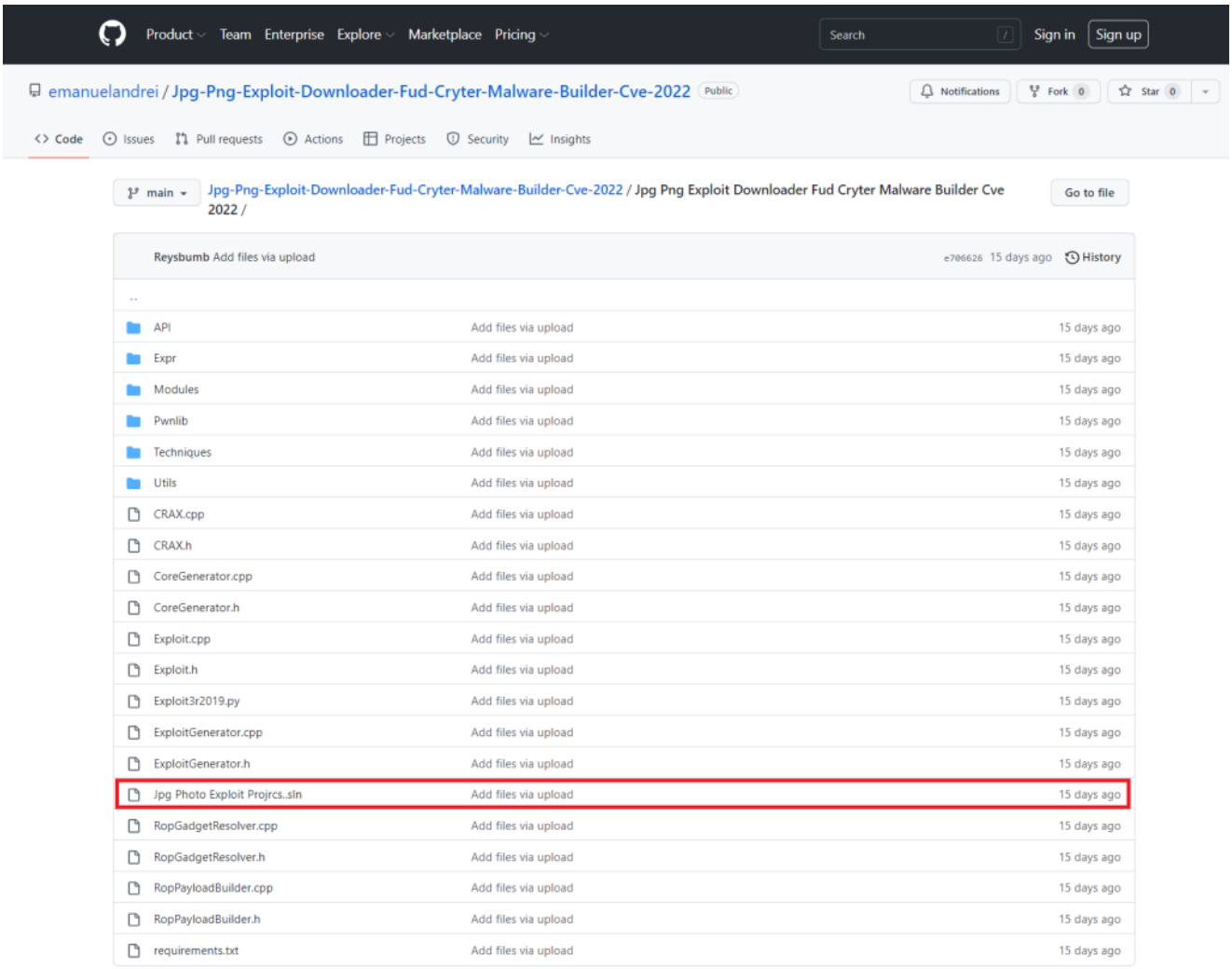
GitHub에 솔루션파일(*.sln) 위장하여 유포되는 RAT 툴

asec.ahnlab.com/ko/37764/

2022년 8월 18일

ASEC 분석팀에서는 최근 GitHub 에서 솔루션파일(*.sln)을 위장하여 RAT 툴이 유포 중인 것을 확인하였다. [그림1] 은 악성코드 유포자가 GitHub에 “Jpg Png Exploit Downloader Fud Cryter Malware Builder Cve 2022” 제목으로 소스코드를 공유한 내용이다. 프로그램의 구성파일이 정상적으로 보이지만 이 중 솔루션파일(*.sln)은 RAT 툴이다. 이와 같은 방법으로 악성코드 유포자는 RAT 툴을 솔루션파일(*.sln)로 위장하여 실행을 유도한다. 일반적으로 프로그래머는 솔루션파일이 포함된 코드를 받고 프로젝트를 열기위해 솔루션파일을 오픈한다. 이러한 심리를 이용한 사회공학기법에 대한 주의가 필요하다.



[그림1] GitHub에 공개된 위장 파일

위 파일들을 받게되면 아래 [그림2] 처럼 파일들이 존재한다. [그림2]의 환경은 “알려진 파일형식의 파일 확장명 숨기기” 가 해제된 환경이다. 이 중 솔루션파일(*.sln)의 아이콘을 갖는 파일은 표기되는 이름도 솔루션 파일처럼 보이기 때문에 실행에 주의가 필요하다. 이는 사용자의 실행을 유도하기 위한 목적으로 제작된 악성코드로 유형을 잘 살펴보면 화면 보호기 임을 알 수 있다. Windows 환경에서 .scr 파일은 실행이 가능한 확장자이기 때문에 실행 시 악성코드에 감염된다.

이름	수정한 날짜	유형	크기
API	2022-08-03 오전 4:51	파일 폴더	
Expr	2022-08-03 오전 4:51	파일 폴더	
Modules	2022-08-03 오전 4:51	파일 폴더	
Pwnlib	2022-08-03 오전 4:51	파일 폴더	
Techniques	2022-08-03 오전 4:51	파일 폴더	
Utils	2022-08-03 오전 4:51	파일 폴더	
CoreGenerator.cpp	2022-08-03 오전 4:51	C++ Source	3KB
CoreGenerator.h	2022-08-03 오전 4:51	C/C++ Header	2KB
CRAX.cpp	2022-08-03 오전 4:51	C++ Source	15KB
CRAX.h	2022-08-03 오전 4:51	C/C++ Header	13KB
Exploit.cpp	2022-08-03 오전 4:51	C++ Source	5KB
Exploit.h	2022-08-03 오전 4:51	C/C++ Header	6KB
Exploit3r2019.py	2022-08-03 오전 4:51	Python File	14KB
ExploitGenerator.cpp	2022-08-03 오전 4:51	C++ Source	7KB
ExploitGenerator.h	2022-08-03 오전 4:51	C/C++ Header	3KB
Jpg Photo Exploit Projrcs..sln	2022-08-03 오전 4:51	화면 보호기	682KB
requirements.txt	2022-08-03 오전 4:51	텍스트 문서	1KB
RopGadgetResolver.cpp	2022-08-03 오전 4:51	C++ Source	4KB
RopGadgetResolver.h	2022-08-03 오전 4:51	C/C++ Header	4KB
RopPayloadBuilder.cpp	2022-08-03 오전 4:51	C++ Source	10KB
RopPayloadBuilder.h	2022-08-03 오전 4:51	C/C++ Header	5KB

[그림2]

다운로드 받은 파일 목록

```
19              Settings.Key = Encoding.UTF8.GetString(Convert.FromBase64String(Settings.Key));
20              Settings.aes256 = new Aes256(Settings.Key);
21              Settings.Por_ts = Settings.aes256.Decrypt(Settings.Por_ts);
22              Settings.Hos_ts = Settings.aes256.Decrypt(Settings.Hos_ts);
23              Settings.Ver_sion = Settings.aes256.Decrypt(Settings.Ver_sion);
24              Settings.In_stall = Settings.aes256.Decrypt(Settings.In_stall);
25              Settings.MTX = Settings.aes256.Decrypt(Settings.MTX);
26              Settings.Paste_bin = Settings.aes256.Decrypt(Settings.Paste_bin);
27              Settings.An_ti = Settings.aes256.Decrypt(Settings.An_ti);
28              Settings.Anti_Process = Settings.aes256.Decrypt(Settings.Anti_Process);
29              Settings.BS_OD = Settings.aes256.Decrypt(Settings.BS_OD);
30              Settings.Group = Settings.aes256.Decrypt(Settings.Group);
31              Settings.Hw_id = HwidGen.HWID();
32              Settings.Server_signa_ture = Settings.aes256.Decrypt(Settings.Server_signa_ture);
33              Settings.Server_Certificate = new X509Certificate2(Convert.FromBase64String(Settings.aes256.Decrypt(Settings.Certifi_cate)));
34              result = Settings.VerifyHash();
35          }
36          catch
37          {
38              result = false;
39          }
```

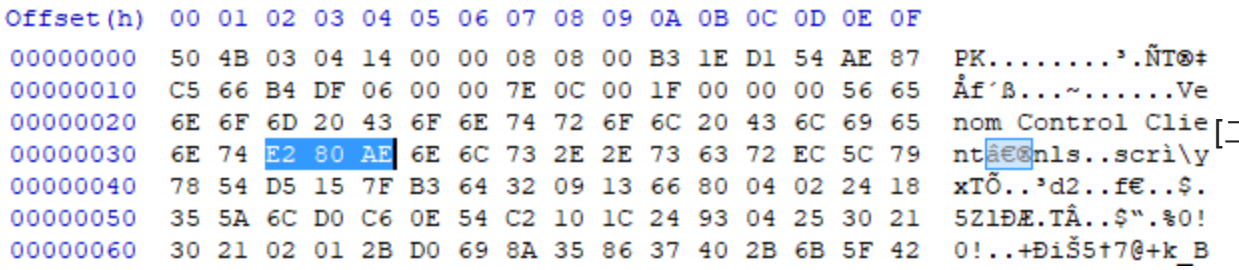
100 %

Locals

Name	Value	Type
Client.Algorithm.Aes256.Decrypt returned	"217.64.31.3"	string
result	false	bool

[그림3] AsyncRAT C2 복호화

솔루션 파일로 위장된 악성코드는 파일 진단을 우회하기 위해 파일 외형을 변경시키는 크립터 툴을 사용했으며, 실행 시 윈도우 정상 프로그램인 AppLaunch.exe, RegAsm.exe, InstallUtil.exe 에 인젝션되어 실행되며 최종 실행되는 악성코드는 RAT 툴 이다.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	50	4B	03	04	14	00	00	08	08	00	B3	1E	D1	54	AE	87	PK.....³.ÑT®‡
00000010	C5	66	B4	DF	06	00	00	7E	0C	00	1F	00	00	00	56	65	Åf´ß...~.....Ve
00000020	6E	6F	6D	20	43	6F	6E	74	72	6F	6C	20	43	6C	69	65	nom Control Clie
00000030	6E	74	E2	80	AE	6E	6C	73	2E	2E	73	63	72	EC	5C	79	nt‮nls..scrì\y
00000040	78	54	D5	15	7F	B3	64	32	09	13	66	80	04	02	24	18	xTÕ..³d2..f€..$.
00000050	35	5A	6C	D0	C6	0E	54	C2	10	1C	24	93	04	25	30	21	5ZlÐÆ.TÂ..$“.%0!
00000060	30	21	02	01	2B	D0	69	8A	35	86	37	40	2B	6B	5F	42	0!..+ÐiŠ5†7@+k_B

[그림4]

악성코드를 ZIP 파일로 압축한 데이터

GitHub와 Windows탐색기의 확장자가 솔루션파일(*.sln) 처럼 보이는 원리는 파일을 압축하여 확인 가능하다. 과거 ASEC블로그에 작성된 내용처럼 [그림4]의 “RIGHT-TO-LEFT OVERRIDE”를 뜻하는 유니코드 문자를 사용하기 때문이다.

> 유니코드 문자열을 이용하여 문서파일로 위장한 악성코드

이렇듯 최근 많은 사용자가 접속하는 GitHub 에서 악성코드 유포자가 악의적인 목적으로 소스코드에 관련된 파일이 아닌 악성코드를 솔루션파일(*.sln)로 위장하여 배포되는 사례가 늘어나고 있다. 사용자들은 신뢰되지 않은 작성자가 공개한 내용의 열람에 주의를 기울여야한다. 또한, 사용하고 있는 백신을 항상 최신 버전으로 업데이트하여 관리하는 주의가 필요하다.

AhnLab V3에서는 해당 악성코드들에 대해 아래와 같이 진단하고 있다.

[파일 진단]

- Trojan/Win.Leonem.C5218555 (2022.08.04.00)
- Trojan/Win.Agent.C4526491 (2021.06.30.03)
- HackTool/Win32.Vbinder.R12127 (2015.02.14.01)
- Trojan/Win.SmokeLoader.R510280 (2022.08.12.04)
- Trojan/Win.MSILZilla.C5129545 (2022.05.15.02)
- Trojan/Win.Generic.C5198415 (2022.07.08.03)

[행위 진단]

- Malware/MDP.Inject.M3037
- Execution/MDP.Powershell.M3991
- Malware/MDP.AutoRun.M1037
- Execution/MDP.SystemManipulation.M1788
- Malware/MDP.Inject.M1252

[IOC 정보]

- hxxps://github.com/emanuelandrei/Jpg-Png-Exploit-Downloader-Fud-Cryter-Malware-Builder-Cve-2022
- 0cfa5f7c008e3dc2df275a99aef9cbbb // Jpg Photo Exploit Projrcs..sln
- b1f02c7efc154019e9f1974939e204b9
- hxxps://github.com/VortexRadiation/VenomControl-Rat-Crack-Source

- 98d7999986d63fbd914bddc3d7b7ecf9 // Venom Control Client.sln
- 8b662719e44ab11419fe3e1d7e96cc03
- hxxps://github.com/VortexRadiation/Jpg-Png-Exploit-Downloader-Fud-Cryter-Malware-Builder-Cve-2022
- 9a01d2f0aad78bcc4a4ca07552154ee1 // Jpg Photo Exploit Proj.sln
- hxxps://github.com/Lessermask/Discord-Image-Token-Password-Grabber-Exploit-Cve-2022
- 9fd996ce42d667ba01c902124bf95f6d // Discord Image Token Grabber.sln

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

.

Categories:미분류, 악성코드 정보

Tagged as:AsyncRAT, 유니코드, malware