FREEBUF

V 加新特性，查看各文件的相关性将更加容易

264人围观 ，发现 1 个不明物体 工具 网络安全

就 一个名叫Graph的新功能，该功能允许用户以可视化的方式查看自己所提交文件之间 相 用户可以轻松地查看到文件所连接到的主机信息，以及文件之间的相关性等等。更 要 给VirusTotal的高级智能平台用户，而且所有VirusTotal的用户都可以它。

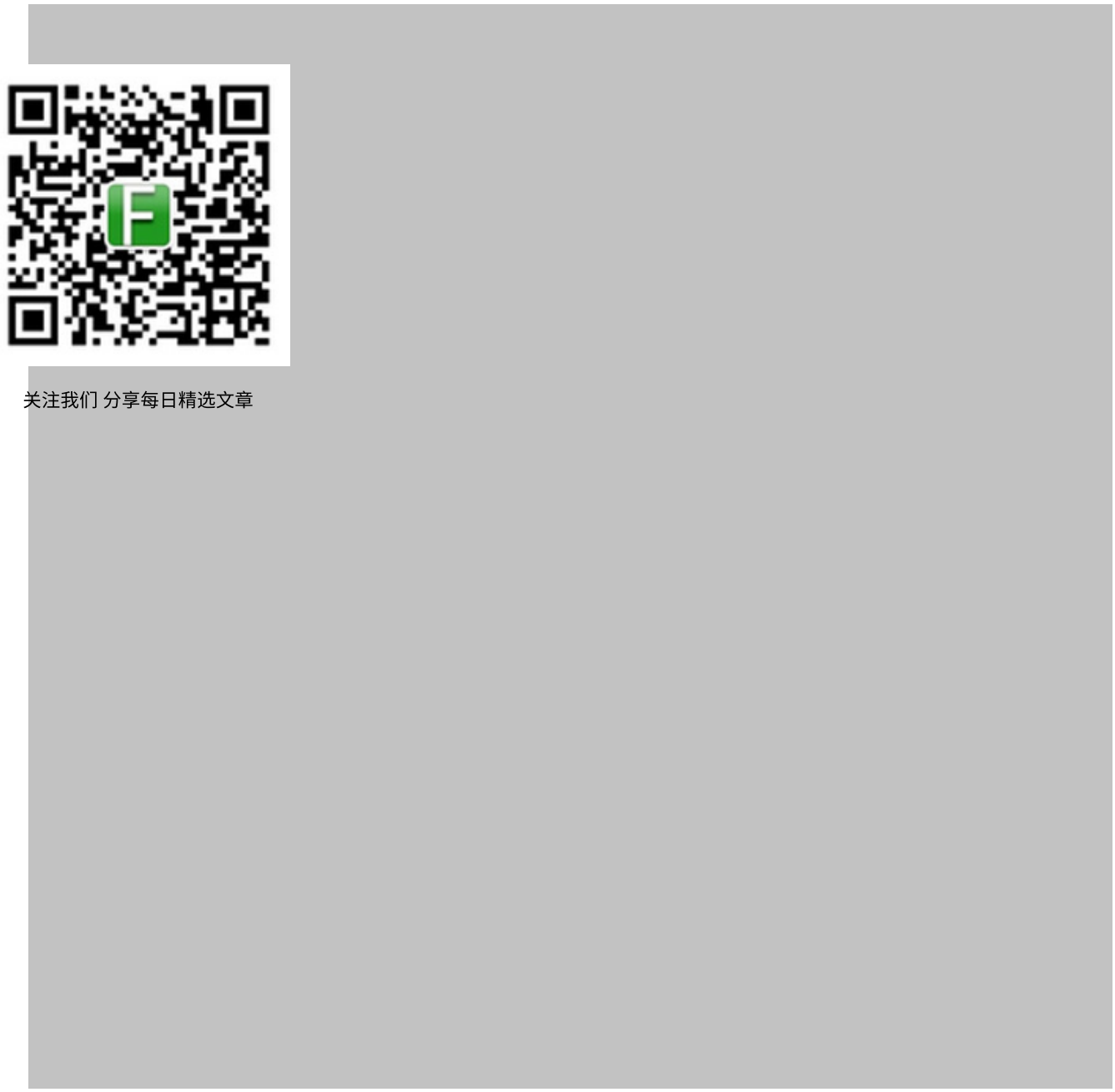
关注我们 分享每日精选文章

工具介绍

这款可视化工具基于VirusTotal的数据集实现，它可以查看到文件、URL地址、域名以及IP地址之间的关系，并且提 了非常方便的数据导航接口。

通过查看图表中的每一个节点，用户可以构建出一个数据网络来查看每一个样本之间的相关性。点击图中的节点后 你不仅可以看到每一个节点的所有相关文件或其他节点信息，你还可以添加标签或查看VirusTotal Public或VirusTota Intelligence的深度分析报告。

用户可以直接访问地址https://www.virustotal.com/graph/并提交已知哈希或进入分析页面提交特定服务来使用VirusTo Graph功能。在分析页面中的下拉菜单中，有一个名叫“Openin VirusTotal Graph”的新选项，点击了这个按钮之后你 入到Graph页面。



进入Graph页面后，你可以看到一个名叫“Root Node”的条目，点击之后你可以查看到各种箭头以及与样本文件相关的信息。接下来，我们一起看一看一份恶意软件样本的文件相关性（Graph）。

下图中包含了Root Node以及两个与样本相关的URL地址。

关注我们 分享每日精选文章

接下来，你可以双击每个节点来了解特定数据对象的详细信息。双击之后，工具会展开显示对象的相关性数据：

关注我们 分享每日精选文章

除此之外，你还可以双击下载下来的文件来寻找出特定文件的相关性信息，这样一来，你就可以更加深入了解样本件，并查看到所有的相关数据、文件、域名和URL地址等信息。

标记对象并保存自定义Graph

除了查看文件的基本Graph图之外，我们还可以自定义Graph。比如说，如果你想分析一个特定的恶意文件样本，然在研究的过程中给各种对象添加标签，你就可以使用VirusTotal Graph提供的对象标记功能了。

你可以右键点击一个对象然后添加标签，如下图所示，我们给一个特定文件对象添加了“Adware Downloader”标签。

关注我们 分享每日精选文章

接下来，你可以点击保存按钮，然后将其保存为一个新的Graph。保存成功之后，你将得到一个用于访问这个Graph链接，你还可以将其共享给他人。

关注我们 分享每日精选文章

虽然新手用户可能需要花一点时间来熟悉VirusTotal Graph的使用，但当你熟悉该工具之后，你就会发现它是一款非实用的恶意软件分析工具了。

为了更好地帮助大家了解该工具的使用，VirusTotal还提供了两个使用演示视频，感兴趣的同学可以点击观看。

演示视频

VirusTotalGraph 文件与 VirusTotal域名文件

看不到，点这里

FB小编Alpha_h4ck编译，转载请注明来自FreeBuf.COM

上一篇：PhpSploit：一款隐蔽性极强的后渗透利用框架
下一篇：Apache Solr远程代码执行漏洞（CVE-2017-12629）从利用到入侵检测

关注我们，分享每日精选文章

已有 1 条评论

langziguang (1级) 2018-01-22 1楼 回

好东西！

亮了

选择文件 未选择任何文件

昵称 请输入昵称 必须 您当前尚未登录。登陆? 注册

邮箱 请输入邮箱地址 必须（保密）

表情 插图

Alpha_h4ck

好好学习，天天向上

4
评论数

最

- 查看各文件的相关性将更加容易 2018.01.20
- PhpSploit：一款隐蔽性极强的后渗透利用框架 2018.01.19
- 英特尔放出Linux微代码以修复Meltdown和Spectre漏洞 2018.01.17

浏览更多

相关阅读

好消息！最新Metasploit加入硬件测试…

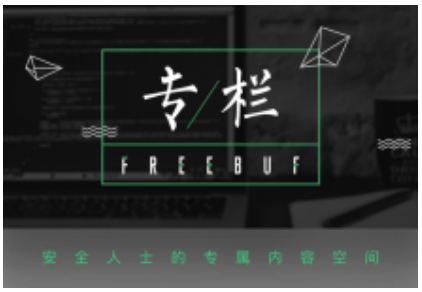
关于SSL/TLS最新漏洞“受戒礼”初步报告

极客DIY：使用树莓派和kali Linux打…

渗透测试中上传文件到目标系统的四…

无线键盘易被监听，不知不觉导致信…

特别推荐



[揭秘：恶意软件是如何操纵ATM机的]

Rabbit_Run 2014-10-09

[反击“猫眼电影”网站的反爬虫策略]

数月亮的孩子 2017-07-26

[漏洞预警：知名论坛系统vBulletin常用SEO插件VBSEO存在严重安全]

dawner 2015-01-09

[【安全大咖说】FriedAppleTeam越狱团队创始人Max Bazaliy专访|]

Elaine_z 2017-07-17