Learn about polymorphic malware and super polymorphism

As mentioned in previous articles, malware (malware) has become a big problem. Unrighteous people are taking advantage of ransomware, keyloggers, bank trojans and cryptojacker to redeem themselves from the victims.

As mentioned in previous articles, malware (malware) has become a big problem. Unrighteous people are taking advantage of ransomware, keyloggers, bank trojans and cryptojacker to redeem themselves from the victims. With free or paid antivirus software, your system's users are enhanced security.

Hackers have a trick to interfere with security systems. Antivirus software often relies on a "signature" to detect whether a program is malicious. When a new virus is detected, its signature is recorded and sent to other people's antivirus software to help detect new viruses more effectively. In a way, signature is the 'fingerprint' of the virus in the profile. Once detected, other antivirus software announced will remove the rogue software as soon as it appears.

But what if a hacker can change the signature for a virus? That way, the virus avoids being detected even if the antivirus software has a log that records the 'fingerprint' of the previous malware. This means that the virus has been camouflaged in a new fashion. This is exactly what polymorphic and polymorphic malware can do, and in the future, some of these "stubborn" malware will spread over the Internet.

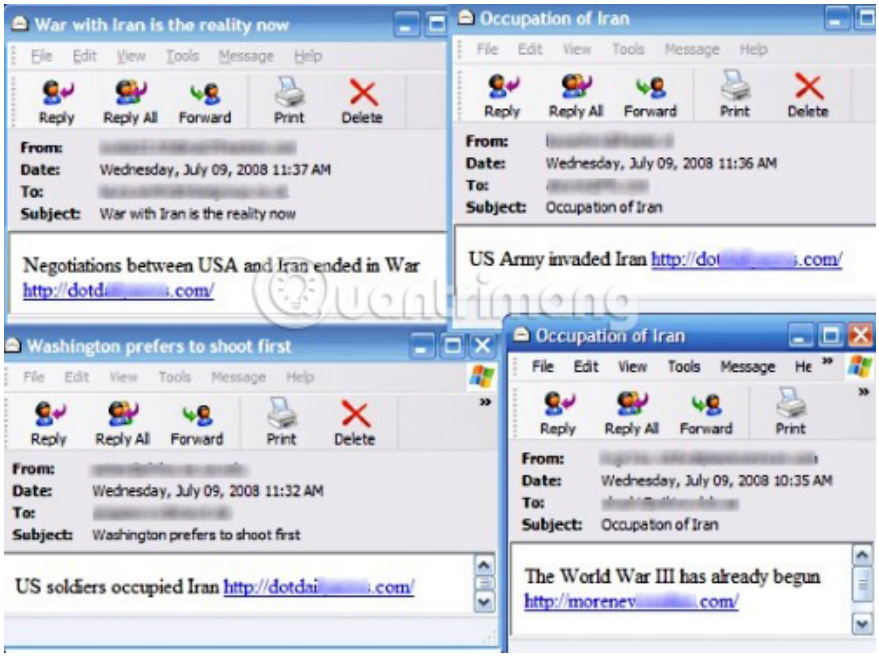
What are polymorphic and polymorphic malware?

1. Polymorphic malware

2. Super polymorphic malware
3. How does AI affect this?
4. What can users do?

Polymorphic malware

Polymorphic malware has a core that always performs the same task, no matter how many times it changes. It always performs the same actions and always strikes the same way, but it continues to adjust the rest of the code to keep its 'versions' always different. Polymorphic malware can be a bit more easily defined than its hyper-polymorphic 'brother' brother, since antivirus software can use the 'core' to detect and identify malware.



An example of today's polymorphic malware is the Storm Worm. It first appeared in 2007 and was named Storm Worm because its initial attack method was to send an email with the subject **230 dead as storm batters Europe** (230 people died after storms in Europe. Europe). Once the victim is infected with malware, their computer will create a new malware every 30 minutes and send it. The subject line will change over time (as seen above), but the worm's main code remains the same.

Super polymorphic malware

Metamorphic (Malamorphic) malware is far more dangerous. While polymorphic malware can be detected by the core, polymorphic malware attempts to reorganize all of its code after each version. It brings together the same logic and functionality that it had before, but adds elements like fake code and reordered functions to make it look different from previous 'versions'. This makes antivirus software much more difficult to detect.

How does AI affect this?

When people are entering a world where AI is becoming more and more complete, a battle between malware creators and security programmers is taking place drastically. Both sides are using AI to enhance their fighting power to gain a competitive advantage.

With the support of AI, the reconstruction of code for polymorphic and polymorphic malware is quick and effective. This means that malware will be harder to detect, be able to spread, and avoid more virus-weaving software.

Of course, with security companies also having access to high-end AI, the battle is going on in both directions. Antivirus software developers can program to detect malware quickly without depending on its signature. By using AI to make reasonable decisions about how malware works, anti-virus software does not need to rely on the 'fingerprint' stored in the file. It only needs to discover the agent in action and isolate suspicious things.

What can users do?

It may be a bit scary to hear about malware that has the ability to evade security, but the fact that antivirus software is the best method a user can use remains unchanged! Do not download seemingly suspicious files,

open suspicious emails or click on strange links that friends on social networks send you. Super malware polymers can't attack if you don't give them a chance!

With the current anti-virus software on the Internet, malware developers are always looking for ways to upgrade their programs to bypass security systems. Now you know about polymorphic and polymorphic malware, as well as the threats it can bring. Do you think things will get worse or will security companies win the war AI? Let us know in the comments below!

See more:

1. How to detect VPNFilter malware before it destroys the router
2. Hidden patterns of malware
3. Summary of popular network attacks today