ADVANCED THREATS IN THE ENTERPRISE

Finding the Evil in the Haystack with RSA ECAT

ABSTRACT

This white paper explains the current challenges that organizations face defending against today's threat landscape and the importance of more advanced malware detection on endpoints. RSA ECAT takes an innovative approach by providing deep host visibility and sophisticated anomaly detection.

April 2014

RSA WHITE PAPER

RSA

EMC²

Part Number H13012

TABLE OF CONTENTS

EXECUTIVE SUMMARY

With thousands of workstations and servers under management, most enterprises have no way to effectively make sure they are free of malware and other advanced threats. Today, many sophisticated, targeted attacks rely heavily on unknown (zero-day) vulnerabilities that are delivered leveraging social engineering tactics. Numerous hacking events made public recently have highlighted the vulnerabilities of even the most renowned security companies, government contractors and Fortune 500 enterprises. The problem can affect any enterprise and a new approach to combat these threats must be implemented in order to deal with it effectively.

EFFECTIVENESS OF CURRENT PROTECTION AND RECENT ATTACKS

The Stuxnet worm and related targeted malware, like Duqu and Flame, show how skilled attackers can use malware to effectively gain access to a company's most valuable assets. More troubling is the time it took for companies to realize they were breached and remediate. One year after the public release of Stuxnet, Iran was still struggling to identify and remove instances of the infection. Similarly, Flame remained undetected for over two years.

The questions we should ask regarding these types of attacks are: "What kind of protection was in place when the intrusions occurred and how effective was it?" Is it reasonable to think that most compromised entities were at least protected by antivirus (AV) and other standard security solutions? Of course, the answer is yes, virtually every victim of targeted attacks had AV and multiple layers of other security products in place already, and yet they were not able to effectively detect the attack.

ANTIVIRUS AND ADVANCED THREATS

AV companies use known virus signatures to identify malware. Although this technique worked well in the past when a few thousands viruses were found in the wild each year, it has been overwhelmed by the growth of malware families. Just one AV vendor alone created more than 500,000 new signatures in 2010 and this flood doesn't show any sign of stopping. Creating signatures requires dedicated, highly skilled personnel that can't keep up with the pace. They will be inevitably reactive, not proactive in identifying threats. They must focus on the most widely distributed malware and put aside those with low distribution rates, which by definition is the case with a targeted attack.

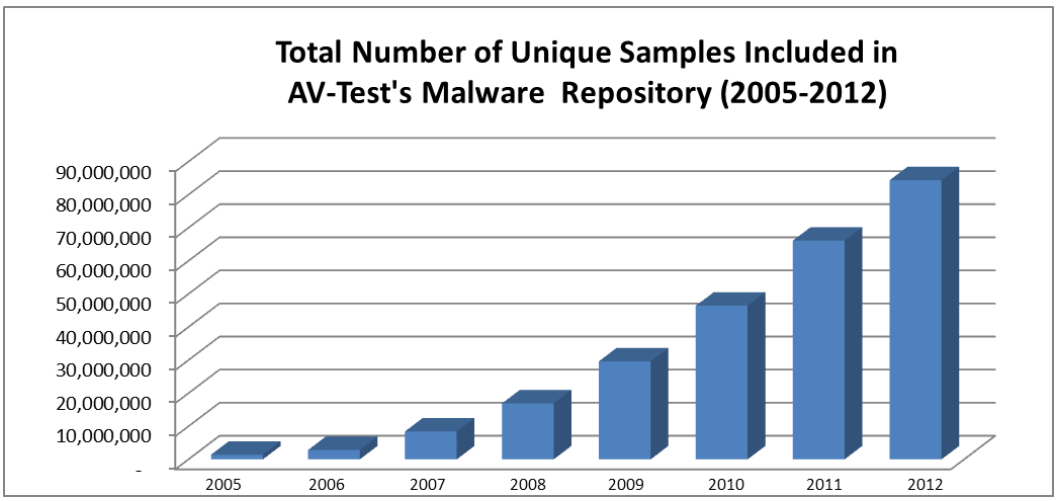

Fig.1: Unique malware file growth 2005-2012 (Source: AV-Test malware repository)

WHAT'S THE SOLUTION?

RSA recognized the need to address the advanced threat problem with a fundamentally different approach than traditional anti-malware solutions. The technologies and approaches described in this whitepaper allow enterprises to answer the questions "Do we have compromised machines and if so, how severe is the threat?" These technologies, combined with experience working with enterprise customers worldwide, are the foundation of RSA ECAT (Enterprise Compromise Assessment Tool), our answer to these questions.

MALWARE DETECTION THROUGH LIVE MEMORY ANALYSIS

The cornerstone of our approach is live memory analysis. Live memory analysis is a process by which agent software performs the analysis of a computer's memory to find traces of compromise and malware behavior. Contrary to the AV or IDS approach of matching suspected malware or traffic patterns with known malware signatures, the live memory analysis conducted by the RSA ECAT agent gives the analyst a view from a centralized console of what is happening inside the computer's memory. This view can quickly expose a malware infection, regardless of whether a signature exists or not.

RSA ECAT has several advantages over traditional approaches:

Be where the action is: Most anti-malware solutions work at the computer's internal and external interfaces (network, disk, USB drive, email, etc.) to try and block malware. When malware bypasses those defenses, a payload gets loaded in memory. That's exactly where the RSA ECAT agent resides, looking for malware footprints and monitoring for dangerous behavior.

Monitor *all* network communications: Since the RSA ECAT agent is on the endpoint it has the ability to monitor the network communications wherever the computer is. Not only does it monitor connections when the computer is in the corporate network, it also monitors connections if the computer is a laptop used at home or at Wi-Fi hotspots, something appliances are not able to do because of their placement at the enterprise network border.

Analyze in memory activity: Network communication is just one behavioral aspect of malware and advanced threats. Many more behaviors can reside in computer memory that can be analyzed and detected and may be more obvious than complex extrusion patterns. Behaviors such as file hiding, key logging or code injection bubble up quickly when performing a complete memory analysis and allow rapid malware detection.

Investigate with all the information needed: The RSA ECAT agent acts as an extension to the analyst's knowledge, allowing him/her to remotely access all the information needed for the analysis, avoiding costly visits and user or server downtime.

Reduce the cost of taking action: Usually, when an abnormal event is detected, the typical reaction is to scan the system with different commercial AV software and if nothing is discovered, reimage the whole system. With the RSA ECAT agent, you know exactly where the malware is installed, what files are running in memory, how they launch at startup and how they interact with trusted applications to bypass your installed security solution. This level of information is invaluable for remediation, incident response and forensics.

Build knowledge about the attackers: It's easier to find the source of an attack and to prevent it from happening again when you have all the information pertaining to it. With access to the offending files, it is possible to investigate how the malware got in, how it works and to put in place the protections required to block similar attacks from happening again.

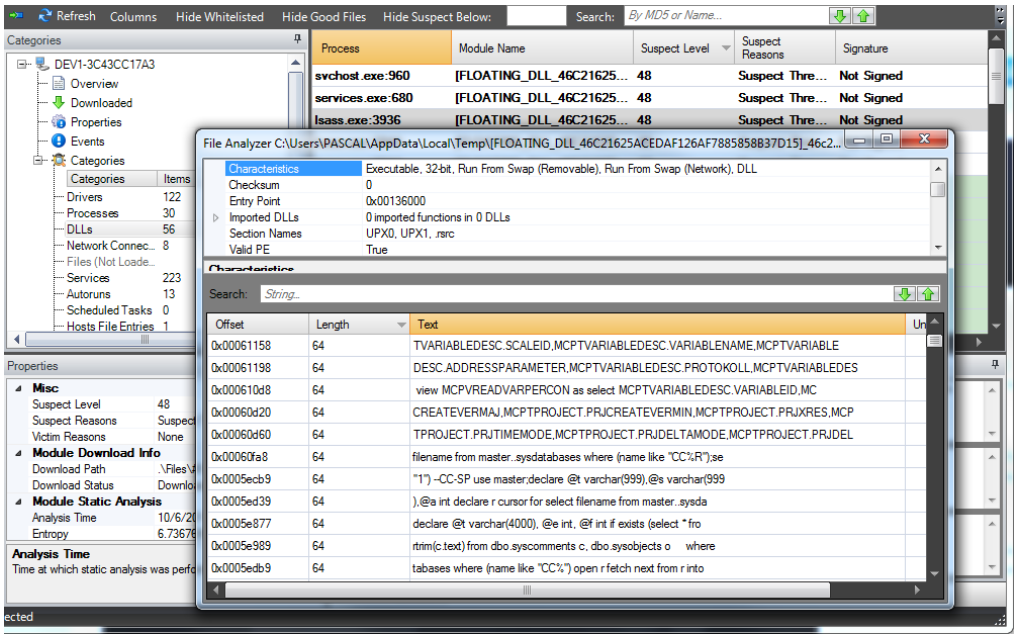

Fig.2: Live memory view of code injected by the Stuxnet into trusted processes. This can be automatically extracted for analysis.

FIGHTING ADVANCED THREATS WITH RSA ECAT SYSTEMATICALLY

In order to effectively detect advanced threats within the network, a systematic approach is needed, seamlessly integrating and deploying the technologies outlined here. RSA ECAT does exactly that. Agents can be deployed across the endpoints for scanning and managed from a central console and server(s).

Deploying RSA ECAT Across the Enterprise:

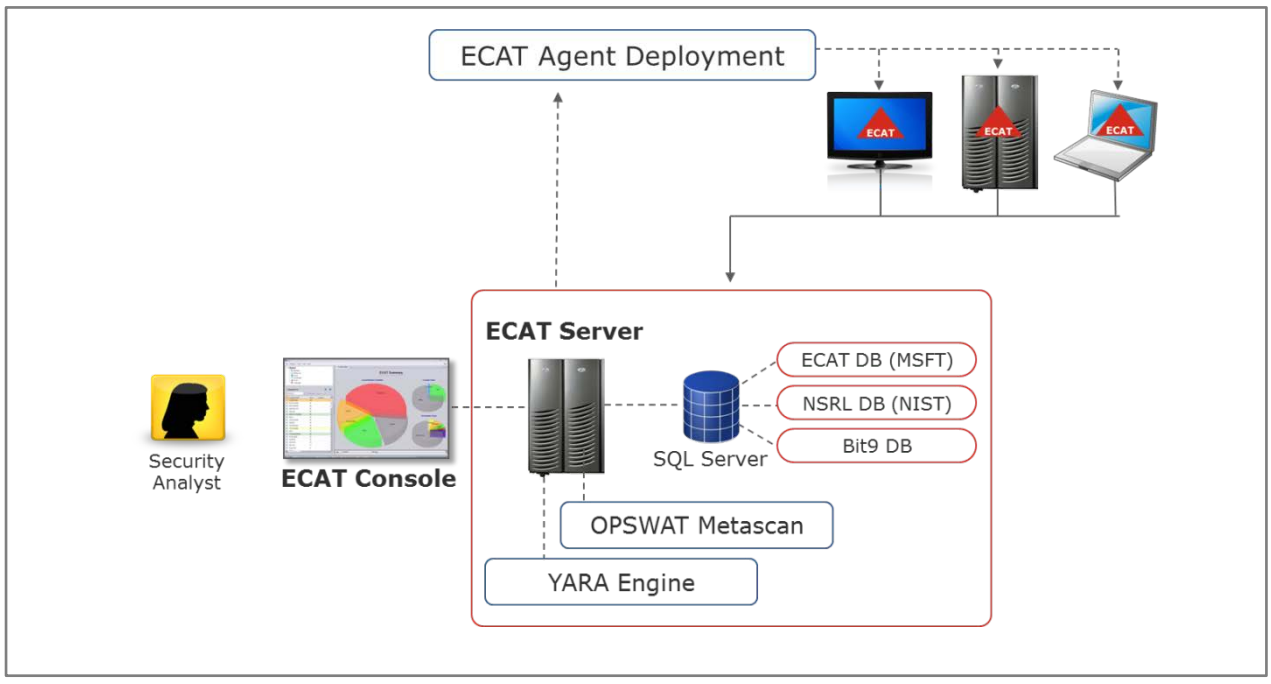

Fig.3: Architecture Diagram

Collecting Data

Either automatically or manually, the RSA ECAT agents can be instructed to perform a scan of the system's memory. A typical memory scan takes between 4 to 10 minutes to complete and can be done in parallel on all systems. It can be performed as a low priority task to avoid slowing the user applications and can be throttled to generate very little activity.

This scan focuses on identifying the code currently running in memory and all the programs that are configured to run automatically at startup like services and autoruns. EXEs, DLLs and drivers are all identified and reported to the server.

Integrity Check- Finding Code Injection

Most malware rely on a decade-old technique, called code injection, to hide their presence on a system and bypass the installed security products. Instead of creating their own process and risk detection, malware will inject code within trusted applications like Internet browsers or Windows services using various techniques, often evading completely antivirus systems.

In order to detect this, all running applications are validated by comparing their memory image to the original disk image. This technique identifies programs that have been modified in memory and locates blocks of injected code.

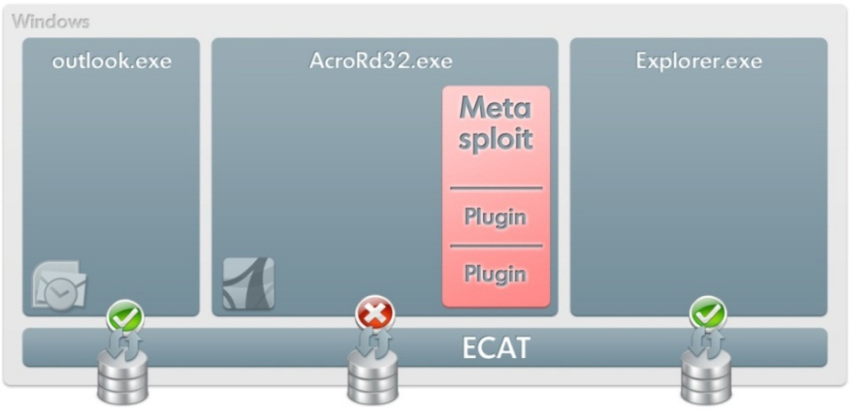

Fig.4: Code Injection into Acrobat Reader using Metasploit

FINDING ANOMALIES

Aside from injecting code into applications, malware often modifies internal operating system structures in order to hide its activity without the user or installed security products noticing. By validating important internal kernel and application structures, anomalies can be identified that are typically generated by malware like hooking, kernel object modification, file/process/registry/communication hiding, and more.

Managing Suspect Files

An effective detection system must allow the analyst to quickly validate if a suspect file is indeed malware or if it is a trusted file exposing abnormal behavior for a legitimate purpose. For example, security or DRM software can use techniques that are similar to those used by malware. To make a clear decision, the analyst should have as much intelligent data as possible about the suspicious module. RSA ECAT delivers this in a variety of ways:

- **Static signature analysis:** RSA ECAT integrates with antivirus multi-scanners, such as OPSWAT™ Metascan®. Verifying a file against eight or more antivirus signature databases and their heuristics engines provides a fast path to identifying 'known bad' files.
- **Digital certificate validation:** Code signature validation of the "digital stamp" on files published by legitimate software vendors.
- **Known good hash lookup:** The counterpart to verifying a file against AV signatures is verifying it against databases of known good files by hash match. For example, RSA ECAT verifies a given file by doing a hash match against several whitelists like NIST NSRL, Silicium's own hash set that includes the full Microsoft file list from MSDN, and the Bit9 GSR.
- **Environment correlation:** Know where the file is installed and on how many systems in the scanned environment. Once a

file has been deemed good or bad, it is flagged as such. In the case of good files, it will be automatically filtered from the alerting system.

Behavior and Suspect Level

With all the information available, performing an analysis of the data from the endpoint gives a grade of the level of suspicion, or compromise of the machine. RSA ECAT can flag the files that are the most suspect by attributing a "Machine Suspect Level" (MSL), a numeric indicator used to triage the potentially infected systems and prioritize the analysis process.

Monitoring and Maintaining the Health of the Network

Once the initial assessment process is completed and the infected machines are cleaned, scheduled scanning should be automatically performed to alert when systems reach predetermined threshold suspect levels. RSA ECAT has a built-in scheduler for this purpose.

KEY FEATURES OF RSA ECAT

RSA ECAT Agent

- Custom low-level access parsers for disk, memory access and registry access
- Code integrity check finds malware hiding in trusted applications, such as Internet Explorer
- Internal structures and code validation (SSDT, IAT/EAT, IDT, inline hooks, etc.)
- Remote memory dumps compatible with Volatility memory forensics framework
- Abnormal communication pattern recognition
- Active tracing for network connections, module loading, file access and registry access
- MFT Viewer: Locate and remotely download hacked and deleted files in a forensically sound manner
- Optional integrated remediation agent

RSA ECAT Server

- Integration with OPSWAT™ Metascan® using 4+ antivirus engines
- Ability to import YARA rules for known-threat identification
- External code-signing validation. The certificates are validated at the server level to avoid being fooled at the workstation level
- Complete enterprise environment correlation to quickly find all instances of malware among thousands of machines
- File and memory whitelisting system
- Built-in monitoring and alerting system
- NIST, NSRL and Bit9 SRS whitelist integration

CONCLUSION

Malware authors today rely on multiple techniques and technologies to evade detection. By the same token, the core of any effective security strategy is layered defense in depth utilizing multiple approaches. Traditional signature-based approaches, like most AV products on the market, fall short on blocking or detecting the most recent, advanced threats. Comprehensive detection and remediation of advanced threats requires tools like RSA ECAT, which combines the technologies and techniques described above to help protect your organization against the latest threats.