

Re: Trojan horse Downloader.Generic.ML

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2005-06/0537.html>

From: Zvi Netiv (*support_at_replace_with_domain.com*)

Date: 06/22/05

Date: Wed, 22 Jun 2005 15:15:01 +0300

kurt wismer <kurtw@sympatico.ca> wrote:

> >> *as malware can make arbitrary changes, processing the entire file is*
> >> *required... if you're only worried about parasitic infection then sure,*
> >> *for some types of files you may only need to check a subset of the*
> >> *entire file, but integrity checkers aren't *just* for detecting that*
> >> *sort of thing...*
> >
> > *Malware doesn't make arbitrary changes, full stop.*
> >
> > *so data diddlers don't exist?*

Not really, and there are good reasons why not. The most famous data diddler, is the now extinct Ripper boot virus. Even at the peak of the boot infectors short era, Ripper was more of a conversation piece than a real threat (Simon Widlake would mention it often). The reason for its rarity is that destructiveness counters prevalence: The more destructive malware is, the lesser are its chances to survive and spread.

> > *That's a fallacy that has*
> > *been nurtured by ignorance, fools (e.g. Lambdin, with his unsolicited CRCs), and*
> > *AVers that had an interest that users assimilate that nonsense.*
> >
> > *what i said is technically correct... malware *can* make arbitrary*
> > *changes – there may not yet be a malware instance that changes bytes X,*
> > *Y, or Z in a file but there's nothing preventing one from being made...*
> >
> > *there is malware the corrupts and/or destroys data – you can contest the*
> > *existence of such malware if you like, but you'd be tilting at windmills...*

Only a fool will claim that there exist no malware that corrupts data, but a producer must really have no sense to optimize an AV product for such rare singularity.

[...]

> > *You are actually saying the same thing, but from a different angle: Users were*
> > *incapable to tell on base of the plain integrity change whether it was caused by*
> > *virus or was benign.*

- >
- > *actually, i don't think they are the same thing... i don't believe users*
- > *are incapable of such, i believe they are unwilling...*

I am both willing and experienced, but unable to tell viral from benign if all that I could use was Stiller's Integrity Master.

[...]

- > >>*there are those who feel that programmatically restoring*
- > >>*infected/corrupted objects to their original state is a losing*
- > >>*proposition... some anti-virus vendors (like sophos) don't offer virus*
- > >>*disinfection for most file infecting viruses because of this philosophy...*
- > >
- > > *Again, part of the above is propaganda, that was cultivated by interested*
- > > *parties.*
- >
- > *sophos used propaganda to justify being a less attractive option? that*
- > *really doesn't make a whole lot of business sense... you (the general*
- > *you) can't claim that action X can't be done satisfactorily so you won't*
- > *do it and expect potential customers to accept that when most other*
- > *vendors provide products that do perform action X...*

Sophos decision to not disinfect was a business decision, and the "ideology" attached to was propaganda. Fact that it worked!

- > > *The fact is that DOS objects, all types, were recovered through*
- > > *integrity methods to their *exact* original state, to the byte, including the*
- > > *time and date stamp.*
- >
- > *you can't recover overwritten objects merely from an integrity*
- > *fingerprint...*

You seem having forgotten the very basics of virus and antivirus technology. Here is a brief reminder (state of the art ca '95) :

The definition of virus (www.invincible.com/glossary.php) is: "A virus is parasitic computer code that replicates by producing functional copies of itself into host files. The infected hosts inherit the replication ability of the affecting virus, in addition to maintaining the original functionality of the host program or file."

The last part requires that everything that was contained in the program in its preinfected state, be still there, plus the necessary changes made by the virus to incorporate its own code in the program flow. A direct deduction is that all virus infections are theoretically reversible, by reverting the changes made to the program, and since nothing from the original code was lost. This is, in a nutshell, the entire theory on which virus disinfection and recovery is based upon.

As to disinfection vs integrity restoration, everything disinfection can do, restoration will do better, and much of what restoration will do, can't be done

by disinfection at all (like disinfection from highly polymorphic viruses, or from new ones).

[...]

> > *Let's extend the above now: Real-time AV optimized integrity checkers can*
> > *detect an infection and block execution of that object. When implemented*
> > *properly, real-time integrity monitoring is nearly infallible at detecting viral*
> > *changes in monitored files.*
>
> *i'm afraid i'm not yet convinced of that...*

I didn't expect you will, yet ... ;)

Regards, Zvi

--

NetZ Computing Ltd. ISRAEL www.invincible.com www.ivi.co.il (Hebrew)
InVircible Virus Defense Solutions, ResQ and Data Recovery Utilities