Dora RAT을 이용한 국내 기업 대상 APT 공격 사례 분석 (Andariel 그룹)

asec.ahnlab.com/ko/65495/

2024년 5월 16일

AhnLab SEcurity intelligence Center(ASEC) 에서는 최근 국내 기업 및 기관을 대상으로 한 Andariel 그룹의 APT 공격 사례를 확인하였다. 공격 대상으로 확인된 조직들은 국내 제조업, 건설 업체 및 교육 기관이었으며, 백도어뿐만 아니라 키로거, 인포스틸러 그리고 프록시 도구들이 공격에 사용되었다. 공격자는 이러한 악성코드들을 이용해 감염 시스템을 제어하고 시스템에 존재하는 데이터를 탈취할 수 있었을 것으로 추정된다.

해당 공격에서는 Andariel 그룹의 과거 공격 사례에서 확인된 악성코드들이 함께 확인되었다. 대표적으로 아래에서 다룰 백도어 악성코드인 Nestdoor가 있으며 이외에도 웹쉘이 함께 확인된 사례도 존재한다. 또한 동일한 파일은 아니지만 과거 Lazarus 그룹의 공격 사례에서 확인된 Proxy 도구가 함께 사용되기도 하였다.

1. 공격 정황

공격 과정에서 발견된 여러 정황들 가운데 직접적으로 확인된 공격 사례로 Apache Tomcat 서버를 운영 중인 웹 서버를 공격하여 악성코드를 유포한 사례가 있다. 해당 시스템은 2013년에 제작된 아파치 톰캣이 동작 중이었기 때문에 다양한 취약점 공격이 사용될 수 있는 조건이다. 공격자는 웹 서버를 공격해 백도어, 프록시 도구 등을 설치하였다.

Target Type	File Name	File Size	File Path
Current	cmd.exe	305.5 KB	%SystemRoot%\syswow64\cmd.exe
Target	winload.exe	2.94 MB	d:\backup\localproxy\winload.exe
Parent	tomcat6.exe	79 KB	d:\tomcat\bin\ tomcat6.exe

Process	Module	Target	Behavior	Data
cmd.exe	N/A	winload.exe	Creates process	N/A
tomcat6.exe	N/A	N/A	Deletes executable file	N/A
tomcat6.exe	N/A	N/A	Changes executable file name	winload.exe

2. 악성코드 분석

2.1. Nestdoor

Nestdoor는 적어도 2022년 5월 경부터 확인되고 있는 RAT 악성코드이다. 공격자의 명령을 전달받아 감염 시스템을 제어할 수 있으며 Andariel 그룹의 공격 사례에서 지속적으로 확인되고 있다. 여기에서는 분류를 위해 수집된 이름을 기반으로 Nestdoor로 분류한다.

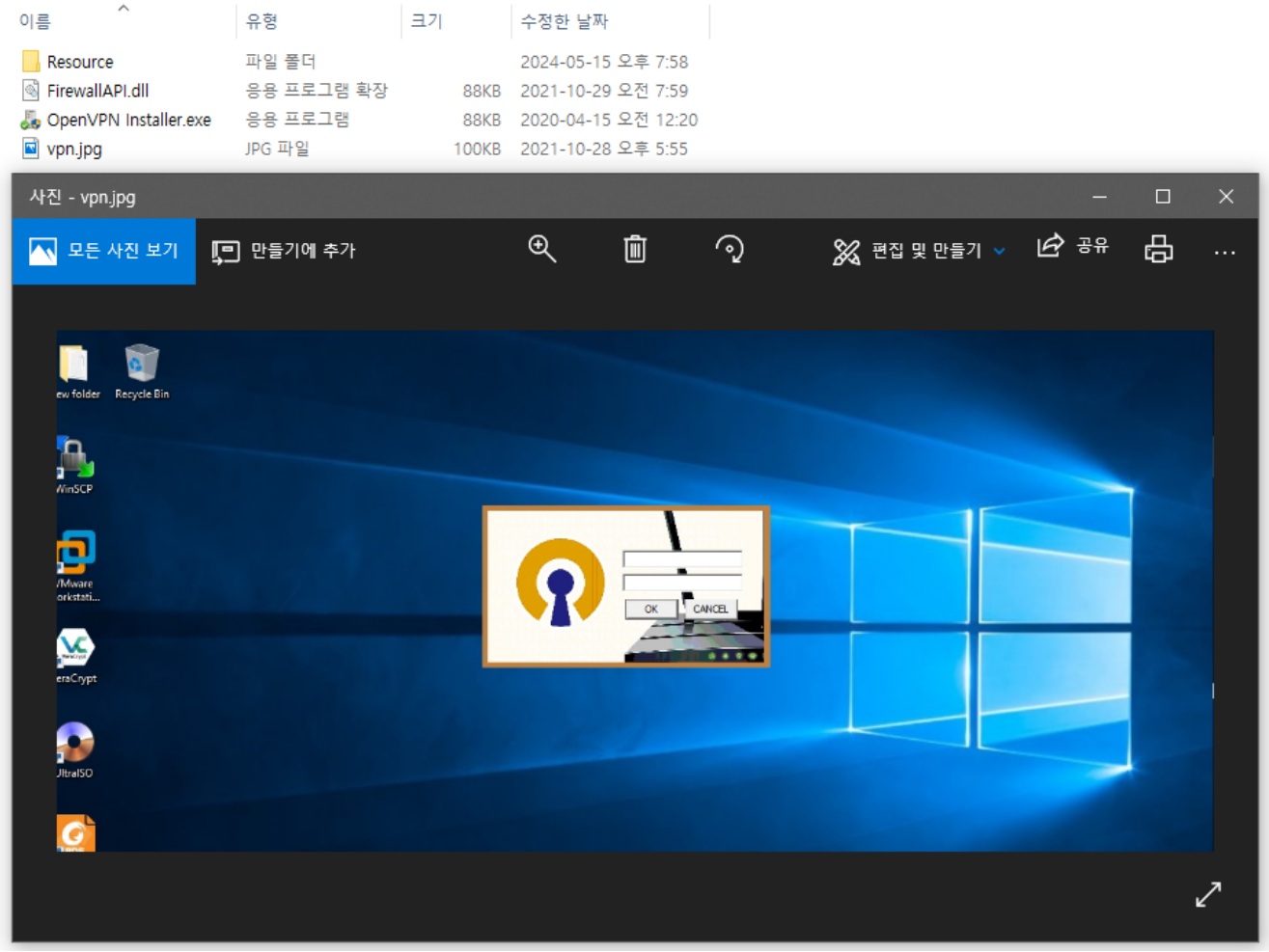
2022년 6월 미국 CISA에서는 VMware Horizon 제품의 Log4Shell 취약점(CVE-2021-44228)을 악용하여 악성코드를 설치하는 공격 사례들을 분석하여 공개하였다. 해당 공격 사례들 중에는 “Unidentified RAT”으로 분류된 악성코드들과 이를 메모리 상에서 실행하는 Loader 악성코드들이 존재한다. **[1] [2]**

“Unidentified RAT”으로 분류된 악성코드들은 C++로 개발되었으며 공격자의 명령을 전달받아 파일 업로드/다운로드, 리버스 쉘, 명령 실행과 같은 악성 행위를 수행할 수 있다. 이외에도 키로깅이나 클립보드 로깅, 프록시 등 다양한 기능들을 제공하며 분석을 방해하기 위해 바이너리를 난독화한 것이 특징이다.

참고로 ASEC에서는 2022년 5월 Lazarus 그룹의 하위 그룹으로 알려진 Andariel 그룹이 VMware Horizon 제품의 Log4Shell 취약점을 악용하여 TigerRAT을 유포한 공격 사례를 공개하기도 하였다. **[3]** 또한 2023년 초에는 Nestdoor가 TigerRAT과 함께 공격에 사용된 사례가 확인되기도 하였으며 TigerRAT과 동일한 C&C 서버를 공유하였다. 즉 Nestdoor는 TigerRAT과 함께 국내 기업들을 대상으로 하는 공격과 Log4Shell 취약점을 악용한 공격 등 여러 공격들에 함께 사용되어 왔다.

구체적인 유포 경로는 확인되지 않았지만 2024년 초에는 OpenVPN을 위장하여 유포한 사례가 확인되기도 하였다. 압축 파일 내부에는 다음과 같이 설치 파일을 위장한 악성코드가 존재하는데 만약 “OpenVPN Installer.exe” 파일을 실행할 경우 동일 경로에 위치한 런처 악성코드

인 “FirewallAPI.dll”이 로드되며 최종적으로 “Resource” 폴더에 존재하는 Nestdoor 악성코드 “openvpnsvc.exe”를 실행하게 된다. Nestdoor는 자신을 작업 스케줄러에 등록하여 지속성을 유지시키며 C&C 서버와 통신한다.



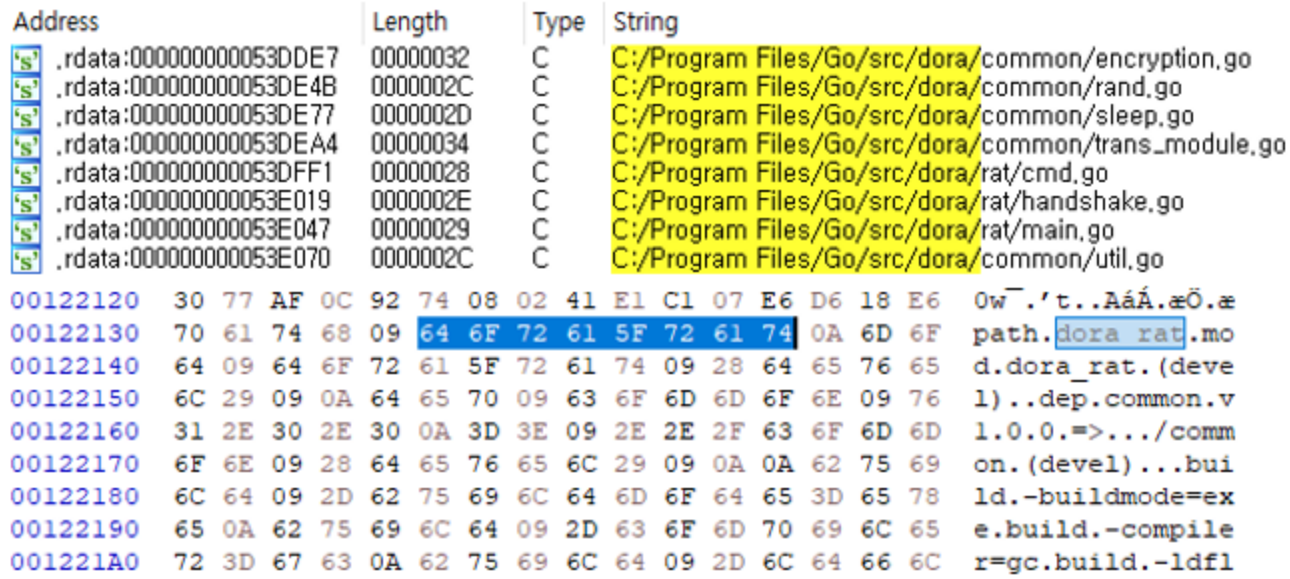
이번 공격에서 확인된 Nestdoor는 OpenVPN 사례와는 유사하지만 과거 유형들과 비교했을 때 차이점이 존재한다. 예를 들어 C&C 통신 과정에서 사용하는 명령 번호가 변경되었으며 더 적은 기능들을 지원한다. 하지만 난독화 방식이나 초기 루틴을 포함한 전체적인 구조는 유사하다. 물론 파일 작업이나 리버스 쉘과 같은 기본적인 기능들은 동일하게 제공하여 공격자가 감염 시스템을 제어할 수 있다는 점에는 차이가 없다.

```
InitializeSRWLock(a1 + 85);
a1[86].Ptr = 0LL;
a1[87].Ptr = 0LL;
a1[88].Ptr = 0LL;
InitializeSRWLock(a1 + 89);
a1[90].Ptr = a1;
LODWORD(a1[11].Ptr) = fn_get
v10 = 0;
if ( aNduuntgumtu5lj[0] )
{
  v11 = aNduuntgumtu5lj;
  do
  {
    ++v10;
    ++v11;
  }
  while ( *v11 );
}
v12 = fn_decodeStr(aNduuntgumtu5lj, v10, v9); // "45.58.159.237"
v13 = 0LL;
if ( aMtizndu2[0] )
{
  v14 = aMtizndu2;
  do
  {
    v13 = (v13 + 1);
    ++v14;
  }
  while ( *v14 );
}
v15 = fn_decodeStr(aMtizndu2, v13, v13);      // "123456"
```

```
if ( !CreatePipe(&hReadPipe, &hFile, &PipeAttributes, 0) )
{
  if ( hFile )
    CloseHandle(hFile);
  v0 = hReadPipe;
  goto LABEL_10;
}
memset(&StartupInfo, 0, sizeof(StartupInfo));
memset(&ProcessInformation, 0, sizeof(ProcessInformation));
GetStartupInfoA(&StartupInfo);
StartupInfo.hStdInput = hReadPipe;
StartupInfo.hStdError = hWritePipe;
StartupInfo.hStdOutput = hWritePipe;
StartupInfo.cb = 104;
StartupInfo.wShowWindow = 0;
StartupInfo.dwFlags = 256;
strcpy(Name, "ComSpec");
GetEnvironmentVariableA(Name, Buffer, 0x104u);
v2 = 0;
CurrentProcess = GetCurrentProcess();
if ( IsProcessInJob(CurrentProcess, 0LL, &Result) )
{
  if ( Result )
  {
    JobObjectW = CreateJobObjectW(0LL, 0LL);
```

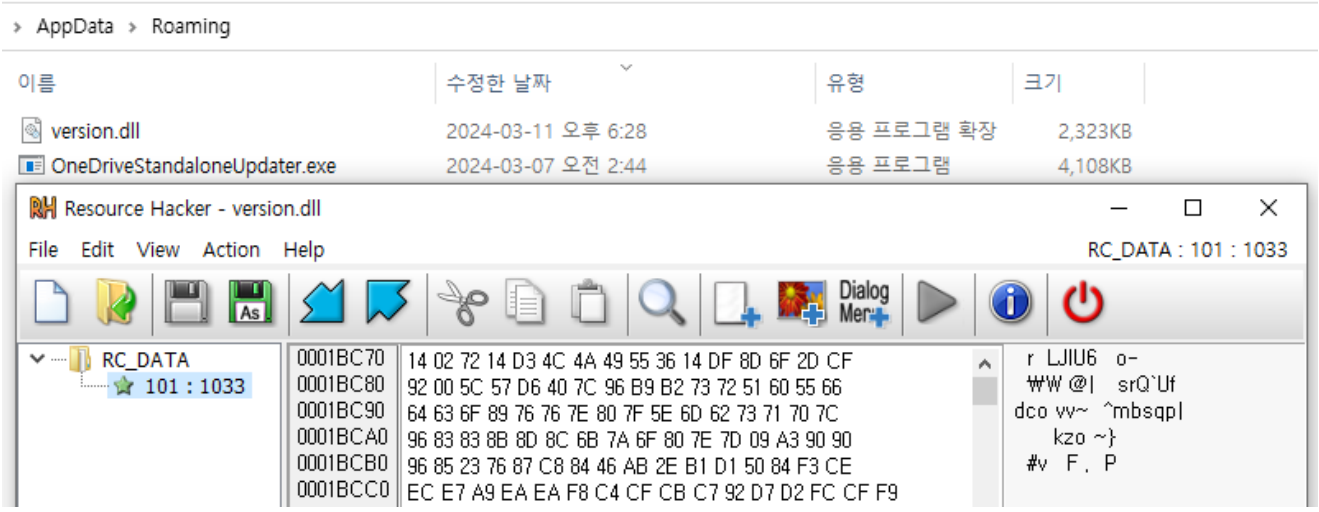
2.2. Dora RAT

최근 들어 Andariel 그룹은 공격 캠페인마다 새로운 백도어 악성코드를 제작하여 사용하고 있으며 대부분 Go 언어를 이용하는 경우가 많다. 이번에 확인된 새로운 악성코드 또한 Go 언어로 개발되었으며 공격자가 Dora RAT이라고 이름 붙였다.

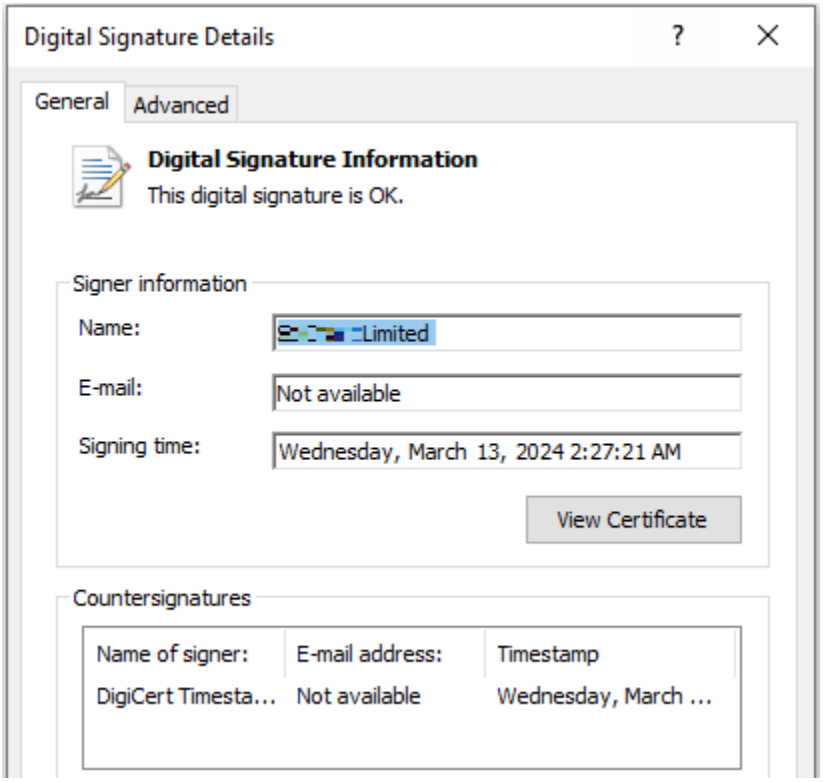


Dora RAT은 리버스 쉘, 파일 다운로드 / 업로드 기능을 지원하는 상대적으로 단순한 형태의 악성코드이다. Dora RAT은 두 가지 형태가 확인되는데 단독 실행 파일로서 동작하는 유형과 탐색기 즉 explorer.exe 프로세스에 인젝션되어 동작하는 유형이 있다.

"spsvc.exe"는 WinRAR SFX 포맷의 실행 파일로서 내부에 정상 프로그램인 "OneDriverStandaloneUpdate.exe"와 인젝터 악성코드인 "version.dll"이 존재한다. 실행 시 "%APPDATA%" 경로에 이들을 설치하고 "OneDriverStandaloneUpdate.exe"를 실행하면 동일 경로에 위치한 "version.dll"이 로드되어 악성 행위를 수행한다. "version.dll"은 내부 리소스에 포함한 데이터 즉 Dora RAT을 복호화하여 탐색기 프로세스에 인젝션한다.



참고로 공격자는 유효한 인증서로 악성코드를 서명하여 유포하기도 하였다. 공격에 사용된 Dora RAT 중에는 영국 소프트웨어 개발 업체의 유효한 인증서로 서명되어 있는 유형들이 확인되었다.



2.3. 기타 악성코드들

2.3.1. KeyLogger / ClipLogger

Dora RAT은 기본적인 제어 기능만 제공하며 이번 공격에서 확인된 Nestdoor 또한 과거 버전과 달리 상대적으로 단순한 기능만을 제공한다. 즉 키로깅이나 클립보드 로깅과 같은 기능들은 지원하지 않는다. 공격자는 이에 따라 Nestdoor를 이용해 키로깅 및 클립보드 로깅을 담당하는 악성코드를 추가적으로 설치하였다.

공격에 사용된 악성코드는 “%TEMP%” 경로에 인자로 전달받은 문자열에 해당하는 파일을 생성하고 로깅한 키 입력 및 클립보드 정보를 저장한다.

```
-------[2024/05/21 11:19] 관리자: C:\Windows\system32\cmd.exe-------
{Enter}
##### Username:test [2024/05/21 11:19] Monitor Started. #####

-------[2024/05/21 11:19] -------

-------[2024/05/21 11:19] *new 1 - Notepad++-------
teskt keylogging{Enter}{Enter}
-------[2024/05/21 11:19] Temp-------

-------[2024/05/21 11:19] *new 1 - Notepad++-------
{Enter}{Enter}{Enter}{Enter}
<Ctrl+V>
test clipboard
<Ctrl+V>
{Enter}{Enter}
```

2.3.2. Stealer

공격자가 설치한 도구들 중에는 시스템에 존재하는 파일들을 탈취하는 악성코드도 존재한다. 수량이나 사이즈가 적을 경우 기존에 설치한 백도어 악성코드들을 이용할 수도 있겠지만 이를 추가적으로 설치한 것을 보면 대량의 파일들을 탈취하기 위한 목적이었을 가능성이 있다.

인자	설명
–protocol	**통신에서 사용할 프로토콜 (tcp / udp)**
–server	**탈취에 사용된 주소 (ip:port 형태)**
–dir, –file	**탈취할 파일의 경로**
–thread, –limit	**성능 제한**

Table 1. Stealer의 인자

2.3.3. Proxy

공격자가 추가적으로 설치한 악성코드들 대부분은 프록시 도구들이었다. 확인된 프록시 도구들 중에는 공격자가 직접 제작한 것으로 보이는 유형들도 존재하지만 오픈 소스 Socks5 프록시 도구들도 함께 확인된다. **[4] [5]**

눈에 띄는 점은 2021년 초 카스퍼스키 사에서 공개한 ThreadNeedle을 이용한 Lazarus 그룹의 공격 캠페인에서 확인된 프록시 도구가 사용되었다는 점이다. 비록 동일한 파일은 아니지만 사이즈나 루틴 및 인증 과정에서 사용되는 문자열까지 동일한 악성코드이다. 참고로 인증 문자열까지 동일한 해당 프록시 유형은 적어도 2014년부터 지속적으로 공격에 사용되고 있다.

```
name.sa_family = 2;
*(_DWORD *)&name.sa_data[2] = ip_b;
*(_WORD *)name.sa_data = htons(port_b);
if ( connect(v5, &name, 16) == -1 )
  break;
if ( fn_sendAuth(v5, 'C8vI') && fn_recvAuth(v5, (int)&v8) && v8 == 'C8vJ' && fn_sendAuth(v5, 'C8vL') )
{
  for ( i = 0; i < 2; ++i )
  {
    while ( 1 )
    {
      v8 = 0;
      if ( !fn_recvAuth(v5, (int)&v8) )
        break;
      if ( v8 == 'C8vI' )
      {
        v7 = (SOCKET *)operator new(4u);
        *v7 = v5;
        CreateThread(0, 0, (LPTHREAD_START_ROUTINE)thread_proxy, v7, 0, 0);
        v5 = socket(2, 1, 0);
```

3. 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. **[6]** 초기 침투 시 주로 스피어 피싱 공격이나 워터링 홀 공격 그리고 소프트웨어의 취약점을 이용하며 공격 과정에서 추가적인 취약점을 이용해 악성코드를 내부망에 배포하는 정황도 확인되고 있다.

사용자들은 출처가 불분명한 메일의 첨부 파일이나 웹 페이지에서 다운로드한 실행 파일은 각별히 주의해야 하며, 기업 보안 담당자는 자산 관리 솔루션이나 접근 통제 솔루션 등 기업 내에서 사용하는 소프트웨어에 취약점이 있다면 최신 버전으로 패치를 수행하여야 한다. 그리고 OS 및 인터넷 브라우저 등의 프로그램들에 대한 최신 패치 및 V3를 최신 버전으로 업데이트 하여 이러한 악성코드의 감염을 사전에 차단할 수 있도록 신경 써야 한다.

파일 진단
– Trojan/Win.Injector.C5610655 (2024.04.09.03)
– Trojan/Win.Agent.C5610733 (2024.04.10.00)
– Backdoor/Win.Nestdoor.C5610641 (2024.04.13.00)
– Backdoor/Win.DoraRAT.C5610712 (2024.04.09.03)
– Dropper/Win.Agent.C5610793 (2024.04.10.00)
– Trojan/Win.Injector.C5610655 (2024.04.09.03)
– Dropper/Win.Agent.C5610654 (2024.04.09.03)
– Trojan/Win.KeyLogger.C5610642 (2024.04.09.03)
– Backdoor/Win.Nestdoor.C5622508 (2024.05.16.03)
– Trojan/Win.Launcher.C5622509 (2024.05.16.03)
– Trojan/Win.PWS.C5068848 (2022.04.12.01)

행위 진단
– Malware/MDP.Fraud.M800

MD5
094f9a757c6dbd6030bc6dae3f8feab3
33b2b5b7c830c34c688cf6ced287e5be
468c369893d6fc6614d24ea89e149e80
4bc571925a80d4ae4aab1e8900bf753c
5df3c3e1f423f1cce5bf75f067d1d05c
URL
https[:]//206[.]72[.]205[.]117/
https[:]//209[.]127[.]19[.]223/
https[:]//45[.]58[.]159[.]237/
https[:]//kmobile[.]bestunif[.]com/
AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.