Position Overview:

Trend Micro Research is seeking a Malware Researcher to join our industry-leading research team. Trend Micro Research supports a global customer base including leading security product vendors, software vendors, and large enterprises with a set of industry-leading technical data feeds, research products, and engineering services.

As a Malware Researcher, you will be part of a team that analyzes advanced malware samples using static and dynamic analysis with the primary goal of decoding and detecting malware communication mechanisms.

Responsibilities:

- Reverse-engineer malware samples to identify malware communication mechanisms and analyze malware network traffic to develop Snort signatures.
- Produce documentation describing malware behaviour and detection strategies.
- Communicate research results to customers, team members, and management.
- Collaborate with team members to improve the analysis and response process.
- Monitor security industry publications, newsgroups and press releases to identify new or active malware threats.

Required Knowledge:

- Advanced knowledge in reverse engineering on various architectures and platforms.
- Familiarity with debugging tools such as IDA Pro, WinDbg, and OllyDbg.
- In-depth knowledge of modern operating systems including Windows and Linux.
- Familiarity with low level programming languages such as C/C++ or assembly language is a plus.
- In-depth knowledge of TCP/IP and other networking protocols. RFC-level understanding of popular protocols like HTTP/FTP/SMTPL/SMTP.
- Familiarity with tools such as Snort, Wireshark, Windows Sysinternals and VMware.
- Familiarity with scripting languages such as Python, Ruby, Perl, JavaScript or Bash.

Required Skills & Abilities:

- Ability to analyze and describe complex application behaviours.
- Experience of reverse engineering is a big plus.
- Excellent English communication skills, both written and oral.
- Great attention to details and personal QA.
- Team player, self-motivated, self-starter with the ability to work with minimal supervision.
Required Professional Designation/Certification:

- Bachelor’s or Master’s degree in computer science or a related field preferred but not required.

Required Experience:

- Industry experience performing similar technical role preferred but not required.