AhnLab

安全月刊

2022.06 Vol.115

2022 年第一季度暗网和深网的趋势报告

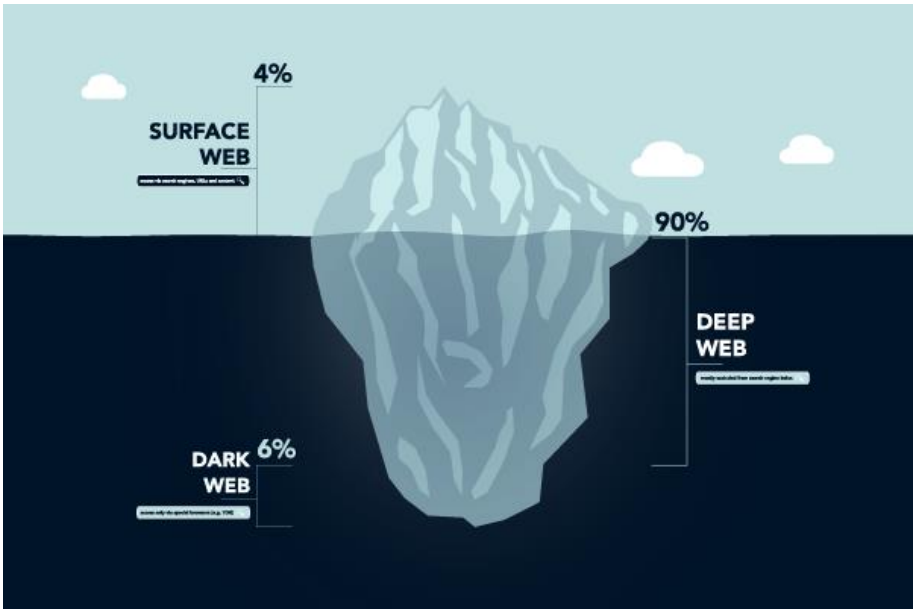
作为攻击发源地的“暗网和深网”，都发生了什么事?

2022年第一季度，由于美俄的新冷战和俄罗斯和乌克兰冲突的加剧，导致网络世界也掀起了波澜。最猖獗的Conti勒索软件组织的身份被曝光，他们使用的源代码也被泄露。此外，臭名昭著的Reville勒索软件组织的大多成员也已被捕，多个地下论坛也被关闭。尽管如此，使用暗网和深网的犯罪仍在持续发生。这样的市场如何可以维持一个像一般企业一样的生态系统？其原因是不断需求和市场的易用性。

在本文中，我们将仔细研究暗网和深网趋势，并重点关注勒索软件、论坛和黑市以及黑客组织。

过去，暗网（Dark Web）一直被认为是仅由一些犯罪分子和黑客使用的空间。然而，根据KISA（韩国互联网与安全局）的数据，发现仅是暗网的访问人数平均每天就多达15,000名。

首先，让我们准确了解暗网的真正含义。



【图1】互联网世界的结构：表层网、深网以及暗网

暗网有时与深网（Deep Web）混用，但含义并不相同。深网是指搜索引擎无法找到的所有网页，据推测它占据了整个互联网的96~99%。暗网是被有意隐藏的深网的一个子集，它可以通过特定浏览器访问。暗网占所有网页的5%。

暗网并非全部用于非法目的，但依然主要被勒索软件和黑客组织用于恶意目的。

暗网和深网的主要问题一：勒索软件

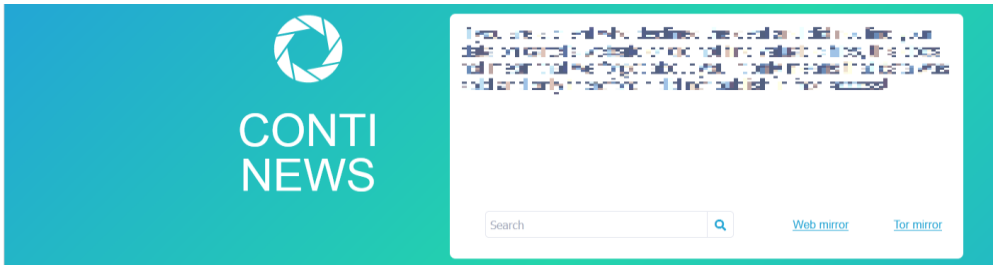
勒索软件组织不断通过品牌重塑来避免制裁。最具代表性的例子是ALPHV勒索软件。被称为ALPHV或BlackCat的勒索软件的制作人被认为是同一个人。该制作人积极招募曾活跃于REvil、DarkSide、BlackMatter和Maze等各种勒索软件组织的人员进行品牌重塑。

- 品牌重塑顺序： DarkSide → BlackMatter → BlackCat (ALPHV)

【图2】ALPHV勒索软件组织的运营页面

近期，几个勒索软件组织正在尝试品牌重塑，改称有些人认为他们的生态系统并不像看起来那么大。

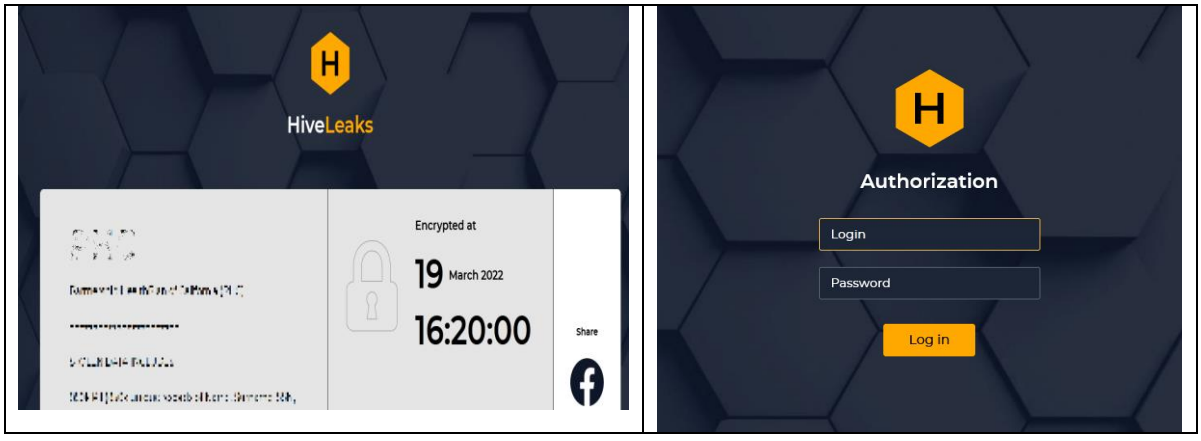
另一个例子是Conti勒索软件。Conti勒索软件被认为是Ryuk勒索软件的品牌重塑，而且非常活跃，迄今为止已有超过800个的组织遭到了Conti勒索软件的攻击。



【图3】Conti勒索软件组织的运营页面

最近， 他们的聊天记录、勒索软件加密/解密源代码和工具都已开始被泄露。但是， Conti勒索软件组织仍然很活跃。由于RaaS（Ransomware as a Service）具有与一般业务类似的生态系统，因此内部数据泄露并不会对运营产生重大影响。

单独运营网站以协商勒索软件的勒索软件组织的数量也在增加。例如， Hive勒索软件组织正在分别运营具有受害者列表的PR网站和用于协商的网站。



【图4】Hive勒索软件组织的运营页面（左）和协商页面（右）

为了与Hive勒索软件组织协商支付赎金（ransom），需要提供勒索笔记中提到的onion地址和登录帐户信息。最近，Hive勒索软件将默认赎金从120万美元提高到200万美元，并且还更改了部分勒索笔记。

有一些勒索软件组织单独运营协商页面， 也有一些勒索软件组织对其进行了变种以使其以在Linux等新环境中运行。LockBit勒索软件组织的变种恶意代码除了Windows环境外，还可以在Linux和ESXi环境中运行。

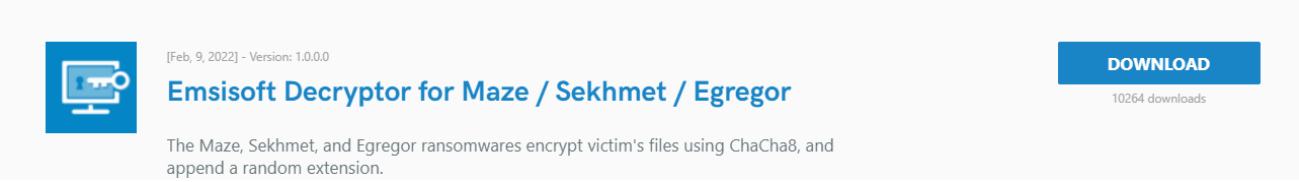
MD5	V3诊断名
3c9e550d41f3de930e678776a6e018ed	Ransomware/Linux.Generic.260872
9661c01af31a41caef2ccd3b6be06e60	Ransomware/Linux.Generic.259496
18a352d33c8c01b6a196adce176c5a96	Ransomware/Linux.Generic.252680

【表1】LockBit勒索软件的Linux变种

LockBit勒索软件与Conti勒索软件一样活跃，受害者名单几乎相同。截至2022年1月，共发布了500多个受害者名单，2月中旬一次14个，3月中旬在两天内发布了22个新的受害名单。

还有一些勒索软件组织采取了与当前活跃的勒索软件组织截然不同的路线。那就是一些突然宣布隐退或被捕的组织。一位被认为是Maze勒索软件的制作人在BleepingComputer.com论坛上公开了Maze、Egregor和Sekhmet的主密钥。基于此密钥，安全公司Emsisoft制作了解密工具。

- 链接：https://www.emsisoft.com/ransomware-decryption-tools/maze-sekhmet-egregor?__c=1



【图5】Emsisoft的Maze/Sekhmet/Egregor解密工具

Maze勒索软件制作人或黑市运营商隐退的原因被认为是个人原因，例如已被捕或害怕被捕、品牌重塑、实现财务目标和健康问题。

也有一些勒索软件组织在宣布隐退之前就已被捕。被称为GanbCrab的勒索软件并经过REvil和Sodinokibi等品牌重塑过程的勒索软件组织的成员于1月被捕。

然而，令人惊讶的是，这些组织仍然在持续活动。这些被捕人员均属于pentesters或是合作公司。有传言称，该组织在核心人员被捕后仍在以新品牌活跃。

【表2】显示了与2021年被捕的REvil勒索软件合作者相关的事件列表。

2021年	国家和拘捕人员
2月、4月、10月	3名REvil和GandCrab合作人在韩国被捕
11月	2名REvil合作人在罗马尼亚康斯坦察被捕
11月	1名GandCrab合作人在科威特被捕

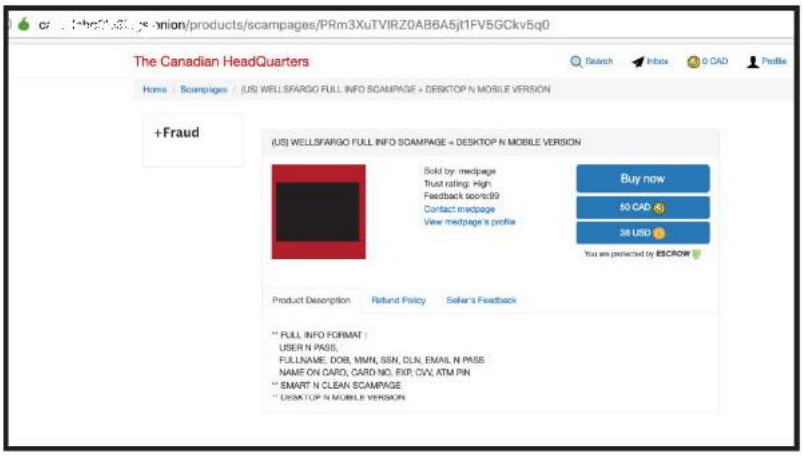
【表2】2021年被捕的REvil勒索软件合作人相关的事件列表

暗网和深网的主要问题二：论坛和黑市

随着政府机构的积极介入， 论坛和黑市也发生了许多变化。有一些被政府机构或执法机构关闭的组织， 而另一些则有自愿隐退或退出诈骗（Exit Scamming）的组织。

1. 关闭CanadianHQ、Monopoly Market等黑市

自2018年开始运营的Canadian HeadQuarters （ CanadianHQ ） 已被加拿大政府关闭。Canadian HeadQuarters， 也称为CanadianHQ， 是较知名的暗网市场之一， 交易有关欺诈、毒品、垃圾邮件服务、网络钓鱼工具包、盗取的凭证和有关访问受僵尸网络感染的计算机的信息。加拿大政府公开了四名黑市经营者的姓名和昵称，并处以了罚款。



Screen shot of a stolen Wells Fargo customer's credit card advertised on the Canadian HeadQuarters site. Image from a Terbium Labs report in 2020

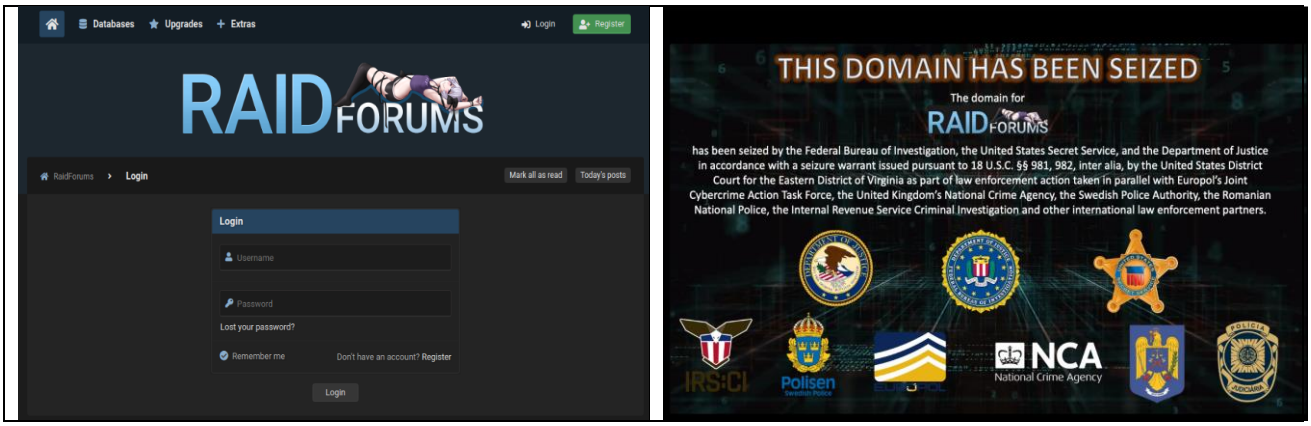
【图6】CandianHQ（来源：Terbium Labs Report in 2020）

Monopoly Market从2019年开始运营， 是最古老的暗网市场。该市场主要销售的商品是毒品， 具体关闭原因不明。但如上所述，推测是因为害怕被执法机构逮捕，或实现财务目标而选择了自愿隐退。

【图7】Monopoly Market

2. 无法访问Raid论坛

Raid Forums，众所周知的数据库（DB）泄漏平台，自2月中旬以来一直处于无法访问的状态。Raid Forums通常被描述为世界上最大的黑客论坛之一，目前拥有超过500,000名的用户。

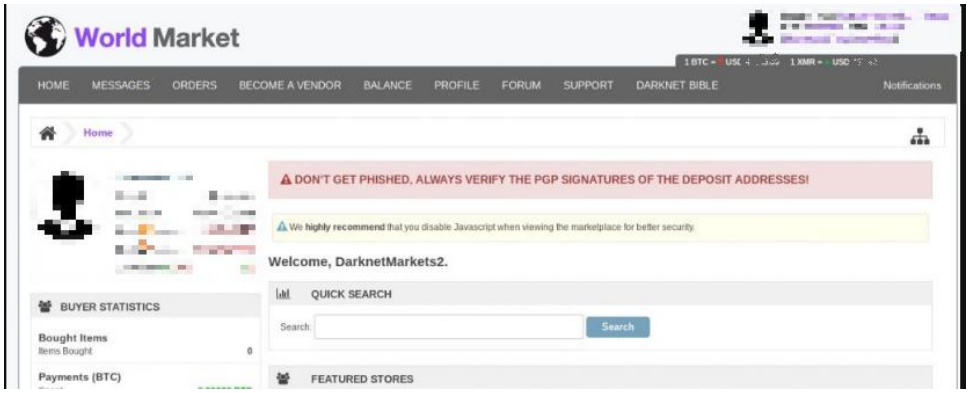


【图8】查封前的Raid Forums登录页面（左），目前被执法机构扣押的域名（右）

如【图8】所示，据了解，美国司法部与英国、瑞典、葡萄牙和罗马尼亚的执法机构通过合作查封了黑客网站Raid Forums.com。与此同时，Raid Forums所有者和管理员于2022年4月12日在英国被捕据报道，目前Raid Forums拥有的网络域名已被美国司法部没收。

3. World Market的退出诈骗（Exit Scamming）

自2020年11月开始运营的World Market最近一直受到退出诈骗问题的困扰。World Market是暗网上的一个市场，主要提供托管（escrow）服务，在完成订单之前持有资金。但是，该服务最近出现了问题。

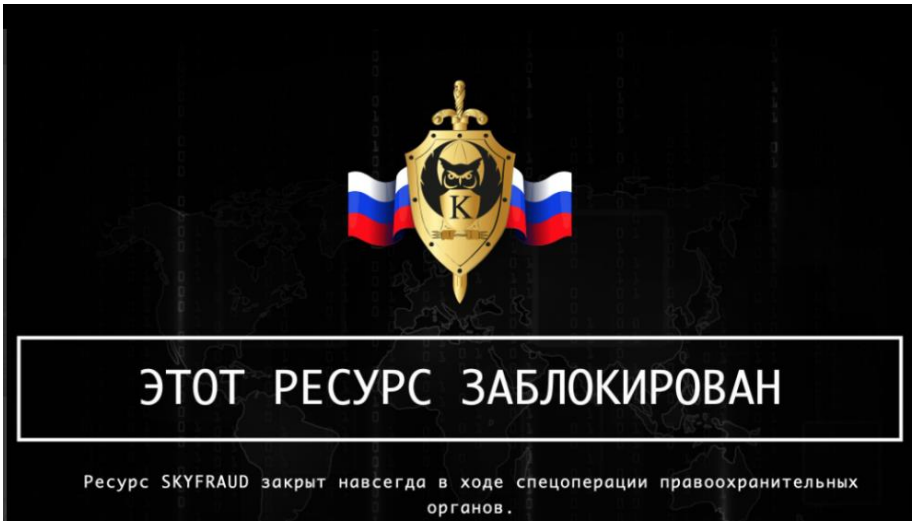


【图9】登录World Market后的画面

据了解，用户委托的加密货币消失、提现延迟或仅提现少量的问题。

4. SkyFraud和Ferum论坛被查封

相对规模较大的出售被盗信用卡信息的（又名Carding论坛）SkyFraud和Ferum论坛现已被查封。



【图10】俄罗斯联邦内政部BSTM-K组织扣押的SkyFraud主页

除该论坛外，还有两个论坛因据信由俄罗斯联邦内政部BSTM-K组织执行的行动而关闭。他们在俄罗斯的SkyFraud主页上留下“下一个是谁？”的消息，暗示随后会在俄罗斯开展逮捕网络犯罪分子的行动。

暗网和深网的主要问题三：黑客组织

随着论坛查封， 黑客组织被查封的消息也随之而来。2022年1月， 美国和保加利亚当局查封了NetWalker勒索软件组织。此外， 一名被确认为合作公司的加拿大男子被判处80个月的有期徒刑， 他所拥有的719.99 BTC和15.72 XMR也被政府没收。

Conti勒索软件组织是通过居住在乌克兰的安全研究人员泄露的消息对话内容来确定了组织和人物。据了解 ， GOLD BLACKBURN和GOLD ULRICK这两个组织构成了勒索软件组织的主力。

GOLD BLACKBURN是一个出于财务动机的网络犯罪组织， 从2014年6月以来一直活跃到现在。2016年底至2022年3月 ， 该组织编写并分发了TrickBot恶意代码 ， 还分发了BazarLoader、Anchor、Zloader、Buer Loader等恶意代码。

GOLD ULRICK仅专注于勒索软件攻击， 自2018年年中以来一直活跃到现在。Ryuk勒索软件于2018年8月开始传播到2021年初，Conti勒索软件在2020年初经过品牌重塑后正在分发。

还有一个事件是，入侵全球多家企业的LAPSUS$组织入侵了Okta，导致部分客户信息遭到泄露。被发现该泄漏事件是由第三方客户支持企业Sykes Enterprise发起的。客户支持公司经常成为黑客组织的目标，因为他们拥有广泛的访问权限来满足客户的要求。

结论

在深网和暗网上活跃的网络犯罪组织与一般商务活动具有相同的生态系统。这些商务活动能够维持下去的原因有两个：不断需求和市场的易用性。

在暗网市场中，即使买卖双方在物理上分离，也可以开展业务。勒索软件可以通过RaaS（Ransomware as a Service）的方式，而恶意代码则是通过MaaS（Malware as a Service）的方式来开展业务。它们可以提供连接买卖双方的中央集中式服务，还拥有用户评级系统和直到履行订单前托管资金的escrow服务。除了易于使用外，由于其高盈利性，导致使用深网和暗网进行恶意攻击的网络犯罪分子数量依然在继续增长。

随着全球各国间持续开展合作以重点打击暗网和深网以及在该领域活跃的网络犯罪分子，世界各地都在紧密关注着他们的动向和变化。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com