HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Qwik-Fix alata

CCERT-PUBDOC-2004-12-101

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

Svakodnevnom pojavom novih malicioznih programa te tehnika i alata kojima neovlašteni korisnici ostvaruju pristup informacijskim sustavima javila se potreba za razvojem naprednijih i sofisticiranijih mehanizama zaštite. Osim korištenja sigurnosnih kontrola koje se baziraju na detekciji neovlaštenog pristupa (IDS, antivirusna zaštita i sl.), potrebno je implementirati i kontrole koje će biti u stanju reagirati na detektirane napade s ciljem njihova zaustavljanja. Jedno od mogućih rješenja ovog problema jest sustav za prevenciju neovlaštenih aktivnosti (eng. *Intrusion Prevention System*).

Qwik-Fix Pro programski alat jest sustav za prevenciju neovlaštenog pristupa koji je namijenjen blokiranju neovlaštenog pristupa na razini jezgre operacijskog sustava (eng. *kernel*), na razini servisa, aplikacija te na mrežnoj razini. Zaustavljanje prijetnji bazira se na istraživanjima koje provodi *PivX Solutions* tvrtka, a blokira crve, viruse i ostale maliciozne programe koji inficiraju Windows operacijske sustave.

Qwik-Fix Pro aplikacija dostupna je u dvije inačice: *Qwik-Fix Pro Enterprise Edition* i *Qwik-Fix Pro Home Edition*. Prva inačica namijenjena je zaštiti osobnih računala i poslužitelja, dok je druga inačica namijenjena samo zaštiti osobnih računala. Razlika među njima je ta što *Enterprise Edition* uključuje i upravljačku konzolu koja omogućuje jednostavniju instalaciju i upravljanje aplikacijom na razini računalne mreže. Ovaj dokument analizira *Qwik-Fix Pro Home Edition* programski alat koji je namijenjen individualnim korisnicima.

2. Instalacija i pokretanje alata

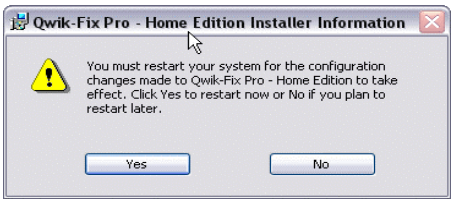
Za instalaciju programskog alata potrebno je dohvatiti probnu inačicu s referentne adrese http://www.pivx.com/qwikfixDownload.asp te ju pohraniti na lokalni disk. Probna inačica ima punu funkcionalnost 30 dana. Prije nego li korisnik ima mogućnost dohvatiti datoteku programskog alata, mora popuniti formu koja je prikazana na slici 1.

Obvezni podaci su ime, prezime i adresa elektroničke pošte (eng. *e-mail*) koja mora biti unesena dva puta, radi provjere ispravnosti unosa. Nakon slanja korisničkih podataka, korisnik putem web stranice dobiva obavijest da su instrukcije za instalaciju i licenčni kod poslani na upisanu adresu elektroničke pošte. Na istoj stranici nalazi se i link za dohvaćanje datoteke i to poseban link za operacijski sustav Windows inačice NT/2000/XP/2003 i drugi link za operacijski sustav Windows inačice 95/98/98SE/ME. Aktivacijom linka korisnik dohvaća datoteku u `.exe` formatu pod imenom `QwikFix-NT-Home.exe`, veličine 5.55 MB. Na referentnoj adresi http://www.pivx.com/whitepapers/QwikFixProWhitepaper071304.pdf može se dohvatiti i brošura o samom alatu, u `.pdf` formatu datoteke veličine 1.07 MB. U trenutku pisanja ovog dokumenta zadnja dostupna inačica alata je 1.4.

Za instalaciju programa potrebno je pokrenuti spomenutu izvršnu datoteku čime započinje proces instalacije. Nakon prihvaćanja licenčnog ugovora i upisa podataka o korisniku (ime, prezime, organizacija) instalacijski postupak instalira program unutar mape `Program Files` na računalu.

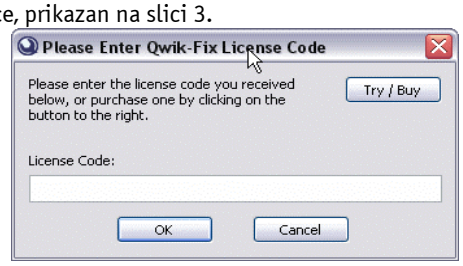
Slika 1: Online forma za Qwik-Fix Home Edition

Nakon uspješne instalacije alata potrebno je ponovno pokrenuti operacijski sustav pri čemu se pojavljuje dijaloški okvir prikazan na slici 2.



Slika 2: Dijaloški okvir za ponovno pokretanje sustava

Nakon što je operacijski sustav ponovno pokrenut, alat se samostalno pokreće i pri tome se prikazuje dijaloški okvir za upis licence, prikazan na slici 3.



Slika 3: Dijaloški okvir za upis licence

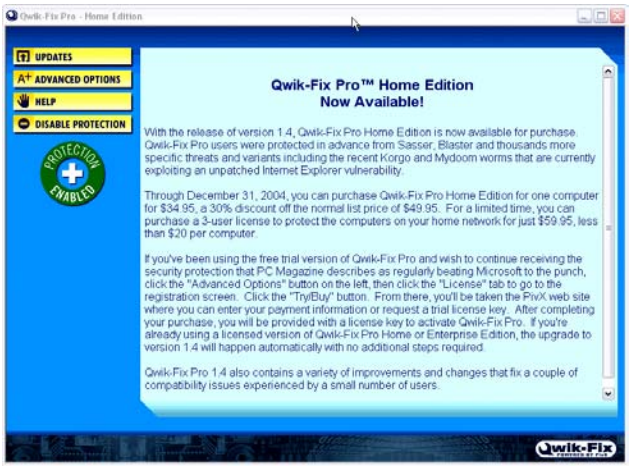
U polje *Licence Code* korisnik upisuje licenčni kod koji je dobio unutar poruke elektroničke pošte pristigle na adresu navedenu prilikom dohvaćanja datoteke.

3. Sučelje alata

Nakon unosa licenčnog koda (samo kod prvog pokretanja alata), otvara se sučelje alata koje je prikazano na slici 4. Sučelje alata sastoji se od opisa programskog alata u glavnom dijelu sučelja te izbornika koji sadrži naredbe:

- `Updates`,
- `Advanced Options`,
- `Help`,

- `Disable Protection`.



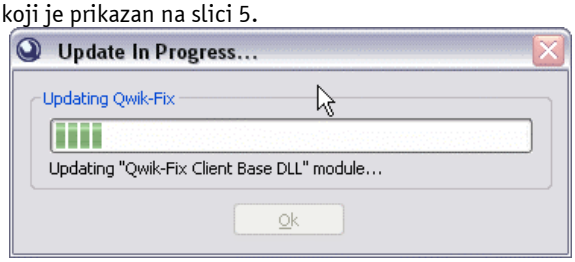
Slika 4: Sučelje alata Qwik-Fix Home Edition

4. Podešavanje alata

Kada je programski alat instaliran i spreman za pružanje odgovarajuće razine zaštite osobnog računala, potrebno je izvršiti dodatna podešavanja kojima će se definirati način rada programa. Za njegovo podešavanje koriste se prije navedene naredbe koje su dalje u dokumentu detaljno opisane.

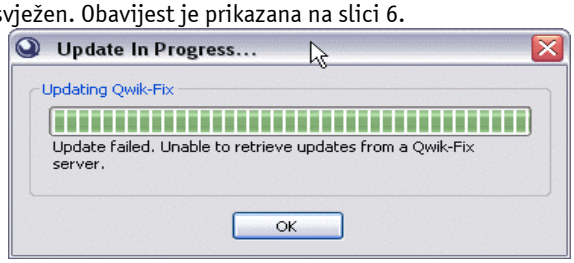
4.1. Ažuriranje alata

Nakon instalacije alata potrebno je izvršiti njegovo ažuriranje. Ažuriranje (nadogradnja alata) izvodi se odabirom naredbe `Updates`. Prilikom tog procesa na ekranu je vidljiv dijaloški okvir koji ukazuje na status ažuriranja, a koji je prikazan na slici 5.



Slika 5: Status procesa ažuriranja alata

Ukoliko se prilikom procesa ažuriranja pojavi pogreška, alat će prikazati obavijest po kojoj je vidljivo da alat nije pravilno osvježen. Obavijest je prikazana na slici 6.



Slika 6: Greška prilikom ažuriranja alata

Obzirom da je redovito ažuriranje osnovni preduvjet za pravilno funkcioniranje, alat je predefinirano podešen tako da u *system tray*-u ima vidljivu ikonu alata koja signalizira na neažurnost alata. Nakon što korisnik provede ažuriranje, ikona alata prekida sa signalizacijom i ukazuje samo na to da je alat aktivan (eng. *enabled*).

Prilikom ažuriranja baze zakrpa, poslužitelju za nadogradnju šalju se slijedeći podaci:

- licenca,

- inačica alata,
- detalji o konfiguraciji operacijskog sustava,
- detalji o odgovarajućim aplikacijama trećih strana.

Ove informacije omogućuju da se na određeno osobno računalo instaliraju samo one zakrpe koje su zaista potrebne obzirom na konfiguraciju te instalirane aplikacije.Prijenos podataka vrši se preko HTTPS protokola, odnosno TCP porta 443.

4.2. Napredne opcije alata

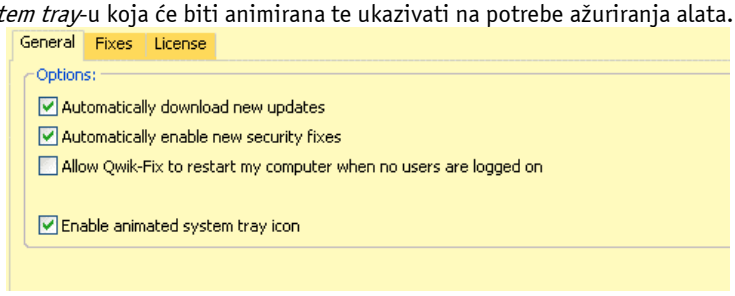
Napredne opcije alata (eng. *Advanced options*) sadrže tri kartice koje omogućuju podešavanje alata. To su:

- `General`,
- `Fixes`,
- `License`.

Kartica `General` prikazana je na slici 7. Na kartici se nalaze četiri opcije koje utječu na opću funkcionalnost sustava, a koje korisnik može uključiti ili isključiti. Opcije su:

- `Automatically download new updates`,
- `Automatically enable new security fixes`,
- `Allow Qwik-Fix to restart my computer when no users are logged on`,
- `Enable animated system tray icon`.

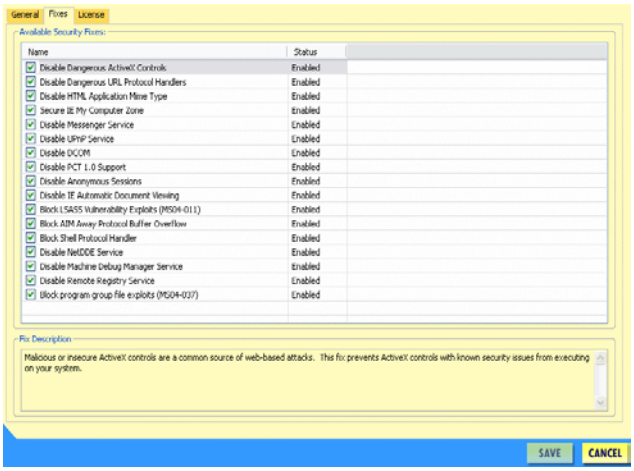
Prva opcija omogućuje automatsko dohvaćanje novih zakrpa što korisniku olakšava održavanje samog alata. Druga opcija automatski primjenjuje novo dohvaćene zakrpe. Treća opcija dozvoljava da alat ponovno pokrene operacijski sustav ukoliko nema korisnika prijavljenog za rad. Četvrta opcija utječe na ikonu u *system tray*-u koja će biti animirana te ukazivati na potrebe ažuriranja alata.



Slika 7: Kartica General

Slika 8 prikazuje karticu `Fixes`. Na ovoj kartici nalazi se popis metoda zaštita koje su trenutno instalirane i koje alat koristi. Svaka metoda zaštita ima dva moguća stanja:

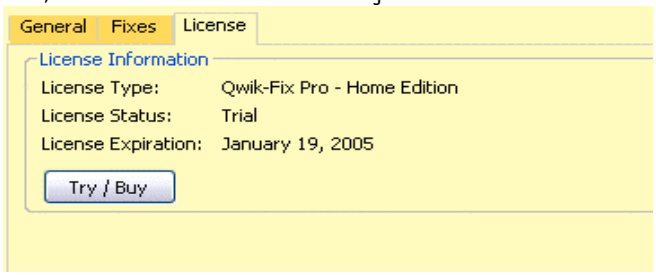
- zaštita je aktivna (eng. *enabled*),
- zaštita je neaktivna (eng. *disabled*).



Slika 8: Kartica Fixes

Sve metode zaštite su predefinirano aktivne, no korisnik ih može deaktivirati isključivanjem pojedinog *checkbox* polja. U tom slučaju, metoda zaštite nije deaktivirana dok se promjena stanja ne potvrdi pritiskom na dugme `Save`. Nakon toga se mijenja status metode zaštite, a alat se vraća u početno sučelje (slika 4). Osim popisa metoda zaštita, ova kartica sadrži i opis svake pojedine metode zaštite (eng. *fix description*). Odabirom određene metode zaštite, u donjem dijelu sučelja pojavljuje se točan opis njene funkcionalnosti.

Posljednja kartica `License` prikazana je na slici 9, a na njoj su vidljive informacije o licenci alata. Vidljiva je vrsta licence, status te datum kada licenca istječe.



Slika 9: Kartica License

Pritiskom na dugme `Try/Buy` otvara se prozor za unos licenčnog koda (slika 3).

4.3. Sigurnosne kontrole

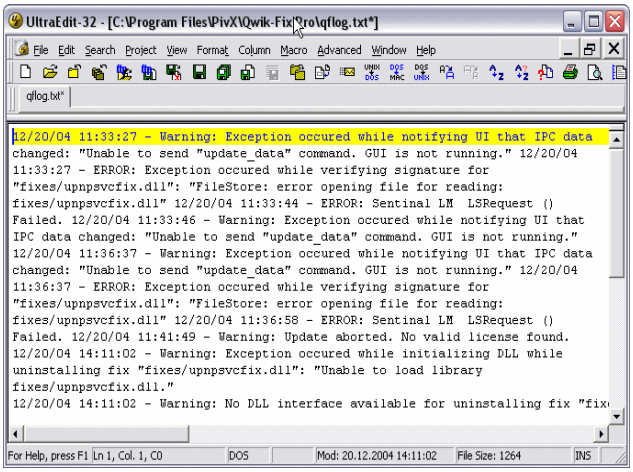
Qwik-Fix Pro sustav za prevenciju neovlaštenih aktivnosti svoju funkcionalnost ne temelji se na potpisima pojedinih napada i složenim sigurnosnim pravilima , već na uklanjanju samog problema kojeg pojedini napad koristi. Na taj način proaktivno se djeluje u smislu sprječavanja neovlaštenih aktivnosti, što znači da će program spriječiti izvršavanje i onih napada za koje sigurnosne zakrpe nisu instalirane (naravno, ukoliko postoje odgovarajuće kontrole koje uklanjaju uzrok problema).

Tvrtka *PivX Solutions* redovito analizira nove tehnike neovlaštenih pristupa te na temelju toga izdaje nove module koji sprječavaju njihovo izvršavanje. To znači da se redovitim osvježavanjem alata dodaju i nove funkcionalnosti koje odgovaraju na aktualne prijetnje.

Nove sigurnosne kontrole instaliraju se redovnom nadogradnjom alata. Svi instalirani moduli nalaze se na lokalnom disku računala na lokaciji `C:\Program Files\PivX\Qwik-Fix Pro\fixes` u obliku `.dll` datoteka. Svaka datoteka predstavlja jednu zakrpu koja se nalazi u popisu na kartici `Fixes` (slika 8).

Na lokaciji `C:\Program Files\PivX\Qwik-Fix Pro` nalazi se tekstualna datoteka `qflog.txt` u koju se spremaju zapisi aktivnosti alata. Slika 10 prikazuje primjer sadržaja navedene datoteke.

Svaka metoda zaštite ima funkciju umanjivanja određene ranjivosti sustava. Lista zaštita mijenja se tijekom vremena kako se otkrivaju nove ranjivosti. Zbog osiguranja maksimalne razine sigurnosti, sve dostupne metode zaštite alata su aktivne, a korisnik ih može deaktivirati prema prije opisanom načinu.



Slika 10: Sadržaj datoteke qflog.txt

Neke od značajnijih sigurnosnih kontrola Qwik Fix programa opisane su u nastavku:

- **Sigurnost Internet Explorer sigurnosnih zona**

Budući da velik broj malicioznih programa iskorištava sigurnosne propuste unutar IE Web preglednika, koji omogućuju izvršavanje proizvoljnog programskog koda u okviru lokalne zone sa najvišom razinom ovlasti, Qwik Fix program sadrži određene sigurnosne kontrole koje to onemogućuju. Na taj način podiže se razina zaštite od malicioznih programa koji se šire putem Internet Explorer Web preglednika.

- **Ograničavanje NULL konekcija**

Anonimni pristup sustavu korištenjem NULL konekcija dobro je poznat sigurnosni problem kod Windows operacijskih sustava. Na taj način neovlaštenim korisnicima omogućuje se prikupljanje brojnih informacija o ciljnom sustavu, a vrlo često se koriste i kao podloga za provođenje znatno složenijih napada. U tom smisli Qwik program ograničava mogućnosti pristupa korištenjem NULL konekcija.

- **Messenger servis**

Qwik Fix program onemogućava Windows Messenger servis koji su brojni maliciozni programi koristili za svoje širenje.

- **Onemogućavanje izvršavanja potencijalno opasnih ActiveX kontrola**

Maliciozne ActiveX kontrole vrlo su česta i ozbiljna prijetnja korisnicima osobnih računala. Qwik Fix program svojim korisnicima i u ovom pogledu pruža određenu razinu zaštite budući da se sprječava izvršavanje malicioznih ActiveX komponenti.

- **Blokiranje DCOM servisa**

S obzirom na broj incidenata u posljednje vrijeme koji su bili uzrokovani sigurnosnim propustima unutar DCOM sučelja, Qwik Fix program postavlja određena ograničenja na način korištenja ovog servisa. Korisnicima je dobro poznat Blaster mrežni crv koji je za svoje širenje koristio upravo sigurnosne propuste unutar DCOM sučelja.

- **Sprječavanje iskorištavanja ranjivosti unutar LSASS sustava**

Program također sadrži modul koji sprječava iskorištavanje sigurnosnog propusta opisanog unutar sigurnosne preporuke MS04-11, kojeg je ujedno koristio i poznati Sasser mrežni crv. Ovaj modul zaštiti će računala bez obzira da li imaju odgovarajuću sigurnosnu zakrpu instaliranu ili ne.

- **Onemogućavanje udaljenog pristupa registry sustavu**

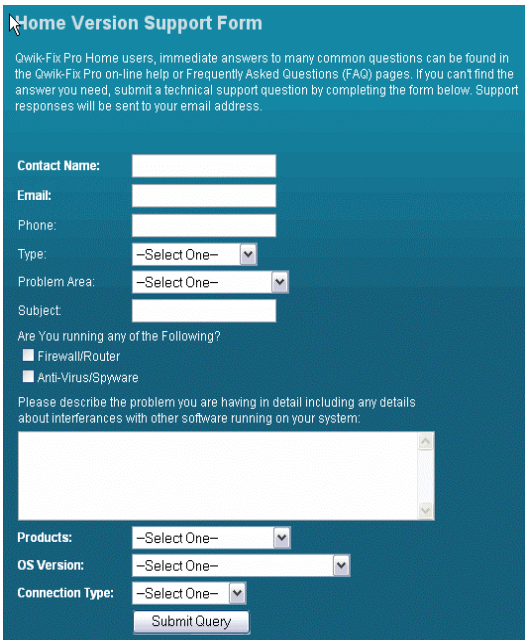
Budući da analize pokazuju da 99% posto sustava ne zahtjeva mogućnost udaljenog pristupa *registry* datoteci, Qwik Fix program onemogućava ovu funkcionalnost.

Također treba napomenuti da su ovdje navedene samo neke od sigurnosnih kontrola koje Qwik Fix program koristi za sprječavanje neovlaštenih aktivnosti. Naravno, svaka od ovih kontrola može biti

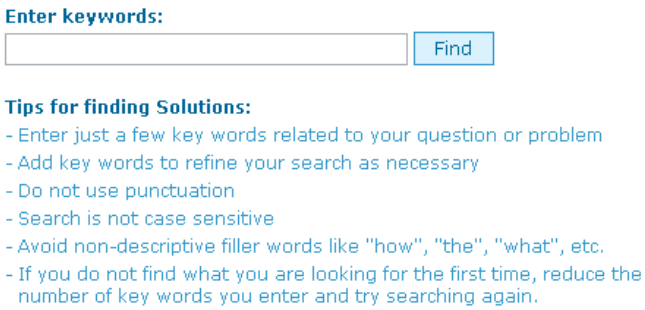
zasebno omogućena ili onemogućena, što znatno olakšava prilagođavanje programa ovisno o zahtjevima korisnika.
Analizom raspoloživih kontrola, koje su u trenutnoj inačici korisniku stavljene na raspolaganje, može se primijetiti da iste odgovaraju većini aktualnih prijetnji vezanih uz osobna računala sa Windows operacijskim sustavom. Također, na temelju provedenog testiranja može se zaključiti da Qwik Fix program, uz sitna podešavanja koja će ga dodatno prilagoditi okuženju u kojem se koristi, predstavlja izvrsno rješenje za zaštitu osobnih računala od prijetnji s Interneta.

4.4. Pomoć

Dugme `Help` otvara referentu stranicu http://www.pivx.com/support.asp na kojoj je korisnicima omogućena podrška. Na ovoj stranici korisnici će pronaći najčešće postavljena pitanja te bazu znanja kao i kontakte za podršku.
Korisnici *Home Edition* inačice alata mogu koristiti najčešće postavljena pitanja na referentnoj adresi http://www.pivx.com/supportFAQ.asp. Ukoliko žele koristiti kontakt za podršku, tada na referentnoj adresi http://www.pivx.com/supportContact.asp trebaju popuniti formu prikazanu na slici 11.
Baza znanja nalazi se na referentnoj adresi http://www.pivx.com/supportKnowledgeBase.asp, prikazana je na slici 12, a sastoji se od upisivanja ključne riječi za koju se traži pomoć.
Osim navedenih sustava pomoći, na raspolaganju je i forum koji korisnici mogu pronaći na adresi http://forums.pivx.com/.



Slika 11: Forma za korisnike podrške Home Edition inačice alata



Slika 12: Baza znanja

4.5. Deaktiviranje alata

Posljednja naredba u izborniku alata jest naredba za aktiviranje / deaktiviranje alata. Predefinirano stanje alata jest da je on aktivan pri čemu se u sučelju alata prikazuje simbol koji je prikazan na slici 13.

Slika 13: Aktivno stanje alata

Ukoliko korisnik pritisne dugme `Disable Protection`, alat se deaktivira, a simbol stanja alata se mijenja, kao što to prikazuje slika 14.

Slika 14: Deaktivirano stanje alata

5. Zaključak

Qwik-Fix Pro Home Edition predstavlja novu generaciju sustava za prevenciju neovlaštenog pristupa. Osnovna prednost programa je njegovo proaktivno djelovanje, odnosno blokiranje servisa ili funkcionalnosti čije ranjivosti maliciozni programi koriste. Ovakvim pristupom omogućuje se blokiranje napada prije nego što su objavljene odgovarajuće sigurnosne zakrpe, odnosno potpisi za antivirusne programe ili IDS sustave čime se znatno podiže sigurnost sustava. Blokiranje napada temelji se na prilagođavanju konfiguracije operacijskog sustava te onemogućavanju odgovarajućih servisa i funkcionalnosti koje omogućuju maliciozno djelovanje.

Ovaj alat ne može potpuno zamijeniti antivirusni program ili tradicionalan način instalacija sigurnosnih zakrpi (eng. *patch management*). Izuzetno je jednostavan za korištenje obzirom na način rada jer se od korisnika zahtjeva redovita nadogradnja alata, dok sigurnosne zakrpe osigurava *PivX Solutions* tvrtka. Međutim, ukoliko administratori zahtijevaju samostalno kreiranje sigurnosnih politika ili konfiguraciju alata, tada ovaj alat nije preporučljiv za korištenje.