Andariel 그룹의 새로운 공격 활동 분석 - ASEC

By ATCP

Published: 2023-08-22 · Archived: 2026-04-05 18:00:50 UTC

목차

주로 국내 기업 및 기관들을 공격 대상으로 하는 Andariel 위협 그룹은 Lazarus 위협 그룹과 협력하는 관계이거나 혹은 Lazarus 그룹의 하위 조직으로 알려져 있다. 2008년부터 국내 대상 공격이 최초로 확인되었으며 주요 공격 대상으로는 국방, 정치기구, 조선, 에너지, 통신 등 안보와 관련된 곳이다. 물론 이외에도 대학교나 운송, ICT 업체 등 국내에 위치한 다양한 기업 및 기관들이 공격 대상이 되고 있다. [1]

Andariel 위협 그룹은 최초 침투 과정에서 주로 스피어 피싱 공격이나 워터링 홀 공격 그리고 공급망 공격을 이용하며, 이외에도 악성코드 설치 과정에서 중앙관리 솔루션을 악용하는 사례도 존재한다. [2]
Andariel 그룹의 특징 중 하나라면 다양한 악성코드를 제작해 공격에 사용하는 점인데 특히 과거 공격에 사용된 Andarat, Andaratm, Phandoor, Rifdoor 외에도 수년 전부터 확인되고 있는 TigerRAT [3], MagicRAT [4] 등 백도어 유형이 많다.

ASEC(AhnLab Security Emergengy response Center)에서는 Andariel 위협 그룹의 공격을 지속적으로 모니터링하고 있으며, 최근 Andariel 그룹의 공격으로 추정되는 공격 사례들이 확인되어 관련 내용들을 블로그에 공개한다. 참고로 해당 공격 사례들에서는 이전 공격에서 확인된 악성코드들이나 C&C 서버가 사용되지 않았기 때문에 직접적인 연관 관계는 존재하지 않는다. 이에 따라 해당 공격들과 Andariel 위협 그룹의 연

관성을 확인하기 위해 먼저 2023년 상반기 Andariel 그룹의 공격 사례들을 분석한 후 이를 기반으로 연관 관계를 정리하며, 필요할 경우 이보다 이전 공격 사례에서 확인된 내용들도 포함한다.

2023년에 확인된 공격들의 특징으로는 Go 언어로 개발된 악성코드들이 다수 확인된다는 점이다. 과거 Innorix Agent를 악용한 공격 사례에서는 Go 언어로 개발된 Reverse Shell이 사용되었으며, 이후 국내 기업들을 대상으로 한 공격에서는 Black RAT이 사용되었다. 이러한 경향은 최근 공격 사례까지 이어져 Goat RAT, DurianBeacon 등 Go 언어로 개발된 또 다른 악성코드들이 공격에 사용되고 있다. 참고로 DurianBeacon은 Go 버전 외에도 Rust 언어로 개발된 버전이 함께 존재하는 것이 특징이다.

```
.rdata:00000000006CFED3 aGDevGoDurianbe db 'G:/Dev/Go/DurianBeacon/Command.go',0
.rdata:00000000006CFED3                                         ; DATA XREF: .rdata:00000000006CAA64↑o
.rdata:00000000006CFEF5 aGDevGoDurianbe_0 db 'G:/Dev/Go/DurianBeacon/SSL.go',0
.rdata:00000000006CFEF5                                         ; DATA XREF: .rdata:00000000006CAAD8↑o
.rdata:00000000006CFF13 aGDevGoDurianbe_1 db 'G:/Dev/Go/DurianBeacon/Utils.go',0
.rdata:00000000006CFF13                                         ; DATA XREF: .rdata:00000000006CAB94↑o
.rdata:00000000006CFF33 aGDevGoDurianbe_2 db 'G:/Dev/Go/DurianBeacon/main.go',0
```

Figure 1. Go 언어로 개발된 DurianBeacon의 소스 코드 정보

최초 유포 사례가 직접적으로 확인되지 않기 때문에 본 포스팅에서는 공격에 사용된 악성코드들을 기반으로 분석을 진행한다. 참고로 다양한 악성코드들이 공격에 사용되는데, 악성코드 제작자가 지정한 이름이 확인될 경우에는 해당 이름을 사용하며 그렇지 않을 경우에는 유사 악성코드나 자사의 진단명을 명시하는 방식으로 정리한다.

1. 과거 공격 사례

1.1. Innorix Agent 악용 사례

2023년 2월 ASEC에서는 “취약한 Innorix 악용한 악성코드 유포 : Andariel” 블로그를 통해 Andariel 위협 그룹이 취약한 버전의 Innorix Agent 사용자를 대상으로 악성코드를 유포한 정황을 공개하였다. [5] 유포에 악용된 Innorix Agent 프로그램은 파일 전송 솔루션 클라이언트 프로그램으로, 한국인터넷진흥원(KISA)에서 취약점 관련 내용을 게시하고 보안 업데이트가 권고된 INNORIX Agent 9.2.18.450 및 이전 버전들로 확인되었다. [6]

Target Type	File Name	File Size	File Path
Current	innorixas.exe	8.17 MB	%SystemDrive%\innorix_agent\innorixas.exe
Target	msdes.exe.irx	40.5 KB	%SystemDrive%\users\%ASD%\msdes.exe.irx

Process	Module	Target	Data
innorixas.exe	N/A	N/A	msdes.exe.irx
innorixas.exe	N/A	N/A	http://4.246.144.112/update.exe

Figure 2. 취약한 Innorix Agent를 이용한 악성코드 유포 정황

위의 공격 사례를 통해 공격에 사용된 악성코드들을 조사한 결과 다수의 국내 대학교에서 악성코드들이 감염되었던 것을 확인하였다. 공격에 사용된 악성코드들은 대부분 백도어 유형이며 모두 이전에 알려진 유형은 존재하지 않는다. 하지만 과거 사용되었던 다른 악성코드나 이후 공격에 사용된 악성코드들과의 연관성이 존재하기 때문에 여기에서는 간략하게 특징을 정리한다.

1.1.1. NukeSped 변종 – Volgmer

과거 블로그에서도 언급했다시피 해당 악성코드는 C&C 서버와의 통신 과정에서 패킷을 암호화하기 위해 다음과 같은 0x10 바이트 키를 사용했다. 해당 키 값은 미국의 사이버인프라보안청(CISA) 보고서에서 Hidden Cobra (Lazarus) 위협 그룹의 Volgmer 악성코드에서 사용한 키 값과 동일하다. [7] (현재 접속 불가)

- **Key : 74 61 51 04 77 32 54 45 89 95 12 52 12 02 32 73**

Volgmer는 상대적으로 최근까지도 공격에 사용되고 있으며 레지스트리 “HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security” 키에 저장된 설정 데이터를 읽어 동작하고 C&C 서버와의 통신에 HTTP 프로토콜을 사용한다. 이러한 점은 과거 CISA 보고서에서 언급한 유형과 거의 유사한데, 이는 Volgmer는 별다른 변형 없이 지속적으로 공격에 사용되고 있다는 것을 의미한다. 또한 해당 악성코드에서 Volgmer와 동일한 키 값이 사용되었지만 이 악성코드가 C&C 서버와의 통신 패킷을 암호화하는데 해당 키 값을 사용하는 것과 달리 Volgmer는 레지스트리에 암호화되어 저장된 설정 데이터를 복호화하는데 사용하였다는 차이점이 존재한다.

이에 따라 위 악성코드를 Volgmer 유형으로 분류하기에는 한계가 있어 NukeSped 변종으로 분류한다. 기본적인 기능만을 제공하는 상대적으로 단순한 형태의 백도어이며 자가 삭제 과정에서 사용되는 Batch 스크립트가 기존 NukeSped 유형과 유사한 점이 특징이다.

```
.rdata:000000014001E248 aHelloServer    db 'Hello Server'       ; DATA XREF: fn_initComm+29↑r
.rdata:000000014001E248                                         ; fn_initComm+3A↑r
.rdata:000000014001E254 byte_14001E254  db 0                    ; DATA XREF: fn_initComm+43↑r
.rdata:000000014001E255                 align 8
.rdata:000000014001E258 ; const char Str2[]
.rdata:000000014001E258 Str2            db 'Hello Client',0     ; DATA XREF: fn_initComm:loc_14000143A↑o
.rdata:000000014001E265                 align 8
.rdata:000000014001E268 ; const char Source[]
.rdata:000000014001E268 Source          db 'uninstall.bat',0    ; DATA XREF: sub_1400017A0+41↑o
.rdata:000000014001E276                 align 8
.rdata:000000014001E278 ; const char data_SelfDelBat[]
.rdata:000000014001E278 data_SelfDelBat db ':L1',0Dh,0Ah        ; DATA XREF: sub_1400017A0+B1↑o
.rdata:000000014001E27D                 db 'del /F "%s"',0Dh,0Ah
.rdata:000000014001E28A                 db 'if exist "%s" goto L1',0Dh,0Ah
.rdata:000000014001E2A1                 db 'del /F "%s"',0Dh,0Ah,0
.rdata:000000014001E2AF                 align 10h
```

Figure 3. 자가 삭제 과정에서 사용되는 Batch 스크립트

1.1.2. Andardoor

닷넷으로 개발되었으며 TestProgram이라는 이름을 갖는 백도어 악성코드이다. 자사 진단명을 기반으로 Andardoor로 분류하며 Dotfuscator 도구를 이용해 난독화된 것이 특징이다. 파일 작업, 프로세스 작업, 명령 실행, 스크린샷 캡쳐 등 감염 시스템을 제어할 수 있는 여러 기능들을 지원한다. C&C 서버와의 통신에는 SSL을 이용한 암호화가 사용되며 서버 이름으로 “clientName”이라는 문자열을 지정하였다.

Figure 4. C&C 서버와의 SSL 통신 루틴

1.1.3. 1th Troy Reverse Shell

1th Troy는 Go 언어로 개발된 Reverse Shell 악성코드이다. 바이너리에 포함된 다음 문자열을 통해 악성코드가 “Reverse_Base64_Pipe”라는 단순한 이름이며 악성코드 제작자는 이를 “1th Troy”로 분류한 것을 확인할 수 있다.

> G:/Code/01__1th Troy/Go/Reverse_Base64_Pipe/Client/client.go

기본적인 명령만을 제공하는 Reverse Shell 답게 지원하는 명령은 “cmd”, “exit”, “self delete”가 있으며, 각각 명령 실행, 프로세스 종료, 자가 삭제 기능을 지원한다.

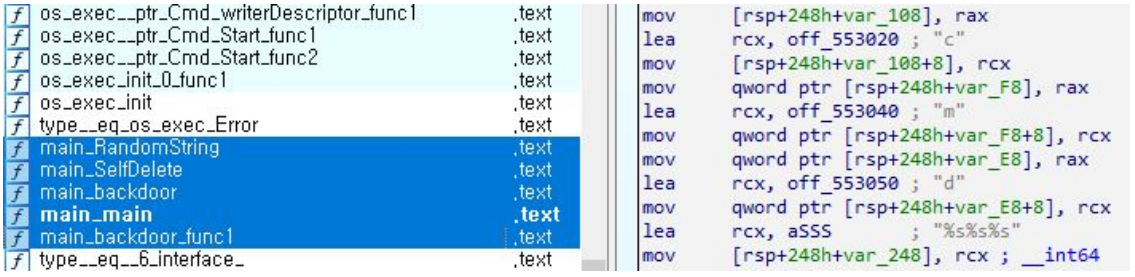

Figure 5. 단순한 형태의 리버스 쉘

1.2. 국내 기업 공격 사례

Andariel 그룹은 2023년 3월에도 국내 방산 업체 및 전자 장비 업체를 공격하여 악성코드들을 유포하였다. 최초 침투 방식은 확인되지 않지만 자사 AhnLab Smart Defense (ASD) 인프라를 통해 mshta.exe 프로세스가 TigerRat을 설치한 로그와 mshta.exe 프로세스를 종료시키는 로그가 확인된다. 이는 스크립트 악성코드를 통해 설치된 것을 의미하며 스피어 피싱 공격이 사용된 것으로 보인다.

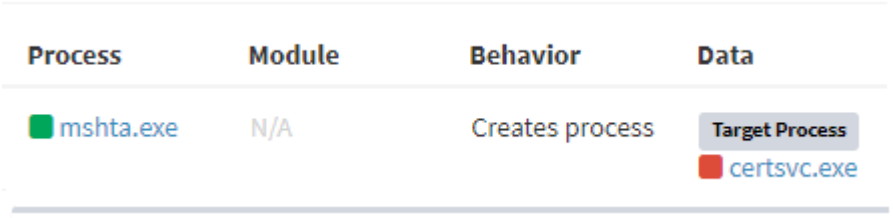

Figure 6. TigerRAT을 설치하는 mshta 프로세스

공격에 사용된 악성코드들은 주로 백도어이며 과거부터 Andariel 그룹이 사용하는 TigerRat이 함께 사용되었다.

1.2.1. TigerRat

TigerRat은 과거 한국인터넷진흥원(KISA)에서 이름붙인 RAT 악성코드로서 [8] 2020년 경부터 최근까지 Andariel 위협 그룹이 공격에 꾸준히 사용하고 있다. 일반적으로 스피어 피싱 메일에 첨부된 악성 매크로 문서 파일이나 워터링 홀 공격을 통해 유포된 것으로 알려져 있다. [9] Andariel 그룹은 취약한 버전의 VMware Horizon 제품을 사용하는 국내 기업을 대상으로 Log4Shell 취약점 공격을 수행해 TigerRat을 설치한 사례도 존재한다. [10]

TigerRat은 파일 작업, 명령 실행과 같은 기본적인 기능들 외에도 정보 수집, 키로깅, 스크린 캡쳐, 포트 포워딩 등 다양한 기능들을 지원하는 백도어 악성코드로서 C&C 서버와 최초로 통신할 때 인증 과정이 존재하는 것이 특징이다. 과거 버전에서는 인증 시 다음과 같이 SSL 통신을 위장한 문자열을 사용하였다. 악성코드에 따라 “HTTP 1.1 /member.php SSL3.4” 또는 “HTTP 1.1 /index.php?member=sbi2009 SSL3.3.7” 문자열을 C&C 서버에 전달한 이후 C&C 서버로부터 “HTTP 1.1 200 OK SSL2.1” 문자열을 전달받을 경우에만 인증에 성공한다.

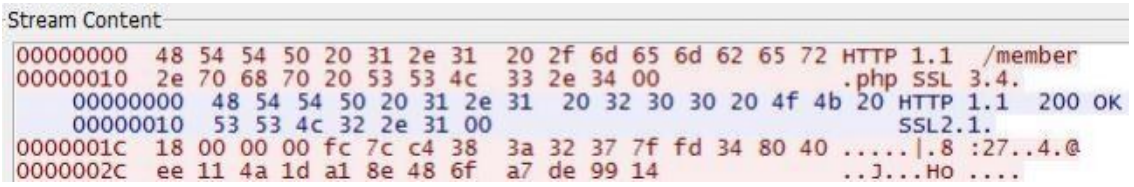

Figure 7. C&C 서버와의 인증에 사용된 문자열 – 과거 버전

하지만 이번에 확인된 TigerRAT은 다음과 같이 랜덤한 0x20 크기의 문자열이 사용된다. 해당 문자열들은 “fool”(dd7b696b96434d2bf07b34f9c125d51d), “iwan”(01ccce480c60fcdb67b54f4509ffdb56)에 대한 MD5 해시로 추정되며, 공격자는 네트워크 진단을 우회하기 위해 인증 과정에서 랜덤한 문자열을 사용한 것으로 보인다.

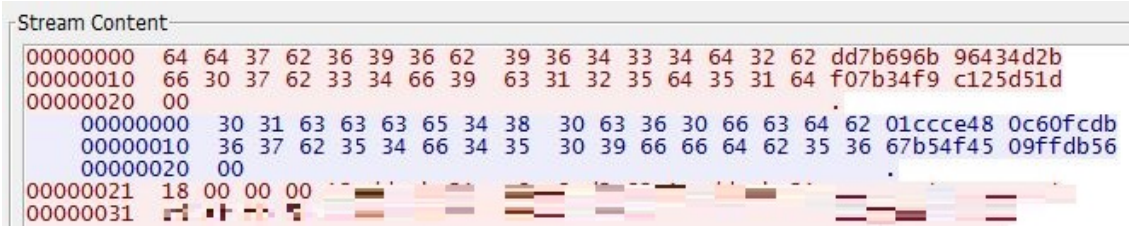

Figure 8. C&C 서버와의 인증에 사용된 문자열 – 최신 버전

- **C&C 요청 문자열 : dd7b696b96434d2bf07b34f9c125d51d**
- **C&C 응답 문자열 : 01ccce480c60fcdb67b54f4509ffdb56**

1.2.2. Black RAT

Black RAT은 공격자가 제작한 것으로 추정되는 백도어 악성코드로서 다른 악성코드들처럼 Go 언어로 제작되었다. 이전 공격에서 확인된 1th Troy 리버스 쉘은 단순한 명령 실행 기능만 지원하지만 Black RAT은

명령 실행 외에도 파일 다운로드, 스크린 캡쳐와 같은 다양한 기능들을 지원한다.

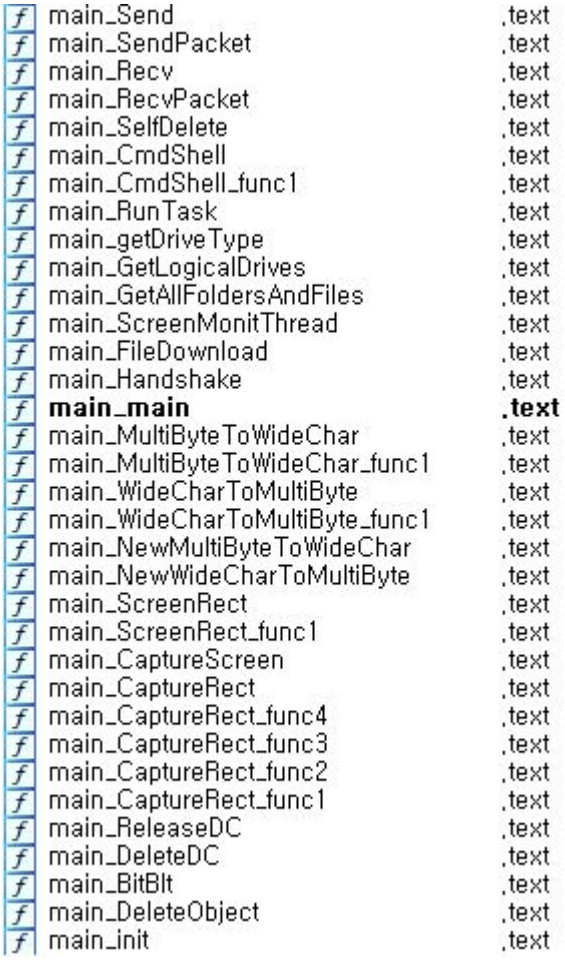

Figure 9. Black RAT이 지원하는 기능들

바이너리에 포함된 다음 문자열을 보면 악성코드 제작자가 해당 악성코드를 RAT으로 분류하였으며 이름을 Black으로 지정한 것을 알 수 있다.

I:/01___Tools/02__RAT/Black/Client_Go/Client.go

1.2.3. NukeSped 변종

해당 공격에서도 전형적인 NukeSped 백도어가 사용되었다. 지원하는 기능은 네트워크 스캐닝, 프로세스 및 파일 조회, 파일 업로드 / 다운로드, 명령 실행 등이 있다. 사용할 API들의 이름은 다음과 같이 암호화되어 있으며 이를 복호화한 이후에 직접 구해서 사용한다. 복호화에는 0x26 사이즈의 키가 사용된다.

```
str_kernel32_dll = fn_decStr("wVWN7BLxxfV1HBby");
kernel32_dll = LoadLibraryA(str_kernel32_dll);
free(str_kernel32_dll);
if ( kernel32_dll )
{
  GetProcAddress = fn_decStr("zVWL0gXylYY/HAj7Olk=");
  GetProcAddress_0 = ::GetProcAddress(kernel32_dll, GetProcAddress);
  free(GetProcAddress);
  LoadLibrary = fn_decStr("xl+e5jv0lLU6CgPf");
  ::LoadLibrary = GetProcAddress_0(kernel32_dll, LoadLibrary);
  free(LoadLibrary);
  GetModuleFileNameA = fn_decStr("zVWLzxj5g6s+PhPyLGTnHtvG");
  ::GetModuleFileNameA = GetProcAddress_0(kernel32_dll, GetModuleFileNameA);
  free(GetModuleFileNameA);
  DeleteFileW = fn_decStr("zlWT5wP4sK43HS0=");
  ::DeleteFileW = GetProcAddress_0(kernel32_dll, DeleteFileW);
  free(DeleteFileW);
  CreateThread = fn_decStr("yUKa4wP4oq8pHRv6");
  ::CreateThread = GetProcAddress_0(kernel32_dll, CreateThread);
  free(CreateThread);
  CreateFileA = fn_decStr("yUKa4wP4sK43HTs=");
  ::CreateFileA = GetProcAddress_0(kernel32_dll, CreateFileA);
  free(CreateFileA);
  v11 = fn_decStr("yUKa4wP4sK43HS0=");
```

Figure 10. 난독화된 API 문자열

- **복호화에 사용되는 키 값 : i<6fu>-0|HSLRCqd.xHqMB]4H#axZ%5!5!?SQ&**

해당 NukeSped 변종에서도 자가 삭제를 위한 Batch 스크립트가 사용되는데 이전 공격에서 사용된 유형과는 약간의 차이가 존재한다.

```
.rdata:0000000140020590 aSSCS:                                  ; DATA XREF: comm_execCmd+196↑o
.rdata:0000000140020590                 text "UTF-16LE", '%s\%S /c "%s"',0
.rdata:00000001400205AC                 align 10h
.rdata:0000000140020580 ; const size_t BufferCount
.rdata:0000000140020580 BufferCount     db '@echo off',0Dh,0Ah  ; DATA XREF: fn_selfDel+1E8↑o
.rdata:0000000140020588                 db ':L1',0Dh,0Ah
.rdata:00000001400205C0                 db 'del "%s"%s "%s" goto L1',0Dh,0Ah
.rdata:00000001400205D9                 db 'del "%s"',0Dh,0Ah,0
.rdata:00000001400205E4                 align 8
```

Figure 11. 자가 삭제 과정에서 사용되는 Batch 스크립트

확인된 NukeSped 변종은 두 종류인데 각각 Reverse Shell 방식과 Bind Shell 방식이다. Bind Shell형태도 Reverse Shell 형태와 동일하게 사용하는 포트 즉 Listen하는 포트 번호는 10443번이다. 해당 NukeSped는 TigerRat과 유사하게 C&C 서버와 통신하기 이전에 인증 과정을 거치는데, TigerRat이 SSL 통신을 위장하였다면 NukeSped는 HTTP 통신을 위장하였다. 즉 아래와 같은 POST 요청을 전송한 후 정확히 매칭되는 HTTP 응답이 올 때에만 C&C 서버와 통신을 진행한다.

Figure 12. 인증에 사용되는 HTTP 패킷

2. 최근 공격 사례

ASEC에서는 Andariel 그룹의 공격을 모니터링하고 있으며 최근 Innorix Agent가 악성코드를 설치하는데 악용되고 있는 사례를 확인하였다. Innorix Agent가 악성코드를 다운로드하는 방식이었던 이전 사례와 달리 직접 생성하는 방식이기 때문에 취약점 공격인지는 알 수 없으며 단순하게 악용된 것일 수 있다.

해당 공격에서 확인된 악성코드들은 기존에 Andariel 그룹이 사용한 유형은 아니지만 Innorix가 공격에 사용된 점 외에도 공격 대상이 국내 대학교들인 점은 과거 공격 사례와 유사하다. 이외에도 비슷한 시점에 국내 ICT 기업과 전자 장비 업체, 조선, 제조업 등 다양한 기업들을 대상으로 한 공격 사례가 확인되었으며 분석 결과 Innorix 악용 공격 사례에서 사용된 악성코드들과의 연관성을 확인할 수 있었다.

여기에서는 먼저 각각의 공격 사례와 공격 과정에서 사용된 악성코드들을 분석한다. 이후 각각의 공격 사례를 동일한 공격자의 소행으로 보고 있는 근거를 정리한 이후 해당 공격들과 과거 Andariel 위협 그룹의 공격 사례들과의 연관성을 정리한다.

2.1. Innorix Agent 악용 사례

2.1.1. Goat RAT

최근 국내 대학교들을 대상으로 한 공격에서 Innorix Agent가 악성코드를 설치했던 사례가 확인되었다. Innorix Agent는 “iexplorer.exe”라는 이름으로 악성코드를 설치하였는데 이는 과거부터 Andariel 그룹이 자주 사용하는 이름들 중 하나이다.

Target Type	File Name	File Size	File Path
Current	innorixas.exe	7.93 MB	%SystemDrive%\innorix_agent\innorixas.exe
Target	iexplore.exe.irx	2.07 MB	%SystemDrive%\users\%ASD%\downloads\iexplore.exe.irx

Process	Module	Target	Behavior	Data
innorixas.exe	N/A	N/A	Creates executable file	iexplore.exe.irx
innorixas.exe	N/A	N/A	Changes executable file name	iexplore.exe.irx

Figure 13. Innorix Agent를 악용하여 Goat RAT을 설치

공격에 사용된 악성코드는 Go 언어로 개발된 악성코드이며 다음과 같은 같은 원본 소스 코드 정보를 확인할 수 있다.

E:/Projects/Malware/6_Goat_23/Goat/Goat.go
E:/Projects/Malware/6_Goat_23/Goat/define.go
E:/Projects/Malware/6_Goat_23/Goat/anti-vaccine.go
E:/Projects/Malware/6_Goat_23/Goat/command.go

비록 이전 공격에 사용된 Go 기반 백도어 악성코드들과 달리 난독화되어 있지만 기본적인 파일 작업이나 자가 삭제와 같은 기능들을 확인할 수 있으며, 실제 다음과 같은 명령들을 실행한 로그도 확인된다.

> cmd /c tasklist
> cmd /c ipconfig /all

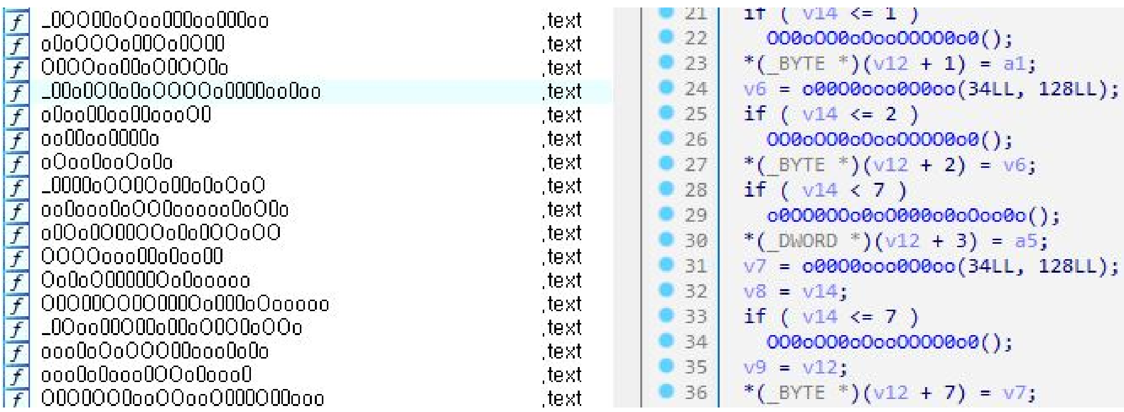

Figure 14. 난독화된 함수 이름

2.2. 국내 기업 공격 사례

2.2.1. AndarLoader

ASEC에서는 Innorix Agent를 악용한 공격 사례와 별개로 유사한 시점에 또 다른 공격을 확인하였다. 최초 유포 경로는 확인되지 않지만 공격에 사용된 악성코드는 위에서 Andardoor로 분류한 닷넷 악성코드와 동일하게 Dotfuscator 도구를 이용해 난독화되었으며 C&C 서버와 SSL 통신을 하는 점도 동일하다. C&C 서버와 연결 시에는 “clientName”를 사용했던 Andardoor와 달리 “sslClient” 문자열이 사용된다.

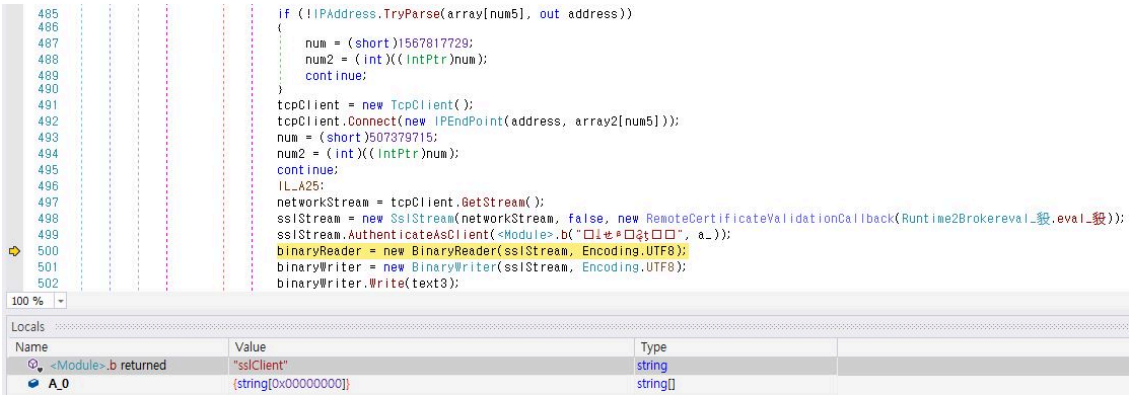

Figure 15. C&C 서버와의 SSL 연결 과정

대부분의 기능들이 직접 구현되어 있던 Andardoor 악성코드와 달리 해당 악성코드는 외부에서 닷넷 어셈블리와 같은 실행 가능한 데이터를 받아 실행하는 다운로더 기능이 전부이다. C&C 서버로부터 전달받은 명령들 중 다음과 같은 명령에 따라 전달받은 코드를 실행하거나 종료할 수 있다. 공격자가 AndarLoader를 이용해 수행한 행위 중에는 미미카츠를 감염 시스템에 설치하는 로그도 확인된다.

분석 당시에는 C&C 서버와 연결이 불가하여 실질적인 기능을 담당하는 부분은 확인하지 못했기 때문에 기존 Andardoor와의 직접적인 유사성은 확인되지 않지만 동일한 난독화 도구를 사용한 점이나 C&C 서버와의 통신 과정이 유사하여 여기에서는 AndarLoader 유형으로 분류하였다.

명령	기능
alibaba	다운로드한 닷넷 어셈블리 실행
facebook	다운로드한 닷넷 메쏘드 실행
exit	종료
vanish	자가 삭제 및 종료

Table 1. 수행 가능한 명령 목록

AndarLoader가 공격자의 명령을 받아 실행한 명령들 중에는 mshta.exe 프로세스를 종료시키는 명령이 존재한다. AndarLoader가 파워쉘을 이용해 설치된 점이나 mshta.exe 프로세스와 관련된 점을 보면 최초 유입 경로가 위에서 다룬 공격 사례처럼 스피어 피싱 공격일 가능성을 보여준다.

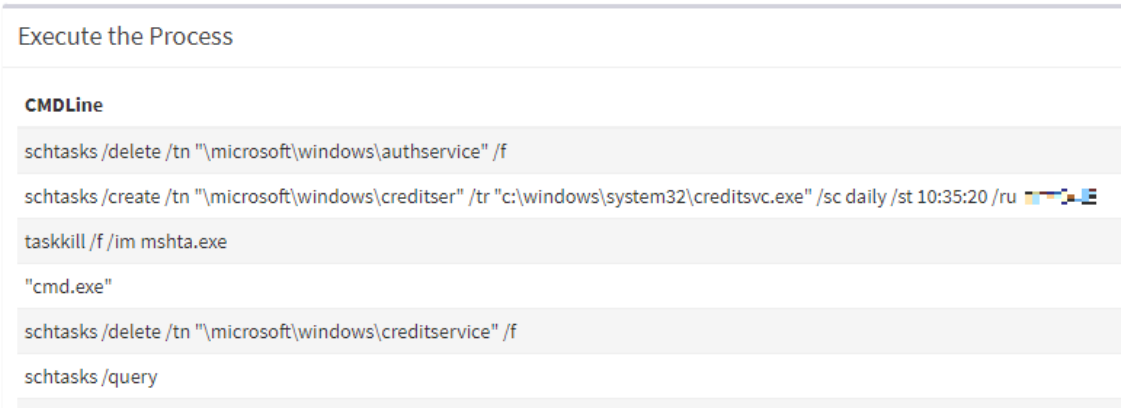

Figure 16. AndarLoader가 실행한 명령

참고로 AndarLoader에 감염된 시스템에는 다음과 같이 mshta.exe 프로세스가 C&C 서버에 접속하는 로그도 함께 확인된다.

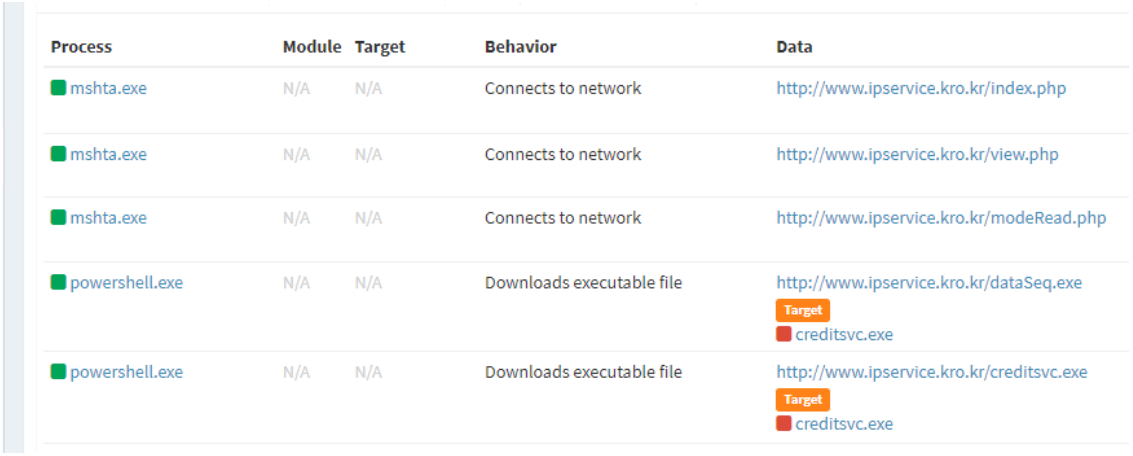

Figure 17. 네트워크 통신 로그

C&C 주소 및 다운로드 주소로 kro.kr 도메인이 사용되었는데 이는 일반적으로 Kimsuky 위협 그룹에서 자주 사용하는 도메인이다. 또한 공격 과정에서 RDP 연결을 위해 Ngrok를 설치한 점도 Kimsuky 위협 그룹의 공격 패턴과 유사하다.

```
"targetProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "service.exe",
      "fileSize": 24948456,
      "filePath": "%SystemDrive%\\users\\%ASD%\\service.exe",
    "commandLine": "%SystemDrive%\\users\\%ASD%\\service.exe  tcp 3389"
  }
},
"currentProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "cmd.exe",
      "fileSize": 289792,
      "filePath": "%SystemRoot%\\system32\\cmd.exe",
    }
  }
},
"parentProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "mshta.exe",
      "fileSize": 43520,
      "filePath": "%SystemRoot%\\system32\\mshta.exe",
    }
```


Figure 18. 설치한 Ngrok를 실행하는 로그

2.2.2. DurianBeacon

AndarLoader 악성코드를 조사하던 중 공격 과정에서 DurianBeacon이라는 이름의 악성코드가 함께 사용된 것이 확인되었다. DurianBeacon은 Go 언어로 개발된 형태와 Rust 언어로 개발된 형태 2가지가 확인되며, 모두 백도어 악성코드로서 C&C 서버로부터 공격자의 명령을 받아 악성 행위를 수행할 수 있다.

A. Go 버전

바이너리에 포함된 다음 문자열을 통해 악성코드 제작자가 해당 악성코드를 DurianBeacon이라는 이름으로 제작한 것을 알 수 있다.

> G:/Dev/Go/DurianBeacon/Command.go
> G:/Dev/Go/DurianBeacon/SSL.go
> G:/Dev/Go/DurianBeacon/Utils.go
> G:/Dev/Go/DurianBeacon/main.go

Go 언어로 개발된 DurianBeacon은 C&C 서버와의 통신 시 SSL 프로토콜을 사용한다. 최초 접속 이후 감염 시스템의 IP 정보, 사용자 이름, 데스크탑 이름, 아키텍처, 파일명을 전송한 후 명령을 대기하며 명령 전달 시 결과를 반환한다. 지원하는 기능들 중에는 감염 시스템의 기본적인 정보를 수집하는 기능 외에 파일 다운로드 / 업로드, 조회, 명령 실행 등의 기능들이 존재한다.

Figure 19. DurainBeacon이 지원하는 기능들

SSL 프로토콜을 이용하기 때문에 통신 패킷은 암호화되어 있지만 내부적으로는 다음과 같은 패킷 구조가 사용된다.

오프셋	사이즈	설명
0x00	0x04	명령 번호
0x04	0x04	명령 인자의 사이즈
0x08	가변	명령 인자

Table 2. DurianBeacon의 명령 패킷 구조

각각의 명령 번호에 해당하는 기능들은 다음과 같다.

명령	기능
0x00	Hibernate
0x01	Interval
0x02	명령 실행 (결과 반환)
0x03	디렉터리 조회

명령	기능
0x04	드라이브 정보
0x05, 0x06, 0x07, 0x08	파일 업로드
0x09, 0x0A, 0x0B	파일 다운로드
0x0C	디렉터리 생성
0x0D	파일 삭제
0x0E	명령 실행
0x0F	종료

Table 3. DurianBeacon의 명령 목록

명령 실행 이후에는 성공 여부나 명령 실행 결과를 C&C 서버에 전달하는데, 응답 또한 명령 패킷과 유사하다.

오프셋	사이즈	설명
0x00	0x04	응답 번호
0x04	0x04	명령 실행 결과의 사이즈
0x08	가변	명령 실행 결과

Table 4. DurianBeacon의 응답 패킷 구조

응답	설명
0x00	명령 결과 반환
0x01, 0x02, 0x03	디렉터리 조회 (시작, 종료 등)
0x04	드라이브 정보
0x05, 0x06, 0x07	파일 업로드 (에러, 성공 등)
0x08, 0x09, 0x0A	파일 다운로드 (에러, 성공 등)
0x0B, 0x0C	디렉터리 생성 (실패, 성공)
0x0D, 0x0E	파일 삭제 (실패, 성공)
0x0F, 0x10	명령 실행 (실패, 성공)

Table 5. DurianBeacon의 응답 목록

B. Rust 버전

연관 파일들을 조사하던 중 Rust 언어로 만들어진 DurianBeacon 또한 공격에 사용된 것을 확인하였다.

- PDB 정보 : C:\Users\Anna\Documents\DurianBeacon\target\x86_64-pc-windows-msvc\release\deps\DurianBeacon.pdb

DurianBeacon은 C&C 서버와의 통신 방식들 중 SSL 외에 XOR을 이용한 패킷 암호화를 지원하며 키는 0x57이다.

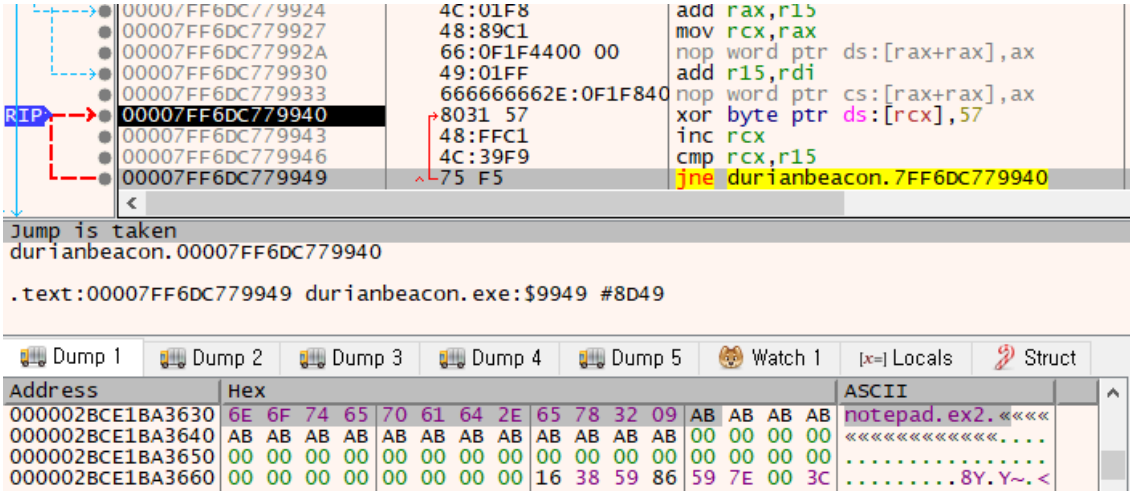

Figure 20. XOR 암호화를 지원하는 Rust 버전의 DurianBeacon

Go 버전과 비교했을 때 패킷 구조 및 명령 또한 동일하다. Rust 버전의 DurianBeacon은 최초 접속 이후 “durian2023” 키워드와 함께 감염 시스템의 IP 정보, 사용자 이름, 데스크탑 이름, 아키텍처, 파일명을 전송한 후 명령을 대기하며 명령 전달 시 결과를 반환한다.

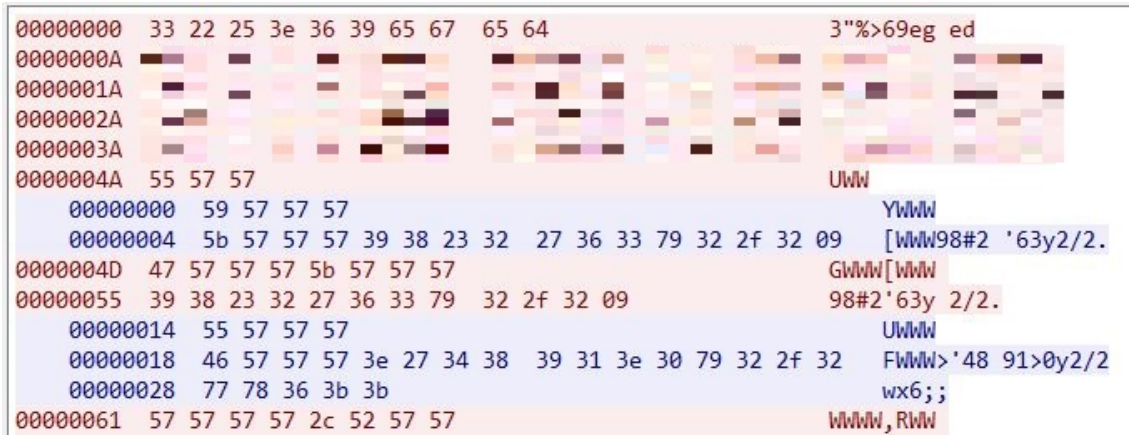

Figure 21. Rust 버전의 통신 패킷 – 테스트

3. 최근 공격 사례들의 연관성

위 항목에서 최근 확인된 두 개의 공격 즉 Innorix Agent를 악용해 국내 대학교를 공격한 사례와 스피어 피싱으로 추정되는 공격을 통해 국내 기업들에 악성코드를 설치한 사례들을 다루었다. 여기에서는 두 종류

의 공격을 동일한 공격자의 소행으로 추정하고 있는 근거를 정리한다.

먼저 자사 ASD 로그를 통해 특정 시스템에서 Durian, Goat RAT, AndarLoader 악성코드가 유사한 시점에 함께 수집된 사례가 존재한다. 해당 시스템은 공격자의 테스트 PC로 추정되는데 AndarLoader 악성코드의 경로명이 다음과 같았기 때문이다.

- AndarLoader의 수집 경로 : d:\01__developing\99__c#_obfuscated\runtime broker.exe

이외에도 백도어 악성코드들의 C&C 서버가 공유된 사례도 존재한다. 공격자가 Innorix Agent를 악용해 악성코드를 설치할 때 대부분 Goat RAT이 사용되었지만 또 다른 악성코드가 설치된 사례도 일정 비율로 존재한다. 해당 악성코드는 비록 수집되지는 않았지만 C&C 서버와의 통신 로그가 남아있으며 해당 주소는 다른 공격에서 사용된 DurianBeacon의 C&C 주소와 동일하였다.

Target Type	File Name	File Size	File Path
Current	innorixas.exe	7.94 MB	%SystemDrive%\innorix_agent\innorixas.exe
Target	iexpe.exe.irx	3.84 MB	%SystemDrive%\users\%ASD%\downloads\iexpe.exe.irx

Process	Module	Target	Behavior	Data
innorixas.exe	N/A	N/A	Creates executable file	N/A
File Less Submit iexp.exe	N/A	N/A	Connects to network	8.213.128.76:53
innorixas.exe	N/A	N/A	Changes executable file name	N/A

Figure 22. Innorix Agent를 통해 설치된 악성코드의 C&C 통신 로그

마지막으로 DurianBeacon이 AndarLoader를 설치한 로그도 확인할 수 있었다. 즉 해당 공격들은 유사한 시점에 발생하였으며 각각의 악성코드들이 설치 과정에서 또는 사용하는 C&C 서버의 주소에서 연관성을 보이고 있다.

Target Type	File Name	File Size	File Path
Current	creditsvc.exe	11 KB	%SystemRoot%\system32\creditsvc.exe
Parent	svchost.exe	54.02 KB	%SystemRoot%\system32\svchost.exe
DropperOfCurrent	agent.exe	427.5 KB	%SystemRoot%\ [redacted] \agent.exe

Process	Module	Target	Behavior	Data
creditsvc.exe	N/A	N/A	Connects to network	10.[redacted]:3389
creditsvc.exe	N/A	N/A	Creates executable file	mimi.exe

Figure 23. DurianBeacon이 AndarLoader를 생성한 로그

최근 확인된 두 개의 공격 사례는 동일한 공격자의 소행으로 추정된다. 여기에서는 해당 공격들과 Andariel 위협 그룹과의 연관성을 확인한다.

A. 공격 대상

- 국내 대학교와 방산, 전자 장비, ICT 업체 등을 대상으로 공격

B. 공격 방식

- 이전 사례와 동일하게 Innorix Agent 악용
- 이전 사례와 동일하게 스피어 피싱 공격으로 추정되는 정황 확인
- 악성코드 설치 시 사용한 경로 및 파일명의 유사성

C. 사용된 악성코드

- Go 언어로 제작된 악성코드들의 사용
- Andardoor 악성코드와 AndarLoader 악성코드의 유사성
- 과거 공격에 사용한 정보 탈취 악성코드와 유사한 악성코드 확인

먼저 공격 대상이 되는 분야가 기존의 공격 사례에서 확인된 대상과 동일하다는 점과 이전 공격에서 확인된 공격 방식들이 동일하게 사용되었다는 점이 있다. Innorix Agent를 악용한 사례는 직접 확인되었으며 추정이긴 하지만 여러 로그들을 통해 스피어 피싱 공격이 사용된 것으로 보이는 정황들도 확인된다.

그리고 악성코드 설치 시 사용된 “iexplorer.exe”라는 이름이 훨씬 이전 Andariel 공격 사례에서부터 확인되고 있다는 점이다. “iexplorer.exe” 외에도 “authsvc.exe”, “creditsvc.exe”와 같이 “svc” 키워드가 포함된 이름도 과거부터 꾸준히 사용되고 있다. 위의 과거 사례에서 사용된 “mainsvc.exe”, “certsvc.exe” 외에도 “netsvc.exe”라는 이름이나 “srvcredit.exe” 같은 유사한 이름이 사용된 사례들도 존재한다.

AndarLoader는 해당 항목에서 다루었다시피 이전 공격에서 사용된 Andardoor와 동일한 도구인 Dotfuscator의 평가판 버전으로 난독화되었으며 C&C 서버와의 통신 방식도 SSL 암호화를 사용한다는 점에서 유사한 것을 알 수 있다. 이외에도 Go 언어로 개발된 악성코드가 2개나 사용되었는데 이는 1th Troy Reverse Shell , Black RAT 등 올해 초부터 지속적으로 Go 언어로 개발된 악성코드가 사용되고 있는 흐름과도 맞아떨어진다.

마지막으로 공격자의 테스트 PC로 추정되는 시스템과 실제 공격 사례에서 직접 제작한 것으로 추정되는 정보 탈취형 악성코드들이 사용되었다는 점이 있다. 과거 사례에서도 Andariel 그룹은 공격 과정 중 계정 정보 탈취를 전담하는 악성코드를 설치하여 인터넷 익스플로러나 크롬, 파이어폭스 웹 브라우저 등에 저장된 계정 정보를 탈취하였다. 해당 악성코드는 커맨드 라인 도구로서 추출한 계정 정보를 커맨드 라인으로 출력하였으며 공격자는 백도어를 이용해 결과를 C&C 서버에 전달하였을 것으로 추정된다.

Figure 24. 과거 공격 사례에서 확인된 정보 탈취 악성코드

최근 공격에 사용된 정보 탈취형 악성코드도 이와 유사한 형태이며 차이점이 있다면 웹 브라우저들만을 정보 탈취 대상으로 하고 계정 정보뿐만 아니라 히스토리까지 탈취 대상으로 한다는 점이 있다. 이외에도 커맨드 라인으로 출력했던 과거와 달리 탈취한 정보를 동일한 경로에 “error.log”라는 이름의 파일로 생성한다.

```
**********Chromium**********


    ==========Credentials==========

Url: https
Username:
Password:
----------
    ==========   History   ==========

Url: ht
Title:
LastVisitedTime: ----------

**********Firefox**********


    ==========Credentials==========

64bit Firefox is only available!

    ==========   History   ==========


**********Internet explorer**********


    ==========Credentials==========

    ==========   History   ==========
```

Figure 25. 최근 공격 사례에서 확인된 정보 탈취 악성코드

5. 결론

Andariel 그룹은 Kimsuky, Lazarus 그룹과 함께 국내를 대상으로 활발하게 활동하고 있는 위협 그룹들 중 하나이다. 초기에는 주로 안보와 관련된 정보를 획득하기 위해 공격을 전개하였지만 이후에는 금전적 이득을 목적으로 한 공격도 수행하고 있다. [11] 초기 침투 시 주로 스피어 피싱 공격이나 워터링 홀 공격 그리고 소프트웨어의 취약점을 이용하는 것으로 알려져 있으며 공격 과정에서 다른 취약점을 이용해 악성코드를 배포하는 정황도 확인되고 있다.

사용자들은 출처가 불분명한 메일의 첨부 파일이나 웹 페이지에서 다운로드한 실행 파일은 각별히 주의해야 한다. 그리고 OS 및 인터넷 브라우저 등의 프로그램들에 대한 최신 패치 및 V3를 최신 버전으로 업데이트하여 이러한 악성코드의 감염을 사전에 차단할 수 있도록 신경 써야 한다.

파일 진단

– Backdoor/Win.Agent.R562183 (2023.03.14.00)
– Backdoor/Win.Andardoor.C5381120 (2023.02.16.01)
– Backdoor/Win.Andardoor.R558252 (2023.02.16.01)
– Backdoor/Win.AndarGodoor.C5405584 (2023.04.05.03)
– Backdoor/Win.DurianBeacon.C5472659 (2023.08.18.02)
– Backdoor/Win.DurianBeacon.C5472662 (2023.08.18.02)
– Backdoor/Win.DurianBeacon.C5472665 (2023.08.18.03)
– Backdoor/Win.Goat.C5472627 (2023.08.18.02)
– Backdoor/Win.Goat.C5472628 (2023.08.18.02)
– Backdoor/Win.Goat.C5472629 (2023.08.18.02)
– Backdoor/Win.NukeSped.C5404471 (2023.04.03.02)
– Backdoor/Win.NukeSped.C5409470 (2023.04.12.00)
– Backdoor/Win.NukeSped.C5409543 (2023.04.12.00)
– Infostealer/Win.Agent.C5472631 (2023.08.18.02)
– Trojan/Win.Agent.C5393280 (2023.03.11.00)
– Trojan/Win.Agent.C5451550 (2023.07.11.00)
– Trojan/Win.Andarinodoor.C5382101 (2023.02.16.01)
– Trojan/Win.Andarinodoor.C5382103 (2023.02.16.01)
– Trojan/Win32.RL_Mimikatz.R366782 (2021.02.18.01)

행위 진단

– Suspicious/MDP.Download.M1004
– Infostealer/MDP.Behavior.M1965

MD5

0211a3160cc5871cbcd4e5514449162b

0a09b7f2317b3d5f057180be6b6d0755

1ffccc23fef2964e9b1747098c19d956

3ec3c9e9a1ad0e6a6bd75d00d616936b

426bb55531e8e3055c942a1a035e46b9

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//13[.]76[.]133[.]68[:]10443/

http[:]//13[.]76[.]133[.]68[:]8080/

http[:]//139[.]177[.]190[.]243/update[.]exe

http[:]//27[.]102[.]107[.]224/update[.]exe

http[:]//27[.]102[.]107[.]224[:]5443/

추가 IoC는 ATIP에서 제공됩니다.

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.

Source: https://asec.ahnlab.com/ko/56256/