VMRAY

CASE STUDY

G DATA Advanced Analytics Relies on VMRay for Rapid Incident Response and Malware Analysis

Based in Bochum, Germany, G DATA Advanced Analytics brings 30 years of experience to the fight against malware and cyber attacks. A subsidiary of G DATA Software AG, the division mainly serves customers in health care and hospitals, small and medium enterprises (SME), law enforcement, and administrative infrastructure for city government.

As Tilman Frosch, the Managing Director of G DATA Advanced Analytics explains, "In essence, we're a fire department for computer networks. When a customer's network has been breached due to a malware attack, we help them respond quickly to minimize the impact. To keep their infrastructure safe, we're always looking for tools that enhance our core expertise, which is incident response and in-depth malware analysis. We recently deployed VMRay Analyzer to ensure a more rapid incident response process and to strengthen containment of malware attacks."

Facing Down Today's Threats

"Although malware constantly evolves, Frosch highlights two ubiquitous threats that his customers face today: ransomeware attacks and malware that escalates privileges. "Ransomware can paralyze a customer's operations, cut off their revenue, and even threaten people's lives," Frosch says. He cites the example of hospitals that provide radiation therapy for cancer patients. "If an attack shuts down vital infrastructure, we know we typically have five days to get the hospital up an running again, before patients' health and recovery may be endangered."

G DATA | ADVANCED ANALYTICS

Why G DATA Advanced Analytics Chose VMRay

CONDUCT malware analysis in just minutes

EFFECTIVE COUNTERMEASURES to contain the damage caused by malware attacks

ISOLATES and protects confidential customer information

TRUST in VMRay's underlying research and technology

EASE OF USE and deployment

Attack methods that escalate the attacker's privileges pose a different challenge, says Frosch. They allow an attack to penetrate deeper into the network, exposing high-value information assets, causing wider damage, and making containment and remediation more costly.

Speed is Imperative

"Where malware attacks are concerned, a rapid response is essential," says Anders Fogh, Principal Security Researcher for G DATA Advanced Analytics. Using the example of online retailer, Fogh says, "The longer an attack goes on the more a retailer loses in sales, revenue, customer loyalty and their public reputation. For our team, VMRay Analyzer is a key tool to quickly and effectively achieve a first assessment of a malware sample within the incident response process."

"VMRay analysis can point toward countermeasures that will disrupt the behavior of the triaged malware, while allowing the healthy parts of the network to operate safely."

ANDERS FOGH **PRINCIPAL SECURITY RESEARCHER/DATA ANALYTICS**

Conducting Analysis in Minutes

During the identification phase of an incident, team members from G DATA Advanced Analytics primarily work onsite with the customer to quickly figure out what is happening. One of the most important steps to understanding a breach is to identify and triage the offending malware sample and then do an initial analysis with VMRay before conducting a manual, in-depth analysis.

“Time is money,” says Fogh. “With VMRay we can complete our initial assessment from start to finish in less than 20 minutes. The output of that analysis gives us a basic idea about the nature of the attack and provides insight into how to handle the incident. Often, we gain indicators of compromise (IOCs), such as IP addresses and changed registry keys. The forensic team can use this information to pivot around and determine how far the network has been penetrated,” says Fogh.

In the containment stage of an incident, the team uses detailed information--on the attackers’ tooling, goals, and capabilities—which has been gained from manual analysis and network and systems forensics. VMRay analysis output provides a complementary view on the triaged malware samples. This assists the team in planning containment measures with high confidence while keeping interruptions at a minimum within the healthy parts of the customer’s infrastructure. For example a careful reading of VMRay logs can detect hints that passwords might be compromised and need to be changed.

"With VMRay’s capabilities we can provide faster answers when customers ask, ‘What should I do right now to contain the damage and get rid of the malware while also ensuring it doesn’t come back next week or next month?"

TILMAN FROSCH **MANAGING DIRECTOR**

A Solution That’s Virtually Undetectable

An affordable solution that is easy to use and deploy, VMRay is virtually undetectable by malware, making it more difficult to evade. It is particularly helpful at quickly extracting shellcode from a malware sample. “Additionally, VMRay lets us set up a dedicated sandbox solution that is deployed independently of other infrastructure. We run a large proprietary sandbox infrastructure at G DATA, however, not every sample can be submitted to this company-wide infrastructure,” says Fogh, noting the heightened confidentiality requirements in some environments, such as law enforcement. “This reinforces our customers’ confidence that their information will never leave our unit.”

"Many attacks can be easily stopped," says Frosch, "but often our customers don’t have the staff or expertise to deal with it. VMRay’s capabilities improve our response time. It helps us to reliably provide initial directions, before we manually dive into a malware sample. In turn, we can provide faster answers when customers ask, ‘What should I do right now to contain the damage and get rid of the malware while also ensuring it doesn’t come back next week or next month?’"

See VMRay in action

To learn more about VMRay Analyzer or to schedule a demonstration,
contact **info@vmray.com** today.

REQUEST A DEMO

