360数字安全
数 字 安 全 的 领 导 者

Lockbit 勒索软件分析报告

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《2022 年勒索软件流行态势报告》指出，受俄乌冲突和疫情等多方面影响，国内外发生的一系列大事件也影响着网络安全的发展形势。这其中，俄乌之间互投多轮“擦除器”勒索软件攻击事件，进一步展现了网络战在现代战争与国际对抗中的应用。此外，LockBit 更新至 3.0 版的同时也加强了对大型政企目标的攻势，这也是一个重大的标志性事件。它预示着勒索攻击已不局限于对个人或企业造成威胁，其攻击影响已经开始触及国家安全。

而国内的勒索软件的攻击事件也此起彼伏，以 Coffee 为代表的本土勒索软件强势兴起，意味着这一条黑色产业链也已经在国内扎根。已经有越来越多的不法人员有组织的参与其中——这将对国内未来的网络安全形成更多挑战。

根据 360 安全云统计，2022 年共处理反勒索服务求助案例 4700 余例。反馈案例中，单个企业大面积中招的事件进一步增多，以 Lockbit 为代表的更针对大中型企业且间距双 / 多重勒索能力的勒索攻击影响也在逐步扩大。

02 Lockbit 勒索软件简述

LockBit 勒索软件家族,又被称作“ABCD”、“LockBit2.0”、“LockBi3.0”等,也有分析人员认为该家族是由“LockerGoga”和 “MegaCortex” 两个勒索软件家族演变而来。一旦受该勒索软件感染，系统中的文件将被加密。受害者需要向黑客支付赎金购买密钥才能解密文件。

该家族最早于 2019 年 10 月被发现。该软件在运行时会检查当前运行的操作系统语言，并主动规避俄语系主机，不会在俄语系主机间进行传播。同时，其采用了当前比较热门的 RaaS（勒索软件即服务）运营模式，也进一步为其大规模的传播和获利提供了便利条件。

被该家族攻击的受害者通常被分为两类：

1. 针对性攻击，此类受害者通常为大中型企业或组织。攻击者在部署勒索软件之前通常还会从受害者的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；

2. 无针对性的撒网式传播，受类害者通常为小型企业或个人 PC。攻击者在此类攻击中通常不会窃取数据而仅是加密其数据文件作为勒索筹码。

Lockbit 自我标榜的一些特点还有：

- 否认来自俄罗斯，号称位于荷兰，只出于经济利益发起攻击，而非政治相关。
- 提供 StealBit（数据窃取器），该窃取器提供绕过网络防护策略的功能，号称能够快速窃取数据。
- 提供不同版本的勒索病毒，可以对计算机网络进行二次加密。
- 号称全世界加密速度最快的勒索病毒，4 分半完成 100G 数据加密。
- 提供自动散播、自动枚举网络资源的能力，快速完成全网加密。能够通过打印机不停打印勒索信息。
- 能够清除各类日志、备份，避免被追查。
- 支持 Windows、Linux、Mac 等系统，并可在 NAS、KVM 等各类平台或设备上运行。同时可以加密大多数版本的 ESXi（4.0 除外）
- 号称不允许加密关键基础设施或加密可能导致死亡的医疗数据，但可以实施数据窃取。

03 Lockbit 演化与 RaaS 模式

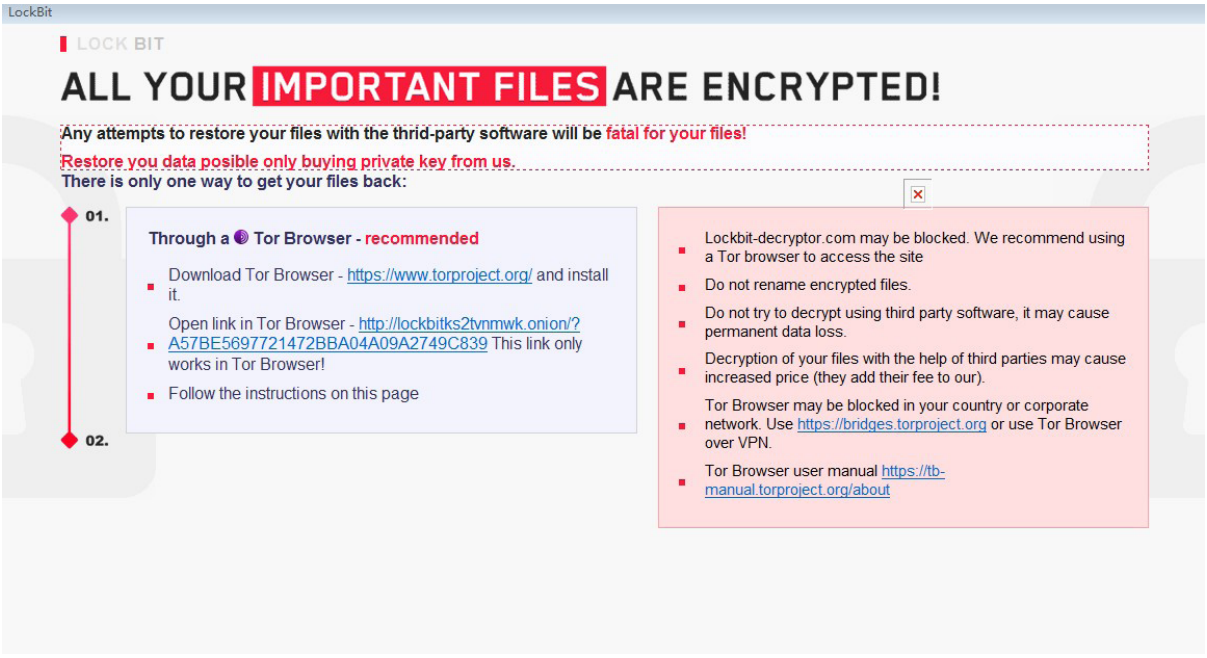
最初成型

Lockbit 的幕后组织所开发的这款勒索软件最初是从 REvil 和 Maze 等其它勒索软件学习经验。因此在 2019 年 10 月一经发布便起点颇高，并一举将勒索软件攻击提高到一个新水平。

但在彼时，勒索软件都处在一个野蛮发展的阶段，虽然有“百家争鸣”之势但整体上并不成章法，各家族也都在试探和摸索更加行之有效的获利方式。故此 Lockbit 虽然有较高的技术水平，但传播也相对较为平稳，并未出现大规模爆发。甚至在 2020 年末开始出现了逐步淡出网络的势头。

重整旗鼓

直到 2021 年 7 月中旬，Lockbit 组织在消失了 6 个月后宣布版本升级，正式更新为 Lockbit2.0 版本。



而 Lockbit 团伙在该版本更新后，对外宣称：

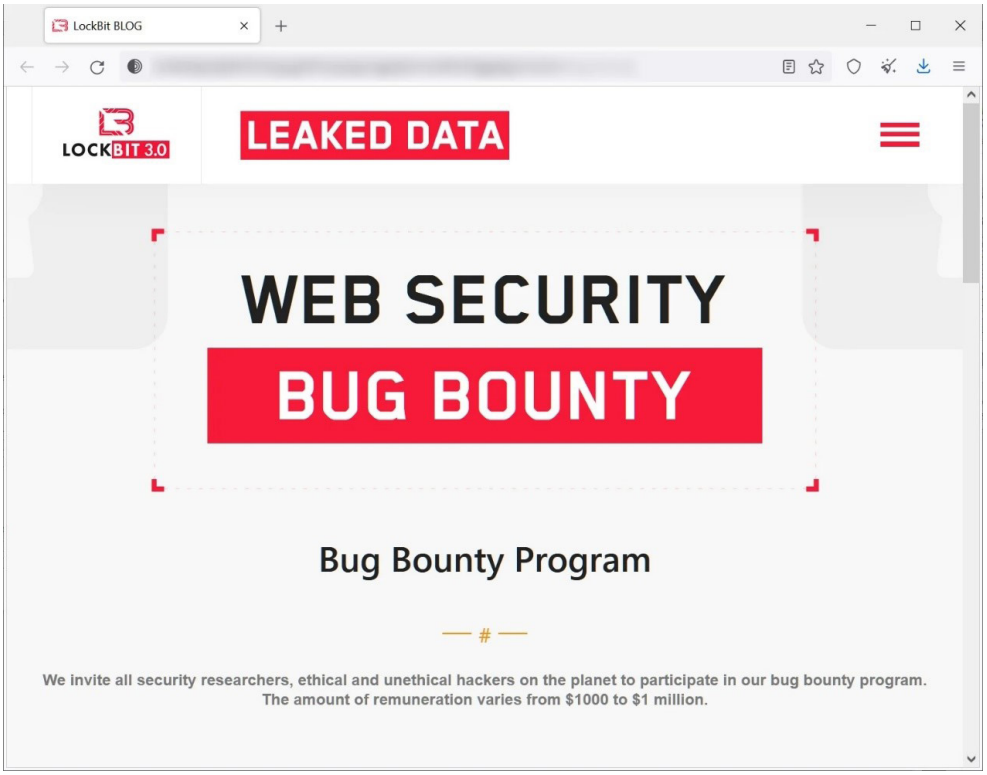
- 全世界加密最快的的勒索软件，并贴出包括其之前版本的加密测试速度对比图。
- 窃取速度快，20 分钟可窃取 100GB 数据。
- 具备在域控内自动传播能力。

以上对外宣传的内容显然并不是为了向受害用户自夸，而是在向其真正的消费者——订阅 RaaS 的攻击者们展示自身强大的技术实力和变现能力。也正是在这一时期，Lockbit 正式开始以 RaaS 的模式进行运营，且这一手段一直被延续至今。而 RaaS 运营模式的开启也正式将 Lockbit 的传播力及影响力推到了一个新的高度。

强势再临

至 2022 年 6 月，Lockbit 发布了其 3.0 版本。通过代码分析，研究人员发现这一最新版本借鉴了 BlackMatter 勒索软件的一些特性，因此该版本又被称为 LockBit Black。

而新版本发布后，该团伙在其官网发布公告称将引入漏洞赏金计划——任何安全研究员可向该家族提供漏洞报告以换取 1000 至 100 万美元的奖金。此外，本次更新还引入 Zcash 支付方式。和比特币不同，Zcash 币更为隐蔽也更难被追踪。



在 2022 年 8 月，Lockbit 再次宣布采用“三重勒索”模式进行运营——除已有的加密文件和窃取数据之外，又将 DDoS 加入其勒索手段中。

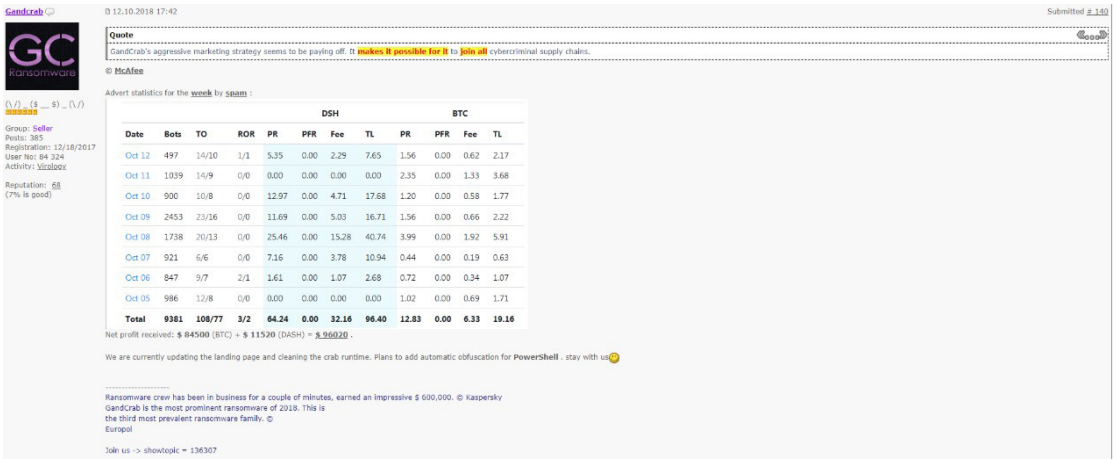
RaaS 运营模式

由此可见，Lockbit 的成功除了其自身强大的技术实力之外，与 RaaS 的运营模式也有莫大的关联。而所谓的 RaaS，即是 Ransom as a Service 的缩写，其含义为“勒索软件及服务”。

勒索软件使用 RaaS 模式最早被发现是在 2017 年。彼时勒索软件已经不再是黑客单打独斗的产物，而是演变为平台化服务，形成了一个相对完整的产业链条。在勒索软件服务平台上，其核心技术是已经直接打包封装好的。众多分包黑客可直接购买调用其服务来获取到一个完整的勒索软件。而这种勒索软件的生成模式便被称之为 RaaS。由于当时提供此类服务的代表性勒索软件家族是 Satan 勒索软件家族，所以那时的黑市中一般用“Satan Ransomware（撒

旦勒索软件）”来指代由 RaaS 服务生成的勒索软件。

RaaS 允许任何攻击者注册一个帐户并创建自己定制版本的勒索软件，而攻击者可以决定如何分发勒索软件。RaaS 平台方则专注于处理赎金支付和新功能开发的相关事务。一般而言，RaaS 平台的开发者会收取受害者所支付赎金一定比例作为抽佣，而其余部分则有购买 RaaS 的攻击者获取。



到 2018 年时，Satan 勒索软件则不再提供该服务，而另一个知名勒索软件家族 GandCrab 则仍然以 RaaS 模式运作。根据 GandCrab 作者自己公布 2018 年 12 月第二周的收入情况，仅在这一周的时间内，与其合作的网络犯罪组织就收入了近 10 万美元。

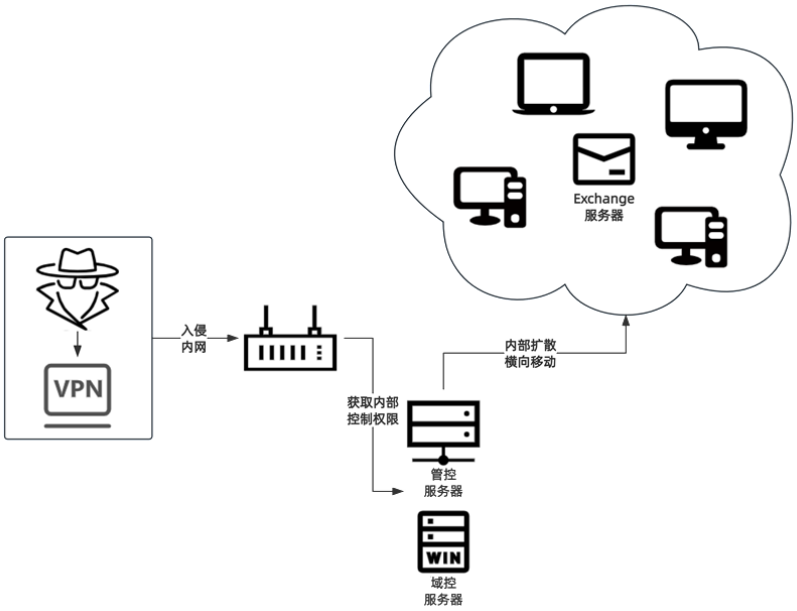
2020 年，RaaS 模式在勒索软件圈内则彻底的流行开来。而这一趋势不仅给勒索软件作者之间增加了竞争，也让黑产从业人员获取勒索软件变的更加方便，进一步加剧了勒索软件的传 播。这也最终导致了其制作、传播、获利的整个链条分工更趋于清晰明确。

另外，在一些针对地区基础设施的攻击中也越来越多的出现了勒索软件的身影。这一现象的背后很可能是针对特定地区的破坏行为，而不单单是直接经济利益上的资金勒索。勒索软件在攻击中扮演了破坏者的角色，同时也在一定程度上起到了转移视线的作用。

自此之后，一直到当前，勒索软件的 RaaS 模式依然是许多勒索软件家族的主要运行模式。

04 Lockbit 攻击技战术特点

由于 Lockbit 属于 RaaS 类勒索组织，其攻击团伙多样，故常见的攻击技术手段，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，其常规攻击路径如下：



◆ 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。

◆ 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。

◆ 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。

◆ 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。

◆ 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。

Lockbit 家族特性：

家族名称	Lockbit
平台	Windows/Linux/Mac/VMware ESXi
攻击目标	包括政府机构在内的全行业
攻击地区	俄语区以外的地区
支持解密	否
勒索信文件	Restore-My-Files.tx、!!!-Restore-My-Files-!!!.txt、Restore-My-Files.txt、LockBit_Ransomware.htat、LockBit-note.hta
加密扩展名	abcd、lockbi、lock2bits、8 位随机字符
是否窃取数据	是
武器库	Exfiltrator-22、ADExplorer、Rclone、MEGASync、Psexec、nmap、Zmap、StealBit、Filezilla、TOX messenger
典型漏洞利用	CVE-2021-21974、CVE-2023-20269、CVE-2023-4966、CVE-2023-27350、CVE-2023-27351

内网渗透中，常到的一些漏洞信息

勒索传播中经常使用到的漏洞		
漏洞编号	涉及产品 / 应用 / 服务 / 设备	相关关键词
CVE-2017-0143	针对 SMB 服务发起攻击	永恒之蓝、WannaCry、共享、445 端口
CVE-2017-0144		
CVE-2017-0145		
CVE-2017-0146		
CVE-2017-0148		

CVE-2021-1675	针对 Windows Print Spooler 服务	打印高危漏洞、PrintNightmare
CVE-2021-34527		
CVE-2021-36958		
CVE-2021-34473	针对 Exchange Server 服务	ProxyShelll 漏洞，Exchange Server
CVE-2021-34523		
CVE-2021-31207		
CVE-2021-36942	NTLM 协议攻击	PetitPotam、Windows LSA 欺骗漏洞
CVE-2021-26411	针对 IE 浏览器	IE 浏览器漏洞
CVE-2021-44228	针对 Apache Log4j2 组件	Log4j2 漏洞、Log4jShell
CNVD-2022-60632	畅捷通 T+ 任意文件上传漏洞	
CVE-2021-40444	微软 MSHTML 远程代码执行漏洞	
CVE-2022-26134	Atlassian Confluence OGNL 注入漏洞	
其它	Web 系统类漏洞	用友 (Yonyou) GRP-U8 / UploadFileData 接口任意文件上传漏洞、用友 (Yonyou) NC accept 接口文件上传漏洞、用友 (Yonyou) NC NCInvokerServlet 接口任意代码执行漏洞
CVE-2021-21972	VMware vSphere Client	云服务器类漏洞
CVE-2021-21985	VMware vSphere Client	
CVE-2020-3992	VMware ESXI	
CVE-2021-22005	Vmware vCenter	

05 LockBit 重点攻击事件

LockBit 成为 2019 年针对工业领域最活跃的勒索病毒之一，以下为该家族各个版本自出现以来发起过的已知攻击事件。

事件披露日期	事件说明
2020 年 2 月 20 日	物流公司 Expeditors 遭到勒索病毒攻击导致全球业务关闭
2020 年 9 月 16 日	LockBit 勒索软件启动数据泄露站点，用于以双重勒索受害者
2020 年 12 月 7 日	直升机制造商 Kopter 遭遇 LockBit 勒索病毒攻击，数据也被发布在暗网站点
2021 年 1 月 21 日	LockBit 在代码中加入重要软件字符串，若已被部署后门机器 存在该软件则被判定为重要系统，并下发勒索病毒。
2021 年 1 月	LockBit 勒索软件组织入侵了法国司法部
2021 年 5 月 6 日	英国铁路网络 Merseyrail 被 LockBit 勒索软件攻击
2021 年 6 月 22 日	LockBit 发布 2.0 版本，声称为全世界最快加密软件
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 8 月 5 日	LockBit 招募会员承诺能赚取数百万美元，同时在购买更多的 RD、VPN、企业邮箱等凭证
2021 年 8 月 16 日	LockBit 2.0 出现在智利、意大利、台湾和英国
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。
2022 年 1 月 27 日	Linux 版 Lockbit 勒索病毒以 Vmware ESXI 服务器作为攻击目标
2022 年 3 月 14 日	普利司通遭 Lockbit 攻击并被泄露数据
2022 年 3 月 30 日	客户关系管理 (CRM) 服务提供商 Atento 称 LockBit 对其造成 4210 万美元的巨额经济损失
2022 年 4 月 13 日	LockBit 勒索病毒团伙潜伏在美国政府网络中长达数月

事件披露日期	事件说明
2022 年 6 月 5 日	美国网络安全的领导厂商 Mandiant 被 LockBit 疑似入侵
2022 年 6 月 26 日	LockBit 勒索病毒通过虚假的版权侵权邮件传播
2022 年 6 月 27 日	LockBit 3.0 推出首个勒索病毒漏洞赏金计划
2022 年 7 月 10 日	LockBit 勒索病毒团伙允许公众搜索他们窃取到的数据
2022 年 7 月 21 日	数字安全巨头 Entrust 遭勒索病毒攻击并泄露了相关数据
2022 年 7 月 25 日	LockBit 攻击了意大利税务机构
2022 年 8 月 27 日	LockBit 勒索团伙正通过改进为三重勒索模式进一步增强勒索成功率
2022 年 9 月 1 日	深圳某科技公司遭 LockBit 勒索软件攻击
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 6 日	LockBit 勒索团伙窃取了咨询和 IT 服务提供商 Kearney & Company 的数据
2022 年 11 月 8 日	LockBit 组织正利用 Amadey Bot 恶意软件进行传播
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 2 月 7 日	Lockbit 勒索软件团伙声称对英国“皇家邮件”发动网络攻击
2023 年 3 月 15 日	LockBit 勒索软件称攻击了美国 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 16 日	已发现针对 Mac 设备的 LockBit 勒索软件
2023 年 4 月 26 日	针对 PaperCut 服务器攻击的背后可能是 Clop 及 LockBit 勒索软件团伙

事件披露日期	事件说明
2023 年 5 月 7 日	美国农业机械制造商 AGCO 遭受 LockBit 勒索软件攻击
2023 年 5 月 26 日	日本京瓷美国分公司 AVX 称 LockBit 勒索软件泄露数据影响了 39000 人
2023 年 5 月 31 日	遭遇 LockBit 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	CISA 表示 LockBit 勒索软件在对美国展开的 1700 次攻击中获利 9100 万美元
2023 年 6 月 27 日	在 LockBit 勒索团伙索要 7000 万美元赎金后，台积电否认遭到勒索攻击
2023 年 11 月 2 日	波音公司证实遭到了 LockBit 勒索软件的网络攻击

06 安全防范建议

发现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。

针对 LockBit 勒索事件的排查建议

事件时间线：

10 月 10 日 Citrix 修复了 CVE-2023-4966 NetScaler 设备漏洞（Citrix Bleed 漏洞）
10 月 17 日 Mandiant 宣称自 2023 年 8 月下旬以来，该漏洞在有限的攻击中被滥用。
10 月 25 日 Assetnote 的研究人员公开了漏洞 Poc
10 月 27 日 LockBit 宣称攻击了波音公司。
11 月 9 日 媒体报道，某金融机构受到攻击。

LockBit 团伙近期对 DP World、波音以及某金融机构等多家公司的攻击，其共同点都是利用 (CVE-2023-4966) 的公开漏洞，漏洞在 10 月 10 日已经修复，在 10 月底有 Poc 公开后，攻击量显著增加。

CVE-2023-4966 信息泄漏漏洞

◆ **组　件：**Citrix:NetScaler ADC 13.1-FIPS, Citrix:NetScaler ADC 12.1-FIPS, Citrix:NetScaler ADC 12.1-NDcPP, Citrix:NetScaler ADC 和 NetScaler Gateway

- **漏洞类型：**越界写入，越界读取
- **实际影响：**信息泄漏
- **主要影响：**敏感数据窃取

该漏洞存在于 Citrix NetScaler ADC 和 Gateway 设备中，是一个信息泄露漏洞。要利用该漏洞，需要将设备配置为网关（VPN 虚拟服务器、ICA 代理、CVPN、RDP 代理）或授权和计费 (AAA) 虚拟服务器。未授权的远程攻击者可通过利用此漏洞，窃取敏感信息。

影响版本如下：

组件	影响版本	安全版本
Citrix:NetScaler ADC 和 NetScaler Gateway	14.1 < 14.1-8.50	>= 14.1-8.50
Citrix:NetScaler ADC 和 NetScaler Gateway	13.1 < 13.1-49.15	13.1 >= 13.1-49.15
Citrix:NetScaler ADC 和 NetScaler Gateway	13.0 < 13.0-92.19	13.0 >= 13.0-92.19
Citrix:NetScaler ADC 13.1-FIPS	< 13.1-37.164	>= 13.1-37.164
Citrix:NetScaler ADC 12.1-FIPS	< 12.1-55.300	>= 12.1-55.300
Citrix:NetScaler ADC 12.1-NDcPP	< 12.1-55.300	>= 12.1-55.300

排查建议：

1. Citrix Bleed 一般仅做为初始攻击，用于获取内网初始访问权限，完整攻击过程还涉及内网横移渗透。
2. 检查所有 Citrix 设备，是否安装最新版补丁，受影响范围见上文。
3. 检查其它网络出口设备，对外服务设备，是否安装最新版补丁。尤其是 CVE-2021-21974、CVE-2023-20269、CVE-2023-4966、CVE-2023-27350、CVE-2023-27351 漏洞。
4. 检查内网是否存在 Exfiltrator-22、ADExplorer、Psexec、nmap、Zmap、Filezilla 工具，如果存在，请确认使用者是否知情。
5. 检查内网是否存在 Rclone、MEGASync，StealBit 等存在数据窃取风险的程序。其中 StealBit 的数据传输特性如下：

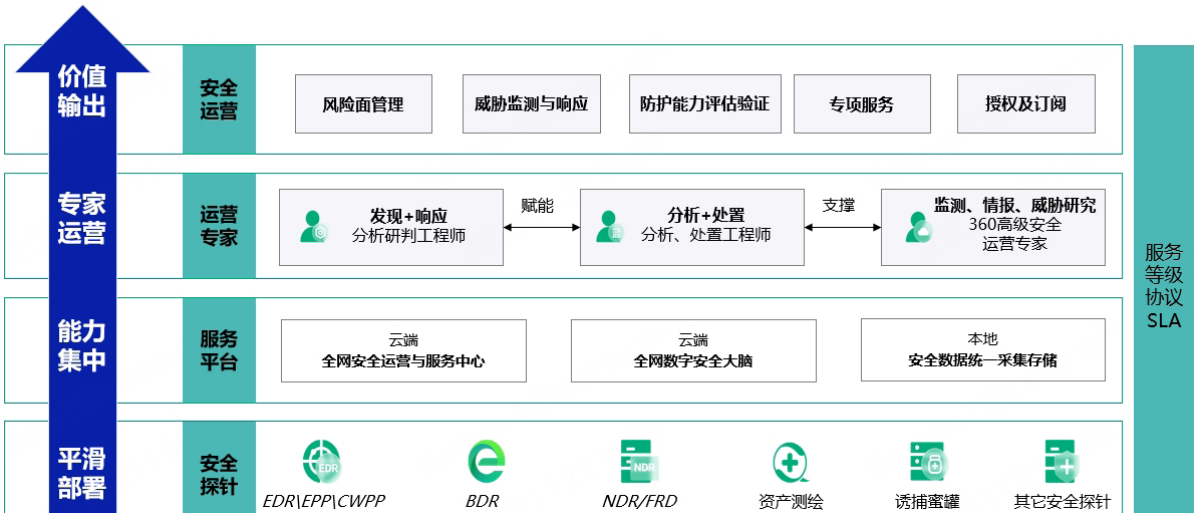
PUT /Hash HTTP/1.1..Host:[hostname].Content-type:application/octet-stream..Transfer-Encoding:chunked.

数据举例：

PUT /04F66B233CEDFC35E98FECDE81F89EF22 HTTP/1.1..Host:XXXXX.Content-type:application/octet-stream..Transfer-Encoding:chunked.

360 针对 LockBit 勒索事件的解决方案

面对来势汹汹的勒索病毒，组织单位更应该未雨绸缪，提前做好勒索病毒预防，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、高效处置的勒索病毒防御体系。



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病毒救援求助提供了“遥遥领先”的安全能力，帮助用户面对勒索病毒做到事前能防御，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