|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 소 속 | 육군 2군단 | | IP | | 공인 : 150.107.86.194 | |
| 팀 명 | 2021 화이트햇 콘테스트 | | | | | |
| 팀 원 | 최재혁 | 송준호 | | 송연주 | | 연동현 |
| 팀장  E-mail | stasika@naver.com | | 팀장 전화번호 | | 010-8848-4535 | |

문 제 풀 이 보 고 서

**\* 핵심 풀이과정 및 플래그 획득 화면 캡처가 포함되어야 합니다.**

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| A1 | | 해킹메일 | 100 |
| **공격자는 신무기와 관련된 무수히 많은 사람들을 대상으로 이메일을 이용해 무작위 공격을 시도했다. 이메일을 수신한 사람들은 연구소 관계자, 무기 개발 방산 회사가 포함되어 있으며, 현재 중요한 자료는 탈취되지 않았을 것으로 예상되지만 피해 규모는 확인되지 않았다. 이 공격이 언제, 어디로부터 시작되었는지 알아야 한다.** | | | |
| 풀이 절차 | Outlook을 이용해 받은편지함을 조사하여 의심되는 메일을 찾는다 | | |
| 정 답 | FLAG{2021\_09\_07\_11\_37} | | |
| 풀 이 과 정 | | | |
| 텍스트이(가) 표시된 사진  자동 생성된 설명 | | | |
| 첨부파일이나 링크가 있는 메일을 조사하던중, 의심되는 파일을 발견함.  첨부파일 링크는(34.63.143.34/download.html)을 가르키고 있으므로 와이어샤크를 통해 해당 html파일을 복구함. (a.pcap파일 활용)  텍스트이(가) 표시된 사진  자동 생성된 설명  파일을 확인해보니 eps 취약점을 이용한 멜웨어임을 확인할수 있음.  시간은 메일에 나와있는 수신시간을 활용해 답을 찾음. 텍스트이(가) 표시된 사진  자동 생성된 설명 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| A2 | | 해킹메일 | 100 |
| 드랍퍼가 위치한 서버의 아이피는 무엇인가?FLAG의 형식은 FLAG{000.000.000.000} 이다 | | | |
| 풀이 절차 | Outlook을 이용해 받은편지함을 조사하여 의심되는 메일을 찾는다. | | |
| 정 답 | FLAG{34.64.143.34} | | |
| 풀 이 과 정 | | | |
| 텍스트이(가) 표시된 사진  자동 생성된 설명 | | | |
| 첨부파일이나 링크가 있는 메일을 조사하던중, 의심되는 파일을 발견함.  첨부파일 링크는(34.63.143.34/download.html)을 미리보기로 제공함.  텍스트이(가) 표시된 사진  자동 생성된 설명  또는 pcap파일의 hostname 에서도 확인할수 있음.  또는 익스플로러의 최근 열어본 페이지에서도 확인할 수 있음. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| A-3 | |  | 미기입 |
| 이메일을 분석하여 플래그를 획득하여라  FLAG의 형식은 FLAG{...} 이다. | | | |
| 풀이 절차 | 메일 내 링크에 들어가서 소스코드를 분석하여  플래그값을 획득함. | | |
| 정 답 | FLAG{Wh0oo0o\_HTML\_C4n\_uS3d\_t0\_By94ss\_F1rew411} | | |
| 풀 이 과 정 | | | |
| 첨부파일을 다운로드 받을 수 있는 링크에 들어가서 소스코드를 보니  V1, V2, V3, V4, V5가 있었음.    모든 과정이 다 진행되면 V1~V5까지 모든 변수가 no hack :( 으로 변경이 되어서 크롬으로  브레이크 포인트를 주면서 진행을 시켜본 결과 각 변수들은  V1 Wh0oo0o  V2 By94ss\_F1rew411  V3 uS3d\_t0  V4 HTML\_C4n  라는 값을 얻었음.    결국 V5에 FLAG{Wh0oo0o\_HTML\_C4n\_uS3d\_t0\_By94ss\_F1rew411} 값을 얻을 수 있음. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| B-1 | |  | 미기입 |
| 드랍퍼에서 획득할 수 있는 악성코드를 분석하여 FLAG를 획득하여라  FLAG의 형식은 FLAG{...} 이다 | | | |
| 풀이 절차 | 악성코드가 심어져있는 한글파일(3분기-취약점-조치권고)를 hwpscan을  이용하여 분석함 | | |
| 정 답 | FLAG{\_S0metimes\_hW9\_do\_M4lic1ous\_Th1n9s\_} | | |
| 풀 이 과 정 | | | |
| 첨부파일을 다운로드 받을 수 있는 링크에 들어가서 소스코드를 보니    Flag is AES 128, CBC, KEY 01234569012345 라는 것을 확인 할 수 있음.  개인키 0123456789012345를 이용하며 AES 128, CBC를 복호화하라는 것을 알 수 있었음.    복호화하라고 준  NicYhtnsn5p5D2p7QBNAF6ORbPn6bcGDgxid3Zx5rCUv9GhbXfZngKqbwdOM+XHp를 복호화하니 Base64문이 나왔고    그것을 복호화하면 답이 나옴 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| C-1 | |  | 미기입 |
| 드랍퍼가 생성한 자동실행 악성코드의 파일 명은 무엇인가?  FLAG의 형식은 FLAG{PATH\_TO\_FILE} 이다 | | | |
| 풀이 절차 | 악성코드가 심어져있는 한글파일(3분기-취약점-조치권고)를 hwpscan을 이용하여 분석함 | | |
| 정 답 | FLAG{%APPDATA%\_Microsoft\_Windows\_Start Menu\_Programs\_Startup\_IIsExt.vbs} | | |
| 풀 이 과 정 | | | |
| 악성코드가 심어져있는 한글파일(3분기-취약점-조치권고)를 분석해보니    이렇게 시작폴더에 IIsExt.vbs를 실행하는 것을 확인할 수 있었음    윈도우가 실행되면 자동으로 실행되는 폴더이고 %APPDATA%로 경로를 단축할 수 있었기에 정답은 {%APPDATA%\_Microsoft\_Windows\_Start Menu\_Programs\_Startup\_IIsExt.vbs | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| C-2 | |  | 미기입 |
| 드랍퍼가 자동 실행 악성 코드를 파일 시스템에 최초로 생성한 시각은 언제인가? FLAG의 형식은 FLAG{YYYY\_MM\_DD\_HH\_mm\_ss} 이다 | | | |
| 풀이 절차 | 악성코드가 심어져있는 한글파일(3분기-취약점-조치권고)를 hwpscan을 이용하여 분석함 | | |
| 정 답 | FLAG{2021\_09\_09\_05\_47\_37} | | |
| 풀 이 과 정 | | | |
| 악성코드가 심어져있는 한글파일(3분기-취약점-조치권고)를 분석해보니    이렇게 시작폴더에 IIsExt.vbs를 실행하는 것을 확인할 수 있었음    해당 폴더에 가면 생성시간이 이렇게 있음.    IIsExt를 보면 %APPDATA%\Microsoft\mib.bin을 createObject하는 것을 확인가능    해당 위치로 가서 보면 이렇게 생성시간이 있음  그러므로 답은 FLAG{2021\_09\_09\_05\_47\_37} | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| C-3 | |  | 미기입 |
| 자동 실행 악성코드가 최초로 실행된 시각은 언제인가?  FLAG의 형식은 FLAG{YYYY\_MM\_DD\_HH\_mm\_ss} 이다 | | | |
| 풀이 절차 | 악성코드가 심어져있는 한글파일(3분기-취약점-조치권고)를 hwpscan을 이용하여 분석함 | | |
| 정 답 | Flag{2021\_09\_09\_05\_49\_37} | | |
| 풀 이 과 정 | | | |
| 악성코드가 심어져있는 한글파일(3분기-취약점-조치권고)를 분석해보니    이렇게 시작폴더에 IIsExt.vbs를 실행하는 것을 확인할 수 있었음    피해자의 PC에는 SysinternalsSuite가 설치가 되어있음.  Sysmon이 있는 것을 확인하여 이벤트 뷰어를 확인해보니    Sysmon에서 로그를 정상적으로 수집하고 있는 것을 확인    Sysmon view를 통해 startup을 확인해보니  프로세스가 2021.09.08 20:49:37에 실행된 것을 확인 할 수 있음.  UTC이기 때문에 +9시간을 더해주면 2021.09.09 05:49:37  그러므로 Flag{2021\_09\_09\_05\_49\_37} | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| D-1 | |  | 미기입 |
| 자동 실행 악성코드가 추가 페이로드를 다운로드 받는 아이피와 파일 경로는 무엇인가? FLAG의 형식은 FLAG{000.000.000.000\_PATH\_TO\_FILE} 이다 | | | |
| 풀이 절차 | Sysmon을 이용하여 스타트업 프로세스를 분석함 | | |
| 정 답 | FLAG{34.64.143.34\_%APPDATA%\_Microsoft\_Word\_Startup\_fontmgr.wll} | | |
| 풀 이 과 정 | | | |
| Startup에 있는 IIsExt.vbs를 확인해보면    파워쉘로 %APPDATA%\Microsoft\mib.bin을 createObject하는 것을 확인할 수 있음.    Mib.bin 파일을 확인해보고 암호화 되어있는 코드를 Base64로 복호화하면    이렇게 코드가 나옴.    Base64로 암호화되어 있는 부분만 따로 복호화하고 압축이 되어있기 때문에 풀어주면  이렇게 ip와 다운로드 받는 위치가 나오게 됨,  그래서 FLAG{34.64.143.34\_%APPDATA%\_Microsoft\_Word\_Startup\_fontmgr.wll} | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| E-1 | | Web | 미기입 |
| 랜섬웨어 악성코드를 다운로드 하는 URL은 무엇인가?  FLAG의 형태는 FLAG{http:// ... } 혹은 FLAG{https:// ...} 이다 | | | |
| 풀이 절차 | 문제 A2에서 특정한 공격자와의 통신을 분석하여 단서를 찾음. Admin.php파일에 파워쉘 코드가 2개가 나오는데 그 중 하나의 코드를 분석하여 플래그를 획득함. | | |
| 정 답 | FLAG{http://34.64.143.34/main.do} | | |
| 풀 이 과 정 | | | |
| A2에서 특정한 공격자 IP와 다운로드 시 발생하는 HTTP status code 200을 이용하여 다음과 같이 검색함.  테이블이(가) 표시된 사진  자동 생성된 설명  [와이어샤크 패킷필터링 결과]  검색하니 맨 처음 패킷이 admin.php를 받은 패킷이었음. 이름이 수상해 확인해보니 해당 파일은 바이너리 파일이었고, IDA를 이용하여 디컴파일하였음.  디컴파일하니 파워쉘 스크립트 코드를 문자열로 할당하는 코드를 발견하였고 파워쉘 코드를 복호화했을 때, 다음과 같이 코드들이 나왔음.    위 코드를 미루어 보았을 때 다음과 같이 플래그를 얻을 수 있음.  플래그는 FLAG{http://34.64.143.34/main.do}임. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| G1 | | 네트워크 | 500 |
| 희생자 PC에 명령 및 제어 목적으로 통신이 맺어진 시각은 언제이며 이 때 공격자 아이피와 희생자의 Local Port는 무엇인가? FLAG의 형식은 FLAG{YYYY\_MM\_DD\_HH\_mm\_ss\_000.000.000.000\_LOCALPORT} 이다.   * 정답 시간은 피해 VM의 이벤트 로그 시간을 기준으로 한다 * YYYY : 년도 * MM : 월 * DD : 일 * HH : 시 * mm : 분 * ss : 초   정답 예시 : FLAG{2023\_12\_16\_11\_09\_00\_10.10.10.10\_1337} | | | |
| 풀이 절차 | Admin.php 파일을 디컴파일하여 공격자의 ip가 34.123.161.169임을 알아냈E1다. 이후 c.pcap파일에서 ip.dst == 34.123.161.169하여 나온 패킷을 조사한다. | | |
| 정 답 | FLAG{2021\_09\_09\_05\_54\_09\_34.123.161.169\_58014} | | |
| 풀 이 과 정 | | | |
| Admin.php를 복호화한 결과    해당하는 파워쉘 스크립트 코드를 문자열로 할당하는 코드를 발견하였고 파워쉘 코드를 복호화했을 때, 다음과 같이 코드들이 나왔음.    따라서 공격자 ip는 34.123.161.169임을 특정할수 있었고, 와이어샤크에서 공격자->피해자로 통신하는 패킷만 필터링해서 조사하였음.  텍스트이(가) 표시된 사진  자동 생성된 설명 | | | |
| 모든 패킷이 58014포트로 통신을 하고 있었으며, tcp로 통신을 하기 때문에 3way handshake를 완료한 시점이 통신을 시작한 시점이라고 판단하였음. | | | |