[Ms.Moneymany's Mysterious Malware] Write-Up

작성자	김서영
분석 일자	2024.05.17.~2024.05.18.
작성 일자	2024.05.17.~2024.05.18.
분석 대상	Infected.pcap
문서 버전	1
작성자 E-mail	sykim1802@naver.com

0. 목차

1. 문제 3
2. 분석 도구 4
3. 환경 4
4. Write-Up 5
5. Flag 11
6. 별도 첨부 12
7. Reference 13

1. 문제

URL	Puzzle #5: Ms. Moneymany's Mysterious Malware – Network Forensics Puzzle Contest (forensicscontest.com)
문제 내용	It was a morning ritual. Ms. Moneymany sipped her coffee as she quickly went through the email that arrived during the night. One of the messages caught her eye, because it was clearly spam that somehow got past the email filter. The message extolled the virtues of buying medicine on the web and contained a link to the on-line pharmacy. "Do people really fall for this stuff?" Ms. Moneymany thought. She was curious to know how the website would convince its visitors to make the purchase, so she clicked on the link. The website was slow to load, and seemed to be broken. There was no content on the page. Disappointed, Ms. Moneymany closed the browser's window and continued with her day. She didn't realize that her Windows XP computer just got infected. You are the forensic investigator. You possess the network capture (PCAP) file that recorded Ms. Moneymany's interactions with the website. Your mission is to understand what probably happened to Ms. Moneymanyâ€™s system after she clicked the link. Your analysis will start with the PCAP file and will reveal a malicious executable. 1. As part of the infection process, Ms. Moneymany's browser downloaded two Java applets. What were the names of the two .jar files that implemented these applets? 2. What was Ms. Moneymany's username on the infected Windows system? 3. What was the starting URL of this incident? In other words, on which URL did Ms. Moneymany probably click? 4. As part of the infection, a malicious Windows executable file was downloaded onto Ms. Moneymany's system. What was the file's MD5 hash? Hint: It ends on "91ed". 5. What is the name of the packer used to protect the malicious Windows executable? Hint: This is one of the most popular freely-available packers seen in "mainstream" malware. 6. What is the MD5 hash of the unpacked version of the malicious Windows executable file? 7. The malicious executable attempts to connect to an Internet host using an IP

	address which is hard-coded into it (there was no DNS lookup). What is the IP address of that Internet host?
문제 파일	 infected.pcap
문제 유형	Network forensics
난이도	3 / 5

2. 분석 도구

도구명	다운로드 링크	Version
Wireshark	Wireshark · Download	4.2.4 x64
HxD	HxD - Freeware Hex Editor and Disk Editor | mh-nexus	2.5.0.0.

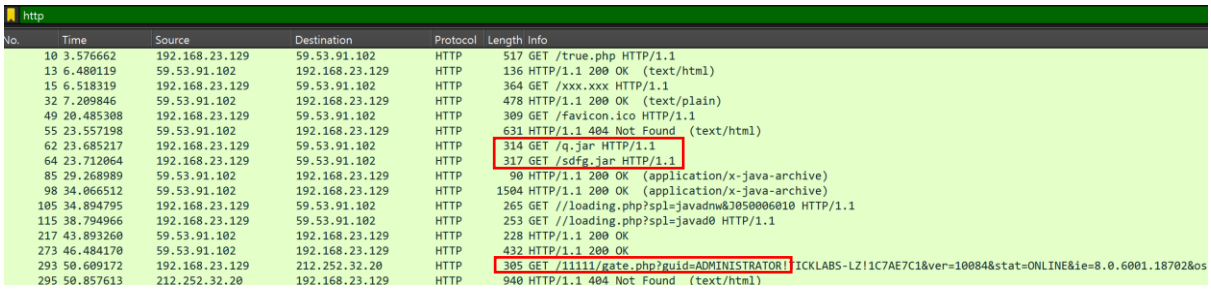
3. 환경

OS
Windows11 x64

4. Write-Up

파일명	infected.pcap
용량	189kb
SHA256	2a8780404d89e5588a3a032f2e69a8ee455a60d1cb3020ceebef2630b50db331
Timestamp	2024-05-17 11:40:54

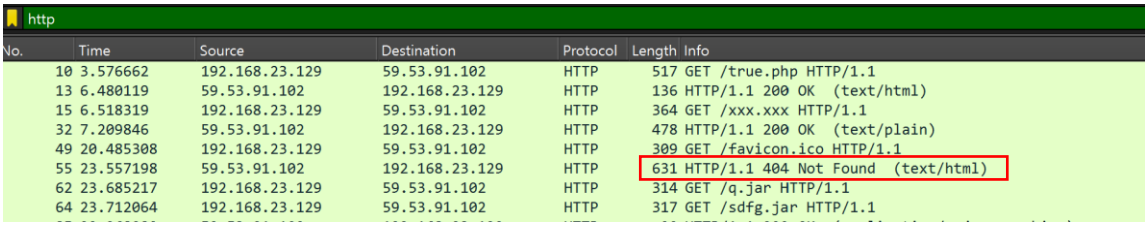
문제 속 Ms.Moneymany 는 웹사이트에 접속하여 컴퓨터가 감염되었다. 따라서 웹사이트와 상호작용한 내용이 기록된 네트워크 패킷(infected.pcap)에서 HTTP(HyperText Transfer Protocol)를 중점적으로 볼 것이다.



[사진 1] HTTP 검색 결과

1. [사진 1]에서 .jar파일 두 개의 파일 이름을 찾을 수 있었다. q.jar과 sdfg.jar이다.

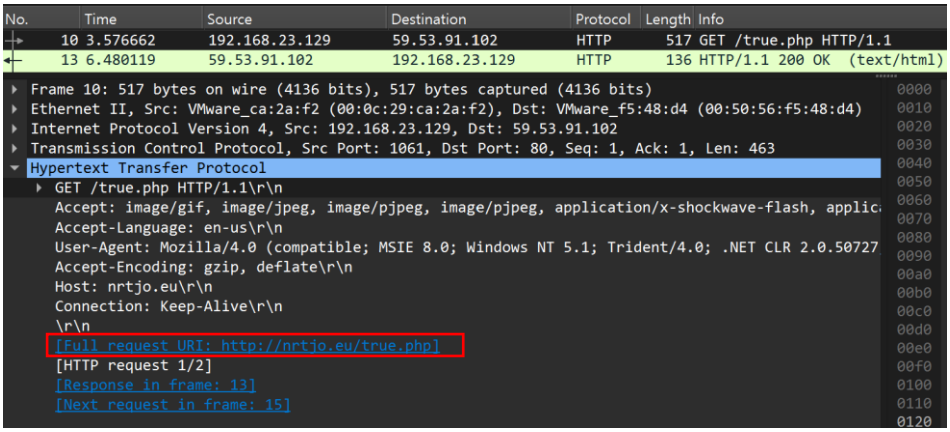
2. [사진 1]에서 guid 는 전역 고유 식별자를 말한다. 감염된 윈도우 시스템에서 Ms.Moneymany 의 사용자명은 ADMINISTRATOR 라는 것을 알 수 있었다.



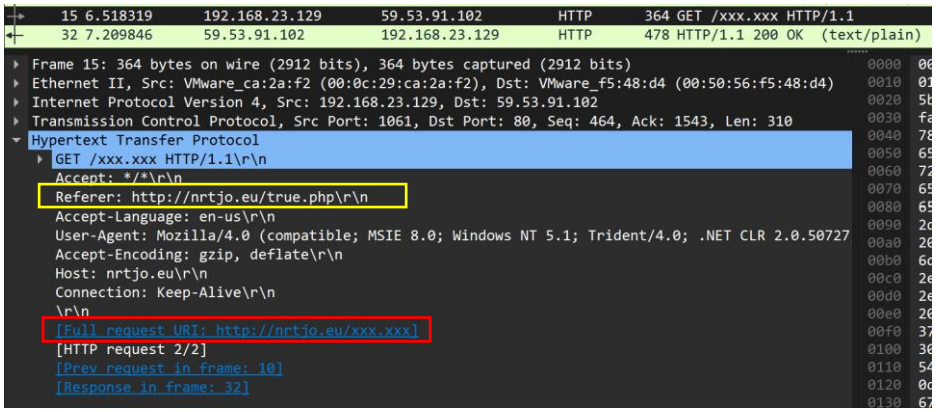
[사진 2] HTTP 검색 결과 맨 위

3. Ms.Moneymany 는 웹사이트를 클릭했을 때 페이지에 아무 컨텐츠도 없었다고 했다. 이 시점이 [사진 2] 속 No.55 패킷이라고 추측할 수 있다.

그렇다면 그 위의 No.10 패킷과 No.15 패킷이 의심되어 살펴보았다



[사진 3] No.10 패킷

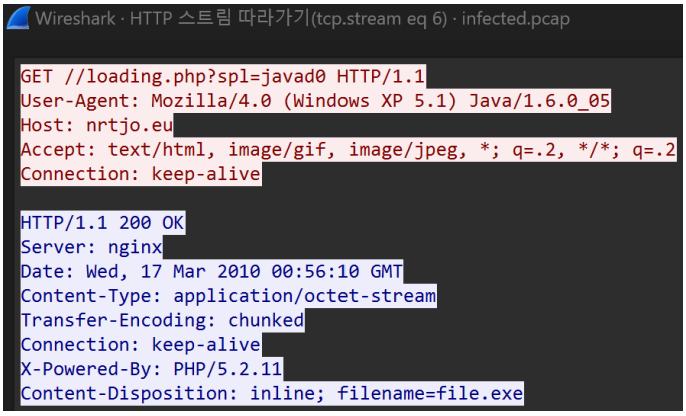


[사진 4] No.15 패킷

둘의 차이점으로 Referer 헤더가 눈에 띄었다. 브라우저가 서버로 Referer 헤더값을 설정하여 보내기 때문에, referer를 참조하여 현재 표시하는 웹페이지가 어떤 웹페이지에서 요청되었는지 알 수 있다.

No.15패킷의 referer가 No.10패킷의 url이다. 즉, No.10 패킷에서 요청된 url을 먼저 클릭했기 때문에 No.15패킷의 url이 그 이후에 요청된 것이다. 따라서 Ms.Moneymany가 클릭한 url은 No.10패킷에 나와있는 http://nrtjo.eu/true.php이다.

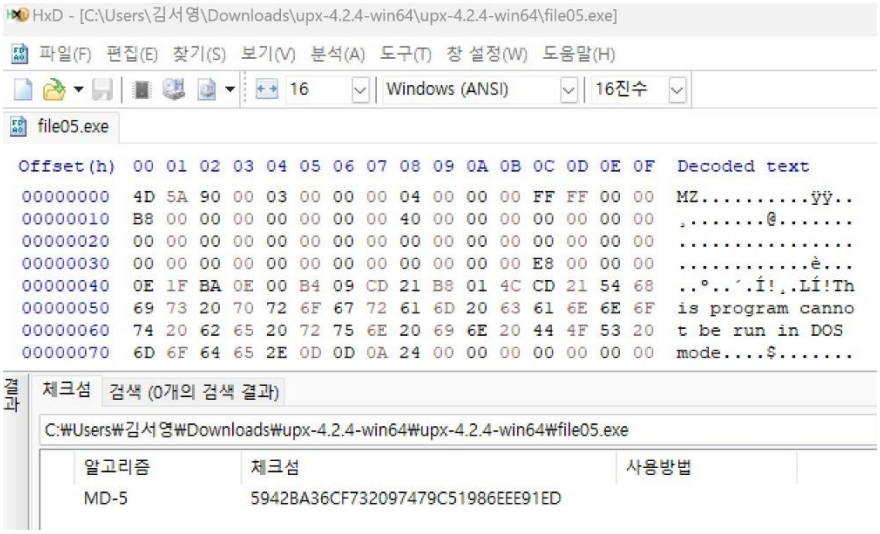
4. http 프로토콜 패킷 중 스트림에 file.exe를 포함한 패킷을 찾았다.



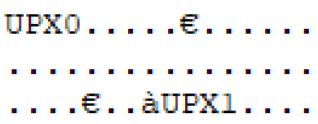
[사진 5] file.exe가 포함된 패킷

[사진 5]의 패킷을 Raw data로 변환하여 file05.exe로 저장 후,

.exe의 파일 시그니처 4D 5A를 찾고 그 앞은 잘라냈다.



[사진 6] Ms.Moneymany가 다운받은 파일의 MD5 값



[사진 7] .exe파일 HxD decoded text

5. UPX 패커를 사용하고 있다는 사실도 HxD를 통해 알게 되었다.

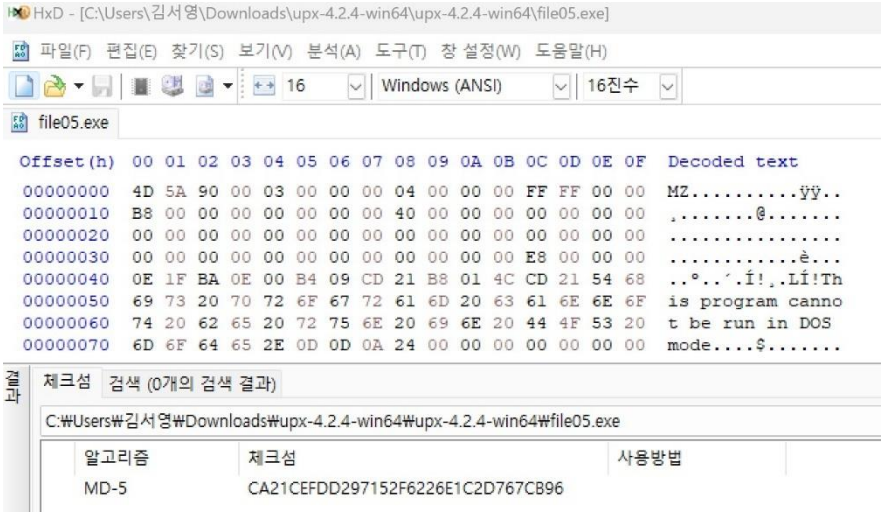
6. upx.exe를 다운받아(Release UPX 4.2.4 · upx/upx (github.com)) unpack하기 위한 준비를 하고, cmd창에서 unpacking을 했다.

```
C:\Users\김서영\Downloads\upx-4.2.4-win64\upx-4.2.4-win64>upx.exe -d file05.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2024
UPX 4.2.4       Markus Oberhumer, Laszlo Molnar & John Reiser    May 9th 2024

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     82432 <-     68096   82.61%    win32/pe     file05.exe

Unpacked 1 file.
```

[사진 8] file05.exe 언패킹



[사진 9] unpack한 file05.exe MD5값

정답과 일치하지 않는 MD5값이 나온다.

총 5번 시도했는데 모두 unpack하기 전의 exe파일의 MD5값은 정답이지만,

Unpack한 후의 exe파일 MD5값은 모두 동일하지만, 정답과 다르다. 계속 시도해보겠다.

7. 악성 실행 파일은 하드 코딩 된 IP 주소를 사용하여 인터넷 호스트에 연결하려고 시도한다. (DNS 조회가 없었음). 해당 인터넷 호스트의 IP 주소를 찾아야 한다.

우선, IP 주소 목록을 찾아보았다.

Wireshark · All Addresses · infected.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
All Addresses	303				0.0056	100%	0.1600	43.028
65.55.195.250	19				0.0004	6.27%	0.0800	6.957
59.53.91.102	250				0.0046	82.51%	0.1600	43.028
213.155.29.144	9				0.0002	2.97%	0.0600	47.151
212.252.32.20	10				0.0002	3.30%	0.0400	50.605
192.168.23.2	15				0.0003	4.95%	0.0300	2.909
192.168.23.129	303				0.0056	100.00%	0.1600	43.028

[사진 10] IP주소 목록

dns

패킷 자세한 정보 | 좁음 및 넓음 | 대소문자 구분 | 표시 필터

No.	Time	Source	Destination	Protocol
289	50.310134	192.168.23.2	192.168.23.129	DNS
93	30.666108	192.168.23.2	192.168.23.129	DNS
44	19.971014	192.168.23.2	192.168.23.129	DNS
7	2.930238	192.168.23.2	192.168.23.129	DNS
6	2.929185	192.168.23.2	192.168.23.129	DNS
4	2.909144	192.168.23.2	192.168.23.129	DNS
288	50.210596	192.168.23.129	192.168.23.2	DNS
90	29.821145	192.168.23.129	192.168.23.2	DNS
43	19.900252	192.168.23.129	192.168.23.2	DNS
3	1.987301	192.168.23.129	192.168.23.2	DNS
2	0.988900	192.168.23.129	192.168.23.2	DNS
1	0.000000	192.168.23.129	192.168.23.2	DNS

[사진 11] DNS 프로토콜 검색 결과(1)

[사진 11]의 DNS 프로토콜 검색에 조회되는 [사진 10]의 마지막 두 IP는 DNS 질의를 하고 있기에 선택지에서 제외된다.

표시 필터 | 찾기 | 취소

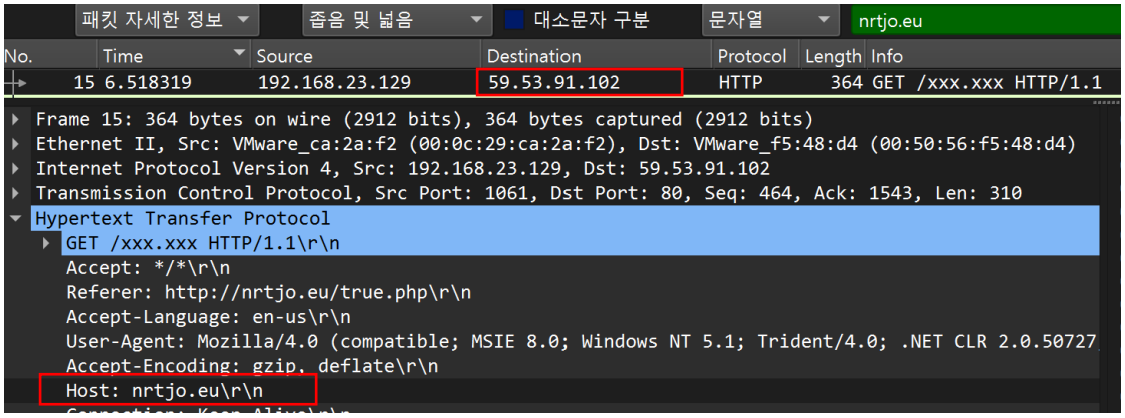
Protocol	Length	Info
DNS	235	Standard query response 0xbca3 A freeways.in A 212.252.32.20 NS ns3.everydns.net NS ns1.everydns.net NS ns2.everydns.net…
DNS	143	Standard query response 0xe78a No such name PTR 102.91.53.59.in-addr.arpa SOA ns.jxncptt.net.cn
DNS	162	Standard query response 0x5b1d A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com NS ns2.vnmhab.com A 59.53.91.102 A 59.53.91.1…
DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com NS ns2.vnmhab.com A 59.53.91.102 A 59.53.91.1…
DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com NS ns2.vnmhab.com A 59.53.91.102 A 59.53.91.1…
DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns2.vnmhab.com NS ns1.vnmhab.com A 59.53.91.102 A 59.53.91.1…
DNS	71	Standard query 0xbca3 A freeways.in
DNS	85	Standard query 0xe78a PTR 102.91.53.59.in-addr.arpa
DNS	68	Standard query 0x5b1d A nrtjo.eu
DNS	68	Standard query 0xfa1c A nrtjo.eu
DNS	68	Standard query 0xfa1c A nrtjo.eu
DNS	68	Standard query 0xfa1c A nrtjo.eu

[사진 12] DNS 프로토콜 검색 결과(2)

[사진 12]에서 DNS 질의가 어느 서버로 가는지 확인하였다.

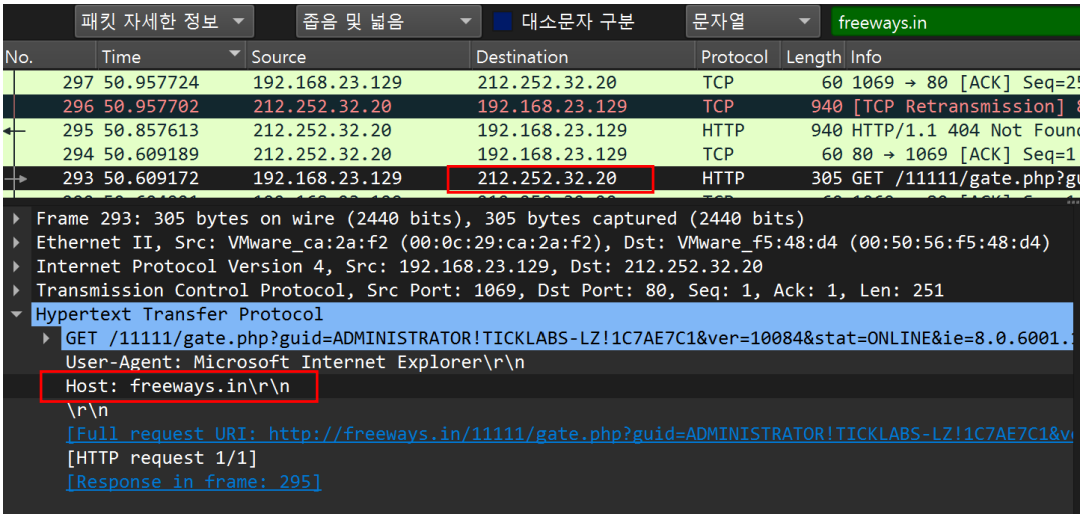
서버는 nrtjo.eu와 freeways.in과 ns1.vnmhab.com이 있다.

이 셋 중 하나라도 packet 문자열에 포함되면 DNS 질의를 한 것이기 때문에, 그 IP는 제외된다.



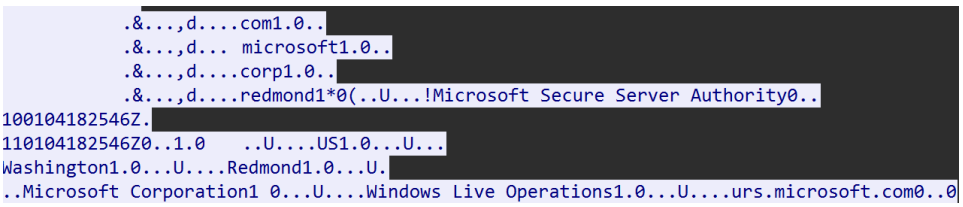
[사진 13] nrtjo.eu 검색 결과

nrtjo.eu 검색 결과에서 호스트가 DNS질의를 하는 서버이기에 [사진 10]의 두 번째 IP도 제외된다.



[사진 14] freeways.in 검색 결과

freeways.in 검색 결과에서 호스트가 DNS질의를 하는 서버이기에 [사진 10]의 네 번째 IP도 제외된다. 그렇다면 후보는 IP addr 65.55.195.250와 IP addr 213.155.29.144 두 가지가 남는다.



[사진 15] IP addr 65.55.195.250의 TCP 스트림

[사진 15]에서 IP addr 65.55.195.250은 microsoft와 관련 있어 보인다. 반면, IP addr 213.155.29.144는 길이도 짧고 별 내용이 없기 때문에, 악성 파일의 인터넷 호스트로 추측할 수 있다.

5. Flag

1. q.jar, sdfg.jar

2. ADMINISTRATOR

3. http://nrtjo.eu/true.php

4. 5942ba36cf732097479c51986eee91ed

5. UPX

6. What is the MD5 hash of the unpacked version of the malicious Windows executable file?

7. 213.155.29.144

6. 별도 첨부

7. Reference

- HTTP referer 란? (tistory.com)
- ch07 - 파일 패킹과 언패킹 (tistory.com)
- LMG Network Forensic puzzle contest 5번 (tistory.com)