My Love/Hate Relationship with U3

By A.J. Newmaster

What is “U3”?

- •U3 LLC develops proprietary applications to run on Microsoft Windows directly from a U3 compatible USB drive.
- Some programs built to use U3 include: Firefox, Thunderbird, Trillian, WinSCP, PuTTY, Foxit Reader, OpenOffice.org, etc.

How does it work?

- Creates 2 partitions on the drive.
  - An emulated CD-ROM drive (ISO 9660)
    - Autorun information and LaunchPad
  - A standard FAT partition
    - Standard storage drive with a hidden “SYSTEM” folder to keep installed U3 applications.

Can’t these run on “regular” USB Drives?

- Yes. Websites like http://portableapps.com/ have these programs (plus more) that you are able to run from ANY thumb drive.

So…Why would I want a U3 drive?

- **Portability**: Can run applications on almost any Windows computer without administrative rights.
- **Software Support**: Lots of applications made for U3
- **Ease of Use**: Comes with “LaunchPad”, a program that mimics the “Start” button in Windows, just a lot less stable.

…So it doesn't do anything a regular drive can't?

- Maybe. Other than software that U3 LLC has developed specifically for U3 drives, I have not found any software that runs only in the U3 environment.
- There are faster, more stable alternatives to U3 software.
- U3 DOES however autorun like a CD-ROM.

So where's the love?

- Used "as-is", I hate U3.
- I have found it slow and unstable.
- It has completely locked my computer while running Nero(U3 acknowledges this in its FAQ).
- It's completely closed source
- It's difficult to uninstall.

Hate: Part Deux

- Leaves traces of U3 software on host machine
- Creates a false sense of security
  - Most LaunchPads have a security lock built into the CD-ROM partition requiring you to enter a password before it will open that data partition. After so many failed password attempts, the drive is supposed to lock itself, preventing brute force attacks.
    - Too bad the data partition isn't encrypted.

Okay, we get it. You hate U3, but what does it do that makes you love it too?

- Able to make sensitive files read-only.
- **Live Forensics**: If you have a set of tools you like to use for live data analysis that run without installation, you can keep them in the read-only partition so the host computer cannot modify them. The information captured by these tools can be saved to the data partition. (Live Demo)

Double Edged Sword

- If “good” software can run (especially autorun) on a read-only drive, so can “bad” software.
- Currently, Norton, McAfee, and Zone Alarm do not pick up any of my scripts or software.
  - Even if they did, they couldn’t delete the “malicious” code because its on a read-only partition :-D

  Live Demo

Yeah..that's not good.

- Although I have created this from scratch, there are many programs out there readily available for any script kiddie to use.
- Hak.5 has created two programs very similar to mine and have very good documentation on how to do it. These tools are:
  - USBSwitchblade
  - USBHacksaw

What can I do to save myself?

1) Lowest Privilege.

Some of the tools I use require an administrator account to run. Though this won't stop everything, it's a good start (and running at the lowest privilege is always recommended)

What can I do to save myself?

2) Always keep a trusted antivirus program active on your machine.

Most software that script kiddies are going to use will be detected and make it unable to run.

What can I do to save myself?

3) Disable Autorun

There are many tutorials on how to do this on the net. It won't stop someone from running their script manually, but it makes it where you at least have a chance. Also, autorun starts even if you have a locked screen saver.

What can I do to save myself?

- There are programs out there like DeviceWall that claim to prevent things like this from happening, but I have never used any of these programs.
- The best thing to do is just be careful. If you don’t want to disable autorun, then hold the left shift button down while you insert the drive. That will disable autorun temporarily.

Remember:

At some companies, the janitor is the richest guy in the place.

Sources

- http://en.wikipedia.org/wiki/U3
- http://www.hak5.org/
- http://u3.com/
- Paranoia

Questions?