Detailed Analysis of AlphaSeed, a new version of Kimsuky's AppleSeed written in Golang

medium.com/s2wblog/detailed-analysis-of-alphaseed-a-new-version-of-kimsukys-appleseed-written-in-golang-2c885cce352a

S2W May 17, 2023

--

Author: BLKSMTH | S2W TALON

> *: May 17, 2023*

Photo by on

Executive Summary

- 2023년 5월 경, S2W의 위협 연구 및 인텔리전스 센터 Talon은 Kimsuky 그룹의 새로운 악성코드로 추정되는 샘플을 VirusTotal에서 헌팅하여 분석을 진행함
- 헌팅된 악성코드는 을 수행
- S2W Talon은 해당 악성코드 내 "E:/Go_Project/src/alpha/naver_crawl_spy/"라는 경로명이 포함되어 있다는 점에서 이 악성코드를 ""으로 명명
- 우리는 AlphaSeed가 Kimsuky 그룹이 기존에 사용하던 AppleSeed 악성코드의 Go 언어 버전으로 추정하고 있으며, 최근 Kimsuky 그룹이 Go 언어로 악성코드를 구현하고 있는
- 과거 Kimsuky 그룹은 아이디와 비밀번호를 악성코드에 삽입하여 메일 서비스로 명령을 전달하였는데, 아이디와 비밀번호 대신 쿠키값으로 로그인을 구현하였으며 이후
- AppleSeed 악성코드와 파일 암호화 방식, 메일 전송 쓰레드, 활용하는 메일함 이름 등 유사점이 존재하고, Kimsuky 그룹이 과거 NavRAT 이라는 악성코드로 네이버 메일을 활용한 명령전달을 수행한 이력이 존재한다는 점에서 Kimsuky 그룹이 AlphaSeed 악성코드의 배후 그룹일 것이라 로 평가함
- Kimsuky 그룹이 Go언어를 통해 악성코드를 업데이트하고 있는 정황들이 발견되고 있기 때문에 주의가 필요

Introduction

2023년 5월 6일, VirusTotal에서 확인된 샘플에서 Kimsuky 그룹의 새로운 악성코드로 추정되는 샘플이 발견되어 분석을 진행하였다. 해당 샘플은 다음(Daum)메일 서비스와 통신하여 악성행위를 수행하는 AppleSeed 악성코드 와는 다르게 네이버 메일로 통신을 시도하며, 또한 Go 언어로 작성된 악성코드라는 점에서 새로운 악성코드 유형으로 예상되었다.

그림 1. VirusTotal 탐지 화면

해당 악성코드는 VMProtect로 패킹되어 있으며,
“**E:/Go_Project/src/alpha/naver_crawl_spy/”** 경로를 내부에 포함하고 있다. 이후 네이버 메일 서비스와 통신하여 정보탈취 및 명령 실행 등의 기능을 수행한다. 기존 Kimsuky 그룹은 아이디와 비밀번호로 네이버 메일 서비스에 로그인하는 방식을 사용했지만, 이번 악성코드에서는 **네이버 로그인에 필요한 Cookie값을 이용해 Chrome Devtools 프로토콜을 사용하도록 서포팅하는 클라이언트 프로그램인 ChromeDP으로 로그인**하는 방식을 사용한다. 이러한 방식의 변화는 C&C 서버로 사용하는 메일계정 정보를 노출하지 않으려는 전략으로 추정되고 있다. 아이디와 패스워드가 확보되는 경우, 누구나 해당 계정으로 네이버 메일 서비스에 접속하여 모든 행위를 수행할 수 있지만, 쿠키 값을 통한 로그인의 경우 별도로 쿠키값을 위조하는 작업이 필요하다.

그림 2. naver_crawl_spy 경로
해당 악성코드는 Go언어로 작성되어 있어 기존 Kimsuky 그룹이 사용하는 악성코드와 코드 유사성 비교가 확인하기 어려웠다. 또한, 분석 당시 악성코드가 사용하는 Cookie 값이 유효하지 않아 추가 악성행위가 식별되지 않았다. 하지만, 기존 Kimsuky 그룹의 AppleSeed 악성코드 유형 중 다음 메일을 C&C서버로 사용하는 유형과 파일 암호화 방식, 메일 전송 쓰레드, 메일 함 이름 등의 유사성이 존재한다는 점에서 Kimsuky 그룹의 새로운 악성코드로 추정하고 있다.

S2W의 위협 연구 및 인텔리전스 센터인 Talon은 해당 악성코드가 기존 **AppleSeed** 악성코드를 Go언어 버전으로 변경한 악성코드로 추정하고 있으며,
“**E:/Go_Project/src/alpha/naver_crawl_spy/**”라는 경로명을 사용하고 있다는 점에서 해당 악성코드 유형을 **“AlphaSeed”**으로 명명하였다.

Sample Information

- (Filename) powergmgmt.dat
- (MD5) 60308FA05380F183BF76F2ACFBE8E145
- (SHA-1) 57B248D18B9EE4106A5922A25EB03F7A9B637D42
- (SHA-256) F28D5CCDC79B0FCC02BE021435252F466A0C41786D9840E43A44EBDF821D3E95

Execution flow

Go언어로 작성된 AlphaSeed 악성코드는 네이버 메일로부터 명령을 받아 수행하며, 감염된 시스템의 정보를 수집 및 탈취 기능을 수행한다. 해당 악성코드는 다음과 같은 실행 과정을 보여준다.

1. regsvr32.exe를 통해 실행되며, %USERPROFILE%\ 경로에 작업 디렉토리(.edge)를 생성하고 자기 자신을 복제 및 로드
2. 로드된 악성 DLL은 키로깅, 스크린 캡처 등 감염된 시스템의 정보를 수집
3. 악성 DLL 내부에 존재하는 Cookie 값을 이용하여 네이버 메일 로그인 후, Ping 메일 전송
4. 메일에 존재하는 명령 전달용 Command 메일을 읽어와 명령 실행

그림 3. AlphaSeed 프로세스

Stage 1. Malicious DLL

1. Create directory & copy itself

실행시 가장 먼저 특정 경로에 작업 디렉토리를 생성하고 및 작업 경로로 지정한다. 이후 자기 자신을 해당 경로에 복사한다.

생성 경로: %USERPROFILE%\.edge

그림 4. .edge 디렉토리

2. Execution method check

현재 프로세스가 EXE 인지 체크한다. EXE 파일 일 경우, 작업 디렉토리에 schtaskw.exe 파일명으로 복사 및 실행하고, 아닐 경우 powermgmt.dat 파일로 복사한 후 regsvr32.exe로 로드한다. 이는 공격자가 DLL 파일 타입 외에도 EXE 파일 타입으로도 해당 악성코드를 실행할 수 있다는 것을 시사한다.

- EXE 일 경우, %USERPROFILE%\.edge\schtaskw.exe
- EXE가 아닐 경우, regsvr32.exe /s “%USERPROFILE%\.edge\powermgmt.dat”

3. Autorun with Registry

이후 부팅 시 항상 자동으로 악성코드가 실행되도록 “MS_SecSvc” 라는 이름으로 레지스트리에 등록한다.

- Registry Path: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Key: MS_SecSvc
- Value: regsvr32.exe /s “%USERPROFILE%\.edge\powermgmt.dat”” /t REG_SZ /v “MS_SecSvc” /f

그림 5. 자동실행 등록 레지스트리

4. Self-deletion

자가삭제 기능을 수행하기 위해 BAT 파일을 생성하여 실행한다. 총 2개의 BAT 파일을 생성하는데, 원본 DLL 파일을 삭제하는 BAT 파일과, 이 BAT 파일을 삭제하는 별도의 BAT 파일을 생성한다.

- BAT file: %USERPROFILE%\.edge\tmp[time_calulate].bat
- BAT file 2: %USERPROFILE%\.edge\tmp[time_calulate].bat

표 1. 자가삭제 BAT 파일

5. Reload DLL

실행된 원본 파일이 powermgmt.dat 파일인지 확인하고 아닐 경우, regsvr32.exe를 통해 로드 후 종료한다. 실제 악성 기능은 로드된 powermgmt.dat 파일을 통해 수행된다.

Command Line : regsvr32.exe /s %USERPROFILE%\.edge\powermgmt.dat

Stage 2. powermgmt.dat

1. Struct Initialization

Stage 2가 실행되면, 악성행위에 필요한 “agent_Agent” 구조체를 초기화한다. 이 구조체는 악성행위 실행시 참고된다.

표 2. agent_Agent 구조체

2. File Encryption & Data Decryption

감염된 시스템으로부터 탈취한 파일에 대하여 암호화를 수행하거나, 공격자 메일로부터 받은 명령을 복호화할 때 RC4와 RSA 알고리즘이 사용된다. 악성코드는 랜덤하게 RC4 Key를 생성하고, 내부에 존재하는 ParsePKCS1PublicKey 함수를 통해 암호화를 위한 Public Key를 생성한다. 이후, Public Key를 통해 RC4 Key를 암호화한다. 공격자 메일로부터 받은 명령 또한 암호화되어 있는데, 이 데이터는 악성코드 내부에 존재하는 별도의 Private Key를 통해 RSA를 복호화하여 RC4 Key를 획득하고, 이후 획득한 RC4 Key로 데이터를 복호화한다.

그림 6. 파일 암호화 & 복호화 프로세스

3. Collect data from infected machine

감염된 시스템의 정보를 탈취하기 위해 3개의 함수를 GoRoutine을 통해 호출한다. 각각의 함수는 키로깅, 스크린샷, 재시작과 같은 기능을 수행한다.

표 3. Function List
goKeylog 함수에서는 감염된 시스템에 입력되는 키 입력 데이터를 작업 디렉토리 하위에 cache_w.db 파일로 저장한다. 이후, 파일을 암호화하고, 네이버 메일을 통해 전송한다.

Keylogging filepath: %USERPROFILE%\.edge\cache_w.db

그림 7. cache_w.db 키로깅 데이터
goSshot에서는 감염된 시스템의 현재 데스크탑 화면을 캡쳐하여 파일로 저장한다. 데스크탑 화면 캡쳐를 위해 Github에 공개된 “kbinani”의 screenshot 패키지를 사용한다.

- Screenshot filepath: %USERPROFILE%\.memdmp\{Timestatmp}_0
- 참고자료:

그림 8. ScreenShot 데이터

4. C&C communication initializing using Naver Mail

AlphaSeed 악성코드는 네이버 로그인에 필요한 별도의 아이디와 패스워드 대신, 유효한 Cookie 값을 이용해 로그인하는 방식을 사용하고 있다. 이는 Infostealer 악성코드로부터 탈취된 쿠키값을 이용하여 계정을 탈취하는 방식과 동일한 방식으로 볼 수 있다. 이후 로그인에 성공하면, 네이버 메일 서비스에 접근하여 정보 탈취 및 명령 전달을 수행한다.

그림 9. ChromeDP를 통한 네이버 메일 통신 프로세스
그림 10. 악성코드 내 네이버 Cookie 데이터
공격자는 쿠키값을 이용하여 계정에 로그인하기 위해 오픈소스로 chromedp를 사용한다. Chromedp는 디버깅, 컨텐츠 검사 등 다양한 기능을 수행할 수 있는 Chrome Devtools 프로토콜을 서포팅하는 클라이언트 프로그램이다.

참고자료:

그림 11. ChromeDP
네이버 메일과 상호작용을 수행하기 위해 패킷 통신을 수행하는 방식이 아닌, chromedp라는 중간 매개체를 이용하여 악성 행위를 위한 스크립트를 실행하는 방식을 사용한다. AlphaSeed는 해당 방식을 통해 특정 버튼을 클릭하거나 메일을 작성하여 전송하는 기능을 수행한다.

그림 12. ChromeDP를 통해 실행되는 스크립트
그림 13. 프로세스 실행 트리
Cookie 값을 통해 네이버 로그인 후, 네이버 메일함 중 **내게쓴메일함**을 이용하여 데이터를 주고 받는다. 내게쓴메일함 내에 특정 이름을 가진 메일함 정보를 가져와 확인하며, 이후 목적에 맞는 메일함을 사용하여 탈취한 정보 및 명령 수행에 사용한다.

표 4. Mailbox List

악성코드 내에는 감염자 정보를 수집하는 ping 기능이 존재한다. 감염자를 식별하기 위한 uid 및 감염된 환경 정보, 감염 당시 시간을 Zlib를 통해 압축한 후 Base64로 인코딩한 데이터 메일 제목으로 사용하여 전송한다. 이후, 공격자는 ping 메일 제목으로 사용된 값을 추출하여 감염자 식별 및 명령 전송에 사용한다.

> {**“uid”:”886xxxxxxxxx”**,”platform”:”windows amd64",”ver”:
> {“major”:1,”minor”:2,”build”:0},”time”:1683982504982}

그림 14. Ping 전송 예시 (테스트 메일 화면)

Cmd 메일함에 저장된 명령 메일을 읽어와 악성 행위를 수행한다. Cmd 메일함에 존재하는 메일 중에서 Ping 메일내 포함된 감염자의 고유 값(uid)이 제목에 포함된 메일 정보를 가져온다. 메일 내 데이터를 AlphaSeed 내 RSA Private Key로 복호화하고, RC4 Key를 확보한다. 이후 RC4 Key로 데이터를 복호화하여 명령을 추출한다. 추출된 명령 코드에 따라 다음과 같은 악성행위를 수행한다.

표 5. Command 별 악성행위

5. Exfiltrate collected data to Naver Mail

감염된 시스템에서 수집한 정보를 각각의 메일함으로 전송한다.

표 6. 탈취 정보별 전송 메일함
공격자는 메일 제목과 본문에 모두 데이터를 포함시켜 전송하지만, AlphaSeed의 실제 통신을 그대로 구현한 결과, 그 부분이 제대로 동작하지 않아 메일 제목에만 데이터가 입력된 점이 확인되었다. 이러한 특징은 아직 AlphaSeed의 기능 구현이 완성되지 않았다는 점을 제시한다.

그림 15. 키로깅 정보 전송 메일 (테스트 메일 화면)

Suspected attacker’s account

AlphaSeed 악성코드가 메일 전송 관련 URL을 조합할 때 유저명으로 추정되는 네이버 계정을 발견할 수 있었다. 분석 당시 악성코드 내 Cookie값이 유효하지는 않았지만, VirusTotal 업로드 당시 해당 계정으로 로그인 후, 메일 전송까지 정상적으로 수행한 것으로 추정되는 통신 기록이 발견되었다.

공격자 의심 계정: moj124578

그림 16. 악성코드 내 메일 주소
그림 17. 악성코드 통신 이력
해당 네이버 계정이 실제로 존재하는 계정이며, 블로그 페이지 또한 존재하는 점까지 확인되었다. 하지만, 해당 계정이 공격자의 계정인지 탈취한 계정을 악용하는 것인지는 확인되지 않았다.

그림 18. 악성코드 내 존재한 메일 관련 블로그

Attribution

AlphaSeed는 Go언어로 작성되었다는 점에서 기존 Kimsuky 그룹의 악성코드와 코드 유사성은 식별되지 않았지만, AppleSeed 악성코드와 유사한 기능이 상당수 확인되었다는 점에서 S2W에서는 Kimsuky 그룹의 악성코드로 식별하였다. 다음 메일을 C&C 서버로 사용하는 AppleSeed 악성코드에 대한 설명은 아래에서도 확인이 가능하다.

참고자료:

다음 메일을 C&C 서버로 사용하는 AppleSeed 악성코드에서도 감염된 시스템의 정보를 메일로 전송하는 Ping 기능과 공격자로부터 명령을 받아 실행하는 Command 기능이 존재한다. **과거 AppleSeed 케이스에서는 SMTP와 IMAPS 프로토콜을 이용해 메일을 전송**했다면, 이번 **AlphaSeed 케이스의 경우 ChromeDP를 이용해 직접 메일을 전송**하는 차이점이 존재한다. 또한, 다음 메일을 통해 명령을 받는 Command 기능을 수행할때 “cmd” 메일함 이름을 사용한다는 점이 이번 케이스와 동일한 특징으로 보인다.

그림 19. 과거 AppleSeed 통신 쓰레드 (출처:)
명령 실행 과정에서도 AppleSeed 와의 공통점이 확인되었다. 두 악성코드 모두 공격자로부터 명령 데이터를 받은 후 RSA Private Key를 통해 RC4 Key를 추출하고, 이후 RC4 Key로 명령 데이터를 추출한 뒤 악성 행위를 수행한다. 기존 AppleSeed에서는 3개의 명령이 확인되었지만, AlphaSeed 내에는 5개의 명령이 확인되었다는 점에서 기능상의 업데이트도 함께 이루어진 것으로 확인된다.

표 7. AppleSeed와 AlphaSeed 명령 비교
추가로, 최근 AhnLab은 Kimsuky 그룹이 Go언어로 작성된 악성코드를 이용해 Meterpreter를 로드하고 최종적으로 Go언어로 작성된 Proxy 악성코드를 사용하였다는 내용을 공개하였는데, Kimsuky 그룹이 과거 AppleSeed 악성코드 감염 이후 Meterpreter를 설치했던 사례들도 확인되었던만큼 Kimsuky이 최근 악성코드를 Go 언어로 제작하려는 움직임이 보이고 있다.

참고자료:

Conclusion

- AlphaSeed 악성코드는 AppleSeed 악성코드와 파일 암호화 방식, 메일 전송 쓰레드, 메일함 이름 등과 유사하다는 점에서 AppleSeed 악성코드를 기반으로 제작된 것으로 확인됨
- Kimsuky 그룹은 기존 AppleSeed 악성코드를 Go언어로 변경하려는 것으로 보이며, 이 과정에서 일부 기능도 업데이트도 된 것으로 확인되었으나 아직 기능이 완벽하게 구현된 것으로 보이지는 않음
- 기존 아이디와 비밀번호를 활용한 전통적인 로그인 방식에서 Cookie값을 이용한 방식으로 메일 서비스를 활용하는 방식으로 전략이 변경됨
- 과거 모바일 버전의 AppleSeed 악성코드도 발견되었던 만큼, Go언어 버전으로 제작할 만큼 Kimsuky 그룹이 주력 악성코드로 AppleSeed를 사용하다는 사실을 확인할 수 있음
- Kimsuky 그룹이 기존 악성코드를 Go언어로 변경하려는 정황들이 확인되고 있다는 점에서, 이에 대한 대비가 필요함

IoC

- f28d5ccdc79b0fcc02be021435252f466a0c41786d9840e43a44ebdf821d3e95
- f78b3c0ccaa02b4b159b36557f6b99a9800bccdb2bd86f655f642a2097362026
- 98916e83b272f5ead73412a5765e1cf1225873c7b0cf0b5e94a341e65451d652
- 37ea9dba7ab6465f4d82c1af38a27339db9bf81ded74299fd6e5075e126b732a

- 5aa1cc14a82db34269de7778536c893ae177345172f70478b4093fa0451744c8
- eb55211ca3b233555397cecf32ac0a86ec85983a1fd1f50bb04d727dddf6b1ec

ATT&CK Matrix

Persistence

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

Defense Evasion

System Binary Proxy Execution: Regsvr32 (T1218.010)

Collection

- Input Capture: Keylogging (T1056.001)
- Screen Capture (T1113)
- Archive Collected Data (T1560)

Exfiltration

Exfiltration Over Web Service (T1567)