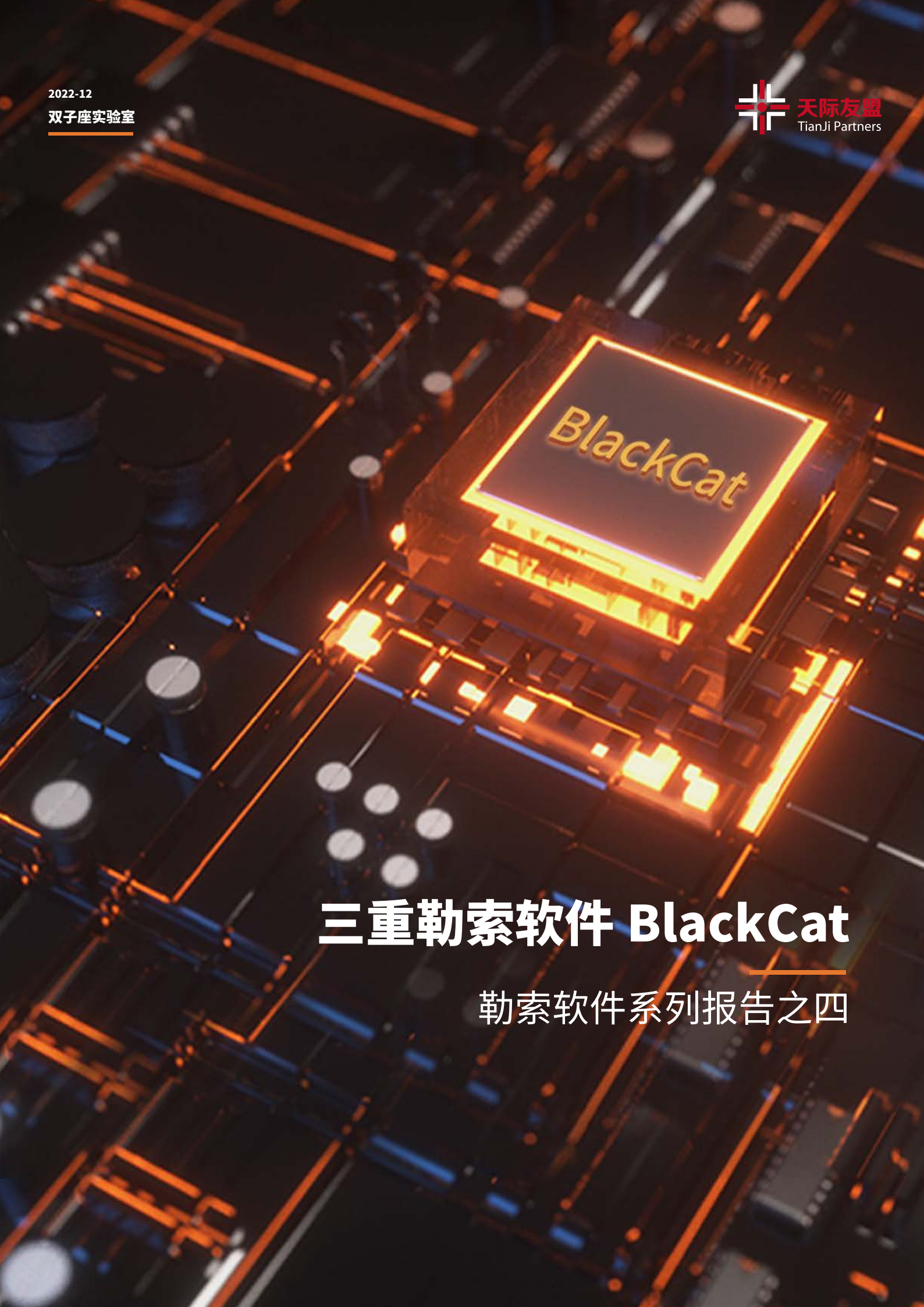
2022-12

双子座实验室

天际友盟
TianJi Partners



三重勒索软件 BlackCat

勒索软件系列报告之四

目录
CONTENTS

前言

世界经济论坛发布的《2022 年全球网络安全展望》报告显示，勒索软件攻击在全球网络领导者网络威胁关心问题中排名第一，成为全球广泛关注的网络安全难题。本系列报告正是以当前最为活跃的勒索软件攻击为主题展开，聚焦暗网中多个活跃的勒索软件组织或团伙，梳理各个勒索软件的发展阶段、剖析关键技术细节、盘点重大攻击事件，对勒索软件组织或团伙进行全面画像，希望为未来应对勒索软件攻击提供有力的参考。

01 背景

作为 2021 年底入侵活动最为频繁的勒索软件，BlackCat 勒索团伙在 2022 年依然有着不俗的表现。2022 年 4 月，FBI 发布警告称，BlackCat 勒索软件在 2021 年 11 月至 2022 年 3 月期间至少被用于攻击了全球 60 个组织。经统计，截止 2022 年 12 月，BlackCat 暗网泄密网站受害者数量目前已高达 230 个，可见 BlackCat 团伙攻击频率持续增加，未来将是针对全球企业的最重要的勒索软件威胁之一。

02 简介

BlackCat 勒索软件（又名 AlphaVM、AlphaV 或 ALPHV）于 2021 年 11 月中旬首次被 Malwarehuntertam 研究人员披露（如图 1），是第一个基于 RUST 语言编写的专业勒索软件家族系列，并因其高度定制化和个性化的攻击而迅速赢得市场。

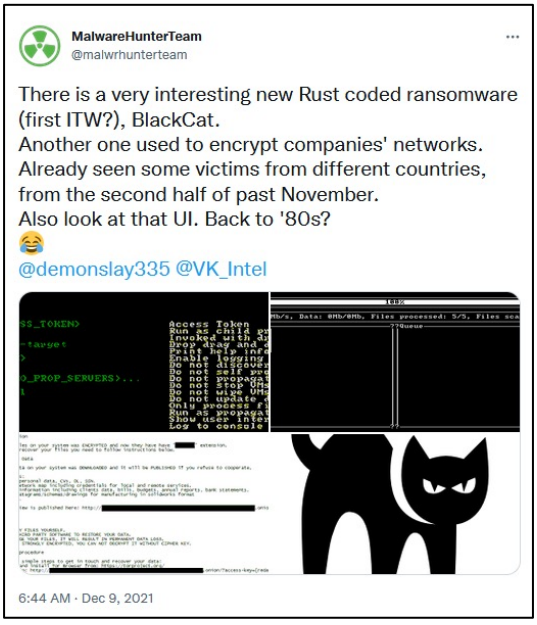


图 1 BlackCat 首次被 Malwarehuntertam 披露

BlackCat 于 2021 年 12 月初开始在某俄罗斯地下犯罪论坛上推广（如图 2），通过招募合作组织进而实施勒索攻击，且合作组织保留 80–90% 的赎金份额，其余部分归 BlackCat 开发者所有，是目前最复杂和技术最先进的勒索软件

即服务 (RaaS) 运营商之一。

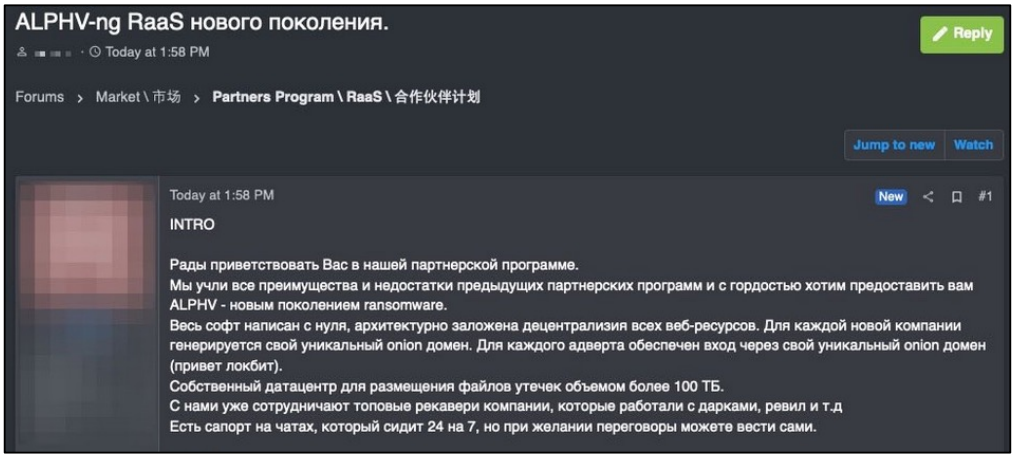


图 2 BlackCat 在俄语论坛得到推广

BlackCat 采用三重勒索策略，不仅会加密文件，窃取敏感数据，并且在暗网泄密网站上列出受害者名单（如图 3），迫使受害者缴纳赎金；而且倘若受害者未在最后期限支付赎金，还会进行分布式拒绝服务 (DDoS) 攻击。最近，BlackCat 采取了更为激进的方式来对受害者进行勒索，其甚至在明网推出了一个新的可搜索被盗数据的网站，这使得该组织的勒索攻击对受害者极具压迫性。

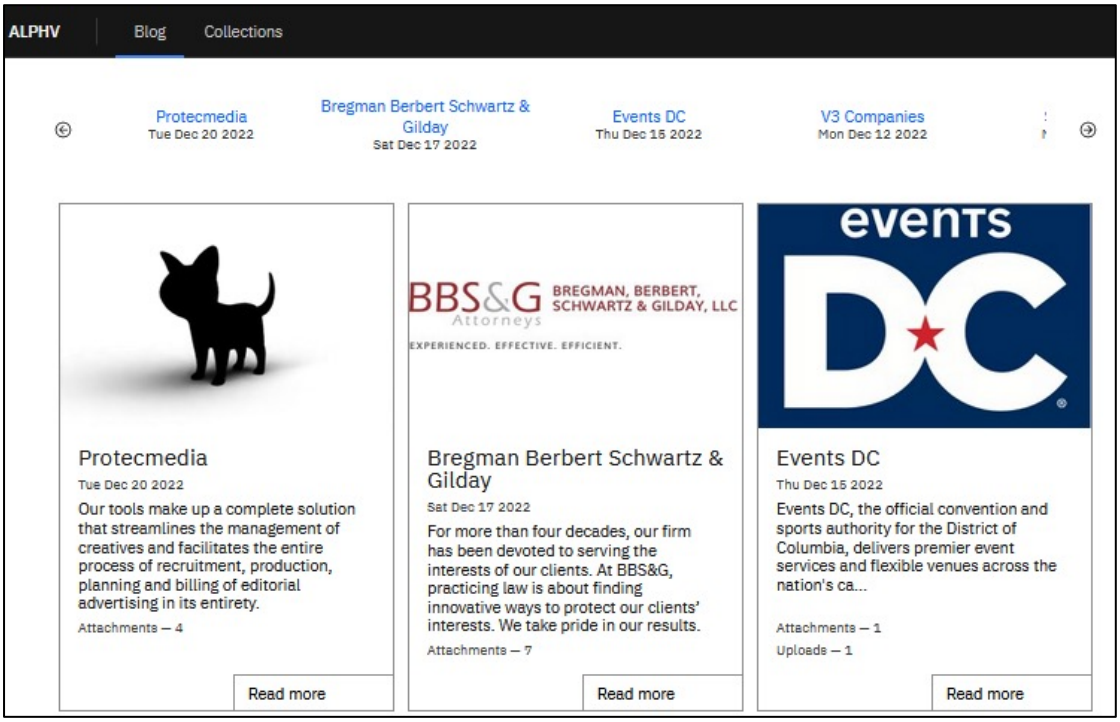


图 3 BlackCat 泄密网站

此外，BlackCat 被认为是现已关停服务的 DarkSide/BlackMatter 勒索团伙的继任者。2022 年 2 月，BlackCat 团伙成员接受 The Record 采访时表示与 BlackMatter 存在联系，但并未证实是其复用。但这也从侧面反映，BlackCat 大概率具有大量的网络和勒索软件操作经验。

03 技术详情

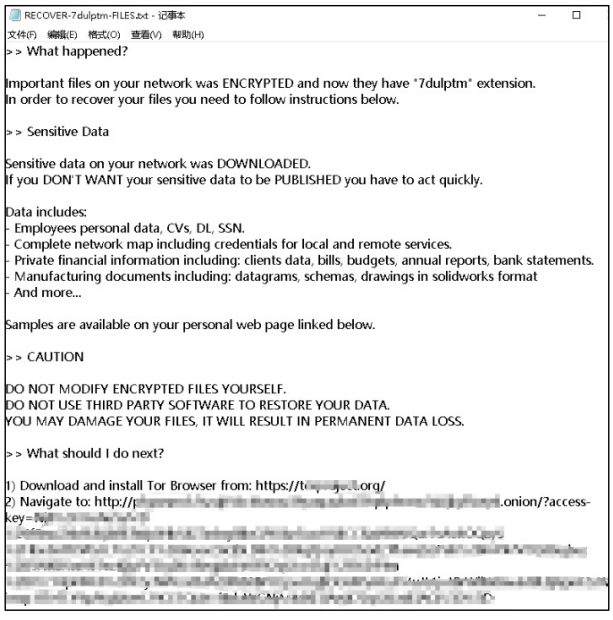
3.1 开发语言

与很多勒索软件不同，BlackCat 采用 Rust 语言编写，这是 BlackCat 的一个主要卖点。Rust 是一种更安全的跨平台编程语言，能够进行并发处理。通过利用此编程语言，攻击者能够轻松地针对 Windows 和 Linux 等各种操作系统架构对其进行编译，这有助于该勒索软件快速传播。同时由于 RUST 提供了众多自主开发的选项，通过命令行调用的 BlackCat 可实现更具个性化的攻击。

3.2 攻击过程

作为一个 RaaS 有效负载，BlackCat 进入目标组织网络的方式同样取决于部署它的 RaaS 附属机构。以往活动中，BlackCat 勒索软件通常利用网络钓鱼邮件进行传播。邮件包含恶意附件或下载链接，文件形式不限于 Microsoft Office 文档、可执行文件、JavaScript 等。此外，Microsoft Exchange Server 漏洞（CVE-2021-26855、CVE-2021-26857、CVE-2021-26858、CVE-2021-27065 和 CVE-2021-31207）也是 BlackCat 勒索软件获取初始访问权限的常见入口点。

成功获取初始访问权限后，BlackCat 主要借助第三方工具集（如 Cobalt Strike）进行交付，然后再使用嵌入式 PsExec 模块自行横向传播。在执行 BlackCat 勒索软件之前，攻击者会使用各种批处理脚本来准备加密环境。之后，恶意软件将从注册表中获取 Windows 系统的 MachineGuid（操作系统安装期间生成的唯一密钥）及其 UUID，然后继续绕过用户帐户控制（UAC）、删除卷影备份、修改引导加载程序、清除 Windows 事件日志并启动加密过程。BlackCat 采用 RSA+AES/ChaCha20 两种方式加密磁盘文件， 加密后文件扩展名为“.7dulptm”。最后释放赎金票据文件：“RECOVER-7dulptm-FILES”（如图 4），该内容指示受害者们访问 Tor 链接。


RECOVER-7dulptm-FILES.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

>> What happened?

Important files on your network was ENCRYPTED and now they have "7dulptm" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

Samples are available on your personal web page linked below.

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

1) Download and install Tor Browser from: https://t[redacted].org/
2) Navigate to: http://[redacted].onion/?access-key=[redacted]

图 4 BlackCat 赎金票据

目前该勒索软件尚未有解密方式，赎金为 40 万到数百万美元不等，受害者可选择比特币和门罗币两种支付方式。但是，如果受害者使用比特币支付赎金，则需额外支付 15% 的费用。

3.3 利用工具

BlackCat 在整个攻击过程中使用了多个工具，包括远程控制工具 Cobalt Strike，用于恢复存储密码的 Mimikatz、LaZagne 和 WebBrowserPassView，以及窃取数据的 GO Simple Tunnel (GOST)、MEGAsync 和 ExMatter。此外，在一些 BlackCat 勒索软件活动中，攻击者还被观察到利用了诸如 fileshredder 之类的反取证工具。

3.4 攻击特点

1、个性化操作

BlackCat 完全通过命令行进行操作，支持多种细节配置（如图 5），允许自定义文件扩展名、赎金说明、加密模式。其自带一个加密配置，包含要终止的服务 / 进程列表、避免加密的目录 / 文件 / 文件扩展名列表以及来自受害者环境的被盗凭证列表以实现持久化。它会删除所有卷影副本，使用 CMSTPLUA COM 接口执行权限提升，并在受害者机器上启用“远程到本地”和“远程到远程”链接。

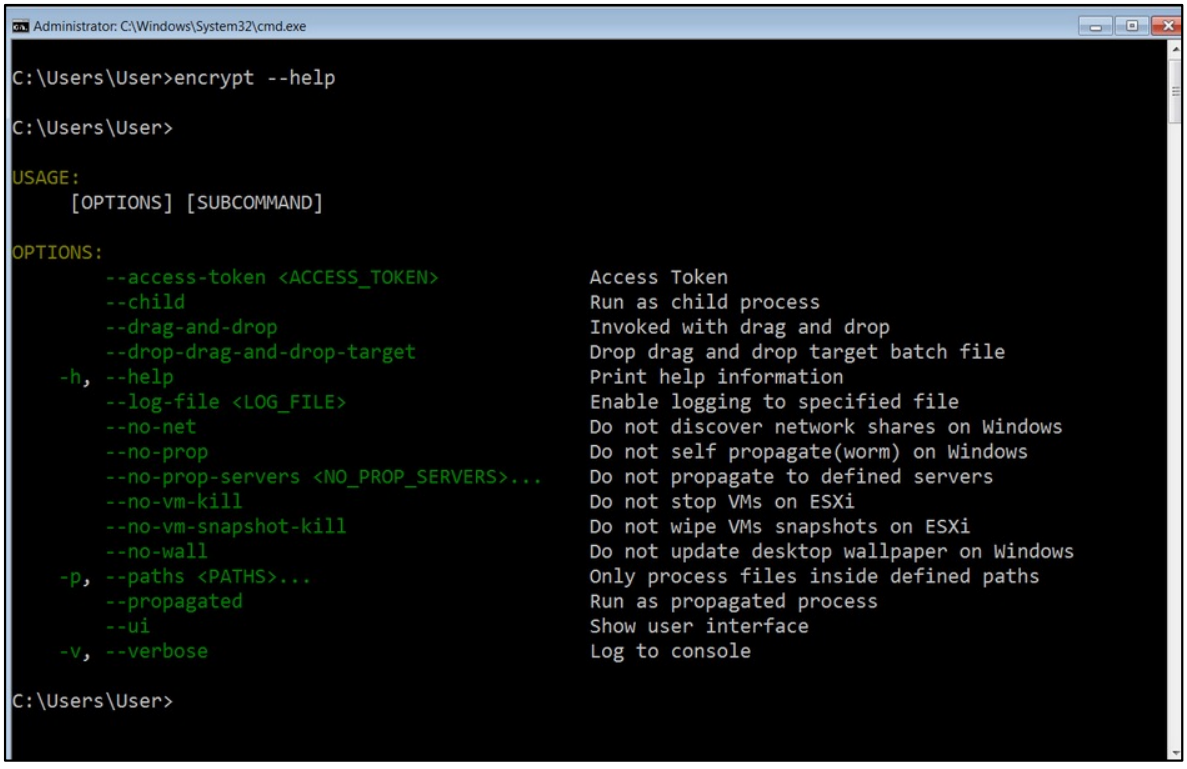


图 5 BlackCat 命令行参数

2、灵活加密

根据官方说明，BlackCat 勒索软件支持四种加密模式。但据 SentinelLabs 研究员 Aleksandar Milenkoski 对 BlackCat 勒索软件样本进行逆向分析得出其加密模式实际存在 6 种，具体描述如下表：

加密模式	描述
Full	全文加密；最安全，最慢
HeadOnly[N]/Fast	仅加密文件前 N 字节；最不安全的解决方案，但速度最快
DotPattern[N,Y]	每隔 Y 字节步数加密 N 字节
SmartPattern[N,P]	加密文件的前 N 个字节，其余部分划分为大小相等的块，这样每个块占文件大小的 10%，再加密每个块字节的 P%；速度 / 密码强度比的最优模式
AdvancedSmartPattern[N,P,B]	加密文件的前 N 个字节，其余部分划分为 B 字节大小相等的块，再加密每个块字节的 P%
Auto	根据文件类型和大小选择最优的 (速度 / 安全方面) 策略来处理文件。

BlackCat 支持 2 种文件加密算法，包括：ChaCha20 和 AES。在自动模式下，BlackCat 勒索软件将检测是否存在 AES 硬件支持 (存在于所有现代处理器中) 并使用它。如果不支持 AES，则利用 ChaCha20 进行加密。

3、压迫性策略

如前文所说，BlackCat 采用三重勒索策略，不仅会加密文件，窃取敏感数据，甚至可能对受害者系统发起 DDoS 攻击以迫使其缴纳赎金。

其中，DDoS 是利用一批受控制的僵尸主机向一台服务器主机发起的攻击，其攻击强度、造成的威胁、破坏性巨大。同时，DDoS 攻击溯源难度大，讹诈成本低，正逐渐成为犯罪团伙的首选勒索手段。除了 BlackCat 勒索软件，Avaddon、REvil、AvosLocker 和 Suncrypt 等勒索软件犯罪团伙频繁利用 DDoS 攻击勒索受害者。例如，REvil 模仿者向数家 VOIP 服务提供商发起了全球性 DDoS 勒索攻击活动。其中一家 VOIP 服务提供商称，DDoS 攻击导致其收入损失 900 万至 1200 万美元。目前来说，想要逃避 DDOS 攻击基本不可能，三重勒索甚至四重勒索将是未来勒索攻击的大势所驱。

04 关联组织分析

通过对部署 BlackCat 勒索软件的关联威胁组织进行分析，目前至少有两个已知的附属机构正在使用 BlackCat，分别是 DEV-023 和 DEV-0504 组织。DEV-0237 也称为 FIN12，该组织以传播 Hive、Conti 和 Ryuk 勒索软件而闻名，但从 2022 年 3 月开始便将 BlackCat 加入了其有效负载清单。DEV-0504 组织此前则主要部署 Ryuk、REvil、LockBit2.0、BlackMatter 和 Conti 勒索软件，现如今也被观察到转向使用 BlackCat 勒索软件。

此外，值得注意的是，BlackCat 和 LockBit 勒索团伙使用的工具和基础设施之间存在重叠。这似乎表明网络罪犯会共享代码和工具，或是攻击者同时参与了两个勒索软件的开发。

05 Top10 攻击国家及行业

通过对 BlackCat 勒索组织泄密网站的受害者名单进行统计，其 Top10 攻击国家如下：

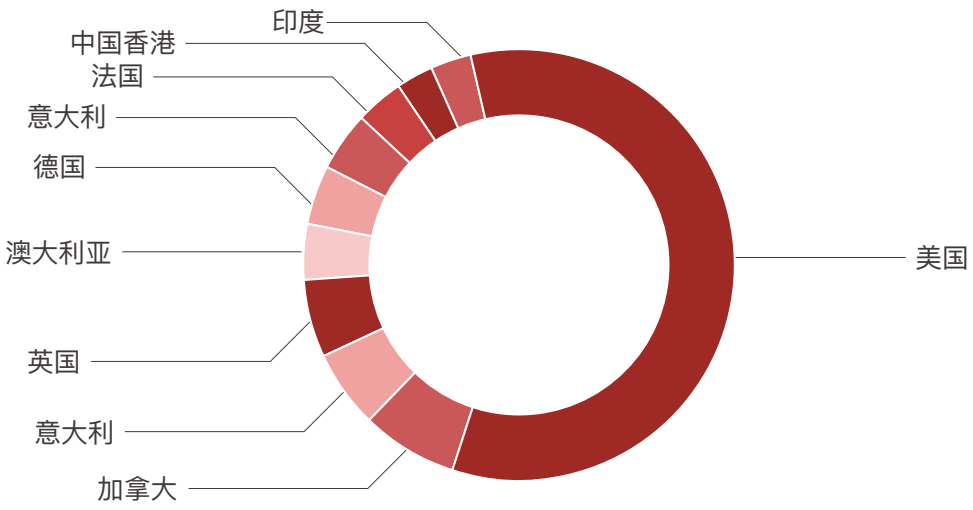


图 6 Top10 攻击国家

BlackCat 勒索组织似乎偏爱美国企业。其中，欧洲和亚太地区的组织也是其主要攻击对象。

BlackCat 勒索组织 Top10 攻击行业如下：

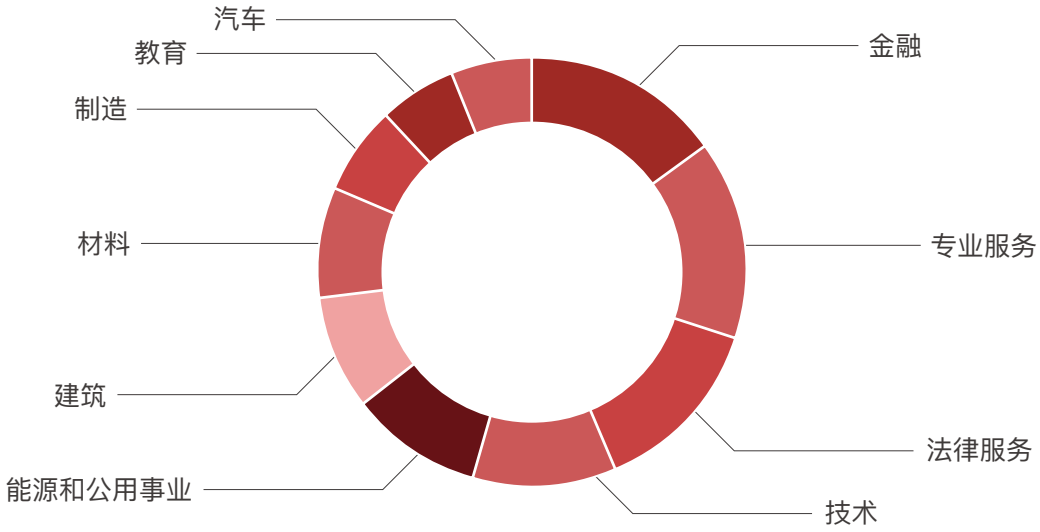


图 7 Top10 攻击行业

金融、专业服务、法律服务等行业依次为 BlackCat 勒索组织重点关注领域。

06 总结及发展趋势

BlackCat 勒索软件采用非传统编程语言，可使攻击者更加轻松地将其部署在 Windows 和 Linux 以及 VMWare 等多种设备之上并进行定制化攻击，未来可能会有越来越多的威胁组织将转向使用具有交叉编译功能的语言。同时，不同威胁组织在攻击活动中对 BlackCat 勒索软件的关联使用也证明该类勒索病毒正变得流行。此外，BlackCat 人员与 DarkSide/BlackMatter 前勒索团伙存在的渊源表明其幕后的行为者似乎经验丰富，其采用三重勒索策略并不断推出更具压迫性的勒索策略将使受害者缴纳赎金的概率大幅上升，BlackCat 团伙未来仍将成为勒索软件市场的主要参与者之一。虽然 BlackCat 目前重点攻击国外用户，但国内用户也应加强防范，规避此类风险。

07 附录

7.1 防护体系建设

防范：

防止勒索软件攻击的最佳时间在入侵发生之前，因此，建议采用主动安全防御策略：

1、做好资产梳理与分级分类管理。建立完整的资产清单，识别内部系统与外部第三方系统间的连接关系，尤其是域合作伙伴共享控制的区域，降低勒索软件从第三方系统进入的风险；

2、严格访问控制策略。创建防火墙规则，仅允许特定的 IP 地址访问；限制可使用 RDP 的用户为特权用户；设置访问锁定策略，调整账户锁定阈值与锁定持续时间等配置；为管理员级别和更高级别设置的账户实施基于时间的访问；

3、做好身份验证管理。设置复杂密码，并保持定期更换登录口令习惯；多台机器，切勿使用相同的账号和口令；启用多因素身份验证 (MFA)；

4、及时更新系统补丁，定期检查、修补系统漏洞，尤其针对高危或 0day 漏洞；

5、备份重要数据和系统。在物理上独立安全的位置（即硬盘驱动器、存储设备、云）维护和保留敏感或专有数据的多个副本。

检测：

检测为勒索软件体系化防护的事中阶段，该阶段勒索软件已渗透到系统内部，但还未大规模爆发。通过应用有效的检测手段，能够降低勒索软件爆发所产生影响。

1、共享威胁情报。使用网络安全设备或组件阻断相关指示器；使用沙盒分析来阻止恶意文件执行 ；

2、文件扩展名检测。借助文件访问监控工具，将勒索软件的扩展名文件重命名操作列入黑名单；

3、采用蜜罐文件。在共享文件夹放置虚假诱饵文件并以警报通知文件打开情况；

4、配备安全防护工具。检测系统中存在可疑工具 ；

5、监控可疑网络端口、协议和服务 ； 识别授权和未授权的设备和软件；对事件日志进行审核。

响应：

感染勒索病毒建议进行如下操作：

1、隔离网络。将感染病毒的机器断开互联网连接，视情况切断网络内不必要的网络连接，避免网络内其他机器被进一步感染渗透；

2、分类处置。当重要文件尚未被加密时，应立即终止勒索软件进程或关闭机器，及时止损；

3、及时报告。及时报告网络管理员，通知其他可能会受到勒索软件影响的人员，造成重大影响时，及时向网络安全主管部门报告；

4、排查加固。排查勒索软件植入途径；及时堵塞漏洞、尽快对网络内机器进行全面漏洞扫描和安全加固；

5、专业恢复。联系专业公司和人员进行数据和系统恢复工作。

7.2 IOCS

SHA256：
67d1f4077e929385cfd869bf279892bf10a2c8f0af4119e4bc15a2add9461fec
0a609fa2db910615b2c1ad235ca46562ff4034800c44802a63a28826669a7eee
cda37b13d1fdee1b4262b5a6146a35d8fc88fa572e55437a47a950037cc65d40
bacedbb23254934b736a9daf6de52620c9250a49686d519ceaf0a8d25da0a97f
47affaed55d85e1ebe29cf6784da7e9cdbd86020df8b2e9162a0b1a67f092dcd
65dbafe9963cb15ce3406de50e007408de7d12c98668de5da10386693aa6cd73
060ca3f63f38b7804420729cde3fc30d126c2a0ffc0104b8e698f78edab96767
SHA1：
9373f26b9c872047a1befd2e776889fded4f360d
97d5153f43eb48b9c2b12ba1f7857173da0e4143
928d66f4fe8da031daccfb7642324f1e10f31ce0
77413cb3f469d00d69941b4973206e4978381987
5c6ca5581a04955d8e4d1fa452621fbc922ecb7b
a186c08d3d10885ebb129b1a0d8ea0da056fc362
67fc605754f3e7304dda8c99f0d7d5003835a5d3

11203786b17bb3873d46acae32a898c8dac09850
026720fca026d971b16d1990146ef6462e8c1664
f95d865ef06f382bc9599a8093308afb9007ab89
5869820f261f76eafa1ba00af582a9225d005c89
dd69b20eb1931487d8b65060f2be3671bd5baf33
c5181892afde538c73109b4c83e2a2730eb9014d
da1e4a09a59565c5d62887e0e9a9f6f04a18b5f4
d42566e04d295a1e9e2823d202a1800cdc1ddd77
c5acefee89cdbf24e99d311f804615aedef8f3df
dc963d8beb490d00261280dc5a9bc9cc700da602
0c7215c4325ded8139ea2f0428412f17e6c8f957
bf41f2014cfbfdd683ba4e259b004bce3b54e3ea
89060eff6db13e7455fee151205e972260e9522a
324c6626ab70399ef9864542ddbeedfb8fbddfb5
38fa2979382615bbee32d1f58295447c33ca4316
087497940a41d96e4e907b6dc92f75f4a38d861a
362aa21546904629b28a56c9d5c4bfd3b53296f5
ce5540c0d2c54489737f3fefdbf72c889ac533a9
e17dc8062742878b0b5ced2145311929f6f77abd
7af51a9e6245415d18be46142f2400a421f19d3a
a8fd52bd107f7b62483c11c15923fbd2256c8bac
94f025f3be089252692d58e54e3e926e09634e40
36dff07387cf3f2393339d30d0672fcbccc7a73c
1d6e2aeed499eb7d317b92b42d4a784b22d02dc6
f466b4d686d1fa9fed064507639b9306b0d80bbf
6116a5b0c0b6c147a2c715aad2eb1cd082941715
23006c877ccc883460497ad35df82e64f338cfc9
e22436386688b5abe6780a462fd07cd12c3f3321
2a53525eeb7b76b3d1bfe40ac349446f2add8784

5ac485d60fe2c096b10cda2624588427928e3f0d
45212fa4501ede5af428563f8043c4ae40faec76
fd0d6046d6e3096bd38df9aa539d4b5502db9f85
57a6dfd2b021e5a4d4fe34a61bf3242ecee841b3
8917af3878fa49fe4ec930230b881ff0ae8d19c9
a03d9e0baa0c7b71b2ed3afe38fb6ddeb346e030
9146a448463935b47e29155da74c68d16e0d7031
74845c914cc9525604ff06212f50b99386240183
75b6eb3cc65a608abd9a96a3c5d158c944aadb15
3e794a584d75c2ceb07287fe450dcdc4d7ce949a
655c2567650d2c109fab443de4b737294994f1fd
3d385b316df5d37d39b10113a67080fc1516e0c9
71e6aa313f9d64086d68d1c0048420fa5c778165
c1187fe0eaddee995773d6c66bcb558536e9b62c
e10dfc54c2fbd2cb8a0a3845fde7ff3ee93634c2
783b2b053ef0345710cd2487e5184f29116e367c
URL：
hxxp://vwuzda4x76mhtutxkjnhzquuq4wgtgwjbv6wrs2m627uhg744ieaskqd.onion/?access-key=g7ZyzfVklepngLBki2XeB4NTccRD1m1R2RymNI23pOXwUVctZIV7CTeiwV2S3fptQli%2F0Yk%2BIL5LVHEU4Gkj4FVKSthcz6R8ObwbdpgIsf7BdTMQP7BgsTt6JpiHBdqv1I%2FQZEsr5dc49d8O3%2BRITphpH%2BMFf3B5uCPkg35GwD7qEi8mGWinXixlPnaCmuq2LZpGqcZe15KVIIMK1dehL277UddgPLCUe11xlVbPOSfGTAdrRUfzeUtiJkX9lSAk5ry%2FYsqcg1IglzjdqTByCGF%2B5BnnbUNJt0NcfGt1IdkUJfXHPrN1m73390kB%2BHkT8CGM9cFME6frN5j%2BoejVmw%3D%3D

7.3 参考资料

1. *https://redqueen.tj-un.com/IntelDetails.html?id=dc395703e8da46f78474892d801942ff*
2. *https://redqueen.tj-un.com/IntelDetails.html?id=7cc07a655eba4a6dab7f38667e914ba1*
3. *https://redqueen.tj-un.com/IntelDetails.html?id=fbd12b6efb864b07ae952bcd5e090ffc*
4. *https://redqueen.tj-un.com/IntelDetails.html?id=af378002ce704169832b8aaf100ef13c*
5. *https://redqueen.tj-un.com/IntelDetails.html?id=c9a61863b340443b9b90bcd609cc45d7*
6. *https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat*
7. *https://www.trendmicro.com/en_us/research/22/d/an-investigation-of-the-blackcat-ransomware.html*

8. https://www.aha.org/cybersecurity-government-intelligence-reports/2022-04-19-fbi-tlp-white-flash-report-blackcatalphv

9. http://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html

10. https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware

11. https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

12. https://www.ics-cert.org.cn/portal/page/122/a6b46a5e911f4d29a2060b7144479db3.html

13. https://unit42.paloaltonetworks.com/blackcat-ransomware/

14. https://www.govinfosecurity.com/blackcat-extortion-technique-public-access-to-breached-data-a-19352

天际友盟
TianJi Partners

专业的情报应用解决方案提供商

400-081-0700 www.tj-un.com

市场合作：mkt@tj-un.com 客户服务：service@tj-un.com 合作伙伴：partner@tj-un.com