

e055b5500085... (/Malware/Malware
/e055b550008507a6d99adc10267734bc3008237d)
/ Cuckoo Raporu (WINDOWS7-32)

Category	Started On	Completed On	Duration	Cuckoo Version	Machine	Options
file	2017-11-14 18:11:49	2017-11-14 18:12:16	27	1.2	Win7-32-AR07	Internet yok-0

File Details

File name	FlashPlayer27pp_ka.exe
File size	1566792 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	470FFFFB
MD5	83f895ae553fc08f45152cef1b449f614
SHA1	e055b550008507a6d99adc10267734bc3008237d
SHA256	8a569d74c63ff14a134b6484979be420496988e9836f71587051c51542b2ab92
SHA512	1dc6f6b81b16ba68d5462be7c494bfc8e0d6ae23862e374623d2804f231b2b49017be5e27c5fb06fca2dfe21855a197bc88a7b944f04fc89ec18a42a03920
Ssdeep	24576:MIx2M0/kx4P7KszrdwU3z6an06LWNLc5e1J0bxRtugx149hyf49+g723d:MDkukx4TrSLM0zeMx+599r
PEID	None matched
Yara	None matched
VirusTotal	VirusTotal lookup disabled, add your API key to the module

Signatures

The binary likely contains encrypted or compressed data.
Checks the version of Bios, possibly for anti-virtualization
Checks for the presence of known windows from debuggers and forensic tools
Tries to unhook Windows functions monitored by Cuckoo
Checks for the presence of known devices from debuggers and forensic tools

Screenshots



Static Analysis

Sections					
Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy	
ld00	0x00001000	0x000006000	0x00032600	7.98146514729308	
.xsrc	0x0000c000	0x000122cb	0x0000a400	7.94390210753105	
.idata	0x00071000	0x00000100	0x00000200	1.14514570815142	
	0x00080000	0x0001a100	0x00000200	0.260771276048256	
dicynvh	0x00221000	0x00013f000	0x00013f000	7.89782483669929	
tdhsnuds	0x00360000	0x00000100	0x00000400	6.34570981220974	
.taggant	0x00361000	0x00000300	0x00000200	0.777702729863249	

Imports

Library kernel32.dll
• 0x47f63b - lstrcpy

Strings

```
!This program cannot be run in DOS mode.
.data
dicynvh
tdhsnuds
taggant
JP adPep
i=cM+
X)fw
L9u" .E
!V0e/fr
d8Rq
Q25R4(
H60a(n0n1
jwancv/
JPoB)9L5D
DW o)
(S)LS!
!s5_o0
V0H1c1Z
McYYXd
"!)Ssq
Wp1"
xLZ/NL+
JXt 'S
j x(CS7b
5hv6S1
P8t Z5
Ju1P#9)
nk5'Eu
~u0p0+
S-0r1-a
j1j9p6A
J4'7Xp9d5+
y5)P5x
SV'//t
~u0M1
s1L_d6-
N-7">0..A
q8b"
oFvKKEA
x.H3jW2
b3V18
60p0T
f0dNLL
U:01"mu
/ACH.=I
; V0Ks
x:54) f
J'R1-
w=CUDR?
qyn155
55B'8..M
5D'Ks1
*GrBb_0
#127L2
z(30,[
JL8ioT
f"~q0V
2qPep1
'u1TF+5
!V0E1c1Z
x81Vz..URV..
Dw..P2c
6V+>1x11
Alva7Y6
```

mTK;3f
c60j7u
9V\7+8d
+jto82K
h\vez-
BuJ,nI
5obuyj7vy6#
h,0Kt7-d
!jMAN
v0597-
9o8n6G,Yu
r'Rdz(
2V7J'
Y69,9(
\$ B6i
8Byj7N
>#3-\
'u6l85
[C-C-CY
Um,0^K
YZ5m_1
NG66,0
>q-qw0U1
\$10W03
V
9p^5pb
"B1"m-Gu0
(,TsqWNSF
N(0c-
#0A-
t-0c6E+
E-Yu0
'0i325
ki762x3
i,uam07I
-q0Ly6<
4nk-0D
jy0V0h
7L7F^6C
2FjEB1
X0011s
Hl`^rq
_Y_0Y0K
-vc[6^
IVa007
xIj7^6
A00K1
\\lqqK
S1-770up
dE(w)K(-x
:67F0Hz
h010,708u62(B
bWwz05
HNG0uq
041-c10
a;okrB
BEX7)T;
W5
q2[00u 0
5je11)
aIR',y-
b10u V
+1u6,0
fny0R6
\$163L
qq[0H
i3m4on
1427TC
D
bvH5C_p0
0C,,0F,
0u07?
^V01s5H
-001h0TY
u,HLE
y0Yn3n1/y
U50HLE
52B(0^H
V0U0^
00q[0K
/(t[0U F
R000Lo
0P0r^s
FEL1y:
X^'^z
tkry)B5
+Cfy6k
W10u6F
33C7s>
bTc- 2
v--00
41j00q
J063700F
i,j0J^
16C7#2
X^7001
h^7)K6
YH)ki2
y00V
t668^q1
't4(7E
^7^000
Cya-1(
J001 V
A00R
^5M6n(2
0M^ 3y1I
i;u0K^C
Vj7zf
p32Z)
0F0y0L/
c;qw3
J0u0y0-
m-(07)
vks00v
u3E,1h
vE(0/1
J vc2)
J;0n0;/0
-"
'LE15
k0k/nh
_jz^E06)
01/r00
K78gvv
;^0a10
c-005
T0Xz00
yPy-01c03
1^kay
VU3707
3v^0K;
+07d0i3
r)0V)
e05P0U
\\0U;00
G)1zf
i,jt0003
Jy-LX
J5eqCX
[o32-4
[o^05v
40^33^
_30n
G;77000
S1-1105)
g0/b33
j400(a
i)1000
faddq"
K0T0V
M00K,
hPp/0UG
v0205^
0^0c160
X06;^0
J0072PW
71000n
T)Y-E:
^0^0-
U2)LT#
J7)0a0F
^0a0p-07
110C,10
z^0y0s
B0-00
R0^1r
000-14
5X0u0o,
2 y0A15
00-^,04
q2Eq0+

```

9CmZK7w
XL(/?+
m[k-k
ZC17fS
Sh1JCS
181[*
9;119"n
ze""n
KPUYDj
YKmqm0n
F'6w)
'c2HDY
m0JHL
P1Gz0Y
71(-40X
k7)+?+o
c3#6E
[+t3v11
sf33om
Ke"u'5
t(31a)
V5{4p;5
(v0vt/b
BQvDmC2
5"8 ju
He8p;:
"e30J
[Y,Y,C;0
21z19[+
5W
PaqD,*
EL(Pf+
"x"mG3Y
3135a)t
1f9w7
"-_E/q
rk=-89/y
\Kc-1a2z
+z1mb"e
t)KSL(
"sm-16
Krzzp0#
"1111
Ba_0WdJ
r6_3Yk
10_xl
+..0Pw1
Ymb;w
8T2Z"vq
P1Xy'2#
#bdr
->hcdKS
M48f5D>
NZfY,
NgtCaK
SMq0:9
j"yPzD)
V0p5,
nh_-9
JymHL
5U+6zZ
9ECaUYI
y1o""7
j0b)-=1U
B6o_6L4
v6-="v'
b12Q)z
0VU;E
D'c+eElo
5hvE-M5
KNw'o
oeEzw(
R/koh+
RzwtPw(
V96ajd
X16v?I
glp06;
d 137Eo2
x10M(
"q1 m5
44x6v'
x h01-3
0Mj)p1
[8"b"73
-.ahTo
+jc" 5
1500o (
p,c1o,"E
vtcf1G
DeD01
-c0JMC'11U
7NBw0;
115A;
C0,h,|e
ZtC'q|
QvTad
q"1s-ca)
o1486e
"41Q_0B-q[.u
xHfNNG
p0p0vA
#11)->
H51"qc
_071-(
1em-6
z04A)3fJ
h2C100)
"zE|
5,\{T#
j7Lz-6
kumf-)
052"1n
W0) z
+/0"ozL
D A+CR
000FZx+2
jpp3e~
F0_vh
E2F16
716x)31vcuk5
->bk"vq)
k8DMZ
Dr#9e|
FyG(}
h02).E
"-r3;L
F'A_s0
"d4P;
tr0rPdc
us
hCA=sd
7Lfn3
6c6d0hd
C(B13d
,fy1d0w)
Nde01X
)Xz2;-
1stcopy
GetModuleFileNameW
kerne132.dll
KEONE32.dll
2wH-(B
6uVdC
017v;
t 2g3y6zms
S)0w
GcFCpd
Gsp.1'
"papiK
H,6k2x
[0v]H
0v"v0
EQ30)0
80ymW
D2x106
Dv_a=]
0'5'11
Z;0aLwY
P2v_op
0u11fw(
0""k'P
d3J;R
0/0z0P
T(6+ 4;
0""q0H"
L4;1HnA
Dw(0K;N
0Mtp;1
Tq(KL""%
\0R,-2)
03hD
F1AGV53

```

n*H1L*
J27L7H
B7H J!
-pBR-
0-1C-
-"]Z7YKX
XKk.x0
zpi(Bb-
E(f9uK
0u013U
Z0u206
\$068Bk
yHr
1'1:91'm
M*1L-Q
1+0DS
ZB+ aa1
r1H"yd
70y511
Bba".,n)R
J00'10
Q:1'1
FmK1EA
u0u0'0
Y161kY6
9:1Y'11
23+70
-Vq4.r/
k'S0Sa
Bak1.7
+-063y
r1'122
/R'-10P
5Q5130U
*f0ny-.E
Jp-3)
Jhk"7T17k
hNE0'12K
BzBAB;
#90'/1
*F0Kx
h-1YFI
J1Aa-
E1.(
Jp080/
3.-012
11'10X0
n*1'-(a
3CfF00
90u)Cn
Jac01>
9100:.
+Btj(
1'vu:1d11
11'f200
93--00k00
Z1ev"
a0ky-R,
"SXLO:
u0'3'1c1
X->5))WU
X1L,1
H710Y<-d
vVR1PV
a'0u05k
tL.YH
J1ap*08
29k(H
Z1u0d(+
k0Tn)r
eq081M[
-by0d-
u2*151
p00'1
i+1a3'U
RW_R_k
R2+0,7
Cf1'04
"0e0(n
J1u01T
6u,5)K
-10u1t
Z_0u01
-1s00!
Mu0uK
"kvo):1qq
{20,C,
2'123-
-Z-ujt
30500
v0u0z
Vr1dp05
=
R0a/f0
J00n-y.
10f6v0
p0u00B
0kX100z
X0'-00
1LB0n
1e0u0
#-1210
c3x061
10070
/0u01)
C,"0e
c4C20W/
v0u0JE1
c-'P0J
J10k10
D)K0+C
L,R000,
*k0-10_10
0104h
"u0u0
101700
Jk0"0FU
E1J100
k10u0
"7L_0P
J0u-1'3
->J050
J01'*(
u-10u0
2'at0i
-E_x00e
71'11p
1Tt:Ru
u0u0n
B0u0k(
11500W
0.010007
r0Y-0T
UGZ104
V10P'6
b0510
Q0u0n)
#1'1210LH
u+k0G0
U1KJd
301v'
L
S700Y
J_-1C*
vY0R0*
"1010_0
J0J_1A1
S10-/3y
*1001
00K2p*
1u- X1J-
J)'700
Ru03Ry
11_C3
z' (.
b_X0
(010y
K0-u0
D'0P0E
Y5T100
S05'Dv
ART20100
W00n
C0647f
U1P0"00
1_001
Z(210P*
20p13
v-30VR
h0u0+
p10u05
->1'1)K

```
.ArY3C
^jEY-
fuRo-t
hd*42aP
Sg(0aP
UE*1b,
k- 0_3
MTYk[
kzRr(F
ahBe--pP
w 7X06fa
/Xs-
44jnx-
f2WA7_
RUE,"G5
j),140D
)LVXX
XRFqQRj
xcRn-
@Q+X4U1
766.0-
+1TfX
>L1K)x0
U.,A,1
h1...76
DIE(+*
j(00Y0_
-1C/JK
Yu1bc-
C0mhw
Ua/ozD?
H1-4*
^*x5TCU0
1771kz
0M_1_4
2IZ.(q
, Q-YR
A-a21--0
4q(r,q]
ns1jg
uq5.0-
)IR_g^
XD'0_0m
1 4 YV
jo)2v-
:JRMVYr
**YVM
'1SL-0
'1Yb4w[
dhqf,a
k xab[
-111Pwb
572/ AB
mb-1M2
)G060F
z'-5c5
0Y06Lah
RUh3yZ(4
iuf42X
Ah_0M
UMm+0IR
Rn(511h
h7508W
Z3(38h
J_0PMA
0770ER
zbDeL
VUq\ :x
05P[X
(hvQ' e
/112BAV
f'11..j
7v+qsn
1,5D+-
5b7V+Y[
'X_31;
_3x06N
kvNF~x
qW7/ q 3
B077/y
SER32_d1
ABaVjP1
T04q(55a
)Ro1'U'H
K-a2Z-
>dc(/
pBB3_tB5
> W'Y[
G1)Gku]
[0Wyz0
8C1 SL
-[aY9<
_0pRV
B04_0
ehAa1B
X5,hyTu
6aHVSY0
776e~)
4a02x1
\_(1K7d
yFz)Y0
)zax\
SK_op=
&,5:7
Sv+ t(
Pa2A*5N
..1Tb6
-S0am1/
x p03:
p (">
'3)).0
80z5
45X_1Td]
)050a(
5kDn-
c4r_B
1:(x)\
1C0P
H0a-d0b
JE'10"
2,1001
vC14L:
8u6)<
V'w-1<-(
= e)tv
)0YTC6w-
LS1-z05X
6_A0u- >-^
cMTrw
4L1305
c:1a5K
e1120P
(0RuU)
110u0^
h'W'E
P210Pud
5A007gn
^111:00b-
5Vrn0B
4-aT /
#544_
evk3d/
bPR0R4F
H_7pb5
u0T'0B
'1'h<0
+ ,9GE' H
j)Dvf(
100uF
cTV4(
NE*00:e
)6q_ r
q5SH7' H
K_R1]z
VcChH
oht3B]]-
34R1,d
F9ct*(
4'wogUA
L-w00)
"55'S;
Except1
on_1nf
_h--s- f
d)6 B C
4a1(0[0[,P
1uH(0]
_W0017H
-mv_v0Z
h0Hx0)
3]1z'D
Fa,"2"
```

```
u,f,eFBD
>ltoc(-
#oUF
-[p#RQ
ZUCX>
'>-ug4
J]n'up
+68U)
J]b2+
ak-Spk
rQpda*?
ed2,"PC
"evt\
+SK'X)
yDCvfg
P"UGZP?
1fZp6wz
xDr'x06)
FURP f
[vtGg&/
~ZJ,UK[q
I<-v% 4
FA'7'0
jgsD
A"4'xt
ZupQZiP
To'xHf
j0XKH3
XB]j8I
Cht,edH
gZcX9
t6o92
00"8]
de0z0d06)
SA7K1
SZBapi
[Lo63
cy0z0d0
0o/v0V
"HNk18t
4u->v0H
v7B1b0
fx:vyj7'5
jYUd
L10t1],
vneB10
uFCd
U03-1f
->[x\jT
0Y"%
#X'hh:>
4h-ug?
gaLS1(d
#-c04183
6on8B7'L
gr,-Z3>0
/uo70H"6
ZV000L
b"ajrJ
a'Y0V5]
Tj6xZ-
"0101%
4wFj-
'vaJ5B;
[ss7U0
~q1x
w1"1L
DyPaJy
s36J5
CHWzLn
$'c2'w'
cx/BAZ
Y:0kx5
a7X'7;
FeEfvXy
lqDZM
0K'x0B
A0w6Z0
:518L
F+0H/
cF%ZTh
Xj0p-
K9D'c0
h7YVvV
l6z0Wv(gc06,
b/0jB)
0915p
/24-0
_Kj'_M
0'0'X'-7e
Q10U1
15[1xW
_jFk+
'110b=0
'1'11s8WV;
E'75JH
i=P7'M
T";9y
j,30qj]
jZ'vk"-
[1;+14
z,y060
ShzaonB;
uuj'_d
F6c6AJj
d0-4a1
d0X5x
c5'j0hX
jX2w6A
bNt1f0p)6
cR1ZlDq
00"1::d
Fp-4j(C,
N4d,"e
~8a1A]z
b20xvV
ZL120P
J'00
P0m'd
5gZJ
/0wvLL
d'50B0
u-(%
"XJ30p+
W-tN[S'
1N0Q00"
VAj,Ed
Dae",8
1420:5
p,al0,
Vj(M,L
Wt51+
j>15'('
00;_J)
76dau0p
5"7j6Q
H/\(0uCN51%
uta,H'P
,01Z-0
0P60L
a0P6<
Bj16-T
C55PaY
YF0Kv
'1b1g
Jk'5-u
&KVra#
r6400"
j)70zE
J7LF0r0LL
J(0'Pd0B
2H'4'x
p81Bw'Xc
L'up8A
P'6N(M
A(Rh70
"-0z,
&0H
"~y3U"F
j"~W,
D=V1:B
4'8A'0
d700q+"
'1e0_e
s,s-n
y00je+
iP0h1x
0y0=0Y
00"')
N'L=0
P0W'x,
htNj=J
```

Jv20 (tU)
^4G0Hz
AVr: g^
9L^G2n
xy0REK
X1skP1
I' uqg
b0Z2w
_jd8R/Pa^"]
x0B0FJ
hh^ ly^
s9J70a0p
^'^u011
j1(H+^
b0V)7y1)
XZ^m
7w1^_dmZ
NF4LXQ
TcCC: 50
CEU: 1
xJ>>->JPL
J5Q0y
:(s0K
8^derq
W01006q
EB.\'
V0e(w
qq: E1+
_a6_Y9
[m0A^vJ
s\ vy1
P^: P1
^m0(L57
I b7J
Ns0: 7/
x5W0)!
ZF[j4<
j^_P^J
By^f(1
31R0Kx
6K^: qn
vM1^gr
a1/: B5
Baw #Z
^m0Bk
^V^U0W^
caf/A0
^w2A
mY1E1)k
0A./0)^0P
QBH^W0\)
NB[]
K^7W0A^~
^~^"00
_ g0T0_3<
SW[_2]
8m34C
0_7J00>
Um)KL: 05<
D_P0
v0)b v
pa0+^H
/0)Q1^
'5yR,[0'
5K_0u0
^f(j_p0
Q_VV1^
JF_y2
c1VYV06
^a1^chu
010)0_LK
551(a/I
J77Y00
+d2u0x
QZ1NKT
_o-XIY5
^5^u0q0q^
'jBr)^
W0:2^s1a
P00L_00
UB0w
J' Ev1F
2^~0d+
^j)0 1J0
4+^0000
^Sur^%
(N(L1~
4000\)
Ps::z7
X1u0)0
s0
5_0A27
000L^H
V00K^S
2d\Y05
_j^0P0
a1\% "00
,m0wP
_~0^m0L
^h)0N0NT
J^5H_5
6y0JTB
j0^00Q
T_Y5:P
^~0^ b
N5xjyh
r00Jp^
j0~4EUBC
R15J00
m.H
_jY0TX
~000A5
r1f1f1
Fx:a\000
DM1YH
r1qy1
s1f/y6
05L_+
h0a /+
0z,<^U-
0r0=0L
N0P005
t~0k0r
4_/z, (
zVu_0b
Zz::j)0,
T000J
#0b00(1 %
#05=00
<~02)
P00J0^
L00J1
0^~^~^
0)Z 55
0V00z+
5uKVP^+
^kZAS_|
0m^/12)
0-A_0^
05000000
7aJ000
E100d(X<~
^00000^
V0NF1T
00p500
[05p\)
^: P05/
F7510z
^1T00~
z04(7TR
40v7PP
00C0041
j0t00a0
_j0L02
V1L~00a
X000YJ
X-Y)00
j0^=0v
05Ct 5.
^~00u^00
^u^706
Bj)0^2
w0C11x
^00L^j0
q00)7p
z_/z 0
K00u00
10A~0v
V0^00^0
z0L_LJ0p
N50v_4
0K^1\)

```

Bw jJ5
8j9u5AB
62Hig*
gJnd'e
54
8H-64r
-g29rq
i708c_v
y80ms11
Z11J
Vn3pe
KWh1r
M8_7u
67<+^X
5g1+q(
f0LlQ
$1t10_QF
N2_BFe
kgc8mg
2Mq+5 m7
Jcp0H4
*16ZDL
yn;711
.55'20
048( t+
X5c10
-lLcH0)0
Gs:TP6
n819L
FBL6y3'Z
HH-0267
Jya'61\
-s6+
RPH8Lx(h
8K_3Ld
lu'6:F
[5'7+
*8K'w1
5(01
AP'S)+
915)+
K' U7B
b7H\,
|
0W16A^6
47W2p
[4'V 6q
MhJq\
n_ 0XY
17>#'/R
bq8K
--c9
aP87ff
5Vky0.L
6'; 6+
'vVW1d
8atL[
FF3zn1
R8a\h5
71ag\+v(
5V\'s's'
o)808W
ghu /-3
M]M+0]P
Vhp10
m6L7gV7
'8i.N)-
&P+08R
AZ'+snpf0
z'1'16;
w-vZ(')+*
'H*6-148K
od 9Y<
Z8)7wz
04L1';
W_ 018
Y2+3
f6R -L
&18g_c
VU38+ t
ePJ)5L
,1-0E5J
07-
b-'p62
saaKXf0+
:'VYX:0
07)ZzJ
\66m,
-vLtlV
Pa8u_p_0
$70U1+
sh:02K
0W07 FF.4
K8qfC)?
1Tcgprry
+VupT
Yy1nfq6
s6G 05
T'->+E
6x([#R0BIES
ow56):u
c8L1\,
J45#n0
c07fx4;
/2_880
tt0+pt
aVW0L
E11+V'P
v2_j4/
XW0P'c
;''CvWU
\30p_J
->'1(1
B*]/8E
01[ 15
' f86+
'1XugE
1_j_3k
'77]:L
j013h+
J_3580r
y5'-+*.dk
cg_R+1
\,8pvc2
x2NF+V
8ut80-
Y15'85
H5Bf0+1
B_R0+e
s+8p0
x_05-qvc
X(27L+
0W 1H
jn)6;/h
'c 1(1
JPFfL+
p7_K5
+01)'su'
2_rmC6
A'PaMc
a0f0P
h'cV->
t1X)19
k_5-W8
+2_<2)
rf(1)P
b<'C,i
M/0;
08P0Lk+K/
D108pk
kl_0t
;K510af4
mw6L+
h1ed+
r'808U5
70ma7
-e;-11-30
W)10;
8Kx6 h'
'0by2)ck
[_\
tJ)80ppu
1000TE
dV63 &
I_7u0.N
;1Yaxz
k11060'
7u0W09)
5h(k_*)'
mX1_L
bc10_pk
Pw-hg

```



```
BTL sgX
gITZr+0
('y0Qm%M
NyET00
/c+td05
r~u0a6
h2~hg1a8
Dm000_5a8
0\\M0H>
Bwps8
bf ~u0a6
e5)
L1(.F00
Wz1)0H
y,8%-20d
000012
:0L'8"
FR)XLC
vTz,cJ
D.TqT0
^a~3a8
46#z>g
Bwc9dw
0.X2F
q-()WT
bpb'1
[+px-
0:g/0p
ta=0]s8
~v0-0-
]Lus%RL
Sh904
MyfEd00
dLB5v46
d1117)1
wX_04t
250dw0LbT
0t;+;0
Jpy1DU
C<-c49
v6d0"
500_3a
1+0\\0K
00_0F6Z
6-706F
Jm+T10
\\00-[
550u0K
3000u0W
>01(xK
W:70/2
!c11.4p]
*1z 3B
V50H~0
6r70CZ'E
[eq;:I
Jh,u0P>
J'h.YW
50]S2-
x0+Tt
a0U1_
qf0ys6
[0pux(
F..A$
Z1'80
\\1z 30;F%-
04v0z:
E505z
Z00N#
[1E1\\0-y
300-0-
ur00SU
1]s)806
'g0L~0V
++T~V
\\PxT0q
00a)~
\\tth0n"
LC4(0
~110//
0[\\A),
11(11140
e~0n"
Teg0010u
d_10p4
0F4q
0K(-v"
d1020+
'JX..
h:0
\\wFJ0n
:2%5"
TL0/1
B1-00-
R(pT00
0_PaJ0>
20V1q0_0
V00=EnTP,
r_H0p(
n20y0n
00'7j0
0K1.)
Uj0=)
mT5\\41
m0T1L
xh1=-T
00n0n0LJ0
g0/00
W'j'tt
vC2"00
'000Y%
t)bc0N
0N00'(
ELP2;4
Vg10"Y
H00-;
\\00C0z
W00W00
0Yy00)
*k4"0(
1)-12P
g0R1-U
yx010"
P0000~
B03d7r
\\w=00B
000011
\\XGL/Z
~Y=JK
000110
Sh\\011(
wY0_0F
t1"-P0
H0z50A
~70n0Q
z'00-
L00n"1
hr 6."0H
~\\L00C
\\A
h01J0J
n5T0N1
9100z0H
7100_5
H1"(G,..
-Y1J
(G:A'n)
B0=0E10W
J(T1L
H0A=06
P1P':]
k0u0K
Y=Z000)
400=0U
\\001
pV('pL
/00-0
2_1CJ0
00y_P4h
0000+0
62)C00
7(X0P>
k0C~w
\\u0K_PJ7
J_jth0W
010Y00
jA1"0
+0100L
144_bFY
t0Rf:;
W005:z
5
```

```
FcUcb
. x 13.
#qBo'G
Y:40 0:
0FLvYP
-:"vSt
##2:1
X1.B-X
00(Rq/efh5a
9u6K1
LWvLSK'Y
Eu' _U
)jEz-w
zunc'v-w=8[
7VY'1
8nopyc
x., 21H
|'=-11
o1955
n=F.ZP
1-2J2
u.TdF
:z*97
h-[VX
P':57w;
ZG/VY5{
\10'h
j%3an=
H0cx38
+Z0U'1
X104r
'5U'8
Qud('=D)c
XE3T,
De('=)
7.JB d_1
c0KZ51
L1=7q.1:M
1UrD65
dFa,h--\
3k.R21
x0Tm0Lr,:
0m=K70
1221(-
dM0L0V
d0Rz1F1
:~Vj/A
d97GT
3V1um4
LuXz{5E1
{7aw
9q0T00
G*510,
/z,1W0
C1+73A
jYKzH6W
<167nd
71jE70
DMBL_0
204K\
+ 953<
'1jF08
H-q01
.JL1-57W=0
"10u1
v0Z11;
1uq_7*
3aE100
oa37+
{YRp{(
ca.28vv
_FK|HP
~K1X1:
(50416
755s' -
/b40
9uT0c5e
C/(-1)7M
|0gP7P7X
b'a,w
'A ad'Cl0q
x%uL0A3
'1 y00
y|P145
60ph211
6Q.H.N
G|1u09e
51s.4+
VW0gZ.
T54v;
1u0k.A5
VW.50r
E8BT1+
"0R(4Sp
7e
)38u45
KXK<v>3
09116v
111H
4aATW;00
ZZp0|
*60BZ
Leh1,00
7aA.a(
q'SK;
ZVC1'(
RTD00
J1-h'X<
7sB v5
25<1)
t0
'80awC
5.uLP+
a11ALZ
0103)\
rPj(\
:60Y6s1
M00Kc
afterF0H
10115H|
m0pk
r.1'21
Lx21e-
0.N0B1
3p1+_*
LXcLP0
0u10P0p
1F
P5>ct0
By'p0J
,0HT T
1C1+V6J0
-(2x:
13<200
b07rpaK
v0h07P
071F.h
100
hguv\
"50AP
U01D0%
.
2a010V
KR J'E
01PFG0
V2x+1jA2r
71- PT
,u'W0a
6-c0314B
"0p00_
1K0B10
g00V10
_A1YK2
\1216TH
kLP 117
W00u"%
0|0'SJB
"x21q
*6ze1
J ed00P
"U0>|L
m0'.r21
r1C0VTE|
pXU-VXK
A 5k0L
d-c0PH'as1
M004C:
101fAr
15aYf/R
PK1UFA(
400DaK
BR5qV0t
```



```
5MDjw(2i
LhRe 5
HVXLENH
pb6c0"
8I"~dx
?"IX5]
5n)ph(T
a 4 0oy
H|b-0F8
JbD(hA
0_0m0-
coC4uB|
D8 4~7J
'ge0-[0:
kB,A"/0M
a
sz0#1)
Np)7;t
Nl<5F3
m"0 _q
0n5Fgn
YPhed
Lh)CkAP
pT640TP
zQP#0()
Nt3 26c
0L5"
"XSh1b5
b
K0KV1p5
K15 8q0
J500%
00T("5
(q)6AB
8uaj4K(C
4V06aX
b7T0H5
00PT++
79ub1D\{
W5Q<SV
C7u0L1
0 E0Dr
g7b0+
(L;p-K6
FVY_0p
' + 8UD
LshQ6
'FX0Kfs
j1_46"Z
Q~.H01
d T0wZf
wL_0(
h/BS('
W0 985g
"00Y0+
q|Du114
M2cT)
0W09g1
VlBq(<
(q)074b
HLSKti(
X08e-D
N06a-
.noZ5zg
4C
(G)20M-
J2P7X
Ka1400_0
07M1<
F7e-GJ
D1E_+4+
L,:?>v
0K7E
Q 0/0
Ch|nt2|5x
::< <0
5m<0|
J;pR19
J/|00
H01~tV4
+8|BP+
B0+b0|<">1
H66x70Q
Lsp{WS
Dv:1: S40x
+E4,.a/
:~A0b-f
50b~1<
t4tFx:J<
L<0>0-
P560T
TUG/09
Lm0060
T66C-Q+
~04|vC:
p000\
Wkg57)
Tsk>0<
>5p00
"~ez_0
4K0:0:
>500|>05
>X_sw:0NGA
>J7000
Z<0v|>
"EN|xx
P7L~L~H
4t0'D_0x
5p|u0
de|W0
J7N_x4
'8C0+
L'00can
0Jw~0')
:011(t
'0000(0v
5-Ph)
t0FEAL
B 3pV0
5Zy0 H0B1
W0R'0'
A1"
K'L0H5
b'0L_|
' (t+P
195|X.
3115
coP1v
1b0|H0
r7k_P5
")1b/
H1D:20
$F2s4q
q|K<0u
\c|k5b
(bN0rJ
J(AZ00
,~0ry0
L)130E
c_KU|
: 4cT4
"scFLDxx0H
0W<K|0n
0730c
0uTYND
J_77n_0
K01('"
x14|AL
m00v0P
08b_Z|
"0_x1
11k|0w|
.1'V|p|
L7Fv
K1Avp_Y
{105.3
y0a000q
dXyLW
_054R01
"0uL_G
(tm0:
/0B0|Q
>0T|05
('Mdu|9
R0+
"05|c
, 'J1Pd
~>N'12
90-91Ld
y'TOTALGc
1~>0L
[0+ 'N
```

[illegible]

Dropped Files

Network Analysis

[Download PCAP File \(/CuckooReport/PcapFile?reportId=5a0aff5017c591044899bc25\)](#)

Anomalies

- **unhook LdrLoadDll** Function hook was modified! (pid=2484, process=flashplayer_27pp_k.a.exe)
- **unhook NtCreateFile** Function hook was modified! (pid=2484, process=flashplayer_27pp_k.a.exe)
- **unhook ExitProcess** Function hook was modified! (pid=2484, process=flashplayer_27pp_k.a.exe)
- **unhook GetCursorPos** Function hook was modified! (pid=2484, process=flashplayer_27pp_k.a.exe)
- **unhook AddrInfo** Function hook was modified! (pid=2484, process=flashplayer_27pp_k.a.exe)
- **unhook gethostbyname** Function hook was modified! (pid=2484, process=flashplayer_27pp_k.a.exe)
- **unhook send** Function hook was modified! (pid=2484, process=flashplayer_27pp_k.a.exe)
- **unhook closesocket** Function hook was modified! (pid=2484, process=flashplayer_27pp_k.a.exe)
- **unhook SocketSend** Function hook was modified! (pid=2484, process=flashplayer_27pp_k.a.exe)

Behavior Summary

Files

Read

- C:\Users\X\cbs\bt7-32-A907\AppData\Roaming\Xywxexa\veaf.feh
- C:\Windows\system32\ntldr.dll
- C:\Windows\Fonts\staticcache.dat
- C:\Windows\system32\rsaenh.dll
- C:\Device\KsecDD
- C:\Windows\system32\len-US\MSCTF.dll.mui

Mutexes

- Global\{597DE0D3-1A8D-477B-F787-939FB57D1573}
- Local\{231CC6A1-3C7F-3D1A-F787-939FB57D1573}
- DBWinMutex
- Local\MSCTF.Asm.MutexDefault1
- Local\{0EB77469-8EB7-1081-F787-939FB57D1573}

Registry Keys

Read

- [illegible]

- (A6EBE008-07F9-400D-B8EB-337A64F7051F)/Category/Category(534C48C1-0607-4098-A521-4FC899C73E90)
- (C1EE01F2-83B6-4A6A-9DD0-E988C088EC82)/Category/Category(534C48C1-0607-4098-A521-4FC899C73E90)
- (0C8D69A8-923F-11D3-85B1-00C04FC32AA1)/Category/Category(534C48C1-0607-4098-A521-4FC899C73E90)
- (E429E25A-E5D3-4D1F-98E3-0C608477E3A1)/Category/Category(534C48C1-0607-4098-A521-4FC899C73E90)
- (F25E9F57-2FC8-4E83-A41A-CCE5F08541E6)/Category/Category(534C48C1-0607-4098-A521-4FC899C73E90)
- (F8F8E938-8C3F-4D08-8AC2-0F816C09F4EE)/Category/Category(534C48C1-0607-4098-A521-4FC899C73E90)
- Software/Microsoft/CTF/KnownSwitchesKeys
- (F1832785-6F8A-4FCF-8D55-78BE7F157091)
- SOFTWARE/Microsoft/CTF/KnownClasses

Modify

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Qysa

Processes

registry filesystem process services network synchronization

flashplayer27pp_ka.exe PID: 2484, Parent PID: 540

Search:

Show 10 entries

Timestamp	Thread	Function	Arguments	Status	Return	Repeated
2015-04-22 20:11:54,137	804	NIDOpenDirectoryObject	DirectoryHandle => 0x0000007C DesiredAccess => 15 ObjectAttributes => C:\Sessions\1\lsass.exe\Objects	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdLoadDll	Flags => 7268764 BaseAddress => 0x76ad9000 FileName => KERNEL32.dll	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdGetProcAddress	Ordinal => 0 FunctionName => LoadLibraryA FunctionAddress => 0x76b22864 ModuleHandle => 0x76ad9000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdGetProcAddress	Ordinal => 0 FunctionName => Process32FirstW FunctionAddress => 0x76b13897 ModuleHandle => 0x76ad9000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdGetProcAddress	Ordinal => 0 FunctionName => RemoveDirectoryW FunctionAddress => 0x76b877d7 ModuleHandle => 0x76ad9000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdGetProcAddress	Ordinal => 0 FunctionName => QueryDosDeviceW FunctionAddress => 0x76b87ed6 ModuleHandle => 0x76ad9000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdGetProcAddress	Ordinal => 0 FunctionName => Process32NextW FunctionAddress => 0x76b13155 ModuleHandle => 0x76ad9000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdGetProcAddress	Ordinal => 0 FunctionName => FindNextFileW FunctionAddress => 0x76b1cb2d ModuleHandle => 0x76ad9000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,147	804	LdGetProcAddress	Ordinal => 0 FunctionName => VirtualProtect FunctionAddress => 0x76b158ab ModuleHandle => 0x76ad9000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,147	804	LdGetProcAddress	Ordinal => 0 FunctionName => CreateToolhelp32Snapshot FunctionAddress => 0x76b12bb1 ModuleHandle => 0x76ad9000	SUCCESS	0x00000000	0

Previous 1 2 3 4 5 ... 207 Next

Volatility