Russian Cybercrime Group FullofDeep Behind QNAPCrypt Ransomware Campaigns

intezer.com/blog-russian-cybercrime-group-fullofdeep-behind-qnapcrypt-ransomware-campaigns/

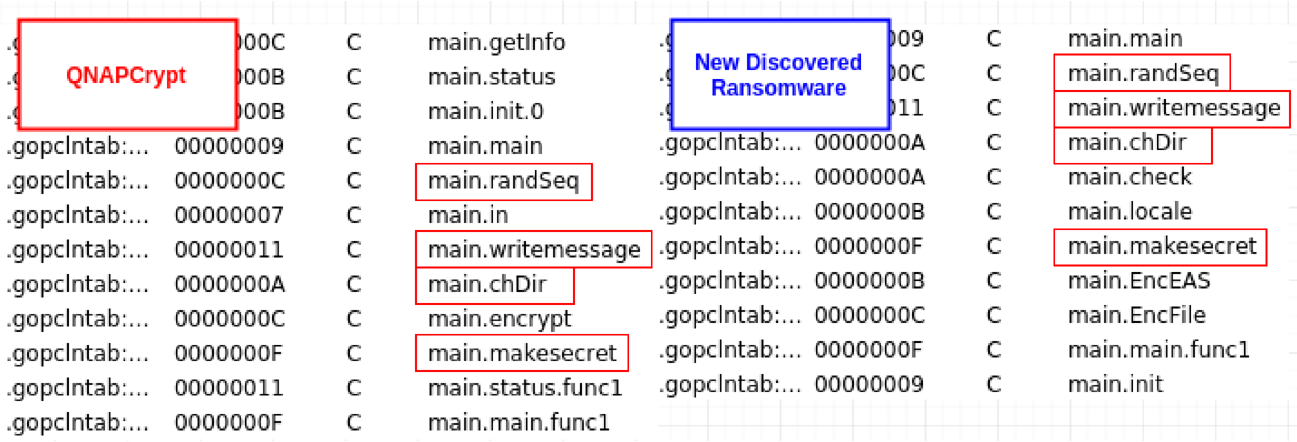
September 20, 2019

Introduction

We previously reported on how we managed to temporarily shut down 15 operative **QNAPCrypt ransomware campaigns** targeting Linux-based file storage systems (NAS servers). We have now identified a new QNAPCrypt sample which is being used by the same threat actor group. The authors behind this new ransomware instance have revealed enough evidence for us to conclude the establishment of **FullofDeep**, a Russian cybercrime group operating from the Union State and the Ukraine. The group is mainly focused on ransomware campaigns.

Technical Analysis

Initially, we received a hit from an older YARA signature, which was created to hunt for QNAPCrypt instances. Although the new ransomware variant does not share large portions of code with the original QNAPCrypt campaigns, the naming convention used in the new ransomware's functions has been observed in previous QNAPCrypt instances:



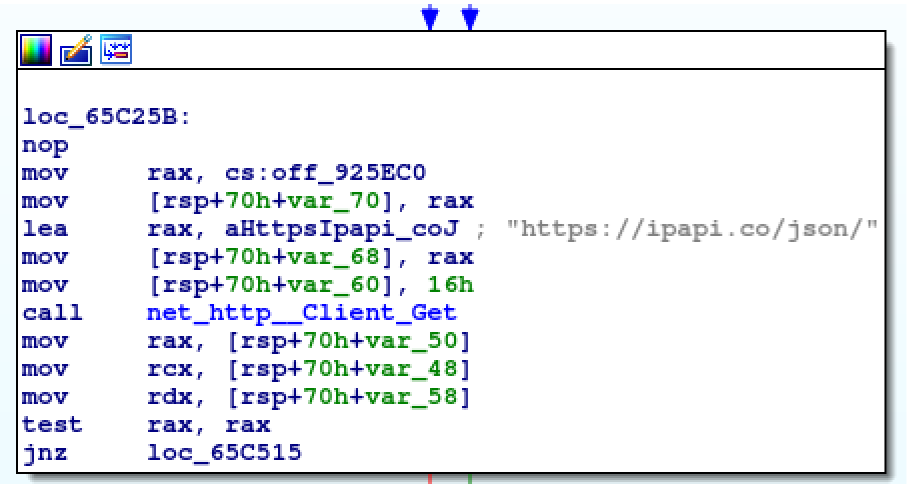
QNAPCrypt

```
.(        )00C    C    main.getInfo
.(        )00B    C    main.status
.(        )00B    C    main.init.0
.gopclntab:...  00000009    C    main.main
.gopclntab:...  0000000C    C    main.randSeq
.gopclntab:...  00000007    C    main.in
.gopclntab:...  00000011    C    main.writemessage
.gopclntab:...  0000000A    C    main.chDir
.gopclntab:...  0000000C    C    main.encrypt
.gopclntab:...  0000000F    C    main.makesecret
.gopclntab:...  00000011    C    main.status.func1
.gopclntab:...  0000000F    C    main.main.func1
```

New Discovered Ransomware

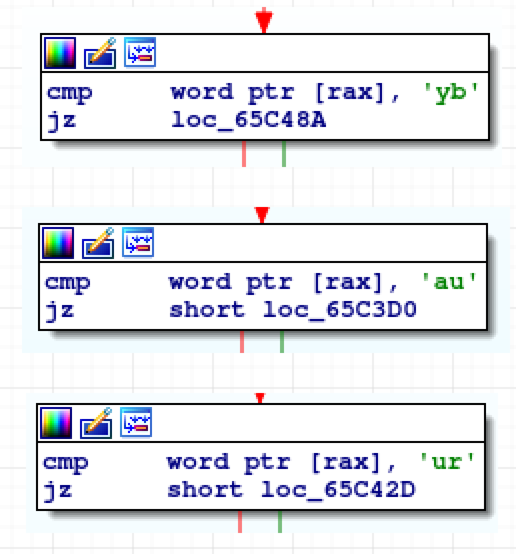
```
.(        )09     C    main.main
.(        )0C     C    main.randSeq
.(        )11     C    main.writemessage
.gopclntab:...  0000000A    C    main.chDir
.gopclntab:...  0000000A    C    main.check
.gopclntab:...  0000000B    C    main.locale
.gopclntab:...  0000000F    C    main.makesecret
.gopclntab:...  0000000B    C    main.EncEAS
.gopclntab:...  0000000C    C    main.EncFile
.gopclntab:...  0000000F    C    main.main.func1
.gopclntab:...  00000009    C    main.init
```

In addition, the new variant utilizes geolocation information in order to determine whether or not the malware will operate:



```
loc_65C25B:
nop
mov     rax, cs:off_925EC0
mov     [rsp+70h+var_70], rax
lea     rax, aHttpsIpapi_coJ ; "https://ipapi.co/json/"
mov     [rsp+70h+var_68], rax
mov     [rsp+70h+var_60], 16h
call    net_http__Client_Get
mov     rax, [rsp+70h+var_50]
mov     rcx, [rsp+70h+var_48]
mov     rdx, [rsp+70h+var_58]
test    rax, rax
jnz     loc_65C515
```

The threat actors behind the new ransomware have filtered Belarusia(BY), Russia(RU), and Ukraine(UA), in order to impede operation if the ransomware is executed from one of these countries. This is similar to the QNAPCrypt implant Anomali previously reported on:

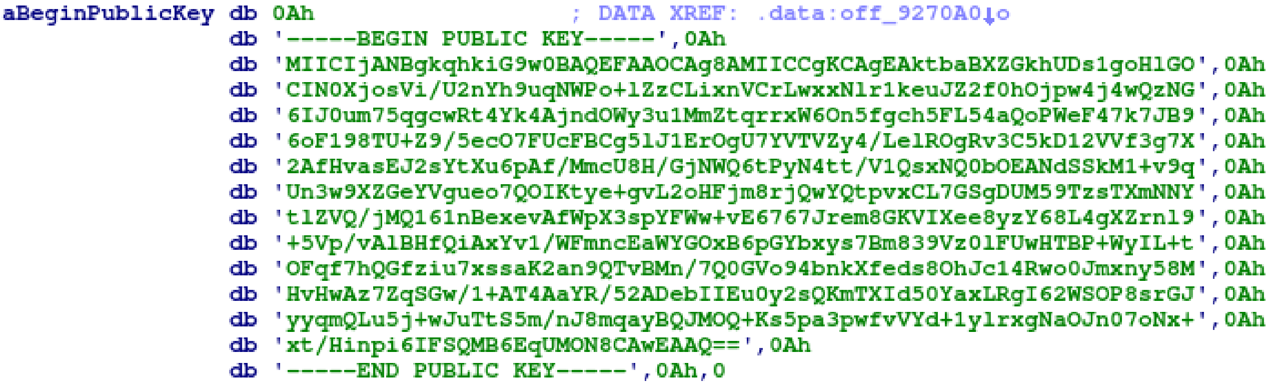


```
cmp     word ptr [rax], 'yb'
jz      loc_65C48A
```

```
cmp     word ptr [rax], 'au'
jz      short loc_65C3D0
```

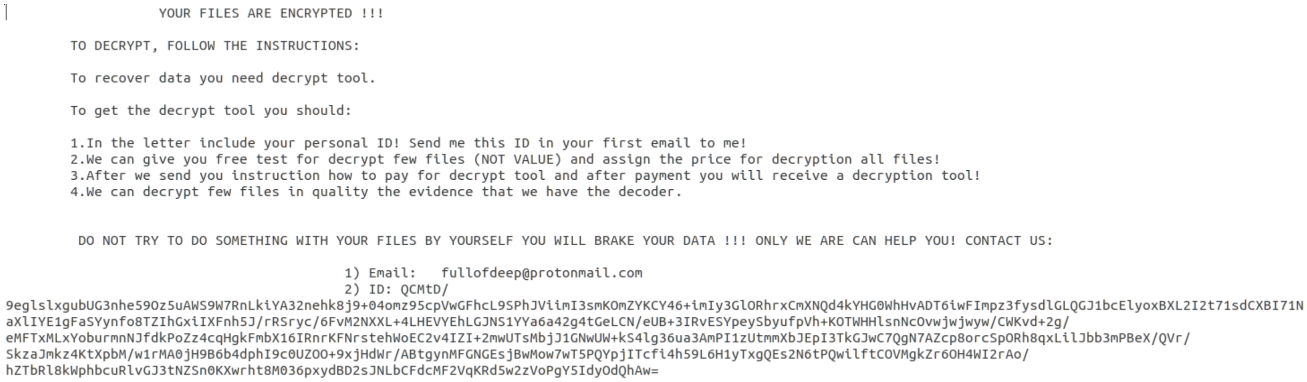
```
cmp     word ptr [rax], 'ur'
jz      short loc_65C42D
```

The overall functionality of the ransomware remains similar to QNAPCrypt. The main configuration of the ransomware is static and hard-coded within the binary, much like the latest version of QNAPCrypt.



```
aBeginPublicKey db 0Ah                      ; DATA XREF: .data:off_9270A0↓o
                db '-----BEGIN PUBLIC KEY-----',0Ah
                db 'MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAktbaBXZGkhUDs1goH1GO',0Ah
                db 'CIN0XjosVi/U2nYh9uqNWPo+1ZzCLixnVCrLwxxNlr1keuJZ2f0hOjpw4j4wQzNG',0Ah
                db '6IJ0um75qgcwRt4Yk4AjndOWy3u1MmZtqrrxW6On5fgch5FL54aQoPWeF47k7JB9',0Ah
                db '6oF198TU+Z9/5ecO7FUcFBCg5lJ1ErOgU7YVTVZy4/LelROgRv3C5kD12VVf3g7X',0Ah
                db '2AfHvasEJ2sYtXu6pAf/MmcU8H/GjNWQ6tPyN4tt/V1QsxNQ0bOEANdSSkM1+v9q',0Ah
                db 'Un3w9XZGeYVgueo7QOIKtye+gvL2oHFjm8rjQwYQtpvxCL7GSgDUM59TzsTXmNNY',0Ah
                db 'tlZVQ/jMQ161nBexevAfWpX3spYFWw+vE6767Jrem8GKVIXee8yzY68L4gXZrnl9',0Ah
                db '+5Vp/vAlBHfQiAxYv1/WFmncEaWYGOxB6pGYbxys7Bm839Vz0lFUwHTBP+WyIL+t',0Ah
                db 'OFqf7hQGfziu7xssaK2an9QTvBMn/7Q0GVo94bnkXfeds8OhJc14Rwo0Jmxny58M',0Ah
                db 'HvHwAz7ZqSGw/1+AT4AaYR/52ADebIIEu0y2sQKmTXId50YaxLRgI62WSOP8srGJ',0Ah
                db 'yyqmQLu5j+wJuTtS5m/nJ8mqayBQJMOQ+Ks5pa3pwfvVYd+1ylrxgNaOJn07oNx+',0Ah
                db 'xt/Hinpi6IFSQMB6EqUMON8CAwEAAQ==',0Ah
                db '-----END PUBLIC KEY-----',0Ah,0
```

As is similar to the original QNAPCrypt samples, the algorithm the attackers chose to encrypt the filesystem with is AES CFB. One noticeable difference is the main ransom note doesn't advertise a specific bitcoin wallet like it did in the original QNAPCrypt samples. Instead, the attackers demand to be contacted via a protonmail email account:



```
                   YOUR FILES ARE ENCRYPTED !!!

        TO DECRYPT, FOLLOW THE INSTRUCTIONS:

        To recover data you need decrypt tool.

        To get the decrypt tool you should:

        1.In the letter include your personal ID! Send me this ID in your first email to me!
        2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
        3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
        4.We can decrypt few files in quality the evidence that we have the decoder.


         DO NOT TRY TO DO SOMETHING WITH YOUR FILES BY YOURSELF YOU WILL BRAKE YOUR DATA !!! ONLY WE ARE CAN HELP YOU! CONTACT US:

                                        1) Email:   fullofdeep@protonmail.com
                                        2) ID: QCMtD/
9eglslxgubUG3nhe59Oz5uAWS9W7RnLkiYA32nehk8j9+04omz95cpVwGFhcL9SPhJViimI3smKOmZYKCY46+imIy3GlORhrxCmXNQd4kYHG0WhHvADT6iwFImpz3fysdlGLQGJ1bcElyoxBXL2I2t71sdCXBI71N
aXlIYE1gFaSYynfo8TZIhGxiIXFnh5J/rRSryc/6FvM2NXXL+4LHEVYEhLGJNS1YYa6a42g4tGeLCN/eUB+3IRvESYpeySbyufpVh+KOTWHHlsnNcOvwjwjwyw/CWKvd+2g/
eMFTxMLxYoburmnNJfdkPoZz4cqHgkFmbX16IRnrKFNrstehWoEC2v4IZI+2mwUTsMbjJ1GNwUW+kS4lg36ua3AmPI1zUtmmXbJEpI3TkGJwC7QgN7AZcp8orcSpORh8qxLilJbb3mPBeX/QVr/
SkzaJmkz4KtXpbM/w1rMA0jH9B6b4dphI9c0UZOO+9xjHdWr/ABtgynMFGNGEsjBwMow7wT5PQYpjITcfi4h59L6H1yTxgQEs2N6tPQwilftCOVMgkZr6OH4WI2rAo/
hZTbRl8kWphbcuRlvGJ3tNZSn0KXwrht8M036pxydBD2sJNLbCFdcMF2VqKRd5w2zVoPgY5IdyOdQhAw=
```

The email address provided is “fullofdeep”, and the ransom note annotates ‘CONTACT US’. These strings draw us to the conclusion that this is a Russian cybercrime group referred to as FullOfDeep, and that the group is deploying different ransomware campaigns. Based on the samples’ overlaps, including both ransomware were written in Go, and in addition to similarities in the implant function naming convention and the geolocation filtering applied, we can assess with high confidence that this new ransomware sample is operated by the same authors behind the original QNAPCrypt campaigns.

Summary

In July, we identified and temporarily seized 15 active QNAPCrypt ransomware campaigns targeting Linux-based file storage systems (NAS servers). This discovery was significant in that it’s rare to see ransomware being used to target the Linux-operating system.

While we prevented the malware from infecting additional victims, we have since hunted for and detected a new ransomware that shares many similarities with the previous QNAPCrypt samples. We can assess with high confidence that FullofDeep, a new Russian cybercrime group specializing in ransomware operations, is behind both the original QNAPCrypt campaigns and the newly identified ransomware instance.

In addition, both the original and new QNAPCrypt samples are indexed in Intezer Analyze's code genome database. If you have a suspicious file that you suspect to be QNAPCrypt, you can upload it to the free Intezer Analyze community edition in order to view the verdict, code and string reuse, and more.

Please refer to the **mitigation recommendations** section in our blog post titled, Why we Should be Paying More Attention to Linux Threats, for best practices Linux users can adopt in order to mitigate the threats posed by QNAPCrypt and other Linux-based threats.

IOCs
50470f94e7d65b50bf00d7416a9634d9e4141c5109a78f5769e4204906ab5f0b
fullofdeep@protonmail.com