2021 年上半年全球勒索软件趋势报告

编号	DBAPP-TIC-21062501
关键字	基础设施、勒索软件
发布日期	2021 年 6 月 25 日
更新日期	2021 年 6 月 25 日
TLP	公开
分析团队	安恒猎影实验室

安恒威胁情报中心-猎影实验室

1. 引言

2021 年，在网络安全快速发展的同时，网络犯罪产业也在逐渐壮大，其中，勒索软件在众多网络威胁中表现最为亮眼，在美国燃油管道事件发生后，被广大新闻媒体报道，热度更是高居不下，引发广泛关注。

勒索软件是目前网络空间中最具破坏性且传播广泛的一种恶意软件，旨在加密目标设备上的文件，阻止目标访问，并索要赎金以换取解密密钥。此外，部分勒索软件还会在攻击过程中窃取目标信息，并威胁在暗网上发布或出售数据，对企业和个人造成严重的影响。

安恒威胁情报中心猎影实验室对 2021 年上半年勒索攻击态势进行了研究分析，并从上半年攻击事件概况、行业影响、攻击趋势等多个角度进行了阐述。

2. 2021 年上半年全球勒索攻击事件概况

据不完全统计， 2021 年光上半年就至少发生了 1200 多起勒索软件攻击事件，与 2020 年发生的已知公布的大约 1420 起勒索攻击事件已经十分接近，其中针对医疗系统和教育行业的攻击增加了 45%，平均赎金从去年的 400,000 美元提高到今年的 800,000 美元，而这仅仅是上半年的统计数据。

在众多勒索软件攻击事件中，有将近 70%的勒索团伙采用双重勒索策略，以数据泄露问题威胁受害者支付巨额赎金，由于赎金通常是通过加密货币进行支付的，而加密货币又具有一定的安全性及匿名性，因此在追查过程中将给执法部门带来一定的难度和挑战。

在攻击目标方面，政府实体和关键基础设施组织遭到勒索软件攻击逐渐变得普遍，其中具有标志性的有美国管道运营商 Colonial Pipeline 勒索事件、美国核武器承包商 Sol Oriens 勒索事件、JBS 肉类生产商勒索事件。这些攻击事件具备 APT 的特点，并呈现出高针对性和复杂性。

勒索犯罪产业在高速发展的同时，也吸引着越来越多的人加入，不断推动勒索产业发展，这使得其攻击和运营迈向成熟，部分勒索犯罪团伙甚至具备实施复杂 APT 攻击的技术能力。

#勒索事件

2021 年上半年发生了非常多的勒索事件，这里我们列举了一些重点事件作为参考。如美国输油管道公司 Colonial Pipeline 遭 Darkside 勒索软件攻击事件、全球最大的肉类供应商 JBS 遭遇 REVil 勒索团伙攻击事件等都有一定的影响力。

#时间轴#

2021 年 2 月中旬，Ziggy 勒索软件管理员宣布停止运营，随后发放了 922 个解密密钥，并声称将退还赎金给受害者。

2021 年 3 月 20 日，全球知名电脑制造商宏碁遭遇 REvil 勒索软件攻击，并索要 5000 万美元赎金（约 3.3 亿人民币），创下最高勒索软件赎金记录。

2021 年 3 月 21 日，美国保险公司 CNA Financial 遭 Phoenix 勒索团伙攻击，因无法自行恢复数据，最终支付 4000 万美元（约 2.57 亿人民币）赎金，创下历史最高的付款赎金记录。

2021 年 4 月 27 日，美国华盛顿警察局遭 Babuk 勒索软件攻击，威胁不支付赎金将曝光线人信息。

2021 年 5 月 7 日，美国输油管道公司 Colonial Pipeline 遭 Darkside 勒索软件攻击，导致东海岸液体燃料停止运营，该公司在 5 月 13 日支付 500 万美元赎金，以获取解密工具恢复系统运行。随后，执法机构查封 Darkside 团伙的基础设施，并追回大部分赎金。

2021 年 5 月 14 日，DarkSide 勒索团伙称无法访问基础设施，决定关闭运营。为防止执法部门打击，Revil 勒索团伙禁止其附属机构攻击社会部门（医疗保健、教育机构）及任何国家的政府部门。同日，爱尔兰卫生服务执行局（HSE）遭 Conti 勒索团伙攻击，并索要 2000 美元赎金，攻击造成全国多家医院的电子系统和存储信息无法正常使用。

2021 年 5 月 31 日，全球最大的肉类供应商 JBS 遭遇 REVil 勒索团伙攻击，导致澳大利亚所有 JBS 肉类工厂停产。6 月 9 日，JBS 美国分部同意支付 1100 万美元赎金，以防止黑客泄露公司数据。

2021 年 6 月 8 日，美国选民沟通平台 iConstituent 遭到勒索软件攻击，导致部分议员无法使用该平台检索选民信息，这是距离政客最近的一次勒索软件威胁。

2021 年 6 月 11 日，美国核武器承包商 Sol Oriens 遭遇 REvil 勒索软件攻击，导致数据被盗。

2021 年 6 月 14 日，Avaddon 勒索软件宣布停止运营，并发放 2934 个解密密钥。

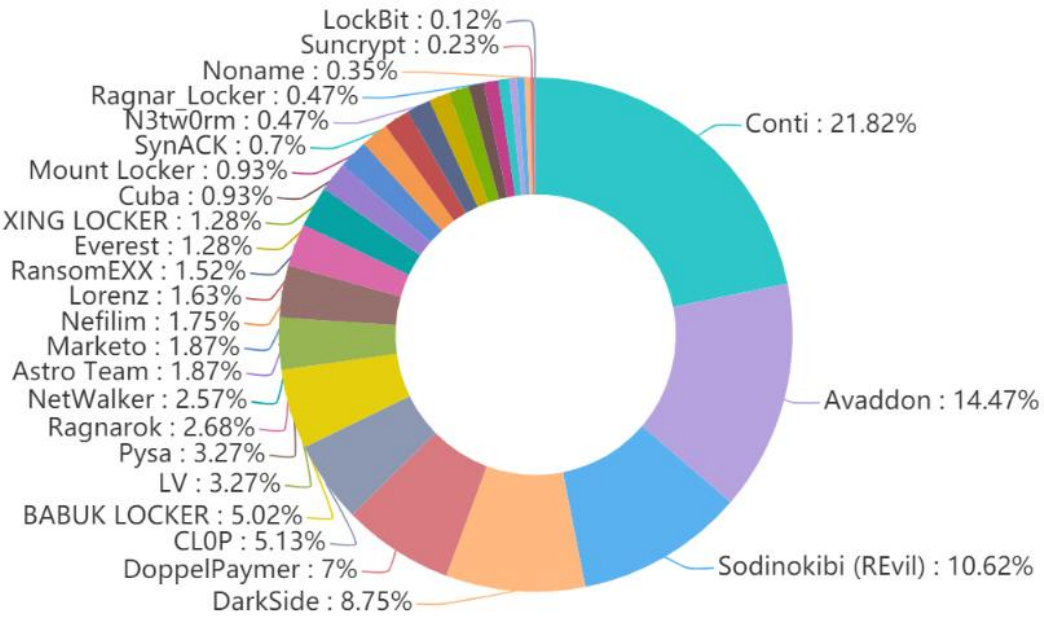
2021 年 6 月中旬，Paradise 勒索软件的.NET 版本源码在俄语黑客论坛泄露，这是继 Dharma 勒索软件在 2020 年泄露之后，近年来源代码泄露的第二个主要勒索软件。

#勒索团伙

2021 年，以勒索软件为主的网络犯罪团伙也发生了翻天覆地的变化，一些团体宣布停止运营，一些团体解散后重组，一些团体暂时停止活动，例如 Egregor 和 Maze。主流勒索团伙的退位将被新兴勒索团伙替换，从而导致勒索犯罪生态的生生不息。

其中，一些勒索软件运营团伙从勒索软件即服务（RaaS）转向私有化服务，并将目光放在了其他系统平台。

2021 年涌现了很多新的勒索团伙加入，其中比较活跃组织的有 Revil、Dark Side、Avaddon、Conti 和 Babuk，2021 年上半年勒索团伙攻击事件占比分布如下图所示。



2021 年上半年勒索团伙攻击事件占比分布图

在 2021 年的勒索攻击事件中，攻击活动最为频繁的是 Conti 组织，占上半年攻击事件的 21.82%，排名第二的 Avaddon 团队在 6 月 14 日宣布关闭运行。而关注度比较高的是 DarkSide 和 Revil 组织，其中 DarkSide 是美国燃油管道攻击事件的始作俑者，现已宣布暂停运营。Revil 组织今年相当活跃，其攻击了多个国家的重要机构和实体，例如美国核武器承包商、巴西司法局、JBS 肉类生产商等。

以下是 2021 年较为活跃的一些勒索组织的简要介绍。

■ **Babuk**

Babuk 是 2021 年加入的新兴勒索团伙，目标是窃取高级机密类文件。其使用的 BabukLocker 勒索软件于 2021 年 1 月被首次披露，作为今年新出现的勒索软件，该运营商不断地对 Babuk Locker 进行版本更新，并增加了针对敲诈勒索而设计的数据提取功能。

Babuk 勒索软件曾多次攻击国外著名的组织或企业，如 NBA 休斯顿火箭队、美国主要军事承包商 PDI 集团以及日本制造商 Yamabiko 公司等。4 月 27 日，Babuk 勒索软件团伙攻击了美国华盛顿特区大都会警察局，威胁警方不交赎金就向当地黑帮泄露警方线人信息，并声称会继续攻击美国的 FBI 及 CSA 部门，性质及其恶劣。

■ **Avaddon**

Avaddon 勒索软件团伙是来自俄罗斯的黑客组织，在 2020 年 6 月 2 日首现于俄罗斯黑客论坛，所开发的 Avaddon 勒索软件除了供自身使用之外，也通过提供勒索即服务（RaaS）谋求外部合作以获取更大的利益。

Avaddon 勒索团伙利用 Phorpiex 僵尸网络传播，攻击对象包括中国和非独立国家联合体，平均赎金要求约为 60 万美元。2021 年 6 月 14 日，Avaddon 勒索软件团伙宣布停止运营，随后关闭所有业务，并为过去的受害者发布了 2934 个解密密钥。

■ Conti

Conti 勒索软件在 2019 年 12 月首次被发现，并在 2020 年 7 月作为个人的勒索软件即服务（RaaS）开始运营，属于新兴的双重勒索软件团伙，被认为是流行的 Ryuk 勒索软件家族的变种。

Conti 勒索软件团伙通过多种流行的恶意软件传播，包括 Trickbot/Emotet 和 BazarLoader。2021 年 5 月，Conti 勒索软件团伙连续攻击了美国国防承包商 BlueForce 和爱尔兰公共卫生服务执行局 HSE，分别索要 969,000 美元和 19,999,000 美元的赎金。在过去的一年中，Conti 勒索软件团伙袭击了美国至少 16 个医疗保健和紧急服务机构，影响了超过 400 个全球组织，其中 290 个受害组织位于美国。

■ DarkSide

DarkSide 组织在 2020 年 8 月成立，以勒索软件即服务（RaaS）形式运营，曾声称不会勒索医疗、教育、非盈利及政府机构。DarkSide 通过收集到的企业信息评估企业的财力，然后再决定勒索的赎金数额。据调查，该组织在成立不到一年的时间内，感染了 99 个组织，其中大约有 47%的受害者支付了赎金，平均付款为 190 万美元，总收入高达 9000 万美元。

2021 年 5 月初，Darkside 勒索软件团伙攻击了 Brenntag 北美分部，随后 Brenntag 被迫向 DarkSide 勒索软件团伙支付了价值 440 万美元的比特币赎金。

5 月 7 日，Darkside 勒索软件团伙攻击了美国最大的输油管道公司 Colonial Pipeline，受害公司向 DarkSide 支付了将近 500 万美元（约 3200 万人民币）的赎金，执法部门追回了大部分赎金，并查封 DarkSide 的网络基础设施，受执法影响，该组织在 5 月 17 日宣布关闭运营。

■ Revil/Sodinokibi

最老练的勒索组织，曾接受过采访，声称可以控制导弹发射系统，近期攻击了多个重要的机构和组织，例如核设施合作商。

Revil 是目前最活跃的勒索软件运营商（RaaS），于 2019 年 5 月 24 日首次

在意大利被发现，Revil 被称为 GandCrab 的“接班人”。GandCrab 曾是最大的 RaaS 勒索软件运营商，在 2019 年 6 月宣布停止运营。

REvil 在最近两年，以国内外大型、中型企业作为攻击目标频繁发起勒索攻击，REvil 勒索软件有一套成熟的运营机制，攻击者负责发起勒索攻击，线上客服负责在线与受害者谈判。

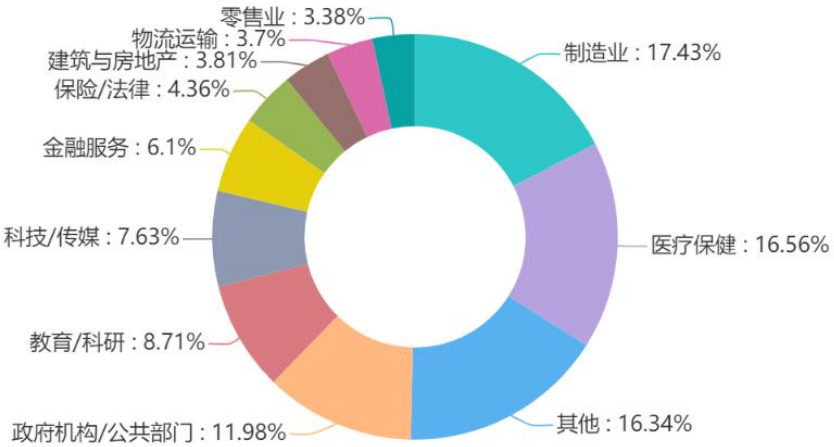
2021 年 3 月，REvil 勒索软件攻击了计算机巨头宏碁公司，并提出高达 5000 万美元的赎金要求，创下最高勒索软件赎金的记录。

5 月 31 日，REVil 攻击了全球最大肉类生产商 JBS 公司，影响了 JBS Foods 在澳大利亚以及美国、加拿大和其他国家的设施。6 月 9 日，该公司的美国分部向 REVil 支付了价值 1100 万美元的比特币，以重新获得对其系统的访问权限。

在多次获得高额赎金后,REvil 勒索软件团伙变得愈发猖狂,6 月 11 日,REvil 勒索软件攻击了美国核武器承包商 Sol Oriens，声称窃取了机密文件，并打算在暗网拍卖窃取的数据。

3. 2021 年上半年全球受勒索软件影响的行业

2021 年上半年，在全球范围内，制造业受勒索软件的影响较为严重，占攻击事件的 17.43%，针对医疗行业的攻击与往年相比，仍处于上升阶段，占比达到了 16.56%。政府机构、教育、科技、传媒、金融等也影响较重。另外，自美国管道供应商勒索攻击事件以来，美国政府表示将大力打压勒索软件，此后，针对美国政府部门的勒索攻击有所放缓。



2021 年上半年勒索攻击事件受害行业分布图

■ 公共部门及能源行业

越来越多的犯罪组织利用勒索软件攻击关键基础设施，这些攻击将可能影响国家的正常运作能力。5 月 7 日，美国最大燃油运输管道商 Colonial Pipeline 公司遭遇勒索软件攻击，被迫暂停石油输送业务，对美国东海岸燃油供应造成严重影响。在管道事件发生后的不久，5 月 14 日，爱尔兰卫生服务执行局(HSE)同样遭到勒索软件攻击，该事件致使医疗服务系统停止，让原本就稀缺的医疗资源变得更加紧张。

根据坦普尔大学(Temple University)整理的公开数据显示，在 2019 年至 2020 年期间，针对关键基础设施的攻击发生了 440 次，而 2021 年，这个数字正在不断上升，并且所有迹象表明，将来的攻击频率还会更高。

■ 教育行业

教育部门一直存储着诸如知识产权、财务数据、职工及学生信息等宝贵数据，犯罪分子瞄准这点，将其列为敛财目标。随着新冠疫情的全球蔓延，很多教育部门选择将课程转移到线上，针对教育行业的攻击将给远程学习系统造成沉重的安

全压力。自 2021 年以来勒索软件攻击中断了至少 700 所院校的学习计划，平均支出在 40 万美元左右。导致这种现象发生的部分原因是高校的网络安全防护能力普遍脆弱，教育部门应加强面对网络威胁时的准备工作。

■ 医疗行业

自新冠疫情发生以来，针对医疗行业的勒索攻击数量正在急剧增加，自去年 11 月份以来，针对医疗机构的网络攻击增加了 45%。据统计，全球医疗保健领域只有 28%的组织能够在数据加密文件前阻止攻击。由于医院的特殊性导致它对数据和业务的实时性要求很高，一旦数据被加密，将影响正常的就医秩序，并引发一系列的问题，甚至影响病患的生死，因此医院往往会选择支付赎金以恢复系统，这使其成为勒索团伙的攻击目标。

医院的信息化建设及防护水平的提高刻不容援，否则类似的勒索事件将继续发生。

■ 制造业

勒索软件已成为制造业的主要威胁，仅在去年，公开记录针对制造业的勒索软件攻击数量就增加了 2 倍。对于制造业公司而言，因为系统宕机问题所带来的影响是巨大的，例如近期发生的“JBS 肉类生产商遭勒索软件攻击事件”就导致了 JBS 美国分部、澳大利亚分部的工厂停止作业，并产生广泛的影响。

对于网络罪犯而言，制造业公司是一个比较有价值的目标，因为很多情况下，制造业公司需要大量的正常运行时间才能满足生产要求，任何导致停机的攻击都可能造成大量损失。因此这些公司在遭到勒索攻击时的付款意愿更强，以快速恢复生产线的正常运行。

■ 金融行业

金融机构通常存储着客户的大量敏感信息，勒索团伙瞄准这点将其列为首要目标。例如近期发生的“美国保险公司 CNA Financial 遭勒索攻击事件”和“意大利 BBC 信贷银行勒索事件”，前者更是支付了 4000 万美元赎金，以恢复系统的正常运行。

金融单位在日常办公时大量使用基于传统文件服务器的文件共享协作模式，一旦遭到攻击，勒索软件将会通过文件服务器的文件共享通道快速传播和扩散，造成整体办公和业务运转停滞。由于这些金融机构每天都会向相关金融监管机构递交相关文件，一旦此类文件也被勒索软件感染，进一步将影响面扩大，后果不堪设想。

■ **政府机构**

政府部门一直是网络威胁攻击的主要对象，这些部门在日常履行政府职能时严重依赖计算机网络，一旦遭到勒索软件攻击，轻则重回纸质化办公，重则导致城市系统瘫痪。例如今年发生的“美国塔尔萨市勒索攻击事件”，受攻击影响，该城市的居民民无法通过电子邮件访问在线账单支付系统、公用事业账单和网络服务。

政府机构应该定期备份关键数据，并加强防护能力，以在被攻击后能够迅速恢复业务系统。

4. 勒索软件攻击趋势

勒索攻击类型的网络犯罪将会影响企业和组织业务的正常运营，自 2020 年来，越来越多的勒索团伙使用双重勒索策略攻击目标企业，即加密设备文件并窃取公司数据，这种以泄露数据为主要威胁的策略对于大型企业非常有效，设备文件被加密，企业可以通过重建系统恢复，但如果被盗数据泄露，将面临法律风险，并可能需要为违规泄密支付高额的罚金，从而引发一系列连锁反应，对公司的声誉造成重大打击。

5 月 30 日，全球最大的肉类生产商遭到 Revil 勒索组织攻击，事后，该公司通过备份系统恢复正常运营，但仍选择支付 1100 万美元的赎金，以防止 Revil 泄露被盗数据。在获取巨额赎金的背后，其实际上的攻击成本却不到 5000 美元，在地下网络犯罪中，勒索软件样本和构建器的价格在 300 到 4000 美元之间，勒索软件即服务的租金为每年 120 到 1900 美元，低成本的攻击和高利润的回报，将刺激着更多的犯罪分子加入勒索行业。

随着勒索成功的事件频繁曝光，一些来自世界各地的犯罪分子嗅到了机会，并加入勒索行业，导致出现针对本地语言的勒索攻击迹象，例如针对韩国境内部署自定义勒索软件的 Andariel 组织；模仿 Locky 的中文勒索软件等，并呈现多平台，轻量化的攻击趋势，而服务模型更是为犯罪分子提供了便利，使其可在不具备技术和经验的情况下也能实施复杂的网络攻击。

而勒索团伙在攻击企业时所提出的赎金也从最初的几万美元，过渡到现在的数百万，甚至数千万的勒索赎金。勒索犯罪团伙会积极尝试各种策略，例如删除系统备份文件、DDOS、电话轰炸、泄露警方线人信息、泄露受害者不雅照、做空公司股票等策略，为达目的不择手段，目的是增加受害者的压力，以提高赎金支付几率。导致勒索事件的性质变得更加恶劣，且更具破坏性和影响力。

现在，勒索软件呈现出攻击水平高、驻留时间短、影响范围广、勒索赎金大的趋势，并且勒索攻击逐渐变得普遍和有效。

我们总结了勒索软件攻击的趋势主要有如下一些方面。

✧ 攻击呈多平台、轻量化攻击趋势

- **勒索软件呈多平台攻击趋势**

根据调查，针对其他平台的勒索攻击正在不断增加，例如常见的 Android、Linux、Unix、ICS、Mac 平台等。其中，移动平台有着庞大的用户群体，相比 PC 的勒索软件，手机勒索病毒在近年来也在迅速发展演变，并从以往的锁屏勒索发展到现在的数据文件加密，对个人用户造成的影响巨大，相关安全问题不容小觑。

部分勒索软件运营商将重心从 Windows 转移到 Unix 和 Linux 平台开发加密模块，目前观察到的组织有 Defray777、Mespinoza、Babuk、Nephilim、Sodinokibi 和 Darkside，这些组织的加入将加快 Linux 平台的勒索软件发展。

- **针对 ICS/OT 工控系统的攻击正在扩散**

另外，一些勒索软件将目光放在 ICS/OT（工业控制系统），工控勒索软件通常具备 APT 攻击的复杂特点，部分工控勒索软件会在感染设备上筛选攻击对象，一旦找到目标，将通过脚本、Active Directory 攻击或其他机制在网络中扩散和有计划地传播，以同时实现感染和系统破坏。

工业控制系统一直是国家关键基础设施的重要组成部分，被广泛用于化工、电网、水利等领域，如果这些设施遭到勒索软件攻击，将可能导致停水、停电等严重后果，受攻击影响所造成的灾害将是不可逆，且极具毁灭性的。

2020 年 1 月，Dragos 工控安全公司披露了一个针对工控系统的 EKANS 勒索软件，该勒索软件试图干预工业控制系统，加密基础数据并将其劫持控制，要求受害者付款以解密数据。针对工控系统的恶意软件通常具备破坏性攻击行为，例如最广为人知的 Stuxnet（震网病毒）攻击事件，该攻击是国家支持的黑客实施的，旨在延迟伊朗核计划。虽然 EKANS 勒索软件的危害性远远比不上 Stuxnet，但它的出现表明网络罪犯正在往工业系统扩散，这也意味着非国家行为体对关键基础设施实体进行攻击或损害的意愿正在加强。

- **轻量化勒索软件**

2021 年 6 月 17 日，研究人员披露一个名为“DarkRadiation”的新型勒索软件，可针对 Linux 平台和 Docker 云容器，DarkRadiation 基于 Bash 脚本编写，感染链涉及多阶段攻击过程，并使用了一组复杂的 Bash 脚本和多个 C&C，脚本具有多个依赖项，通过硬编码 API 密钥与 Telegrambot 进行通信。

由于脚本不需要重新编译，即可进行快速迭代更新，通过简单的混淆器工具生成不同的脚本，可以有效规避依赖于静态文件签名检测的安全软件，从而变得更加灵活，适用性更强，预计未来将有更多轻量化的勒索软件出现。

✧ 佯装成勒索攻击掩盖真实意图

随着勒索事件的激增，一些受民族国家支持的网络组织看到了机会，将攻击伪装成勒索事件以掩盖真实意图，对目标进行网络间谍活动或实施破坏性攻击，其中比较著名的是 NotPetya 攻击事件。

2017 年 6 月，乌克兰遭受 NotPetya 勒索软件的大规模攻击，NotPetya 瞄准了乌克兰的流行会计软件（M.E.Doc）更新服务器，向用户推送包含病毒的软件更新，这个假的乌克兰税收软件更新在多个领域横向传播，像蠕虫一样感染网络，造成俄罗斯最大石油企业 Rosneft 等超过 80 家俄罗斯、乌克兰公司遭到网络袭击。黑客向能源交通、企业、银行业和国家机构等植入病毒并封锁电脑，相关用

户被要求支付 300 美元的赎金。该事件带来超过 100 亿美元的总损失。2020 年 10 月 19 日，美国司法部宣布起诉 6 名俄罗斯情报人员，指控其与 2017 年的 NotPetya 网络攻击有关，起诉书称，这 6 个人为了俄罗斯的利益，有意、蓄意地相互勾结，通过未经授权侵入电脑，部署恶意软件等方式进行了一系列破坏性行为。

通过勒索攻击活动掩盖真实意图的策略，逐渐被部分民族国家支持的威胁组织所使用。例如被认为与伊朗政府有关联的 Agrius、n3tw0rm 和 Pay2Key 组织，这些勒索团伙开出的赎金较低，并且与受害企业的联络并不积极，缺乏经济动机。被认为以勒索攻击之名，行间谍活动之实，目的是攻击以色列的实体组织，从战略层面打击敌对国家。

✧ 服务模型降低攻击门槛

网络安全在飞速发展的同时，地下市场也在蓬勃发展，并衍生出恶意软件开发和黑客服务，这类服务的供应主要通过以下几种方式提供：

1. 雇用黑客根据客户定义的要求编写恶意软件。
2. 通过地下市场或犯罪论坛购买自定义恶意软件。
3. 使用 RaaS 平台，常见的有 RaaSberry、Ranion、EarthRansomware 和 Redfox。

犯罪分子可以通过 RaaS 平台，在不懂技术的前提下创建自己的勒索软件并进行传播，只需要支付定额的费用即可一直使用，并逐渐发展成为一种名为犯罪软件即服务（CaaS）的新型网络犯罪模式。犯罪软件即服务（CaaS），指的是网络犯罪生态系统中技术人员向其他网络犯罪分子提供产品和服务的做法。

CaaS 服务在犯罪论坛和地下市场相当普遍，并具有很大的影响力，这是一个由需求驱动的市场，这种模式的危险之处有以下几点：

1. 降低网络犯罪门槛。
2. 溯源困难。这种模式使执法部门很难将攻击事件归因到特定的犯罪人员。
3. 促进高级威胁的发展。高级威胁攻击者可以使用该服务下的攻击手段和

攻击工具掩盖行动的真实意图，达到混淆视听的效果。

当 CaaS 模型应用到常见的恶意软件时，便诞生了各式各样的服务模型，例如勒索软件即服务（RaaS）、恶意软件保护即服务（PaaS）、恶意软件即服务（MaaS）以及初始访问即服务等。

其中应用比较广泛的是勒索软件即服务（RaaS）模式，该模式覆盖了绝大部分的勒索软件运营商，由于这种模式攻击成本低、且效率高，在短时间内涌现了不少新兴的勒索团伙，并使得勒索事件的数量出现了快速上升的迹象。值得一提的是，部分勒索犯罪团伙从 RaaS 运营模式转为私有化服务，只提供给具备专业知识的客户，以提高勒索攻击的成功率。

✧ 三重勒索策略或将成为主流

勒索团伙一直在尝试使用各种方法对受害公司施加压力，以增加其获取赎金的可能性，除了常见的二重勒索策略（文件加密和数据泄露）之外，还有另外一种危害极大，但易于发起，且攻击成本极低的勒索策略，也就是所谓的分布式拒绝服务攻击（DDOS）。

在 DDOS 攻击中，攻击者使用大量集中的 Web 流量攻击目标网站，导致其 Web 服务器瘫痪或造成网络卡顿问题，从而影响业务的正常运行。由于 DDOS 攻击隐蔽性强，且检测困难，因此这种攻击方式成为了难以防范的存在。

目前，部分勒索软件已整合了 DDOS 攻击能力，一些勒索软件运营商直接将 DDOS 攻击列入到 RaaS 的服务列表中，例如 SunCrypt 和 Ragnor Locker 是最早使用 DDOS 策略的勒索软件运营商，其他采用这种策略的组织包括 Avaddon 和 DarkSide。DDOS 攻击结合文件加密和数据泄露操作，组成了三重勒索策略，不仅能加密受害者电脑文件，还能对外出售敏感数据，并利用被感染电脑发送恶意网络流量，以此影响受害者系统的带宽或运行速度，若同时实施这三种攻击，所带来的后果将是非常严重且不可逆转的。

✧ 针对小型企业的攻击事件上升

2019 年 10 月，一家总部位于阿肯色州的电话销售公司在遭到勒索攻击后，

为了恢复系统而支付赎金，但后续的数据恢复工作未能按计划进行，公司领导层决定暂停所有服务，致使 300 多名员工失业。

这些小型企业通常不具备大型组织的防护及数据保护能力，由于缺乏正确处理攻击事件和防范此类攻击的知识，导致企业在面对网络攻击时非常脆弱，无法在勒索攻击中迅速恢复，甚至面临公司因攻击而倒闭的风险。勒索团伙会根据小型企业的收入调整勒索赎金，并发起了更多的攻击，预计未来针对小型企业的勒索攻击事件将会有明显的上升趋势。

✧ 通过模仿提高赎金支付几率

- **冒充其他勒索团伙以逃避制裁**

勒索团伙模仿其他犯罪组织的品牌重塑行为被认为是一种普遍的存在。例如俄罗斯的 Evil Corp 网络犯罪集团，在 2021 年 4 月底的攻击中冒充 Babuk 勒索团伙，Babuk 组织之前运营着一个名为 PayloadBin 的泄露网站，EvilCorp 组织通过将 WastedLocker 重新命名为 PayloadBin，试图诱骗受害者违反 OFAC（美国禁止受害者对 EvilCorp 组织支付赎金，支付的企业将面临被指控违反制裁的风险）规定。

- **冒充知名勒索团伙以提高赎金支付几率**

Prometheus 是一个新兴的勒索团伙，该组织在针对美国、英国和其他几个国家的攻击中，自称是 Revil 勒索组织的其中一员，但研究人员并没有发现两个组织之间的联系，Prometheus 可能是利用 Revil 组织在勒索领域的声誉和名气来增强攻击的可信度，说服受害者付款。

✧ 犯罪分子相互合作

部分勒索团伙会在黑客论坛或地下市场招募合作伙伴，以高额奖金吸引其他人加入勒索领域，为他们分发勒索软件，作为回报，这些合作伙伴将获得 60%以上的赎金。另外，一些勒索团伙还试图招募具有恶意软件开发能力或渗透测试能力的黑客为他们工作，例如 Revil 组织在黑客论坛上存放 99 个比特币作为竞赛奖金，以促进黑客技术。这些具有高技术能力的黑客加入将使勒索攻击变得更加

复杂。随着勒索软件收入的逐步提高，他们变得越来越有组织和选择性，并只招募最好的人才。

一些勒索团伙（例如 Ryuk、Egregor 和 Revil）还会选择与各种用于初始感染的恶意软件（例如 TrickBot、BazaLoader 和 IcedID）背后的参与者紧密合作，例如最多产的恶意软件 Emotet，这是一种具有破坏性的多功能恶意软件分发器，在 2018 年至 2020 年期间大量分发勒索软件，在今年 1 月，执法部门摧毁了 Emotet 的基础设施，防止进一步的感染。

✧ 通过有效信息选取高价值目标

勒索团伙在攻击目标时会先进行侦查，利用开源监视工具识别高价值目标，或寻找易受攻击的目标，当选取攻击目标后，通过分析目标公司的收入状况，制定公司承受范围内的赎金金额。如果一些初始访问代理（TrickBot、BazaLoader 和 IcedID）已经入侵了目标公司，勒索团伙将会与其建立合作，购买访问权限，利用现有的恶意软件后门实现横向移动和全域入侵。

5. 全球对于勒索软件的看法

英国政府通信总部(GCHQ)网络安全部门负责人表示，勒索软件是英国面临的主要威胁。英国国家网络安全中心（NCSC）首席执行官 Lindy Cameron 在演讲中表示，网络犯罪分子所处的生态系统正在不断发展，随着 RaaS 模式的成功，黑客加密数据并要求支付巨额赎金的现象正在不断升级，并变得越来越专业。

在美国管道运营商 Colonial Pipeline 遭黑客攻击之后，美国司法部将考虑把勒索软件攻击的调查提升到与恐怖主义类似的优先级别。

在北约的 G7 峰会上，G7 成员国领导人（来自英国、美国、加拿大、日本、德国、法国和意大利，加上欧盟）发布联合声明，承诺共同努力，以解决来自勒索软件犯罪网络的不断升级的共享威胁。并呼吁所有国家紧急识别和破坏其境内运作的勒索软件犯罪网络，让犯罪分子对其行为负责。由于大多数勒索软件攻击是由俄罗斯勒索软件团伙实施的，因此，G7 领导人还特别呼吁俄罗斯追究在其境内实施勒索软件攻击的犯罪分子的责任。

从 G7 峰会上发表的联合声明可以看出，各种领导人已达成打击勒索软件威胁的共识。随着全球逐渐建立打击摧毁勒索犯罪网络的共识，未来的勒索犯罪团伙的运营风险将会增加。

6. 事后恢复

据调查，勒索软件攻击后的平均恢复成本从去年的 700,000 美元增加至今年的 1,700,000 美元，考虑到事件响应和恢复时间所带来的各种因素，实际恢复成本将远超勒索团伙所提出的赎金要求，主要体现在以下几点：

1. 事件响应成本：大部分企业通常并不具备安全响应团队，当攻击事件发生时，需要聘请信息安全专家来调查事件、找回数据或修复系统。事件响应对于查明黑客的入侵路径很有帮助，能够有效防止再次遭受类似攻击。由于大多数勒索软件的加密不可逆，也可能出现花费了时间和成本却无法对恢复业务有帮助的情况。
2. 数据备份成本：为避免再次遭到网络攻击导致的系统瘫痪，企业应做好备份数据和关键系统映像的准备，定期备份网络并脱机存储，以便在遭遇类似威胁攻击时能快速重建服务器。
3. 系统升级成本：企业遭到攻击通常是因为使用低版本或带有缺陷的系统、软件，因此需要彻查并升级相关系统和基础设施，确保安装的是最新的操作系统和安全补丁程序，同时弃用或替换有缺陷的软件或产品，并应用多因素身份验证来确保网络免受网络攻击。
4. 声誉损失成本：勒索攻击事件会对企业造成一定的声誉损失，从而影响供应商和其他第三方之间的合作关系，甚至由此产生信任危机，导致合作终止。
5. 法律风险成本：对于大部分国家而言，有明确的法律规定企业禁止泄露敏感信息，否则将面临因数据泄露而导致的巨额罚金等法律风险问题。例如被美国实施经济制裁的 Evil Corp 勒索组织，向 Evil Corp 支付赎金的行为将被美国视为违反 OFAC（外国资产控制办公室）法规，企业将面临严重的指控，由于现在勒索软件普遍使用双重勒索策略，企业如果不支付赎金，将面临另一种数据泄露的法律风险，无论是哪种境地，企业都处于两难的状态。

大多数公司在遭受勒索攻击时，把目光放在了如何快速恢复数据并重新上线业务系统，却忽略了网络入侵问题。在今年发生的一起勒索攻击事件中，一家未透露名称的公司支付了数百万美元以获取解密密钥，在解密后的两周内未能查清攻击原因，导致该公司被相同的勒索软件再次勒索，该公司最终支付了第二笔赎金。这个案例充分说明了事后分析的重要性。

一些公司因迫切想恢复业务而选择支付赎金，但根据调查结果显示，只有不到 10%的公司在支付赎金后恢复所有数据，更多的受害者只能恢复一般数据。即使支付数据，也不能保证勒索团伙信守承诺发放安全无害且能正确使用的解密密钥，即便密钥是正确的，也很难保证勒索团伙会删除受害公司的数据，勒索团伙完全可以制作副本，并在地下市场上出售给其他网络犯罪分子，以便进行二次勒索，这些案例表明支付赎金并不能确保数据或系统将不再受到损害。 对于一般企业而言，只能采取以预防为主的检测策略来提前应对威胁，在损害业务之前阻止攻击发生。

7. 总结

勒索软件一直是广泛存在的网络安全问题，自诞生以来就在迅速发展，并由此衍生出复杂且成熟的网络犯罪产业，如今已成为庞大的网络犯罪生态系统，并从网络走向现实，对全球 150 个国家的教育、医疗、金融、能源等多个行业造成严重的影响。其所直接或间接造成的数据损坏、业务中断、企业声誉损害、生产力停滞、经济损失等损害甚至影响国家经济发展。

勒索软件攻击加速网络犯罪行业发展，使其成为一种越来越具有破坏性的网络犯罪形式。而在勒索威胁快速增长的同时，如何有效打击这种网络犯罪成为了目前需要迫切解决的问题，这需要各国的私营企业和执法部门联合行动，共同对抗网络威胁，遏止勒索攻击事件的发生。

参考链接

FROM WIPER TO RANSOMWARE: THE EVOLUTION OF AGRIUS

https://assets.sentinelone.com/sentinellabs/evol-agrius

The Crimeware-as-a-Service model is sweeping over the cybercrime world. Here’s why
https://cybernews.com/security/crimeware-as-a-service-model-is-sweeping-over-the-cybercrime-world/

The First Step: Initial Access Leads to Ransomware
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

How Ransomware Attacks Are Threatening Our Critical Infrastructure
https://www.sentinelone.com/blog/how-ransomware-attacks-are-threatening-our-critical-infrastructure/

Bash Ransomware DarkRadiation Targets Red Hat- and Debian-based Linux Distributions
https://www.trendmicro.com/en_us/research/21/f/bash-ransomware-darkradiation-targets-red-hat--and-debian-based-linux-distributions.html

EKANS Ransomware and ICS Operations
https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

NCSC CEO warns that ransomware is key cyber threat
https://www.ncsc.gov.uk/news/rusi-lecture