Kira Stancil

Software Design
4670 Bell Street, New York, NY 10004
United States

View the full portfolio at http://www.thecreativefinder.com/youria

Professional Experience and Curriculum Vitae
Polymorphic malware is a type of virus that mutates as it spreads, making it difficult to detect and block. They are paired with self-redistributing code that can change itself regularly. The polymorphic virus encrypts its own code, and for this reason it is nearly impossible to detect. Any malware can be modified by a polymorphic virus: Trojans, worms, keyloggers, and more.

Examples of polymorphic malware
The especially famous Storm Worm polymorphic backdoor Trojan, discovered back in 2007, could change itself every 10-30 minutes. The speed of its change has become a real headache for cybersecurity experts trying to root out the threat.

Modern polymorphic malware can change up to 3-4 times per minute. However, many antivirus suites use signature-based search methods. This method struggles to find something that can change the program.
According to research, polymorphic malware makes up 94% of all malware. So how do you defend against this ever-evolving threat?

How can I prevent polymorphic malware infection?
If you want to surf the Internet in relative safety, then your devices must be protected by the most modern means of protection, use a good malware guard and pair it with a VPN, me personally using https://chrome.google.com/webstore/detail/free-vpn-for-chrome-vpn-p/majdfhpaihoncoakbjgbdhglocklcgno and I highly recommend it. You should be especially ready because an attacker is armed with disguised viruses.

Methods of protection against polymorphic plague:

1. Use heuristic scanning. It is effective, but only up to a certain level - only if the polymorphic virus contains the code of old malware. Viruses that have never been seen before will not be considered harmful.
2. Use behavioral analysis. It is about using tools that can identify threats and deal with them based on how they work, rather than trying to stop them.
3. Maintain updates. Don't ignore updates, spend 10 minutes rebooting your device and make sure all software is up to date. Manufacturers such as Adobe and Microsoft regularly respond to security vulnerabilities by patching them with software updates. Outdated software is a good way to provide an opportunity for malware infection.
4. Don't open suspicious links. If you receive any emails that look suspicious, send them directly to the trash can.
5. Be constantly aware of what is happening. The best way to prevent malware from invading your digital life is to be aware of the different types of viruses and signs of infection to look out for if they raise suspicion. Find out what exactly your antivirus program is protecting against and if there are any threats that it cannot deal with. If so, then it makes sense to change the protection to a more reliable one.

Previous Clientele
Please kindly get in touch for more information.
Awards and Accolades
Please kindly get in touch for more information.
Awards and Accolades
Please kindly get in touch for more information.

Kira Stancil

Software Design
4670 Bell Street, New York, NY 10004
United States

View the full portfolio at http://www.thecreativefinder.com/youria

Please kindly get in touch for portfolio works.