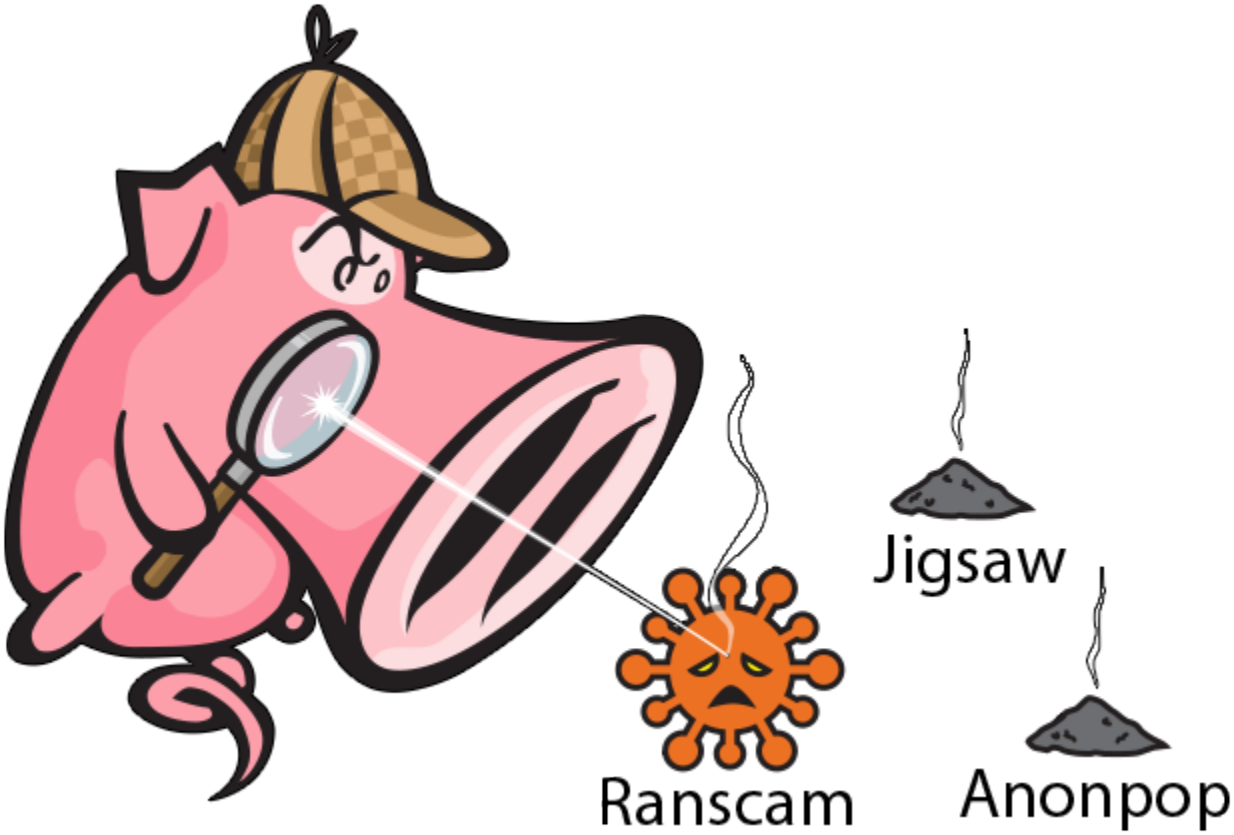
2016 年 7 月 25 日，星期一

勒索软件：因为 OpSec 坚不可摧？

作者：Edmund Brumaghin 和 Warren Mercer

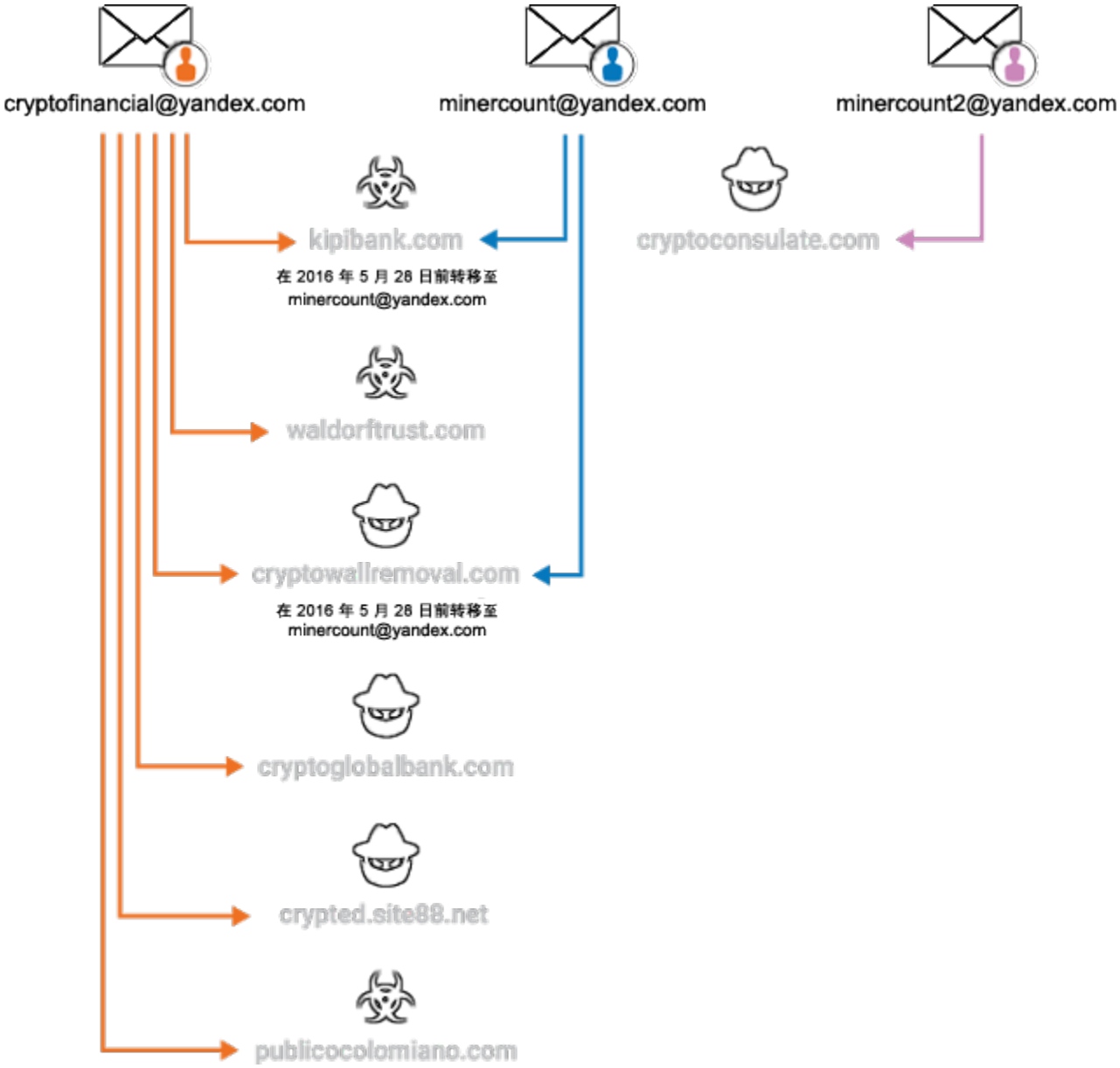


摘要

Talos 最近发布了针对一个破坏性勒索软件的新型变体（我们将其称作 Ranscam）的研究结果。在对 Ranscam 样本进行的进一步分析中，我们发现了几个危害表现 (IOC)，这也引起了我们的好奇心：除了 Ranscam 以外，这位威胁发起者是否还参与或负责了其他恶意软件呢？带着这个问题，我们开始将研究范围扩大到其他破坏性“Ranscam 软件”，以确定它们之间是否存在某些共同特征，可以表明它们是由同一个威胁发起者或团队操控的。我们发现，我们认定的 Ranscam 威胁发起者与几个已知破坏性勒索软件变体（例如 Jigsaw 和 AnonPop）之间存在一些有趣的联系。

寻找联系

您可能还记得，我们在之前针对 Ranscam 的研究中发现，与此恶意软件关联的域名均为同一注册者：cryptofinancial[@]yandex[.]com。我们决定从这一点入手。通过利用可以从 OpenDNS Investigate 获得的逆向 WHOIS 信息，我们开始研究所有与此电子邮件地址相关的域名。根据 WHOIS 历史信息，我们很快发现 Ranscam 发起者使用的其中两个域名最近被转移到了第二个注册者帐户，注册者所使用的电子邮件地址是 minercount[@]yandex[.]com。从这两个电子邮件地址关联的注册者详细信息中我们发现，二者所使用的电话号码完全相同。



在注册者帐户之间转移的两个域名为：

kipibank[.]com（所有权转移日期为 2016 年 2 月 26 日）

cryptowallremoval[.]com（所有权转移日期为 2016 年 5 月 28 日）

DOMAINS ASSOCIATED WITH CRYPTOFINANCIAL@YANDEX.COM

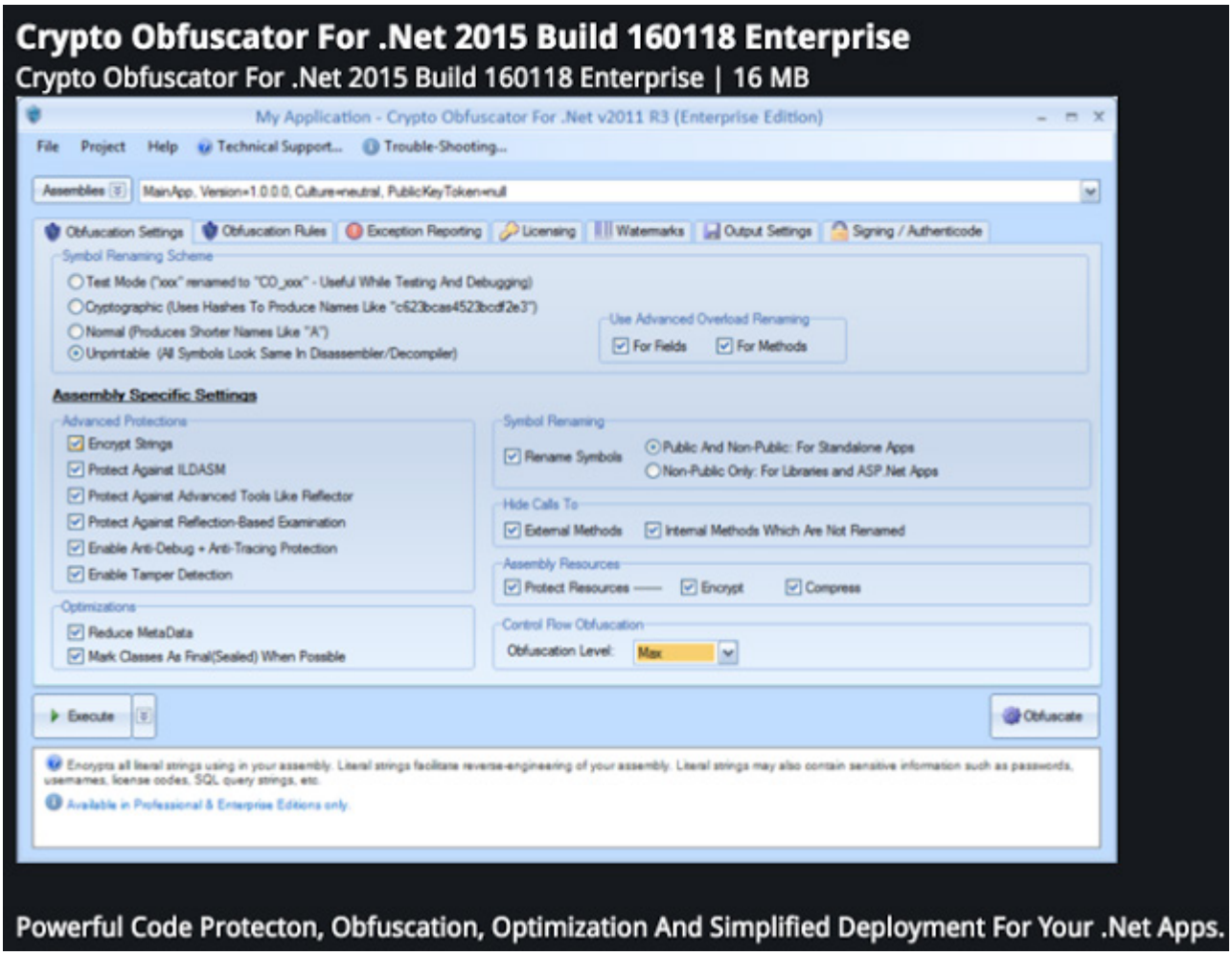
Domain Name	Security Categories	Content Categories	Last Observed
kipibank.com	Malware		Past
publicocolombiano.com	Malware		Current
waldorftrust.com	Malware		Current
cryptoglobalbank.com			Current
cryptowallremoval.com			Past

Showing 5 of 5 results

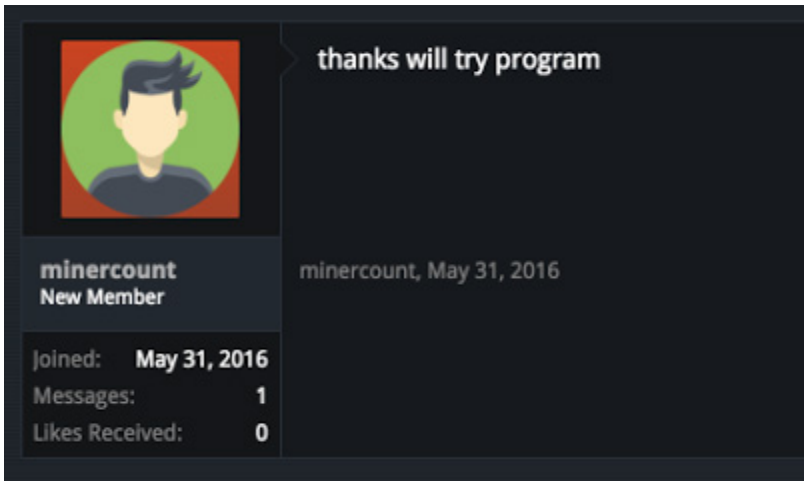
接着，我们开始研究之前发现的其他普遍存在的恶意样本，这些样本都与最近转移的两个域名有关。我们发现，AnonPop 与 Jigsaw（之前发现的两种破坏性勒索软件变体，会删除受害者的文件）一直托管在当前（或之前）与 cryptofinancial[@]yandex[.]com 关联的域名中，也就是我们研究的着手点。

此外，我们在多个地下黑客和编程论坛上发现了一个别名为“minercount”的在线发起者，此人的活动特征与 Ranscam 和 AnonPop 中已经确定的特征有关。这两个恶意软件变体均以经过模糊处理的 .NET 可执行文件形式传送。我们发现，一个名为“minercount”的用户曾在一个详细介绍某个版本的 Crypto Obfuscator 的帖子中发表回帖。正如您想到的那样，这个 Crypto Obfuscator 版本正是针对 .NET 可执行文件的！

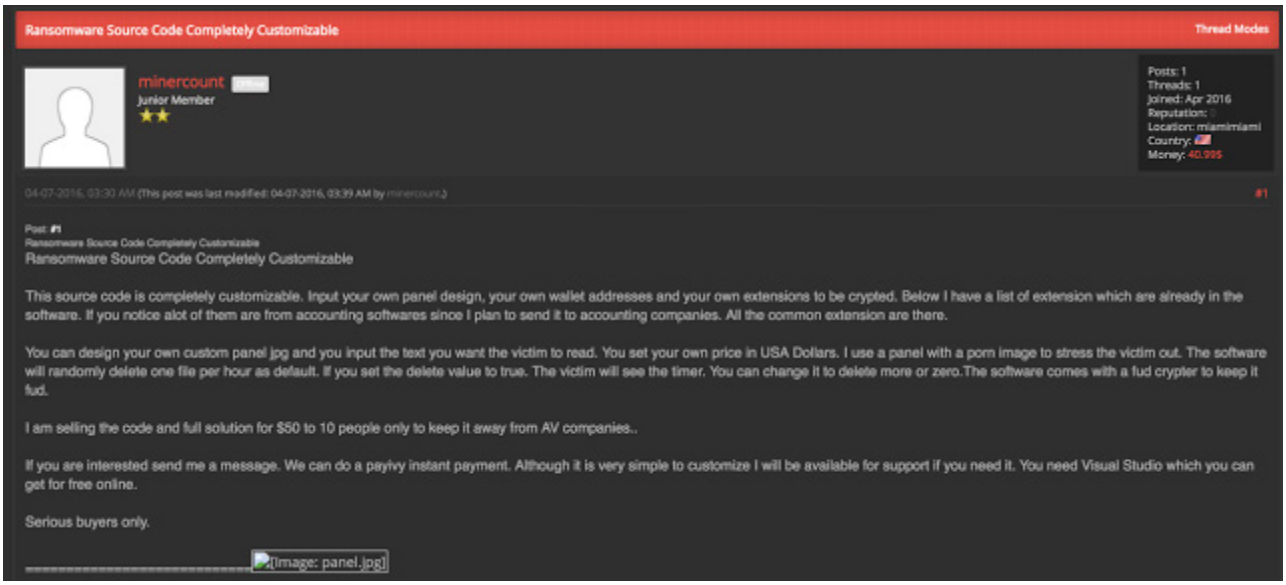
该版本公告（如下所示）恰好与我们所调查的威胁发起者可能使用的模糊处理实用程序有关。



很明显，这位名为“minercount”的威胁发起嫌疑人在这个论坛上进行了注册，而他唯一的帖子就是对这个模糊处理实用程序的开发者表示感谢：



细查其他一些论坛后，我们在四月份又发现了“minercount”，他正在提供一款完全可定制的勒索软件程序：



我们还发现这位威胁发起嫌疑人谈到他打算使用该工具来敲诈会计公司，并以 50 美元的低价向前 10 个购买者出售该工具，从而确保反病毒公司无法获得样本。

有趣的是，在帖子的详细内容中，他还发布了一个指向托管在自己的基础设施上的管理面板图像 (kipibank[.]com/panel.jpg) 的链接。您应该记得，这是之前属于 cryptofinancial[@]yandex[.]com 的一个域名，后来转移至 minercount[@]yandex.com。此域名也被用于托管 Jigsaw 样本以及 Anonpop 使用和/或感染后尝试下载的各个组件。

示例：

hXXp://www[.]kipibank[.]com/55.exe # Jigsaw

hXXp://www[.]kipibank[.]com/anon.jpg # AnonPop

hXXp://www[.]kipibank[.]com/i2.html # Anonpop

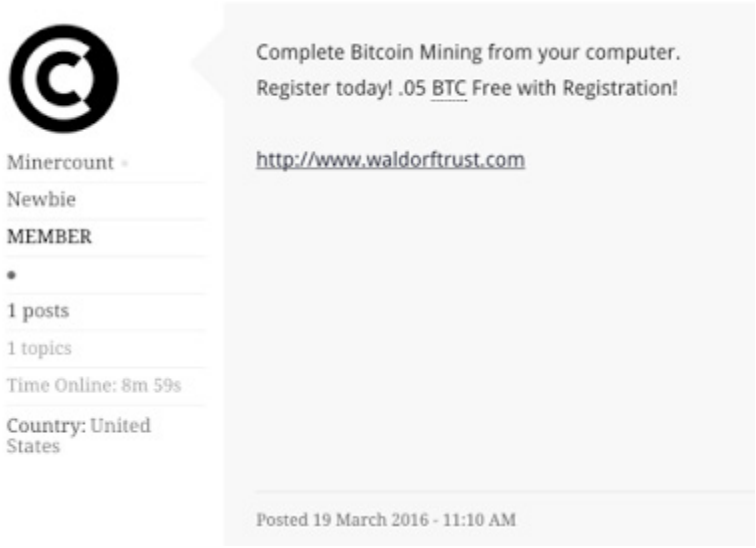
hXXp://www[.]kipibank[.]com/complaint376878.zip # Anonpop

```
Serious buyers only.<br />
<br />
==========</span><img src="http://www.kipibank.com/panel.jpg"
Extensions:<br />
```

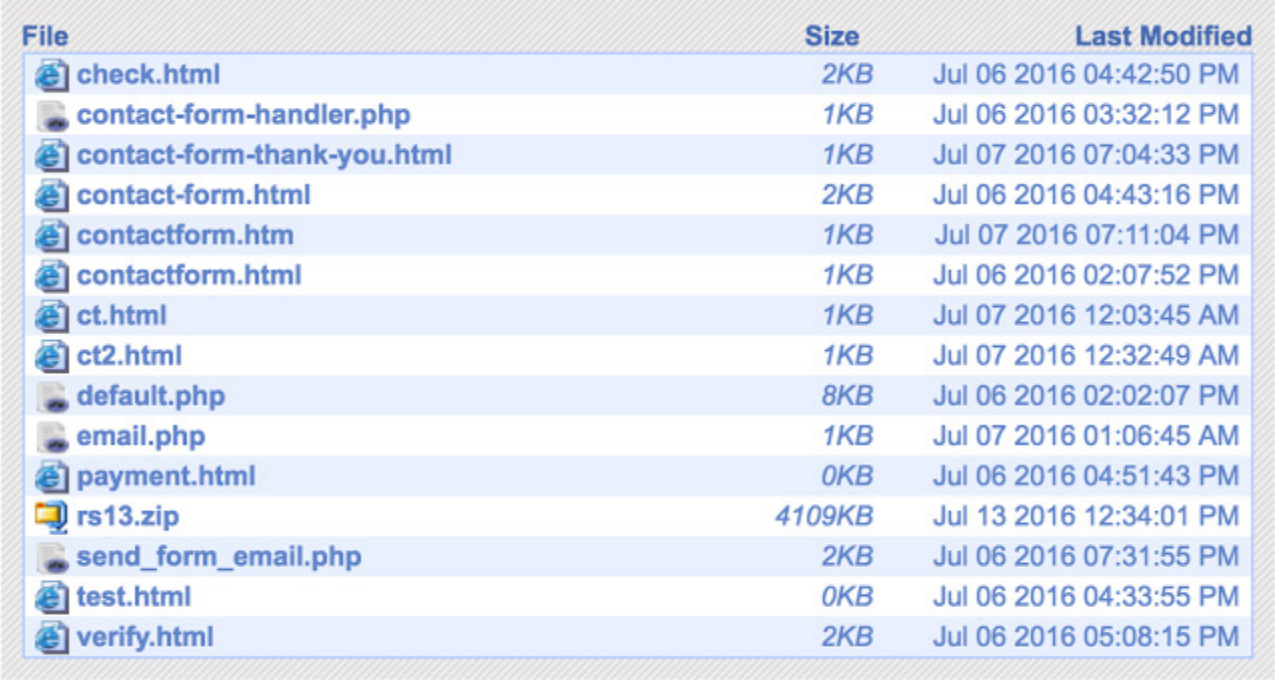
最后，在撰写本文时，我们在某个比特币挖矿网络论坛上也发现了使用该用户名的注册用户。此人发布了一个包含指向域名 waldorftrust[.]com 的链接的帖子，该域名注册者所使用的电子邮件地址同样为 cryptofinancial[@]yandex[.]com。由于我们已经确定了 Jigsaw 样本同样托管在这里，因此这个域名也明显与 Jigsaw 有关。

示例：

hXXp://waldorftrust[.]com/56.exe # Jigsaw



在撰写本博文的过程中，我们还发现了之前未发现/未发布的一个新版本 Ranscam，我们所调查的威胁发起者已经将其上传至自己的一个网站，该网站没有采取任何措施来隐藏内容。“default_public”实例仍然可以下载得到。从目录列表可以看出，该实例是在 7 月 13 日作为名为“rs13.zip”的文件上传的（也就是在我们首次发布关于 Ranscam 的博文之后）。我们认为，此人很喜欢 Ranscam 这个名称，并相应地为其新版本 RS 命名。下图显示压缩存档文件包含了完整的 Visual Studio 项目文件以及已编译的二进制 mnstr.exe（包括 SHA256）。



File	Size	Last Modified
check.html	2KB	Jul 06 2016 04:42:50 PM
contact-form-handler.php	1KB	Jul 06 2016 03:32:12 PM
contact-form-thank-you.html	1KB	Jul 07 2016 07:04:33 PM
contact-form.html	2KB	Jul 06 2016 04:43:16 PM
contactform.htm	1KB	Jul 07 2016 07:11:04 PM
contactform.html	1KB	Jul 06 2016 02:07:52 PM
ct.html	1KB	Jul 07 2016 12:03:45 AM
ct2.html	1KB	Jul 07 2016 12:32:49 AM
default.php	8KB	Jul 06 2016 02:02:07 PM
email.php	1KB	Jul 07 2016 01:06:45 AM
payment.html	0KB	Jul 06 2016 04:51:43 PM
rs13.zip	4109KB	Jul 13 2016 12:34:01 PM
send_form_email.php	2KB	Jul 06 2016 07:31:55 PM
test.html	0KB	Jul 06 2016 04:33:55 PM
verify.html	2KB	Jul 06 2016 05:08:15 PM

有趣的是，对该新版本 Ranscam 的静态分析表明与 Visual Studio 项目所关联源文件中存在完整的编译器工件，如下所述：

C:\Users\Monument\Desktop\winpopfiles\RansNEW\RS630\winopen\bin\Debug\winopen.pdb

此外，我们还观察到完整的编译器工件中包含 jigsaw 样本，这看起来似乎是由使用同一用户名的人制作的：

C:\Users\Monument\Desktop\mean\BitcoinBlackmailer\BitcoinBlackmailer\obj\Release\BitcoinBlackmailer.pdb

Reddit 问题

到目前为止，我们已经能够确定这些恶意软件样本会使用一些相同的基础设施与 IOC。根据在一些隐蔽论坛上的活动和行为，我们进一步印证了其可能的身份。我们当前的计划是根据行为或更多在线活动，进一步确认这些联系，以便进一步印证各种勒索软件变体之间的联系。因此，我们采取了明智的安全研究员在这种情况下应有的做法，我们决定浏览 Reddit。

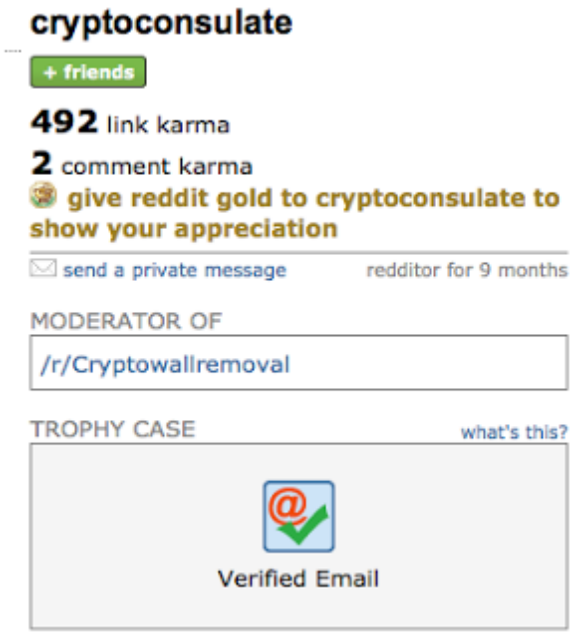
通过搜索与我们所调查两个电子邮件帐户相关的域名，我们发现了一个有趣的事实。有一个 Reddit 用户曾发表了大量的简短的帖子，这些帖子中包含与比特币相关的 Reddit 分类内容，而帖子中的链接指向了我们调查的其中几个域名。对于每个帖子，该用户会同时发布到多个与比特币相关的其他 Reddit 分类内容。此外，我们没有观察到任何其他 Reddit 用户发布过指向这些域名的链接。

waldorftrust[.]com（所有者为 cryptofinancial[@]yandex[.]com]）

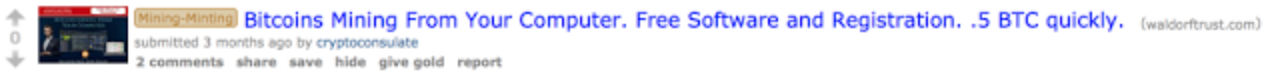
cryptowallremoval[.]com（所有者为 minercount[@]yandex[.]com，之前的所有者为 cryptofinancial[@]yandex[.]com）

cryptoglobalbank[.]com（所有者为 cryptofinancial[@]yandex[.]com）

我们还发现域名 cryptoglobalbank[.]com 被用于散布与 Anonpop 相关的下载程序。与这些帖子关联的用户使用了“cryptoconsulate”用户名，并且是一个名为 /r/cryptowallremoval 的 Reddit 分类内容的版主。而分类内容又关联到域名 cryptowallremoval[.]com，该域名最初注册到 cryptofinancial[@]yandex[.]com，随后转移至 minercount[@]yandex[.]com。



当我们开始关注这位特定的 Reddit 用户后，我们注意到，此人之前提交过一个帖子，声称是一份开采比特币的指南。此帖链接到一个托管在 waldorftrust[.]com/bitcoinsmining 的可执行文件。



而实际上，它是一个名称为“waldorf.exe”的 AutoIT 可执行文件。毫无疑问，该文件会在执行时向系统投放勒索软件。与此样本相关的勒索信如下：

在此勒索软件显示的勒索信中，列出的比特币钱包为：

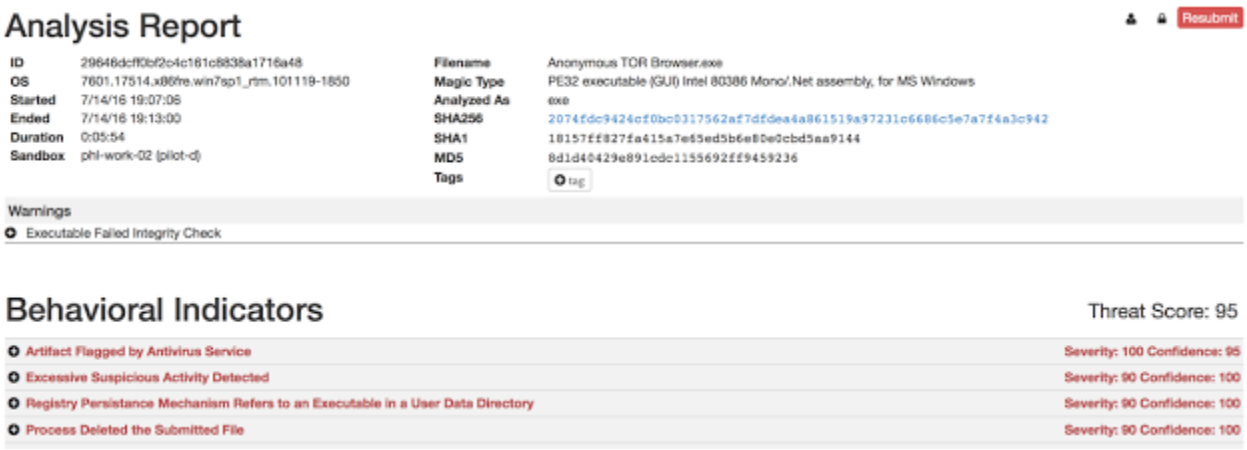
1HXQ5fs6PNhSuQurU7Ccy9HCRnULs1aa2v

此时毫无疑问的是，这个地址与我们分析过的 Jigsaw 样本使用的是同一个比特币地址。可能我们的这位威胁发起者并不是 Jigsaw 的作者，而仅仅是从作者或者黑暗网络论坛直接购买了 Jigsaw。

这是与 Ranscam 和 Jigsaw 的威胁发起者非常直接的联系。我们认为威胁发起者不太可能分享与此比特币地址关联的私钥，因为这可能会导致其他威胁发起者迅速传播该比特币密钥及任何相关的比特币交易。比特币地址的重复使用反映出这个人对 OpSec 缺乏充分了解。

我们还发现了同一个用户发表的帖子，这一次则声称是一份保持比特币交易匿名的指南：

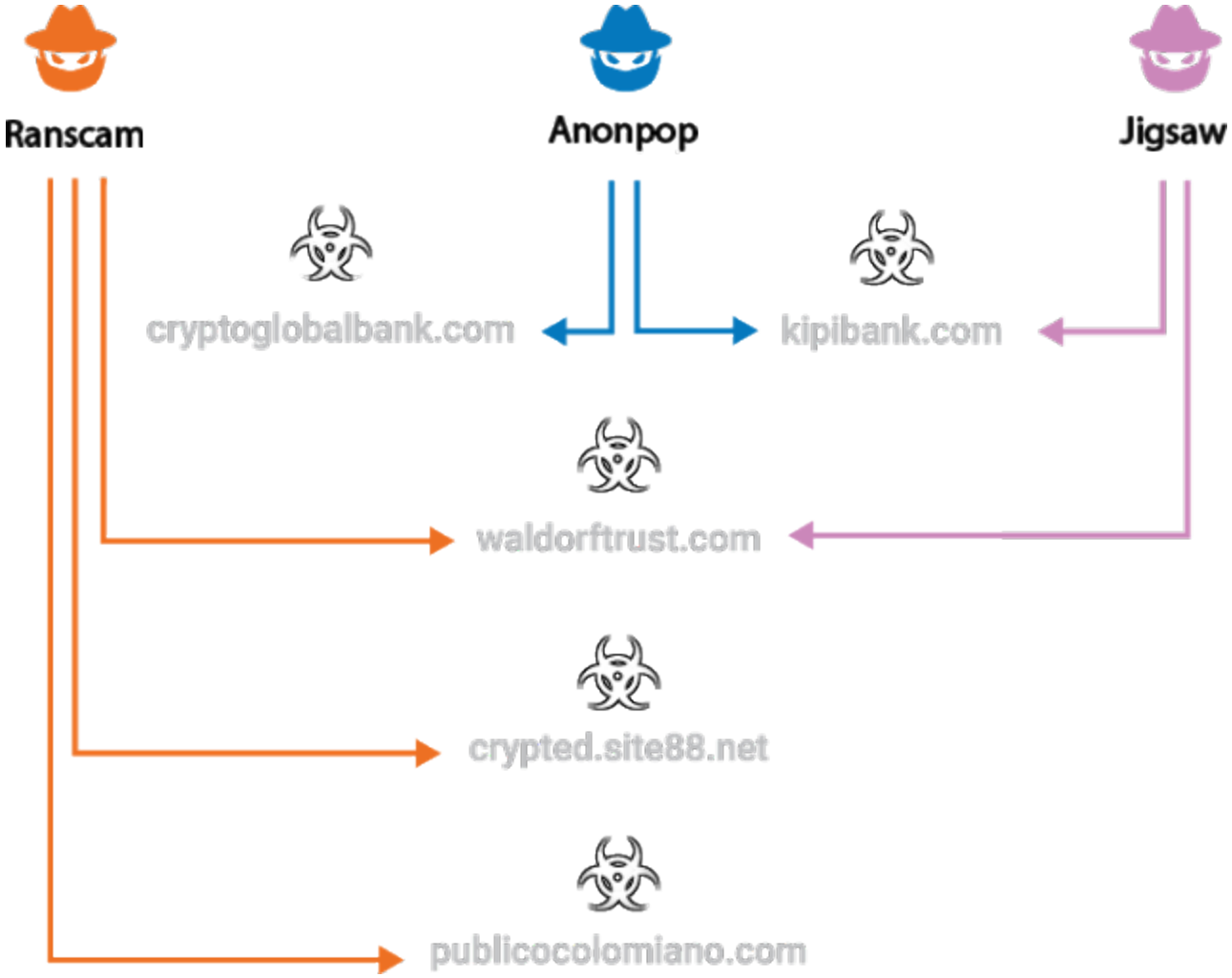
此帖链接到托管在 MEGA Upload 上的一个 ZIP 存档文档。该 ZIP 存档文件包含一个 PDF、一个可执行文件（声称是 Tor Browser 修改版本）和一个文本文件。我们获取了此存档文件的一份副本，并进行了分析。以下是 ThreatGrid 针对其中所包含可执行文件的报告：



因此，我们现在还能够确定，这位威胁发起者不但是破坏性勒索软件散布者，同时也是受版权保护资料的传播者。ZIP 存档文件中包含的 PDF 是一本电子书，名为“Darknet: A Beginner's Guide to Staying Anonymous Online”，作者是 Lance Henderson。

我们确定，注册 cryptoconsulate[.]com（与我们所调查 Reddit 用户的名称相符）域名的帐户与电子邮件地址 minercount2[@]yandex[.]com 有关。有趣的是，最初注册此域名时使用的注册者姓名与用于属于 cryptofinancial[@]yandex[.]com 的所有域名的注册者姓名相符。我们还注意到，在撰写本文时，cryptoconsulate[.]com 和 cryptowallremoval[@]com 均解析到同一 IP 地址 (108.167.140.232)。

在研究了所有的基础设施、恶意软件和威胁实施者信息后，我们可以汇总出共享的基础设施。这表明散布的恶意软件与威胁发起者使用的基础设施之间存在直接联系。



总结

通过进一步分析与 Ranscam 相关的 IOC，我们能够指出与之前所发现的其他破坏性恶意软件变体（包括 Jigsaw 和 Anonpop）相关 IOC 的一些联系。通过跟踪与 Ranscam 相关的威胁发起者活动，我们观察到此破坏性恶意软件的新版本在不断产生，并试图用于胁迫受害者支付赎金，而不需要威胁发起者投入资源以维持高级或隐蔽的活动。

这同时也证明了虽然针对系统的破坏性勒索软件会有很多变体，但是并不能直接表明在勒索软件领域开展活动的威胁发起者数量也很多。如本例所示，一个威胁发起者就可能负责实施多个不同的变体，试图最大程度提高获利情况，或者改善其战术以试图最大程度提高从受害者那里获得的收入。

危害表现 (IOC)

文件名

BitcoinBlackmailer.exe
mnster.exe
t4.exe
t5.exe
anonpop.exe

散列

622d4a52e70c9831eafb2427b51abfbb311ecc34b719432cc19906c80c88aa92 (SHA256)
7cd8f7baf45a7a1847f4329e31cf88a9a549830d6ca00ea1837e99567619bb8f (SHA256)
763cbd6fb5d35d040ab1783c517c4fca43c81a0d72cc4c873b89c789cc2d6bec (SHA256)
Fca8fc0f91c9507f4ef678efbff06386fa10bc8819d74a3cdef03072484bda36 (SHA256)
2074fdc9424cf0bc0317562af7dfdea4a861519a97231c6686c5e7a7f4a3c942 (SHA256)
Ba6c31e51350c074c6092e270a3401ccee2e78aaa2e48d23e0ab2e11e7ef18d8 (SHA256)
0d0c99a3cc19099f68f6c9aec7e2dc5bf40cc83e629e3751ead76b0d36d548fc (SHA256)

域名

Kipibank[.]com
waldorftrust[.]com
cryptoconsulate[.]com
cryptowallremoval[.]com
cryptoglobalbank[.]com
crypted[.]site88[.]net
publicocolombiano[.]com

防护产品

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	保护
AMP	✔
CWS	✔
ESA	✔
网络安全	✔
WSA	✔

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。
CWS 或 WSA 的 Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。
IPS 和 NGFW 网络安全防护功能拥有最新的签名库，可以检测威胁发起者的恶意网络活动。
ESA 可以拦截威胁发起者在攻击活动中发出的恶意电子邮件。

发布者：WARREN MERCER；发布时间：上午 11:01
标签：ANONPOP、比特币、JIGSAW、OPSEC、RANSCAM、勒索软件