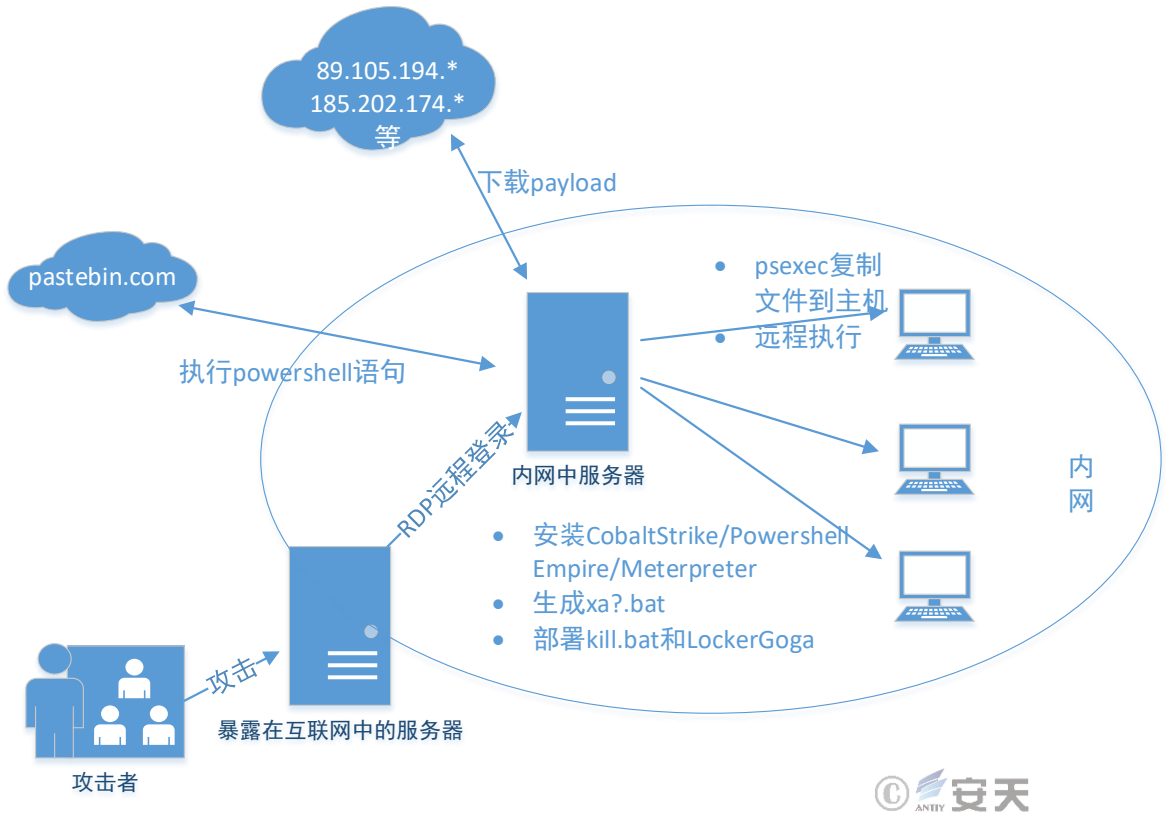


图 2-8 FIN6 组织攻击流程/链路

攻击者在远程登录到内网服务器后，会安装 Cobalt Strike、Powershell Empire 以及 Meterpreter 来辅助攻击。攻击者利用提前存储在 pastebin.com 上的 powershell 命令，下载 payload_1。Powershell 所执行的命令经过压缩和 base64 编码，解密后如下图所示。该命令由 Invoke-

SMBWmi.ps1(https://gist.github.com/rvrsh3ll/7c2ece5f8d097fbe4c7a)修改而来，功能为利用 powershell 执行 payload。payload_1 又继续下载 payload_2，由于 payload_2 大小为 0 字节，因此并未追踪到最终结果。

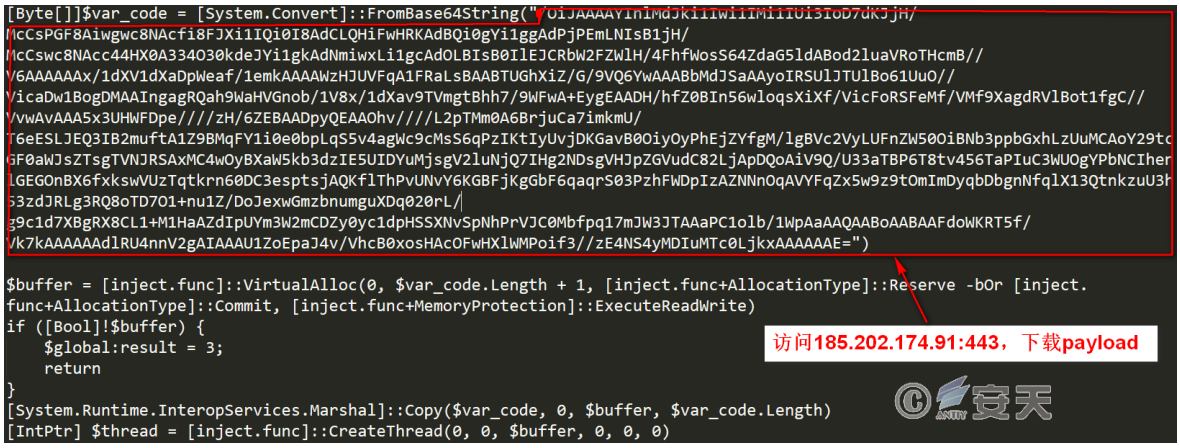


图 2-9 解密后的 powershell 命令

攻击者会使用 Adfind 查询并收集活动目录（Active Directory）中存储的网络对象相关信息（包括用户名、主机名、子网以及组等）。

```
adfind.exe -f (objectcategory=person) >    ad_users.txt

adfind.exe -f objectcategory=computer > ad_computers.txt

adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt

adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt

adfind.exe -f "(objectcategory=group)" > ad_group.txt

adfind.exe -gcb -sc trustdmp >    ad_trustdmp.txt

7.exe a -mx3 ad.7z ad_*
```

攻击者利用从活动目录中收集到的信息和一些已经掌握的口令信息，生成针对特定主机的批处理文件 xa?.bat(xab.bat、xac.bat 等)。批处理文件中命令如下。

```
start copy svchost.exe \\10.1.1.1\c$\windows\temp\start psexec.exe \\10.1.1.1 -u domain\domainadmin -p "password" -d -h -r mstdc -s -accepteula -nobanner c:\windows\temp\svchost.exe
```

该命令将 svchost.exe（勒索软件）拷贝到目标主机的共享文件夹 c:\windows\temp\start，再利用 psexec.exe 连接目标主机，使用参数-r 指定 psexec 创建的服务名为 mstdc（系统服务），然后运行勒索软件程序，加密目标主机文件。

注：psexec 通过指定的账户口令连接到远程主机，创建并启动 psexesvc 服务，psexesvc 服务会创建新的命名管道，psexec 连接至 psexesvc 创建的管道，将账号、口令以及要执行的命令发送至管道，psexesvc 从管道接收这些信息，创建新的会话，执行命令[7]。

在部署勒索软件之前，攻击者会先在目标主机上执行 kill.bat（MD5: 595a37f59f4fe020876d4e1329e167d6），结束文档编辑器、数据库、邮箱客户端以及游戏客户端等常见进程，停止备份相关服务，停止反病毒引擎相关服务。kill.bat 如下。

```
net stop "Acronis VSS Provider" /y

net stop "Enterprise Client Service" /y

net stop "Sophos Agent" /y

……

sc config VeeamBackupSvc start= disabled

sc config VeeamBrokerSvc start= disabled

sc config VeeamCatalogSvc start= disabled

……

taskkill /IM CNTAoSMgr.exe /F

taskkill /IM Ntrtscan.exe /F

taskkill /IM mbamtray.exe /F
```

3 FIN6 组织针对性勒索活动的过程

FIN6 组织攻陷内网之后，会在内网中部署勒索软件，本小节以 LockerGoga 为例，阐述勒索软件的运行过程。LockerGoga 勒索软件会根据不同的参数执行指定的操作。

表 3-1 LockerGoga 根据不同的参数执行不同的操作

无参数	将自身移动到临时文件夹，重命名为 originalname{4 个随机数字}.exe，以参数-m 启动移动后的文件，在桌面上写勒索信。
-m	以主进程的方式启动，创建互斥量<MX-originalname>，创建命名共享内存<SM-originalname>，遍历文件，收集文件列表信息，注销会话，修改管理员和普通用户口令，以参数-s 创建多个自身子进程。
-s	以子进程的方式启动，从共享内存读取要加密的文件路径，加密文件。
-i	进程间通信。
-l	在根目录下创建日志文件。

3.1 提升自身权限，修改管理员口令，禁用网络适配器

LockerGoga 以不同参数运行后都会进行提权操作。在使用参数-m 启动后，会创建进程 logoff.exe 来进行会话注销，使用 net.exe 修改管理员账户口令以及其他用户口令，新口令为“HuHuHUHoHo283283@dJD”。在加密完成后枚举 WiFi 和以太网适配器，并试图禁用适配器来阻断主机与外网的连接。

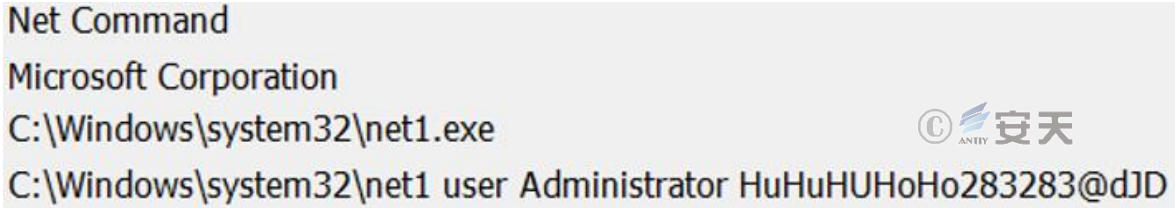


图 3-1 修改管理员账户口令

3.2 使用 AES 算法加密文件，删除系统日志

LockerGoga 以参数-m 启动后，会遍历文件，收集文件列表信息，然后以参数-i SM-originalname -s 创建自身子进程，使用子进程进行加密。其中 SM-originalname 为共享内存命名，本例中为 SM- tgytutrc，样本通过创建共享内存的方式，从父进程向子进程传递要加密的文件路径。

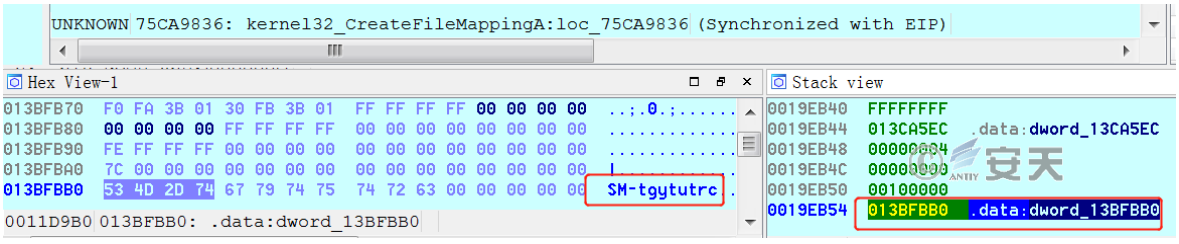


图 3-2 创建共享内存

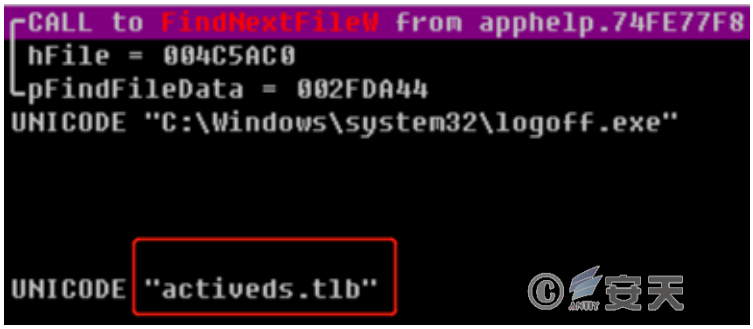


图 3-3 获取文件列表

以参数-i SM-originalname –s 启动的进程会判断互斥量 MX-originalname 是否存在，若不存在则程序退出。子进程会从共享内存中读取 base64 编码的文件路径，解码后执行加密操作。样本使用 AES 算法加密文件，利用随机数生成 AES 密钥和初始化向量(IV)，使用硬编码在样本中的 RSA 公钥加密 AES 密钥相关信息。样本中虽硬编码了文件类型，但实际加密过程中并未只加密硬编码在样本中的文件类型。使用 RSA 公钥加密数据的结构如下。

表 3-2 RSA 公钥加密数据的结构

00 00 00 00(4 字节)	16 字节 AES IV	16 字节 AES key	goga（4 字节）

```
sub_409C80(
  &v155,
  (int)" MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDLscAMf6QMU0OLT967Q0oMVN/9xRbC6Ymz HVVE05zgpDJRQQLmPPYcPnehaeynF8HGFYb"
       "RIEaD0pk4WZwGPLtcRaYuQS1M6v+2j4Vp8faA woNdi7+jI2xw0kQao29FJ8WUQDvrPqODALf8bjiOIO7f1Nc5g9vOEbWyCA1w/vbaVwIBEQ==",
  219,
  0);
```

图 3-4 RSA 公钥

加密后的数据会附加在加密文件结尾，结构如下。

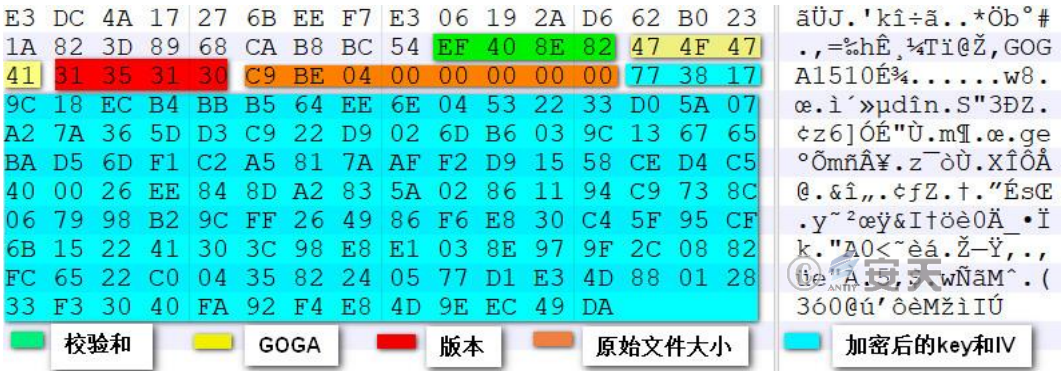


图 3-5 被加密文件尾部结构

LockerGoga 会使用 wevtutil.exe 清除 windows 事件日志，语句如下。

```
"C:\Windows\System32\wevtutil.exe" cl Microsoft-Windows-WMI-Activity/Trace
```

3.3 规避检测

3.3.1 使用有效签名

LockerGoga 的样本使用了有效的数字签名来规避反病毒引擎检测，涉及到的数字签名如表 4-2 所示。在这些签名未被撤回之前，LockerGoga 在 VT 上的检出率极低。

表 3-3 LockerGoga 使用的数字签名

MIKL LIMITED	Issuer	COMODO RSA Code Signing CA
	Serial number	3D 25 80 E8 95 26 F7 85 2B 57 06 54 EF D9 A8 BF
ALISA LTD	Issuer	Sectigo RSA Code Signing CA
	Serial number	5D A1 73 EB 1A C7 63 40 AC 05 8E 1F F4 BF 5E 1B
KITTY'S LTD	Issuer	Sectigo RSA Code Signing CA
	Serial number	37 8D 55 43 04 8E 58 3A 06 A0 81 9F 25 BD 9E 85

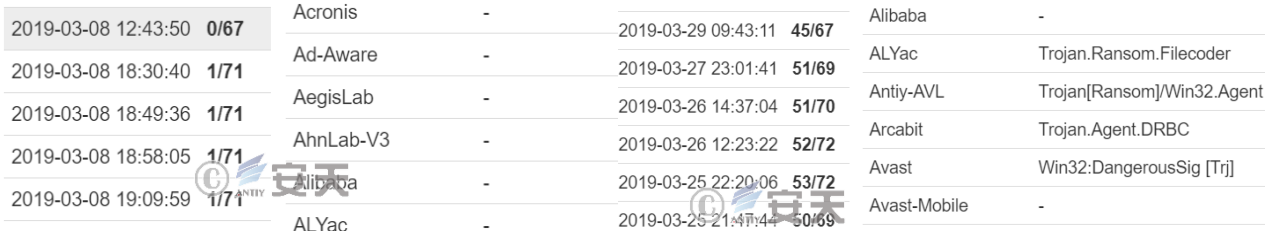


图 3-6 数字签名有效时 VT 检出率

3.3.2 使用多进程加密文件

一些基于沙箱的检测系统对系统中进行写入操作的文件数量设置了一定的阈值，会监视进行写入操作的文件的数量并会将这些文件的扩展名进行关联。若 LockerGoga 使用同一进程进行文件加密操作，则极大可能会超过上述的阈值，并且其写入的文件扩展名都为“.lock”，很容易被该类沙箱视为异常操作。因此，LockerGoga 使用多进程加密文件可能绕过该类检测技术[8]。

单个进程对大量文件进行加密时，会产生大量的 I/O 请求，可能会被基于过量 I/O 操作的检测系统检测到。LockerGoga 使用多个进程进行加密操作，并且每个进程只加密少量的文件，控制了单个进程发出 I/O 请求的数量，便可以绕过该类检测技术[8]。

4 安天针对勒索软件的解决方案

4.1 防护建议：多维布控

安天建议企业客户针对勒索软件类的安全威胁防护可从预警、防御、保护、处置和审计几个步骤来进行有效防御和处理，保护系统免受攻击。

- 将未知应用程序进行特征检测鉴定，对勒索行为进行动态实时监控，及时发现恶意程序与勒索行为并进行阻断。
- 企业将具有重要价值的文件资源的主机设置为重要计算机或受限计算机，一旦勒索软件或其它可疑程序运行时，可以通过可信应用基线（白名单）检测的方式及时将其发现，并予以阻止。
- 可采用安全文档措施保护具有重要价值的文件。
- 通过云端追溯功能来对勒索软件进行全网追查，便于事后审计和定损。

4.2 安天智甲：有效防御

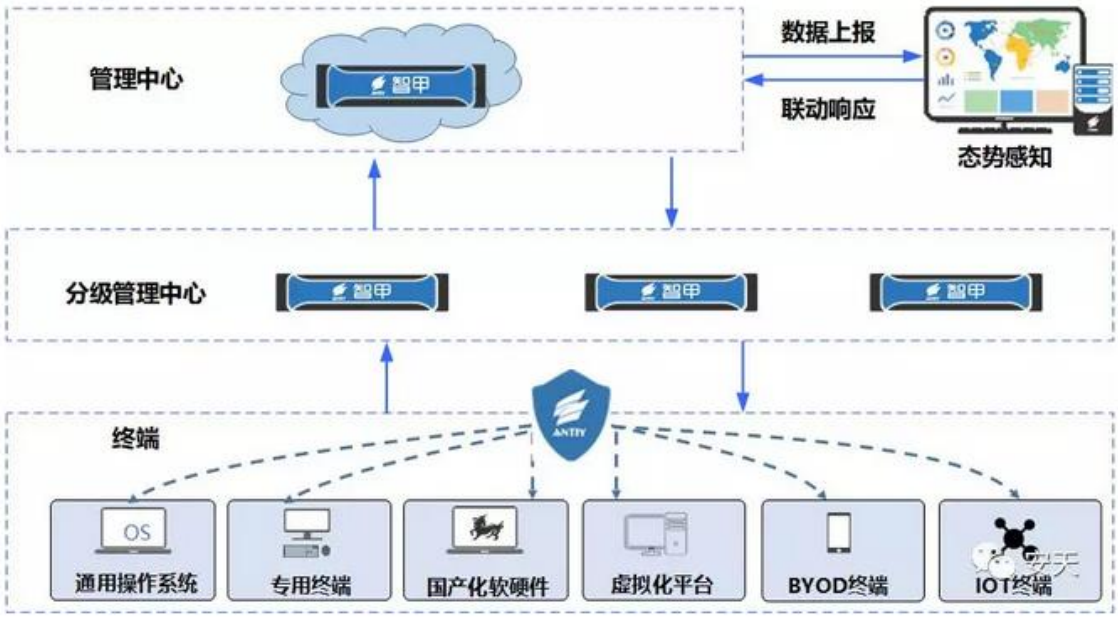
安天智甲具有国际和国内领先的多维度勒索软件防御技术，内置安天自主研发的下一代威胁检测引擎，具有实战化处置勒索软件的能力，可对勒索软件进行向量级拆解。其具有特有的勒索软件行为模型库，结合安天下一代威胁检测引擎输出的向量拆解结果，构筑了一套有效识别未知勒索软件的检测机制。安天智甲采用终端边界防御、行为动态监控、主动防御、文档保护的多维防护机制进行勒索软件防护，在不依赖文件哈希检测的情况下，也能有效阻止勒索软件的勒索行为，有效防御能力可达到 98%。

图2 安天智甲有效防护FIN6攻击活动

5 安天智甲简介

安天智甲是一款面向政府、军工、能源、金融、交通、电信等各行业用户的企业级防护产品，产品集成了病毒检测查杀、系统加固、主动防御、介质管控、文档保护、行为画像等功能，并能有效与管理中心和安天态势感知产品互动，协助客户建立更全面的资产防护体系和风险认知能力，使态势感知能够有效落地。

5.1 安天智甲：更全面的场景应用—多场景支持、满足差异化需求



安天智甲不仅是一款终端防护产品，还能够以资产保障和威胁认知为视角，以形成有效的资产深度普查和端点画像为能力输出，并将数据同步至安天态势感知平台中，让用户对整个端点的资产一览无余。

5.2 安天智甲：更广阔的适配性—全面兼容国产化系统

5.3 安天智甲：更强大的功能—不仅仅是反病毒

5.4 安天智甲：更精准的威胁感知——3D 可视化拓扑、感知全局态势

终端威胁详情展示

网络拓扑结构展示

6 总结

从 FIN6 组织近期的攻击活动来看，其不仅在实施针对 POS 系统的攻击活动，同时也在运营勒索软件攻击活动。因此目前还不能简单给出 FIN6 组织的目标已经从 POS 系统逐渐转移到勒索活动这样的结论。不论是 Ryuk 勒索活动，还是 LockerGoga 勒索活动，FIN6 组织都能够准确地定位目标，对目标网络中的关键信息系统实施定制化的勒索攻击，致使受害者蒙受巨大的经济和声誉损失。因此，大型企业或组织应该高度警惕和重视利用勒索软件实施的针对性勒索攻击，对于绑架用户数据的勒索软件而言，若没有可靠的事前防御和检测能力，面对已经被勒索软件加密的用户数据，侧重于保护系统安全的反病毒软件也无能为力。只有安装专门针对保护数据安全的工具或部署针对企业安全特点的安全产品，才能避免给勒索软件以可乘之机。安天建议企业客户除了及时进行漏洞修复，不要随意打开邮件附件之外，还要使用安全防护软件如安天智甲进行有效防护。

附录一：参考资料

[1] Crowdstrike :Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

[2] Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-FIN6-intrusion.html

[3] Bleepingcomputer :New LockerGoga Ransomware Allegedly Used in Altran Attack
https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/

[4] Techcrunch :UK’s Police Federation hit by ransomware
https://techcrunch.com/2019/03/21/police-federation-ransomware/

[5] Motherboard :Ransomware Forces Two Chemical Companies to Order ‘Hundreds of New Computers’
https://motherboard.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers

[6] Morphisec :NEW GLOBAL ATTACK ON POINT OF SALE SYSTEMS
https://blog.morphisec.com/new-global-attack-on-point-of-sale-systems

[7] Paper：老牌工具 PsExec 一个琐碎的细节

https://paper.seebug.org/503/

[8] Mcafee ：LockerGoga Ransomware Family Used in Targeted Attacks

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/lockergoga-ransomware-family-used-in-targeted-attacks/