360数字安全
数字安全的领导者

勒索软件家族介绍

LockBit 4.0

360数字安全集团高级威胁研究分析中心
（CCTGA勒索软件防范应对工作组成员） 编

目录 | CONTENTS

01 勒索软件流行态势概述

勒索软件自 2015 年出现以来始终处于一种高歌猛进的态势。根据 360 数字安全集团高级威胁研究分析中心编写的《2023 年勒索软件流行态势报告》指出，勒索家族的核心加密功能进一步同质化，2023 年新增的主流勒索软件家族均无法通过技术手段解密，RaaS 模式成为更为普遍的运营模式。双重勒索或多重勒索模式的赎金索求逐渐成为主流，支付赎金的受害者比例有所增加。

双重/多重勒索软件所勒索的赎金金额通常集中在 10 万~100 万美元的区间内，这一区间的赎金金额占比超过 7 成；而窃取的数据量则大部分在 10G 以上，更有超 2 成案例窃取了 500G 以上的数据，而被盗数据中又以财务数据和个人隐私数据为主。

而国内的勒索软件的攻击事件也此起彼伏，国内流行勒索软件家族以 phobos、BeijingCrypt 和 TellYouThePass 为主，这三大勒索软件家族的反馈占比超过 51%。根据 360 安全云统计，2023 年共完成处理超 2750 例勒索软件攻击求助，

显示勒索软件攻击仍是不容忽视的威胁。全年勒索软件攻击的传播态势平稳，但大型企业受到的攻击有增无减，勒索软件家族针对大型企业采取更具针对性的攻击策略。

02 LockBit 勒索软件家族简述

LockBit 勒索软件家族，最早于 2019 年 10 月被发现，又被称作“ABCD”、“LockBit2.0”、“LockBit3.0”勒索软件。在 2024 年 4 月，该家族更新为“LockBit4.0”。也有人认为该家族是由“LockerGoga”和“MegaCortex”家族演变而来，采用 RaaS（勒索软件即服务）模式进行运营。

受到该家族勒索攻击的受害者通常被可分为两类：

第一类受害者通常为大中型企业或组织。攻击者会对这类受害者发起有针对性的攻击，还会在部署勒索软件之前先从受害者内部网络中窃取大量敏感数据作为威胁受害者支付赎金的重要筹码；

第二类受害者通常为小型企业或个人 PC。攻击者对此类受害者采取的往往是“撒网式”攻击，并且一般不会对此类受害者进行数据的窃取，而仅仅是加密其文件。

家族演变时间线

2019 年 10 月，LockBit 勒索软件被首次发现，并一跃成为当年针对工业领域最活跃的勒索软件之一。

2021 年 7 月中旬，LockBit 团伙在消失 6 个月后宣布版本升级，正式更新为 LockBit2.0 版本。

2022 年 6 月，LockBit 借鉴 BlackMatter 勒索软件代码，发布其 3.0 版本该版本，该版本又被称为 LockBit Black。

2024 年 2 月，FBI 与欧洲刑警组织等多个国家组织联合行动，对 LockBit 进行了打击，破坏了其基础设施并抓捕了其人员。

2024 年 2 月，FBI 行动一周后，LockBit 再次回归，并对 FBI 等的行动成果予以否认。

2024 年 4 月，LockBit 更新至 4.0 版本，LockBit 3.0 的生成器被公开。LockBit 家族正式进入 4.0 时代与后 3.0 时代。2024 年 4 月后，LockBit3.0 勒索软件的攻击行为开始失去家族特征，成为一类通用的加密载荷。

家族特点

- **针对高价值目标**

  威胁程度最高的勒索组织，攻击过数百家大型机构，以窃取数据而闻名。

- **多重维度攻击**

  其攻击维度囊括了利用未修复的漏洞、钓鱼邮件、社交工程策略等；尤其擅长漏洞攻击，并主要外围攻击目标为 VPN 网关等设备。

- **快速加密**

  加密速度快，其制作团队甚至自称是全世界加密最快的勒索软件。

- **快速窃取数据**

  窃取数据速度快，该勒索软件可在 20 分钟内窃取到约 100GB 数据。

- **自我传播能力**

  具备在域控内自动传播能力。双重勒索，攻击时会窃取数据，并以泄露数据为要挟。

- **自诩网络安全团队**

其幕后运营团队将自己标榜为“网络安全团队”。

◆ **多平台加密**

跨多个操作系统进行加密。不仅包括 Windows、Linux、MacOS 等各种版本操作系统，还针对 KVM 等虚拟机平台，并且还能够对 NAS 存储设备实施加密。这一能力也使其成为了一种多平台威胁。

◆ **多变种**

由于 LockBit2.0 源码的泄露以及 LockBit3.0 构建器被公开，导致基于该家族勒索软件派生出了众多的变种勒索软件。

勒索活动特点

对过往 LockBit3.0 勒索软件家族的活动统计，LockBit 勒索家族在索要赎金时表现出一定的倾向性，其通常会根据受害者的规模和被窃取数据的价值来调整赎金金额。对于一般受害者，他们更倾向于索要中等数额的赎金，而对于中大型企业,会基于受害者支付能力和数据敏感性的进行考量，甚至可能会索要高达上千万美元的赎金。下面是一个简要的统计情况：

赎金范围	占比
<10 万美元	10.6%
10 万美元~100 万美元	70.7%
100 万美元~1 千万美元	15.4%
>1000 万美元	3.3%

对监测到的 LockBit 数据窃取案例进行总结，以数据量为维度，发现被窃取数据量主要分布在 10GB 到 100GB 之间，次之是 100GB 到 500GB 之间。

数据量范围	占比
<1GB	2.6%
1GB~10GB	13.5%
10GB~100GB	36.7%
100GB~500GB	32.8%
>500GB	14.4%

03 LockBit 勒索软件家族技特点及信息

家族基本信息

下表给出了 LockBit 勒索软件家族的基本信息。

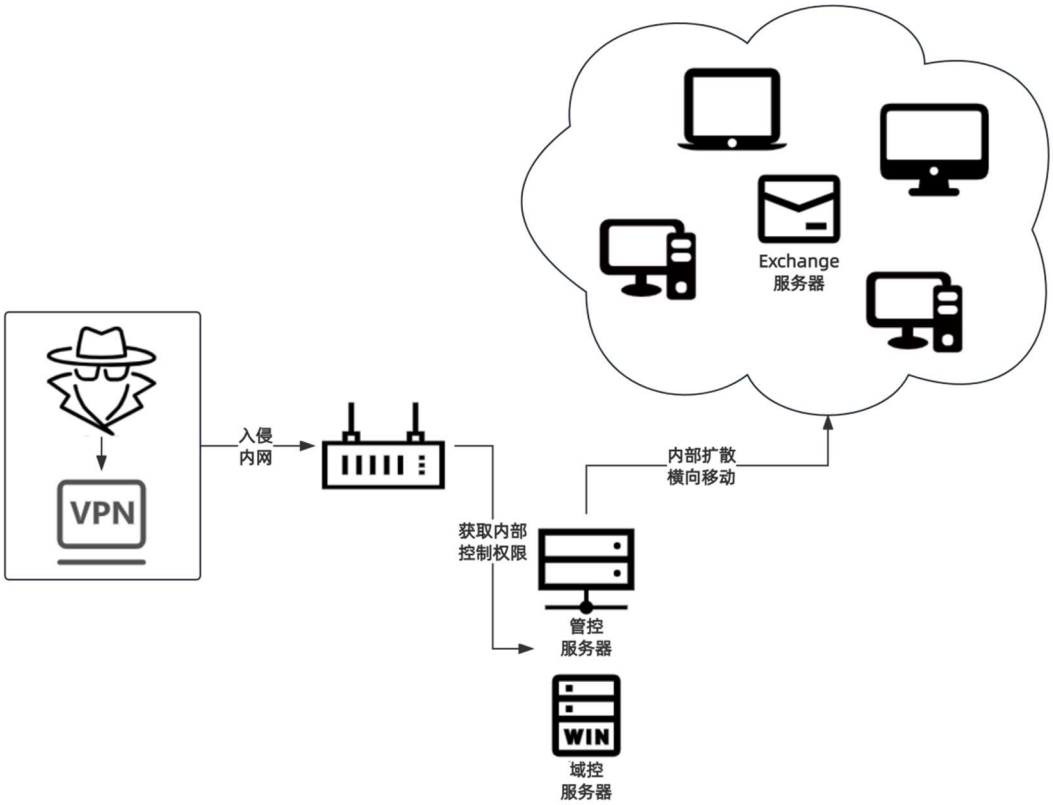
感染平台	Windows / Linux / MacOS / KVM / NAS
勒索信文件	#Read-for-recovery.txt / xxxxxxxxx.README.txt
联系邮箱	LockBitdecrypt@msgsafe.io LockBitdecrypt@onionmail.org
加密扩展名	LockBit / 9 位随机字符
支持解密	否
是否窃取数据	是
主要目标行业	制造业、能源、教育、政府、互联网及软件、文娱传媒、社会组织、服务业
攻击地区	全球

下表给出的则是 LockBit 勒索家族的一些基本技术信息。

加密算法	Chacha20 / RSA1024
武器库	PsTools 工具集 / ntdsutil / PuTTy / Cobalt Strike LockBit-0.1 / PCHunter / PowerTool Process Hacker / ScreenConnect / PowerView CrackMapExec / GMER / HrWord / LaZagne MEGAsync / Minikatz
其它辅助程序	PowerShell.exe / PsExec.exe / mstsc.exe PuTTY.exe / PortStarter / secretsdump ntdsutil.exe / AnyDesk / wevtutil.exe
典型漏洞利用	CVE-2023-4966 / CVE-2021-21974 CVE-2023-20269 / CVE-2023-27350 CVE-2023-27351 / CVE-2023-22515 CVE-2024-1708 / CVE-2024-1709

攻击手段及步骤

LockBit 属于 RaaS 类勒索组织，此类运营模式的勒索组织往往在一个顶层团队下存在众多具体实施攻击及部署工作的下属团伙。故此，常见的勒索软件攻击手段在 LockBit 的攻击案例中均有出现。但一般来说，针对中大型企业的攻击手段通常较为固定，下图给出的便是其常规的攻击路径。



总结起来，LockBit 的攻击步骤大体上可划分为 5 个阶段。

1. 初始访问

在针对企业的攻击中，常见的初始访问目标包括：Web 服务器，Exchange 服务器，VPN 网关，远程桌面、虚拟桌面网关，失去维护但没有及时废弃的老旧设施，保护不当的员工电脑。在初始访问探测中，一般攻击者会选择探测企业暴露在

公网的各类资产，寻找防护薄弱点（如没有打补丁的设备），发起攻击。攻击一旦成功，攻击者会尝试在这个节点部署后门程序、后门账户、代理程序，为下一步攻击做准备。

2. 内网渗透横移

在拿到初始访问节点后，攻击者将开始探测内网，寻找同样存在弱点的主机，实施攻击，攻击者会格外关注文件共享服务器，内网网站数据库等高价值资源，并重点寻找关键设施实施攻击。

3. 拿下关键节点

常见的关键设施节点包括：管理员计算机，域控服务器，IT 管理平台，安全产品控制台等权限较高的控制端。 常见攻击方法包括口令暴破，漏洞攻击。

4. 大范围控制设备

在获取到管控平台权限后，利用管控平台，对旗下管理的所有设备实施控制。如利用域控下发窃密程序，投递勒索。这个过程一般发生在凌晨，黑客通常选择无人值守的时间段发起这一攻击。

5. 窃取数据与投毒

攻击者在控制一定数量的信息系统设备后，就会开始发起勒索攻击。针对中大型企业，一般会选择先窃取数据，再发动勒索的方式。

下表中给出的则是 LockBit 运营者在内网渗透过程中所常用到的一些漏洞信息。

漏洞编号	涉及产品/应用/服务/设备	漏洞类型
CVE-2023-22515	Atlassian Confluence	身份验证漏洞
CVE-2023-4966	Citrix Gateway Citrix NetScaler ADC	缓冲区溢出漏洞
CVE-2021-21974	VMware ESXI	堆溢出漏洞
CVE-2023-20269	Cisco ASA / Cisco FTD	未经授权的访问漏洞
CVE-2023-27350	PaperCut	不当访问控制漏洞
CVE-2023-27351	PaperCut	用户账户数据漏洞
CVE-2024-1708	ConnectWise ScreenConnect	路径遍历漏洞
CVE-2024-1709	ConnectWise ScreenConnect	身份绕过漏洞

LockBit3.0 现状现状

自 2024 年 2 月 LockBit 被 FBI 牵头的多个执法部门联合打击之后不久，LockBit3.0 生成器便被泄露。在此之后，360 安全大脑捕获到大量 LockBit3.0 的各类变种。因此，LockBit3.0 的传播逐渐失去了其原本的家族特征，演变成为各类黑产团伙使用的通用攻击工具。

比如在下图的案例举例，其勒索提示信息内使用繁体中文要求受害者向指定的比特币钱包地址汇入 0.02BTC 作为解密文件的赎金。

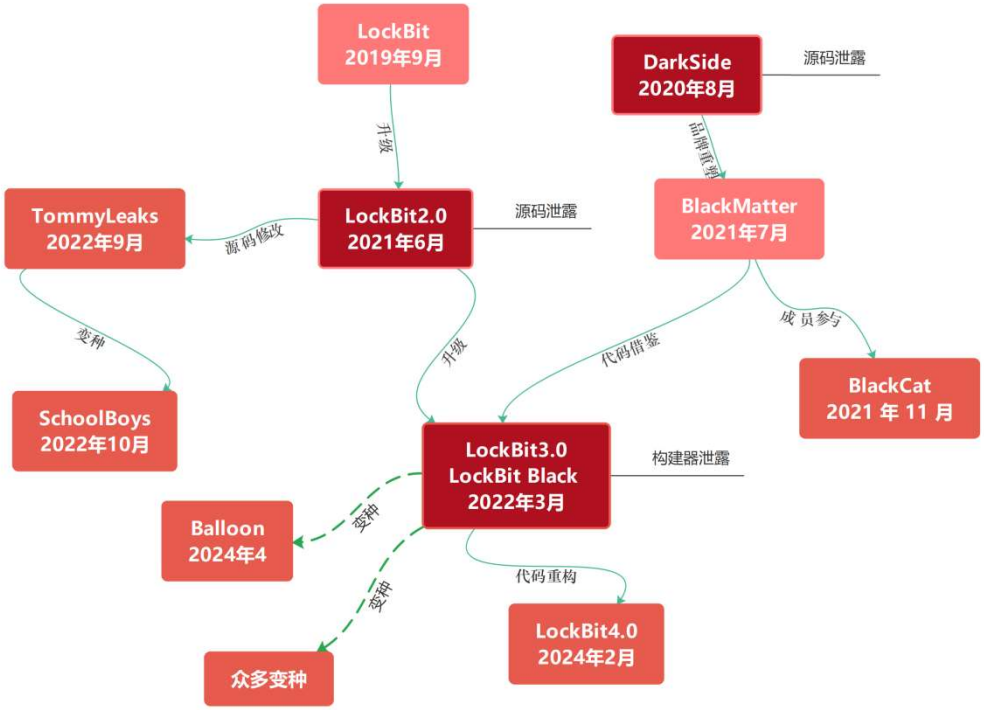
```
>>>> 我们是一个善良的黑客组织，您的资料已被窃取并且加密，
您需要支付价值人民币一万元的比特币0.02BTC给我们帮您解密被加密文件。
如果您不支付赎金我们也会给您解密所有文件，请在一个礼拜后联系下面的邮箱，我们会发送解密器给您解密所有文件
请不要担心，解密器是一定会解密所有被加密文件

>>>> 您需要聯絡我們並使用您的個人解密 ID  傳送一個被加密文件給我們，免費幫您解密一個文件

>>>> 發送ID和一個加密文件到：21512232318132@proton.me
>>>> 備用聯絡信箱： 3121651321321132@tutamail.com
>>>> 您的個人解密 ID：7D7894D19E2F9F68912407EE8AAF8EB5

要解密全部文件需要您支付：0.02BTC
比特币地址：19ZPm6ybmGoUdaqPvcfQHz7o7SWCPJcQ1b

TOR网站可以看到您泄露的秘密：http://h3osabcqrbkutyrh77nptes44pqzldj5rk5mxnv46mmrapesp565bsyd.onion/
您可以透過：幣安/火幣，歐易等虛擬貨幣交易所購買比特幣支付，這是一個很方便的過程！

寫信聊天並等待答复，我們將始終答复您。
有時您需要等待我們的答复，因為我們攻擊許多公司。

>>>> 警告！ 不要删除或修改任何文件，這可能會導致恢復問題！

>>>> 警告！ 如果您不支付贖金，我們將再次多次攻擊您的公司！
```

同时开始扩散的还有 LockBit3.0 的解密器。但遗憾的是遭到泄露的解密器只能解密被特定版本 LockBit 加密的文件。由于不同加密程序所使用的公私钥对不同，导致解密器无法做到通用解密。

LockBit4.0 诞生

在执法行动事件之前，LockBit 就被监控到正在秘密开发一个名为 LockBit NG Dev

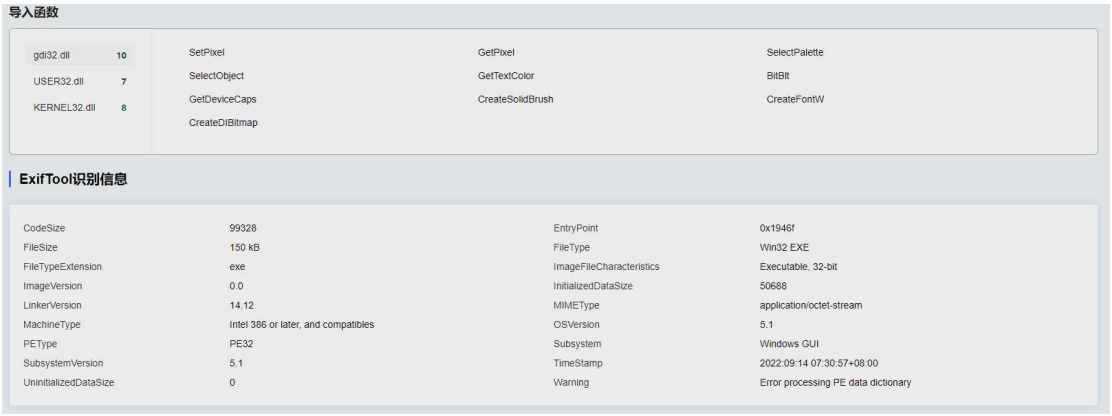
的恶意软件开发项目（NG 意为 Next Generation，即“下一代”）。而在被联合打击后不久，基于该项目的新版勒索软件 LockBit4.0 便正式推出。根据 LockBit 团伙的宣传，此次 4.0 版本使用.NET 对 LockBit 的代码进行了重构。不过 360 安全大脑也监测到了使用 C++创建的 4.0 版本。



LockBit4.0 与 LockBit3.0 的对比分析

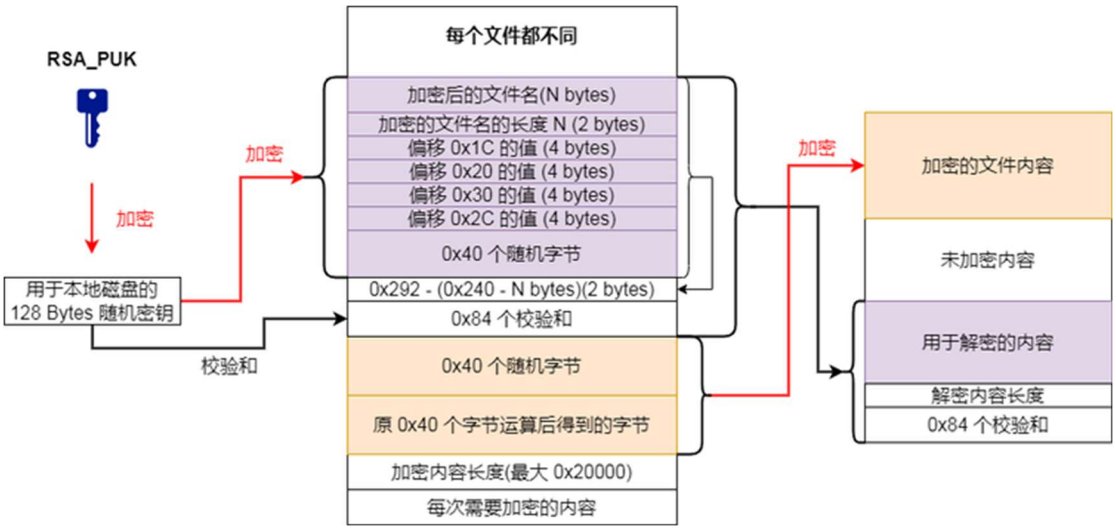
病毒结构

LockBit4.0 勒索软件使用 Windows 32 位可移植可执行文件（PE）。包括了 3.0 的一些特性如：自脱壳、反调试、绕过 UAC 提权、多线程加密等操作



加密过程

LockBit4.0 仍然使用 RSA 结合 Salsa-20 的方式对文件进行加密，使用二层加密方式，下图为该版本 LockBit 的加密流程。



获取到的 LockBit4.0 样本和此前的 3.0 样本本质上并没有太大的区别，其中一些配置存在些许变化。

```
decryption id: "23635679E8E94A14"
guid: "{7F788721-CD4C-3841-436D-C74851E34BD7}"
ransom ext: ".xa1Xx3AXs"
ransom note name: "xa1Xx3AXs.README.txt"
bot_id: "26db217cf53242eaa29c2201486ab17d"
mutex name: "Global\7c21db26ea4232f501229ca27db16a48"
uid: "3130000000000000000000000000000000"
```

配置信息使用了 APLib 进行压缩,解压缩后包含 RSA 公钥、掩码等，还包括自定义 Base64 的编码数据。

而 4.0 版本内置的 RSA 公钥为：

AQABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAjY1Z56OlKFMAYvC
8NjHhkHAFF3+QoaqUZKjr6nlS9UbQfcVIsbrkjfP1UFjhcKB1L8qgVN
F1xsQDr+smftC4xlaZ3882jzv7WJ+ihBZjorKyBiByhF64bAQzd7/XH
zcEGl0Uk6O0mCaI5S/SOh2ejkE9ExjVYI+QA/xO+/CpPcw==

配置说明

我们对 LockBit 4.0 的配置进行了解密，详细内容如下表所示：

配置字段	值	含义注释
encrypt_mode	auto	加密模式
encrypt_filename	FALSE	加密文件名
impersonation	TRUE	冒充
skip_hidden_folders	FALSE	跳过隐藏文件夹
language_check	FALSE	语言检查
local_disks	TRUE	本地磁盘
network_shares	TRUE	网络共享
kill_processes	TRUE	结束进程
kill_services	TRUE	结束服务

running_one	TRUE	单实例运行
print_note	TRUE	打印提示
set_wallpaper	TRUE	设置壁纸
set_icons	TRUE	设置图标
send_report	FALSE	发送报告
self_destruct	TRUE	自我销毁
kill_defender	TRUE	关闭杀软
wipe_freespace	FALSE	擦除空闲空间
psexec_netspread	FALSE	psexec 网络扩散
gpo_netspread	TRUE	gpo 网络扩散
gpo_ps_update	TRUE	gpo ps 更新
shutdown_system	FALSE	关闭系统
delete_eventlogs	TRUE	删除事件日志
delete_gpo_delay	1	删除 gpo 延迟

除上述基本配置字段外，还有一些较为重要的配置信息所对应内容如下：

- **white_folders - 文件夹白名单**

  $recycle.bin; config.msi; $windows.~bt; $windows.~ws; windows; boot; system volume information; tor browser; windows.old; intel; msocache; perflogs; x64dbg; public; all users; default; microsoft;

- **white_files - 文件名白名单**

autorun.inf; boot.ini; bootfont.bin; bootsect.bak; desktop.ini; iconcache.db; ntldr; ntuser.dat; ntuser.dat.log; ntuser.ini; thumbs.db; GDIPFONTCACHEV1.DAT; d3d9caps.dat;

- white_extens - 文件后缀白名单

386; adv; cab; cmd; com; cpl; cur; deskthemepack; diagcab; diagcfg; diagpkg; drv; exe ;hlp; icl; icns; ico; ics; idx; ldf; lnk; mod; mpa; msc; msp; msstyles; msu; nls; nomedia; ocx; prf; rom; scr; shs; spl; sys; theme; themepack; wpx;l ock; key; hta; pdb; search-ms;

- white_hosts - hosts 白名单

WS2019

- kill_processes - 进程清理列表

sql; oracle; ocssd; dbsnmp; synctime; agntsvc; isqlplussvc; xfssvccon; mydesktopservice; ocautoupds; encsvc; firefox; tbirdconfig; mydesktopqos; ocomm; dbeng50; sqbcoreservice; excel; infopath; msaccess; mspub; onenote; outlook; powerpnt; steam; thebat; thunderbird; visio; winword; wordpad; notepad; calc; wuauclt; onedrive;

- kill_services - 服务清理列表

vss; sql; svc$; memtas; mepocs; msexchange; sophos; veeam; backup; GxVss; GxBlr; GxFWD; GxCVD; GxCIMgr;

- impers_accounts - 弱口令列表

ad.lab:Qwerty!; Administrator:123QWEqwe!@#;

Admin2:P@ssw0rd;

Administrator:P@ssw0rd;

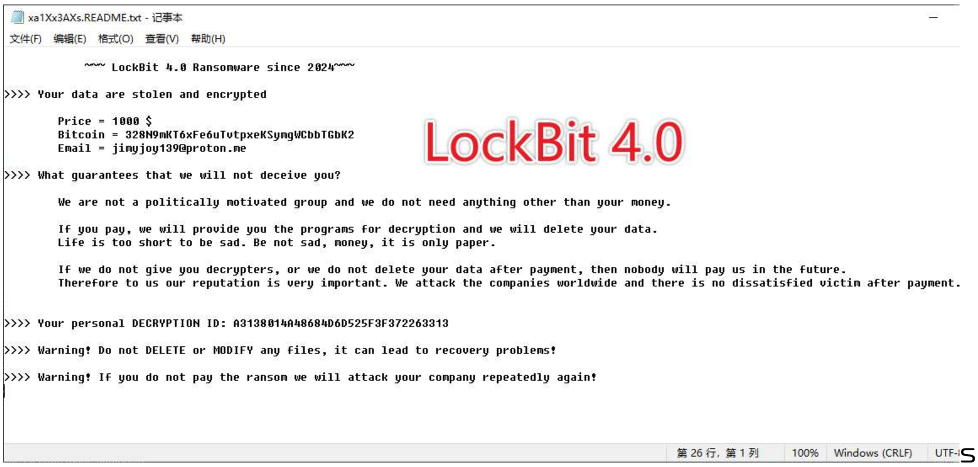
Administrator:Qwerty!;

Administrator:123QWEqwe;

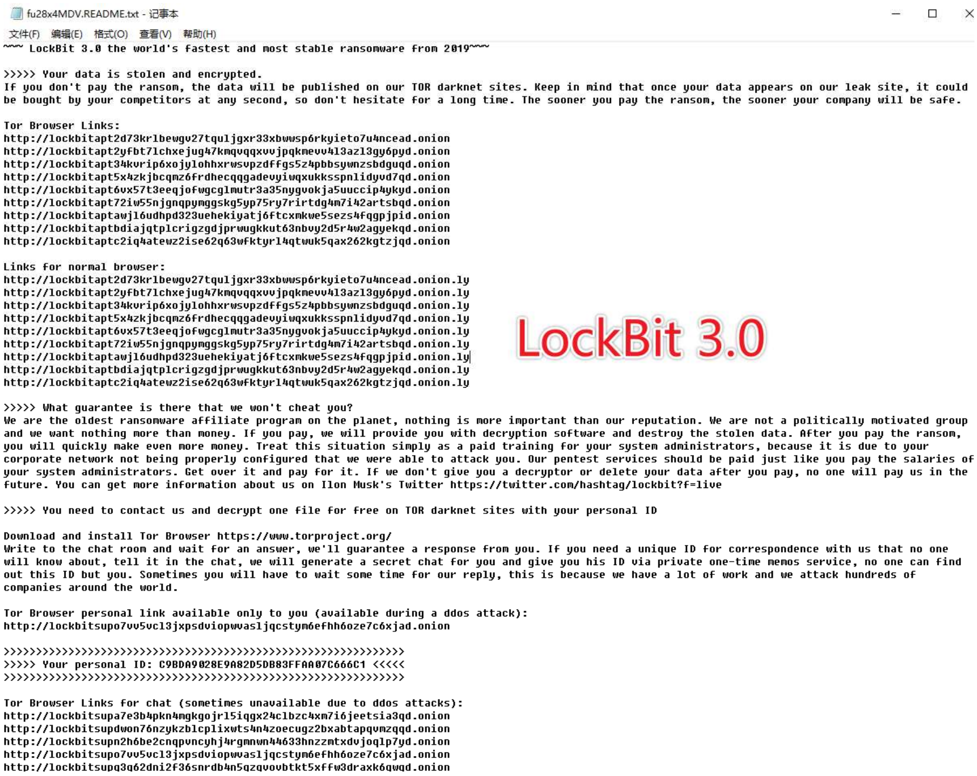
Administrator:123QWEqweqwe;

勒索方式

LockBit 要求受害者支付赎金并威胁称，除非支付赎金否则将公布窃取到的敏感数据。4.0 版本给受害者留下的勒索信较此前的 3.0 版本也有所变化——将之前的暗网链接全部去除，并用 Proton 邮箱（采用了端到端加密技术）进行替代。推测这一做法的主要目的是为了让普通用户更容易与攻击者取得联系。



```
xa1Xx3AXs.README.txt - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)

          ~~~ LockBit 4.0 Ransomware since 2024~~~

>>>> Your data are stolen and encrypted

        Price = 1000 $
        Bitcoin = 328N9mKT6xFe6uTvtpxeKSymgWCbbTGbK2
        Email = jimyjoy139@proton.me

>>>> What guarantees that we will not deceive you?

        We are not a politically motivated group and we do not need anything other than your money.

        If you pay, we will provide you the programs for decryption and we will delete your data.
        Life is too short to be sad. Be not sad, money, it is only paper.

        If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
        Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

>>>> Your personal DECRYPTION ID: A3138014A48684D6D525F3F372263313

>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!

第 26 行，第 1 列   100%   Windows (CRLF)   UTF-8
```

```
fu28x4MDV.README.txt - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could
be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group
and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom,
you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your
corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of
your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after you pay, no one will pay us in the
future. You can get more information about us on Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=live

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one
will know about, tell it in the chat, we will generate a secret chat for you and give you his ID via private one-time memos service, no one can find
out this ID but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of
companies around the world.

Tor Browser personal link available only to you (available during a ddos attack):
http://lockbitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad.onion

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>> Your personal ID: C9BDA9028E9A82D5DB83FFAA07C666C1 <<<<<
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Tor Browser Links for chat (sometimes unavailable due to ddos attacks):
http://lockbitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd.onion
http://lockbitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd.onion
http://lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd.onion
http://lockbitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad.onion
http://lockbitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd.onion
```

IOC

暗网地址

http://LockBitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://LockBitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://LockBitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://LockBitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://LockBitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion
http://LockBitaptq7ephv2oigdncfhtwhpqgwmqojnxqdyhprxxfpcllqdxad.onion
http://LockBitaptstzf3er2lz6ku3xuifafq2yh5lmiqj5ncur6rtlmkteiqd.onion
http://oyarbnujct53bizjguvolxou3rmuda2vr72osyexngbdkhqebwrzsnad.onion
http://yq43odyrmzqvyezdindg2tokgogf3pn6bcdtvgczpz5a74tdxjbtk2yd.onion
http://www.LockBitapt.uz
http://LockBitkodidilol.onion
http://LockBitks2tvnmwk.onion/?C841D0BEAB3F0D59D02963D0CC884E3F
http://LockBitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://LockBitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://LockBitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://LockBitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://LockBitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://LockBitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://LockBitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://LockBitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
http://LockBitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://LockBitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://LockBitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://LockBitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://LockBitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly
http://LockBitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd.onion
http://LockBitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd.onion
http://LockBitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad.onion
http://LockBitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd.onion
http://LockBitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd.onion
http://LockBitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd.onion
http://LockBitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd.onion
http://LockBitsupxcjntihbmat4rrh7ktowips2qzywh6zer5r3xafhviyhqd.onion
http://LockBitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd.onion
http://LockBitaptoofrpignlz6dt2wqqc5z3a4evjevoa3eqdfcntxad5lmyd.onion.ly
http://LockBit7ouvrsdgtojeoj5hvu6bljqtghitekwpdy3b6y62ixtsu5jqd.onion
http://LockBit6knrauo3qafoksvl742vieqbujxw7rd6ofzdtapjb4rrawqad.onion
http://LockBit4lahhluquhoka3t4spqym2m3dhe66d6lr337glmnlgg2nndad.onion
http://LockBit3olp7oetlc4tl5zydnoluphh7fvdt5oa6arcp2757r7xkutid.onion
http://LockBit435xk3ki62yun7z5nhwz6jyjdp2c64j5vge536if2eny3gtid.onion

http://LockBit3g3ohd3katajf6zaehxz4h4cnhmz5t735zpltywhwpc6oy3id.onion
http://LockBit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion
http://h3osabcqrbkutyrh77nptes44pqzldj5rk5mxnv46mmrapesp565bsyd.onion
http://2xyr7jug4b5uhndzelsf7vgrxygttutc6h5mqzpwp7y6blk6owhxliqd.onion

加密程序 MD5

44144d055d8d36aa7d2c88f58a50a669
e544b3593a6441f9654839e11aa0bea5
29342223a522646e69cac0d314b94625
515600ed8ed24196e4bf7eadcb610f2e
622800e4cc294223d87204286c3edc31
de66ed388ded986371c7b17d9ee30aeb
f440c3ffa3e4b95a0efcd52b32b7fffc
e72a60ab1862f86d9ea06dde929995cd
83a5f372f3da773e965effc8eb18ad99
013ed22a28eca6d06219da1d6fdc1c2b
679475b7a73405dd0c3fd038d0b107b8
229fa624e0968780127a186a8ae41d2a
b927dd845c06e97594ffbc299f624eec
9eca7d082444bf74f84af6a27e045724
540a5627ce482adf8e76bbf2c15dc05a
c032713a2e972f90bce3640c0edf95f7
12450f3dba7ad4bb8f8fa4988011b913
35cbdad6fda4ee54899967e6fc839a32
88512d09561c3b6f56c2ecc25f958ce3
ec487dc040b36305968803e273c9b957

钱包地址

328N9mKT6xFe6uTvtpxeKSymgWCbbTGbK2
bc1qa34mrngkdf897fwkxlzpcud09hjlqe7yjkgr7r
1KsiEH5ZrfS3XhLVUU758rMKnP65kz2GYz
bc1q9x0sg3w0gwl0yfyml78zp7mdpuan005scwvytu
bc1qwx9y37xd8sznjj0yw85q9fd9qfyaur9xasc2h4
bc1qr4mhf2zqtgd45x9clfmuekf42z4eglh4aydlnk
19ZPm6ybmGoUdaqPvcfQHz7o7SWCPJcQ1b

邮箱

注：多数 LockBit3.0 变种通过电邮赎金谈判，相关邮箱多为泄露构建器生成的样本所有。

LockBitdecrypt@msgsafe.io
goodmen@cock.li
jimyjoy139@proton.me

LockBitdecrypt@onionmail.org
decryptor@cyberfear.com
pbdgja7el1@tutanota.com
wgongruntian@airmail.cc
pmmneevqkj@onionmail.org
Er60t1@proton.me
paqrenlisong0@gmail.com
Hw2k0SZdxa@msgsafe.io
ea7rt3nu0k@onionmail.org
wdengminglang@cock.li
JnSeYvZw34@onionmail.org
balloon@onionmail.org
tianihokeem66@gmx.com
pGU2NJ4TQk@mail2tor.com
skiffdecrypt@mail2tor.com
quvn5llxkk@mailfence.com
mrboot@privyinternet.com
skiffdecrypt@onionmail.com
Q6uBdWWuu4@proton.me
unrasolo1970@proton.me
balloon@onionmail.com
returnback@cyberfear.com
gameovercreation@cock.li
balloon_onion@proton.me
returnbac@onionmail.org
caypishijistor29@gmx.com
blackproton@zohomail.com
7Rnn7AvDNk@onionmail.org
mail@help8888.top
21512232318132@proton.me
recoverymanager@cock.li
everdaygreens@cock.li
321598789321@tutamail.com
pcabcd@countermail.com
QSKhVaBPFv@onionmail.org
fiileky2023@yahooweb.co
abcd-help@countermail.com
VEGtpN4krwJgWeeJ@proton.me
fiileky2023@onionmail.com
supportpc@cock.li
onionmail@onionmail.org

04 LockBit 重点攻击事件

LockBit 勒索软件团伙不仅针对大型企业，还对中小型企业和个人设备发起攻击，至少成功攻击了 2 万台设备。在双重勒索软件领域，LockBit 已成为感染受害者最多的家族，其在暗网公布的被盗数据量超过 2600 起，远超排名第二的 Conti 家族，后者有 865 名受害者。

以下是公开信息中记录的索要百万美元以上赎金的攻击案例（不包括未知和已支付赎金的情况）：

公司/网站	勒索金额（万美元）	时间	官网	国家	行业
accenture.com	5000	2021/8/11	accenture.com	爱尔兰	租赁及商务服务业
CHSF	1000	2022/8/24	chsf.fr	法国	卫生及社会工作
flatironssolutions.com	100	2023/1/24	flatironssolutions.com	美国	信息和通信产业
treves-group.com	600	2023/2/21	treves-group.com	法国	制造

cloud51.com	100	2023/5/ 2	cloud51.com	美国	信息和通信产业
mbwswim.com	450	2023/5/9	mbwswim.com	美国	制造
bankbsi.co.id	2000	2023/5/12	bankbsi.co.id	印尼	金融
RMS	500	2023/5/29	retailmerchantservices.co.uk	英国	金融
harwoodlloyd.com	150	2023/6/2	harwoodlloyd.com	美国	租赁及商务服务业
etships.com	100	2023/6/5	etships.com	美国	交通运输
rammutual.com	150	2023/6/13	rammutual.com	美国	金融
eriematerials.com	300	2023/6/13	eriematerials.com	美国	批发零售
gslelectric.com	300	2023/6/13	gslelectric.com	美国	租赁及商务服务业

tsmc.com	7000	2023/6/29	tsmc.com	中国台湾	制造
sirva.com	100	2023/10/5	sirva.com	美国	交通运输
chs.ca	150 万	2023/10/21	chs.ca	美国	社会组织
restargp.com	250 万	2023/12/5	restargp.com	日本	金融
crinetics.com	4000 万	2024/3/18	crinetics.com	美国	科学研究与技术服务

以下是被国内外安全厂商通报过的关于 LockBit 的攻击事件：

2020 年 2 月 20 日，Expeditors 疑似遭到勒索软件攻击导致全球业务关闭。

2021 年 5 月 6 日，英国铁路网络 Merseyrail 可能被 LockBit 勒索软件攻击。

2021 年 8 月 3 日，意大利拉齐奥地区遭遇勒索软件攻击，导致该地区新冠疫苗接种工作受到影响。

2021 年 9 月 1 日，曼谷航空公司遭遇 LockBit 勒索软件攻击。

2021 年 9 月 2 日，意大利能源公司 EGR 遭遇 LockBit 攻击，但仅轻微中断。

2022 年 3 月 14 日，普利司通遭 LockBit 攻击并被泄露数据。

2022 年 8 月 18 日，LockBit 声称对安全巨头 Entrust 进行勒索攻击，并泄露数

据。

2022 年 8 月 23 日，LockBit 袭击法国医院 CHSF 后，向其索要 1000 万美元作为赎金。

2022 年 10 月 24 日，Pendragon 汽车经销商拒绝了 LockBit 勒索软件 6000 万美元的赎金诉求。

2022 年 11 月 3 日，LockBit 勒索软件对 Continental 汽车公司发动攻击。

2022 年 12 月 13 日，LockBit 声称攻击了加利福尼亚财政部。

2022 年 12 月 30 日，LockBit 声称攻击了葡萄牙的里斯本港口。

2023 年 1 月 1 日，勒索软件团伙道歉并向 SickKids 医院提供免费解密器。

2023 年 1 月 3 日，铁路巨头 Wabtec 披露在受到 LockBit 攻击后数据遭到泄露。

2023 年 2 月 7 日，LockBit 勒索软件团伙声称对“皇家邮件”发动网络攻击。

2023 年 3 月 15 日，LockBit 勒索软件称攻击了 Essendant 公司。

2023 年 3 月 21 日，LockBit 勒索软件团伙声称也开始对奥克兰市发动攻击。

2023 年 4 月 5 日，奥克兰市确认二月份勒索软件攻击后发生第二次大规模数据泄露。

2023 年 5 月 18 日，LockBit 泄露从印度尼西亚 BSI 银行窃取的 1.5TB 数据。

2023 年 5 月 31 日，勒索软件攻击后 MCNA 牙科数据泄露影响 890 万人。

2023 年 6 月 14 日，LockBit 勒索软件在美国 1700 次攻击中勒索了 9100 万美元。

2023 年 11 月 2 日，波音公司证实在 LockBit 勒索软件索赔中遭受网络攻击。

2023 年 11 月 9 日，中国工商银行美国子公司工银金融服务遭遇勒索软件攻击。

2023 年 11 月 9 日，京瓷 AVX 称勒索软件攻击影响了 39000 人。

2023 年 11 月 20 日，加拿大政府披露承包商被黑客攻击后数据遭泄露。

2023 年 12 月 28 日，Eagers Automotive 因网络攻击而停止交易。

2023 年 12 月 29 日，医院要求法院强制云存储公司归还被盗数据。

2024 年 1 月 31 日，LockBit 团伙声称对 12 月芝加哥社区医院遭受的网络攻击负责。

2024 年 2 月 14 日，LockBit 声称勒索软件袭击了佐治亚州富尔顿县。

2024 年 4 月 22 日，LockBit 勒索软件通过针对第三方软件提供商攻击获得了华盛顿市 800GB 数据。

05 安全防范建议

遭受勒索软件攻击后的处理流程

1. 发现有设备中招，不要惊慌，及时有效的处置，能够降低损失，减少再次被攻击可能性。

2. 对被攻击设备及时进行隔离，切断网络连接。如果同一子网下多台设备中招，可切断整个子网对外连接。

3. 企业面临最常见入口攻击包括：远程桌面弱口令，Web 服务漏洞，数据库弱口令。企业内网设备常由于内部设备发起的横向渗透，而遭受攻击。因此，在发现攻击的第一时间，可先切断除管理员外，其它外部对远程桌面的访问。关闭服务器 web 服务端口，关闭服务器数据库外部访问端口。作为应急响应手段。

4. 尽快联系安全厂商或其它安全团队，对内部网络进行排查处理。

5. 查清问题原因，对风险点位做加固修复。公司内部所有机器口令均应更换，在确定黑客掌握了多少内部口令的情况下，应做最坏打算。

6. 应对勒索攻击，最有效手段是查清原因，避免再次中招。忽视事故原因，盲目重置系统，会带来更严重安全隐患。

勒索软件应急处置清单

✧ 检查中招情况

检查有哪些设备被攻击，常见被攻击特征有：文件后缀为被改，文件夹留下勒索信息，桌面背景被修改，弹出勒索提示信息。

☐ 公网服务器

☐ 域控设备与管控设备

☐ 内网共享服务器

☐ 办公机（检查是否仅是共享文件夹被加密）

✧ 控制勒索蔓延

根据现场情况，对已经发现的被攻击设备或者存在风险的设备与网段进行临时管控，常见管控方法包括：

● 访问控制

☐ 网络隔离/主机隔离

☐ 端口访问控制（常见端口包括：445、135、137、139、3389、22、6379、3306、7001）

☐ 设置 IP 访问黑白名单：禁止国外 IP 访问/仅允许特定 IP 访问 或 仅允许本地 IP 访问

☐ 控制重要设备的访问权限，或对重要设备做临时下线处理。

● 物理隔离

☐ 关闭设备/设备断电

☐ 拔出网线/禁用网卡/禁用无线网卡/移除移动网卡

- **密码策略**

  - ☐ 修改全部管理员账号密码
  - ☐ 禁用归属不明账号
  - ☐ 临时停用非必要账号，修改所有普通用户账号密码

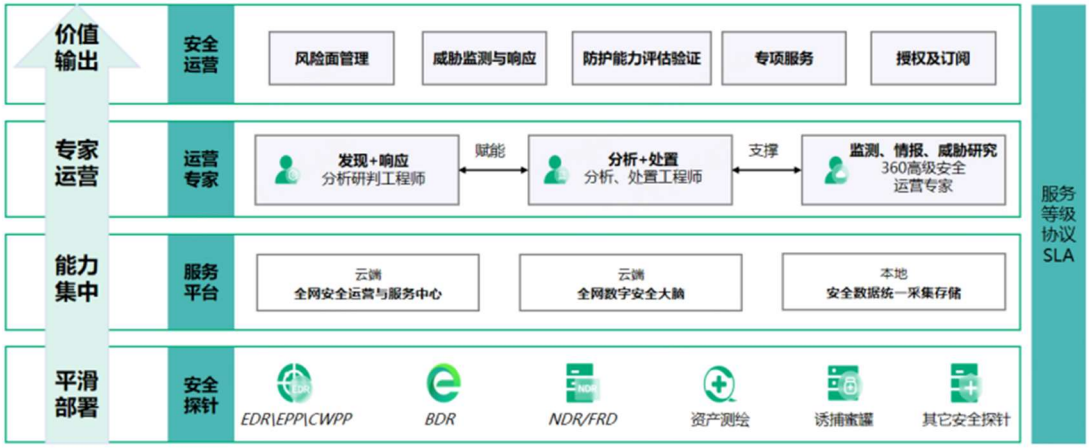
✧ 排查关键节点

在完成上述应急处置后，尽快确认以下事项，并联系安全团队进行进一步排查。（注意：被加密的文件本身不是病毒。）

- ☐ 确定机器感染勒索软件时间
- ☐ 收集可疑样本、被加密文件（少量）、勒索提示信息（一份）
- ☐ 收集中招设备系统安全日志与防火墙日志
- ☐ 检查存储有敏感信息设备是否被异常访问
- ☐ 检查设备中账户情况，包括第三方软件账户，最近新增账户
- ☐ 检查数据库账户，VPN 账户，NAS 账户，VNC 类软件配置
- ☐ 排查 Web 日志
- ☐ 排查最近运行记录
- ☐ 临时禁用发现的攻击账号
- ☐ 使用安全软件进行扫描
- ☐ 完成后续安全加固工作，安装补丁，修补存在的其它问题。

360 针对企业勒索事件的解决方案

面对来势汹汹的勒索软件，组织单位更应该未雨绸缪，提前做好勒索软件预防，加强核心资产防护工作。360 基于多年攻防实战经验和能力推出 360 安全云，云化数据、探针、专家、平台和大模型能力，开放共享给广大客户，并以安全云为核心打造 360 防勒索解决方案，通过“布探针，建平台，通能力，享服务”构建了有效预防、持续监测、高效处置的勒索软件防御体系。



1. 布探针：数据采集标准统一化

安全数据是安全大脑分析的基础，各类型探可提供原始安全数据。该方案帮助客户部署 30+种低侵入、强适配、轻量化、可拓展的探针，不仅解决了安全数据源头多、难收集、数据格式异构、数据质量低等问题，还直接连接 360 安全云上的基础设施，依托亿万终端、大数据分析、AI 和持续运营等能力，真正具备可视化检测和响应各类威胁的能力。

2. 建平台：实现预警避险、精准防护

要看见高级别的安全风险必须依靠强大的数据基础，而轻量级大数据平台可汇聚终端、流量、业务访问等全场景行为数据。据悉，该平台内置解析规则，200+厂商、

2000+数据源，并具有“运营商”级别的数据处理能力，数据处理效率 5 倍以上。此外，该方案通过成熟的大数据技术和架构，实现全网安全数据统一纳管、全网安全能力集中协同，真正做到对勒索攻击行为的主动发现、动态分析、预警阻断。

3. 通能力：实现漏洞与威胁实时监测

定期检测勒索攻击途径是减少数据勒索的基础工作，该方案依托 360 安全云的资产探测和丰富资产指纹库，实现终端资产和数据资产全方位探测，并通过本机、云端、集中容灾备份数据与文件，保障核心数据安全。此外，360 自行研发的智能诱捕技术和异常加密行为分析可实时监测勒索风险，提高勒索攻击的识别与防御效果。

4. 享服务 ：SaaS 化服务方案满足需求

该方案通过 SaaS 化服务模式，向客户提供按需定制的托管安全服务。具体而言，360 云端勒索安全运营专家依托全网安全大数据和数据勒索防护经验，向客户提供个性化防勒索专项服务，包含利用勒索威胁预告服务、勒索能力评估服务、勒索应急响应服务等，客户可灵活按需选择或定制安全服务，减少安全支出成本。

目前，360 安全云防勒索解决方案针对不同客户体量与需求推出多元产品及服务套餐，已累计为政府、公安、医疗等行业的超万例勒索软件救援求助提供了“遥遥领先”的安全能力，帮助用户面对勒索软件做到事前能防御，事中能控制、事后能补救，彻底解决客户的后顾之忧。

如需进一步咨询相关服务请联系：

电话：400-0309-360

邮箱：wuluting@360.cn