

# Geedge Networks 内部文件泄露 (Jira、Confluence、GitLab 等 100,000 多份) #519

打开 Geedge Networks 内部文件泄露 (Jira、Confluence、GitLab 等 100,000 多份) #519



工作岗位 打开上周由wkrp编辑

成员

我们讨论过中国公司积至 ([Geedge Networks](#))。去年,有消息称[积至为缅甸的VPN封锁提供了设备](#)。该公司的创始人之一是著名的“防火墙之父”[方滨兴](#)。[积至的另一位负责人郑超](#)是我们讨论过的审查相关研究论文的合著者: [#275](#)、[#282](#)、[#444](#)。

如今,关于 Geedge Networks 内部文件泄露的新闻报道和报道层出不穷,包括来自 Jira (漏洞追踪器)、Confluence (维基百科) 和 GitLab (源代码) 的报道。据称,多家新闻机构和技术人员已合作一年,对这些文件进行了分析。以下是直接接触这些文件的人员提供的主要报道,据我所知:

- 《[环球邮报](#)》: [泄露文件显示一家中国公司正在出口防火墙的审查技术](#) ([存档](#))
- 标准: [澳大利亚出口商的中国互联网总体情况](#) ([存档](#))
- [追踪资金流向](#): [中国在欧盟公司的帮助下向威权政权出口审查技术](#) ([档案](#))
- InterSecLab: [互联网政变](#) ([存档](#)) [PDF 76 页](#) ([存档](#))
- 国际特赦组织: [控制的阴影: 巴基斯坦的审查制度和大规模监视](#) ([存档](#)) [PDF 102 页](#) ([存档](#))
- 缅甸正义: [监控丝绸之路](#)([存档](#)) [PDF 47 页](#)([存档](#))

据我所知,此次泄密的具体内容尚未公开。即便如此,这些公开的文章和报告中也包含了大量信息。其中至少包括:向缅甸、巴基斯坦、埃塞俄比亚、哈萨克斯坦以及至少一个其他未确定国家出口的证据;在中国新疆、江苏和福建等省份的运营;Geedge 产品的技术信息;以及与中国科学院研究实验室[MESA的合作](#)。

**工作岗位** 额外 [中国](#) [哈萨克斯坦](#) [印度](#) [巴基斯坦](#) [埃塞俄比亚](#) [缅甸](#) [马来西亚](#) [巴林](#) [阿尔及利亚](#) [上周](#)

**工作岗位** 更改了标题 ~~Geedge Networks 内部文件泄露 (Jira、Confluence、源代码等 100,000 多份)~~ Geedge Networks 内部文件泄露 (Jira、Confluence、GitLab 等 100,000 多份) [上周](#)



工作岗位 上周由wkrp编辑

成员 作者

以下是这三篇新闻文章的注释和重点。

**《[环球邮报](#)》: [泄露文件显示一家中国公司正在出口防火墙的审查技术](#)**

泄露的内部文件显示, Geedge 直接与政府和互联网服务提供商合作, 安装用于审查和监控的产品。这些产品的功能包括追踪用户位置和网络访问历史, 以及屏蔽服务和规避系统。

.....泄露了超过 10 万份与[Geedge Networks](#)有关的内部文件, 这是一家鲜为人知的中国公司, 它悄悄地在开发中国防火长城方面发挥了关键作用, 并向世界各国政府提供类似的审查能力.....

这些文件不仅提供了关键的见解, 让我们了解 Geedge 如何向其专制客户出口尖端审查技术, 赋予他们原本可能无法拥有的能力, 而且还让我们了解了防火长城本身的演变。

这包括过滤网站和应用程序、实时在线监控、限制特定区域的互联网数据或实施互联网中断、通过在线足迹识别匿名用户以及阻止用于绕过审查的工具 (包括虚拟专用网络 (VPN)) 的解决方案。

Geedge 至少在另外五个国家开展业务: 哈萨克斯坦、埃塞俄比亚、缅甸 ([#369](#))、巴基斯坦以及一个代号为 A24 的未确定国家。哈萨克斯坦于 2018 年成立, 是 Geedge 的早期客户。

Geedge 成立于 2018 年, 其首批客户之一是哈萨克斯坦政府, 该公司向其出售了其旗舰产品天沟安全网关 (TSG), 该产品提供的功能类似于中国自己的防火长城, 可监控和过滤通过它的所有网络流量, 并试图绕过此类审查。

[同样的工具已在埃塞俄比亚和缅甸](#)推出，并在该国军政府实施VPN禁令的过程中发挥了重要作用。文件显示，Geedge 在许多情况下与其他私营公司合作，包括埃塞俄比亚的 Safaricom 或缅甸的 Frontiir 和 Ooredoo 等互联网服务提供商 (ISP)，以实施政府审查。所有与 Geedge 合作的 ISP 均未回应置评请求。

[缅甸在“缅甸正义”组织的“监控丝绸之路”报告中被特殊对待](#)。巴基斯坦在“大赦国际”组织的[“控制阴影”](#)报告中被特殊对待。

关于巴基斯坦，《[环球邮报](#)》的一篇文章称，Geedge 在 Sandvine 留下的现有设备上安装了包括 Tiangou 安全网关 (TSG) 在内的新系统。（Sandvine 现更名为 AppLogic。）

由于在巴基斯坦的工作受到越来越多的审查，Sandvine 于 2023 年退出了巴基斯坦，并很快被 Geedge 取代。文件显示，Geedge 显然利用了现有的 Sandvine 设施，同时还提供了新技术来支持伊斯兰堡的网络监控系统（该国的国家防火墙）。

AppLogic 在一份声明中表示，它不知道 Geedge 的存在，该公司重新利用的任何硬件都是现成的设备，“不包含 Sandvine 解决方案独有的任何特殊功能”。

[文章引用了#369（评论）](#)中发布的同一招聘广告，其中提到了另外四个国家：马来西亚、巴林、阿尔及利亚和印度：

Geedge最近发布的一则[招聘广告](#)也提到了“一带一路”倡议。该广告要求应聘者“能够说英语或其他外语”，并愿意前往“巴基斯坦、马来西亚、巴林、阿尔及利亚和印度”进行为期三到六个月的商务旅行。

除了外国之外，文件还显示 Geedge 还涉足了中国新疆、江苏和福建等省份。这可能表明防火墙系统更加分散，区域性更强，正如[#416](#)和[“墙后的墙”](#)等帖子中关于河南省的讨论一样。

Geedge 与中国科学院大学的研究实验室 MESA 密切合作。我们之前在一篇关于 MESA 的“SAPP”网络分析平台的读书会帖子中 ([#471, 评论](#)) 提到过 MESA。Geedge的首席技术官[郑超 \(Zheng Chao\)](#) 于 2012 年 1 月与 MESA 共同创立。

Geedge 的文件中，方先生被自豪地称为“防火墙之父”。公司其他高层人员，例如首席执行官王元地和首席技术官郑超，都被列为互联网审查[论文的共同作者，以及Geedge 申请专利](#)的创造者。该公司还与中国科学院[大规模高效流分析实验室](#)（MESA Lab）保持着密切的合作关系，文件显示两家机构的人员之间经常合作。

2024 年 7 月，在新疆举行的会议上，MESA 实验室的一名研究员做了笔记，与会者谈到利用技术“打击使用工具”绕过防火长城的行为，并建立“新疆分中心”作为“反恐先锋”和“省级能力示范”。

该公司对规避系统和 VPN 进行了专门研究，以便对其进行阻止。

泄密文件显示，该公司员工正在对许多常用工具进行逆向工程，并寻找屏蔽它们的方法。一组文件列出了九个已“解析”的商业VPN，并提供了各种识别和过滤流量的方法。中国国家防火墙早已展现出类似的能力，大多数商业VPN在中国境内无法访问，许多专用的反审查工具也难以访问。

## 标准：澳大利亚出口商的中国互联网总体状况

### ▼ 机器翻译成英文：中国如何将其对互联网的全面监控输出到国外

一家中国公司正在向专制国家提供这方面的技术。这将对反对派人士和记者造成严重后果。

索菲亚·鲍曼  
2025年9月9日 05:00

他的名字代表着一个庞大的体系：方滨兴，教授，党员，数字控制的缔造者。任何想知道他做什么、他代表什么的人，都必须读懂字里行间的含义——或者在中国防火墙之外寻找答案。因为方滨兴是中国那个筛选、控制、甚至让信息消失的体系的创始人之一：所谓的“防火墙”。

2011年，在武汉的一次演讲中，据称一名身份不明者向方滨兴投掷了一枚鸡蛋和一只鞋子。这是对这位将中国互联网变成自由壁垒之人的象征性抗议。方滨兴的办公室当时否认了此事。

## 全面监控成为出口热点

2018年，方舟子创立了Geedge Networks公司，他原本计划通过这家公司将自己的发明——中国防火墙——打造成一项出口热销产品。独家研究表明，Geedge Networks曾向多个国家（其中大多数是专制国家）提供审查和监控技术，而且可能仍在继续。其问题客户包括缅甸、巴基斯坦、哈萨克斯坦、埃塞俄比亚以及中国地方当局。

DER STANDARD 与荷兰平台[Follow the Money](#)和加拿大报纸《[环球邮报](#)》合作，在非政府组织[国际特赦](#)组织、主要关注缅甸军政府的活动组织[“缅甸正义”](#)、Tor 项目和 Intersec Lab 的帮助下，对此事进行了数月的研究，Intersec Lab 也为该组织提供了技术支持。

[Intersec Lab 的 IT 安全专家分析](#)显示，Geedge Networks 提供的技术极其强大。这些技术使当局能够监控特定区域（例如抗议期间）个人数据流量。它们可以精准检测并阻止用户此前用于规避当局数字审查的个人虚拟专用网络 (VPN)。它们甚至可以向网站植入恶意代码或发起 DDoS 攻击，从而瘫痪单个网站。

## “严重的人道主义后果”

讽刺的是，Geedge Networks 提供这些工具的国家长期以来一直饱受诟病。美国非政府组织“自由之家”将中国、缅甸、埃塞俄比亚、巴基斯坦和哈萨克斯坦列为互联网自由“不自由”的国家。

例如，在埃塞俄比亚就可以看到其具体含义。从2020年开始，政府关闭了提格雷地区的互联网长达两年之久——当时正值一场严重侵犯人权的武装冲突。这阻碍了食品和医疗援助的协调。自由之家的基安·韦斯坦森表示，封锁造成了“严重的人道主义后果”。

2021年军事政变后，缅甸也大幅加强了对数字领域的管控。目前，只有军方预先批准的网站才能访问。与此同时，路障会检查手机，以查找是否安装了VPN应用程序。如今，科技正在做着士兵曾经做过的事情。

研究表明，Geedge Networks 的审查和监视技术目前也正在上述国家使用。

埃塞俄比亚、哈萨克斯坦、巴基斯坦和中国均未回应《标准报》的置评请求。缅甸当局也未能联系到置评。Geedge Networks 和方滨兴也未回复所有询问。

## 来自西方的监控技术

与此同时，Geedge Networks 并非第一家向独裁者和审查制度盛行的当局提供此类技术的公司。西方公司也活跃于这一市场，并多年来一直受到批评。

例如，非政府组织“隐私国际”在2015年披露，巴基斯坦正在使用德国公司的监控技术。即使在当时，巴基斯坦的大规模监控狂潮也已众所周知。据媒体报道，其中一家德国公司Utimaco也在缅甸积极开展业务。当被问及此事时，Utimaco表示，该公司始终遵守所有法律法规。此外，该公司从未与缅甸任何移动网络运营商直接开展业务。

后来，据称加拿大公司Sandvine向巴基斯坦提供了一套系统，使当局能够屏蔽不受欢迎的网站。2023年，Sandvine（现已更名为Applogic Networks）撤出了巴基斯坦。但显然至少有部分Sandvine硬件留在了巴基斯坦。

研究表明，Geedge Networks 至少在最初阶段曾重复使用过该技术。Applogic Networks 向《STANDARD》表示对此毫不知情。此外，该公司强调，其技术不能用于解密用户数据或部署间谍软件。

## 欧洲痕迹

一家法国公司也无意中成为了 Geedge Networks 的同谋。法国泰雷兹集团销售可用于管理许可证的软件。Geedge Networks 显然利用了这一点来控制其所售产品，从而能够在限定时间内限制软件的功能。

泰雷兹集团经要求向《标准晚报》证实，这家中国公司是其客户之一。然而，Geedge Networks 的软件并不依赖这家法国产品运行。该公司声称与监控无关。

此外，Geedge Networks 似乎使用了一台德国服务器，通过下载链接向客户分发其软件。其动机尚不清楚。但众所周知，中国防火墙使得从国外访问中国网站变得越来越困难。德国相关部门尚未回应《标准晚报》就此事的询问。

## 数字威权主义模式

与西方供应商不同，像 Geedge Networks 这样的公司不太可能受到道德标准的约束。相反，在这里，传播自身技术似乎是一个压倒一切的政治目标。

自由之家的基安·韦斯坦森表示，中国希望“输出其数字威权主义模式”。对于缅甸这样的专制邻国来说，尤其如此。

尽管审查制度早已成为中国民众的常态，但在缅甸，反抗的浪潮正在兴起。参与此次调查的“缅甸正义”组织去年就警告不要与Geedge Networks合作。巴基斯坦“Bolo Bhi”组织的乌萨马·基尔吉 (Usama Khilji) 也发出了警告。“巴基斯坦是一个民主国家，我们拥有基本权利——我们不能像中国政府对待其公民那样被对待，”他在调查结果公布之前就表示。

Geedge Networks 的一个新职位目前正在中国的一个在线招聘网站上发布。申请者的标准之一是愿意出差——不仅要去巴基斯坦，还要去马来西亚、印度、巴林和阿尔及利亚。因此，Geedge Networks 的业务似乎正在蓬勃发展，阿尔及利亚、马来西亚、印度和巴林可能也已经在使用其服务或表现出兴趣。相关国家的相关部门尚未回应《标准晚报》的提问。

“防火墙”的精髓早已深入人心。它潜入网络，拦截数据，过滤信息。有时甚至连它的创造者本人也受到影响：2016年，方滨兴在一次演讲中想展示一个韩国网站，结果被他自己设计的防火墙屏蔽了。（索菲亚·鲍曼，2025年9月9日）

本文列出了 Geedge 技术除了跟踪用户和阻止访问之外的其他功能：将恶意软件注入 HTTP 会话，以及直接发起 DDoS 流量攻击。

Die Technologien, die Geedge Networks anbietet, sind überaus mächtig, zeigt [eine Analyse der IT-Sicherheitsexperten von Intersec Lab](#). Sie ermöglichen Behörden, den Datenverkehr von Einzelpersonen in bestimmten Regionen zu überwachen, beispielsweise während Protesten. Sie können gezielt einzelne Virtual Private Networks (VPN) und blockieren, mit deren Hilfe Nutzer bislang die digitale Zensur von Behörden umgehen konnten. 请注意网站中的代码可能会启动或启动 DDoS-Angriffe 并删除该网站中的代码。

[Intersec Lab 的 IT 安全专家分析](#)显示, Geedge Networks 提供的技术极其强大。这些技术使当局能够监控特定区域 (例如抗议期间) 个人数据流量。它们可以精准检测并阻止用户此前用于规避当局数字审查的个人虚拟专用网络 (VPN)。它们甚至可以向网站植入恶意代码或发起 DDoS 攻击, 从而瘫痪单个网站。

该文件还提到, Geedge 软件正在巴基斯坦重新利用的 Sandvine 硬件上部署。显然, Geedge 非常重视软件与硬件的分离。

巴基斯坦 Sandvine 的 Später 是由巴基斯坦的 System geliefert haben 提供的, 它是 Internet 上的块状块。2023 年, Sandvine 于 Applogic Networks 中运营, 并在 Land zurück 中运行。Aber offenbar hinterließ es zumindest Teile der Sandvine-Hardware 位于巴基斯坦。

了解这一传奇故事后, Geedge Networks 就开始了我们的工作。Applogic Networks 采用 STANDARD 技术, 并已使用该技术。开发者将在 Unternehmen 中使用该技术, 并将其与间谍软件集成在一起。

后来, 据称加拿大公司 Sandvine 向巴基斯坦提供了一套系统, 使当局能够屏蔽不受欢迎的网站。2023 年, Sandvine (现已更名为 Applogic Networks) 撤出了巴基斯坦。但显然至少有部分 Sandvine 硬件留在了巴基斯坦。

研究表明, Geedge Networks 至少在最初阶段曾重复使用过该技术。Applogic Networks 向《STANDARD》表示对此毫不知情。此外, 该公司强调, 其技术不能用于解密用户数据或部署间谍软件。

法国公司 [泰雷兹集团 \(Thales Group\)](#) 为 Geedge 提供许可证执行服务。Geedge 至少使用一台位于德国的服务器进行软件下载。(如果下载服务器托管在中国, 或许是为了避免 GFW 的干扰。)

Auch ein französisches Unternehmen wurde – wohl unfreiwillig – zum Helfer von Geedge Networks。法国泰雷兹集团是一家软件公司, 由 Lizenzen 负责管理。Geedge Networks 非常乐意为您提供控制服务。请注意软件的功能特性。

泰雷兹集团标准版的最佳性能是中国的标准。Geedge Networks 的软件是一款法国产品, 具有功能。Mit der Überwachung habe man nichts zu tun。

Geedge Networks 提供德国服务器、软件和下载链接。Die Motive dafür bleiben unklar。请注意, Zugriff 的中国防火墙是澳大利亚的中国网站。德国的部长级会议以标准主题为基础。

一家法国公司也无意中成为了 Geedge Networks 的同谋。法国泰雷兹集团销售可用于管理许可证的软件。Geedge Networks 显然利用了这一点来控制其所售产品, 从而能够在限定时间内限制软件的功能。

泰雷兹集团经要求向《标准晚报》证实, 这家中国公司是其客户之一。然而, Geedge Networks 的软件并不依赖这家法国产品运行。该公司声称与监控无关。

此外, Geedge Networks 似乎使用了一台德国服务器, 通过下载链接向客户分发其软件。其动机尚不清楚。但众所周知, 中国防火墙使得从国外访问中国网站变得越来越困难。德国相关部门尚未回应《标准晚报》就此事的询问。

## 追踪资金流向: 中国在欧盟公司的帮助下向威权政权出口审查技术

本文概述了 Geedge 的各种产品, 这些产品可以捆绑销售或单独销售。Cyber Narrator 是一种高级仪表盘, 非技术用户可以直接与之交互。Tiangou Secure Gateway (TSG) 是实际的网络监控和阻断设备。TSG Galaxy 是一个数据存储和分析管道。Network Zodiac 是其他系统的管理器和监视器。

InterSecLab 的数据分析显示, Geedge Networks 的产品组合包含多种不同的技术。“网络叙述者”是客户交互的主要界面。它甚至允许非技术熟练的个人监控特定区域的互联网用户群体, 例如在示威活动期间。

然后是“天沟安全网关”——据信是旗舰产品。这款工具不仅可以阻止 VPN, 还可以在网站中插入恶意代码或对网站发起攻击。

另一款产品是“TSG Galaxy”, 用于存储收集到的用户数据, 而“Network Zodiac”则监控所有其他系统并报告任何错误。

Geedge 设备 (例如 TSG) 的安装数量可能比此次泄密事件中提到的国家还要多, 因为 Geedge 的公共营销网站上说“全球有 40 多家服务提供商”:





一家中国媒体报道了黄斌星在2024年的一次演讲中宣布，公司的目标是拓展“国际市场”，并在全球范围内推广中国技术。他似乎确实做到了这一点，因为文件显示，缅甸、巴基斯坦、埃塞俄比亚和哈萨克斯坦都持有至少其旗舰产品天沟安全网关的许可证。此外，Geedge Networks的网站宣称其服务于“40多家全球服务提供商”，这表明其覆盖范围远超泄露文件所称。

Geedge 于 2023 年 2 月提交了一张支持工单，内容涉及埃塞俄比亚社交媒体的封锁。这与当时埃塞俄比亚已知的封锁措施 (#210) 相关。

2023年2月，在全国抗议浪潮中，Geedge Networks的一份支持工单显示，他们的专家被召去修复YouTube和Twitter等社交媒体平台的问题。在同一时间段内，社交媒体平台的访问被屏蔽。

至少有一张 Jira 支持票显示了捕获电子邮件纯文本的证据：

内部文件显示，Geedge Networks 的工具（包括 Tiangou Secure Gateway）曾在巴基斯坦使用——至少有一次，一家全球航运公司与一家巴基斯坦公司之间的电子邮件通信被拦截。

-   **工作岗位** 在 6 期中提到了这一点 5天前
- 据报道，缅甸自 2024 年 5 月 30 日起封锁 VPN，由一家中国公司 Geedge Networks 实施 #369
  - 据报道，巴基斯坦国家“网络管理系统”防火墙使用中国设备 #510
  - 国际限速（中国） #520
  - [英文翻译] 一种网络访问控制规则的描述方法、构建方法及介质（专利申请CN109391590，2017年） #444
  - [英语翻译]基于Web中间件的高级逃避技术研究是实现（北京理工大学 2018） #471
  - 埃塞俄比亚社交媒体封锁，2023年2月9日 #210

  **工作岗位** 额外 读书小组 5天前



工作岗位 5天前

成员 作者

[InterSecLab 的报告](#) (PDF格式, 76 页) 非常出色，包含大量具体的技术细节。它详细介绍了 Geedge 的产品套件、其与MESA研究实验室的合作，以及在各国的部署时间表。

第 7 页

这项研究基于对 Geedge Networks 与 InterSecLab 共享的超过 10 万份泄露文档的分析，揭示了 Geedge Networks 系统的特性和功能，包括深度数据包检测、移动用户实时监控、互联网流量的精细控制以及可针对每个地区定制的审查规则。此次泄露还披露了 Geedge Networks 与学术机构 Mesalab 的关系，以及他们与客户政府的互动。这对数据主权的影响重大，我们的研究结果引发了人们对监控和信息控制技术商品化的担忧。

本研究考察了 Geedge Networks 系统在各国的最新发展情况，包括已知的部署时间表。通过分析该公司的内部文档，InterSecLab 得以记录商用国家防火墙的扩张历程，并推测此类系统的普及将对全球互联网的未来产生何种影响。

Geedge 产品

天沟安全网关

Tiangou 安全网关 (TSG) 是多用途防火墙和监控单元的全称。TSG 包含所有主要的深度数据包检测 (DPI)、过滤、跟踪、限制和攻击功能。TSG 提取的数据会被存储到 TSG Galaxy 中进行分析。

第 22 页

TSG 的功能非常广泛，包括通过深度包检测进行监视和审查的功能、识别和阻止 VPN 和规避工具的功能、限制流量的功能、监控、跟踪、标记和阻止个人互联网用户的功能以及使用恶意软件感染用户的功能。

TSG 可以安装在名为TSGX的集成硬件平台上，也可以与客户现有的硬件协同工作。（报道称，在巴基斯坦，Geedge 的 TSG 安装在 Sandvine 留下的设备上。）TSG 运行名为 TSG-OS的操作系统，该系统基于 Red Hat Enterprise Linux 和 Docker（参见 郑超等人撰写的《一种灵活高效的基于容器的 NFV 中间件网络平台》）。

可以根据需要安装任意数量的 TSG 节点，并使用名为 Ether Fabric 的数据包代理 通过五元组哈希在所有节点上进行负载均衡。TSG 集群管理系统称为 中央管理 (Central Management)，简称毕方 (Bifang)。

TSG 依赖于名为 MARSIO 的用户空间网络系统。也就是说，它自行进行路由和数据包处理，绕过 Linux 内核以提高效率。它使用DPDK。（再次参见 2018 年的[“灵活高效的基于容器的 NFV 中间件网络平台”](#)。）

TSG 银河

TSG Galaxy 是一个数据存储和聚合系统（[提取、转换、加载 数据仓库](#)），其中包含有关 TCP 和 UDP 会话以及 TLS、SIP、DNS 和 QUIC 等协议的元数据信息。Cyber Narrator 可以查询 Galaxy 中的信息。

[第 20 页](#)

TSG Galaxy 是 Geedge Networks 的 ETL（提取、转换、加载）数据仓库解决方案，专为互联网规模的大规模监控而设计，可收集和汇总有关所有互联网用户的大量数据以及客户所在国家/地区通过互联网发送的数据。它基于开源 Apache Kafka 流处理平台<sup>5</sup>构建，该平台是一种常见的数据处理软件，常用于为在线零售商和广告商提供客户分析。本次研究分析的泄露数据包括 TSG Galaxy 的 SQL 模式<sup>6</sup>，该模式表明 TSG Galaxy 用于存储所有 TCP 和 UDP 会话的记录、主要用于宽带和移动数据的传输协议以及该国境内的所有 SIP 会话。SIP 是用于 VoIP（互联网语音协议）的协议，是大多数现代电话网络的基础。这意味着 TSG Galaxy 不仅可以监控互联网上的网络流量和内容，还可以监控电话通话。

TSG Galaxy 使用互联网协议流信息导出 (IPFIX) 分析流量，并使用深度包检测 (DPI) 提取元数据。使用 DPI，他们可以提取详细的指纹，包括 TLS 和 QUIC 服务器名称指示、DNS 查询和电子邮件标头。TSG Galaxy 还实施了连接指纹识别技术，例如 JA3 哈希，使 Cyber Narrator 能够识别模式，从而帮助确定用户使用的操作系统以及他们使用的应用程序进行连接。此技术可用于帮助识别用户是否正在使用 VPN 等规避工具来掩盖流量或绕过审查。在 TSG Galaxy 中，所有这些信息都与来自互联网服务提供商的信息相结合，通过各种标识符（包括 IP 地址、用户 ID、IMEI 和 IMSI<sup>7</sup>）将其与个人互联网用户关联起来。从 TSG Galaxy 提取的元数据被发送到数据库，客户端可以通过 Cyber Narrator 进行查询。

[网络叙述者](#)

Cyber Narrator 是一款专为非技术用户设计的用户界面，可用于查询和显示 TSG 收集并存储在 TSG Galaxy 中的信息。Cyber Narrator 可以控制服务和协议的阻止，并提供查找访问过特定内容的用户标识符的功能。Cyber Narrator 使用远程 WebSketch 服务，该服务使用来自第三方数据代理或 Geedge 自身研究的元数据对 IP 地址等标识符进行注释。

[第 19 页](#)

Cyber Narrator 是一款功能强大的工具，能够追踪单个客户层面的网络流量，并通过将移动用户的活动与特定的小区标识符 (cell ID) 关联起来，实时识别其地理位置。该系统还允许政府客户查看汇总的网络流量。

...Cyber Narrator 可以让客户政府和安全部队更轻松地标记使用规避工具或访问客户政府认为可能存在恶意行为的其他应用程序或网页的个人用户。Cyber Narrator 的分析功能还可以阻止对特定网站或虚拟专用网络 (VPN) 服务的访问。通过 Cyber Narrator，客户政府还可以识别在限制访问之前访问过相关内容或服务的个人。

[网络十二宫](#)

Network Zodiac 或哪吒 (Nezha) 是一个用于监控其他组件的系统，类似于[Grafana](#)。显然，Network Zodiac 仪表板能够通过 SSH 连接到任何其他主机（例如 TSG 节点），如果 Network Zodiac 主机被攻陷，这显然会带来巨大的风险。

[第 33 页](#)

Network Zodiac 与主流开源解决方案的一个显著区别在于其集成的 Web 终端，该终端允许网络管理员使用 SSH 远程连接到任何受监控的端点。此功能使客户端能够直接访问网络设备，以便进行故障排除和管理。然而，它也使客户端面临巨大的安全风险。在最坏的情况下，黑客甚至可能访问客户端部署在某个国家/地区的所有安全设备。

## TSG 功能

TSG 具有典型的多协议深度包检测和阻止功能，但还具有令人惊讶的限制、注入、跟踪和攻击功能。

### 镜像模式和串联模式

TSG 和 Ether Fabric 可以以路径上（“镜像”或“被动”）模式或路径内（流阻塞或“主动”）模式安装。

[第 37 页](#)

Geedge 系统可以部署在两种主要模式下，即镜像模式和串联模式，以帮助控制互联网。在镜像模式下（有时在文档中称为“被动模式”），数据通过网络分路器镜像到 Geedge 设备。具体来说，网络分路器是一个光纤旁路交换机。数据包无需等待处理即可继续传输到目的地。在这种模式下，即使 Geedge 系统发生故障，互联网仍可继续运行。这种模式的优势在于它不会因处理延迟或拥塞而增加网络延迟。在镜像模式下，客户端无法阻止特定流量通过，而必须依靠数据包注入来阻止连接。

在串联模式（文档中也称为“主动”模式）下，流量必须先经过 Geedge 设备才能继续到达目的地。.....此模式的优势在于可以完全阻止特定流量通过网络。这通常是那些希望获得绝对控制权但牺牲可靠性和网络质量的客户所选择的解决方案。

将此与2024 年[巴基斯坦官员的声明进行比较](#)：

但为了监控本地流量，新防火墙将使用所谓的“内联网络”，其作用类似于安全检查站，每个数据包都必须经过检查，然后允许通过或阻止 - 而不是简单地观察和记录流量而不干扰其流动的替代机制。

该ISP官员表示，使用串联网络“必然会降低网速”。

## 深度数据包检测

报告中提到了 HTTP、DNS、电子邮件、TLS、QUIC 和 SIP 协议。

服务器名称指示 (SNI) 可以从 TLS 和 QUIC 中提取。（有关中国基于 QUIC SNI 的审查，请参阅[“揭露和规避中国防火墙基于 SNI 的 QUIC 审查”](#)。）

### 第 20 页

使用 DPI，他们可以提取详细的指纹，包括 TLS 和 QUIC 服务器名称指示、DNS 查询和电子邮件标头。

如果客户端安装了 MITM 证书，则可以解密 TLS 流量；否则 TSG 必须依赖加密流量分类启发式方法：

### 第 23 页

TSG 能够通过两种主要方法分析传输层安全 (TLS) 流量。第一种方法是使用中间人 (MITM) 技术进行完全解密，这需要订阅者安装自签名的根证书颁发机构 (CA) 证书。第二种方法采用深度数据包检测 (DPI) 和机器学习技术从加密流量中提取元数据。后一种方法更为常用，因为它对互联网用户不可见，因此互联网用户无需安装 CA 证书或配置任何代理设置。.....负责实施 TLS MITM 攻击的组件称为 Tiangou 前端引擎 (TFE)。

## 流量限制

### 第 25 页

TSG 集成流量整形功能，可对特定服务的流量进行优先级排序或限制，从而降低服务质量，而非直接阻止服务。这可以通过直接流量整形或应用差分服务代码点 (DSCP) 标记来实现，DSCP 标记是限制或优先处理流量的行业标准。

## 注入和修改

TSG 能够注入流量并修改流量。它可以出于阻止的目的进行此类操作，甚至可以用恶意软件感染用户，或诱导用户发起 DDoS 攻击，[就像“大炮”](#)一样。

### 第 23 页

TSG 还能够通过欺骗重定向响应、更改标头、注入脚本、替换文本和覆盖响应主体等技术实时修改 HTTP 会话。

### 第 26 页

TSG 配备了路径内注入功能，允许将恶意代码插入通过网络传输的文件中。Geedge Networks 明确表示，此功能旨在将恶意软件插入通过 TSG 系统的互联网流量中。

TSG 的路径内注入功能系统能够针对特定用户精准地定位恶意代码，支持对各种文件格式（包括 HTML、CSS 和 JavaScript）以及 Android APK 文件、Windows EXE 文件、macOS DMG 磁盘映像和 Linux RPM 软件包进行即时修改。此外，TSG 还可以修改多种图像格式（例如 JPG、GIF、PNG 和 SVG）以及各种存档格式（例如 ZIP 和 RAR），以及办公文档、PDF、JSON 和 XML 文件。Cyber Narrator 也对此进行了补充，它拥有分析功能，可以识别最合适的 URL 进行劫持，从而感染特定个人。例如，它可以定位用户经常访问但未使用传输层安全性 (TLS) 的网站。

### 第 27 页

泄露的数据中，Geedge Networks 最令人困惑的产品之一是 DLL Active Defence，这款产品通常出现在网络犯罪黑市中。乍一看，它似乎是一个旨在防御分布式拒绝服务 (DDoS) 攻击的系统；然而，仔细观察就会发现，它实际上是一个针对政治上不受欢迎的网站和其他互联网服务发起 DDoS 攻击的平台。这似乎是 Geedge 自己对“中国大炮”的实现，正如 2015 年公民实验室报告中所描述的那样。<sup>13</sup>

DLL 的实现方式是利用互联网扫描来识别流量放大点，例如递归 DNS 服务器，这些服务器可以作为反射式拒绝服务攻击的发射台。它利用 TSG 中的路径内注入功能，有效地招募毫无戒心的用户计算机参与攻击，从而创建僵尸网络。这是首例经证实的网络安全公司向客户提供本质上是“引导式”DDoS 租赁解决方案的案例。

将网络流量归因于真实身份

第 25 页

健全性目录 (SAN)，即用户信誉流量管理系统，是一种用户感知系统，旨在将 TSG 与互联网服务提供商 (ISP) 现有的信令和身份验证、授权和计费 (AAA) 协议（包括 RADIUS、3GPP 和 CGNAT）无缝集成。这种集成有助于将流量归因于真实身份。

第 49 页

Geedge 的 Sanity Directory 组件的核心功能之一是将流量归因于特定的 SIM 卡。这不仅可以实现大规模监控，还可以针对巴基斯坦及 Geedge 运营的其他国家/地区的特定个人进行高度精准的微型监控。

识别和阻止规避工具

Geedge 拥有付费 VPN 帐户，并运营着安装了 VPN 应用程序的移动设备网络，以研究其网络行为：

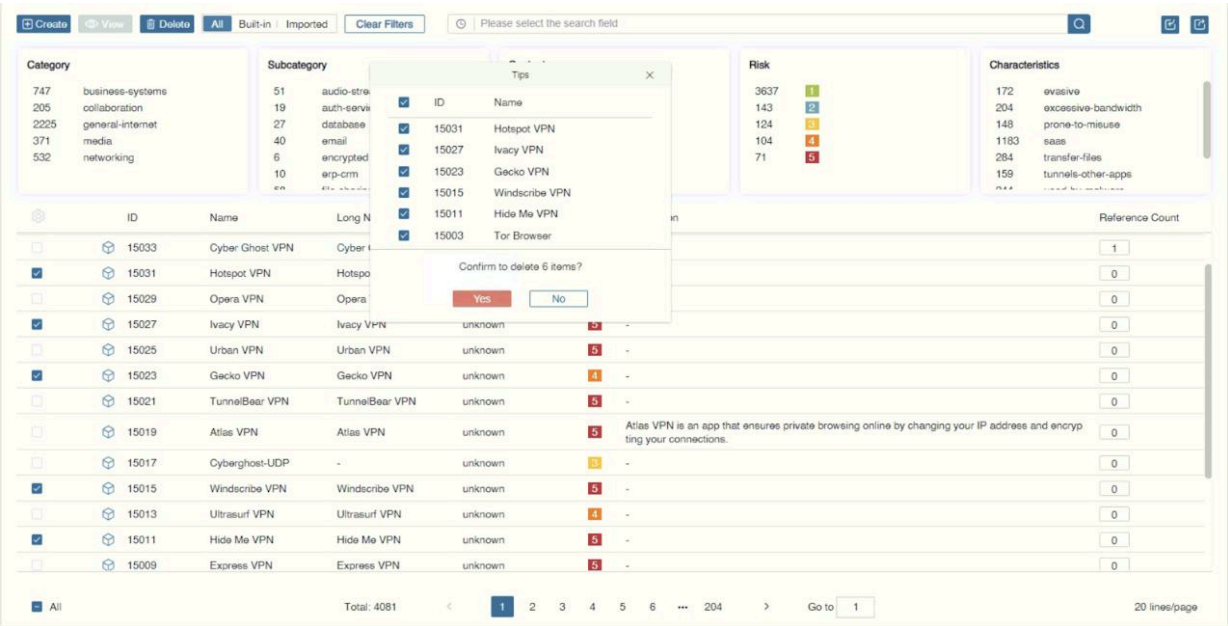
第 24 页

TSG 还采用深度数据包检测技术，全面识别与虚拟专用网络 (VPN) 相关的协议以及 OpenVPN 和 WireGuard 等规避工具。然后，它允许客户与 Geedge Networks 合作制定规则集，以阻止对特定服务提供商的访问，同时 Geedge 管理一个移动设备场，以便在受控环境中安装和运行 VPN 应用程序。

第 63 页

为了创建阻止规则，Geedge Networks 使用逆向工程，同时采用静态和动态分析。静态分析包括反编译应用程序的源代码，以查找返回服务器列表的 API，然后可以阻止这些服务器。动态分析包括运行 VPN 应用程序并分析其网络流量以识别阻止模式。

泄露的证据表明，Geedge Networks 在热门 VPN 提供商处持有付费账户，用于分析和屏蔽其应用程序。TSG 硬件还可以识别 IPsec、OpenVPN 和 WireGuard 等热门 VPN 协议。



有一个名为 AppSketch 的应用程序网络指纹数据库，其中包含许多特定应用程序的指纹，例如单个 VPN 服务。参见上面的屏幕截图。

脚注 10 关于 AppSketch 指纹的收集，提到了我们之前讨论过的SAPP（#471）和 Maat（#444）技术。

为了提取这些 [AppSketch] 指纹，Geedge 和 Mesalab 的学生使用了开源工具 tcpdump 的修改版本，他们将其称为 tcpdump\_mesa。随后，指纹被转换为规则集，利用以下四个深度数据包检测系统之一：SAPP（流分析处理平台），一个 C 语言数据包解析和注入库；Stellar，一个状态防火墙插件平台，与 SAPP 相比，它在更高的抽象级别上运行；以及 Maat，一个声明式系统。与 SAPP 和 Stellar 不同，Maat 不需要编程知识即可开发新规则。Maat 能够匹配常见的连接指纹，包括 JSON 文件中指定的 IP 地址、域名、TLS 服务器名称指示 (SNI) 和 JA3/JA4 指纹。Maat 规则通过使用 Redis 数据库在 TSG 集群内的节点之间同步，从而确保这些规则应用的一致性。

一个有趣且令人惊讶的功能是通过观察过去已知 VPN 用户的行为来发现新的 VPN 端点。（这让人想起了“通过图形表示的行为识别 VPN 服务器”，其作者隶属于 MESA。）



[第9页](#)

此外，Geedge Networks 产品能够识别特定个人为已知 VPN 用户。一旦这些已知的翻墙工具用户转移到尚未被屏蔽的新提供商，Geedge Networks 就可以监控用户的流量，并利用他们留下的痕迹来识别未来需要屏蔽的新 VPN。

[第 26 页](#)

此外，该系统可以识别单个用户为已知的VPN用户，随后跟踪他们的互联网使用情况，并将任何未来未知的高带宽流量归类为可疑流量。这种个性化分类可以在互联网用户切换到新的VPN提供商时识别并阻止之前未识别的服务，从而可能暴露新的VPN，不仅牵连到已识别的互联网用户，还牵连到该服务的所有其他用户。

无法识别的高带宽流量也可能导致阻塞：

[第 25 页](#)

即使 TSG 无法识别与用户活动相关的具体应用程序或服务，它也能将任何异常的大流量标记为可疑流量。识别后，系统可以配置为在预定时间（例如 24 小时）后阻止标记的流量。这种方法与 GFW 的观察结果相符，据观察，GFW 会在一段时间后阻止任何高带宽加密流量，即使它无法识别流量的具体性质<sup>9</sup>。

该报告（[第63页](#)）讨论了Tor网桥、[Snowflake](#)和[WebTunnel](#)。报告指出，Geedge拥有一种枚举Tor网桥的方法，但目前尚不确定是内部开发还是外包。Cyber Narrator的一张[广告截图中](#)包含字符串“Snowflake”。泄露的文件包含MESA学生对WebTunnel的研究，尽管当时他们还没有发现任何阻断技术。

Geedge 拥有一款专门用于枚举赛风终端的工具，名为 Psiphon3-SLOK。该工具与 Geedge 在 2024 年 5 月进入缅甸时观察到的赛风连接变化相关。

[第 64 页](#)

根据泄露的数据，Geedge Networks 似乎试图通过开发一种称为 Psiphon3-SLOK 的内部工具来规避这一保护措施。

在与赛风团队的沟通中，我们了解到，2024年5月下旬，来自缅甸的用户数量急剧上升，并且客户选择服务器的方式也发生了变化，这与赛风的服务器枚举和定向屏蔽措施相一致。这一时期恰逢缅甸部署 Geedge 系统。

## 远程访问客户网络

TSG Galaxy 中存储的客户数据可供 MESA(!) 的学生和研究人员访问，并可用于研究。

[第 21 页](#)

这项研究的一个重要发现是，TSG Galaxy 在政府客户所在地收集的所有互联网用户数据似乎都可以被 Geedge Networks 的员工访问。数据还表明，真实客户数据的快照有时会与中国科学院的学术实验室 Mesalab 共享，该实验室似乎与 Geedge Networks 关系密切。数据表明，Mesalab 的工程专业学生利用真实客户信息进行研究，旨在更好地理解并阻止规避互联网审查的行为。

[第 24 页](#)

此外，Geedge Networks 的员工似乎能够在办公室内创建 Wi-Fi 网络，将任何设备远程连接到客户网络。此功能使他们能够验证阻止机制在实际场景中是否有效运行。

## 部署至中国境外的国家

该报告详细概述了 Geedge 在哈萨克斯坦、埃塞俄比亚、巴基斯坦和缅甸的部署情况。有关巴基斯坦和缅甸的更多详细信息，请参阅 [《控制的阴影》](#) 和 [《监视丝绸之路》](#)。

部署 Geedge 设备需要 Geedge 工作人员亲自前往安装地点的 ISP，并与 ISP 人员直接沟通。（顺便说一句，这一事实也揭露了[缅甸 Frontiir](#)等 ISP 的丑闻，他们在被问及 Geedge 问题时撒了谎。（[第 53 页](#)）

[第 35 页](#)

在新的国家或省份部署时，Geedge 员工将前往客户所在地，在政府和当地 ISP 的场地安装硬件。当地 ISP 是 Geedge 系统部署不可或缺的一部分。ISP 需要允许 Geedge 员工在安装期间访问其场地，并提供网络规划，说明如何将 Geedge 硬件集成到 ISP 的现有系统中。用于收集和存储海量数据的 Geedge 硬件位于每个 ISP 的数据中心内。

在泄露的文件中，各国均以代号标识。除A24外，所有代号均与特定国家/地区相关。大多数情况下，代号由国家/地区名称的首字母加上两位数年份组成（年份显然并不总是与首次部署年份一致）。

## 哈萨克斯坦 (代号K18、K24)

Geedge 成立于 2018 年。泄密事件表明，哈萨克斯坦政府是其第一个客户，从 2019 年开始。该报告将 Geedge 的部署与政府对全国范围内 TLS MITM 的愿望联系起来，例如我们在[#6](#)、[#56](#)和[#339](#)中看到的那样。

### 第 42 页

Geedge 的产品 Tianguou Secure Gateway (TSG) 能够实施类似于政府颁发的根证书的攻击，<sup>26</sup>这可能是 Geedge 最初与哈萨克斯坦政府接洽的卖点。

一张日期为 2020 年 10 月 16 日的图片列出了运行三个独立 Geedge 产品的国家中心和其他 17 个城市的 IP 地址：Bifang (中央管理)、Galaxy (TSG-Galaxy 的原名) 和 Nezha (Network Zodiac 的旧名)。27 Geedge 的一份不完整的网络规划文件从 2020 年 9 月开始记录与哈萨克斯坦国家中心相关的事件。该日志收集了截至 2022 年 10 月的事件，并包含一个表格，列出了项目的修订，包括日期、版本号、所做的更改以及负责每次更新的作者。

## 埃塞俄比亚 (代号E21)

Geedge 于 2021 年开始在埃塞俄比亚工作。

本节提到了[郑超 \(Zheng Chao\)](#)的名字：

### 第 45 页

2022 年 12 月的日志条目显示，Geedge 首席技术官郑超批准了位于亚的斯亚贝巴的两个 Safaricom 区域数据中心的工作。

我们之前提到过，TSG 可以在镜像模式或串联模式下运行。该报告声称，将系统从镜像模式切换到串联模式可能会导致系统关机，并将其与[2023 年 2 月的社交媒体封锁事件](#)联系起来。

### 第 46 页

Geedge 的修订日志表明，从镜像模式切换到串联模式与政府准备关闭互联网之间存在关联。<sup>42</sup>例如，从镜像配置转换为串联配置可能预示着互联网即将关闭，因为广义上讲，镜像模式更适合监控，而串联模式更适合互联网关闭。日志显示，埃塞俄比亚总共有 18 次切换到串联模式，其中两次是在 2023 年 2 月互联网关闭之前在 Safaricom 数据中心进行的。

## 巴基斯坦 (代号P19)

Geedge 于 2023 年在巴基斯坦成立，同年 Sandvine 退出了巴基斯坦。在[《控制的阴影》](#)报告中，国际特赦组织将 Geedge 运营的防火墙称为“WMS 2.0”（网络管理/监控系统 2.0），以区别于其取代的早期版本的 WMS。

[Geedge 在巴基斯坦的存在与此前有关中国参与国家防火墙的报道](#)相符。巴基斯坦官员的言论与 Geedge 的 TSG 的已知能力相符：

### 第 48 页

巴基斯坦一位高级互联网服务提供商 (ISP) 高管在接受半岛电视台采访时使用的措辞与 Geedge 的营销材料非常相似。<sup>51</sup>[这位](#)未透露姓名的高管表示，新的 WMS 不仅部署在该国的互联网网关，还部署在移动服务提供商和 ISP 的本地数据中心。<sup>52</sup>由于之前的系统只能监控进出巴基斯坦的内容，巴基斯坦无法审查由 Netflix 和 Meta 运营的本地缓存内容分发网络 (CDN) 托管的内容。这位高管比较了 WMS 1.0 和 WMS 2.0，表示：“与 Sandvine 系统不同，新的基于深度数据包检测 (DPI) 的系统现在能够监控本地互联网流量”，使用“内联网络”，而这种网络也更有可能会降低用户的网速。这位高管还指出，中国（Geedge）的技术能够以“精细的级别”管理应用程序和网站，其功能比 Sandvine 更强大。

Geedge 的 Sanity Directory 能够将网络活动归因于特定的 SIM 卡。在巴基斯坦，SIM 卡又与真实身份相关联：

### 第 49 页

自2015年以来，每张新发给该国移动用户的SIM卡都必须注册到特定用户，并与通过国家数据库和注册管理局（NADRA）注册的指纹等生物识别信息关联。人们需要NADRA的个人资料才能访问医疗保健、银行和教育等基本服务。NADRA的个人资料还链接到其他数据库，例如选民登记和税务记录，这些数据库结合起来构成了每位公民的全面记录。<sup>[57]</sup> (<https://www.amnesty.org/en/documents/asa33/0206/2025/en/>) Geedge 的“健康目录”组件的核心功能之一是将流量归因于特定的SIM卡。

## 缅甸 (代号M22)

[缅甸之所以意义重大，是因为当“缅甸正义”组织报道了](#)Geedge 的事迹时，这是 Geedge 在外国的工作首次被公众所知。

除了之前报道过的[Frontiir](#)之外，此次泄密还提及了缅甸所有 ISP 的数据中心。此前，当被问及时，Frontiir 曾错误地否认其开展过任何监控项目。

[第 53 页](#)

规划文件列出了缅甸境内所有国有和私营互联网服务提供商 (ISP) 的数据中心。其中不仅列出了“四大”互联网服务提供商 MyTel、Ooredoo、MPT 和 ATOM，还列出了 Frontiir、Global Technology Group、Golden TMH Telecom、Stream Net、IM-Net、缅甸宽带电信、缅甸电信网络公共有限公司、Campana 和中国联通等一些规模较小的服务提供商。

该文件还包含所有 ISP 的连接测试报告。这些报告提供了 2024 年全年不同日期进行的网站连接测试信息。测试的目的似乎是为了评估每个 ISP 网络审查的有效性。

Frontiir 的一位发言人否认其网络上“构建、规划或设计任何与监控相关的设备”。然而，泄露的文件显示，缅甸所有互联网服务提供商 (包括 Frontiir) 的建筑物内都安装了 Geedge 硬件。

以下是缅甸政府想要封锁的应用程序和 VPN 列表的信息：

[第 54 页](#)

泄露的文件还包含有关屏蔽 VPN、Tor (尤其是基于 Tor 的移动应用 Orbot) 和 Psiphon 的详细信息。缅甸希望屏蔽的 VPN 列表比埃塞俄比亚或哈萨克斯坦等其他一些附庸国提供的 VPN 列表更长。这些文件还记录了屏蔽“高优先级应用”规则的制定情况，其中涵盖了 55 款需要屏蔽的应用，其中包括即时通讯应用 Signal 和 WhatsApp。

## 代号 A24

Geedge 的一位客户代号仅为 A24。泄密事件发生时，双方的业务关系似乎尚处于初期阶段。

[第 55 页](#)

虽然泄露的文件包含与本报告提到的客户国家相关的具体地点和/或互联网服务提供商，但与 A24 相关的数据并不包含任何能够识别客户的指标。关于 A24 客户身份的唯一线索是首字母 A 和年份 2024。

除此之外，信息表明，在泄密事件发生时，A24 和 Geedge 的合作关系似乎还处于早期阶段。该合作关系涉及两次 Geedge 设备的概念验证部署，一次采用镜像模式，另一次采用串联模式，以便向客户明确这两种模式之间的区别。

## 中国的区域防火墙

报告显示，Geedge 参与了中国地区、省级防火墙，尤其是新疆的防火墙。

[第9页](#)

除了与国际政府客户合作外，这项研究还提供了证据，表明中国正在兴起一种省级防火墙模式，以补充国家防火墙。Geedge Networks 正在与中国多个地方政府合作构建省级防火墙，各地区的审查规则可能有所不同。InterSecLab 已在新疆、福建和江苏等地确定了中国省级防火墙项目。

## 新疆 (代号 J24)

[新疆](#)的代号是 J24。泄露的文件直接指出，新疆的区域防火墙将成为中国在全国部署的样板。

[第 56 页](#)

泄露的文件包含 2024 年 6 月 22 日中国科学院新疆分中心 (简称“新疆分中心”) 一次演讲的笔记。这些笔记很可能是由 Geedge 的一名员工记录的，记录显示，Geedge 的项目“旨在将新疆分中心打造成为反恐先锋力量，尤其是在反规避方面”。71 笔记中提到，“国家 (防火墙) 正在从集中式模式向分布式模式演变”，新疆分中心的目標是“成为省级 (防火墙) 建设的典范，可供其他地区复制或借鉴”。

与大多数其他 Geedge 部署一样，新疆的部署也采用中央指挥中心与“运营商”数据中心相连的结构。

[第 57 页](#)

与早期项目相比，J24 规模更大，不再通过最终用户互联网服务提供商 (ISP) 进行运营。相反，它采用了与 Geedge 为外国客户开展的其他业务领域类似的架构，即由一个“国家中心” (在新疆，Geedge 将其称为中央指挥中心) 负责监督分布式区域中心 (Geedge 称之为运营商中心)。在 J24 项目中，这些运营商中心位于中国电信、中国移动、中国宽带网络和中国联通的数据设施内。与所谓的国家中心一样，中央指挥中心可以远程管理部署在运营商站点的监控设备。根据一份文件，这些 ISP 设施内共有 17 个运营商中心。

新疆部署的要求表明了严密而侵入性的监视，这与我们所了解的该省的压迫情况一致。

第 57 页

在题为《CBNR-J24 需求组织》的文件中，Geedge 概述了其在新疆部署 Cyber Narrator 所需的一系列功能。Geedge Networks 的目标是将用户互联网行为、生活方式和人际关系的汇总和分析功能融入 Cyber Narrator。他们还希望添加根据目标用户交流对象构建关系图谱的功能，并根据用户使用的应用程序或访问的网站对用户进行分组。

未来发展的要求还提到增加检查哪些用户连接到特定移动基站的能力，以便支持通过这些站进行位置三角测量，并检测何时大量人群聚集在特定区域。

此外，该项目还计划添加创建地理围栏的功能，当特定人员进入指定区域时触发警报。此外，该项目还重点关注查询历史位置数据以追踪其过去的行踪。Geedge 的目标是能够标记那些频繁更换 SIM 卡、拨打国际号码或使用规避审查工具和外国社交媒体应用程序的个人。

J24 项目还包含针对特定群体的功能。这些功能可以在地图上显示受监控群体的地理分布，并检测群体成员在特定地点的异常聚集。这使得运营商能够追踪和预测大规模抗议和示威活动的形成。

福建、江苏等省

有一些关于格奇在福建和江苏省工作的记录，但与其他地区相比较少。

第 58 页

文件显示，Geedge Networks 于 2022 年开始在台湾沿海的福建省开展类似的省级防火墙试点项目。然而，与其他部署相比，有关该项目的信息有限。在泄露的文件中，该试点项目没有代号，简称为“福建项目”。

第 59 页

一些文件还提到了中国东部沿海省份江苏的一个项目。Geedge 与当地政府江苏省公安厅 (JPSB) 合作的明确动机是打击网络诈骗。通讯显示，JPSB 不愿允许 Geedge 创建大数据集群，而是希望 Geedge 在现有基础设施上部署其工具。一个名为“江苏南京”的初始测试环境于 2023 年 2 月投入运营，而“江苏反诈骗项目”似乎已于 2024 年 3 月 15 日投入生产模式。



工作岗位 4天前

成员 作者

据我所知，泄漏的实际内容尚未公开。

[Enlace Hacktivista](#) 的内容看起来像是这样的。

- <https://enlacehacktivista.org/geedge.torrent> (BitTorrent)
- <https://files.enlacehacktivista.org/geedge/> (直接 HTTPS 下载)

总共，这些文件的大小约为 600 GB。其中 500 GB 在一个文件 mirror/repo.tar 中。

```
7206346 mirror/filelist.txt
497103482880 mirror/repo.tar
14811058515 geedge_docs.tar.zst
2724387262 geedge_jira.tar.zst
35024722703 mesalab_docs.tar.zst
63792097732 mesalab_git.tar.zst
71382 A HAMSON-EN.docx
16982 A Hamson.docx
161765 BRI.docx
14052 CPEC.docx
2068705 CTF-AWD.docx
19288 Schedule.docx
26536 TSG Solution Review Description-20230208.docx
704281 TSG-问题.docx
35040 chat.docx
27242 ty-Schedule.docx
111244 待学习整理-23年MOTC-SWG合同草本V.1-2020230320.docx
52049 打印.docx
418620 替票证明.docx
260551 领导修改版-待看Reponse to Customer's Suggestions-2022110-V001--1647350669.docx
```



[mesalab\\_git.tar.zst](#)文件大小为 64 GB, 似乎包含 Geedge/MESA 源代码库, 包括 Git 提交历史记录。目前为止, 所有报告均未深入研究过该源代码, 因此仍有许多内容需要研究和学习。

mesalab\_git.tar.zst 中的文件是[Git 包](#)。你可以像从 SSH 或 HTTPS URL 克隆一样从包中克隆。以下是示例:

```
$ tar -xvf mesalab_git.tar.zst -- ./MESA_Platform/http.bundle
./MESA_Platform/http.bundle

# If your version of tar doesn't support .tar.zst files, you may need to do something like:
# zstd -dc mesalab_git.tar.zst | tar -xvf - -- ./MESA_Platform/http.bundle

$ git bundle list-heads MESA_Platform/http.bundle
fedf3431b3a1e29ee3d27d130e9651b7f73b79aa refs/heads/Fix-TSG-16812
30fc2e796a1ed0eb6f5cd47bd8ccb1dcf40225b1 refs/heads/develop
0ddf0cd934dd0ad9ec742790e6aeb4980bcdb64e refs/heads/master
b0df6e0c2846300ac15673a19fc10ce5fd409153 refs/heads/obsolete-docanalyze-use-zlib
3fb34e8bbfc561cbf8b6e8af1e8835b8974f6ef1 refs/tags/v2.0.0
e8f12eeef500b246ce3fade3cb886e3cd7cbc2b9 refs/tags/v2.0.1
[...]

$ git clone MESA_Platform/http.bundle MESA_Platform/http
Cloning into 'MESA_Platform/http'...
Receiving objects: 100% (531/531), 2.55 MiB | 45.03 MiB/s, done.
Resolving deltas: 100% (290/290), done.

$ cd MESA_Platform/http

MESA_Platform/http$ ls
autorelease.sh
autorevision.sh
bin
ci
cmake
CMakeLists.txt
readme.md
src
test

MESA_Platform/http$ git branch -a
* master
remotes/origin/Fix-TSG-16812
remotes/origin/HEAD -> origin/master
remotes/origin/develop
remotes/origin/master
remotes/origin/obsolete-docanalyze-use-zlib

MESA_Platform/http$ git log
commit 0ddf0cd934dd0ad9ec742790e6aeb4980bcdb64e (HEAD -> master, origin/master, origin/HEAD)
Author: 李佳 <lijia@geedgenetworks.com>
Date: Wed Mar 20 08:21:06 2024 +0000

    Add unit test

commit 0571d0bc63c240d4c0adccaa40869a76cfe6013b (tag: v2.0.20)
Author: 刘学利 <liuxueli@geedgenetworks.com>
Date: Thu Mar 7 05:30:32 2024 +0000

    OMPUB-1170: Bugfix memory leak

commit b8f494c571d412e748d7cb832ae7e94c41ac8b5b (tag: v2.0.19)
Author: liuxueli <liuxueli@geedgenetworks.com>
Date: Wed Mar 6 16:49:07 2024 +0800

    OMPUB-1170: Bugfix memory leak

commit 328131dcc4cb95e399fce8947507cf2a92cf1b76 (tag: v2.0.18)
Author: liuxueli <liuxueli@geedgenetworks.com>
Date: Wed Jan 24 10:29:15 2024 +0800

    Feature: HTTP unzip content is consistent with the packet life cycle

commit e78749d810f9c261cab54ec56fa35e17f18a757a (tag: v2.0.17)
Author: 杨威 <yangwei@geedgenetworks.com>
Date: Tue Sep 19 08:49:03 2023 +0000
```

```
Update ci/travis.sh
[...]
```

可以在 geedge\_jira.tar.zst 中查找诸如“OMPUB-1170”之类的问题编号：

```
$ tar -O -xf geedge_jira.tar.zst -- ./issues/OMPUB-1170.json | jq .fields.summary
"【WMS-UTR项目】多台tsgx出现tsg_os_container_restart告警"
```

以下是 mesalab\_git.tar.zst 的内容列表：

#### ▼ mesalab\_git.tar.zst 的文件列表

```
-rw-r--r-- 0/0      4207469 2015-10-20 20:00 ./AV/digest_detection.bundle
-rw-r--r-- 0/0      328996 2015-10-20 20:00 ./AV/frag_monitor.bundle
-rw-r--r-- 0/0     12651137 2015-10-20 20:00 ./AV/frag_rssb.bundle
-rw-r--r-- 0/0       2685 2015-10-20 20:00 ./Alpha_lib/hello_ci_world.bundle
-rw-r--r-- 0/0     35115933 2015-10-20 20:00 ./BaiyangLi/ConfSummary.bundle
-rw-r--r-- 0/0     76346747 2015-10-20 20:00 ./BaiyangLi/IPLocator.bundle
-rw-r--r-- 0/0      113901 2015-10-20 20:00 ./EnderByEndera/commddetection.bundle
-rw-r--r-- 0/0     3799294 2015-10-20 20:00 ./EnderByEndera/realtime_protection.bundle
-rw-r--r-- 0/0     65667560 2015-10-20 20:00 ./Grityu/model_duplication.bundle
-rw-r--r-- 0/0     327308894 2015-10-20 20:00 ./IPReuse/Deploy_Env.bundle
-rw-r--r-- 0/0      5709341 2015-10-20 20:00 ./IPReuse/IPReuse_docs.bundle
-rw-r--r-- 0/0      311380 2015-10-20 20:00 ./IPReuse/code.bundle
-rw-r--r-- 0/0      257797 2015-10-20 20:00 ./IPReuse/mctrl.bundle
-rw-r--r-- 0/0     73383725 2015-10-20 20:00 ./IPReuse/mgw.bundle
-rw-r--r-- 0/0     72748028 2015-10-20 20:00 ./IPReuse/mr1.bundle
-rw-r--r-- 0/0      137343 2015-10-20 20:00 ./IPReuse/udpecho.bundle
-rw-r--r-- 0/0     154208 2015-10-20 20:00 ./IPReuse/vpn_access.bundle
-rw-r--r-- 0/0     35378805 2015-10-20 20:00 ./IPReuse/vpn_cgi.bundle
-rw-r--r-- 0/0     135686611 2015-10-20 20:00 ./IPReuse/vpn_install.bundle
-rw-r--r-- 0/0      12937 2015-10-20 20:00 ./Jiangshan/miniodemo.bundle
-rw-r--r-- 0/0     143427105 2015-10-20 20:00 ./K18_NTCS_WEB/NTC.bundle
-rw-r--r-- 0/0     140691229 2015-10-20 20:00 ./K18_NTCS_WEB/argus-ntc.bundle
-rw-r--r-- 0/0     87926696 2015-10-20 20:00 ./K18_NTCS_WEB/argus-service.bundle
-rw-r--r-- 0/0     111924888 2015-10-20 20:00 ./K18_NTCS_WEB/nfs.bundle
-rw-r--r-- 0/0      12263 2015-10-20 20:00 ./LiFulian/quic-block.bundle
-rw-r--r-- 0/0     378999132 2015-10-20 20:00 ./MESA_Platform/build-env.bundle
-rw-r--r-- 0/0     2477189 2015-10-20 20:00 ./MESA_Platform/dns.bundle
-rw-r--r-- 0/0     40606892 2015-10-20 20:00 ./MESA_Platform/gquic.bundle
-rw-r--r-- 0/0     2675883 2015-10-20 20:00 ./MESA_Platform/http.bundle
-rw-r--r-- 0/0     70446451 2015-10-20 20:00 ./MESA_Platform/marsio.bundle
-rw-r--r-- 0/0     62987183 2015-10-20 20:00 ./MESA_Platform/quic.bundle
-rw-r--r-- 0/0     87835695 2015-10-20 20:00 ./MESA_Platform/sapp.bundle
-rw-r--r-- 0/0     17847926 2015-10-20 20:00 ./MESA_Platform/ssl.bundle
-rw-r--r-- 0/0     721068 2015-10-20 20:00 ./MESA_framework/MESA_handle_logger.bundle
-rw-r--r-- 0/0     982245 2015-10-20 20:00 ./MESA_framework/mesa_jump_layer.bundle
-rw-r--r-- 0/0     270734598 2015-10-20 20:00 ./Minato/coredns_dnsovertor.bundle
-rw-r--r-- 0/0     29031093 2015-10-20 20:00 ./OreoPang/piratedvideowebsite.bundle
-rw-r--r-- 0/0      102213 2015-10-20 20:00 ./PanGu/DeployEnv.bundle
-rw-r--r-- 0/0     178830465 2015-10-20 20:00 ./PanGu/ObjectScanner.bundle
-rw-r--r-- 0/0     23756034 2015-10-20 20:00 ./PanGu/PanGu_docs.bundle
-rw-r--r-- 0/0      27624 2015-10-20 20:00 ./PanGu/mesa_plug.bundle
-rw-r--r-- 0/0      27947 2015-10-20 20:00 ./PanGu/ntc_app_plug.bundle
-rw-r--r-- 0/0      61017 2015-10-20 20:00 ./PanGu/ntc_http_collect.bundle
-rw-r--r-- 0/0      55818 2015-10-20 20:00 ./PanGu/ntc_ip_comm.bundle
-rw-r--r-- 0/0      35879 2015-10-20 20:00 ./PanGu/ntc_radius_plug.bundle
-rw-r--r-- 0/0      47807 2015-10-20 20:00 ./PanGu/ntc_ssl_collect.bundle
-rw-r--r-- 0/0     2015164 2015-10-20 20:00 ./PanGu/pangu_valve.bundle
-rw-r--r-- 0/0     385476900 2015-10-20 20:00 ./PanGu/t2httpcontentsscanner.bundle
-rw-r--r-- 0/0     207877454 2015-10-20 20:00 ./ZhangJianlong/galaxy-auto-deploy-cluster.bundle
-rw-r--r-- 0/0     23449095 2015-10-20 20:00 ./active-defense/houyi-deploy.bundle
-rw-r--r-- 0/0      11577 2015-10-20 20:00 ./appsketch-works/app-test-fork.bundle
-rw-r--r-- 0/0     1040030 2015-10-20 20:00 ./appsketch-works/app-test-log.bundle
-rw-r--r-- 0/0     413372 2015-10-20 20:00 ./appsketch-works/app-test.bundle
-rw-r--r-- 0/0      4356 2015-10-20 20:00 ./appsketch-works/app-tiktok.bundle
-rw-r--r-- 0/0      3001 2015-10-20 20:00 ./appsketch-works/asw-build.bundle
-rw-r--r-- 0/0     1934710 2015-10-20 20:00 ./appsketch-works/asw-controller.bundle
-rw-r--r-- 0/0     11992128 2015-10-20 20:00 ./appsketch-works/asw-gui.bundle
-rw-r--r-- 0/0      44996 2015-10-20 20:00 ./appsketch-works/asw-runner.bundle
-rw-r--r-- 0/0     5656069 2015-10-20 20:00 ./appsketch-works/device-api.bundle
-rw-r--r-- 0/0      9931 2015-10-20 20:00 ./appsketch-works/pcap-comment.bundle
-rw-r--r-- 0/0      13036 2015-10-20 20:00 ./appsketch-works/pcap-decode.bundle
```

-rw-r--r--	0/0	3002	2015-10-20	20:00	./appskech-works/webshark.bundle
-rw-r--r--	0/0	9955	2015-10-20	20:00	./chaoc/demo-fqdn-sampling-statistics.bundle
-rw-r--r--	0/0	42606	2015-10-20	20:00	./chaoc/easy-stream-application.bundle
-rw-r--r--	0/0	2768	2015-10-20	20:00	./chaoc/flink-networks.bundle
-rw-r--r--	0/0	2982	2015-10-20	20:00	./chaoc/ipfix-decoder.bundle
-rw-r--r--	0/0	6530	2015-10-20	20:00	./chaoc/test-json-serialization.bundle
-rw-r--r--	0/0	11467997	2015-10-20	20:00	./chenguanlin/chenguanlin_thesis.bundle
-rw-r--r--	0/0	511935	2015-10-20	20:00	./chenguanlin/gie_server.bundle
-rw-r--r--	0/0	61454	2015-10-20	20:00	./chenguanlin/td_evaluation.bundle
-rw-r--r--	0/0	7449973	2015-10-20	20:00	./chengyifei/e2tc.bundle
-rw-r--r--	0/0	975394	2015-10-20	20:00	./chengyifei/yy_strategy_adjust.bundle
-rw-r--r--	0/0	74098809	2015-10-20	20:00	./chongming/traffic_replay.bundle
-rw-r--r--	0/0	451553507	2015-10-20	20:00	./chongming/tsg_test.bundle
-rw-r--r--	0/0	1845474	2015-10-20	20:00	./common_tools/tcp_burst.bundle
-rw-r--r--	0/0	3094911	2015-10-20	20:00	./common_tools/tcpdump_mesa.bundle
-rw-r--r--	0/0	782567	2015-10-20	20:00	./cuiyiming/MESA_flexible_logger.bundle
-rw-r--r--	0/0	50633508	2015-10-20	20:00	./cuiyiming/MESA_summer_training_2018.bundle
-rw-r--r--	0/0	11585235	2015-10-20	20:00	./cuiyiming/feature_extract_plugin.bundle
-rw-r--r--	0/0	98720797	2015-10-20	20:00	./cuiyiming/gradproj.bundle
-rw-r--r--	0/0	537134	2015-10-20	20:00	./cuiyiming/luasapp.bundle
-rw-r--r--	0/0	67442278	2015-10-20	20:00	./current2023/evasion-detect.bundle
-rw-r--r--	0/0	577001	2015-10-20	20:00	./current2023/evasion-test.bundle
-rw-r--r--	0/0	63790410	2015-10-20	20:00	./current2023/ui.bundle
-rw-r--r--	0/0	2814073	2015-10-20	20:00	./cyber-narrator/cn-reporter-template.bundle
-rw-r--r--	0/0	329535336	2015-10-20	20:00	./cyber-narrator/cn-ui.bundle
-rw-r--r--	0/0	105716721	2015-10-20	20:00	./cyber-narrator/cn-web.bundle
-rw-r--r--	0/0	90878	2015-10-20	20:00	./cyber-narrator/license-admin-api.bundle
-rw-r--r--	0/0	20475871	2015-10-20	20:00	./cyber_narrator/flink-stream-schedule-platform.bundle
-rw-r--r--	0/0	253115154	2015-10-20	20:00	./daxiaoxu/xmr_bsexpr1.bundle
-rw-r--r--	0/0	36058713	2015-10-20	20:00	./daxiaoxu/xmr_bsexpr2.bundle
-rw-r--r--	0/0	273248	2015-10-20	20:00	./daxiaoxu/xmr_bsexpr3.bundle
-rw-r--r--	0/0	20341272	2015-10-20	20:00	./dengzeyi/sequenceshield.bundle
-rw-r--r--	0/0	197136681	2015-10-20	20:00	./docs/logo.bundle
-rw-r--r--	0/0	2302685	2015-10-20	20:00	./docs/regulations.bundle
-rw-r--r--	0/0	20929	2015-10-20	20:00	./dongxiaoyan/autotest_tsg.bundle
-rw-r--r--	0/0	24816	2015-10-20	20:00	./dongxiaoyan/gap_nezha_ui.bundle
-rw-r--r--	0/0	2119602854	2015-10-20	20:00	./dongxiaoyan/gap_tsg_api.bundle
-rw-r--r--	0/0	17935172	2015-10-20	20:00	./dongxiaoyan/gap_tsg_ui.bundle
-rw-r--r--	0/0	72823586	2015-10-20	20:00	./dongxiaoyan/tsg_autotest.bundle
-rw-r--r--	0/0	31808452	2015-10-20	20:00	./doris/doris_dispatch.bundle
-rw-r--r--	0/0	34751183	2015-10-20	20:00	./durain/durain_doc.bundle
-rw-r--r--	0/0	7738	2015-10-20	20:00	./fumingwei/sapp_test.bundle
-rw-r--r--	0/0	5547	2015-10-20	20:00	./fumingwei/tsg-containerd.bundle
-rw-r--r--	0/0	462355	2015-10-20	20:00	./galaxy/K18/galaxy-push-service-.bundle
-rw-r--r--	0/0	87975634	2015-10-20	20:00	./galaxy/K18/galaxy-service.bundle
-rw-r--r--	0/0	8647477	2015-10-20	20:00	./galaxy/deployment/ansible-deploy-hub.bundle
-rw-r--r--	0/0	1094698678	2015-10-20	20:00	./galaxy/deployment/bmj-deploy.bundle
-rw-r--r--	0/0	171577701	2015-10-20	20:00	./galaxy/deployment/k8s.bundle
-rw-r--r--	0/0	604858552	2015-10-20	20:00	./galaxy/deployment/online-config.bundle
-rw-r--r--	0/0	71534	2015-10-20	20:00	./galaxy/deployment/schema-updater-tool.bundle
-rw-r--r--	0/0	20412815	2015-10-20	20:00	./galaxy/deployment/tsg-olap-data-initialization.bundle
-rw-r--r--	0/0	112623299	2015-10-20	20:00	./galaxy/deployment/updata-record.bundle
-rw-r--r--	0/0	752206562	2015-10-20	20:00	./galaxy/galaxy-integration.bundle
-rw-r--r--	0/0	45259	2015-10-20	20:00	./galaxy/galaxy-offline-service.bundle
-rw-r--r--	0/0	9801	2015-10-20	20:00	./galaxy/platform/algorithm/business-rules-engine.bundle
-rw-r--r--	0/0	181614	2015-10-20	20:00	./galaxy/platform/algorithm/druid-extensions.bundle
-rw-r--r--	0/0	60133	2015-10-20	20:00	./galaxy/platform/algorithm/sketches.bundle
-rw-r--r--	0/0	54347	2015-10-20	20:00	./galaxy/platform/algorithm/snowflake.bundle
-rw-r--r--	0/0	48233213	2015-10-20	20:00	./galaxy/platform/galaxy-data-platform.bundle
-rw-r--r--	0/0	14226827	2015-10-20	20:00	./galaxy/platform/galaxy-job.bundle
-rw-r--r--	0/0	78198	2015-10-20	20:00	./galaxy/platform/galaxy-navigation.bundle
-rw-r--r--	0/0	292910130	2015-10-20	20:00	./galaxy/platform/galaxy-qgw-service.bundle
-rw-r--r--	0/0	459089	2015-10-20	20:00	./galaxy/platform/galaxy-report-service.bundle
-rw-r--r--	0/0	23389965	2015-10-20	20:00	./galaxy/platform/galaxy-tool.bundle
-rw-r--r--	0/0	129670055	2015-10-20	20:00	./galaxy/platform/galaxy-troubleshooting-api.bundle
-rw-r--r--	0/0	112490	2015-10-20	20:00	./galaxy/platform/galaxy-ua-parser.bundle
-rw-r--r--	0/0	39278379	2015-10-20	20:00	./galaxy/platform/groot-stream.bundle
-rw-r--r--	0/0	18874351	2015-10-20	20:00	./galaxy/platform/tsg-olap-troubleshooting.bundle
-rw-r--r--	0/0	39380	2015-10-20	20:00	./galaxy/tsg_olap/app-protocol-stat-traffic-agent.bundle
-rw-r--r--	0/0	98603	2015-10-20	20:00	./galaxy/tsg_olap/app-protocol-stat-traffic-merge.bundle
-rw-r--r--	0/0	15104	2015-10-20	20:00	./galaxy/tsg_olap/app_recommend.bundle
-rw-r--r--	0/0	513146684	2015-10-20	20:00	./galaxy/tsg_olap/dll-multipoint-aggregation.bundle
-rw-r--r--	0/0	285852	2015-10-20	20:00	./galaxy/tsg_olap/dos-detection-job.bundle
-rw-r--r--	0/0	138912	2015-10-20	20:00	./galaxy/tsg_olap/file-chunk-combiner.bundle
-rw-r--r--	0/0	59922	2015-10-20	20:00	./galaxy/tsg_olap/flume/dynamic_complement.bundle
-rw-r--r--	0/0	17393	2015-10-20	20:00	./galaxy/tsg_olap/flume/flume-interceptor.bundle

-rw-r--r--	0/0	10247	2015-10-20	20:00	./galaxy/tsg_olap/flume/interceptor/flume-http-avro-gtpc.bundle
-rw-r--r--	0/0	48244586	2015-10-20	20:00	./galaxy/tsg_olap/generate-baseline.bundle
-rw-r--r--	0/0	349266	2015-10-20	20:00	./galaxy/tsg_olap/log-completion-schema.bundle
-rw-r--r--	0/0	68212	2015-10-20	20:00	./galaxy/tsg_olap/log-olap-analysis-schema.bundle
-rw-r--r--	0/0	71301876	2015-10-20	20:00	./galaxy/tsg_olap/log-stream-doublewrite.bundle
-rw-r--r--	0/0	65574	2015-10-20	20:00	./galaxy/tsg_olap/log-stream-voip-relation.bundle
-rw-r--r--	0/0	46514	2015-10-20	20:00	./galaxy/tsg_olap/p19-file-sync-service.bundle
-rw-r--r--	0/0	38345	2015-10-20	20:00	./galaxy/tsg_olap/radius-account-knowledge.bundle
-rw-r--r--	0/0	41161	2015-10-20	20:00	./galaxy/tsg_olap/radius-relationship-hbase.bundle
-rw-r--r--	0/0	27033	2015-10-20	20:00	./galaxy/tsg_olap/relationship-gtpc-user.bundle
-rw-r--r--	0/0	13858166	2015-10-20	20:00	./galaxy/tsg_olap/sip-rtp-correlation.bundle
-rw-r--r--	0/0	33151	2015-10-20	20:00	./galaxy/tsg_olap/storm/log-address-hbase.bundle
-rw-r--r--	0/0	60982	2015-10-20	20:00	./galaxy/tsg_olap/storm/log-stream-aggregation.bundle
-rw-r--r--	0/0	229667	2015-10-20	20:00	./galaxy/tsg_olap/storm/log-stream-completion.bundle
-rw-r--r--	0/0	18753	2015-10-20	20:00	./galaxy/tsg_olap/storm/log-stream-connections.bundle
-rw-r--r--	0/0	45986	2015-10-20	20:00	./galaxy/tsg_olap/storm/log-stream-topn.bundle
-rw-r--r--	0/0	20493	2015-10-20	20:00	./galaxy/tsg_olap/storm/log-subscriber-hbase-datacenter.bundle
-rw-r--r--	0/0	14294	2015-10-20	20:00	./galaxy/tsg_olap/storm/radius-account-knowledge.bundle
-rw-r--r--	0/0	44738	2015-10-20	20:00	./galaxy/tsg_olap/storm/storm-olap-aggregation.bundle
-rw-r--r--	0/0	61138	2015-10-20	20:00	./galaxy/tsg_olap/storm-dos-detection.bundle
-rw-r--r--	0/0	92311	2015-10-20	20:00	./galaxy/tsg_olap/topn-metrics.bundle
-rw-r--r--	0/0	10468	2015-10-20	20:00	./galaxy/tsg_olap/tsg-complement.bundle
-rw-r--r--	0/0	45468	2015-10-20	20:00	./galaxy/tsg_olap/tsg_galaxy_producer-v3.0.20191115.bundle
-rw-r--r--	0/0	399303565	2015-10-20	20:00	./galaxy/tsg_olap/xj-log-etl.bundle
-rw-r--r--	0/0	13852974	2015-10-20	20:00	./gregory/yydns_vue.bundle
-rw-r--r--	0/0	1861380	2015-10-20	20:00	./handingkang/alias_prefix.bundle
-rw-r--r--	0/0	39925	2015-10-20	20:00	./handingkang/dnsdbdesign.bundle
-rw-r--r--	0/0	33554	2015-10-20	20:00	./handingkang/fakedns6-v2.bundle
-rw-r--r--	0/0	11439062	2015-10-20	20:00	./handingkang/fakedns6.bundle
-rw-r--r--	0/0	6861369	2015-10-20	20:00	./handingkang/ohmybs.bundle
-rw-r--r--	0/0	1034429	2015-10-20	20:00	./handingkang/ohmydns.bundle
-rw-r--r--	0/0	2071234	2015-10-20	20:00	./handingkang/ohmydns2.bundle
-rw-r--r--	0/0	32456	2015-10-20	20:00	./handingkang/ohmyserver.bundle
-rw-r--r--	0/0	76711356	2015-10-20	20:00	./handingkang/ohmyweb.bundle
-rw-r--r--	0/0	3699580	2015-10-20	20:00	./handingkang/ohxmap.bundle
-rw-r--r--	0/0	13479	2015-10-20	20:00	./handingkang/prober.bundle
-rw-r--r--	0/0	322134378	2015-10-20	20:00	./handingkang/yserver.bundle
-rw-r--r--	0/0	26145078	2015-10-20	20:00	./handingkang/yydns.bundle
-rw-r--r--	0/0	589422	2015-10-20	20:00	./handingkang/yserver.bundle
-rw-r--r--	0/0	8390	2015-10-20	20:00	./hcy/190823-bcs.bundle
-rw-r--r--	0/0	109357451	2015-10-20	20:00	./hcy/ConfSummary.bundle
-rw-r--r--	0/0	8296361	2015-10-20	20:00	./hcy/TechSummary.bundle
-rw-r--r--	0/0	4589	2015-10-20	20:00	./hewenliang/https-measure.bundle
-rw-r--r--	0/0	51451703	2015-10-20	20:00	./hezhenjie/heatao_techsum.bundle
-rw-r--r--	0/0	370591	2015-10-20	20:00	./hezhenjie/videoportalddetection.bundle
-rw-r--r--	0/0	167087379	2015-10-20	20:00	./intelligence-learning-engine/vpn-finder-plugins.bundle
-rw-r--r--	0/0	1544434	2015-10-20	20:00	./jiangpenghui/openlookeng_poc.bundle
-rw-r--r--	0/0	21308	2015-10-20	20:00	./jiangpenghui/qq_file_send.bundle
-rw-r--r--	0/0	100116	2015-10-20	20:00	./jiangping/bloomfilter.bundle
-rw-r--r--	0/0	30081661	2015-10-20	20:00	./jiangping/msflow.bundle
-rw-r--r--	0/0	14298	2015-10-20	20:00	./jiangping/supervlan.bundle
-rw-r--r--	0/0	23084	2015-10-20	20:00	./l1453/ddos_classify.bundle
-rw-r--r--	0/0	99875	2015-10-20	20:00	./l1453/ddos_detect.bundle
-rw-r--r--	0/0	14220555	2015-10-20	20:00	./l1453/ddos_openworld.bundle
-rw-r--r--	0/0	80780	2015-10-20	20:00	./lijia/tsg_oam.bundle
-rw-r--r--	0/0	133847587	2015-10-20	20:00	./liliqing/appdiscover.bundle
-rw-r--r--	0/0	13817098	2015-10-20	20:00	./linxin/coredump-tools.bundle
-rw-r--r--	0/0	13118	2015-10-20	20:00	./linxin/deviceplugindemo.bundle
-rw-r--r--	0/0	37161	2015-10-20	20:00	./linxin/webhookdemo.bundle
-rw-r--r--	0/0	10528	2015-10-20	20:00	./lirenjie/conferencesummary.bundle
-rw-r--r--	0/0	46300	2015-10-20	20:00	./lirenjie/lrj_vxlan.bundle
-rw-r--r--	0/0	17033246	2015-10-20	20:00	./little_stone/fingerprint.bundle
-rw-r--r--	0/0	6180	2015-10-20	20:00	./little_stone/mzy_logapi.bundle
-rw-r--r--	0/0	5363638	2015-10-20	20:00	./little_stone/webcomponent.bundle
-rw-r--r--	0/0	5205	2015-10-20	20:00	./little_stone/webhopper.bundle
-rw-r--r--	0/0	8500759	2015-10-20	20:00	./liuchang/mesa_sts.bundle
-rw-r--r--	0/0	25485145	2015-10-20	20:00	./liuchang/pkt_seq_matcher.bundle
-rw-r--r--	0/0	906652	2015-10-20	20:00	./liujunpeng/Minio.bundle
-rw-r--r--	0/0	109544	2015-10-20	20:00	./liujunpeng/hiredisMESA.bundle
-rw-r--r--	0/0	3503690	2015-10-20	20:00	./liujunpeng/redis.bundle
-rw-r--r--	0/0	2712102	2015-10-20	20:00	./liujunpeng/redis_cluster_install.bundle
-rw-r--r--	0/0	64326024	2015-10-20	20:00	./liuwentan/maat-rust-binding.bundle
-rw-r--r--	0/0	1571688	2015-10-20	20:00	./liuxueli/install-standalone-redis.bundle
-rw-r--r--	0/0	11941	2015-10-20	20:00	./liuyang/inline_device.bundle
-rw-r--r--	0/0	550233	2015-10-20	20:00	./liuyu/bbq.bundle
-rw-r--r--	0/0	17676428	2015-10-20	20:00	./lixinyan/diamondv.bundle



-rw-r--r--	0/0	444434	2015-10-20	20:00	./lixinyan/email-mapping-system.bundle
-rw-r--r--	0/0	673946709	2015-10-20	20:00	./lixinyan/email-spoofing-detection.bundle
-rw-r--r--	0/0	519288	2015-10-20	20:00	./liyubing/p4exercise.bundle
-rw-r--r--	0/0	18550	2015-10-20	20:00	./luwenpeng/certificate.bundle
-rw-r--r--	0/0	10212	2015-10-20	20:00	./luwenpeng/mini-rust-runtime.bundle
-rw-r--r--	0/0	42564	2015-10-20	20:00	./luwenpeng/rust_dpi.bundle
-rw-r--r--	0/0	2652	2015-10-20	20:00	./luwenpeng/stellar.bundle
-rw-r--r--	0/0	11315049	2015-10-20	20:00	./lyf/sdprojects.bundle
-rw-r--r--	0/0	124337	2015-10-20	20:00	./maxiaoqing/Task.bundle
-rw-r--r--	0/0	4276	2015-10-20	20:00	./maxiaoqing/av_container_identify.bundle
-rw-r--r--	0/0	3826	2015-10-20	20:00	./modikai/cache_prober.bundle
-rw-r--r--	0/0	3005	2015-10-20	20:00	./modikai/diamondv.bundle
-rw-r--r--	0/0	11128383	2015-10-20	20:00	./modikai/dtool.bundle
-rw-r--r--	0/0	7760296	2015-10-20	20:00	./modikai/echodns.bundle
-rw-r--r--	0/0	12353268	2015-10-20	20:00	./modikai/edns_svcb_https.bundle
-rw-r--r--	0/0	3213	2015-10-20	20:00	./modikai/fpdns_client.bundle
-rw-r--r--	0/0	17026560	2015-10-20	20:00	./modikai/fpdns_server.bundle
-rw-r--r--	0/0	2967	2015-10-20	20:00	./modikai/gfw_test.bundle
-rw-r--r--	0/0	3763183	2015-10-20	20:00	./modikai/rogue_ns.bundle
-rw-r--r--	0/0	373732	2015-10-20	20:00	./nezha/demo_exporter.bundle
-rw-r--r--	0/0	477962	2015-10-20	20:00	./nezha/doc.bundle
-rw-r--r--	0/0	656754042	2015-10-20	20:00	./nezha/nezha-fronted.bundle
-rw-r--r--	0/0	282419	2015-10-20	20:00	./nezha/nz-agent.bundle
-rw-r--r--	0/0	676286894	2015-10-20	20:00	./nezha/nz-build-env.bundle
-rw-r--r--	0/0	1917895965	2015-10-20	20:00	./nezha/nz-build.bundle
-rw-r--r--	0/0	220847	2015-10-20	20:00	./nezha/nz-confagent.bundle
-rw-r--r--	0/0	112281	2015-10-20	20:00	./nezha/nz-talon.bundle
-rw-r--r--	0/0	198376	2015-10-20	20:00	./nezha/nz-transfer.bundle
-rw-r--r--	0/0	255494757	2015-10-20	20:00	./nezha/nz-web.bundle
-rw-r--r--	0/0	27087	2015-10-20	20:00	./nezha/olp_exporter.bundle
-rw-r--r--	0/0	3117	2015-10-20	20:00	./nezha/playbook.bundle
-rw-r--r--	0/0	2361771	2015-10-20	20:00	./niubinghui/luapluginmanage.bundle
-rw-r--r--	0/0	10028665	2015-10-20	20:00	./nms/nmsclient.bundle
-rw-r--r--	0/0	197966742	2015-10-20	20:00	./nms/nmsdoc.bundle
-rw-r--r--	0/0	27883477	2015-10-20	20:00	./nms/nmsserver.bundle
-rw-r--r--	0/0	8363468	2015-10-20	20:00	./nms/nmssync.bundle
-rw-r--r--	0/0	126962650	2015-10-20	20:00	./nms/nmsweb.bundle
-rw-r--r--	0/0	14818848	2015-10-20	20:00	./nms/oam.bundle
-rw-r--r--	0/0	496590238	2015-10-20	20:00	./operation-and-maintenance/ansible-playbook-test.bundle
-rw-r--r--	0/0	35887814	2015-10-20	20:00	./public_resources/benchmark_pcap.bundle
-rw-r--r--	0/0	2817638	2015-10-20	20:00	./public_resources/sapp_doc.bundle
-rw-r--r--	0/0	400094528	2015-10-20	20:00	./pxz/hos_client_cpp_module.bundle
-rw-r--r--	0/0	10917030	2015-10-20	20:00	./pxz/tsg_lua_module.bundle
-rw-r--r--	0/0	2807384	2015-10-20	20:00	./pzx/tensor-k18.bundle
-rw-r--r--	0/0	2015950430	2015-10-20	20:00	./qiuyuqi/diamondv.bundle
-rw-r--r--	0/0	3336	2015-10-20	20:00	./qiuyuqi/dnsdbdesign.bundle
-rw-r--r--	0/0	1742555	2015-10-20	20:00	./renkaige/redis_cluster_install.bundle
-rw-r--r--	0/0	81944539	2015-10-20	20:00	./shihao Yue/yy_deploy_script.bundle
-rw-r--r--	0/0	787555	2015-10-20	20:00	./shihao Yue/yy_llm.bundle
-rw-r--r--	0/0	3722058858	2015-10-20	20:00	./solutions/tsg-scripts.bundle
-rw-r--r--	0/0	3549540	2015-10-20	20:00	./stellar/dns_decoder.bundle
-rw-r--r--	0/0	8963689	2015-10-20	20:00	./stellar/ftp_decoder.bundle
-rw-r--r--	0/0	7628725	2015-10-20	20:00	./stellar/http_decoder.bundle
-rw-r--r--	0/0	51131296	2015-10-20	20:00	./stellar/quic_decoder.bundle
-rw-r--r--	0/0	16048393	2015-10-20	20:00	./stellar/ssl_decoder.bundle
-rw-r--r--	0/0	1809615	2015-10-20	20:00	./stellar/stellar-2022.bundle
-rw-r--r--	0/0	6633	2015-10-20	20:00	./stellar/stellar-dev-env.bundle
-rw-r--r--	0/0	20173431	2015-10-20	20:00	./stellar/stellar-on-sapp.bundle
-rw-r--r--	0/0	1325020	2015-10-20	20:00	./stellar/stellar-rs.bundle
-rw-r--r--	0/0	412346940	2015-10-20	20:00	./stellar/stellar.bundle
-rw-r--r--	0/0	31414004	2015-10-20	20:00	./swarmkv/swarmkv.bundle
-rw-r--r--	0/0	1191714242	2015-10-20	20:00	./tango/9140_hardware.bundle
-rw-r--r--	0/0	3119108	2015-10-20	20:00	./tango/FieldStat.bundle
-rw-r--r--	0/0	67384197	2015-10-20	20:00	./tango/adc_hardware.bundle
-rw-r--r--	0/0	42345465	2015-10-20	20:00	./tango/certstore.bundle
-rw-r--r--	0/0	45218	2015-10-20	20:00	./tango/fw_dns_plug.bundle
-rw-r--r--	0/0	2064796	2015-10-20	20:00	./tango/kni.bundle
-rw-r--r--	0/0	575063419	2015-10-20	20:00	./tango/maat.bundle
-rw-r--r--	0/0	7476395	2015-10-20	20:00	./tango/performance-test-nginx-server.bundle
-rw-r--r--	0/0	54661319	2015-10-20	20:00	./tango/shaping-engine.bundle
-rw-r--r--	0/0	127261868	2015-10-20	20:00	./tango/tango_docs.bundle
-rw-r--r--	0/0	48146	2015-10-20	20:00	./tango/tfe-kmod.bundle
-rw-r--r--	0/0	123688869	2015-10-20	20:00	./tango/tfe.bundle
-rw-r--r--	0/0	3529484	2015-10-20	20:00	./tango/tsg-service-chaining-engine.bundle
-rw-r--r--	0/0	126030194	2015-10-20	20:00	./tango/tsg_container.bundle
-rw-r--r--	0/0	3119932	2015-10-20	20:00	./tango/tsg_master.bundle

-rw-r--r--	0/0	53297	2015-10-20	20:00	./tango/tsgx_hardware.bundle
-rw-r--r--	0/0	19774489	2015-10-20	20:00	./tango/verify-policy.bundle
-rw-r--r--	0/0	127099807	2015-10-20	20:00	./tongzongzhen/dpdk.bundle
-rw-r--r--	0/0	1430734	2015-10-20	20:00	./tongzongzhen/fuzzing-demo.bundle
-rw-r--r--	0/0	2517682	2015-10-20	20:00	./tsg/PacketAdapter.bundle
-rw-r--r--	0/0	357716047	2015-10-20	20:00	./tsg/cli-deploy.bundle
-rw-r--r--	0/0	3164954	2015-10-20	20:00	./tsg/dp_telemetry_app.bundle
-rw-r--r--	0/0	18743445	2015-10-20	20:00	./tsg/hasp-tools.bundle
-rw-r--r--	0/0	543888171	2015-10-20	20:00	./tsg/oam.bundle
-rw-r--r--	0/0	12197460753	2015-10-20	20:00	./tsg/tsg-deploy.bundle
-rw-r--r--	0/0	391812321	2015-10-20	20:00	./tsg/tsg-diagnose.bundle
-rw-r--r--	0/0	66615780	2015-10-20	20:00	./tsg/tsg-doc.bundle
-rw-r--r--	0/0	3734555897	2015-10-20	20:00	./tsg/tsg-os-buildimage.bundle
-rw-r--r--	0/0	792940795	2015-10-20	20:00	./tsg/tsg-os-onie.bundle
-rw-r--r--	0/0	1090920	2015-10-20	20:00	./tsg/tsg-performance-test-tools.bundle
-rw-r--r--	0/0	98299245	2015-10-20	20:00	./tsg/tsg-scripts-platform.bundle
-rw-r--r--	0/0	957	2015-10-20	20:00	./tsg/tsg_test.bundle
-rw-r--r--	0/0	71806569	2015-10-20	20:00	./tsg/wannat-ansible-deploy.bundle
-rw-r--r--	0/0	5737448	2015-10-20	20:00	./tsg-manual/tsg-admin-guide.bundle
-rw-r--r--	0/0	44449639	2015-10-20	20:00	./tsg-ui/demo.bundle
-rw-r--r--	0/0	346651	2015-10-20	20:00	./vendor/cJSON.bundle
-rw-r--r--	0/0	97743	2015-10-20	20:00	./vendor/hiredis.bundle
-rw-r--r--	0/0	4438486	2015-10-20	20:00	./vendor/pcrc.bundle
-rw-r--r--	0/0	4957429	2015-10-20	20:00	./vendor/rdkafka.bundle
-rw-r--r--	0/0	1936462	2015-10-20	20:00	./voip-analysis/sip-voip-completion.bundle
-rw-r--r--	0/0	6764	2015-10-20	20:00	./wangfengmei/ipreset.bundle
-rw-r--r--	0/0	365753	2015-10-20	20:00	./wanglihui/ip-learning-graph.bundle
-rw-r--r--	0/0	10032	2015-10-20	20:00	./wangmeiqi/2ch-tcn.bundle
-rw-r--r--	0/0	1539545583	2015-10-20	20:00	./wangmeiqi/datacollect_new.bundle
-rw-r--r--	0/0	13109224	2015-10-20	20:00	./wangmeiqi/datacollect_old.bundle
-rw-r--r--	0/0	14631800	2015-10-20	20:00	./wangmeiqi/hswfp.bundle
-rw-r--r--	0/0	29962588	2015-10-20	20:00	./wangmeiqi/obfs4_meek_snowflake.bundle
-rw-r--r--	0/0	502845	2015-10-20	20:00	./wangmeiqi/obfs4_verify.bundle
-rw-r--r--	0/0	3320	2015-10-20	20:00	./wangmeiqi/tf.bundle
-rw-r--r--	0/0	177907959	2015-10-20	20:00	./wangmeiqi/wfp_dataprocess.bundle
-rw-r--r--	0/0	49755	2015-10-20	20:00	./wangwei/cn-object-scheduler.bundle
-rw-r--r--	0/0	54928	2015-10-20	20:00	./wangwei/fj-transform-api.bundle
-rw-r--r--	0/0	70947	2015-10-20	20:00	./wangyan/singleflowaggregation.bundle
-rw-r--r--	0/0	71144202	2015-10-20	20:00	./wangyouzhan/comm_audit.bundle
-rw-r--r--	0/0	27686	2015-10-20	20:00	./wangyouzhan/dns_jt_audit.bundle
-rw-r--r--	0/0	25808	2015-10-20	20:00	./wangyouzhan/http_jt_audit.bundle
-rw-r--r--	0/0	120025	2015-10-20	20:00	./wangyouzhan/http_statistic_fs.bundle
-rw-r--r--	0/0	1957270	2015-10-20	20:00	./wangyu/imc_2017_2018.bundle
-rw-r--r--	0/0	6567673	2015-10-20	20:00	./web-sketch/webskt-query-agent.bundle
-rw-r--r--	0/0	10957193	2015-10-20	20:00	./wuhongwei/2021.bundle
-rw-r--r--	0/0	4228640	2015-10-20	20:00	./wujiating/censorship_detection.bundle
-rw-r--r--	0/0	3454	2015-10-20	20:00	./wujiating/cnirc-2nd.bundle
-rw-r--r--	0/0	168824543	2015-10-20	20:00	./wujiating/detection.bundle
-rw-r--r--	0/0	2016081791	2015-10-20	20:00	./wujiating/diamondv.bundle
-rw-r--r--	0/0	2929689391	2015-10-20	20:00	./wujiating/fingerprinting.bundle
-rw-r--r--	0/0	8398655	2015-10-20	20:00	./wujiating/google-2020.bundle
-rw-r--r--	0/0	1989947	2015-10-20	20:00	./wujiating/python-https.bundle
-rw-r--r--	0/0	189050	2015-10-20	20:00	./yangyongqiang/yyq_test.bundle
-rw-r--r--	0/0	263189	2015-10-20	20:00	./yangzhiqing/2w_web_tance.bundle
-rw-r--r--	0/0	524	2015-10-20	20:00	./yangzhiqing/demo1.bundle
-rw-r--r--	0/0	4332172	2015-10-20	20:00	./yangzhiqing/erqi_web_domain_zhili.bundle
-rw-r--r--	0/0	324329286	2015-10-20	20:00	./yangzhiqing/fwxzc_erqi.bundle
-rw-r--r--	0/0	101208939	2015-10-20	20:00	./yangzhiqing/lvtong.bundle
-rw-r--r--	0/0	3462203	2015-10-20	20:00	./yangzhiqing/xd-yicundu.bundle
-rw-r--r--	0/0	1138168	2015-10-20	20:00	./yinjiangyi/uaanalyser.bundle
-rw-r--r--	0/0	22410219	2015-10-20	20:00	./yinjiangyi/webskt-query-agent.bundle
-rw-r--r--	0/0	40849	2015-10-20	20:00	./yulingjing/url_label_restiful.bundle
-rw-r--r--	0/0	18302	2015-10-20	20:00	./yzc/http_check.bundle
-rw-r--r--	0/0	6036	2015-10-20	20:00	./yzc/http_count.bundle
-rw-r--r--	0/0	4434	2015-10-20	20:00	./zengmeng/231031nxdomain.bundle
-rw-r--r--	0/0	6468	2015-10-20	20:00	./zengmeng/240825dnssecpool.bundle
-rw-r--r--	0/0	235417406	2015-10-20	20:00	./zhangchengwei/MinioRelated.bundle
-rw-r--r--	0/0	39301	2015-10-20	20:00	./zhangchengwei/qq_online_file.bundle
-rw-r--r--	0/0	126566	2015-10-20	20:00	./zhanghongqing/knowledge-log.bundle
-rw-r--r--	0/0	1908691184	2015-10-20	20:00	./zhangqingfeng/zhangqingfeng.bundle
-rw-r--r--	0/0	23569932	2015-10-20	20:00	./zhangshuai/ConfSummary.bundle
-rw-r--r--	0/0	17863599	2015-10-20	20:00	./zhangshuo1/domain-classification.bundle
-rw-r--r--	0/0	58497561	2015-10-20	20:00	./zhangyang/diagnose-tools.bundle
-rw-r--r--	0/0	9973	2015-10-20	20:00	./zhangyang/ffi_demo.bundle
-rw-r--r--	0/0	53049	2015-10-20	20:00	./zhangyang/fs4-demo.bundle
-rw-r--r--	0/0	17552172	2015-10-20	20:00	./zhangyang/libzt.bundle

```
-rw-r--r-- 0/0      10315184 2015-10-20 20:00 ./zhangyang/lwip.bundle
-rw-r--r-- 0/0      150396 2015-10-20 20:00 ./zhangyang/maat_demo.bundle
-rw-r--r-- 0/0      28115 2015-10-20 20:00 ./zhangyang/mini-rust-runtime.bundle
-rw-r--r-- 0/0     5350849 2015-10-20 20:00 ./zhangyang/monoio.bundle
-rw-r--r-- 0/0     379972664 2015-10-20 20:00 ./zhangyang/qemu-uintr.bundle
-rw-r--r-- 0/0      124183 2015-10-20 20:00 ./zhangyang/rs-timeout.bundle
-rw-r--r-- 0/0     9041463 2015-10-20 20:00 ./zhangyang/uintr-event.bundle
-rw-r--r-- 0/0    1728405298 2015-10-20 20:00 ./zhangyang/uintr-linux-kernel.bundle
-rw-r--r-- 0/0     626544 2015-10-20 20:00 ./zhangyang/variable_monitor.bundle
-rw-r--r-- 0/0     68814 2015-10-20 20:00 ./zhangyang/watch_monitor.bundle
-rw-r--r-- 0/0    159397818 2015-10-20 20:00 ./zhangyang/zerotierone.bundle
-rw-r--r-- 0/0    2884416271 2015-10-20 20:00 ./zhangzhihan/device-management-scripts.bundle
-rw-r--r-- 0/0     235091 2015-10-20 20:00 ./zhangzhihao/1a.bundle
-rw-r--r-- 0/0      7620 2015-10-20 20:00 ./zhangzhihao/ccproxy.bundle
-rw-r--r-- 0/0    384759422 2015-10-20 20:00 ./zhangzhihao/heavykeeper.bundle
-rw-r--r-- 0/0     29812 2015-10-20 20:00 ./zhangzhihao/rdma-example.bundle
-rw-r--r-- 0/0     122633 2015-10-20 20:00 ./zhangzhihao/softiwarp.bundle
-rw-r--r-- 0/0    20353792 2015-10-20 20:00 ./zhaokun/tsg_policy_api.bundle
-rw-r--r-- 0/0    269393524 2015-10-20 20:00 ./zhaokun/tsg_ui_script.bundle
-rw-r--r-- 0/0     31802 2015-10-20 20:00 ./zhaoyijun/nat_format.bundle
-rw-r--r-- 0/0     4181738 2015-10-20 20:00 ./zhaoyixiang/realtime_protection.bundle
-rw-r--r-- 0/0    149919112 2015-10-20 20:00 ./zhaoyixiang/scanner.bundle
-rw-r--r-- 0/0    261609623 2015-10-20 20:00 ./zhaoyixiang/ssl.bundle
-rw-r--r-- 0/0     2933151 2015-10-20 20:00 ./zhijinghua/dns-log-transforming.bundle
-rw-r--r-- 0/0     5015970 2015-10-20 20:00 ./zhijinghua/mesa-traffic-identification.bundle
-rw-r--r-- 0/0      26140 2015-10-20 20:00 ./zhijinghua/portscan-detection.bundle
-rw-r--r-- 0/0     3040539 2015-10-20 20:00 ./zhongyoub/nfv-conclusion.bundle
-rw-r--r-- 0/0    1250448169 2015-10-20 20:00 ./zhuyujia/diamondv.bundle
-rw-r--r-- 0/0     5363638 2015-10-20 20:00 ./zhuyujia/webcomponent.bundle
-rw-r--r-- 0/0    1608253521 2015-10-20 20:00 ./zhuyujia/webhopper.bundle
-rw-r--r-- 0/0     26145294 2015-10-20 20:00 ./zhuyujia/yydns.bundle
-rw-r--r-- 0/0    14394722 2015-10-20 20:00 ./zhuyujia/yydns_vue.bundle
-rw-r--r-- 0/0     701112 2015-10-20 20:00 ./zhuzhenjun/libosfp.bundle
-rw-r--r-- 0/0     38871 2015-10-20 20:00 ./zx_dataserker/field_splitter_complement.bundle
-rw-r--r-- 0/0     246412 2015-10-20 20:00 ./zx_dataserker/yb_flume_cus_sink_file.bundle
-rw-r--r-- 0/0    198711635 2015-10-20 20:00 ./zyq/time_series_anomaly_detection.bundle
```

根据对文件名的浏览，以下是一些我优先查看的存储库：

```
IPReuse/IPReuse_docs
IPReuse/vpn_access
IPReuse/vpn_install
MESA_Platform/dns
MESA_Platform/gquic
MESA_Platform/http
MESA_Platform/marsio
MESA_Platform/quic
MESA_Platform/sapp
MESA_Platform/ssl
active-defense/houyi-deploy
common_tools/tcp_burst
common_tools/tcpdump_mesa
cuiyiming/lua_sapp
cyber-narrator/cn-web
cyber-narrator/license-admin-api
docs/regulations
dongxiaoyan/gap_tsg_api
galaxy/deployment/k8s
galaxy/tsg_olap/dll-multipoint-aggregation
hezhengjie/videoportal-detection
intelligence-learning-engine/vpn-finder-plugins
liujunpeng/hiredisMESA
liuwentan/maat-rust-binding
nezha/nz-agent
solutions/tsg-scripts
stellar/dns_decoder
stellar/ftp_decoder
stellar/http_decoder
stellar/quic_decoder
stellar/ssl_decoder
stellar/stellar
tango/maat
tango/shaping-engine
```

```
tango/tfe
tsg-manual/tsg-admin-guide
tsg/tsg-deploy
tsg/tsg-doc
wangmeiqi/obfs4_meek_snowflake
wangmeiqi/obfs4_verify
zhangshuo1/domain-classification
zhijinghua/mesa-traffic-identification
```

如果有兴趣，也许我们可以组织团队来划分源代码库并进行研究。

-   **乌朱伊乌朱曼丹** 提到了这个 3天前
-  [江苏和河北的DNS劫持 UjuiUjuMandan/exhentai-igneous-generator#1](#)



工作岗位 前天

成员 作者

如果有兴趣，也许我们可以组织团队来划分源代码库并进行研究。

### 王美琪/obfs4\_verify

这看起来像是几个针对 obfs4 的初级主动探测器。它们获取网桥的 IP:port和网桥的带外“证书”信息（假定已知），并尝试与服务  
器握手，看看服务器是否像 obfs4 网桥那样响应。

6188	README.md	
121933	obfs4验证文档.docx	
2999	parse.go	
396970	pyelligator-master.zip	
12967	testverify.go	
7015	testverify.py	
7799	verify_obfs4.py	

obfs4验证文档.docx 是一份文档，解释了项目的目的，讲解了 obfs4 握手的步骤，并对 Go 代码进行了注释。

### obfs4节点验证文档

一、原理  
客户端与服务器使用Tor obfs4插件进行通信前，首先要建立握手。通过模拟obfs4客户端的握手行为向待验证的obfs4节点  
发送握手请求，如果能得到预期的响应，则验证目标节点为obfs4节点。

### Obfs4节点验证文档

客户端和服务端使用 Tor obfs4 插件进行通信之前，必须先建立握手。此过程模拟 obfs4 客户端的握手行为，并向需要验  
证的 obfs4 节点发送握手请求。如果收到预期的响应，则目标节点被验证为 obfs4 节点。

testverify.go 文件是探测器的 Go 版本。它主要包含从原始 obfs4proxy 源代码中  
的[transports/obfs4/obfs4.go](#)和[transports/obfs4/handshake\\_ntor.go](#)复制的代码，以及一个小的主函数，用于尝试与硬编码桥  
进行握手。

```
func main() {
    var ptName string
    ptName = "obfs4"
    var certStr string
    certStr = "iJ8il3a2gVXuNdZoaPwQ0Qgd0JyBAi4fcY642f6sTErVNZ14Ax7c9w9qa36mUXQhbm9v0g"
    // certStr = "M6tiPcFv8YK2jE8pYZb9AKMMHag4OrhHFwMOXHR+J9s8Ty9X9V+Bn0emEZmfnqhdHkdA"
    var iatStr string
    iatStr = "0"
    var address string
    address = "185.185.251.132:443"
    // address = "45.32.201.89:51433"
    var result int
    result = verify(ptName, certStr, address, iatStr)
    fmt.Println(result)
}
```



testverify.py 和 verify\_obfs4.py 看起来像是探测器 Python 版本中的两个不同版本。它可能是 Go 语言到 Python 的翻译，因为我无法识别它的实现。testverify.py 和 testverify.go 具有相同的两个桥接地址。verify\_obfs4.py 则有一个不同的地址：

```
if __name__ == '__main__':
    ptName = "obfs4"
    for i in range(10):
        item=bridgestr()
        item.certStr = "dCLdS35RUyZ/H93CQ7B1EdCF4Q0Cvw9+AmB116o6CU0ZGhm2TNDjwee9XYi/SVn9/gnKQ"
        item.address="104.168.126.106:42154"
        result = verify(ptName, item.certStr, item.address)
        print result
        i=i+1
```

我不知道这些是否是真正的 obfs4 网桥。

该代码库共有 7 次提交，均于 2024-06-28 由 提交 meiqi wang <wangmeiqi@iie.ac.cn> 。它看起来像是一个未更新或维护的测试项目。它硬编码了网桥 IP 地址和凭证，并且仅通过打印到标准输出来报告输出。代码看起来很业余，不像是一个可以运行的软件。

或许值得注意的是，这个存储库没有使用2024 年已知的任何[公钥区分攻击](#)，也没有表现出对它们的任何认识。

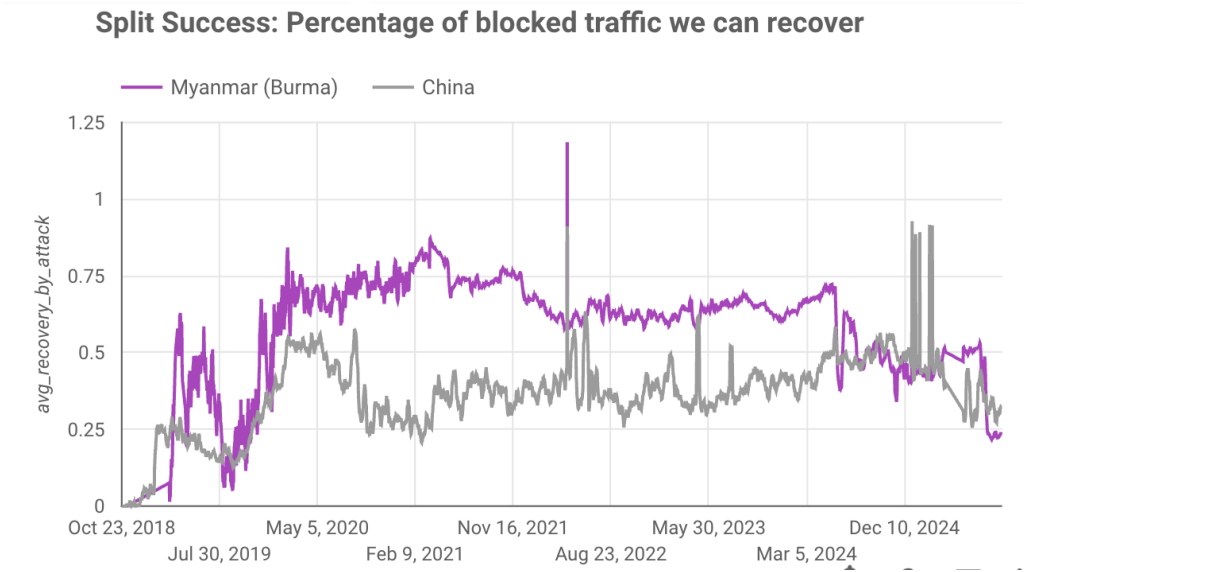


福图纳 前天 由fortuna编辑

[这是来自我们Intra 应用](#)的数据，显示了该应用从基于 SNI 的阻塞中恢复的成功程度。如果 Intra 在超时前未能收到响应，则会触发带有 TLS 记录碎片的 TLS 连接重试，我们会测量重试是失败还是成功（“我们可以恢复的流量”）。

缅甸的成功率在2024年5月之后显著下降，与中国的成功率持平。这与报告中提供的时间线一致。

（请注意，到 2025 年 8 月，这两个国家的增长率将进一步下降）



工作岗位 前天

成员 作者

缅甸的成功率在2024年5月之后显著下降，与中国的成功率持平。这与报告中提供的时间线一致。

有意思。谢谢你的关注。

我在 geedge\_jira.tar.zst 中没有看到对 Intra 的引用，但有一个问题引用了 Outline，issues/OSS-378.json。本期标题为【M22项目】VPN特征提取-宋龙坤（[Project M22]VPN特征提取-宋龙坤）。

2024-09-27 宋龙坤 (Song Longkun):

20240924对Orbot进行逆向分析, 解析有效域名1个, 除此之外未发现其他有效或有效特征;  
20240924对Ostrich VPN进行逆向分析, 解析有效域名2个, 除此之外未发现其他有效或有效特征;  
20240924对Outline VPN进行逆向分析, 解析有效域名2个, 除此之外未发现其他有效或有效特征;  
20240925对PandaVPN Lite进行逆向分析, 解析有效域名2个, 除此之外未发现其他有效或有效特征;  
20240925对Pawxy进行逆向分析, 解析有效域名5个, 疑似134个服务器IP, 除此之外未发现其他有效或有效特征;  
20240926对ProtonMail进行逆向分析, 解析有效域名4个, 除此之外未发现其他有效或有效特征;  
20240926对Proxy OvpnSpider进行逆向分析, 未发现有效或有效特征;  
PrivatePackets.io、Proxy.sh VPN官网无效, 应用商店未找到对应应用。

20240924 对 Orbot 的逆向分析发现了一个有效域名, 但未发现其他有效或有效的特征。20240924  
对 Ostrich VPN 的逆向分析发现了两个有效域名, 但未发现其他有效或有效的特征。20240924  
对 Outline VPN 的逆向分析发现了两个有效域名, 但未发现其他有效或有效的特征。20240925  
对 PandaVPN Lite 的逆向分析发现了两个有效域名, 但未发现其他有效或有效的特征。20240925  
对 Pawxy 的逆向分析发现了五个有效域名和 134 个疑似服务器 IP 地址, 但未发现其他有效或有效的特征。20240926  
对 ProtonMail 的逆向分析发现了四个有效域名, 但未发现其他有效或有效的特征。20240926  
对 Proxy OvpnSpider 的逆向分析未发现有效或有效的特征。  
PrivatePackets.io 和 Proxy.sh VPN 的官方网站已停止服务, 在应用商店中也未找到相应的应用程序。

2024年10月31日 宋龙坤 (Song Longkun):

20241030  
VPN序号137共提取Pawxy VPN服务器IP 144个, 目前在安卓模拟器平台中连续有效对VPN的所有节点拨测成功20次均无法正常连接, 爆发。VPN  
序号132 Outline VPN需要使用别人的Outline服务器私钥或自己的Outline服务器私钥创建才可使用。对VPN的官网及APK包进行分析, 未发现及疑似特征。VPN  
序号146编写代理OvpnSpider自动抓包程序, 并提取服务器IP 107个。

20241030  
编号137的VPN: 共提取了144个Pawxy VPN服务器IP地址。在安卓模拟器上连续20次调用该VPN的所有节点均失败, 成功阻止连接。  
编号132的VPN: Outline VPN需要使用第三方Outline服务器私钥或自定义私钥。对该VPN官网和APK包的分析未发现任何有效或可疑的特征。  
编号146的VPN: 开发了Proxy OvpnSpider自动抓包程序, 提取了107个服务器IP地址。



工作岗位 前天·由wkrp编辑

成员 作者

### wangmeiqi/obfs4\_meek\_snowflake

[该存储库看起来像是 meek、obfs4 和 Snowflake 的指纹识别器, 基于深度指纹识别方法 \(ACM CCS 2018\)。](#)

```
3726 ClosedWorld_DF_NoDef.py
6212 README.md
3080 environment.yml
256 readme
3556 test_meek.py
3563 test_obfs4.py
3582 test_snow.py
792 模型情况.txt
17454928 models/meek_bk.h5
17454928 models/obfs4_bk.h5
17454928 models/snow_bk.h5
```

README.md 只是一个自动生成的 GitLab README 文件。该文件包含使用说明:

1. 测试meek模型: python test\_meek.py ./data/meek\_mix.npz ./models/meek\_bk.h5
  2. 测试obfs4模型: python test\_obfs4.py ./data/obfs4\_mix.npz ./models/obfs4\_bk.h5
  3. 测试雪花模型: python test\_snow.py ./data/snow\_mix.npz ./models/snow\_bk.h5
- 
1. 测试 meek 模型: python test\_meek.py ./data/meek\_mix.npz ./models/meek\_bk.h5
  2. 测试 obfs4 模型: python test\_obfs4.py ./data/obfs4\_mix.npz ./models/obfs4\_bk.h5
  3. 测试雪花模型: python test\_snow.py ./data/snow\_mix.npz ./models/snow\_bk.h5

models/\*\_bk.h5 文件包含在仓库中，但 data/\*\_mix.npz 文件不包含在内。根据文件(1)，models/\*\_bk.h5 文件采用[分层数据格式](#)。文件 模型情况.txt (模型情况) 列出了每个模型的训练/测试细分：

三个模型结构：DF模型  
数据长度：前30个包

meek模型训练：3000个正例（文涛侧面的meek流） 30000个负例（崇儒侧面的背景tcp流）  
测试数据：2200个正例（新捕的meek流） 22096个负例（20000个崇儒侧面的tcp流，2000个obfs4流，96个雪花tcp流）  
  
obfs4模型 训练：20,000个正例（文涛obfs4流） 200,000个负例（崇儒背景tcp流）  
测试：20,000个正例（文涛obfs4流） 202,296个负例（200,000个崇儒背景tcp流，2200个meek流，96个雪花tcp流）  
  
雪花模型 训练：2000个正例（1000文涛snowflake流，1000新捕snowflake流） 20000个负例（崇儒背景udp流）  
测试：2000个正例（1000文涛snowflake流，1000新捕snowflake流） 20000个负例（崇儒背景udp流）

三种模型结构：DF模型  
数据长度：前30个数据包

Meek 模型训练：3000 个正例（来自 Wentao 的 Meek 流量），30000 个负例（来自 Chongru 的背景 TCP 流量）  
测试数据：2200 个正例（新捕获的 Meek 流量），22096 个负例（20000 个来自 Chongru 的背景 TCP 流量，2000 个 obfs4 流量，96 个雪花 TCP 流量）  
  
obfs4 模型训练：20,000 个正例（Wentao obfs4 流量），200,000 个负例（来自 Chongru 的背景 TCP 流量）  
测试数据：20,000 个正例（Wentao obfs4 流量），202,296 个负例（200,000 个来自 Chongru 的背景 TCP 流量，2,200 个 Meek 流量，96 个雪花 TCP 流量）  
  
雪花模型 训练：2000个正例（1000条文涛雪花流，1000条新捕获的雪花流） 20000个负例（重如背景UDP流）  
测试：2000个正例（1000条文涛雪花流，1000条新捕获的雪花流） 20000个负例（重如背景UDP流）

有趣的是，他们在测试过程中将来自其他传输协议的流量作为负样本的一部分（例如，obfs4 和 Snowflake 就是 meek 的负样本）。我不知道文涛（Wentao）、崇儒（Chongru）和新捕（Xinbu）是什么。（编辑：新捕 = [newly captured](#)。）

[ClosedWorld\\_DF\\_NoDef.py](#) 是[deep-fingerprinting/df](#)存储库中[同名文件](#)的编辑版本。

test\_meek.py、test\_obfs4.py 和 test\_snow.py 基本上是同一个文件，只是每个文件的传输名称不同。这些文件似乎源自 ClosedWorld\_DF\_NoDef.py。这些程序似乎将模型（.h5 文件）应用于测试数据（.npz 文件），并报告诸如准确率和召回率之类的统计数据。它们是 Python 2 程序，而不是 Python 3 程序。

[与wangmeiqi/obfs4\\_verify](#)类似，此仓库中的所有提交均由 wangmeiqi/obfs4\_verify 提交 meiqi wang <wangmeiqi@iie.ac.cn>，提交日期均为 2024-06-28。它看起来像是学生项目代码，而非实际可操作的代码。



福图纳 昨天

我在 geedge\_jira.tar.zst 中没有看到对 Intra 的引用，但有一个问题引用了 Outline，issues/OSS-378.json。本期标题为【M22项目】VPN特征提取-宋龙坤（[Project M22]VPN特征提取-宋龙坤）。

@wkrp谢谢你的关注。你知道“两个有效域名”是什么意思吗？  
至于Intra，我猜这次下架只是因为审查更加严格，而不是真的针对Intra。



乌朱伊乌朱曼丹 昨天:由UjuUjuMandan编辑

我不知道文涛、崇儒、新捕是什么。

第一个看起来像普通的中文名字，最后一个则是新捕获的。

- 王文涛: [https://en.wikipedia.org/wiki/Wang\\_Wentao](https://en.wikipedia.org/wiki/Wang_Wentao)
- 崇儒? 字面意思就是崇尚儒家。



工作岗位 昨天

成员 作者

你知道“两个有效域名”是什么意思吗？

我对 OSS-378 的最佳猜测是，它与“[移动设备实验室](#)”以及VPN 应用的“[静态和动态分析](#)”有关。比如，他们在二进制文件中搜索 URL 和 IP 地址，然后多次运行该程序，查看它发出了哪些 DNS 查询和网络连接。

OSS-378 包含一个指向 Confluence 文档的链接， <https://docs.geedge.net/display/TSGEN/M22-VPN+List> 该文档位于 geedge\_docs.tar.zst 中（以及许多其他标题中带有“M22”的页面）。“M22-VPN 列表”似乎包含一个包含约 280 个 VPN 的巨型列表，其中包括 Outline、Orbot、Mullvad 等。

Outline 在列表中排在第 132 位，其优先级很高。

序号 (数字)	优先级 (优先级)	是否提供特征 (可用特征)	VPN名称 (VPN 名称)	图标 (图标)	用户提供的链接 (用户提供的链接)	官网 (官方网站)	Android 包名 (Android 包名)
132	高 (高)		概要 VPN		<a href="https://getoutline.org/">https://getoutline.org/</a>	<a href="https://getoutline.org/">https://getoutline.org/</a>	



王x404 昨天

我不知道文涛、崇儒、新捕是什么。

第一个看起来像普通的中文名字，最后一个则是新捕获的。

- 王文涛: [https://en.wikipedia.org/wiki/Wang\\_Wentao](https://en.wikipedia.org/wiki/Wang_Wentao)
- 崇儒? 字面意思就是崇尚儒家。

他们都是中国名字。



琼恩·白雪公主 昨天·由JonSnowWhite编辑

我们 (@FelixLange1998我 (和我) 很想看看 ssl/tls 文件，但 torrent 下载和直接下载似乎都比较慢。有人成功下载了整套文件吗?





波尼·克莱尔·德卢恩 昨天

虽然审查基础设施能够利用恶意证书颁发机构 (CA) 进行中间人攻击 (MITM) 并不完全令人意外, 但像 Xray 这样的加密代理的图形客户端缺乏证书链哈希固定功能却相当令人担忧, 尤其是在运行加密代理客户端的设备可能被植入了恶意证书颁发机构, 而很少有人会费心去检查的情况下。在我看来, 图形客户端和可共享链接标准如果支持哈希固定功能, 将会受益匪浅。



乌朱伊乌朱曼丹 昨天

- <https://web.archive.org/web/20241202193445/http://www.mesalab.cn/> (含本科生照片)

因此, MESA 是 Massive Effective Stream Analysis 的缩写, 但中文名称与此完全无关, 而是处理架构组。

我怀疑这是在模仿 20 世纪 60 年代科罗拉多州的[梅萨实验室](#)。



RPRX 昨天 由 wkpr 编辑

虽然审查基础设施能够利用恶意证书颁发机构 (CA) 进行中间人攻击 (MITM) 并不完全令人意外, 但像 Xray 这样的加密代理的图形客户端缺乏证书链哈希固定功能却相当令人担忧, 尤其是在运行加密代理客户端的设备可能被植入了恶意证书颁发机构, 而很少有人会费心去检查的情况下。在我看来, 图形客户端和可共享链接标准如果支持哈希固定功能, 将会受益匪浅。

我也反对这件事, 不过对 Xray-core 来说似乎不太实用, 原因有三:

1. Xray 主推 [REALITY](#), 出现是“偷自己”, 完全不依赖 CA, 可以抵御证书链攻击, 就连认证也最重要加上了任选的抗量子, TLS 还没有
2. 如果使用 CDN, 则证书经常更换, 不同入口节点的证书可能都不同, pin 证书这个方式不太现实
3. Xray 正在商议在 CDN 等场景中使用 [VLESS 加密](#), 它遵循非常高的安全标准, 可以有效防止被解密/MITM 出被代理的数据

还有就是现在很多直连机场都在使用 REALITY 了, 越来越多的类似 TLS 的连接正在连接无法被 MITM [XTLS/Xray-core#5066 \(评论\)](#)

另外中转机场的 SS 有被解密后 MITM 内层 TLS 的风险, 这个安全漏洞就挺严重的, 我可以发一个帖子详细说明

我也考虑过这一点, 但对于 Xray-core 来说这似乎不切实际, 原因有三:

1. Xray 主要推广的是 [真实性](#)。即使在“窃取自身信息”的情况下, 它也完全绕过了对 CA 的依赖, 能够抵御证书链攻击, 并率先推出了可选的后量子身份验证, 但 TLS 尚未实现。
2. 如果使用 CDN, 证书会频繁更改, 并且不同的入口节点可能具有不同的证书, 这使得证书固定不切实际。
3. Xray 正在积极推广适用于 CDN 等场景的 [VLESS 加密](#)。它遵循极高的安全标准, 可有效防止针对代理数据的解密/中间人攻击。

此外, 许多直连 VPN 现在使用 REALITY, 使得类似 TLS 的连接越来越能抵抗 MITM 攻击: [XTLS/Xray-core#5066 \(评论\)](#)

此外, 像 Shadowsocks 这样的基于中继的 VPN 在解密后, 内部 TLS 层存在遭受中间人攻击的风险。这个安全漏洞相当严重——我可以在这里发布详细的解释。



RPRX 昨天 由 wkpr 编辑

如果使用 CDN, 则证书经常更换, 不同入口节点的证书可能都不同, pin 证书这个方式不太现实

可能 pin root 证书好一点, 我不确定 Xray 现有的 PinnedPeerCertificateChainSha256 PinnedPeerCertificatePublicKeySha256 是否支持

CDN 总归是建议使用 VLESS 加密的, 那么无所谓, 我觉得是时候把简单的 TLS / QUIC 也搞得“不够安全”了

如果使用 CDN，证书会频繁更改，并且不同的入口节点可能具有不同的证书，这使得证书固定不切实际。

固定根证书可能会更好，但我不确定 Xray 现有的 PinnedPeerCertificateChainSha256 和 PinnedPeerCertificatePublicKeySha256 是否支持这一点。

但是，使用 CDN 时，通常建议采用 VLESS 加密，所以这并不重要。我认为现在是时候将普通的 TLS/QUIC 归类为“不够安全”了。



波尼·克莱尔·德卢恩 昨天·由 PonyClairDeLune 编辑

也许固定根证书更好。我不确定 Xray 现有的 PinnedPeerCertificateChainSha256 和 PinnedPeerCertificatePublicKeySha256 是否支持它。

@RPRX 我的想法正是如此，只锁定可能的根证书。Cloudflare 有 LE、GTS、Sectigo 和 SSL.com，CloudFront 使用亚马逊的内部服务，Fastly 使用“Certainly”……等等。当需要与标准 Web 基础设施配对时，REALITY 并不完全适用，因此客户端最好使用根证书锁定，尤其是对于可共享的链接。

关于 VLESS 加密……我主张在需要第三方基础设施时使用它，但如果 TLS 一开始就能被审查者解密，那么我们会面临 Shadowsocks 等公司面临的困境。不过，像 CDN 这样的 Web 基础设施提供商可能不太在意。



RPRX 13小时前·由 wkpr 编辑

@PonyClairDeLunepin 这件事其实很难推动，我认为更根本的解决方案是不能继续将 TLS / QUIC 视为可靠的加密方式[#526](#)

然而，固定加密实际上相当难以实现。我认为更根本的解决方案是不再将 TLS/QUIC 视为可靠的加密方法[#526](#)



琪悦 12小时前

我不知道文涛、崇儒、新捕是什么。

第一个看起来像普通的中文名字，最后一个则是新捕获的。

- 王文涛: [https://en.wikipedia.org/wiki/Wang\\_Wentao](https://en.wikipedia.org/wiki/Wang_Wentao)
- 崇儒? 字面意思就是崇尚儒家。

不，你想太多了

他们实际上是普通话名字

🔗 RPRX 提到了这个 [12小时前](#)

- ⦿ TLS / QUIC 不应被继续视为可靠的加密方式，以及针对 Shadowsocks/TLS 中 TLS 的复合式 MITM，最后对于 VLESS Encryption 的介绍 / TLS/QUIC 不应再被视为可靠的加密方式，以及针对 Shadowsocks/TLS 中 TLS 的复合式 MITM 攻击。最后介绍一下 VLESS 加密。 #526



工作岗位 11小时前

成员 作者

因此，MESA 是 Massive Effective Stream Analysis 的缩写，但中文名称与此完全无关，而是处理架构组。

这是正确的。MESA（处理架构组）是[信息工程研究所](#)第二研究室的几个组之一。第二个实验室被称为[NERCIS，信息安全国家工程研究中心](#)（信息内容安全国家工程研究中心），但直到最近它才被称为 NELIST，信息安全技术国家工程实验室（信息内容安全技术国家工程实验室）。

[网上的帖子](#)列出了第二实验室的研究组（研究组）和课题组（课题组）：

- 信息检索研究组（信息检索研究组）
  - 社会计算课题组（社会计算课题组）
  - Web 挖掘课题组（Web 挖掘课题组）
  - 知识挖掘课题组（知识挖掘课题组）

- 内容计算课题组 (内容计算课题组)
- 前瞻技术课题组 (前瞻性技术课题组)
- 网络信息对抗课题组 (网络信息对抗课题组)
- 保密防护课题组 (保密保护专题组)
- Network安全课题组 (网络安全课题组)
- 数据管理课题组 (数据管理主题组)
- 处理架构组 (处理架构组, MESA)



乌朱伊乌朱曼丹 8小时前·由UjuiUjuMandan编辑

虽然审查基础设施能够利用恶意证书颁发机构 (CA) 进行中间人攻击 (MITM) 并不完全令人意外, 但像 Xray 这样的加密代理的图形客户端缺乏证书链哈希固定功能却相当令人担忧, 尤其是在运行加密代理客户端的设备可能被植入了恶意证书颁发机构, 而很少有人会费心去检查的情况下。在我看来, 图形客户端和可共享链接标准如果支持哈希固定功能, 将会受益匪浅。

我认为已安装的 CA 甚至不会被 Golang 或 Rust 可执行文件信任。即使是原生 Android 应用默认也不会信任用户存储中的 CA (如果开发者在网络安全配置中设置了此功能, Google Play 会对此提出异议) 。

对于 iOS, 它依赖于 TLS 库, Shadowrocket 似乎默认使用 OpenSSL 而不是系统的 SecureTransport, 因此也不受影响。



萨莫查 8小时前

mesalab\_docs.tar.zst 的“96711429\_attachments\_石逢钊-加密流量识别简述”这个文件 study/attachments 看起来挺有意思的。它似乎是GFW识别加密数据的技术基础 (这只是一份调查/概述, 而非设计规范) 。

它列出了以下内容作为技术参考:

- FS-Net: 用于加密流量分类的流序列网络
- 深度指纹识别: 利用深度学习破坏网站指纹识别防御
- 在移动消息应用中使用加密互联网流量进行服务使用分类

我发现的第一件有趣的事情是, 论文“FS-Net: 用于加密流量分类的流序列网络”利用**数据包长度和顺序**作为对加密流量进行分类的信息 (*FS-Net 明确将数据包长度序列作为输入, 并使用 bi-GRU/编码器-解码器对其序列进行建模*) 。

此模式与薛迪文在《利用封装的 TLS 握手对混淆代理流量进行指纹识别》一文中的发现相符, 该文通过加密后仍然可见的**数据包长度、时序和方向**模式来识别 TLS-over- TLS。虽然它们采用的分类方法不同, 但都以数据包大小和顺序作为关键特征。

我将继续深入研究这三篇论文, 看看它们是否与当前的 GFW 设计相符, 并在此分享我的想法 :)



RPRX 1小时前·由wkrp编辑

“识别特征接口”也不是新闻了, 多层加密这几乎没有帮助, 对于木马这样的深度学习可以识别 TLS 中的 TLS: [木马杀手](#)

更值得关注的是“网站/App指纹识别”, 这个要做到精准可用挺难的 (无SNI时), 根据GFW对ECH的态度, 可能进展不大, 这也涉及继ECH之后着力解决的下一个问题, 一个比较有意义的现实事件是“ChatGPT padding”, 不过它的前提也是针对了特定的 SNI

“识别时间模式”早已不是什么新鲜事了, 再加一层加密也几乎没什么好处。对于那些不需要深度学习就能检测TLS-in-TLS的木马病毒: [Trojan-killer](#)

更值得注意的是“网站/应用指纹识别”, 在没有 SNI 的情况下, 准确可靠地实施这项技术极具挑战性。鉴于 GFW 对 ECH 的立场, 这一进展可能有限。这是继 ECH 之后, 业界正在应对的下一个重大问题。一个相对重要的现实案例是“ChatGPT 填充”事件, 尽管它也针对的是特定的 SNI。



工作岗位 54分钟前

成员 作者

mesalab\_docs.tar.zst 的“96711429\_attachments\_石逢钊-加密流量识别简述”这个文件 study/attachments 看起来挺有意思的。它似乎是GFW识别加密数据的技术基础（这只是一份调查/概述，而非设计规范）。

@SaamoCha好发现！

[深度指纹识别](#)是mesalab\_git.tar.zst 中[wangmeiqi/obfs4\\_meek\\_snowflake](#)存储库的明显基础。

[FS-Net](#)是被引用次数最多的 MESA 出版物之一。（[ET-BERT](#)也是关于加密流量分类主题的出版物之一。）FS-Net 的作者都是 IIE 或 MESA 人员：

- 刘畅 (Liu Chang) [dblp](#)
- 贺龙涛 (He Longtao) [主页](#) [dblp](#)
- 熊刚 (Xiong Gang) [mesalab.cn 个人资料](#) [主页](#) [dblp](#)
- 曹自刚 (Cao Zigang) [dblp](#)
- 李镇 (Lizhen) [主页](#) [dblp](#)

熊刚可能是这些作者中最有名的一位。他甚至在中文维基百科上写了一篇文章，讲述他参与GFW的经历：<https://zh.wikipedia.org/wiki/熊刚>。

另一位 MESA 学生何正杰 (He Zhengjie) 有一个博客，其中几篇文章提到了 FS-Net 和其他加密流量分类研究：

- 2021-02-12 [流量识别概述](#)( [archive](#) ) [流量识别概述](#)
- 2020-10-18 [DataCon加密流量](#)参赛总结( [archive](#) ) [DataCon加密数据大赛总结](#)