Hellsing Indicators of Compromise

MD5s:

```
015915BBFCDA1B2B884DB87262970A11
036E021E1B7F61CDDFD294F791DE7EA2
04090aca47f5360b84f6a55033544863
055BC765A78DA9CC759D1BA7AC7AC05E
085FAAC21114C844529E11422EF684D1
0BA116AA1704A415812552A815FCD34B
0CBEFD8CD4B9A36C791D926F84F10B7B
0CC5918D426CD836C52207A8332296BC
0dfcbb858bd2d5fb1d33cd69dcd844ae
0F13DEAC7D2C1A971F98C9365B071DB9
0FFE80AF4461C68D6571BEDE9527CF74
13EF0DFE608440EE60449E4300AE9324
14309b52f5a3df8cb0eb5b6dae9ce4da
17EF094043761A917BA129280618C1D3
2682A1246199A18967C98CB32191230C
2CCE768DC3717E86C5D626ED7CE2E0B7
3032F4C7A6E4E807DD7B012FA4B43718
31B3CC60DBECB653AE972DB9E57E14EC
3A40E0DEB14F821516EADAED24301335
3de2a22babb69e480db11c3c15197586
4DBFD37FD851DAEBDAE7F009ADEC3CBD
4F19D5D2C04B6FC05E56C6A48FD9CB50
58670063EC00CAF0D2D17F9D52F0AC95
588f41b1f34b29529bc117346355113f
5dec2e81037b2d72320516e86a2bcfbd
5f776a0de913173e878844d023a98f1c
5fc86559ae66dd223265540fd5dfaf3b
621e4c293313e8638fb8f725c0ae9d0f
67E032085DC756BB7123DFE942E5DCA4
73396BACD33CDE4C8CB699BCF11D9F56
824C92E4B27026C113D766C0816428A0
8BEFABB08750548D7BA64717D92B71E0
8E5FD9F8557E0D39787DD205ABFFA973
9317458E0D8484B77C0B9FA914A98230
a23d7b6a81dc0b460294e8be829f564d
a642c3dfd7e9dad5dc2a27ac6d8c9868
A6703722C6A1953A8C3807A6FF93D913
```

```
aa906567b9feb1af431404d1c55e0241
ac073ad83555f3748d481bcf796e1993
e8770d73d7d8b837df44a55de9adb7d5
fe07da37643ed789c48f85d636abcf66
```

C&Cs - hostnames and IPs:

122[.]10[.]9[.]73
122[.]9[.]247[.]4
122[.]10[.]9[.]155
122[.]9[.]247[.]4
23[.]88[.]236[.]96
122[.]10[.]26[.]24
a[.]huntingtomingalls[.]com
ack[.]philippinenewss[.]com
af[.]huntingtomingalls[.]com
afc[.]philippinenewss[.]com
afnews[.]philippinenewss[.]com
articles[.]whynotad[.]com
ccid[.]mooo[.]com
d6[.]philippinenewss[.]com
de[.]philippinenewss[.]com
dec[.]huntingtomingalls[.]com
df1[.]huntingtomingalls[.]com
df2[.]huntingtomingalls[.]com
df3[.]huntingtomingalls[.]com
df4[.]huntingtomingalls[.]com
df5[.]huntingtomingalls[.]com
email[.]philippinenewss[.]com
email[.]philstarnotice[.]com
files[.]philippinenewss[.]com
files[.]philstarnotice[.]com
freebsd[.]extrimtur[.]com
gr[.]philippinenewss[.]com
guaranteed9[.]strangled[.]net
hosts[.]mysaol[.]com
ima03[.]now[.]im
img02[.]mooo[.]com
imgs09[.]homenet[.]org
knl[.]russkoeumea[.]com
login[.]philstarnotice[.]com
mail[.]philippinenewss[.]com
my[.]philippinenewss[.]com

na[.]huntingtomingalls[.]com
na[.]philstarnotice[.]com
new[.]philippinenewss[.]com
news[.]huntingtomingalls[.]com
news[.]philstarnotice[.]com
ng[.]philstarnotice[.]com
ns01[.]now[.]im
ny[.]huntingtomingalls[.]com
ny[.]philstarnotice[.]com
philippinenews[.]mooo[.]com
philnews[.]twilightparadox[.]com
pic[.]philstarnotice[.]com
pm[.]philstarnotice[.]com
pop[.]philippinenewss[.]com
pop[.]philstarnotice[.]com
premium9[.]crabdance[.]com
second[.]photo-frame[.]com
shoping[.]jumpingcrab[.]com
so[.]philippinenewss[.]com
web[.]huntingtomingalls[.]com
web01[.]crabdance[.]com
webmm[.]indiadigest[.]in
wg[.]philippinenewss[.]com
zq[.]philippinenewss[.]com
flags13[.]twilightparadox[.]com

Domain registrations:

- huntingtomingalls[.]com - ssdfsddfs@qsdfsq.com
- philippinenewss[.]com - sambieber1990@yahoo.com
- philstarnotice[.]com - sambieber1990@yahoo.com

Filenames:

- %systemroot%\system32\irmon32.dll
- %systemroot%\system32\FastUserSwitchingCompatibilityex.dll
- %systemroot%\system32\inetinfo32.dll
- %systemroot%\system32\drivers\drivers\diskfilter.sys
- %systemroot%\system32\usbcon.exe
- %windir%\temp\xKat.exe
- %systemroot%\system32\drivers\drivers\usbmgr.sys
- %appdata%\Microsoft\MMC\mmc.exe
- %systemroot%\system32\Iasex.dll
- %systemroot%\system32\Ipripex.dll

- %windir%\temp\mm_server.exe
- %windir%\temp\sys.exe
- %windir%\temp\test.exe

Yara rules:

```
rule apt_hellsing_implantstrings {

meta:

        version = "1.0"
        filetype = "PE"
        author = "Costin Raiu, Kaspersky Lab"
        copyright = "Kaspersky Lab"
        date = "2015-04-07"
        description = "detection for Hellsing implants"

strings:

    $mz="MZ"

    $a1="the file uploaded failed !"
    $a2="ping 127.0.0.1"

    $b1="the file downloaded failed !"
    $b2="common.asp"

    $c="xweber_server.exe"
    $d="action="

        $debugpath1="d:\\Hellsing\\release\\msger\\" nocase
        $debugpath2="d:\\hellsing\\sys\\xrat\\" nocase
        $debugpath3="D:\\Hellsing\\release\\exe\\" nocase
        $debugpath4="d:\\hellsing\\sys\\xkat\\" nocase
        $debugpath5="e:\\Hellsing\\release\\clare" nocase
        $debugpath6="e:\\Hellsing\\release\\irene\\" nocase
        $debugpath7="d:\\hellsing\\sys\\irene\\" nocase


        $e="msger_server.dll"
        $f="ServiceMain"

condition:
```

```
        ($mz at 0) and (all of ($a*)) or (all of ($b*)) or ($c and $d) or (any of ($debugpath*)) or ($e and
$f) and filesize < 500000

}

rule apt_hellsing_installer {

meta:

        version = "1.0"
        filetype = "PE"
        author = "Costin Raiu, Kaspersky Lab"
        copyright = "Kaspersky Lab"
        date = "2015-04-07"
        description = "detection for Hellsing xweber/msger installers"

strings:

    $mz="MZ"

        $cmd="cmd.exe /c ping 127.0.0.1 -n 5&cmd.exe /c del /a /f \"%s\""

        $a1="xweber_install_uac.exe"
        $a2="system32\\cmd.exe" wide
        $a4="S11SWFOrVwR9UlpWRVZZWAR0U1aoBHFTUl2oU1Y="
        $a5="S11SWFOrVwR9dnFTUgRUVlNHWVdXBFpTVgRdUlpWRVZZWARdUqhZVlpFR1kEUVNSXa
hTVgRaU1YEUVNSXahTVl1SWwRZValdVFFZUqgQBF1SWlZFVllYBFRTVqg="
        $a6="7dqm2ODf5N/Y2N/m6+br3dnZpunl44g="
        $a7="vd/m7OXd2ai/5u7a59rr7Ki45drcqMPl5t/c5dqIZw=="
        $a8="vd/m7OXd2ai/usPl5qjY2uXp69nZqO7l2qjf5u7a59rr7Kjf5tzr2u7n6euo4+Xm39zl2qju5dqo
4+Xm39zl2t/m7ajr19vf2OPr39rj5eaZmqbs5OSI Njl2tyI"
        $a9="C:\\Windows\\System32\\sysprep\\sysprep.exe" wide
        $a10="%SystemRoot%\\system32\\cmd.exe" wide
        $a11="msger_install.dll"
        $a12={00 65 78 2E 64 6C 6C 00}


condition:

        ($mz at 0) and ($cmd  and   (2 of ($a*))) and filesize < 500000
}


rule apt_hellsing_proxytool {

meta:
```

```
        version = "1.0"
        filetype = "PE"
        author = "Costin Raiu, Kaspersky Lab"
        copyright = "Kaspersky Lab"
        date = "2015-04-07"
        description = "detection for Hellsing proxy testing tool"

strings:

    $mz="MZ"

        $a1="PROXY_INFO: automatic proxy url => %s "
        $a2="PROXY_INFO: connection type => %d "
        $a3="PROXY_INFO: proxy server => %s "
        $a4="PROXY_INFO: bypass list => %s "
        $a5="InternetQueryOption failed with GetLastError() %d"
        $a6="D:\\Hellsing\\release\\exe\\exe\\" nocase


condition:

        ($mz at 0) and (2 of ($a*)) and filesize < 300000
}


rule apt_hellsing_xkat {

meta:

        version = "1.0"
        filetype = "PE"
        author = "Costin Raiu, Kaspersky Lab"
        copyright = "Kaspersky Lab"
        date = "2015-04-07"
        description = "detection for Hellsing xKat tool"

strings:

    $mz="MZ"

        $a1="\\Dbgv.sys"
        $a2="XKAT_BIN"
        $a3="release sys file error."
        $a4="driver_load error. "
        $a5="driver_create error."
        $a6="delete file:%s error."
        $a7="delete file:%s ok."
        $a8="kill pid:%d error."
```

```
        $a9="kill pid:%d  ok."
        $a10="-pid-delete"
        $a11="kill and delete pid:%d error."
        $a12="kill and delete pid:%d  ok."

condition:

        ($mz at 0) and (6 of ($a*)) and filesize < 300000

}


rule apt_hellsing_msgertype2 {

meta:

        version = "1.0"
        filetype = "PE"
        author = "Costin Raiu, Kaspersky Lab"
        copyright = "Kaspersky Lab"
        date = "2015-04-07"
        description = "detection for Hellsing msger type 2 implants"

strings:

    $mz="MZ"

        $a1="%s\\system\\%d.txt"
        $a2="_msger"
        $a3="http://%s/lib/common.asp?action=user_login&uid=%s&lan=%s&host=%s&os=%s&proxy
=%s"
        $a4="http://%s/data/%s.1000001000"
        $a5="/lib/common.asp?action=user_upload&file="
        $a6="%02X-%02X-%02X-%02X-%02X-%02X"

condition:

        ($mz at 0) and (4 of ($a*)) and filesize < 500000

}



rule apt_hellsing_irene {

meta:

        version = "1.0"
```

```
        filetype = "PE"
        author = "Costin Raiu, Kaspersky Lab"
        copyright = "Kaspersky Lab"
        date = "2015-04-07"
        description = "detection for Hellsing msger irene installer"

strings:

    $mz="MZ"

        $a1="\\Drivers\\usbmgr.tmp" wide
        $a2="\\Drivers\\usbmgr.sys" wide
        $a3="common_loadDriver CreateFile error! "
        $a4="common_loadDriver StartService error && GetLastError():%d! "
        $a5="irene" wide
        $a6="aPLib v0.43  -  the smaller the better"

condition:

        ($mz at 0) and (4 of ($a*)) and filesize < 500000

}
```