CSO
FROM IDG

CAREER TRACKER

What it takes to be a malware analyst

What it takes to be a **malware analyst**

The proliferation of ransomware and other attacks has increased demand for experts who can analyze how the software works and devise a response.

BY BOB VIOLINO

THE RISE IN RANSOMWARE attacks shows that malware is still very much a major cybersecurity problem for organizations. The professionals on the security team perhaps best suited to address the challenge are malware analysts.

"Cybersecurity incidents are on the rise around the world, with prominent recent examples including the worldwide WannaCry ransomware attack, and the need for experienced malware experts is outstripping the available supply of talent," says Domini Clark, principal at Blackmere Consulting, a recruiter of information security professionals.

"We are seeing more positions titled 'malware analyst' in the market. However, other titles are related to this work, including security consultant or reverse engineer and threat researcher," Clark says.

The majority of these roles are found in security consulting firms, security products companies and government contractors, versus enterprise environments, Clark says. However, there are exceptions to this with large organizations. "The truth is, many enterprise environments simply lack the resources to keep pace with dynamic threats, nor can they justify the spend for a team specific to malware analysis," she says. "Instead, they rely on vendors for this intelligence."

As with other information security skills, there is a significant shortage of malware analysts, Clark says. A supply-and-demand search using Careerbuilder's data portal, which pulled data from nationwide figures over the last two years, shows the title "malware analyst" resulted in 1,726 job postings and only 52 "active" candidates.

Those who possess these skills, including Brian Rogalski, malware analyst at electronics company Raytheon, are certainly keeping busy examining the latest malware attacks. Rogalski says he always liked computers, and built his first one through trial and error while in high school. "I think I knew I would always end up in the field," he says.

After focusing on hardware, software and networking aspects of IT in his initial jobs, Rogalski began looking at security as a possible focal point. "It was a natural progression for me," he says. "I think subconsciously my interest in security indirectly became prevalent through spy movies. I was always fascinated with James Bond and other types of espionage movies. I felt like I wanted to be a part of that world."

In the movies espionage activities always had the help of technology. "That coupled with a natural curiosity of how things work got me interested more about technology," he says.

Early in his career, Rogalski worked as a risk analyst at Fidelity Investments and a security and network architect at Boston Electronics. It wasn't until he joined financial services technology company DST Technologies in 2006 that he got a taste of malware analytics.

While at DST, Rogalski was part of a small information security team, and one of his duties was to evaluate threats to the financial industry. "One

threat was the Zeus banking trojan," he says. "At the time although I knew what it did from a high level, I was curious to know how exactly the trojan worked."

It was then that his interest in malware analysis began to take shape. "At the time, I didn't realize the good the malware analysis or reverse engineering process could have on the security community and the world," Rogalski says.

"Cybersecurity incidents are on the rise around the world, with prominent recent examples including the worldwide WannaCry ransomware attack, and the need for experienced malware experts is outstripping the available supply of talent."

-DOMINI CLARK, PRINCIPAL AT BLACKMERE CONSULTING

Following his time at DST he worked as a malware analyst for other companies before joining Raytheon in 2014. He also runs his own malware analysis and consultation services.

"The reason I work for the people I work for and the companies I do is to drive the malware analysis and security community to do greater things," Rogalski says. This comes in the form of research, analysis and intelligence-related products.

CAREER PROFILE

Malware analyst

CORE KNOWLEDGE | Software research, system analysis, threat modeling, network traffic analysis, intrusion detection, assembly language, code review, encryption, knowledge of dynamic and static analysis tools, and solid programming and scripting skills

POTENTIAL EMPLOYERS | Consulting firms, security solutions vendors, some large enterprises

NATIONAL MEDIAN SALARY | **$80,400** (according to Payscale)

"It is all to stop the cyber bad guys and to help protect others, to give back to people," he says. "I know that technology keeps moving, increasing and becoming more prevalent in every aspect of our lives. As our dependence on technology and computing increases, so do the opportunities for people to exploit them. For me, making sure that I am always agile and keeping up with advances in technology allow me to keep making new opportunities for myself."

In addition to professional success, Rogalski's skills have led to personal benefits as well. "Malware analysis has given me the chance to explore the world," Rogalski says. "There is such a need for analysts that if you can do this type of work, then there is a chance that security companies from anywhere in the world may need your help."

During his career Rogalski has lived and worked in Boston, Washington D.C., the United Arab Emirates and the United Kingdom. "My motivation has always been to do some good while doing what [I] love," he says. "For me that is traveling and learning about new cultures and having new life experiences."

Rogalski did not attend college when he was younger because neither he nor his family had the money needed for him to pursue a college

degree. "At first I did not see the benefit. Now I see how important it is and I am pursuing my education," Rogalski says. He is currently taking courses at Western Governors University, an accredited online college, to obtain a BA in computer science with a cyber security focus. His goal is to earn a master's degree and eventually a PhD.

"Recently, many national and military agencies have begun funding quantum computing research, Rogalski says. Quantum computers "will be able to solve computational problems, but more quickly," he says. This will create an even greater attack surface for hackers to exploit."

-BRIAN ROGALSKI, MALWARE ANALYST, RAYTHEON

"The world of computing is evolving, so must we," Rogalski says. "I am always trying new ways to improve my skills. Right now, we are seeing the worlds of physics and computing merge. I hope to learn and earn a degree in physics and learn more about quantum computing."

Recently, many national and military agencies have begun funding quantum computing research, Rogalski says. Quantum computers "will be able to solve computational problems, but more quickly," he says. This will create an even greater attack surface for hackers to exploit.

"In my opinion, this is the next big thing," Rogalski says. "It seems clear to me that simply having a computer science degree will not be sufficient to keep pace with technology and smart hackers. If I am going to stay agile and keep ahead of the adversaries, I am going to need more education in advanced mathematics and physics and then apply that knowledge to create protection mechanisms similar to what we have now, but just at a subatomic level."

In the meantime, demand for malware analysts will likely continue to rise, as will compensation for these professionals. "As with all supply and demand examples, low supply and high demand increases price," Clark says. "Of course, it is also resulting in an increasing number of experts turning to independent consulting, a trend that often increases the price even further as consulting rates skyrocket."

In addition to increased compensation, experts with niche skills in areas such as malware analysis can often call their own shots, including remote work, decreased travel and the ability to turn down projects that aren't exciting to them, Clark says.

Becoming a malware analyst does require a strong understanding of security, however. "If you're looking to get in on the game you have to come to the table with a wide array of expertise in multiple areas," Clark says. That includes software research, system analysis, threat modeling, network traffic analysis, intrusion detection, assembly language, code review, encryption, knowledge of dynamic and static analysis tools as well as solid programming and scripting skills. ■