A Guide to Understanding & Defending Against Advanced Malware

ADVANCED MALWARE

Advanced Malware is one of the biggest threats your company can face. It's not well understood, it's secretive, and it can often go undetected for months because it's always changing and evolving to circumnavigate the latest security systems.

Different hackers have different motives - some are for a political or social cause, some plan to sell your information on the dark market for financial gain, and some are foreign nation states hoping to steal secret and proprietary information from private companies. While each type of malware behaves a little differently, all have the same objective: to gain access to your network and exploit sensitive information.

TYPES OF MALWARE

1. Ransomware - includes the crypto-locker and crypto-wall virus. Crypto-locker is a type of ransomware that takes over your files by encrypting them. It doesn't necessarily look like a virus, it just goes through your system and encrypts your files. The FBI has started to shutdown servers used to encrypt files.

2. Spyware - a type of malware intended to monitor a user's activities without their knowledge. Spyware can be difficult to detect and is usually aimed at gathering sensitive information such as passwords, banking information, or even just internet usage habits.

3. Scareware - an unethical marketing tactic to scare you into purchasing antivirus software. With scareware, a window will pop up on the user's computer designed to look like a legitimate warning. It will claim that the computer has been infected, and will try to sell the user an antivirus solution that promises to get rid of the virus, i.e. scaring the user into making a fraudulent purchase.

4. Trojan horse - much like in Greek mythology, a Trojan horse is a virus disguised as something interesting, useful or routine that will try to convince the user to download it. Most commonly, it will be an email attachment disguised as something harmless.

5. Worms - a form of malware that can spread through your network by replicating itself and targeting security failures to infect other computers in your network. Worms are destructive viruses rather than an information gathering virus, and will usually consume a large portion of bandwidth that slows your computer down.

6. Rootkits - a Rootkit copies or masks itself as core files in order to gain unauthorized access to your data and control of a computer system without being detected. The attacker will target the root or the admin of a computer system, and they can be extremely difficult to remove.

Advanced Malware is always changing and evolving to circumnavigate the latest security systems.

Who Makes Advanced Malware?

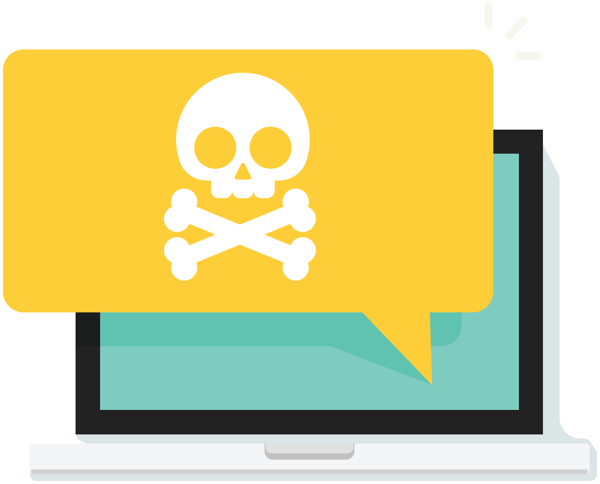
It is unknown where most of these viruses come from. Usually it is computer hackers working for themselves or a larger system of organized crime. These attacks can come from anywhere worldwide, but it is speculated that most come from developing nations where people are seeking opportunities to make money, gather account information, and cause trouble for others.

The FBI has a special cyber task force dedicated to seeking out and prosecuting cyber adversaries targeting U.S. interests, including government and private organizations. According to the FBI Cyber Division, hackers are usually motivated by one of the following:

- **Hacktivism:** using computer network exploitation to advance a political or social cause.
- **Cyber-Crime:** the theft of personal information via a computer or network for purpose of extortion and financial gain.
- **Insider-Crime:** theft of proprietary information for personal, financial and ideological reasons.
- **Cyber-Espionage:** nation-state actors who conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.
- **Cyber-Terrorism:** groups that sabotage computer systems that operate our critical infrastructure, such as electric grids.
- **Cyber-Warfare:** nation-state actors who sabotage military and critical infrastructure systems to gain an advantage in the event of a conflict.

How do you get infected?

People bring in viruses without knowing it through their personal devices, laptops, USB drives, tablets, phones, etc., but malware is most often contracted via email and sketchy websites. A very common scenario is when an employee opens an email attachment from an unknown sender. The attachment may look innocent on the surface, but it could very well be infected with Cryptowall.



Cryptowall will search the employee's computer and all accessible remote drives, and render them useless via encryption. This puts your whole organization and network at huge risk, especially when you consider global read-write network files.

What happens if you get infected with Cryptowall?

Once Cryptowall is in the network and has encrypted all your files, you'll receive a ransom note in the form of website link instructing you to pay a specified amount for un-encryption. The hackers will demand that you pay anywhere from $500 to a few thousand dollars to get the un-encryption key. However, there is NO GUARTENTEE that they will actually deliver on that promise and unencrypt your files.

It is recommended that you never pay the ransom; it will simply fund the hackers to continue their mission of creating malware. Instead, you should rely on your backup systems, revert to the latest version of your network before the virus, and then wipe your system clean to get rid of Cryptowall. If you do not have a robust backup system, do your best to recreate the encrypted data, and immediately implement the best practices below.

Best Practices:

Advanced Malware is a frightening threat that no one wants to deal with, but there are things you can do to protect yourself. We've put together a checklist for you on what you should be doing to protect your network and your business from costly downtime. Each business is different, and you should consult an IT Profesional to develop a tailored a defense plan suited for your compliance requirements and specific needs. This checklist is the minimum baseline defense that everyone should implement into their business plan.

Defense Plan:

- **Backup –** it is crucial to your business that you have a strong backup system in place. You should be backing up your entire network on an hourly or continuous basis so that if you ever do become infected with malware, you can wipe your system clean, and revert to the latest backup before the infection spreads.
- **Update Windows –** much more important than anti-virus!
- **Update your Antivirus –** it's very important to update your antivirus daily, or use a web-based antivirus solution because advanced malware is changing and evolving all the time. If your antivirus solution is out of date, you will be vulnerable to Zero-Day Viruses, which are unknown, unrecorded malware advancements.
- **Employee user agreements –** usually advanced malware will enter your network through human error like when someone connects to your network through an unsecured internet connection, or opens an infected email link. It is crucial that everyone in your organization understands these threats, and adheres to your organization's user policies.

Want to dig deeper on Advanced Malware?

Contact Us Today

SEATTLE • PORTLAND • PHOENIX • TUCSON • FLAGSTAFF
866.575.9512

BLACKPOINT-IT.COM