TEVORA

tevora.com

Incident Response

Malware Analysis and Reverse Engineering

Evading detection is the key to success for cybercriminals. Malware delivery tactics and digital attributes are constantly evolving to bypass the latest firewalls and network gateways.

As a result, the cybercriminal's body of work is rapidly expanding, representing millions of active threats. Some are known and defensible using malware detection technology. Others are new and so sophisticated that they can modify their own digital signatures to prevent detection.

The good news is that you don't have to go it alone. If you suspect a compromise, Tevora's Malware Analysis and Reverse Engineering services have what it takes to stop the threat, clean the system, and build your defenses to guard against future attacks.

Threat Dissection

While "families" of malware possess similar traits, the goals, purpose, and skills behind each piece of malicious software are as unique as its criminal creator. With further variation driven by the need to continually evolve to avoid detection, malware permutations can be as varied and unique as snowflakes—each with its own scripting patterns, payload delivery, and behavior.

Tevora takes a comprehensive and highly scalable approach to detecting and analyzing unknown, advanced, and targeted malware. Using automated tools, our process begins with the examination of network traffic, file activity, and registry keys for basic "indicators of compromise." These help us rapidly identify and quarantine suspected malware and minimize its impact on your environment.

How Tevora Dissects and Reverses Threats

1. **Isolate**
   - Use automated malware detection and analysis tools to gain a high-level understanding of how the malware interacts with the environment
   - Using tools and visual examination, determine how the malware has been packaged to obfuscate its inner workings
   - Conduct a static analysis to examine code structure for insights on how payload is executed
2. **Analyze**
   - Deploy malware in an isolated environment to discover all functionality and behavior, and determine motive
   - Snapshot system configurations, files, and settings before and after running malware to identify anomalies
   - Monitor network traffic to identify any inbound and outbound connections
3. **Respond**
   - Reverse engineer the malicious code to review functionality and logic for hidden agenda or purpose
   - Look for additional functionality within the malware that may not have been triggered
   - Apply insights from analysis and reverse engineering to determine how to eradicate the malware, and the appropriate defenses for future protection

HITRUST Authorized CSF Assessor

TEVORA

tevora.com

Our Purpose

To protect the world from cyberthreats.

Insightful Advice
Expert Resource
Confident Delivery

About Us

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Irvine, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's digital assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments, so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization's unique pressures and challenges, so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership, and—year after year—apply our cumulative learnings to continually strengthen the company's digital defenses.

Go forward.
We've got your back.

We then isolate the malicious software in our advanced malware analysis lab in an environment that mirrors your network. There, our experienced analysts conduct a static analysis of the code structure to understand the malware's purpose based on its embedded resources and strings, hashes, and other attributes.

Our team also performs a dynamic forensic analysis of the malware through its attack life cycle. We execute the malicious code in our isolated environment to learn its behavior. Close monitoring by our team and "before-after" snapshots of system configurations, files, and settings enable a better understanding of what the malware is designed to do. It also helps us identify other systems and information that are at risk.

Reversing the Threat

The in-depth phases of our analysis return a wealth of knowledge of the malware's purpose and behavior. Reverse engineering—including decoding encrypted data and decompiling and disassembling the exe binary—surfaces deeper insights into the code to reveal its critical logic and functionality. These provide valuable and actionable insights that support the effective removal of the malware from your system and drive the appropriate strategies for defending against it in the future.

Good Security Is Good Business

Our credentialed Tevora senior consultants apply their depth of experience to view each security issue through a business lens. We know that an MBA is as important as a CISSP, and we take the time to learn your unique challenges. Tevora's Malware Analysis and Reverse Engineering services combine our technical knowledge with practical business acumen to develop and execute strategies that help you navigate an evolving threat landscape, fortify your assets, and build a secure foundation for the future.

HITRUST Authorized CSF Assessor