

Hatteras Software along with the Wake Forest Chamber

Viruses and Malware

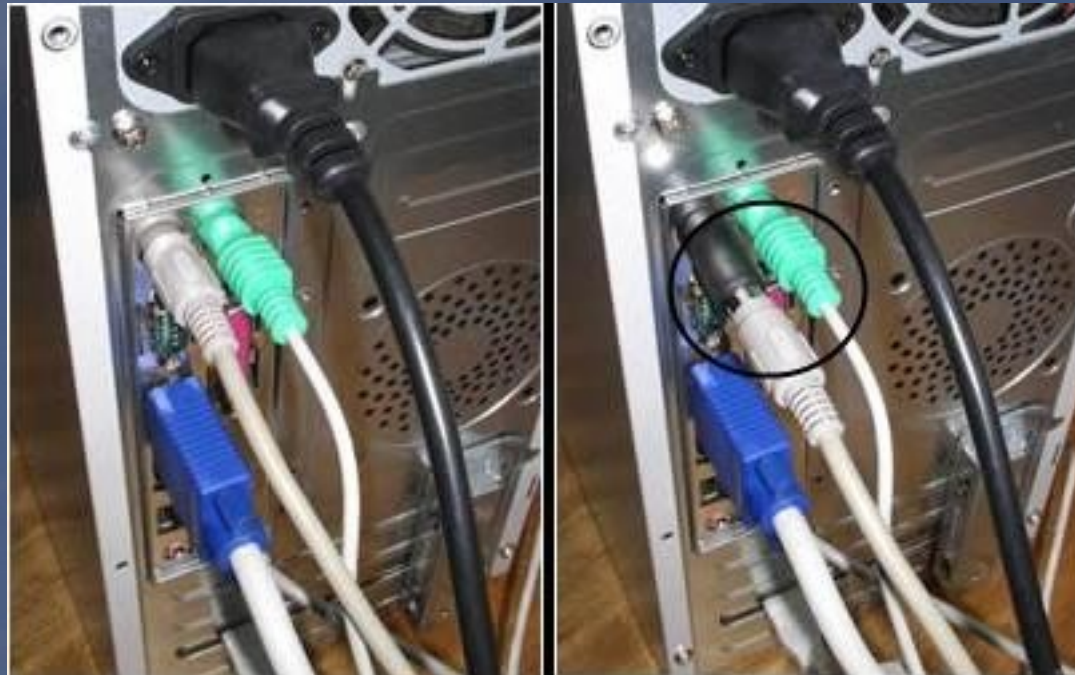
Virus Alert



<http://www.youtube.com/watch?v=zvfD5rnkTws>

- Malware – Superset category referring to computer viruses or spyware.
- Virus – A software program capable of reproducing itself and potentially causing harm to a computer. Generally requires human help to propagate.
- Worm – A computer virus that is able to replicate itself to other systems by connecting to a service and taking advantage of a flaw in that service.
- Trojan – A computer virus that attaches itself to other files on the system or is attached to a file and spread by email. Can be a PDF, Word file, Powerpoint presentation, etc.
- Spyware – Malware that is designed to watch a user's computer usage and steal information from the system.

- Keylogger – Malware or hardware that is designed to collect a user's keystrokes. Generally used to steal user IDs and passwords.



- Rootkit – Malware that masks its presence by overriding system functions such as directory listings, process list, registry entries, etc.

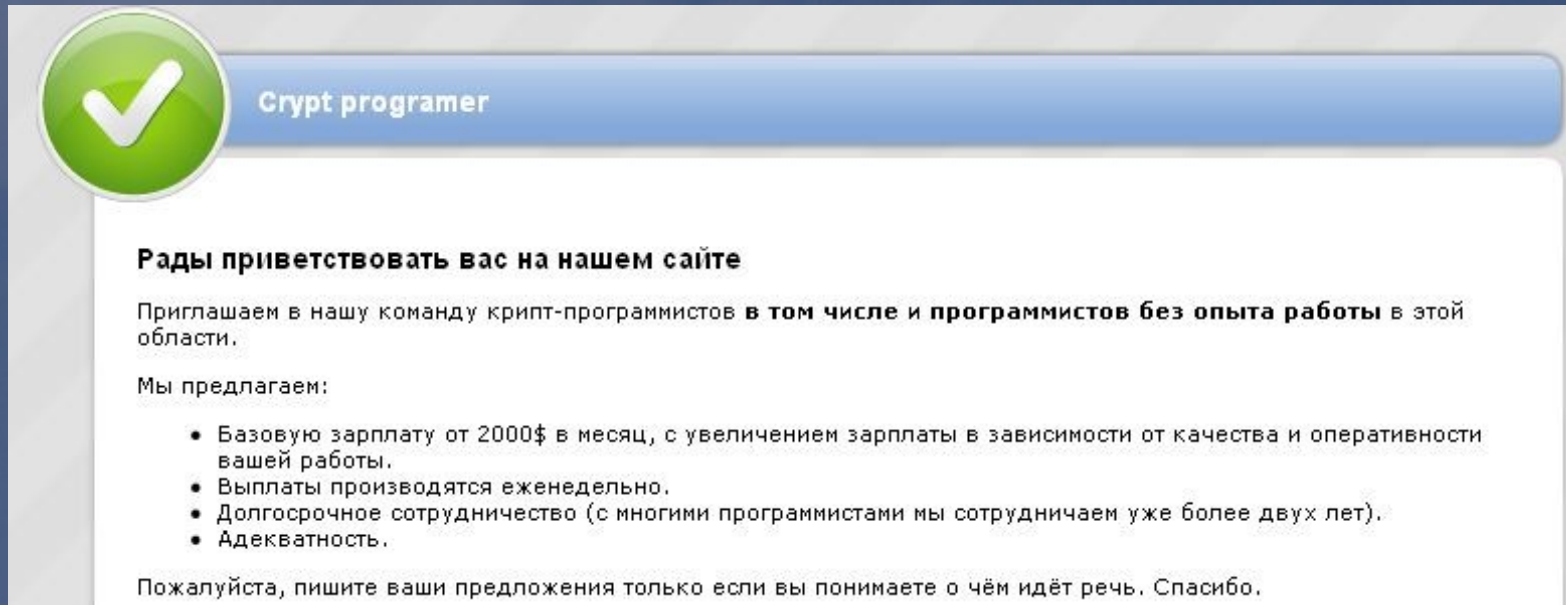
- Use and keep your Anti-Virus and Anti-Spyware software up to date. Update definitions daily, full scan weekly.
 - Should detect rootkits.
 - Should use heuristic or “behavior based” detection.
- Use a firewall program that alerts when an unauthorized program connects to the network or wants to accept incoming connections.
- Use Firefox or Google Chrome with the Adblock+ extension.
- Avoid using the default OS software such as Internet Explorer, Media Player, etc.
- Install updates on a timely basis.

Prevention – PEBKAC and ID10T Errors

The computer is artificially intelligent, you are really intelligent.

- Or: Programs will only go so far. You make up the difference.
- Scan attachments before you open them.
- Do not open attachments from untrusted sources.
- Verify with the sender that they really did send you the attachment when you get an unexpected attachment.
- Disable auto-play.
- Do not insert untrusted media.
- Scan files before you open them if someone gives you a thumb drive or CD.

- Identity theft is big business. Low risk, high reward.



The screenshot shows a recruitment post for a 'Crypt programmer'. It features a green checkmark icon in a circle on the left. The text is in Russian and includes a welcome message, an invitation to join a team of crypto-programmers (including those with no experience), and a list of benefits: a base salary of \$2,000 per month with increases based on performance, weekly payments, long-term cooperation, and adequacy. The post concludes with a request for applicants to understand the offer and a 'Thank you'.

✓ Crypt programmer

Рады приветствовать вас на нашем сайте

Приглашаем в нашу команду крипто-программистов **в том числе и программистов без опыта работы** в этой области.

Мы предлагаем:

- Базовую зарплату от 2000\$ в месяц, с увеличением зарплаты в зависимости от качества и оперативности вашей работы.
- Выплаты производятся еженедельно.
- Долгосрочное сотрудничество (с многими программистами мы сотрудничаем уже более двух лет).
- Адекватность.

Пожалуйста, пишите ваши предложения только если вы понимаете о чём идёт речь. Спасибо.

“We invite you to join our team of crypto-programmers, including programmers with no experience in this field.

We offer:

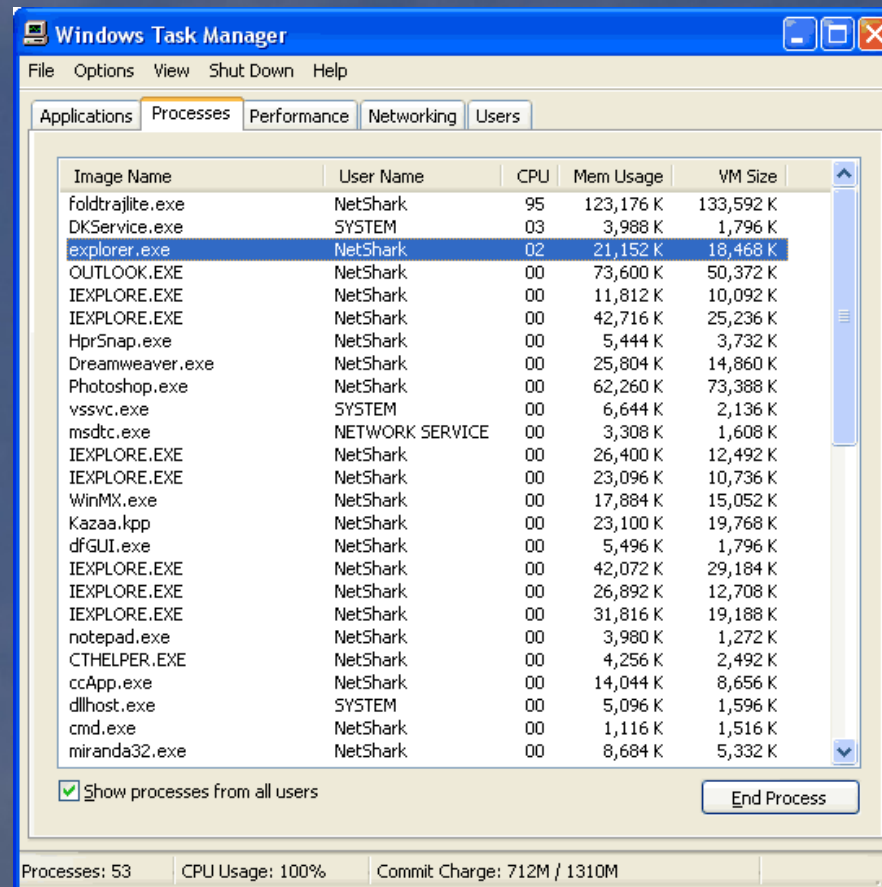
- * Base salary from \$2,000 per month, with an increase in salary, depending on the quality and timeliness of your work.
- * Payments are made weekly.
- * Long-term cooperation (with many programmers, we have been in business for more than two years).

The Problem

- Anti-Virus companies are outnumbered and can only do their best effort.
- Report by Information Week (Oct'10) showed that AV stopping ability declined by 6%
 - 10% - 45% chance a virus will get by AV software.
- False positives with heuristic or “behavior based” detection.

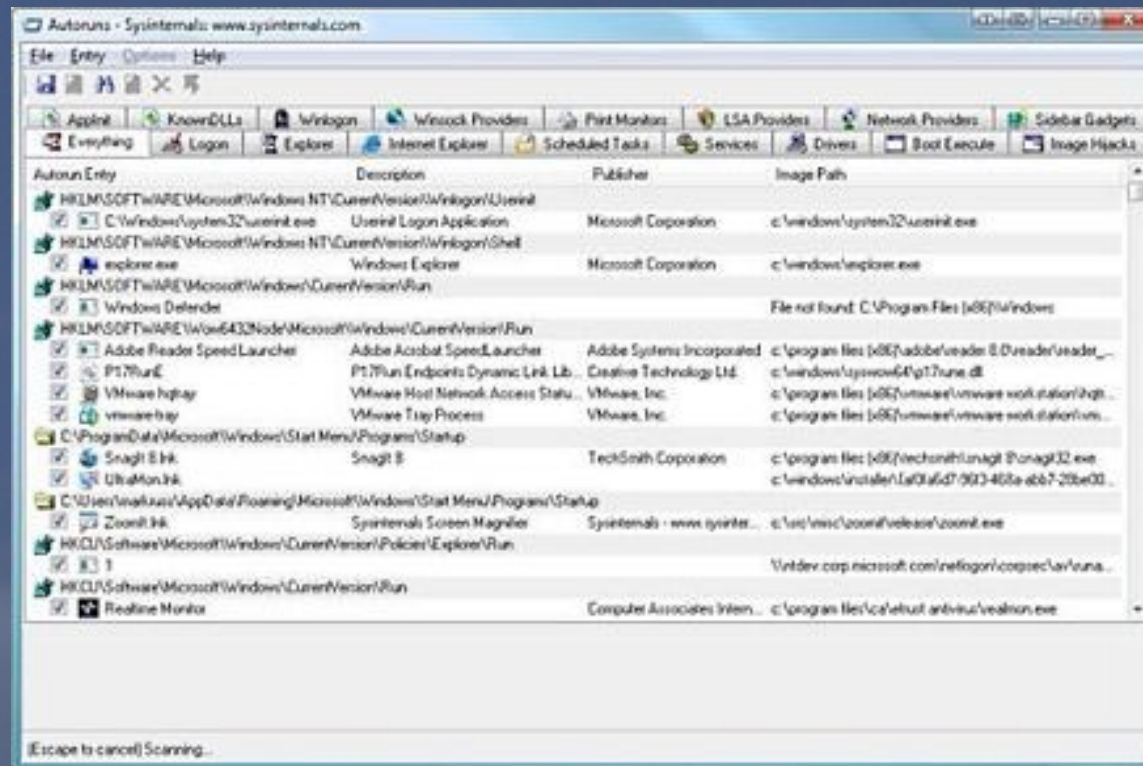
Detecting Viruses

- Best to use your anti-virus software to detect and remove.
- Use the Task Manager to determine why your system is being slow.



Detecting Viruses

- Use a registry cleaner like Norton to detect and remove any problems in your registry. These issues can reduce speed.
- Do not let programs auto run when the system starts.
 - <http://technet.microsoft.com/en-us/sysinternals/bb963902> - Autoruns



Detecting Viruses

- If a new program asks for access to install software, connect to the internet, or accept incoming connections, verify that you installed it and that it should be doing this.
- If you get a warning from “Anti-Virus 2011” that you are “infected.” These programs are scams. They will first use your credit card fraudulently. Then they will sell the info for identity theft.
 - Definite signs: Cannot start the task manager.
 - Fix: Reboot into safe mode, use autoruns to find and disable the Malware.
 - This is actually one of the the easiest infections to solve.

Erik Nedwidek
Hatteras Software
nedwidek@lighthouseitc.com