2022-12

双子座实验室

天际友盟
TianJi Partners

疯狂收割的勒索软件 Cuba

勒索软件系列报告之三

目录
CONTENTS

01 背景
02 技术详情
03 Cuba 背后的组织
04 总结
05 附录

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

Cuba 勒索软件家族于 2019 年 12 月首次被发现，距今已经活跃三年多的时间。但是，该勒索团伙通过不断的改变策略和工具，使其在 2022 年变得更加积极活跃，成为极具威胁的勒索软件家族之一。2022 年，该勒索软件背后的组织被追踪为威胁组织 Tropical Scorpius，该组织主要通过后门软件在攻击活动中分发 Cuba 勒索软件。

Cuba 勒索软件目前已经攻击了全球 100 多个国家或组织，接近 80% 的受害者位于北美，但它也攻击了欧洲和其他地区的国家，其攻击行业非常广泛，涉及政府、制造、物流和运输、房地产、金融、医疗保健、信息技术、能源、教育、公共事业、高新技术等领域。

自该组织于 2019 年首次浮出水面以来，Cuba 勒索软件团伙在其泄密网站上总共披露了 67 个组织，这还不包括一些已经付了赎金的公司。和其它勒索软件相比较，该勒索团伙运作非常成功，截至 2022 年 8 月，FBI 披露 Cuba 组织在攻击全球 100 多名受害者后，索要总计超过 1.45 亿美元赎金，并且已成功赚到了超过 6000 万美元的赎金，收益非常可观。Cuba 组织攻击的目标主要国家为美国，行业则集中在金融、政府设施、医疗保健、关键制造、信息技术五大关键基础设施领域的实体或公司。

02 技术详情

2.1 攻击方式

Cuba 勒索软件早期一般通过 Hancitor 加载有效载荷，Hancitor 恶意软件是一种加载程序，以将远程访问木马 (RAT) 和其他类型的勒索软件等窃取程序投放到受害者的网络上而闻名。

Cuba 攻击活动中初始恶意软件的投放主要通过以下途径：

漏洞利用：利用商业软件中的已知漏洞，如 Microsoft Exchange Server 中的 ProxyShell 和 ProxyLogon 漏洞；自 2022 年春季以来，Cuba 利用了更多的已知漏洞，包括利用 Windows 通用日志文件系统（CLFS）驱动程序中的 CVE-2022-24521 漏洞窃取系统令牌并提升权限，利用 CVE-2020-1472（也称为“零登录”）漏洞获取域管理权限等。

网络钓鱼活动 ：通过网络钓鱼邮件、恶意附件等传递恶意载荷；

泄露或被盗凭据：攻击者通过获取泄露的凭据数据或购买被盗数据进行登录尝试；

合法工具及服务： Cuba 使用合法的 Windows 服务（例如 PowerShell、PsExec 等）远程部署有效负载；或使用合法的远程桌面协议（RDP) 工具来获得对受害者网络的初始访问权限。

总体来说，Cuba 喜欢通过 Hancitor（又名 Chancitor）恶意软件，利用钓鱼邮件、被盗凭据、Microsoft

Exchange 漏洞或远程桌面协议工具传送信息窃取程序、远程访问木马和勒索软件到受害者的系统。在目标网络站稳脚跟后，Cuba 使用合法的 Windows 服务远程部署有效负载，并利用 Windows 管理员权限远程执行勒索软件和其他进程。

2.2 攻击过程

Cuba 勒索组织一直在不断的开发自己的恶意软件，变更 TTP，部署新的工具集。 我们以 Tropical Scorpius 组织攻击过程为例看一下 Cuba 勒索组织整个攻击流程。

1. 初步侦察建立立足点

Tropical Scorpius 组织利用 Microsoft Exchange 基础设施的漏洞作为最初的攻击媒介进行侦察活动，以识别易受攻击的系统。随后，Tropical Scorpius 会部署 Webshell，以在受害者网络中建立立足点。

2. 窃取凭证升级权限

Tropical Scorpius 在攻击活动中使用有效帐户的凭据来提升权限。攻击者还利用了 Mimikatz 和 WICKER 等凭证窃取工具。攻击者通常会操纵或创建 Windows 帐户并修改文件访问权限，将其添加到管理员和 RDP 组中。

3. 内部侦察识别目标

成功入侵后，攻击者的目的是识别活动的网络主机，并识别要过滤的文件，以便在其后面的勒索攻击中使用。攻击者在此过程主要使用了侦察工具 WEDGECUT，其文件名通常为 check.exe。它通过向名为 comps2.ps1 的 PowerShell 脚本生成的主机列表发送 PING 请求来标识活动主机，该脚本使用 Get-ADComputer cmdlet 枚举活动目录。攻击者以交互方式浏览文件系统以识别感兴趣的文件。

4. 横向移动部署后门

攻击者使用了多种横向移动方法，包括 RDP、SMB 和 PsExec 等，横向移动后，攻击者会部署各种后门，包括公开可用的 NetSupport RAT，以及 Cobalt Strike BEACON 和 BUGHATCH，这些后门通常使用内存加载器 TERMITE 进行部署，并且使用 PowerShell 启动执行。

5. 命令与控制

在 Cuba 与服务器交互过程中，研究人员发现了一个自定义远程访问木马，其中包含独特的命令和控制协议。基于二进制文件中的字符串以及功能，将其命名为 ROMCOM RAT。ROMCOM 会收集系统和用户信息，并尝试通过 WinHTTP API 将其发送到硬编码的 C2 服务器。如果成功，则相应地解析和处理响应。如果连接失败，ROMCOM 会尝试使用 ICMP 请求连接到 C2 服务器并与之通信。

目前 ROMCOM 2.0 版本似乎正在积极开发中，因为在 2022 年 6 月，研究人员发现了上传到 VirusTotal 的类似样本，该版本还扩展了可处理命令的列表，其在现有 10 个命令的基础上又增加了 10 个，包括添加了下载专门用于对系统进行单个或多个屏幕截图的有效负载，以及提取所有已安装程序的列表以发送回 C2 的功能。

6. 加密数据完成任务

为了完成勒索任务，Tropical Scorpius 试图窃取相关用户文件，然后识别和加密联网机器。为了方便加密，攻击者使用了一个名为 shar 的批处理脚本，然后通过 Cuba 勒索软件进行加密。在最近一次的入侵中，Tropical Scorpius 使用名为 av.bat 的批处理脚本部署了 BURNTCIGAR 恶意软件。BURNTCIGAR 是 2021 年底首次发现的恶意程序，它可以终止与端点安全软件相关的进程，以允许勒索软件和其他工具自由执行。

2.3 加密过程

虽然 Cuba 不断开发和更新他们的工具集，但 Cuba 勒索软件的核心有效载荷自 2019 年以来基本保持不变。Cuba 使用 ChaCha20 密码算法进行对称加密和 RSA 加密来保护 ChaCha20 密钥。Cuba 是多线程的，通过资源访问同步进行快速的加密，以避免文件损坏。

Cuba 会使用 GetKeyboardLayout API 检索受害者的活动区域设置标识符。当俄语在计算机支持的语言列表中时，进程会删除并使用简单的命令行终止自身而不再加密文件系统。

Cuba 会根据文件大小对文件进行不同方式的加密。如果文件长度小于 0x200000 字节，则对整个文件进行加密。如果大于则会以 0x100000 字节的块对文件进行加密，加密块之间的中断根据整体大小而有所不同。每个加密文件还带有一个初始的 1024 字节标头，其中包含 FIDEL.CA，然后是包含特定 ChaCha 密钥的 RSA–4096 加密块和随机数。成功加密文件后，扩展名 .cuba 会附加到文件名中。

另外，Cuba 在近期活动中还增加了两个更新，一是建立了将在运行时终止的目标进程和服务列表，并增加了目录和扩展名的数量以避免加密；二是相关通信不再只依赖于 Tor 站点，还通过 TOX 提供通信，由于其安全的消息传递功能，TOX 在勒索软件组织中逐渐变得越来越流行。加密数据以后，Cuba 会留下赎金记录，早期记录如下所示：

Sample Cuba Ransom Note, as of Mid-October 2021

Good day. All your files are encrypted. For decryption contact us.
Write here iracomp3@protonmail.com
We also inform that your databases, ftp server and file server were downloaded by us to our servers.

* Do not rename encrypted files
* Do not try to decrypto your data using third party software,
it may cause permanent data loss.

图 1 早期 Cuba Ransomware note

后期记录中添加了 TOX 方式：

Greetings! Unfortunately we have to report that your company were
compromised. All your files were
encrypted and you can't restore them without our private key. Trying
to restore it without our help may
cause complete loss of your data. Also we researched whole your
corporate network and downloaded all
your sensitive data to our servers. If we will not get any contact
from you in the next 3 days we will public
it in our news site.
You can find it there (
https[:]// cuba4ik ztyawtdgr2xymvy6nvgw5cglswg3si76icnqd.onion/)
Tor Browser is needed (https[:]//www.torproject.org/download/)
Also we respect your work and time and we are open for communication.
In that case we are ready to discuss
recovering your files and work. We can grant absolute privacy and
compliance with agreements by our side.
Also we can provide all necessary evidence to confirm performance of
our products and statements.
Feel free to contact us with quTox (https[:]//tox.chat/download.html)

图 2 Cuba ransomware note

03 Cuba 背后的组织

3.1 黑客组织 Tropical Scorpius

2022 年，结合 Cuba 勒索软件的多起攻击活动，研究人员把其背后的组织归结为 Tropical Scorpius（又名 UAC-0132、UNC2596）。Tropical Scorpius 一直利用相同的 Cuba 勒索软件有效载荷进行攻击活动。Tropical Scorpius 已使用 Cuba 勒索软件攻击了不同领域的组织，包括法律服务、地方政府、制造、运输和物流、批发和零售、金融服务、医疗保健、高科技、公用事业、能源、建筑和教育等行业。

3.2 Cuba 的关联组织

自 2022 年春季以来，多个安全厂商和开源报告已确定 Cuba 勒索软件组织与工业间谍勒索软件攻击者之间存在明显联系，具体表现在：

1）工业间谍勒索软件使用的赎金票据与 Cuba 赎金票据非常相似，两份票据都包含完全相同的联系信息；

2）根据第三方报道，疑似 Cuba 勒索软件组织入侵了一家外国医疗保健公司，但攻击者却部署了工业间谍勒索软件，并且其配置与 Cuba 勒索软件有明显的相似之处；

3) Unit 42 观察到一个 Cuba 勒索软件的有效载荷用于加密受感染系统上的文件并将 .cuba 扩展名附加到文件中，但随后观察到泄露的数据却在工业间谍勒索软件网站上发布出售。虽然不确定为什么 Tropical Scorpius 攻击者会利用工业间谍官网而不是他们自己的泄密站点来披露这些数据，但显示易见，两者的关系的确比较密切，其背后的组织极有可能为同一伙人。

工业间谍勒索软件官网：

图 3 Industrial spy 官网

下图为工业间谍勒索网站披露的三类数据，第一类 PREMIUM 数据为 7 天内售卖并且只卖一手的数据；如果数据超过 7 天，则移到 GENERAL，可进行多次售卖且价格较低；第三类为 FREE 数据，可以无偿免费下载，并且在数据库里永不删除。

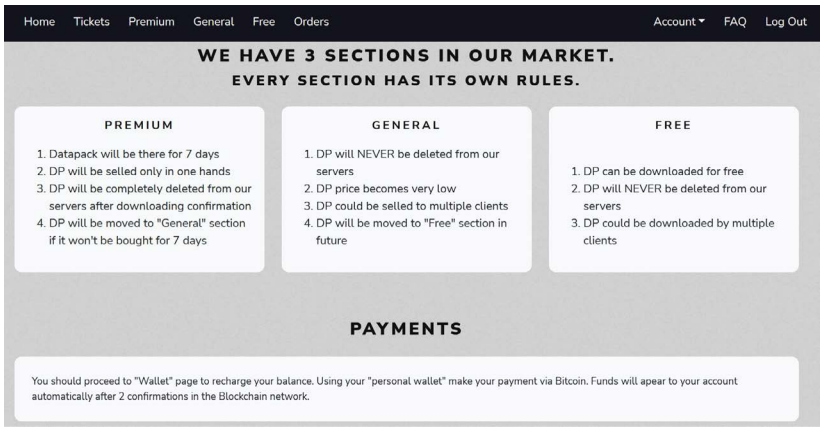
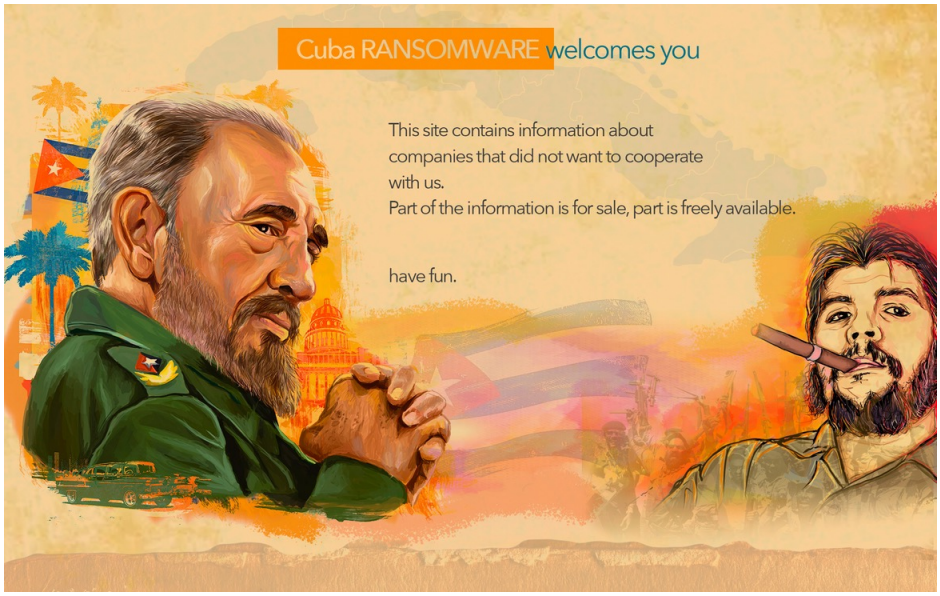


图 4 工业间谍售卖数据类型

下图为 Cuba 勒索软件运营者在暗网的数据披露网站，目前其官网上总共发布了 67 家公司的数据，其中 66 家数据已经是 free 状态，只有一家是待售状态。



Cuba 列出来的攻击公司列表：

* 以上公司数据已经是 free 状态

除了免费披露的数据，Cuba 官网目前只公布了一家需付费公司或组织的数据（可能由于交易原因，Cuba 并没有直接指明具体是哪家公司），付费内容如下图所示：

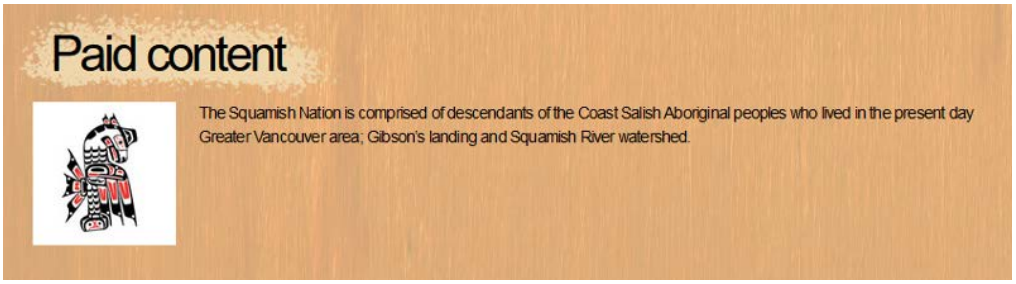


图 5 需付费内容

04 总结

Cuba 勒索软件虽然存在时间较长，但其攻击活动在 2022 年异常活跃，其采取双重勒索策略，攻击目标广泛，运作非常成功，目前已经赚取了比较丰厚的赎金。虽然研究人员确认 Tropical Scorpius 为其背后的组织，但 Cuba 勒索软件不一定只为一个组织所使用，很有可能有新的组织和活动继续使用 Cuba。 从攻击目标看，Cuba 攻击者并未回避敏感目标，他们攻击的行业非常广泛，包括政府及非营利性组织，这说明该组织运作庞大，目标多样化，且攻击成功率并不低。但是 Cuba 并不攻击以俄语作为主要语言的国家，其主要目标还是针对美国的公司，以获取经济利益为其首要目的。

05 附录

5.1 防护体系

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程序 ；

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。

5.2 IOCS

SHA256
00ddbe28a31cc91bd7b1989a9bebd43c4b5565aa0a9ed4e0ca2a5cfb290475ed
01242b35b6def71e42cc985e97d618e2fabd616b16d23f7081d575364d09ca74
02a733920c7e69469164316e3e96850d55fca9f5f9d19a241fad906466ec8ae8
02B17677BEC8A4FBB77FDDB347BFDCC651FF2B25187131CCE45C326E3CF42FE5
05f90cad3627f5253e1a03156793bc6cada7f4ce0d510f55139f0285fcff589d
08eb4366fc0722696edb03981f00778701266a2e57c40cd2e9d765bf8b0a34d0
0a3517d8d382a0a45334009f71e48114d395a22483b01f171f2c3d4a9cfdbfbf
0afed8d1b7c36008de188c20d7f0e2283251a174261547aab7fb56e31d767666
0c2ffed470e954d2bf22807ba52c1ffd1ecce15779c0afdf15c292e3444cf674
0cf6399db55d40bc790a399c6bbded375f5a278dc57a143e4b21ea3f402f551f
0d5e3483299242bf504bd3780487f66f2ec4f48a7b38baa6c6bc8ba16e4fb605
0eff3e8fd31f553c45ab82cc5d88d0105626d0597afa5897e78ee5a7e34f71b3
0f385cc69a93abeaf84994e7887cb173e889d309a515b55b2205805bdfe468a3
10a5612044599128981cb41d71d7390c15e7a2a0c2848ad751c3da1cbec510a2
141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944

1807549af1c8fdc5b04c564f4026e41790c554f339514d326f8b55cb7b9b4f79

1817cc163482eb21308adbd43fb6be57fcb5ff11fd74b344469190bb48d8163b

188E66158E0F96AD1FFD3F090E2570B8644CD80733C7AAFB931E893A4F280165

1b943afac4f476d523310b8e3afe7bca761b8cbaa9ea2b9f01237ca4652fc834

1d142c36c6cdd393fe543a6b7782f25a9cbafca17a1cfa0f3fc0f5a9431dbf3f

1f825ef9ff3e0bb80b7076ef19b837e927efea9db123d3b2b8ec15c8510da647

1f842f84750048bb44843c277edeaa8469697e97c4dbf8dc571ec552266bec9f

271ef3c1d022829f0b15f2471d05a28d4786abafd0a9e1e742bde3f6b36872ad

28140885cf794ffef27f5673ca64bd680fc0b8a469453d0310aea439f7e04e64

2EB3EF8A7A2C498E87F3820510752043B20CBE35B0CBD9AF3F69E8B8FE482676

310afba59ab8e1bda3ef750a64bf39133e15c89e8c7cf4ac65ee463b26b136ba

33352a38454cfc247bc7465bf177f5f97d7fd0bd220103d4422c8ec45b4d3d0e

3468C6DEB3827F5C161A8622E7D794444C7B38225F6F15002193D2572A4D132E

3a8b7c1fe9bd9451c0a51e4122605efc98e7e4e13ed117139a13e4749e211ed0

3d4502066a338e19df58aa4936c37427feecce9ab8d43abff4a7367643ae39ce

40101fb3629cdb7d53c3af19dea2b6245a8d8aa9f28febd052bb9d792cfbefa6

4306c5d152cdd86f3506f91633ef3ae7d8cf0dd25f3e37bec43423c4742f4c42

482b160ee2e8d94fa6e4749f77e87da89c9658e7567459bc633d697430e3ad9a

4b5eefa1727b97b6f773be3937a8cc390f0434ddc2f01dc24b68b690fafbcc93

54627975c0befee0075d6da1a53af9403f047d9e367389e48ae0d25c2a7154bc

571f8db67d463ae80098edc7a1a0cad59153ce6592e42d370a45df46f18a4ad8

5cd95b34782ca5acf8a34d9dc184cb880a19b6edcaf4a4553fa0619b597c2f50

61971d3cbf88d6658e5209de443e212100afc8f033057d9a4e79000f6f0f7cc4

6396ea2ef48aa3d3a61fb2e1ca50ac3711c376ec2b67dbaf64eeba49f5dfa9df

672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1

6d5ca42906c60caa7d3e0564b011d20b87b175cbd9d44a96673b46a82b07df68

729950ce621a4bc6579957eabb3d1668498c805738ee5e83b74d5edaf2f4cb9e

74fbf3cc44dd070bd5cb87ca2eed03e1bbeec4fec644a25621052f0a73abbe84

78ce13d09d828fc8b06cf55f8247bac07379d0c8b8c8b1a6996c29163fa4b659

79d6b1b6b1ecb446b0f49772bf4da63fcec6f6bfc7c2e1f4924cb7acbb3b4f53

7a17f344d916f7f0272b9480336fb05d33147b8be2e71c3261ea30a32d73fecb

7e00bfb622072f53733074795ab581cf6d1a8b4fc269a50919dda6350209913c

7e765942d89cd3bfaca41034cd959b8d741085bd8bcedbb741e15ed685227a5e

7f4bdf94a0e0457f41bdd1a8d8d9fc39fc383d3d0a331048828d391bbf727a1e

81bdd622f0cb9d7e2ac5325a74606fa7818bd4205f37184eba68cdcbe96942f6

88d13669a994d2e04ec0a9940f07ab8aab8563eb845a9c13f2b0fec497df5b17

8a3d71c668574ad6e7406d3227ba5adc5a230dd3057edddc4d0ec5f8134d76c3

8E64BACAF40110547B334EADCB0792BDC891D7AE298FBFFF1367125797B6036B

907f42a79192a016154f11927fbb1e6f661f679d68947bddc714f5acc4aa66eb

944ee8789cc929d2efda5790669e5266fe80910cabf1050cbb3e57dc62de2040

952b34f6370294c5a0bb122febfaa80612fef1f32eddd48a3d0556c4286b7474

9882c2f5a95d7680626470f6c0d3609c7590eb552065f81ab41ffe074ea74e82

9aa1f37517458d635eae4f9b43cb4770880ea0ee171e7e4ad155bbdee0cbe732

a7c207b9b83648f69d6387780b1168e2f1eabd23ae6e162dd700ae8112f8b96c

af4523186fe4a5e2833bbbe14939d8c3bd352a47a2f77592d8adcb569621ce02

b14341b1ffe9e2730394b9066c6829b4e2f59a4234765ae2e97cfc6d4593730a

b160bd46b6efc6d79bfb76cf3eeacca2300050248969decba139e9e1cbeebf53

b5d202456ac2ce7d1285b9c0e2e5b7ddc03da1cbca51b5da98d9ad72e7f773b8

B9AFE016DBDBA389000B01CE7645E7EEA1B0A50827CDED1CBAA48FBC715197BB

bcf0f202db47ca671ed6146040795e3c8315b7fb4f886161c675d4ddf5fdd0c4

bd270853db17f94c2b8e4bd9fa089756a147ed45cbc44d6c2b0c78f361978906

bda4bddcbd140e4012bab453e28a4fba86f16ac8983d7db391043eab627e9fa1

bff4dd37febd5465e0091d9ea68006be475c0191bd8c7a79a44fbf4b99544ef1

c206593d626e1f8b9c5d15b9b5ec16a298890e8bae61a232c2104cbac8d51bdd

c385ef710cbdd8ba7759e084051f5742b6fa8a6b65340a9795f48d0a425fec61

c4b1f4e1ac9a28cc9e50195b29dde8bd54527abc7f4d16899f9f8315c852afd4

c646199a9799b6158de419b1b7e36b46c7b7413d6c35bfffaeaa8700b2dcc427

d010fbb1afeb610338c49ae2425b6b7c4a9f4c469aedd096a15b32527565d7db

db3b1f224aec1a7c58946d819d729d0903751d1867113aae5cca87e38c653cf4
e0d89c88378dcb1b6c9ce2d2820f8d773613402998b8dcdb024858010dec72ed
e35593fab92606448ac4cac6cd2bd6b4df5d7ab3b733ba4b9472994cf0e3d87d
e82cc49c03320a0fb6ec3512c0ca3332eb1b40070cc53a78bc80b77b4aba975c
e942a8bcb3d4a6f6df6a6522e4d5c58d25cdbe369ecda1356a66dacbd3945d30
ecefd9bb8b3783a81ab934b44eb3d84df5e58f0289f089ef6760264352cf878a
EEDC68C92C50BE88C5935651D6B772D4728C3566581BE1F24D4CE7EF63A76D2E
f1103e627311e73d5f29e877243e7ca203292f9419303c661aec57745eb4f26c
f538b035c3de87f9f8294bec272c1182f90832a4e86db1e47cbb1ab26c9f3a0b
f5db51115fa0c910262828d0943171d640b4748e51c9a140d06ea81ae6ea1710
f8144fa96c036a8204c7bc285e295f9cd2d1deb0379e39ee8a8414531104dc4a
f869e8fbd8aa1f037ad862cf6e8bbbf797ff49556fb100f2197be4ee196a89ae
fd87ca28899823b37b2c239fbbd236c555bcab7768d67203f86d37ede19dd975

IP		
103.114.163.197	171.25.193.9	204.13.164.118
103.27.203.197	185.153.199.164	209.76.253.84
104.217.8.100	185.153.199.169	212.192.241.230
107.189.10.143	185.153.199.176	213.32.39.43
108.170.31.115	190.114.254.116	216.45.55.3
128.31.0.34	192.137.100.96	216.45.55.30
128.31.0.39	192.137.100.98	217.79.43.148
131.188.40.189	192.137.101.205	222.252.53.33
141.98.87.124	192.137.101.46	23.227.197.229
144.172.83.13	193.23.244.244	23.227.198.246
149.255.35.131	193.34.167.17	31.184.192.44
154.35.175.225	194.109.206.212	31.44.184.82
157.245.70.127	195.54.160.149	37.120.193.123
159.203.70.39	199.58.81.140	37.120.247.39
37.44.253.21	45.86.162.34	84.17.52.135

38.108.119.121	45.91.83.176	86.59.21.38
40.115.162.72	64.235.39.82	92.222.172.172
45.164.21.13	64.52.169.174	92.222.172.39
45.32.229.66	79.141.169.220	94.103.9.79
DOMAIN		
irrislaha.com	siagevewilin.com	kurvalarva.com
leptengthinete.com	surnbuithe.com	CombinedResidency.org
optasko.com		
EMAIL		
admansmit001@protonmail.com	fedelsupportagent@cock.li	helpallen@protonmail.com
admin@cuba-supp.com	fiaadministrator@cock.li	iracomp1@protonmail.ch
ad_default@protonmail.com	frankstore@cock.li	iracomp2@protonmail.ch
afts_agent@protonmail.com	helpadmin1@protonmail.com	iracomp3@protonmail.ch
cloudkey@cock.li	helpadmin2@cock.li	iracomp@cock.li
cuba _ support@exploit.im	helpadmin2@protonmail.com	ivantisupport@cock.li
dark_sysadmin@protonmail.ch	helpallen@cock.li	logme@cock.li
LR_FWS_H2M_ET@protonmail.ch	morebeerplease@cock.li	system_admC@protonmail.com
mail_supportRG@protonmail.com	roselondon@cock.li	under _ amur@protonmail.ch
mfra@cock.li	roselondon@protonmail.com	under_amur@protonmail.ch

5.3 参考资料

1. *https://www.ic3.gov/Media/News/2021/211203-2.pdf*
2. *https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware*
3. *https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/*
4. *https://www.cisa.gov/uscert/ncas/alerts/aa22-335a*
5. *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cuba-ransomware.pdf*

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