THREAT ANALYSIS

LATEST CYBER ESPIONAGE MALWARE ATTACKS

DRAGONFISH DELIVERS NEW FORM OF **ELISE** MALWARE TARGETING **ASEAN DEFENCE MINISTERS' MEETING** AND ASSOCIATES

The well-known threat group called DRAGONFISH or Lotus Blossom are distributing a new form of Elise malware targeting organizations for espionage purposes. The threat actors associated with DRAGONFISH have previously focused their campaigns on targets in Southeast Asia, specifically those located in countries near the South China Sea. These attacks have mainly targeted high-profile government, military and political institutions, but other victims include those operating in the education and telecommunication industries. iDefense analysts have identified a campaign likely to be targeting members of— or those with affiliation or interest in—the ASEAN Defence Ministers' Meeting (ADMM).

This threat analysis provides security operations center (SOC) analysts and engineers with detailed information pertaining to the workings of the Elise malware family and the indicators of compromise (IoCs) to assist them in their own independent analyses.

This threat analysis will help to inform organizations and support their decision making on how to better contain or mitigate the threat through monitoring or blocking.

They may consider using the information to inform hunting activities for systems that may already have been compromised, or by using the IoCs by adding them to hunting lists or endpoint detection & response (EDR) solutions as well as to network- and host-based backlists to detect and deny malware implantation—and command and control (C2) communication—or whatever mitigations they determine are most appropriate for their environments.

Given the inherent nature of threat intelligence, it is based on information gathered and understood at a specific point in time.

TECHNICAL REPORT

DESCRIPTION

iDefense analysts have identified a campaign likely to be targeting members of or those with affiliation or interest in the ASEAN Defence Minister's Meeting (ADMM). iDefense assesses with high confidence that this campaign is associated with the threat group DRAGONFISH (also known as Lotus Blossom and Spring Dragon).
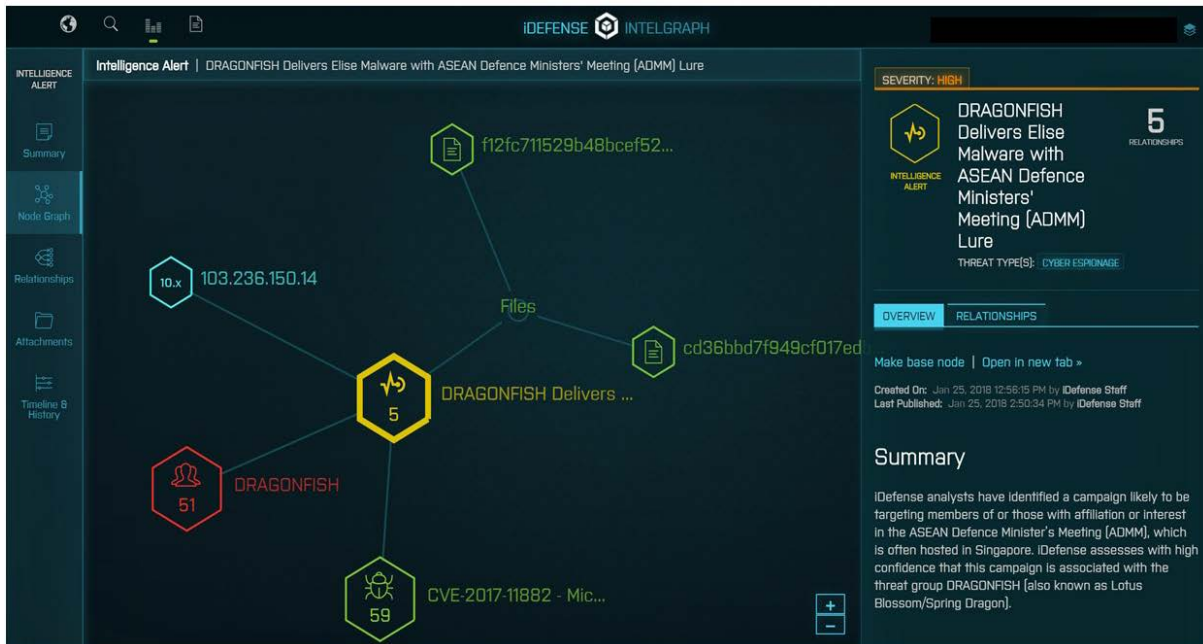
MALWARE ANALYSIS

Knowledge of DRAGONFISH's tactics, techniques, and procedures (TTPs) helps to better inform detection and response to attacks by this threat group.

The sample iDefense identified is a malicious Microsoft Corp. Word document (see Exhibit 1) with the following properties:

- MD5: f12fc711529b48bcef52c5ca0a52335a
- Author: mary
- Last Modified by: mary
- Created Time Stamp: 2018:01:19 14:56:00 (Jan. 19, 2018, 2:56 p.m.)
- Last Modified Time Stamp: 2018:01:19 14:56:00 (JAn. 19, 2018, 2:56 p.m.)

Exhibit 1: Decoy Document

The Word document, which includes information on ADMM-Plus members, has a malicious executable file embedded as an OLE object (see Exhibit 2).

Exhibit 2: Original Source Path

```
id |index      |OLE Object                |OLE Package
---+-----------+--------------------------+---------------------------------
0  |0000326Fh  |format_id: 2 (Embedded)   |Filename: 'a.b'
   |           |class name: 'Package'     |Source path: 'E:\\office\\a.b'
   |           |data size: 72889          |Temp path = 'C:\\Users\\mary\\A
   |           |                          |ppData\\Local\\Temp\\a.b'
---+-----------+--------------------------+---------------------------------
```

The embedded file named a.b is dropped to the %temp% folder once the Word document is opened and is executed by exploiting the CVE-2017-11882 vulnerability. The payload is consequently moved to \AppData\Roaming\Microsoft\Windows\Caches\ as a file named NavShExt.dll and the executable a.b is deleted.

This file NavShExt.dll is a PE32 dynamic-link library (DLL), and the filename suggests that the malware author intended to disguise the file as a legitimate Symantec Corp. anti-virus component called the Norton Security Shell Extension Module.
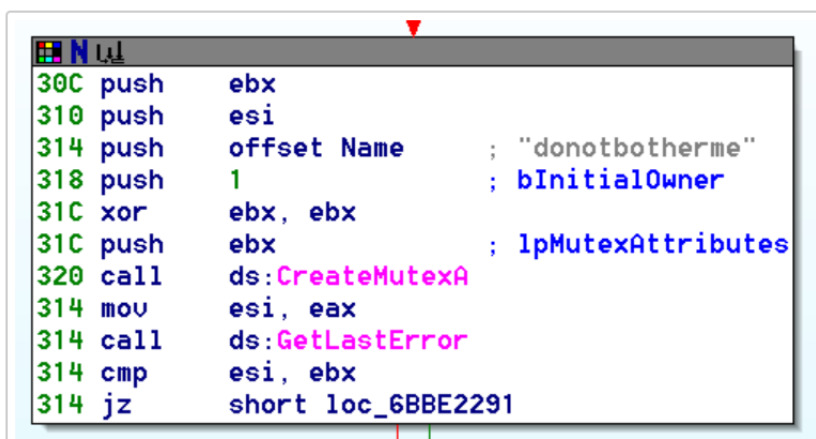
The DLL has the following properties:

- MD5 Hash: cd36bbd7f949cf017edba0e6aaadf28c

- Compile Time: 2018-01-12 17:59:58 (Jan. 12, 2018, 5:59 p.m.)

- Export Function: Setting

The malware performs the following set of actions:

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

7. 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

Exhibit 3: Mutex Creation


```
    N
30C push      ebx
310 push      esi
314 push      offset Name      ; "donotbotherme"
318 push      1                ; bInitialOwner
31C xor       ebx, ebx
31C push      ebx              ; lpMutexAttributes
320 call      ds:CreateMutexA
314 mov       esi, eax
314 call      ds:GetLastError
314 cmp       esi, ebx
314 jz        short loc_6BBE2291
```

Based on the currently available intelligence we also believe the malware is capable of providing the attacker with a remote shell on the host and can completely uninstall itself.

Execution debug messages are stored in the %temp% folder in a file named FXSAPIDebugLogFile.tmp. Example messages include Client Start!, indicating a

successful infection, or an error message such as [2018-1-25 13:35:22] Try All Addr Failed! Sleep For: 10.100000 Minutes!, indicating that the C2 sever cannot be reached and the malware will sleep for a fixed amount of time.

Logs are encrypted using the following static AES key: Ss)4:WKsRr(3/VJrQq&2.UIqPp%1-THp.

Of particular interest is an embedded, custom application in a .data section that is responsible for loading and executing executables and DLLs from inside the main binary. The application supports the following command-line options:

- runexe 1.exe /c command...
- rundll 1.dll, DllMain

When attempting to find more information about this application, iDefense discovered a file with the MD5 hash cfa7954722d4277d26e96edc3289a4ce, which features the same application and was mentioned in a 2015 report titled *Operation Lotus Blossom* by the Unit42 team at partner organization Palo Alto Networks.

Several observations detailed in this report on Elise variant C align with the findings disclosed above:

- Similar targeting of Southeast Asia
- Same export function name in the dropper DLL: Setting
- Identical custom application to load and execute EXEs or DLLs
- Heavy anti-virtual-machine features
- Similar obfuscation techniques used to exfiltrate data to C2 server (using base64-encoded cookie values)

In contrast to the earlier campaigns, debug paths are completely stripped. Persistence is achieved using the Run Registry key with the value name IAStorD:

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

As mentioned earlier, two hidden DLLs can be discovered that are additionally injected into iexplore.exe and have the export functions named DePatchEntry or EvilEntry. These DLLs provide additional loading and other anti-analysis functionalities.

The malware attempts to spoof the host and query non-existing domains, such as the following:

- 3qyo4o7.7r7i3[.]info
- dtdf5vu.nt7yq[.]info
- j.4tc3ldw.g9ml.www0[.]org
- 38qmk6.0to9[.]info
- ubkv1t.ec0[.]com

- 7g91xhp.envuy3[.]net

- l.hovux.eln9wj7.7gpj[.]org

- w.7sytdjc.wroi.cxy[.]com

This is likely done to throw off malware analysts or network administrators. The real C2 server, 103.236.150[.]14, is actually hardcoded (see Exhibit 4).

Exhibit 4: Real C2 Server Hardcoded in the Malware

MITIGATION

To mitigate the threat of the described campaign, security teams can consider blocking access to the C2 server 103.236.150[.]14 and, where applicable, ensure that the Microsoft Security Update KB2553204 is installed in order to patch the CVE-2017-11882 vulnerability.

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\

For further information regarding the Microsoft Security Update KB25533204, please visit:

https://support.microsoft.com/en-us/help/2553204/description-of-the-security-update-for-office-2010-november-14-2017

Given the inherent nature of threat intelligence, the content contained in this alert is based on information gathered and understood at the time of its creation. It is subject to change.

ACCENTURE PROVIDES THE INFORMATION ON AN "AS-IS" BASIS WITHOUT REPRESENTATION OR WARRANTY AND ACCEPTS NO LIABILITY FOR ANY ACTION OR FAILURE TO ACT TAKEN IN RESPONSE TO THE INFORMATION CONTAINED OR REFERENCED IN THIS REPORT.

CONTACT US

For additional mitigation steps and more detailed information, please reach out to your Accenture contact. Where support is needed, Accenture Security can provide resources designed to mitigate risks and remediate gaps in ICS security programs.

Kelly Bissell
kelly.bissell@accenture.com

Joshua Ray
joshua.a.ray@accenture.com

Uwe Kissman
uwe.kissman@accenture.com

Ryan LaSalle
ryan.m.lasalle@accenture.com

Gareth Russell
gareth.russell@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 435,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.