HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

BHO objekti

CCERT-PUBDOC-2004-06-79

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

BHO (eng. *Browser Helper Objects*) objekti često se spominju kada su u pitanju *spyware*, *malware* ili drugi parazitski programi. Iako su BHO objekti zamišljeni kao tehnologija koja bi olakšavala rad i upravljanje Internet Explorer Web preglednikom, pokazalo se da se u praksi njihove mogućnosti najčešće iskorištavaju zlonamjerno.
Problem postaje dodatno naglašen kada se u obzir uzme činjenica da detekcija BHO objekata pri normalnom radu računala nije jednostavna. Nije ih moguće vidjeti korištenjem *Task Manager* programa za nadzor i praćenje rada sustava, budući da se ne pokreću samostalno već isključivo iz instance Internet Explorer-a, tako da je jedini način za njihovu detekciju direktna provjera odgovarajućeg ključa *Registry* datoteke ili korištenje specifičnih alata koji taj postupak automatiziraju.
U nastavku dokumenta biti će detaljnije opisano što su to ustvari BHO objekti, a također će biti opisani i neki alati koji se mogu iskoristiti za kontrolu nad tim objektima.

2. Što su BHO objekti

BHO (eng. *Browser Helper Objects*) objekti su COM (eng. *Component Object Model*) komponente koje se učitavaju prilikom pokretanja Internet Explorer-a. BHO objekti pokreću se unutar memorijskog prostora Web preglednika, te mogu izvršavati akcije nad svim dostupnim prozorima i modulima. Korištenje BHO objekata započelo je s Internet Explorerom inačice 4.
Osnovna ideja za uvođenje BHO objekata bila je otvaranje mogućnosti prilagođavanja Internet Explorer-a. BHO objekti, naime, mogu detektirati bilo koji događaj (eng. *event*) unutar Web preglednika, pristupati izbornicima i alatima, otvarati prozore, nadgledati poruke (eng. *messages*) i akcije unutar preglednika. Ukratko, korištenjem BHO objekata moguća je gotovo potpuna kontrola ponašanja Internet Explorer programa.
Osim kroz Internet Explorer, od ljuske inačice 4.71 (Windows 95 i Windows 4.0 s instaliranom Active Desktop Shell update komponentom), uporabu BHO objekata podržava i Windows Explorer program (Tablica 1).

Inačica ljuske	Proizvod	Podrška za BHO	
		Internet Explorer	Windows Explorer
4.00	Windows 95, Windows NT 4.0	4.0	–
4.71	Windows 95, Windows NT 4.0 s Active Desktop Shell Update komponentom	4.0	√
4,72	Windows 98	√	√
5.00	Windows 2000, Windows Me	√	√
6.00	Windows XP	√	√

Tablica 1: *Podrška za BHO u različitim inačicama ljuske (shell32.dll)*

Općenito, prilikom svakog otvaranja glavnog prozora preglednika učitava se odgovarajući skup BHO objekata koji ostaje aktivan sve dok se prozor ne zatvori. Slična stvar je i s Windows Explorer programom, iako kod njega postoje i neke iznimke [1]. No načelno gledajući prilikom svakog pokretanja `explorer.exe` ili `iexplore.exe` aplikacija učitavaju se i odgovarajući BHO objekti.
Ponašanje BHO objekata je vrlo dinamično. Prilikom svakog otvaranja Windows ili Internet Explorer aplikacije iz *Registry* datoteke učitava se odgovarajući skup BHO objekata. Popis BHO objekata nalazi se u sljedećem ključu:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
Browser Helper Objects
```

gdje se nalazi popis klasa koje identificiraju odgovarajuće `.dll` biblioteke povezane s pojedinim BHO objektom. Svaki BHO ima jedinstvenu CLSID oznaku koja je navedena u gornjem *Registry* ključu i koja referencira odgovarajući ključ unutar *Registry* ključa

```
HKEY_CLASSES_ROOT\CLSID\
```

Ukoliko u *Registry* datoteci dođe do promjene ključa koji identificira BHO objekte, u različitim instancama preglednika koje su istovremeno aktivne moguće je imati učitan različiti skup BHO objekata.

3. Uporaba BHO objekata

Fleksibilnost BHO objekata opisana u prethodnom poglavlju otvara razne mogućnosti njihove uporabe za unaprjeđenje rada s Web preglednikom. Neki komercijalni proizvodi, poput npr. Adobe Acrobat-a koriste BHO objekte za integraciju s Internet Explorer-om. Također, i *Google Toolbar*, traka s alatima popularne tražilice Google jest ustvari BHO objekt. Korisnici *Google Toolbar*-a u *Registry* datoteci imaju upisane sljedeće vrijednosti:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
Browser Helper Objects\{AA58ED58-01DD-4d91-8333-CF10577473F7}
```

i

```
HKEY_CLASSES_ROOT\CLSID\{AA58ED58-01DD-4d91-8333-CF10577473F7}
       @="Google Toolbar Helper"

HKEY_CLASSES_ROOT\CLSID\{AA58ED58-01DD-4d91-8333-CF10577473F7}\InprocServer32
       @="c:\program files\google\googletoolbar2.dll"
       "ThreadingModel"="Apartment"
```

Nažalost, osim korisnih mogućnosti uporabe BHO objekata, postoji velik broj primjera u kojima BHO objekte koriste razni parazitski programi, kao što su razni *adware*, *malware* i *spyware* programi, *browser hijackers* itd. Postoji nekoliko stotina parazitskih programa, odnosno zlonamjernih BHO objekata koje programi za detekciju BHO objekata prepoznaju, a njihov broj se stalno povećava.
Neke od tih programa, odnosno BHO objekata, korisnik sam instalira ne znajući pri tome da je uz željenu aplikaciju instalirao i BHO objekt koji dalje ima mogućnost praćenja rada i upravlja njegovim Web preglednikom (npr. Go!Zilla, http://www.gozilla.com/), dok se drugi BHO objekti mogu instalirati i bez korisničke eksplicitne instalacije iskorištavanjem nekog od mnogih nedostataka unutar Internet Explorer-a.

3.1. Onemogućavanje rada

Ukoliko uporaba BHO objekata nije nužna, njihovo pokretanje moguće je onemogućiti. To je moguće napraviti na dva načina. Prvi način sastoji se od sljedećih koraka:

1. Zatvoriti sve instance Internet Explorer-a, otvoriti izbornik *Start*, *Settings*, *Control Panel*.
2. Odabrati opciju *Internet Options*.
3. Odabrati *Advanced* karticu.
4. Unutar *Browsing* odjeljka isključiti *Enable third-party browser extensions* opciju.

Druga mogućnost jest direktno uređivanje *Registry* datoteke, odnosno postavljanje string vrijednosti `"Enable Browser Extensions"` na `"No"` unutar sljedećeg ključa:

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
```

U oba slučaja uporaba BHO objekata onemogućava se samo u kontekstu trenutno prijavljenog korisnika.

3.2. Selektivno uklanjanje BHO objekata

Iako se onemogućavanjem rada BHO objekata uklanja mogućnost njihove zlonamjerne uporabe, istovremeno se može izgubiti dio ili potpuna funkcionalnost nekih legitimnih korisničkih aplikacija. Zbog toga je selektivno uklanjanje pojedinih (zlonamjernih) BHO objekata za većinu korisnika puno prihvatljivija opcija. Zlonamjerne BHO objekte moguće je ručno ukloniti na sljedeći način:

1. Otvoriti *Registry* datoteku i provjeriti sljedeći ključ:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
   Browser Helper Objects
   ```

te identificirati sve postojeće BHO objekte, odnosno njihovu CLSID referencu.

2. Za sve identificirane CLSID reference provjeriti njihove odgovarajuće ključeve unutar ključa:

   `HKEY_CLASSES_ROOT\CLSID\`

3. Provjeriti legitimnost `.dll` biblioteka za svaki CLSID identifikator.
4. Ukoliko se uoči postojanje nelegitimnih `.dll` biblioteka, potrebno je obrisati odgovarajuću CLSID referencu iz *Registry* ključa navedenog u koraku 1, CLSID iz ključa navedenog u koraku 2, te ukloniti nelegitimnu `.dll` biblioteku.

Ovaj postupak može biti prilično složen i dugotrajan, a zahtijeva i dobro poznavanje Windows operacijskih sustava. Zbog toga je za većinu korisnika puno prihvatljivije korištenje programskih alata koji automatski uklanjaju zlonamjerne BHO objekte.

Većina *anti-spyware* alata kao što su npr. AdAware (http://www.lavasoft.de) ili SpyBot Search & Destroy (http://www.safer-networking.org) uklanjaju i maliciozne BHO objekte, no osim tih alata postoji i nekoliko specijaliziranih alata koji služe samo za rukovanje BHO objektima. Dva takva alata, BHODemon i BHOList, opisana su u nastavku ovog dokumenta.

4. Alati

4.1. BHODemon

BHODemon je *freeware* alat za zaštitu Internet Explorer preglednika od neovlaštene uporabe BHO objekata. Kroz sučelje alata moguće je uključivati/isključivati pokretanje pojedinih instaliranih BHO objekata. Osim toga, alat se pokreće u *tray*-u, te u stvarnom vremenu nadgleda *Registry* datoteku i upozorava prilikom instalacije novih BHO objekata.

Alat radi na svim inačicama Windows operacijskih sustava (Windows 9x, Me, NT, 2000 i XP), a trenutno aktualna inačica alata je 2.0.

4.1.1. Instalacija

Instalacija alata je vrlo jednostavna. Sa Web stranica proizvođača (http://www.definitivesolutions.com/bhodemon.htm) potrebno je slijediti link za *download* te skinuti `.zip` datoteku koja sadrži instalacijski program i raspakirati ga. Prije instalacije potrebno je prihvatiti uvjete licence, odabrati lokaciju programskih datoteka i ime programske grupe u *Start, Programs* izborniku, te mogućnost postavljanja ikone na *Desktop* ili u *Quick Launch* izbornik.

4.1.2. Korištenje

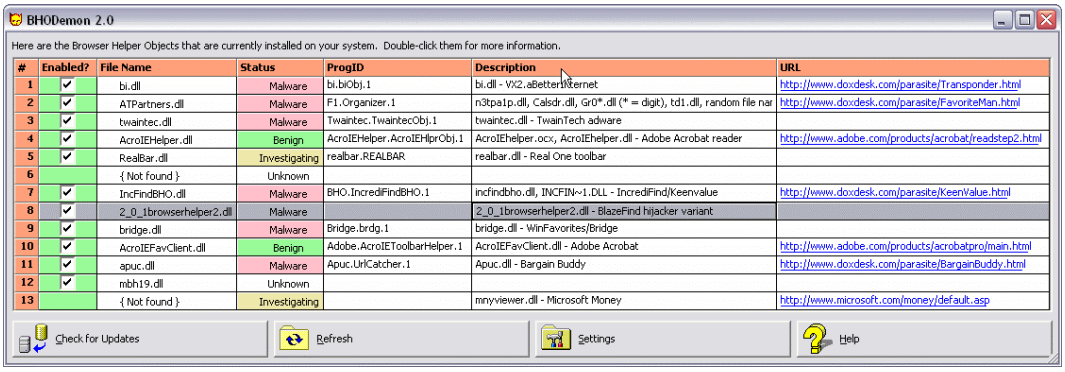
Prilikom pokretanja BHODaemon-a otvara se jednostavno grafičko sučelje unutar kojeg ne postoje uobičajene trake s izbornicima (Slika 1). Prozor ima samo radno područje unutar kojeg se nalazi prikaz trenutno instaliranih BHO objekata, zajedno s dodatnim informacijama i traku s alatima iz koje je moguće odabrati jednu od četiri naredbe:

- *Check for updates* – podešavanje osvježavanja programa. Moguće je podesiti provjeru na tjednoj, mjesečnoj, tromjesečnoj bazi ili je isključiti.
- *Refresh* – osvježavanje radnog područja aplikacije (provjera *Registry* datoteke).
- *Settings* – podešavanje postavki programa. U trenutnoj inačici moguće je podesiti uključivanje/isključivanje *Tip of the day* opcije, boju zaglavlja i testirati poruku kod detekcije novog BHO objekta.
- *Help* – otvara Web stranicu s uputama za korištenje alata. Da bi se ova opcija mogla koristiti, korisnik mora biti *online*.

U radnom području aplikacije moguće je vidjeti sve trenutno instalirane BHO objekte na računalu; te iste aktivirati/deaktivirati. Za svaki od instaliranih BHO objekata moguće je vidjeti sljedeće atribute:

- *Enabled* – označava da li je odgovarajući BHO aktivan ili ne. Uključivanjem ili isključivanjem *checkbox* opcije moguće je aktivirati ili deaktivirati pojedine BHO objekte instalirane na računalu.
- *File Name* – ime dinamičke biblioteke (`.dll`) koju referencira BHO.
- *Status* – status BHO objekta. Status može imati jednu od sljedećih vrijednosti:

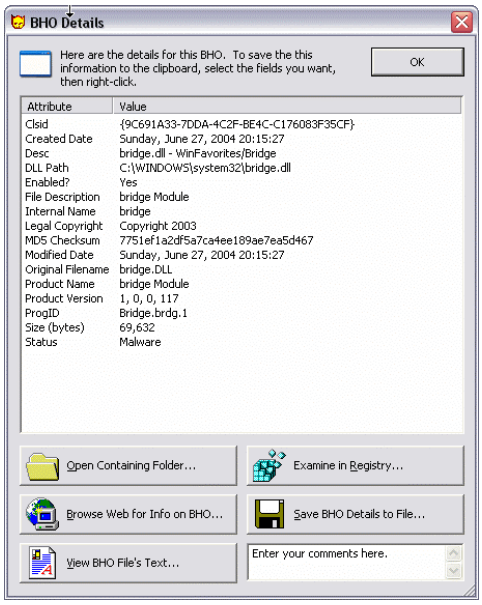
  - *Malware* – oznaka da se radi o malicioznom objektu,
  - *Benign* – oznaka da se radi o legitimnom objektu,
  - *Investigating* – ova oznaka označava da se status odgovarajućeg BHO ispituje,
  - *Unknown* – oznaka da je status BHO objekta nepoznat.
- *ProgID* – identifikator pojedinog BHO objekta.
- *Description* – opis BHO objekta, odnosno ime proizvođača.
- *URL* – URL na kojem je moguće dobiti više informacija (Web stranice proizvođača) o pojedinom BHO objektu ili aplikaciji koja ga je instalirala.



Slika 1: *Izgled BHODemon aplikacije*

Dvostrukim pritiskom na pojedini BHO u radnom području otvara se novi prozor u kojem se nalazi popis detaljnih informacija o BHO objektu zajedno sa sljedećim naredbama (Slika 2):

- *Open Containing Folder* – otvara direktorij u kojem se nalazi `.dll` biblioteka koju referencira BHO objekt.
- *Browse Web for Info on BHO* – pretražuje Web za dodatnim informacijama o pojedinom BHO objektu korištenjem Google tražilice. Da bi se ova opcija mogla koristiti korisnik mora biti *online*.
- *View BHO file text* – omogućava pregled BHO objekta u tekstualnom obliku.
- *Examine in Registry* – otvara *Registry* datoteku i pozicionira pogled na odgovarajuću BHO referencu.
- *Save BHO Details to File* – omogućava pohranu detaljnih informacija o BHO objektu u tekstualnu datoteku.



Slika 2: *Prikaz detaljnih informacija o pojedinom BHO objektu*

Deaktivacija pojedinog BHO objekta kroz BHODemon provodi se na sljedeći način:

1. BHODemon preimenuje `.dll` dinamičku biblioteku mijenjajući joj ekstenziju iz `.dll` u `.dll_BHODemonDisabled_random`, gdje `random` označava slučajno generirani niz znakova.
2. U odgovarajući ključ (koji referencira BHO) i koji se nalazi u

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
   Browser Helper Objects
   ```

   dodaje se podključ s jednom (*Default*) string vrijednosti:

   ```
   ReadMe-BHODemon
   @="This BHO has been disabled by BHODemon."
   ```

Pritiskom na gumb za minimizaciju prozora BHODemon ostaje aktivan u *tray*-u, te u stvarnom vremenu pregledava *Registry* datoteku i prijavljuje detekciju novoinstaliranih BHO objekata (Slika 3).

Slika 3: *Detekcija instalacije novog BHO objekta*

4.1.3. Prednosti i nedostaci

BHODemon je koristan program koji služi za detekciju BHO objekata te njihovu identifikaciju na temelju vlastite baze informacija. Također, moguća je selektivna aktivacija/deaktivacija pojedinih BHO objekata instaliranih na računalu, isto kao i detekcija novih instalacija BHO objekata u stvarnom vremenu.
Na temelju dobivenih informacija korisnik eventualno može ručno ukloniti pojedini BHO koji je identificiran kao nelegitimni prema ranije opisanom postupku.
Osnovni nedostatak programa jest što ne podržava mogućnost potpunog uklanjanja BHO objekata već isključivo njihovu deaktivaciju, pa je u slučaju želje ili potrebe za potpunim uklanjanjem pojedinog BHO potrebno koristiti neke druge alate kao što su AdAware i SpyBot Search & Destroy.

4.2. BHOList

BHOList je *freeware* program koji predstavlja jednostavno sučelje za pregled kolekcije BHO objekata (Tony Klein BHO Collection – http://www.sysinfo.org) javno dostupne na Webu. Program ima jednostavno sučelje kroz koje je moguće pregledavati popis postojećih BHO objekata te sortirati ili pretraživati taj popis prema određenim pravilima. Trenutna inačica programa jest 1.40v2.

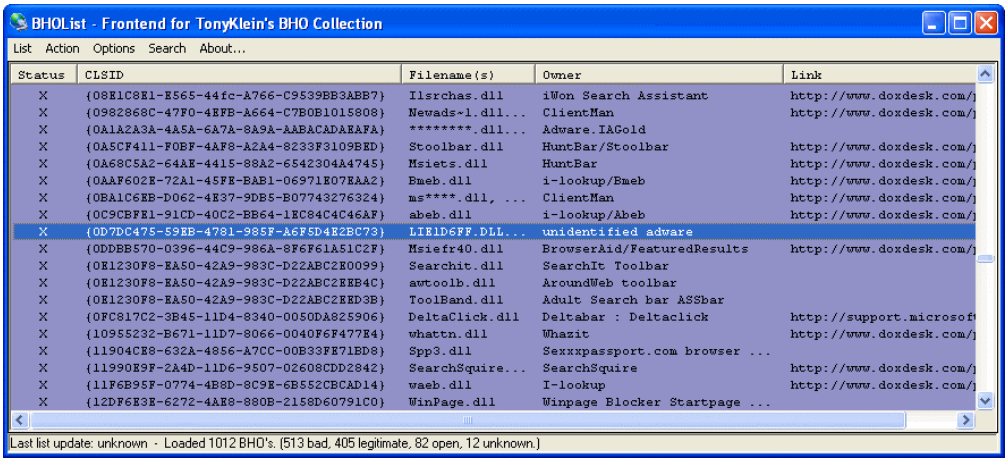
4.2.1. Instalacija

Program ne zahtijeva posebnu instalaciju već je dovoljno napraviti *download* `.zip` datoteke koja sadrži izvršni program te ga raspakirati u željeni direktorij. Pokretanje je jednostavno, no program za svoj rad koristi `comctl32.ocx` ActiveX kontrolu. Ukoliko ta komponenta ne postoji na sustavu u direktoriju `%WINDIR%\system32`, BHOList neće funkcionirati. Ako ta kontrola ne postoji na sustavu moguće ju je skinuti s Microsoft-ovih stranica ili na sljedećoj adresi http://freeware.it-mate.co.uk/?Cat=OCX_Files i raspakirati u gore navedeni direktorij.

4.2.2. Korištenje

Nakon pokretanja BHOList programa otvara se grafičko sučelje koje se sastoji od trake s alatima i radnog područja (Slika 4).
Traka s alatima sadrži sljedeće izbornike:

- *List* – odabir opcija vezanih uz prikaz radnog područja. Sadrži sljedeće naredbe:
  - Switch to BHOList/Switch to Toolbar List – prijelaz između prikaza popisa BHO objekata ili Toolbar alata; ova opcija momentalno nema korisnu funkcionalnost,
  - Show only installed BHOs – prikazuje samo BHO objekte instalirane na računalu,
  - Update BHOs from SWI – osvježava popis BHO objekata s referentne lokacije na Webu,
  - Dump to file – pohrana trenutno otvorene liste BHO objekata u datoteku,
  - Load from dumped file – učitavanje liste iz datoteke,
  - Exit – izlaz iz programa.
- *Action* – omogućava pregled ili kopiranje sadržaja pojedinog retka radnog područja aplikacije. Iste akcije moguće je postići dvostrukim pritiskom na pojedini BHO unutar radnog područja programa (Slika 5).
- *Options* – omogućava podešavanje opcija aplikacije. Sadrži sljedeće naredbe:
  - *Start as BHO list* – aplikacija se pokreće u pregledu BHO objekata,
  - *Start as Toolbar list* – aplikacija se pokreće u pregledu Toolbar alata,
  - *Load from Sysinfo on startup* – aplikacija prilikom pokretanja učitava popis s referentne lokacije (http://www.sysinfo.org),
  - *Load from file on startup* – aplikacija prilikom pokretanja učitava popis iz datoteke,
  - *URLs to fetch list from* – predefinirane URL adrese za učitavanje BHO odnosno Toolbar lista (http://www.sysinfo.org/bholist.txt i http://www.sysinfo.org/toolbarlist.txt),
  - *Store settings only for current user* – postavke se pohranjuju samo za trenutno prijavljenog korisnika.
- *Search* – pretraživanje teksta.
- *About* – informacije o programu i autoru.



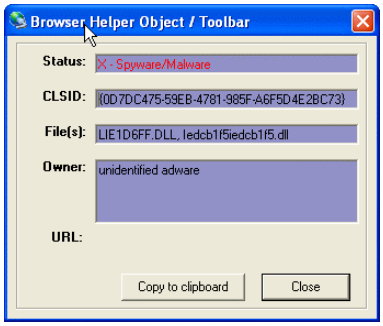
Slika 4: *Sučelje BHOList aplikacije*

U radnom području aplikacije moguće je pregledavati referentnu listu BHO objekata i informacije koje su vezane uz pojedini BHO. Pogled je moguće ograničiti samo na BHO objekte instalirane na računalu te sortirati prema raspoloživim atributima:

- *Status* – označava status BHO objekta. Moguće su sljedeće vrijednosti:
  - *L (Legitimate)*– označava legitimne BHO objekte,
  - *X (Malware)* – označava maliciozne BHO objekte,
  - *O (Open)* – označava objekte kojima je status otvoren (istražuju se),
  - *? (Unknown)* – označava objekte kojima je status nepoznat.
- *CLSID* – CLSID oznaka klase BHO objekta.
- *Filename(s)* – datoteka ili datoteke koje su referencirane BHO objektom, odnosno CLSID identifikatorom u *Registry* datoteci.
- *Owner* – proizvođač (vlasnik) pojedinog objekta.
- *Link* – URL adresa na kojoj je moguće naći više informacija o proizvodu/BHO objektu.

Rad s aplikacijom je jednostavan, pošto je njezina osnovna i jedina funkcionalnost prikaz popisa trenutno poznatih BHO objekata. Korisna opcija jest ograničavanje popisa BHO objekata samo na one

koji su trenutno instalirani na računalu. U trenutku nastanka ovog dokumenta BHOList učitavanjem s referentne lokacije prepoznaje ukupno 1012 BHO objekata, od kojih je 513 malicioznih, 405 legitimnih, 82 čiji se status ispituje, te 12 s nepoznatim statusom. Obzirom na svojstva pojedinih legitimnih objekata, moglo bi se ustvrditi da bi neki od njih također mogli spadati u kategoriju malicioznih, no obzirom da se instaliraju na legitiman način (uz odobrenje korisnika) i status im se tako označava.



Slika 5: *Pregled atributa pojedinog BHO objekta*

4.2.3. Prednosti i nedostaci

BHOList je jednostavna aplikacija koja omogućava lokalni prikaz, sortiranje i pretraživanje liste BHO objekata (Tony Klein BHO Collection) koja je također i javno dostupna na Internetu na adresi http://www.sysinfo.org. Osim mogućih problema kod instalacije (eventualno nepostojanje `comctl32.ocx` ActiveX komponente), na rad samog programa ne mogu se uputiti neke posebne primjedbe, pošto alat funkcionira u skladu s očekivanim. Korisna opcija jest i ograničavanje prikaza BHO objekata samo na one koji su instalirani na računalu.
Naravno, alat sam po sebi je nedovoljan, pošto u slučaju detekcije malicioznih BHO objekata ne pruža nikakve mogućnosti za njihovu deaktivaciju ili potpuno uklanjanje.

5. Zaključak

U dokumentu je opisan način rada BHO objekata i njihova osnovna funkcionalnost. BHO objekti kao takvi vrlo su korisni pošto omogućavaju dodatnu kontrolu i proširenje osnovnih mogućnosti Internet Explorer Web preglednika. Iz istog tog razloga, ali i zbog prilično teškog postupka detektiranja BHO objekte vrlo često koriste razni maliciozni programi, od *adware* programa do *browser hijackera*.
Pokazuje se da je povremeni pregled instaliranih BHO objekata nužan ukoliko se želi osigurati nesmetan i siguran rad korisnika. Pregled BHO objekata može se provoditi ručno, no isto tako postoje alati koji olakšavaju taj postupak kao što su BHODemon i BHOList.
Alati BHODemon i BHOList su korisni alati za detekciju BHO objekata i njihovo aktiviranje/deaktiviranje (BHODemon). Unatoč tome, ti alati ne pružaju mogućnost potpunog uklanjanja BHO objekata, pa je na temelju dobivenih informacija moguće ručno uklanjanje BHO objekata ili korištenje drugih alata kao što su AdAware i SpyBot Search and Destroy.

6. Reference

[1] Browser Helper Objects: The Browser the Way You Want It,
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp
[2] BHODemon 2.0,
http://www.definitivesolutions.com/bhodemon.htm
[3] BHOList,
http://www.spywareinfo.com/~merijn/
[4] Parazitski programi, CCERT-PUBDOC-2002-12-11,
http://www.cert.hr/filehandler.php?did=45
[5] What is a Browser Helper Object?
http://www.sysinfo.org/bhoinfo.html