CAICT 中国信通院

勒索病毒安全防护手册

中国信息通信研究院

2021 年 9 月

前　言

勒索病毒是一种极具传播性、破坏性的恶意软件，主要利用多种密码算法加密用户数据，恐吓、胁迫、勒索用户高额赎金。近期，勒索病毒攻击形势更加严峻，已经对全球能源、金融等领域重要企业造成严重影响。由于勒索病毒加密信息难以恢复、攻击来源难以追踪，攻击直接影响与生产生活相关信息系统的正常运转，勒索病毒对现实世界威胁加剧，已成为全球广泛关注的网络安全难题。

为加强勒索病毒攻击防范应对，在工业和信息化部网络安全管理局指导下，中国信息通信研究院联合中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、安天科技集团股份有限公司、杭州安恒信息技术股份有限公司、奇安信科技集团股份有限公司、绿盟科技集团股份有限公司[1]等单位编制《勒索病毒安全防护手册》，梳理勒索病毒主要类型、传播方式，分析勒索病毒攻击特点，聚焦事前预防，事中应急、事后加固三个环节，研提勒索病毒安全防护框架和实操参考，以期与公众共享，共同防范化解攻击风险。

[1] 注：编制单位按首字笔画排序，排名不分先后

目 录

一、相关背景

勒索病毒是一种极具破坏性、传播性的恶意软件，主要利用多种密码算法加密用户数据，恐吓、胁迫、勒索用户高额赎金。近期，勒索病毒攻击事件频发，一系列攻击严重影响金融、能源、交通等领域服务于生产生活的信息系统正常运转，勒索病毒对现实世界威胁加剧。

（一）勒索病毒攻击事件数量持续走高

2021 年上半年，国际方面，统计全球公开披露的勒索病毒攻击事件 1200 余起，与 2020 年全年披露的勒索病毒攻击事件数量基本持平；国内方面，国家工业互联网安全态势感知与风险预警平台监测发现勒索病毒恶意域名的访问量 5.05 万次，同比增长超过 10 倍，其中，近一年来，勒索病毒恶意域名访问量如图 1.1 所示。

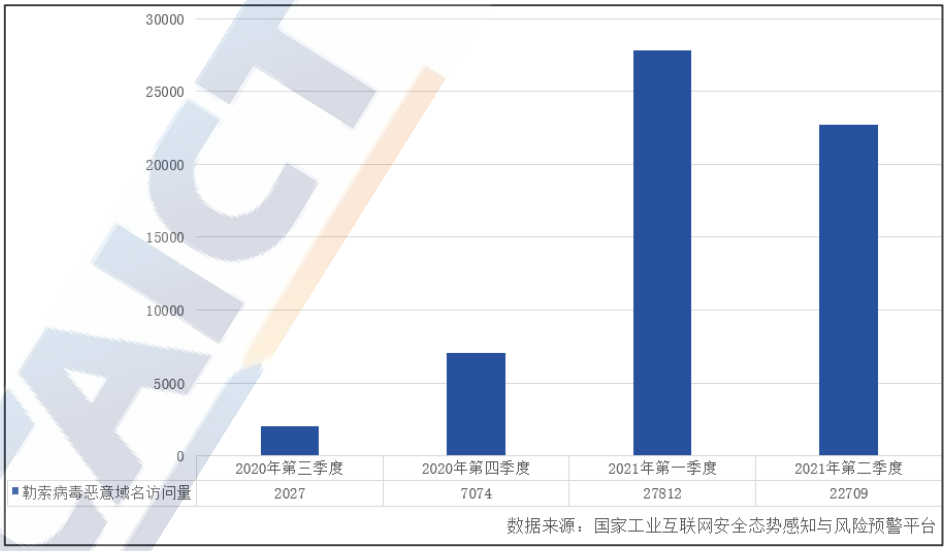

图 1.1 近一年勒索病毒恶意域名访问量

（二）勒索病毒攻击风险传导趋势明显

近期，全球医疗、教育、金融、科技等重点行业企业相继遭受勒索病毒攻击，引发企业业务停滞、工厂停产等严重后果，如对英国北方铁路公司自助售票系统的攻击导致企业售票网络瘫痪、对巴西肉类加工巨头 JBS 的攻击导致企业在澳全部肉类加工厂停运等。2021 年上半年影响生产生活的典型勒索病毒攻击事件如图 1.2 所示。

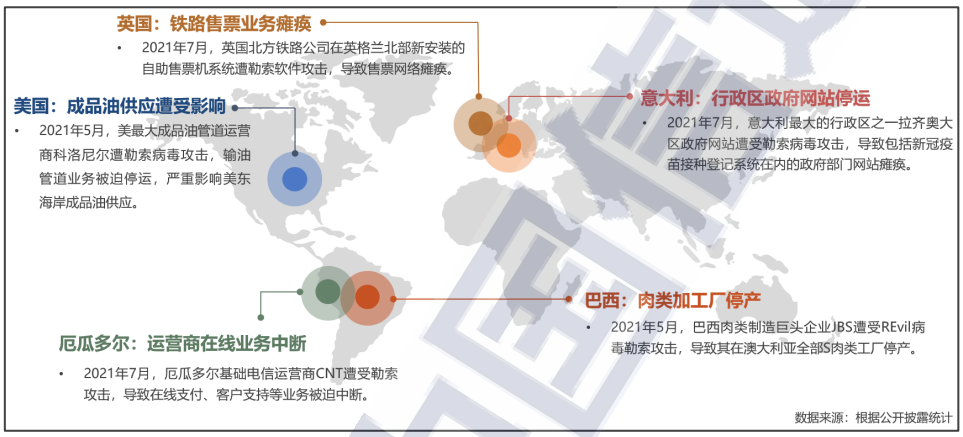

图 1.2 2021 年上半年影响生产生活的典型勒索病毒攻击事件

二、勒索病毒概述

典型勒索病毒包括文件加密、数据窃取、磁盘加密等类型，攻击者主要通过钓鱼邮件、网页挂马等形式传播勒索病毒，或利用漏洞、远程桌面入侵等发起攻击，植入勒索病毒并实施勒索行为。

（一）勒索病毒主要类型

1. 文件加密类勒索病毒。该类勒索病毒以 RSA、AES 等多种加密算法对用户文件进行加密，并以此索要赎金，一旦感染，极难恢复文件。该类勒索病毒以 WannaCry 为代表，自 2017 年全球大规模爆发以来，其通过加密算法加密文件，并

利用暗网通信回传解密密钥、要求支付加密货币赎金等隐蔽真实身份的勒索病毒攻击模式引起攻击者的广泛模仿，文件加密类已经成为当前勒索病毒的主要类型。

2. 数据窃取类勒索病毒。该类勒索病毒与文件加密类勒索病毒类似，通常采用多种加密算法加密用户数据，一旦感染，同样极难进行数据恢复，但在勒索环节，攻击者通过甄别和窃取用户重要数据，以公开重要数据胁迫用户支付勒索赎金。据统计，截至 2021 年 5 月，疑似 Conti 勒索病毒已经攻击并感染全球政府部门、重点企业等 300 余家单位，窃取并公开大量数据。

3. 系统加密类勒索病毒。该类勒索病毒同样通过各类加密算法对系统磁盘主引导记录、卷引导记录等进行加密，阻止用户访问磁盘，影响用户设备的正常启动和使用，并向用户勒索赎金，甚至对全部磁盘数据进行加密，一旦感染，同样难以进行数据恢复。例如，2016 年首次发现的 Petya 勒索病毒，对攻击对象全部数据进行加密的同时，以病毒内嵌的主引导记录代码覆盖磁盘扇区，直接导致设备无法正常启动。

4. 屏幕锁定类勒索病毒。该类勒索病毒对用户设备屏幕进行锁定，通常以全屏形式呈现涵盖勒索信息的图像，导致用户无法登录和使用设备，或伪装成系统出现蓝屏错误等，进而勒索赎金，但该类勒索病毒未对用户数据进行加密，具备数据恢复的可能。例如，WinLock 勒索病毒通过禁用 Windows 系

统关键组件，锁定用户设备屏幕，要求用户通过短信付费的方式支付勒索赎金。

（二）勒索病毒典型传播方式

1. 利用安全漏洞传播。攻击者利用弱口令、远程代码执行等网络产品安全漏洞，攻击入侵用户内部网络，获取管理员权限，进而主动传播勒索病毒。目前，攻击者通常利用已公开且已发布补丁的漏洞，通过扫描发现未及时修补漏洞的设备，利用漏洞攻击入侵并部署勒索病毒，实施勒索行为。

2. 利用钓鱼邮件传播。攻击者将勒索病毒内嵌至钓鱼邮件的文档、图片等附件中，或将勒索病毒恶意链接写入钓鱼邮件正文中，通过网络钓鱼攻击传播勒索病毒。一旦用户打开邮件附件，或点击恶意链接，勒索病毒将自动加载、安装和运行，实现实施勒索病毒攻击的目的。

3. 利用网站挂马传播。攻击者通过网络攻击网站，以在网站植入恶意代码的方式挂马，或通过主动搭建包含恶意代码的网站，诱导用户访问网站并触发恶意代码，劫持用户当前访问页面至勒索病毒下载链接并执行，进而向用户设备植入勒索病毒。

4. 利用移动介质传播。攻击者通过隐藏 U 盘、移动硬盘等移动存储介质原有文件，创建与移动存储介质盘符、图标等相同的快捷方式，一旦用户点击，自动运行勒索病毒，或运行专门用于收集和回传设备信息的木马程序，便于未来实

施针对性的勒索病毒攻击行为。

5. 利用软件供应链传播。攻击者利用软件供应商与软件用户间的信任关系，通过攻击入侵软件供应商相关服务器设备，利用软件供应链分发、更新等机制，在合法软件正常传播、升级等过程中，对合法软件进行劫持或篡改，规避用户网络安全防护机制，传播勒索病毒。

6. 利用远程桌面入侵传播。攻击者通常利用弱口令、暴力破解等方式获取攻击目标服务器远程登录用户名和密码，进而通过远程桌面协议登录服务器并植入勒索病毒。同时，攻击者一旦成功登录服务器，获得服务器控制权限，可以服务器为攻击跳板，在用户内部网络进一步传播勒索病毒。

三、勒索病毒攻击现状

结合近期攻击事件，勒索病毒攻击主要在攻击目标、攻击手段等方面呈现新特点，同时攻击者开始构建精准复杂的攻击链，发起勒索病毒攻击。

（一）近期勒索病毒攻击特点

1. 瞄准行业重要信息系统，定向实施勒索病毒攻击。攻击者瞄准能源、医疗等承载重要数据资源的行业信息系统作为勒索病毒攻击“高价值”目标，摒弃传统利用钓鱼邮件、网页挂马等“广散网”无特定目标的勒索病毒传播模式，向涵盖探测侦察、攻击入侵、病毒植入等的精准化勒索病毒攻击链转变，如嗅探网络发现攻击入口、利用漏洞攻击入侵等，针

对行业重要信息系统发起定向攻击，植入勒索病毒并勒索超高额赎金。

2.伴装勒索病毒攻击，掩盖真实网络攻击意图。攻击者通过甄别重点攻击目标，假装加密数据文件并实施勒索，利用勒索病毒遍历系统文件、覆盖系统引导目录，以及类后门木马的功能，伴装实施勒索病毒攻击，隐藏其窃取敏感信息、破坏信息系统等的真实攻击意图。据披露，在 Agrius、Pay2Key 等黑客组织的攻击活动中，被认为假装加密数据并勒索赎金，掩盖其直接破坏信息系统的攻击行为。

3.针对工控系统专门开发勒索病毒，工业企业面临攻击风险加剧。攻击者通过集成工控系统软硬件漏洞，或内嵌强制中止实时监控、数据采集等工业领域常用系统的恶意功能，开发和升级形成 Cring、EKANS 等具备专门感染工控系统能力的勒索病毒，针对工业企业实施攻击，引发企业生产线、业务线停工停产的严重影响。此外，通过攻击入侵投递和植入 REvil、DarkSide 等典型勒索病毒，同样存在利用勒索病毒攻击工业企业的可能。

4.漏洞利用仍是攻击主要手段，引发勒索病毒传播一点突破、全面扩散。攻击者主要利用已公布漏洞，通过漏洞扫描、端口扫描等方式主动发现未及时修补漏洞的设备，利用漏洞“一点突破”网络安全防线，实施远程攻击入侵，并在攻击目标内部网络横向移动，扩大勒索病毒感染范围，实施

勒索行为。2021 年上半年，网络安全威胁和漏洞信息共享平台监测发现网络产品安全漏洞 1.7 万个，其中，可能遭到攻击者综合利用、传播病毒的高危漏洞 5400 余个。

5. 以虚拟化环境作为攻击跳板，双向渗透传播勒索病毒。勒索病毒攻击开始以虚拟化环境为通道，通过感染虚拟机、虚拟云服务器等，强制中止虚拟化进程，或利用虚拟化产品漏洞、虚拟云服务器配置缺陷等，实现虚拟化环境的“逃逸”，进而向用户和网络“双向渗透”传播勒索病毒。据披露，名为 Hello Kitty 的勒索病毒近期主要攻击 VMWare 虚拟云服务器，感染在其上运行的虚拟机，并向用户设备传播。

6. 经济利益驱动运作模式升级，初步形成勒索病毒黑产链条。部分勒索病毒攻击团伙开发形成“勒索病毒即服务”，面向团伙“会员”提供“开箱即用”的勒索病毒攻击服务，如购买勒索病毒程序、靶标系统访问权限，或订购针对特定目标的勒索病毒攻击服务等。同时，在病毒开发、攻击入侵等环节招募“合作伙伴”，“分工协作”增加勒索病毒攻击成功率。据披露，REvil 勒索病毒攻击团伙负责开发病毒、勒索谈判、赎金分成等，其“合作伙伴”负责入侵目标网络等。

（二）典型勒索病毒攻击流程

聚焦勒索病毒攻击链，近期勒索病毒攻击团伙在成功实施网络攻击入侵的基础上，植入勒索病毒并实施勒索行为，其典型攻击流程主要包括探测侦察、攻击入侵、病毒

植入、实施勒索 4 个阶段。

1. 探测侦察阶段

（1）收集基础信息。攻击者通过主动扫描、网络钓鱼以及在暗网黑市购买等方式，收集攻击目标的网络信息、身份信息、主机信息、组织信息等，为实施针对性、定向化的勒索病毒攻击打下基础。

（2）发现攻击入口。攻击者通过漏洞扫描、网络嗅探等方式，发现攻击目标网络和系统存在的安全隐患，形成网络攻击的突破口。此外，参照勒索病毒典型传播方式，攻击者同样可利用网站挂马、钓鱼邮件等方式传播勒索病毒。

2. 攻击入侵阶段

（1）部署攻击资源。根据发现的远程桌面弱口令、在网信息系统漏洞等网络攻击突破口，部署相应的网络攻击资源，如 MetaSploit、CobaltStrike、RDP Over Tor 等网络攻击工具。

（2）获取访问权限。采用合适的网络攻击工具，通过软件供应链攻击、远程桌面入侵等方式，获取攻击目标网络和系统的访问权限，并通过使用特权账户、修改域策略设置等方式提升自身权限，攻击入侵组织内部网络。

3. 病毒植入阶段

（1）植入勒索病毒。攻击者通过恶意脚本、动态链接库 DLL 等部署勒索病毒，并劫持系统执行流程、修改注册

表、混淆文件信息等方式规避安全软件检测功能，确保勒索病毒成功植入并发挥作用。

（2）扩大感染范围。攻击者在已经入侵内部网络的情况下，通过实施内部鱼叉式网络钓鱼、利用文件共享协议等方式在攻击目标内部网络横向移动，或利用勒索病毒本身类蠕虫的功能，进一步扩大勒索病毒感染范围和攻击影响。

4. 实施勒索阶段

（1）加密窃取数据。攻击者通过运行勒索病毒，加密图像、视频、音频、文本等文件以及关键系统文件、磁盘引导记录等，同时根据攻击目标类型，回传发现的敏感、重要的文件和数据，便于对攻击目标进行勒索。

（2）加载勒索信息。攻击者通过加载勒索信息，胁迫攻击目标支付勒索赎金。通常勒索信息包括通过暗网论坛与攻击者的联系方式、以加密货币支付赎金的钱包地址、支付赎金获取解密工具的方式等。

四、勒索病毒攻击安全防护举措

（一）勒索病毒攻击安全防护框架

由于不同的安全防护措施在勒索病毒攻击的不同阶段发挥不同程度的作用，通过梳理勒索病毒典型安全防护措施，按照核心防护措施（●）、重要防护措施（◎）、一般防护措施（○），与勒索病毒攻击的 4 个阶段形成映射关系，构建形成勒索病毒攻击安全防护框架。建议用户根据自身情

况，选择恰当的防护措施，防范化解勒索病毒攻击风险。

1. **核心防护措施。**该类措施在特定勒索病毒攻击阶段发挥核心防护作用，有效阻断勒索病毒攻击行为或全面消除勒索病毒攻击引发的特定影响等。例如，数据备份、数据恢复主要针对勒索病毒攻击实施勒索的阶段，通过攻击前备份数据、攻击后恢复数据，消除由于勒索病毒加密、窃取数据，引发数据丢失，甚至是业务中断等方面的攻击影响。

2. **重要防护措施。**该类措施在特定勒索病毒攻击阶段发挥重要防护作用，但与核心防护措施相比，未能发挥全面防范应对勒索病毒攻击的效果。例如，采取恰当的安全管理措施，如严格的网络隔离、访问控制等，在攻击者获取访问权限实施攻击入侵方面发挥核心防护作用，但在侦察探测的收集基础信息攻击阶段，攻击者可能采取主动网络探测、暗网黑市购买等多种方式，安全管理在该阶段未能发挥全面防范应对的效果，发挥重要防护作用。

3. **一般防护措施。**该类措施在特定勒索病毒攻击阶段发挥一般的防护作用，但与核心防护措施和重要防护措施相比，仅能在一定程度上发挥防范应对勒索病毒攻击的效果。例如，制定应急预案主要针对攻击者已经开始实施勒索病毒攻击，明确应急处置机制、流程等，在已经发现遭受勒索病毒攻击的情况，启动预案并采取措施应对攻击风险，但在勒索病毒攻击发生前，安全防护措施主要以事前防范为

主，因此制定应急预案在攻击者正式实施攻击前发挥一般防护作用。

攻击阶段 / 防护措施			勒索病毒攻击阶段							
			探测侦察		攻击入侵		病毒植入		实施勒索	
			收集基础信息	发现攻击入口	部署攻击资源	获取访问权限	植入勒索病毒	扩大感染范围	加密窃取数据	加载勒索信息
典型防护举措	事前预防	应急预案	○	○	○	◎	●	●	●	●
		安全管理	◎	●	◎	●	◎	●	○	○
		产品部署	●	●	◎	●	●	●	◎	○
		数据备份	○	○	○	○	○	○	●	◎
		安全意识	○	●	◎	◎	●	●	●	◎
	事中应急	隔离设备	○	○	○	◎	●	●	●	●
		排查范围	○	○	◎	●	●	●	●	●
		事件研判	●	●	○	●	●	●	●	◎
		病毒破解	○	●	○	●	●	●	●	○
	事后加固	数据恢复	○	○	○	○	○	○	●	○
		加强管理	●	●	◎	●	●	●	●	○
		修补隐患	●	●	◎	●	●	●	◎	◎
		设备恢复	○	◎	○	○	○	○	○	○

图例：核心防护措施（●）、重要防护措施（◎）、一般防护措施（○）

图 3.1 勒索病毒安全防护框架

（二）勒索病毒攻击安全防护实操参考

按照勒索病毒攻击“事前、事中、事后”三个阶段，从管理、技术两个方面防范化解攻击风险，典型勒索病毒攻击安全防护措施和实操主要包括以下几个方面。

1. 事前：夯实防范基础

（1）制定网络安全应急预案。建立内部涵盖勒索病毒攻击等网络安全突发事件的应急组织体系和管理机制，加强勒索病毒攻击应对统筹管理，明确工作原则、职责分工、应急流程、关键措施等。一旦发生勒索病毒攻击事件，立即启动内部网络安全应急预案，并按照预案要求及时开展应急处置工作，确保有效控制、减轻、消除勒索病毒攻击影响。

- 职责分工：明确组织内部网络安全应急预案中的具体职责及分工，建立涵盖勒索病毒攻击等网络安全突发事件的应急组织体系，通常由组织特定部门牵头，高度协调内部相关部门，识别风险、加强防范、做好应急，从组织安全、个人安全等层面防范化解网络安全突发事件。
- 应急流程：明确涵盖勒索病毒攻击等在内的网络安全突发事件应急流程和主要工作内容，其中，针对勒索病毒攻击的应急流程通常包括但不限于立即隔离感染勒索病毒的设备、排查主要业务系统的感染范围、利用备份数据进行数据恢复等。
- 关键措施：明确涵盖勒索病毒攻击等在内的网络安

全突发事件应急响应关键措施，包括但不限于定期组织网络安全演习、建立网络安全监测处置专业技术手段、加强网络安全应急响应技术支撑队伍建设、储备漏洞检测和网络扫描等网络安全应急装备、开展网络安全应急培训等。

（2）加强组织内部网络安全管理。在网络隔离、资产管理等方面采取措施，如进行物理和逻辑的网络隔离、及时更新杀毒软件和漏洞补丁、避免关键信息系统在互联网上暴露、与供应商签订协议明确安全责任和义务、评审供应商提供服务情况等。

- 网络隔离：采用合理的网络分区，限制勒索病毒的入侵和传播。如根据不同业务需要将网络分为隔离区、内网区、外来接入区、内网服务器区等，并限制不同分区间的网络访问。在同一分区内，采用虚拟局域网技术隔离不同部门资产，降低由于单一设备感染勒索病毒，导致勒索病毒在内部网络进一步传播的可能。

- 访问控制：对组织关键业务系统设置严格的访问权限，如按照权限最小化原则开放必要的访问权限、根据访问控制策略设置访问控制规则等。及时对访问控制规则进行更新，删除多余或无效的访问控制规则，如定期对开放的访问权限进行梳理，及时删除因人员离职、资产 IP 变更后存留的访问权限。

- 资产管理：排查组织资产暴露情况，梳理暴露资产

真实范围，梳理范围涵盖组织分公司、下级机构等相关资产，梳理时间根据自身实际情况如每周、月、半年等进行资产梳理。同时，按照最小化原则，尽可能减少在资产互联网上暴露，特别是避免重要业务系统、数据库等核心信息系统在互联网上暴露。

- 漏洞排查：对组织资产进行漏洞排查，一旦发现资产存在安全漏洞，及时进行修补。采用漏洞扫描等设备和产品的，对漏洞扫描设备进行集中管理，建立完整、持续的漏洞发现和管理手段；具备导入第三方漏洞报告能力，支持导入和分析主流厂家漏洞和配置核查扫描结果；针对扫描的漏洞结果加强漏洞知识库关联，及时获取漏洞信息和解决方案等。

- 身份鉴别：对用户进行身份标识和鉴别，如保证身份标识具有唯一性、采用动态口令等两种或两种以上身份鉴别、具备防范口令暴力破解的能力、口令等身份鉴别信息符合复杂度要求并定期更换、推行口令定期强制修改和出厂口令修改等。同时，通过采用扫描软硬件对系统口令定期进行安全性评估，识别发现并及时消除口令安全风险。

- 软件管理：规范组织内部软件版本管理机制，避免使用盗版或来路不明的软件，使用软件风险评估系统或工具定期检测关键业务系统使用的相关软件版本，避免由于软件版本低引发安全风险。基于网络流量对组织内部访问“风险网站”进行检测和阻断，降低由于下载和安装恶意软件，导

致感染勒索病毒的可能。

- 供应链管理：部署供应链安全风险防控措施，包括供应链相关人员管理、供应链生命周期管理、采购外包与供应商管理。采用的网络设备、安全产品、密码产品等产品与服务的采购和使用符合国家有关规定。与选定的供应商签订协议，明确供应链各方履行的安全责任和义务，定期审视、评审和审核供应商提供的服务，对其变更服务内容加以控制。

（3）部署专业网络安全产品。在终端侧、网络侧等部署网络安全产品，并日常排查设备告警情况。例如，在终端侧，安装具有主动防御功能的安全软件，不随意退出安全软件、关闭防护功能、执行放行操作等，并设立应用软件白名单，及时保持白名单的准确性、完整性、实时性；在网络侧，部署流量监测、阻断等类型的网络安全设备，加强针对勒索病毒攻击威胁的监测、溯源等。

- 终端侧：在终端侧部署杀毒软件、终端安全管理系统等终端安全产品，对勒索病毒进行检测和查杀。终端安全产品应支持防暴力破解、端口扫描以及系统登录防护、弱口令检测能力；可支持云端威胁情报联动、本地实时监测等多种模式，具备勒索病毒专杀的功能；具备勒索病毒免疫、应用进程防护等能力，如利用文件防护产品，检测文件的执行、生成、修改、重命名等，发现遍历大量文件、文件修改操作、调用加密算法库等时，及时提示和拦截。利用勒

索病毒诱饵文档，发现恶意修改文档的行为，并拦截关联进程。针对核心的应用数据，支持驱动级的文件保护、设置合规进程访问策略等，杜绝非合规进程对文件的任意修改。

- 网络侧：通过在网络边界部署防火墙、堡垒机等产品，仅允许授权用户对关键业务系统进行访问，实现访问权限限制和管理，并与检测系统联动，通过流量解析实施勒索病毒攻击告警，防火墙根据告警封禁攻击 IP 地址；部署 IPS、UTS 等流量监测阻断产品，通过还原流量中传播的勒索病毒样本，联动威胁情报、沙箱分析等，识别和阻断投递过程中勒索病毒；部署邮件安全网关、邮件威胁分析系统等产品，检测和拦截邮件投递的勒索病毒。

- 中心侧：部署网络安全威胁管理平台、漏洞扫描系统等产品，对安全漏洞威胁、弱口令风险等实现及时发现和闭环管理；部署网络安全态势感知平台，通过对原始流量、网络告警等信息的收集和分析，监测勒索病毒攻击情况、发现病毒传播线索；针对性部署勒索病毒攻击常用高风险漏洞蜜罐，发现勒索病毒横向传播行为，在勒索病毒接触到真实攻击目标前进行预警，同时对通过蜜罐环境捕获到的勒索病毒和传播方式进行溯源分析。

- 服务器侧：结合服务器计算、存储等方面资源优势，在具备支持驱动级的文件保护以及防暴力破解、端口

扫描等终端侧防护措施的基础上，通过投放诱饵文档，实时监控诱饵文档的改动，依据文档的 MD5 值判定系统是否遭受勒索病毒加密，一旦单位时间内多个诱饵文件连续发生改动，即正遭受勒索病毒攻击，立即终止修改诱饵文件的进程，并隔离进程对应的文件；对已知勒索病毒，可通过内核抢占字符，实现对特定勒索病毒的攻击免疫；当发现系统中文件创建、修改或进程启动、模块加载等事件时，应用层应主动调用杀毒引擎对此文件进行病毒扫描检查；建立应用进程的白名单，实现对恶意应用进程的拦截。

（4）加强用户网络安全意识。以培训、演练等提高网络安全意识，在用户层面切断勒索病毒传播的入口。例如，在文件方面，不点击来源不明的邮件附件、打开邮件附件前进行安全查杀等；在网站方面，不从不明网站下载软件等；在外接设备方面，不混用工作和私人的外接设备、关闭移动存储设备自动播放功能并定期进行安全查杀等。

- 文件方面：在文件安全方面的安全意识包括但不限于不安装来路不明的软件、不点击来源不明的邮件附件、禁用微软 Office 软件宏功能，以及不轻易打开文件扩展名为 js、vbs、wsf、bat、cmd、psl、sh 等脚本文件和 exe、scr、com 等可执行程序，对于陌生人通过邮件等方式发送的压缩文件包打开前进行安全查杀等。
- 网站方面：在网站安全方面的安全意识包括但不

限于不从不明网站下载软件、不点击不可信来源邮件中的URL 等，同时浏览网页时应提高安全警惕，不浏览含有色情、赌博等不良信息的网站，使用具有安全功能或安全提醒的浏览器软件，降低遭遇网站挂马、网站钓鱼等安全风险的可能。

- 外接设备方面：在设备安全方面的安全意识包括但不限于不使用来路不明的移动存储设备、不混用工作和私人的外接移动存储设备、定期对移动存储设备进行安全查杀等，在工作设备与移动存储设备外连时，关闭移动存储设备的自动播放功能，并使用安全软件对移动存储设备进行安全查杀。

- 远程使用方面：在远程使用方面的安全意识包括但不限于远程访问仅向必要人员授权、关键终端采用双重认证、设定账户异常锁定策略、修改默认远程使用端口如RDP 协议 3389 端口和 SSH 协议 22 端口、通过防火墙限制和只允许特定地址连接、限制远程访问数据库。

（5）做好重要数据备份工作。根据文件和数据的重要程度分类分级进行存储和备份，如主动加密存储重要、敏感的数据和文件，防范利用勒索病毒的双重或多重勒索行为。明确数据备份的范围、内容、周期等，定期采取本地备份、异地备份、云端备份等多种方式进行数据备份，增加遭受勒索病毒攻击且数据文件加密、损坏、丢失等情况下恢复数据的

可能。

- 数据分级分类策略:在理清组织内部数据资产全貌的基础上，根据数据对组织重要程度、数据本身属性等，采取分级分类的方式存储和备份数据。如按照公开、内部、秘密数据，或根据数据对应的不同业务类型，对数据进行存储和备份。

- 敏感数据加密存储：对关键数据、敏感数据和文件进行加密存储，如利用加密工具、加密系统、加密硬件等方式，对存储数据的硬件设备进行全盘加密或对存储数据的扇区进行加密、将数据文件加密存储至硬件设备、在数据传输中进行加密等。

- 定期进行数据备份：采取实时备份、定时备份等方式对数据进行备份。如在存储设备发生传输、接收等数据变化时进行同步或异步实时备份，设置明确数据备份时间定时进行数据备份，或通过设置数据存储目录变化、应用操作结束等数据备份触发条件进行数据备份。

2. 事中：做好应急响应

（1）隔离勒索病毒感染设备。确认遭受勒索病毒攻击后，应采取断网、关机等方式隔离感染设备。其中，可采取拔掉设备网线、禁用设备网卡、关闭无线网络等方式断网，防止勒索病毒通过感染设备自动连接的网络在内部传播并进一步感染其他设备。

- 物理隔离：确认遭到勒索病毒攻击，为防止感染设备自动通过连接的网络进一步传播病毒，同时防止攻击者通过感染设备继续攻击入侵其他设备，采取断网、断电的方式隔离感染设备，同时关闭设备的无线网络、蓝牙连接等，禁用网卡并拔掉设备全部外部存储设备。

- 修改口令：为防止由于口令泄露、破解等导致攻击者攻击入侵，进而实施勒索病毒攻击，同时防止攻击者使用泄露、破解的口令进一步扩大攻击范围，立即修改感染设备的登录密码、同一局域网下的其他设备密码、最高级系统管理员账号的登录密码。

（2）排查勒索病毒感染范围。在已经隔离感染设备的情况下，对数据备份、网络分布、信息泄露等情况进行排查，并检查核心业务是否遭受攻击影响。对于感染情况不明的设备，应提前进行磁盘备份，在隔离网内现场或线上排查，避免启动设备时因残留勒索病毒再次感染。

- 信息泄露排查：一旦发现遭受勒索病毒攻击，及时排查信息泄露情况。同时，在隔离勒索病毒感染设备后，及时排查存储有敏感信息的设备异常访问情况，确认是否存在敏感数据泄露的风险。

- 网络拓扑排查：了解现场环境的网络拓扑、业务架构、设备类型等关键信息，评估勒索病毒传播范围、攻击手段等，对勒索病毒失陷区域作出初步判断，为控制病毒扩散

和根除病毒威胁提供支撑。

- 业务系统排查：在确认设备感染勒索病毒后，并已经进行隔离的情况下，应即对核心业务系统和备份系统进行排查，重点排查核心业务系统是否遭受攻击影响，生产经营相关系统是否遭到加密，进一步确定勒索病毒感染范围。

- 数据备份排查：隔离勒索病毒感染设备后，及时排查数据备份和可用情况。对于重要服务器等设备采取数据备份冗余策略，在一台服务器遭受加密后，及时查看备份设备是否可以迅速有效对接，确保核心业务正常运转。

（3）研判勒索病毒攻击事件。通过感染的勒索病毒勒索信息、加密文件、桌面背景、可疑样本、弹窗信息等借助工具对勒索病毒进行分析，或求助网络安全专业人员对勒索病毒感染时间、传播方法、感染种类等进行排查，确定感染的勒索病毒类型，便于尝试进行病毒破解等。

- 研判勒索病毒种类：勒索病毒在感染设备后，攻击者通常通过加载勒索提示信息胁迫用户支付赎金。遭受勒索病毒攻击的组织可从加密的磁盘目录中寻找勒索提示信息，并根据勒索病毒的标识判断本次感染的勒索病毒种类。

- 研判攻击侵入手段：通过查看设备保留的日志和样本，判断攻击者攻击入侵的方式。如日志信息遭到删除，通过查找感染设备上留存的勒索病毒的样本或可疑文件，判断攻击者攻击入侵的方式，便于进行安全隐患修补。

（4）尝试进行勒索病毒破解。在确定勒索病毒类型的基础上，尝试利用勒索病毒本身加密特性、流程等破解，进而恢复遭到加密的全部或部分数据，如针对已经公布私钥、以文件大小作为密钥等的部分勒索病毒尝试进行破解。其中，病毒破解技术专业性极高，可联系网络安全企业寻求协助。

- 已知私钥破解：通过各种渠道获取到勒索病毒攻击团伙私钥进行破解。如 GandCrab、Avaddon 等勒索病毒私钥已经公开，相关解密工具可用于进行特定勒索病毒的破解。
- 加密漏洞破解：通过分析挖掘勒索病毒本身编写的不规范问题，获取密钥生成方式，如动态虚拟专用网络采用的加密算法利用文件大小作为密钥，生成密钥进行解密。
- 明密文碰撞解密：部分勒索病毒采用加密生成的固定长度密钥串，可能通过明密文对比计算获取勒索软件使用的加密密钥，进而进行勒索病毒的破解。
- 暴力破解：通过对勒索软件有限的密钥空间进行穷尽，如针对利用时间做种子产生伪随机数作为密钥的情况，进行暴力破解获取密钥。

3. 事后：实施安全加固

（1）利用备份数据进行恢复。根据遭受勒索病毒攻击影响相关设备数据备份的情况，按照数据恢复要求、备份日志，衡量数据恢复时间成本、数据重要程度，确认数据恢复范围、顺序及备份数据版本，利用离线、异地、云端等备份数据恢复。

- 本地数据恢复：利用本地数据备份的数据进行恢复。本地备份数据同样遭到勒索病毒加密的，可利用磁盘修复工具、文件容错机制，或联系专业数据恢复企业进行数据恢复。

- 异地数据恢复：使用数据备份副本进行数据恢复，将备份的数据迁移至本地。异地备份数据遭到加密时，同样利用磁盘修复工具、文件容错机制，或联系专业数据恢复企业进行数据恢复。

- 云端数据恢复：将云快照备份的特定时间节点数据或云镜像备份的全量数据，下载至本地进行云端数据恢复。数据本身存储、应用均在云端，根据组织对本地存储、应用需求，选择性进行数据恢复。

（2）更新网络安全管理措施。根据勒索病毒攻击事件暴露出的问题，针对性修订完善网络安全管理制度，做好攻击预警和处置，同时对攻击事件进行复盘，并更新网络安全突发事件应急预案，进一步落实网络安全责任。

- 完善管理制度：根据勒索病毒攻击事件暴露出的问题，及时有针对性的完善网络安全管理制度。例如，检查、识别网络安全管理流程执行的现行管理标准与国家相关法律法规、管理规定、方针策略等要求和特点适应；准确识别获取的法律法规标准对组织的适用性要求，进行必要的网络安全管理制度和管理标准更新，及时清理过期的规章制度，确保

组织网络安全管理制度符合持续改进的要求。

- 更新应急预案：应急预案与应急实践是相互补充与促进的关系。在执行应急预案的情况下，应对每次网络攻击事件进行复盘，并根据暴露出的网络安全问题，对应急预案包含的应急流程、关键措施等进行更新。例如，当出现因钓鱼邮件而引发的勒索病毒事件，则需要在应急预案中设立专项处理钓鱼邮件的管理小组，细化每个责任人的职责，同时需要细化个人安全管理制度的条例。

（3）加强网络安全隐患修补。在消除勒索病毒攻击影响的情况下，开展网络安全隐患排查和修补。例如，在权限管理方面，重点排查弱口令、账户权限、口令更新和共用等问题；在漏洞修补方面，及时更新系统、软件、硬件等漏洞补丁。

- 口令管理：严格执行账户口令安全管理，重点排查弱口令问题，进一步健全组织内部口令管理机制。例如，规定全部个人终端、服务器等设备配置口令，禁止存在无口令现象；在传递账号和口令时，采取加密措施进行传输，避免在传输过程中遭到截取；口令设置应具有足够的长度和复杂度，且使用数字、字母和符号等组合形式搭配；明确口令更新周期、定期进行修改，在规定期限内使用口令，用户必须在管理员要求更改口令时进行口令更改；新口令与旧口令间应没有直接的联系，加强利用旧口令推测新口令的防范；口令不应取具有特定含义的组合形式，如使用者姓名、生日和

其他易于猜测的信息；严格检查口令的重复率，以防攻击者利用统一口令攻击入侵多台设备。

- 漏洞修补：完善组织资产漏洞、补丁升级、配置加固等，健全统一管理的安全机制和安全运营规范，例如，建立资产漏洞库、补丁源、补丁可靠性验证、定制补丁升级预案、补丁灰度升级、留存审查机制等安全措施，并按照安全运营规范规定的角色、职责、流程严格执行，确保系统自身的安全性；通过对所有系统的情况进行调查或利用漏洞扫描工具进行检测，了解其实际漏洞存在情况；禁用官方已经停止更新维护的系统，及时更新至新系统再投入使用；在发现软件和硬件产品存在漏洞时，应及时禁用，避免攻击者在此期间利用该漏洞进行攻击，关注补丁发布情况，修补漏洞再恢复使用。

- 权限管控：做好组织内部权限管控管理，保证员工各司其职，做到责任到人、权责分明。例如，员工在工作职责发生变化时，现有职责与现有账号权限不符合时，应当申请权限的变更，管理员发现用户具有当前工作不需要的权限，应告知并停止多余的权限；定期检查账户情况，通过联系账号负责人决定账号的关停情况和权限范围等；开通账号应按照原则建立权限，以最小权限、最小资源的形式对其提供服务，如需更高权限，需根据实际情况进行审核批准。

- 内网强化：在内外网间根据安全需求，将防火墙、网

闸单向传输、入侵检测、深包检测还原与缓存等手段有机结合建立安全屏障。在终端侧应部署立足于有效防护的终端防御软件。每天定期排查设备的事件告警，避免出现事件已经发生却仍未知晓的情况；加固系统防护策略；排查主机相关安全设置，将存在问题的及时进行修改。严格管控移动设备接入内网，避免安全威胁通过移动设备传入，并在内网不同区域间建立网络监控机制，及时发现、处置不同区域之间网络安全事件，避免网络安全事件危害扩大。在组织内部部门网络间做好相应管控措施，防止安全威胁事件从单一部门传播到整个网络。部门间进行互联时，应按照独立访问的原则建立互通访问权限，以最小权限访问、最小资源的形式进行互联互通。

4. 恢复感染设备正常使用。感染勒索病毒设备再次投入使用的，在采取磁盘格式化、系统重装、删除可疑文件和程序、消除勒索信息和加密文件等措施的情况下，避免二次感染勒索病毒，再恢复设备正常使用。

- 磁盘格式化：在确保勒索病毒无法进行隐藏、再次执行等情况下，进行磁盘格式化。由于部分勒索病毒对系统主引导记录进行篡改，将勒索病毒自身移动至系统磁盘中隐藏，实现持久化的驻留，无法对操作系统磁盘进行格式化，应将勒索病毒进程终止，删除样本母体、衍生物、添加的注册表项及启动项，确保系统磁盘中不存在勒索病毒，且勒索病毒

无法再次执行，避免再次感染勒索病毒。

- 删除可疑文件和程序：删除可疑文件和程序前，应终止勒索病毒进程，避免出现进程占用，导致无法删除。部分勒索病毒将自身名字修改为系统进程，可使用安全软件、专杀工具等查看当前系统程序的使用情况，避免终止进程错误导致系统无法正常运行，同时可使用安全软件病毒查杀功能查找并删除隐藏在系统中的可疑文件和程序。部分勒索病毒执行中，将自身文件属性设置为隐藏或移动至临时目录、启动项目录或系统根目录下，同时，在注册表添加启动项，实现开机启动功能，达到持久化驻留的目的，可将文件隐藏属性打开，移除可疑文件和程序，删除其添加的注册表项，确保设备重启无再次勒索情况。

- 消除勒索信息和加密文件：根据勒索病毒感染、数据文件恢复等情况，选择恰当的措施，消除勒索信息和加密文件。例如，已经通过病毒破解、数据恢复等恢复加密文件，可直接删除被加密文件；无法对加密文件进行解密，且被加密文件具有一定的重要性，可对加密文件进行备份保存，以便于未来利用解密工具等恢复加密文件，备份工作完成可直接删除加密文件。

附录一

近期勒索病毒攻击事件

（一）起亚美国遭 DoppelPaymer 勒索病毒攻击，导致长时间 IT 系统中断

2021 年 2 月，起亚汽车美国公司（KMA）遭 DoppelPaymer 勒索病毒攻击，要求起亚在两到三周内支付约 2000 万美元的比特币赎金（约合人民币 1.29 亿元），一旦延期支付，赎金将达到约 3000 万美元（约合人民币 1.93 亿元）。攻击者在其数据泄露网站称，已经窃取起亚美国大量数据，起亚美国若未与之谈判，将在两到三周内公布数据。此次，勒索病毒攻击导致起亚美国长时间 IT 系统中断，影响其应用程序、电话服务、支付系统等。

（二）CAN 保险公司遭勒索病毒攻击，支付高额勒索赎金

2021 年 3 月，美国最大的保险公司之一 CNA Financial 遭 Phoenix 勒索病毒攻击，因无法自行恢复数据，CNA 支付 4000 万美元（约合人民币 2.57 亿元）高额赎金。CNA 在声明中拒绝就赎金发表评论，并提出在处理此事时已遵守美国相关法律、法规等。

（三）宏碁遭 REvil 勒索病毒攻击，攻击团伙索要高额赎金

2021 年 3 月，中国台湾计算机制造商宏碁（Acer）遭 REvil 勒索病毒攻击。REvil 勒索病毒团伙在其数据泄露网站公布遭窃取文件的图片作为证据，包括财务电子表格、银行余额和银行通信等，索要赎金 5000 万美元（约合人民币 3.25 亿元），经谈判如提前支付赎金，勒索病毒团伙可提供 20%的赎金折扣，提供解密工具、漏洞报告，并删除窃取到的文件。

（四）美最大成品油管道运营商科洛尼尔遭暗面组织勒索病毒攻击，严重影响美东海岸成品油供应

2021 年 5 月，美国最大成品油管道运营商科洛尼尔（Colonial Pipeline）公司遭到暗面（Darkside）勒索病毒攻击，导致美国东部沿海主要城市输送油气的管道系统被迫下线，成品油供应中断。科洛尼尔支付约 500 万美元（约合人民币 3200 万元）的加密货币勒索赎金，获得暗面组织提供的勒索病毒解密工具，但由于该工具恢复数据速度缓慢，科洛尼尔已采用备份数据进行系统恢复。

（五）巴西肉类制造巨头企业 JBS 遭 REvil 勒索病毒攻击，致多地暂停作业

2021 年 5 月，巴西肉类制造巨头企业 JBS 遭受 REvil 病毒勒索攻击，导致其位于美国和加拿大地区的部分工厂暂停作业，其中，澳大利亚所有 JBS 肉类工厂停产。6 月 9 日，JBS 美国分部同意支付 1100 万美元（约合人民币 7030 万元）比特币赎金，以防止黑客泄露公司数据。

（六）安盛保险集团遭 Avaddon 勒索病毒攻击，海量数据遭到窃取

2021 年 5 月，保险巨头安盛位于泰国、马来西亚、中国香港、菲律宾的分公司遭受 Avaddon 勒索病毒攻击。Avaddon 在其数据泄露网站上称，已经从安盛亚洲业务中窃取 3TB 的敏感数据，包括客户的医疗报告、身份证复印件、银行账户报表、索赔表格、付款记录、合同信息等。

（七）美核武器分包商遭 REvil 勒索病毒攻击，企业员工信息遭泄露

2021 年 6 月，美国能源部核安全管理局（NNSA）的核武器分包商 Sol Oriens 遭受 REvil 勒索病毒攻击。企业员工信息数据文件（包括姓名、社保号码、工资表以及员工培训计划等）遭受窃取，但攻击者未获得核武器合作项目文件等机密内容的访问权限。未来攻击者可利用员工信息发动社会工程学攻击，进一步获取企业内部敏感信息。

（八）北约“北极星”计划云平台供应商遭受勒索病毒攻击，攻击者索要高额赎金

2021 年 6 月，勒索病毒攻击者入侵西班牙企业 Everis 及其位于南美洲的子公司，北约“北极星”计划云平台相关代码、文档等敏感信息可能遭到窃取。攻击者称有能力植入后门，攻击出于政治动机，威胁将数据发送到俄罗斯情报部门，以此勒索超 10 亿欧元（约合人民币 76 亿元）的赎金。

（九）西班牙电信运营商 MasMovil Ibercom 遭 REvil 勒索病毒攻击，数据遭到窃取

2021 年 7 月，西班牙电信运营商 MasMovil Ibercom 遭 REvil 勒索病毒攻击，且 REvil 勒索攻击团伙在其专门的数据泄露网站中表示，已窃取该企业大量敏感信息，并公开备份文件、经销商名单等部分数据截图作为已成功实施网络攻击的证据。

（十）攻击者利用托管服务软件供应链机制传播勒索病毒，已致 800 余家商店关闭

2021 年 7 月，疑似 REvil 勒索病毒攻击团伙利用安全漏洞，攻击入侵美国软件供应商卡西亚（Kaseya）软件补丁和漏洞管理系统 VSA 服务器设备，并利用软件更新机制传播 REvil 勒索病毒。REvil 勒索病毒攻击团伙声称在此次事件中锁定大量系统，并胁迫感染勒索病毒的受害者支付价值约 7000 万美元（约合人民币 4.5 亿元）的比特币勒索赎金。该事件导致瑞典连锁超市巨头 Coop 已关闭 800 多家商店服务。

附录二

典型勒索病毒

（一）REvil/Sodinokibi

REvil/Sodinokibi勒索病毒于2019年4月首次发现，主要针对Windows、Linux平台，属于数据窃取类勒索病毒，其传播方式主要包括钓鱼邮件、远程桌面入侵、漏洞利用等。该病毒家族套用、利用现有恶意工具作为攻击载体，同时传播勒索病毒、挖矿木马、窃密程序，并通过加密用户文件、窃取用户数据进行双重勒索。

（二）DarkSide

Darkside勒索病毒于2020年8月首次发现，主要针对Windows、Linux平台，属于数据窃取类勒索病毒，同时具有勒索病毒即服务功能。Darkside勒索病毒RSA1024和Salsa20算法加密文件，同时应用多线程技术，提升文件加密的速度。Darkside勒索病毒团伙通常采用“解密和泄密”的双重勒索策略，威胁攻击目标支付赎金。

（三）Conti

Conti勒索病毒于2019年12月首次出现，主要针对Windows、Linux平台，属于数据窃取类勒索病毒，并在2020年7月作为个人的勒索病毒即服务（RaaS）开始运营，感染攻击目标删除卷影副本，并禁用修复、删除本地设备备份目录，采

用并发线程技术对感染设备的文件快速加密。自2020年8月以来，该组织在暗网数据泄露网站，威胁攻击目标发布窃取到的数据。

（四）Avaddon

Avaddon勒索病毒于2020年6月首次发现，主要针对Windows平台，并通过钓鱼邮件等传播，采用RSA2048和AES256加密算法对文件进行加密。2021年6月，Avaddon勒索病毒攻击团伙称将停止运营，并关闭所有业务，并为已经遭受攻击的受害者发布2934个解密密钥。

（五）DoppelPaymer

DoppelPaymer勒索病毒于2019年6月首次发现，主要针对Windows平台，属于数据窃取类勒索病毒，通过钓鱼邮件、远程桌面入侵等传播，采用RSA和AES进行加密，因与BitPaymer勒索病毒大部分代码相同，可能是BitPaymer的变种，同样由INDRIK SPIDER黑客组织运营。

（六）Ryuk

Ryuk勒索病毒于2018年8月首次发现，主要针对Windows平台，属于数据窃取类勒索病毒，由黑客组织GRIM SPIDER幕后操作运营，利用Cobalt Strike和PowerShell Empire等工具，及通过钓鱼邮件、漏洞利用等方式传播，其主要攻击目标领域包括科技、医疗、能源、金融以及政府部门，攻击导致企业服务瘫痪、系统被迫下线等严重后果。

（七）RansomLock

RansomLock勒索病毒于2013年1月首次发现，主要针对Windows凭条，属于锁屏类勒索病毒，通过公共互联网连接执行传播，通常将主机名、IP地址、屏幕分辨率等感染设备信息发送至攻击者命令和控制服务器，回传适合整个屏幕大小的图像文件，锁定感染设备屏幕，显示蓝屏死机错误的消息，同时屏幕显示消息，计算机存在健康风险，拨打电话解锁屏幕。

（八）Lucy

Lucy勒索病毒于2018年9月首次出现，主要针对移动平台，通过社交媒体链接和即时消息APP传播，对感染安卓设备的文件进行加密，并显示勒索信息。勒索信息称美国联邦调查局（FBI）起诉受害者在设备上处理色情内容，并将用户详细信息上传到美国FBI网络犯罪部数据中心，要求受害者需要通过信用卡支付赎金。

（九）Babuk Locker

Babuk Locker是2021年1月发现的勒索病毒，其勒索病毒攻击团伙持续对Babuk Locker进行版本更新，并增加针对勒索专门设计的数据提取功能，用于窃取高价值目标重要数据信息。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62305730

传真：010-62300264

网址：www.caict.ac.cn