SOLUTIONARY®
AN NTT GROUP SECURITY COMPANY

White Paper

How Malware Analysis Benefits Incident Response

How to realize better protection, response efficiency and increased granularity in your security program.

How Malware Analysis Benefits Incident Response

Contents

SOLUTIONARY

Introduction

Pending a security breach, incident response helps mitigate the loss of intellectual property, personally identifiable information and other critical private data. Incident response programs strive to limit the damage of a security breach or attack, along with the cost of recovery. Whether handled by a dedicated internal team or a trusted security partner, incident response programs are vital to an effective security strategy. Incident response includes several components, from resource identification and preparation to technical investigation and containment, but malware analysis is one specific area of security that has become increasingly beneficial to the process.

Today malware can be highly sophisticated, targeted and complex, as well as commercialized and scalable for widespread attacks. With malware at the root of so many security breaches, malware analysis is a vital component of an incident response program. It helps responders understand the extent of a malware-based incident and rapidly identify additional hosts or systems that could be affected. Actionable information from malware analysis can help an organization more effectively mitigate vulnerabilities exploited by malware and help prevent additional compromise.

Phases of Incident Response

To better understand the relationship between malware analysis and incident response, it is first necessary to review the phases of incident response.

Phases of Incident Response

Phase 1 - Preparation

Identify an incident response team and outline responsibilities. Prepare the team to respond to security events resulting in an incident. Of course, an effective defense-in-depth security strategy should also be implemented and maintained to reduce the likelihood of a successful attack.

Phase 2 - Detection and Analysis

When an incident occurs, incident response team members must quickly gather, analyze and interpret events and log files from intrusion detection systems, firewalls, routers, switches, domain controllers, and other networked systems. Interpretation and analysis are critical to this phase as they help determine the level of security impact for a given incident.

During this phase, the incident response team will likely attempt to determine the attacker's intent, which can further guide incident response efforts. Some questions that may be asked during this analysis include:

- Was the attack specifically targeted at the organization or was it opportunistic?
- Was the attack intended to penetrate the organization directly or simply to gain lateral access to the real target by leveraging vendor and business-to-business relationships?
- Was the attack part of an initial reconnaissance by the attacker and can the information be used to thwart future attacks?

Malware analysis is relevant to all phases of incident response—preparation, detection and analysis, containment and eradication, and post-incident activity.

Phase 3 - Containment, Eradication and Recovery

Containing a security incident helps mitigate losses. After containment, eradication may be necessary. This includes deleting malware and disabling compromised accounts. During recovery, administrators restore systems to normal operation and remediate identified vulnerabilities to help prevent similar incidents from reoccurring, especially since successful attacks are often followed with similar techniques against similar targets.

Phase 4 - Post-Incident Activity

Learning from incidents and improving processes and defenses are critical, but often overlooked. A post-incident review helps identify weakness and improvement opportunities in security architecture, as well as the incident response team's abilities.

The Value of Malware Analysis for Successful Incident Response

Malware analysis is relevant to all phases of incident response—preparation, detection and analysis, containment and eradication, and post-incident activity. As incident response planning and preparation take place, organizations should consider whether their teams have a properly trained and equipped responders who can quickly and effectively perform malware analysis. Without these resources, organizations could struggle to identify malware as the root cause of an incident. They may also take longer to contain incidents or fail to completely understand and eradicate malware from their networks, causing incremental damage and loss over time.

When Incidents Occur

When malware is the source of a breach, knowledge of its capabilities and behavior are crucial to effective incident response. Quick and reliable malware analysis can reveal the functionality of the malicious code. It can identify any changes the malware may have made to affected systems, and it can provide preliminary host- and network-based indicators for detection signatures. Malware analysis often requires in-depth reverse engineering of malicious code and unknown software for a deep understanding of its capabilities, intent, attack vector, motivation and tactics. Organizations should not be scrambling to find and equip malware analysts in the wake of a breach. When malware analysis is already part of an incident response program, it helps ensure a more swift and effective response and containment.

Malware analysis can be used to spot technical indicators, key elements or forensic artifacts that are unique to the malicious code, whether in the way the malware behaves or in components of the code itself.

Incident Response for Advanced Malware Threats – the Value of Technical Indicators

The malware used in advanced threats typically goes undetected by common antivirus and network-based detection solutions. Targeted attacks using unique malware have a stronger likelihood of successfully compromising the intended target. In the case of advanced, targeted malware-based attacks, malware analysis plays a critical role in incident response, especially when it comes to isolating technical indicators related to malcode.

Malware analysis reveals technical indicators that can be used to spot additional infections and compromised resources. These technical indicators are forensic artifacts unique to the malicious code. They can relate to the way the malware behaves or the code itself, and can be identified on a host or network. Technical indicators include traditional forensic artifacts such as MD5 checksums or hashes, malware compile times, file size, name, path locations and registry keys. Technical indicators can also include domain names, IP addresses, email addresses, URIs or URLs, or any suspicious network communication. Finding technical indicators may require advanced malware analysis techniques, such as memory forensics analysis, identification of running process components, and imported/exported libraries used by an executable. Technical indicators can be logically grouped together to increase

detection effectiveness into what are known as Indicators of Compromise or IOCs. Many of the technical indicators can help create host- and network-based signatures that are used by many security software solutions.

Malware Analysis and Post-Incident Activity

While post-incident activity is often an overlooked phase of the incident response process, it is probably the most important one. During this phase, information learned by malware analysis should be documented and included in the incident summary reports or separate malware analysis documents for dissemination. The information should be used to help prevent future malware-based incidents of similar nature. Sharing information about the incident and its analysis with appropriate business units in the organization can also help ensure others are aware of the threats and mitigation efforts and help bolster the capabilities to defend against future threats.

While post-incident activity is often an overlooked phase of the incident response process, it is probably the most important one.

Understanding Malware Analysis Techniques

Malware analysis examines malicious code in order to identify it on a host or network, and to reveal how it works, how to contain it and how to eliminate it. Isolating technical indicators is a major piece of this puzzle. Malware analysis is an important component of overall security strategy, but as stated earlier, its ability to uncover technical indicators associated with malware make it highly beneficial for incident response. As technical indicators are revealed, responders can further identify other resources affected by the same malware. In addition, malware analysis provides the information required for effective eradication and recovery.

Malware analysis involves two key techniques: static analysis and dynamic analysis. Static analysis examines malware without actually running it. Dynamic analysis (also known as behavior analysis) executes malware in a controlled and monitored environment to observe its behavior. These techniques are further categorized as basic or advanced. Although there are benefits for conducting static and dynamic analysis as separate tasks, the value provided by conducting both techniques is realized when reverse engineering complex malware. Performing static and dynamic analysis together helps identify the true intent and capabilities of malware and can provide a series of technical indicators that may not be achievable by static analysis alone.

Basic Static Analysis

Basic static analysis examines malware without viewing the actual code or instructions. It employs different tools and techniques to quickly determine whether a file is malicious or not, provide information about its functionality and collect technical indicators to produce simple signatures. Technical indicators gathered with basic static analysis can include file name, MD5 checksums or hashes, file type, file size, and recognition by antivirus detection tools.

Basic Dynamic Analysis

Basic dynamic analysis actually runs malware to observe its behavior, understand its functionality and identify technical indicators that can be used in detection signatures. Technical indicators revealed with basic dynamic analysis can include domain names, IP addresses, file path locations, registry keys, additional files located on the system or network, or communication with an attacker-controlled external server in an attempt to download additional malware files.

Advanced Static Analysis

Advanced static analysis loads malware into a disassembler to reverse engineer and analyze the program instructions and determine program functionality. Advanced analysis requires deeper skills and understanding of assembly, code constructs, and the concept of how operating systems use code libraries. Advanced techniques can provide additional details about malware that are not generally revealed through basic analysis.

Advanced Dynamic Analysis

Advanced dynamic analysis uses a debugger and other specialized tools to examine the execution of malware while it is active. In some cases, basic dynamic analysis may not provide fruitful results or malware may require additional information to run. Using a debugger to manually step through malware program code provides another way to extract detailed information from malware files.

Host- and Network-based Approaches to Malware Analysis

Malware analysis typically follows two different approaches: host-based and network-based, both of which can be performed in serial or parallel. An incident response and/or malware analysis team may work both approaches simultaneously, or start with the network-based approach to gain information for working the host-based approach. Each analysis is based on the situation at hand and the information, skills, technology and capabilities available to the responders.

The Host-based Approach

Host-based analysis is often chosen first, usually because a specific system has been identified as being infected or compromised, either through a network- or host-based alert. The alert can range from an IDS signature or anti-virus message to user awareness.

Host-based analysis begins with a review of the affected resource, following the traditional analysis process for host-based forensics. The primary goal is to identify and collect suspected malware files for additional analysis. Some examples of suspect files include executable files running from or stored in temporary file locations, files recently accessed or opened from remote resources (thumb drives, remote folders, etc.), and Dynamic Link Libraries (DLLs) loaded by an application from unusual paths.

Malware analysis of identified files is further enhanced by technical indicators, which can drive targeted incident investigation and response efforts. Analysis often produces a list of additional files and hosts for examination, which can identify other resources involved in an incident and additional malware to analyze.

Once collected, technical indicators can be used to identify infection via login scripts, custom IDS/IPS signatures or network scans of identified listening ports and services. If not already underway, deploying network sniffers or packet capture devices to capture associated network traffic should be considered.

The Network-based Approach

The network-based approach generally starts with network log analysis or packet capture analysis. An alert prompts the collection and correlation of log data to create an incident timeline. That data is often required to start the analysis process. Log data can come from any resource capable of producing detailed data output that is useful to reproducing how the scenario unfolds. This may include firewall logs, router logs, proxy logs and syslog data. The network-based approach also involves analyzing full network-packet captures to determine what has happened from the network perspective.

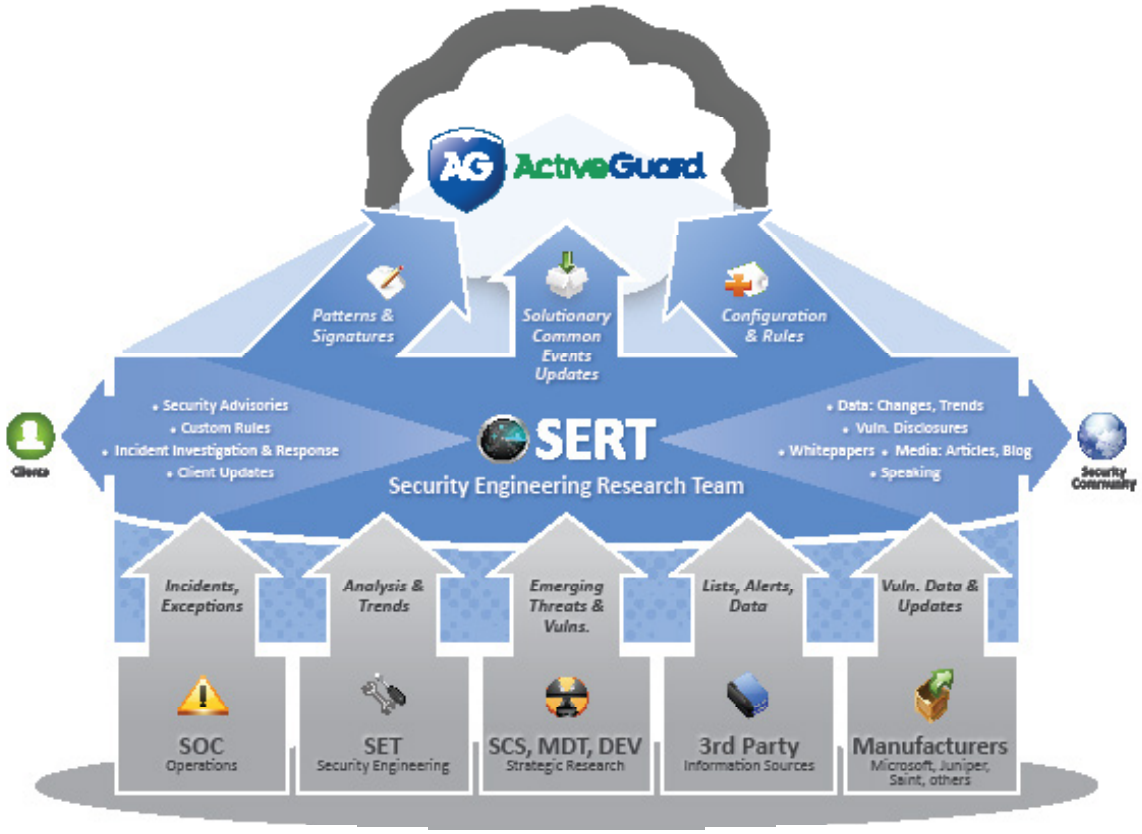
Correlated log data can be used to follow a malware attack communication and determine any executable or other suspicious files which were downloaded or uploaded. Indicators discovered in the log data that point to affected resources should prompt a review of the identified host via host-based analysis techniques. This is an example of network-based and host-based approaches working together.

If full-packet captures are available, packet analysis will provide more detailed information about the attack, possibly including Command and Control (C&C) channels and communication traffic. Packet captures enable responders to single out any suspicious files for analysis, and to observation of associated network traffic.

When confronted with C&C channels, advanced threats will often obfuscate the communication through encoding routines or encryption algorithms. The coupling of host-based and network-based malware analysis will provide greater insight into the communication and may enable decoding or decryption of malicious traffic.

Malware analysis, along with event log analysis, is a key component of incident response. The combination can provide organizations with the tools needed to identify and respond to threats as they arise. Early recognition of a security event, along with forensic data about the incident, can significantly reduce the time between incident identification and mitigation.

Enhanced Incident Response with SERT Malware Analysis, Global Threat Intelligence and ActiveGuard®



The Solutionary Security Engineering Research Team (SERT) conducts 24/7 security threat research, vulnerability analysis and incident response. With years of experience protecting clients and helping them respond effectively to security incidents, the SERT team understands the importance of swift malware identification, containment and eradication as part of incident response.

SERT professionals research emerging threats, malware, vulnerabilities, detection techniques, attack trends and the security landscape to provide clients with early-warning notifications of risks and threats. SERT includes an expert team of malware and network forensic analysts specifically trained in malware analysis techniques

and approaches. Clients that rely on Solutionary for incident response benefit from a powerful combination that includes:

- Expert malware analysis, including identification of technical indicators
- Powerful security intelligence and contextual awareness delivered via the ActiveGuard® platform
- Continuous threat research and a closed-loop process for incident response that addresses preparation, detection and analysis, containment and eradication, and post-incident activity

SERT global threat intelligence feeds the ActiveGuard platform, the cloud-based, context-ware technology behind Solutionary services. ActiveGuard is able to accurately collect and correlate vast amounts of contextual data from virtually any application or device capable of producing a log file, including applications, databases, endpoints, firewalls, IDS/IPS, UTMs, WAFs, FIMs and network devices. ActiveGuard automatically enriches collected security data with a variety of contextual information such as vulnerabilities, assets, GeoIP, malicious hosts, privileged and non-privileged users to detect threats and increase accuracy. The contextual awareness in ActiveGuard acts as a force multiplier, enabling Solutionary to improve security while making it more efficient.

When a malware-related incident occurs, the SERT team quickly examines malicious code and associated traffic to understand the malware and define its functionality. Further analysis enables SERT to identify the scope and intent of the code, including the technical indicators so helpful to attack identification, containment and eradication, and post-incident activity. The advanced analytics in ActiveGuard in combination with threat intelligence and malware analysis from SERT help recognize, contain and eradicate advanced threats and zero-day attacks. With a large, diverse client base, Solutionary is able to leverage intelligence across thousands of clients to detect and respond to advanced and emerging threats faster than internal client teams.

With malware at the root of so many security breaches, strong analysis is required for effective incident response. An incident response program that includes expert malware analysis and global threat intelligence helps responders identify malware-based incidents and understand their ramifications. Actionable information from malware analysis can help an organization more effectively mitigate vulnerabilities exploited by malware and help prevent additional compromise.

About Solutionary

Solutionary, an NTT Group security company (NYSE: NTT), is the next generation managed security service provider (MSSP), focused on delivering managed security services and global threat intelligence. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs. The patented, cloud-based ActiveGuard® service platform uses multiple detection technologies and advanced analytics to protect against advanced threats. The Solutionary Security Engineering Research Team (SERT) researches the global threat landscape, providing actionable threat intelligence, enhanced threat detection and mitigating controls. Experienced, certified Solutionary security experts act as an extension of clients' internal teams, providing industry-leading client service to global enterprise and mid-market clients in a wide range of industries, including financial services, healthcare, retail and government. Services are delivered 24/7 through multiple state-of-the-art Security Operations Centers (SOCs).

For more information, visit www.solutionary.com

Learn More

To learn more about malware analysis and find ways to implement it in your security plan, contact Solutionary today.

Contact Solutionary at SCSManagement@solutionary.com or 866-333-2133

Solutionary, an NTT Group security company, is the next generation managed security services provider (MSSP), focused on delivering managed security services and global threat intelligence.

Solutionary.com

Solutionary, Inc.

9420 Underwood Avenue

Omaha, NE 68114

2005WP 05/13