**Final Project**

**and**

**Report**

**Dragonfish's Elise Malware**

**Prepared by Jadea Parchment**

**UID: U19093109**

Table of Contents

[Abstract 3](#_heading=h.gjdgxs)

[Scenario Introduction 3](#_heading=h.30j0zll)

[Threat Actor 3](#_heading=h.1fob9te)

[Target 3](#_heading=h.3znysh7)

[Campaign 4](#_heading=h.2et92p0)

[The Exploit 4](#_heading=h.tyjcwt)

[Stages of the Attack 4](#_heading=h.3dy6vkm)

[Reconnaissance 4](#_heading=h.1t3h5sf)

[Weaponizing 4](#_heading=h.4d34og8)

[Delivery 4](#_heading=h.2s8eyo1)

[Exploit 5](#_heading=h.17dp8vu)

[Stix Viz Representation 6](#_heading=h.3rdcrjn)

[Soltra/Edge Representation 7](#_heading=h.26in1rg)

[Install 8](#_heading=h.lnxbz9)

[Command and Control](#_heading=h.35nkun2) 9

[Actions on Objectives](#_heading=h.1ksv4uv) 9

[Incident Handling Process 10](#_heading=h.44sinio)

[Identification Phase 10](#_heading=h.2jxsxqh)

[Eradication and Recovery Phase 10](#_heading=h.z337ya)

[Lessons Learned Phase](#_heading=h.3j2qqm3) 10

[Exploit References 11](#_heading=h.1y810tw)

[References 11](#_heading=h.4i7ojhp)

****

# Abstract

This paper delves into examining the phases of an attack using “**Dragonfish's Elise Malware**”, specifically, exploring the exploitation of vulnerability CVE-2017-11882. A malicious DLL is injected into the Internet Explorer, which enables data harvesting, communication with a command and control server, and possible remote access; where targeted organizations ‘ operational integrity and data security would be severely at risk. The analyzed exploit was initially released on 01/19/2018 and was last updated the same day ([Accenture Security Dragonfish.pdf](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=35b97015fe&attid=0.2&permmsgid=msg-a:r2906060266310513405&th=18f0d5cf095c6ecb&view=att&disp=safe&realattid=f_lvd1f3561&saddbat=ANGjdJ8A4IpVz8o869btzavIWck0NoKpXGgU5tblulRIqHlsbPKXxWjclA6br00O7MM-TWbL5xGLQ8ZOqBRTRWWa6HuBbWYmAp9zv7ohH7TTcSHnBwrfUFQsTRBUNo-8bgyg9QQWmPLuCzmgZ_j-WKb6Cvx6-MYuuG0eTApd7SfBRKq1Pr5JxDQsVNdTs6r688BToUtUvzlQCEjMnQkqOfw7PgKwbxcuzzYdwua4ZbfLX-IBHgekmkstuklb4qPfdxw1cAwKF9w4dqwx44dYPjLyyKVp5Guh1EHk1n7TBrk5vKonAAwvZP2Fc73kTEsdUQ8IP9H-L6Fqzm_2A_9_xzGUxK7I1Yp1bw2m-ks9lBKHWGfiiVrJ5GRQ5fCPtJ-Ky_2qnYCKQGcVNxV7KDGt9cdF4Kq5n6aez4CQTCNKcyKpwteJYOXnF55ggVEB6S2a0y3m5trwRiizQXwvn_lpzDHyHQv2PX0nrH3BrC_alunIzwxPUIr8no1wv4s-7_PSmcsyKLWuT7ypdQ8FFrqtoyLku8PySzib830l8KwVtlfivpQptnTgashbMd014Uk7QbqoI3ZQSK8iZQU7mhslZrZkovGl5ZP4AHKjwrTx0ztgyzY4HeELKDOHH0Zs3FXS8CIe39uGL6WsLXDd9NAiOlvakrO0YyiQEyiWk9GiHyixd3dzuh8_Zr575rVD3gH1TMW1qjHYU92euxo4876nlIOle8bEa4UPxN3BOwR0l9UNUx90ZfFStBivbL03s3rmWeay5GM3Iu5E5ZDINa2D7yBuz0IZbNtNAI2Py1qQN2Dda2cX0ZQsmAa7TzxmJl_xzWpZipPzbyR1WpklbF3Uxqy0Drip5jNT5fYSHNt0h8oaZ_b_rJiuYhBZKkYbkdX7wt49PRfzvRpVUmqUO4camu3gmu9ml03OaRT0YGUKHV9CwambDxQEypJvL7Q3RRMB4OOHlI2KOlNspe60o8Qa8cGAWVT-hL_NxivCuS2rjdjLuPXjRvE2Pz4kByKYAa4)).

The phases of the attack will be broken down using the DHS “Kill Chain”, which is represented below:



# Scenario Introduction

Key actors for the attack scenario will briefly be identified and described in this section. This organization is done to define the STIX objects into their perspective roles.

Threat Actor

The threat actor behind this campaign is the Dragonfish/ Lotus Blossom group, renowned for its sophisticated cyber espionage activities. Their primary objective generally revolves around gathering sensitive information from targeted organizations, often for geopolitical advantage or strategic intelligence.

Target

The primary targets of this campaign are organizations affiliated with the ASEAN Defence Ministers' Meeting (ADMM). These may include government agencies, military institutions, and political entities within Southeast Asia. The attackers aim to infiltrate these networks to extract sensitive data and intelligence.

Campaign

Dragonfish’s Elise Malware Campaign dispenses malicious Microsoft Word documents, through email phishing, social engineering tactics and compromised websites. These documents actually have embedded executables, which have harmful OLE objects that distribute the Elise Malware when opened on targeted systems.

The Exploit

Elise malware is distributed specifically exploiting the CVE-2017-11882 vulnerability. The attackers employ various strategies, including injection into processes like iexplore.exe and communication with a Command and Control (C2) server, aiming to infiltrate targeted systems to get sensitive data, such as IP addresses and software inventories.

# Stages of the Attack

## Reconnaissance

Dragonfish likely conducts thorough research identifying specific targets associated with the ASEAN Defence Ministers’ Meeting (ADMM). Through analyzing organizational structures, network scanning and pinpointing key individuals within the organization, the attacker is able to identify exactly what information to gather for exploitation.

## Weaponizing

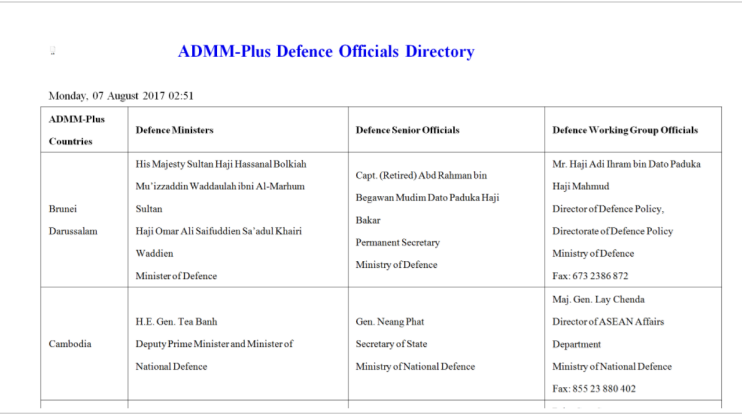
Findings are then weaponized by developing and distributing malicious Microsoft Word documents embedded with the Elise malware. These documents are curated to exploit known vulnerabilities, including CVE-2017-11882, in order to infiltrate the targeted systems when opened by users.

Figure 1: Showing the original file path

## Delivery

Weaponized Microsoft Word documents are usually delivered to targets through email phishing, social engineering tactics, or compromised websites. These delivery tactics are meant to entice recipients within the ASEAN Defence Ministers’ Meeting (ADMM) to open the malicious documents initiating the attack.

## Exploit

After malicious documents are opened, the Elise malware exploits the systems’ vulnerabilities including CVE-2017-11882 in Microsoft Office applications. This exploitation allows the malware to gain unauthorized access to the victim's system and execute its malicious payload without the user's knowledge or consent. Visual aids for campaigns can be seen below:

### Stix Viz Representation

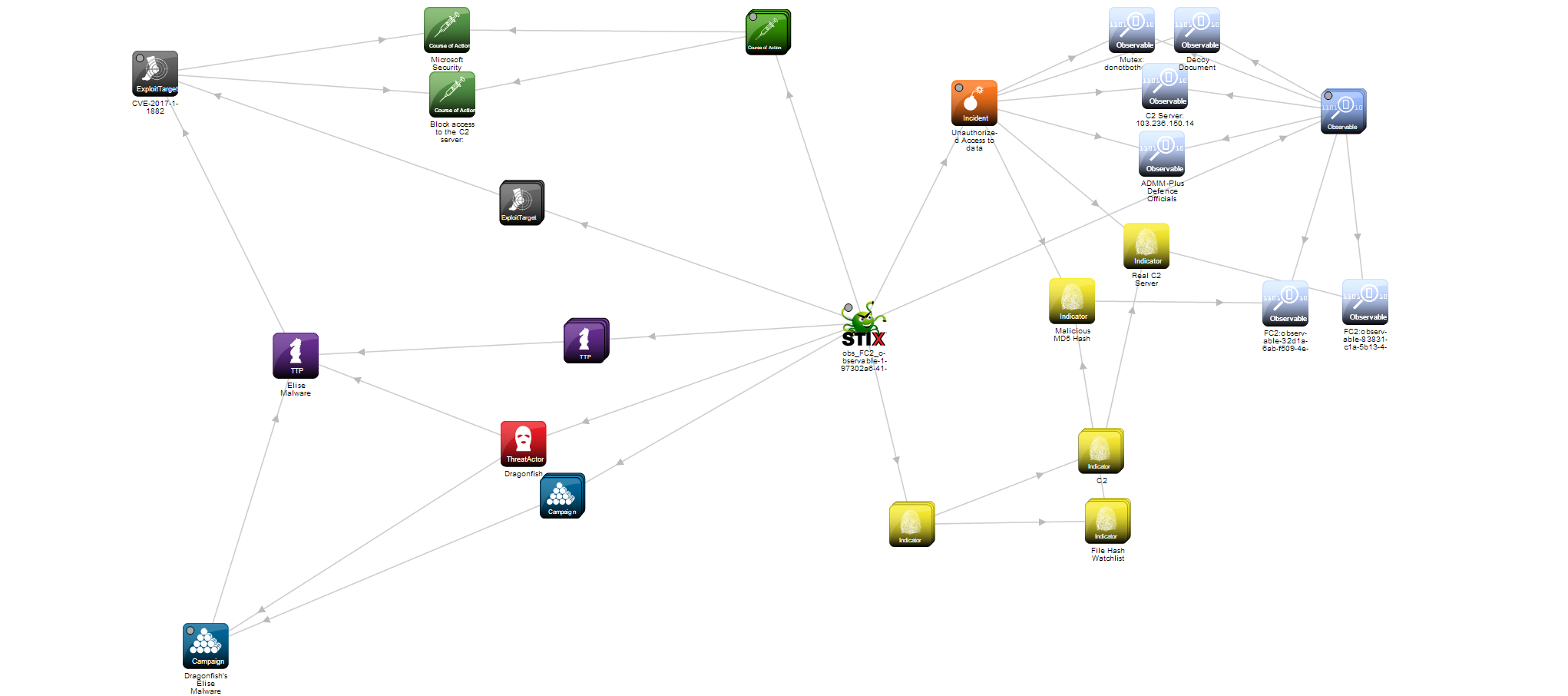
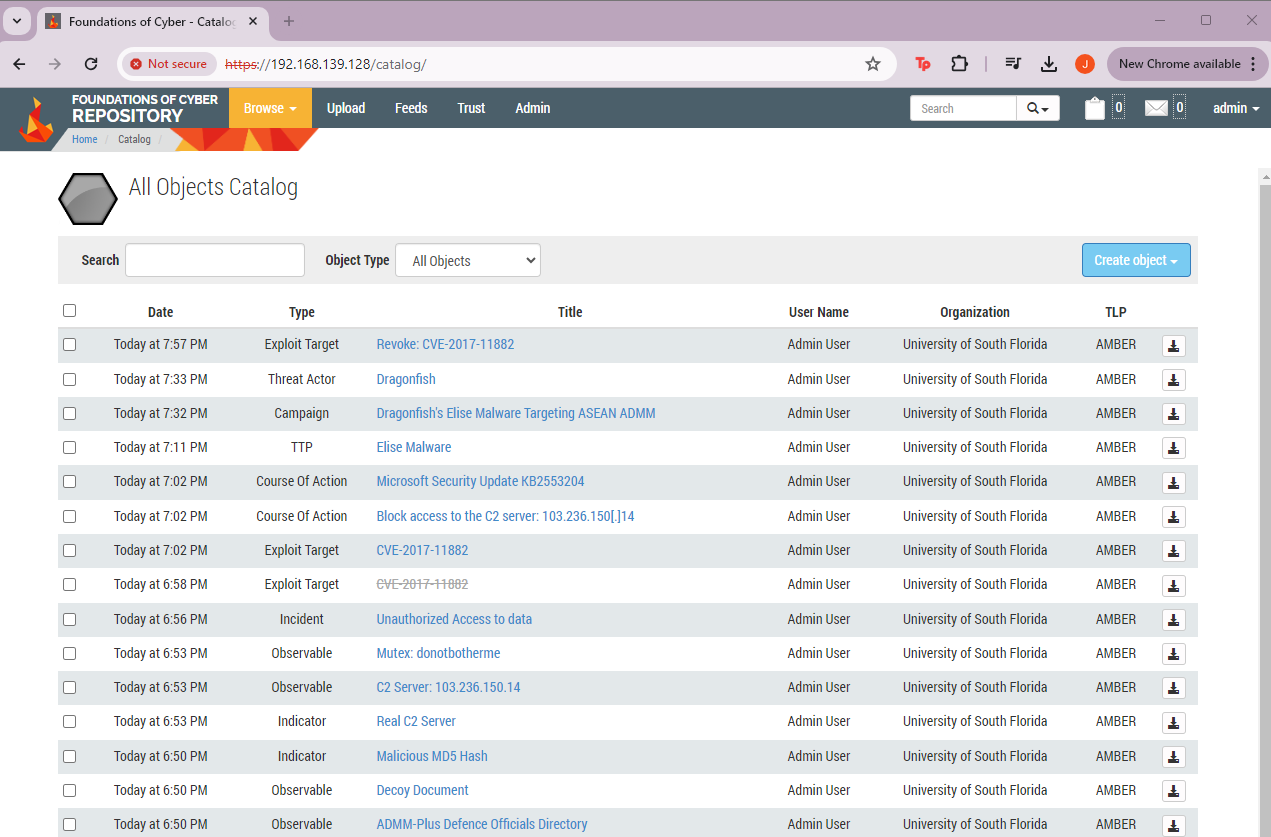


Figure 2: Showing Dragonfish's Elise Malware in StixViz image

Soltra/Edge Representation 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

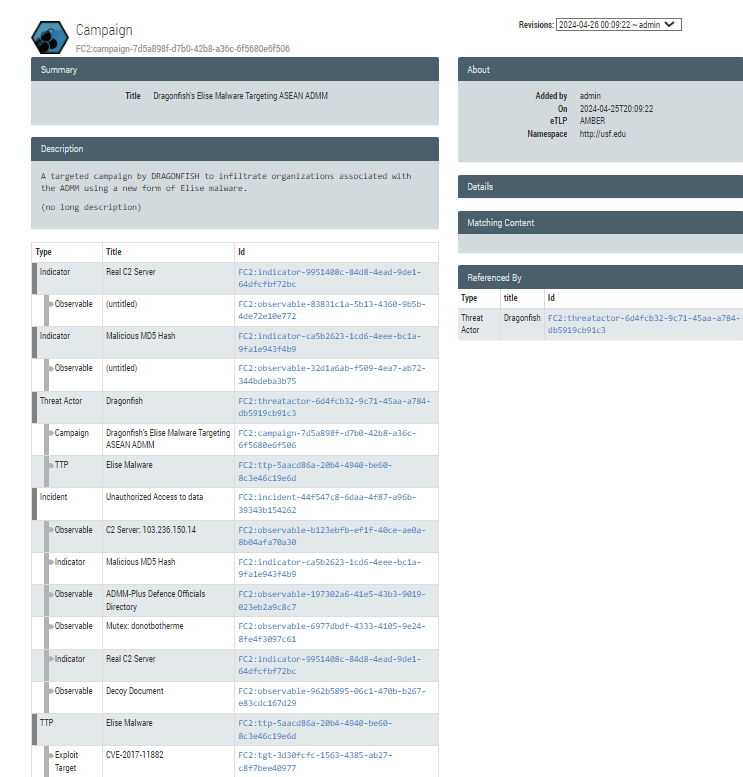


Figure 3: Showing Dragonfish's Elise Malware in Soltra/Edge image

## Install

The Elise malware installs itself on the target's system, enabling further malicious activities. This installation phase allows access to be maintained so espionage objectives can be carried out on the compromised system over an extended period of time. The installation process entails:

“1. Starts iexplore.exe (Internet Explorer) in a suspended state

2. Injects NavShExt.dll into the iexplore.exe process and calls the DLL

export Setting function

3. The iexplore.exe process continues to run in the background

4. Creates a mutex named donotbotherme (see Exhibit 3) to avoid having

duplicated executions

5. Creates a file named thumbcache\_1CD60.db in

AppData\Local\Microsoft\Windows\Explorer\ where the harvested data is

stored

6. Sends data to and downloads files and commands from the designated C2

server”

([Accenture Security Dragonfish.pdf](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=35b97015fe&attid=0.2&permmsgid=msg-a:r2906060266310513405&th=18f0d5cf095c6ecb&view=att&disp=safe&realattid=f_lvd1f3561&saddbat=ANGjdJ8A4IpVz8o869btzavIWck0NoKpXGgU5tblulRIqHlsbPKXxWjclA6br00O7MM-TWbL5xGLQ8ZOqBRTRWWa6HuBbWYmAp9zv7ohH7TTcSHnBwrfUFQsTRBUNo-8bgyg9QQWmPLuCzmgZ_j-WKb6Cvx6-MYuuG0eTApd7SfBRKq1Pr5JxDQsVNdTs6r688BToUtUvzlQCEjMnQkqOfw7PgKwbxcuzzYdwua4ZbfLX-IBHgekmkstuklb4qPfdxw1cAwKF9w4dqwx44dYPjLyyKVp5Guh1EHk1n7TBrk5vKonAAwvZP2Fc73kTEsdUQ8IP9H-L6Fqzm_2A_9_xzGUxK7I1Yp1bw2m-ks9lBKHWGfiiVrJ5GRQ5fCPtJ-Ky_2qnYCKQGcVNxV7KDGt9cdF4Kq5n6aez4CQTCNKcyKpwteJYOXnF55ggVEB6S2a0y3m5trwRiizQXwvn_lpzDHyHQv2PX0nrH3BrC_alunIzwxPUIr8no1wv4s-7_PSmcsyKLWuT7ypdQ8FFrqtoyLku8PySzib830l8KwVtlfivpQptnTgashbMd014Uk7QbqoI3ZQSK8iZQU7mhslZrZkovGl5ZP4AHKjwrTx0ztgyzY4HeELKDOHH0Zs3FXS8CIe39uGL6WsLXDd9NAiOlvakrO0YyiQEyiWk9GiHyixd3dzuh8_Zr575rVD3gH1TMW1qjHYU92euxo4876nlIOle8bEa4UPxN3BOwR0l9UNUx90ZfFStBivbL03s3rmWeay5GM3Iu5E5ZDINa2D7yBuz0IZbNtNAI2Py1qQN2Dda2cX0ZQsmAa7TzxmJl_xzWpZipPzbyR1WpklbF3Uxqy0Drip5jNT5fYSHNt0h8oaZ_b_rJiuYhBZKkYbkdX7wt49PRfzvRpVUmqUO4camu3gmu9ml03OaRT0YGUKHV9CwambDxQEypJvL7Q3RRMB4OOHlI2KOlNspe60o8Qa8cGAWVT-hL_NxivCuS2rjdjLuPXjRvE2Pz4kByKYAa4))

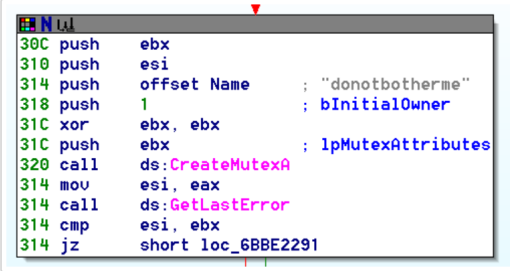


Figure 4: Showing Mutex creation

## Command and Control

With the malware successfully installed, the threat actors establish communication with a Command and Control (C2) server, allowing them to remotely control the compromised systems, to receive commands and upload harvested data. Debug messages stored in the %temp% folder provide insights into the malware's operations, indicating successful attacks or error messages when the C2 server cannot be reached.

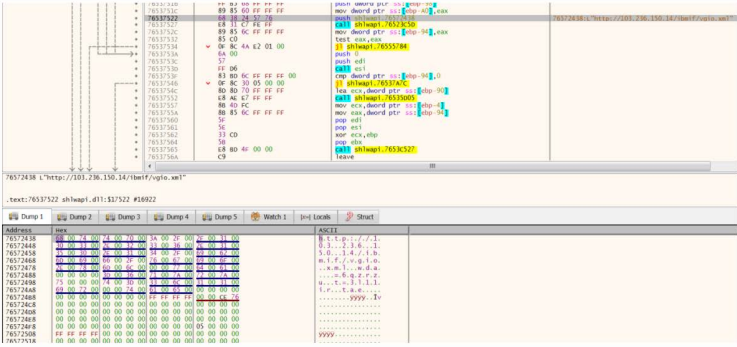


Figure 5: Showing Real C2 Server HardCoded in the Elise Malware

## Actions on Objectives

The sensitive information gathered by Dragonfish related to the ASEAN Defence Ministers’ Meeting (ADMM) and associated organizations can be seen below:

“Harvests extensive system information from the machine, such as the

following:

• LAN and WAN IP addresses (for the latter, it uses the free IP address

service ipaddress.com)

• Proxy information

• Installed software list

• Process enumeration via tasklist

• List of all the files on the user’s desktop”

([Accenture Security Dragonfish.pdf](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=35b97015fe&attid=0.2&permmsgid=msg-a:r2906060266310513405&th=18f0d5cf095c6ecb&view=att&disp=safe&realattid=f_lvd1f3561&saddbat=ANGjdJ8A4IpVz8o869btzavIWck0NoKpXGgU5tblulRIqHlsbPKXxWjclA6br00O7MM-TWbL5xGLQ8ZOqBRTRWWa6HuBbWYmAp9zv7ohH7TTcSHnBwrfUFQsTRBUNo-8bgyg9QQWmPLuCzmgZ_j-WKb6Cvx6-MYuuG0eTApd7SfBRKq1Pr5JxDQsVNdTs6r688BToUtUvzlQCEjMnQkqOfw7PgKwbxcuzzYdwua4ZbfLX-IBHgekmkstuklb4qPfdxw1cAwKF9w4dqwx44dYPjLyyKVp5Guh1EHk1n7TBrk5vKonAAwvZP2Fc73kTEsdUQ8IP9H-L6Fqzm_2A_9_xzGUxK7I1Yp1bw2m-ks9lBKHWGfiiVrJ5GRQ5fCPtJ-Ky_2qnYCKQGcVNxV7KDGt9cdF4Kq5n6aez4CQTCNKcyKpwteJYOXnF55ggVEB6S2a0y3m5trwRiizQXwvn_lpzDHyHQv2PX0nrH3BrC_alunIzwxPUIr8no1wv4s-7_PSmcsyKLWuT7ypdQ8FFrqtoyLku8PySzib830l8KwVtlfivpQptnTgashbMd014Uk7QbqoI3ZQSK8iZQU7mhslZrZkovGl5ZP4AHKjwrTx0ztgyzY4HeELKDOHH0Zs3FXS8CIe39uGL6WsLXDd9NAiOlvakrO0YyiQEyiWk9GiHyixd3dzuh8_Zr575rVD3gH1TMW1qjHYU92euxo4876nlIOle8bEa4UPxN3BOwR0l9UNUx90ZfFStBivbL03s3rmWeay5GM3Iu5E5ZDINa2D7yBuz0IZbNtNAI2Py1qQN2Dda2cX0ZQsmAa7TzxmJl_xzWpZipPzbyR1WpklbF3Uxqy0Drip5jNT5fYSHNt0h8oaZ_b_rJiuYhBZKkYbkdX7wt49PRfzvRpVUmqUO4camu3gmu9ml03OaRT0YGUKHV9CwambDxQEypJvL7Q3RRMB4OOHlI2KOlNspe60o8Qa8cGAWVT-hL_NxivCuS2rjdjLuPXjRvE2Pz4kByKYAa4))

Based on Dragonfish’s history, the primary objective of extracting these typically include espionage activities aimed at obtaining strategic intelligence for geopolitical advantage or other nefarious purposes.

# Incident Handling Process

## Identification Phase

Detection of the Elise malware may involve monitoring for unusual network activity, through the detection of suspicious network connections to known malicious domains. Additionally, analyzing suspicious files and their activities or the presence of unauthorized processes on critical systems. Identifying indicators of compromise (IoCs) is crucial for initiating an effective incident response and mitigating the impact of attacks.

## Eradication and Recovery Phase

There is a crucial need for strong cybersecurity practices, collaboration with security partners like iDefense assists with being informed on emerging threats, providing an approach that can significantly mitigate the risk of similar attacks in the future. Possible mitigation would include: blocking access to the C2 server- 103.236.150[.]14, requiring patching through the installation of Microsoft Security Update KB2553204 to specifically address the CVE-2017-11882 vulnerability and implore analysts to focus on identifying key artifacts which would enhance detection capabilities.

“For threat hunting, iDefense also suggests that analysts to look for the following artifacts:

• A value named IAStorD in the autorun key

• A file named FXSAPIDebugLogFile.tmp

• A mutex handle named donotbotherme

• thumbcache\_1CD60.db in AppData\Local\Microsoft\Windows\Explorer\”

([Accenture Security Dragonfish.pdf](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=35b97015fe&attid=0.2&permmsgid=msg-a:r2906060266310513405&th=18f0d5cf095c6ecb&view=att&disp=safe&realattid=f_lvd1f3561&saddbat=ANGjdJ8A4IpVz8o869btzavIWck0NoKpXGgU5tblulRIqHlsbPKXxWjclA6br00O7MM-TWbL5xGLQ8ZOqBRTRWWa6HuBbWYmAp9zv7ohH7TTcSHnBwrfUFQsTRBUNo-8bgyg9QQWmPLuCzmgZ_j-WKb6Cvx6-MYuuG0eTApd7SfBRKq1Pr5JxDQsVNdTs6r688BToUtUvzlQCEjMnQkqOfw7PgKwbxcuzzYdwua4ZbfLX-IBHgekmkstuklb4qPfdxw1cAwKF9w4dqwx44dYPjLyyKVp5Guh1EHk1n7TBrk5vKonAAwvZP2Fc73kTEsdUQ8IP9H-L6Fqzm_2A_9_xzGUxK7I1Yp1bw2m-ks9lBKHWGfiiVrJ5GRQ5fCPtJ-Ky_2qnYCKQGcVNxV7KDGt9cdF4Kq5n6aez4CQTCNKcyKpwteJYOXnF55ggVEB6S2a0y3m5trwRiizQXwvn_lpzDHyHQv2PX0nrH3BrC_alunIzwxPUIr8no1wv4s-7_PSmcsyKLWuT7ypdQ8FFrqtoyLku8PySzib830l8KwVtlfivpQptnTgashbMd014Uk7QbqoI3ZQSK8iZQU7mhslZrZkovGl5ZP4AHKjwrTx0ztgyzY4HeELKDOHH0Zs3FXS8CIe39uGL6WsLXDd9NAiOlvakrO0YyiQEyiWk9GiHyixd3dzuh8_Zr575rVD3gH1TMW1qjHYU92euxo4876nlIOle8bEa4UPxN3BOwR0l9UNUx90ZfFStBivbL03s3rmWeay5GM3Iu5E5ZDINa2D7yBuz0IZbNtNAI2Py1qQN2Dda2cX0ZQsmAa7TzxmJl_xzWpZipPzbyR1WpklbF3Uxqy0Drip5jNT5fYSHNt0h8oaZ_b_rJiuYhBZKkYbkdX7wt49PRfzvRpVUmqUO4camu3gmu9ml03OaRT0YGUKHV9CwambDxQEypJvL7Q3RRMB4OOHlI2KOlNspe60o8Qa8cGAWVT-hL_NxivCuS2rjdjLuPXjRvE2Pz4kByKYAa4))

## Lessons Learned Phase

There were a few lessons learned throughout this report, the main one is that Microsoft Word documents can have embedded malicious executables, so users should avoid opening suspicious files and should understand common malware behavior. Additionally, vulnerable government organizations like the ASEAN Defence Ministers’ Meeting are prime targets for cyberattacks and need to be aware of potential threat actors. They need to understand their attractiveness to cyberattack groups, have vast knowledge on their tactics and have strong cybersecurity defenses in place. Lastly, targeted mitigation efforts, such as blocking C2 server access and patching vulnerabilities like CVE-2017-11882, are crucial for effectively mitigating the risk of similar attacks in the future.

# Exploit References

1. Dragonfish's Elise Malware Campaign
2. CVE-2017-11882
3. Operation Lotus Blossom Report by Palo Alto Networks

# References

1. Accenture Security. “Accenture Security Dragonfish Threat Analysis Report”. PDF:

[Accenture Security Dragonfish.pdf](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=35b97015fe&attid=0.2&permmsgid=msg-a:r2906060266310513405&th=18f0d5cf095c6ecb&view=att&disp=safe&realattid=f_lvd1f3561&saddbat=ANGjdJ8A4IpVz8o869btzavIWck0NoKpXGgU5tblulRIqHlsbPKXxWjclA6br00O7MM-TWbL5xGLQ8ZOqBRTRWWa6HuBbWYmAp9zv7ohH7TTcSHnBwrfUFQsTRBUNo-8bgyg9QQWmPLuCzmgZ_j-WKb6Cvx6-MYuuG0eTApd7SfBRKq1Pr5JxDQsVNdTs6r688BToUtUvzlQCEjMnQkqOfw7PgKwbxcuzzYdwua4ZbfLX-IBHgekmkstuklb4qPfdxw1cAwKF9w4dqwx44dYPjLyyKVp5Guh1EHk1n7TBrk5vKonAAwvZP2Fc73kTEsdUQ8IP9H-L6Fqzm_2A_9_xzGUxK7I1Yp1bw2m-ks9lBKHWGfiiVrJ5GRQ5fCPtJ-Ky_2qnYCKQGcVNxV7KDGt9cdF4Kq5n6aez4CQTCNKcyKpwteJYOXnF55ggVEB6S2a0y3m5trwRiizQXwvn_lpzDHyHQv2PX0nrH3BrC_alunIzwxPUIr8no1wv4s-7_PSmcsyKLWuT7ypdQ8FFrqtoyLku8PySzib830l8KwVtlfivpQptnTgashbMd014Uk7QbqoI3ZQSK8iZQU7mhslZrZkovGl5ZP4AHKjwrTx0ztgyzY4HeELKDOHH0Zs3FXS8CIe39uGL6WsLXDd9NAiOlvakrO0YyiQEyiWk9GiHyixd3dzuh8_Zr575rVD3gH1TMW1qjHYU92euxo4876nlIOle8bEa4UPxN3BOwR0l9UNUx90ZfFStBivbL03s3rmWeay5GM3Iu5E5ZDINa2D7yBuz0IZbNtNAI2Py1qQN2Dda2cX0ZQsmAa7TzxmJl_xzWpZipPzbyR1WpklbF3Uxqy0Drip5jNT5fYSHNt0h8oaZ_b_rJiuYhBZKkYbkdX7wt49PRfzvRpVUmqUO4camu3gmu9ml03OaRT0YGUKHV9CwambDxQEypJvL7Q3RRMB4OOHlI2KOlNspe60o8Qa8cGAWVT-hL_NxivCuS2rjdjLuPXjRvE2Pz4kByKYAa4)

1. NIST. “Vulnerability Summary for CVE-2017-11882”. URL:

<https://nvd.nist.gov/vuln/detail/cve-2017-11882>

1. STIX. “Documentation”. URL:

<https://stixproject.github.io/documentation/>