

Modeling a New Threat: Embedded Malware

EXECUTIVE SUMMARY

Corporations spend millions of dollars each year on computing hardware and software to keep their organizations running smoothly. A portion of these purchases, however, are contaminated with malicious computer code designed to alter the functionality of the application, reveal the actions of the user, or exfiltrate proprietary data. Hidden, embedded malware lurks in hardware, software, and even peripheral devices around the world, quietly stealing organizations' prized intellectual assets.

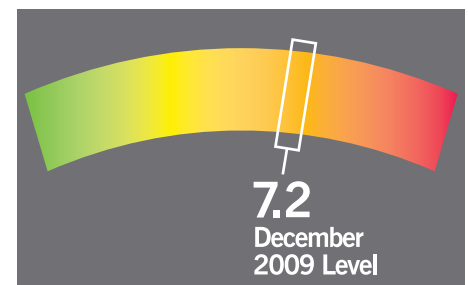
What's being compromised, and even outright stolen?

- Intellectual property
- Competitive information
- New product development data
- M&A plans
- Financial information
- Trade secrets
- Even national security secrets

Given our universal reliance on the computer as an essential business tool, it is critical to provide better tools for proactive risk mitigation in the procurement and deployment of computer hardware and software. Most enterprises struggle with the tradeoffs between cost and the need to protect computing resources and intellectual assets from compromise. This paper reveals the prevalence and nefarious nature of embedded malware risk as well as a revolutionary new approach to protect organizations from this insidious threat.

**Hidden, embedded
malware lurks in
hardware, software, and
even peripheral devices
around the world...**

THE CISCO GLOBAL ARMS RACE INDEX



According to the Cisco Global ARMS Race Index persistent enterprise infections are common worldwide.

Today there are a growing number of opportunities for malicious hardware to be introduced along the supply chain. Malicious hardware has been identified in multiple technology products by both manufacturers and end-users. Advanced analytics now enable organizations to accurately assess the relative threat of embedded malware to computer hardware (including embedded firmware), software, and peripheral devices. This rank-ordering of risk enables organizations to lower malware risk across enterprise systems by delivering actionable information to drive better specification, procurement, and deployment practices. The result is lower malware vulnerability across the enterprise and better cost containment directly improving the bottom line.

HOW MUCH DOES MALWARE COST COMPANIES?

According to Ponemon Institute, the average organizational cost of a data breach reached \$6.75 million in 2009. Ponemon also reported that the most expensive data breach event in their 2009 study cost one organization nearly \$31 million to resolve.

INFORMATION ASSURANCE AND CYBER-SECURITY A CORPORATE REALITY FOR DEFENDING THE BALANCE SHEET

Less than a decade ago, most people thought of cyber-warfare as a matter for science fiction novels. Yet today, it is a water cooler topic, covered regularly in the mainstream media. The threat is real and both enterprises and consumers are grossly under-protected. Embedded malware is one threat to information assurance and cyber-security that is particularly challenging to identify and control.

WHAT INDUSTRIES ARE AT THE HIGHEST RISK?

According to SafeScan's "Annual Global Threat Report 2009," critical infrastructure organizations including:

- Energy companies
- Oil companies
- Chemical companies
- Mining companies
- Pharmaceutical companies

Source: SafeScan's "Annual Global Threat Report 2009"

There are many motivations for the creation of malware: military advantage, terrorism, activism, financial gain, blackmail and extortion, political or economic espionage, competitive advantage, vandalism, and mischief. Today malware is used primarily to invade systems for financial gain, but that is just the tip of the iceberg in terms of the threat to corporations.

Intellectual property, technology, and information-rich enterprises are under attack. Knowledge arbitrage is a real threat that directly impacts a company's balance sheet. And the perpetrators of embedded malware have developed incredibly sophisticated attacks that are specifically tailored to effectively capture and exfiltrate only the most valuable data including geological surveys, drug discovery formulae, prospectuses, financial reports, and even shipping routes and manifests.

Once malware establishes a foothold in a target system, the attackers can launch network enumeration tools to retrieve additional user names, network shares, and available services of networked computers. These tools allow the perpetrator to discover additional targets within the enterprise and retrieve the required system information to further perpetrate the target's network.

Increased rate of exposure to data theft Trojans

Energy and Oil	356%
Pharmaceutical & Chemical	322%
Government	252%
Banking Finance	204%

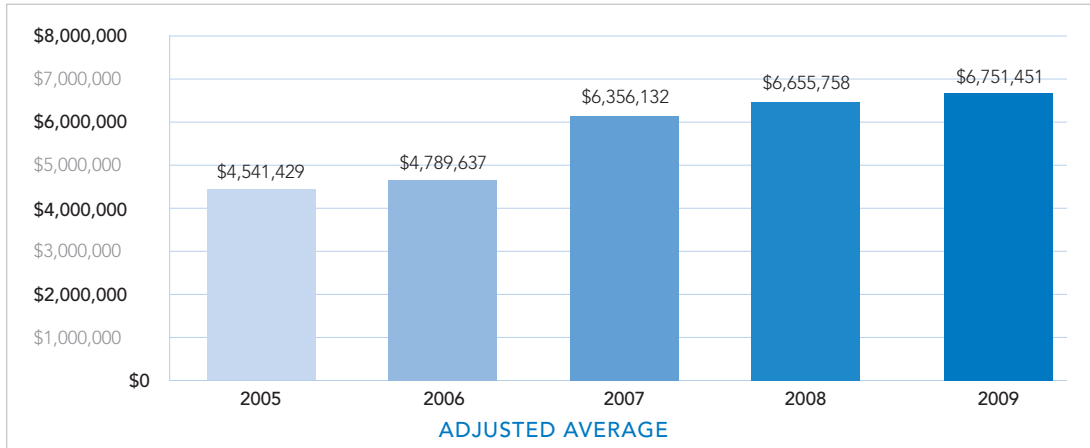
Source: SafeScan's "Annual Global Threat Report 2009"

As shocking as the prevalence and acceleration of attacks, is the amount of time that criminals have access to compromised systems where they are actively monitoring activity and exfiltrating data. **According to CSO Online, the average time cyber-criminals were able to access the target systems and data was 156 days¹.** Imagine what an attacker can learn about your company monitoring activity and exfiltrating files over a five-month period.

CYBER-CRIMINALS ACCESS THE TARGET SYSTEMS AND DATA FOR 156 DAYS

Every day businesses are under attack and most don't even know it. Regardless of the motivation, these attacks are enormously costly to organizations. There are the hard costs of financial losses, productivity downtime, customer impact, and damage control, but losing intellectual property or trade secrets can cause irreparable damage.

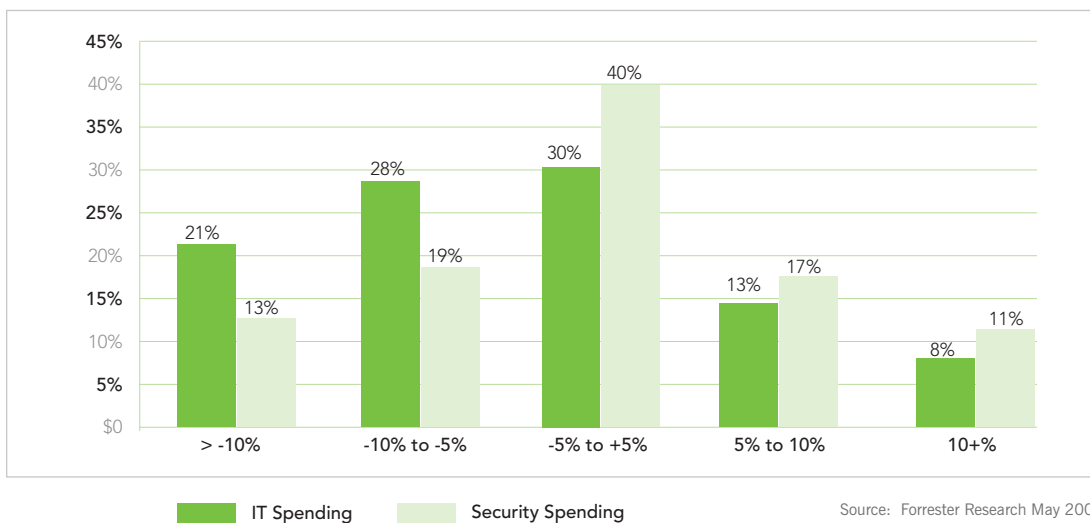
THE COST OF DATA BREACH EVENTS CONTINUES TO ESCALATE



Source: Ponemon Institute

Enterprise security personnel are actively developing Information Assurance and Cyber-Security programs, and purchasing technology and services, to fight to keep assets secure, but until now, combating this treacherous embedded malware has been tedious in the extreme or outright infeasible. Unlike a virus, malware buried inside firmware often goes unchecked, or appears to be legitimate code. Detecting this hidden malware requires rigorous testing of each component, a costly and time-consuming process, particularly in large organizations with many hundreds or thousands of hardware and system configurations.

SECURITY SPEND CONTINUES TO RISE AND TAKE A GROWING SHARE OF OVERALL IT SPEND



Source: Forrester Research May 2009

May						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

June						
S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

July						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

August						
S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

September						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

October						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

¹http://www.csoonline.com/article/570813/Data_Exfiltration_How_Data_Gets_Out

A NEW APPROACH TO EMBEDDED MALWARE RISK MITIGATION

Malware is everywhere. Attacks continue to accelerate both in pace and in sophistication. Most, if not all, organizations lie exposed. What can organizations do to protect their prized organizational assets?

Most of today's solutions have a focus on detecting attempts to infiltrate a network system from the outside, for example using Misuse Detection Systems (IDS/IPS), which focus on known attack signatures or using Anomaly Detection Models to evaluate and assess the risk of network activity based on normal patterns of network behavior. There is certainly a place for these solutions in an organization's Information Assurance arsenal. However, these solutions are largely incapable of addressing malware originating from the supply chain.

Some organizations perform component-by-component inspections, but this is an extremely expensive and non-scalable practice. Today's corporations need effective ways to improve malware threat assessment and management. Organizations are adopting malware risk assessment analytic models to more effectively manage these risks.

Analytic models are used to determine the baseline risk of embedded malware in a given system, and to assess potential acquisition options during the procurement process.

These risk assessments help organizations make the best decisions about procuring new hardware, software, and peripherals to reduce the risk of embedded malware, and also help set strategy for component replacements. Companies don't have to get rid of components that are higher risk. They can reallocate these assets to parts of the company that do not access mission-critical, highly sensitive data. This helps optimize the trade-offs between security and budget.

Malware threat assessment models measure hardware and software malware risk providing companies a better understanding of the risk of their system overall, and the risk of each individual component making up the system. Knowing the risk of embedded malware enables the organization to make the most informed decisions about hardware and software purchases, replacement or repurposing, and risk mitigation.

A multi-factorial sourcing threat assessment model is used to analyze hardware and software at the subcomponent level and translates the incidental risk into an overall likelihood of malware presence for each sourced product and for the organization as a whole.

Having access to an objective evaluation of malware risk in hardware and software components, as well as peripherals, strengthens the overall organizational security and enables the organization to more effectively manage information security investment trade-offs. For example, the risk assessment can be used as criteria in purchasing decisions, and alternative components can be identified that reduce the malware risk of the system, as seen in the figure at the right.

Using a malware threat assessment model delivers a meaningful baseline of an organization's current state, and also provides the means for prioritizing and mitigating risks efficiently and cost-effectively. The malware threat assessment model can be supported by information assurance services to provide the detailed information required for an organization to take control of embedded malware risk and reduce it to an acceptable level.

Analytic models effectively rank-order embedded malware threat across enterprise systems enabling investment trade-off decisions to reduce risk ►



KUITY'S FIVE-STEP PROCESS TO REDUCE EMBEDDED MALWARE RISK

1. Baseline the current infrastructure using a Malware Threat Assessment Model to understand how strong an organization's information assurance program is today. Identify risks that can expose the enterprise to critical data theft and loss.
2. Manage and reduce the overall threat risk by identifying the preferred state and building an adoption path. This includes prioritizing the phase-out or replacement of high-risk hardware and software candidates, based on cost-benefit assessment.
3. Model and visualize the impact of potential information assurance strategies. Understand the cost-benefit trade-offs and the impacts of existing policies and potential policy modification decisions in a simulation environment.
4. Mitigate threats in the procurement process to develop optimal sourcing and understand the ROI of making changes to sourcing criteria.
5. Evaluate and quantify the organization's dollars at risk, in terms of intellectual property exposure to determine the optimal budget.



Improving embedded malware risk and management by following best practices from establishing baseline metrics through determining an optimized budget.

Using the right tools and structuring information assurance activities around a logical workflow, enterprises and security personnel finally have a rational way to protect themselves from the risks posed by the hidden malware arriving at their gates each day.

Protect your organization's most valuable assets by taking a holistic approach to defending your information and your information systems. KUIITY is pleased to offer information assurance solutions and services to help our clients assess and reduce malware-derived enterprise risk. KUIITY's information assurance solutions and services enable organizations to actively understand risk reduction elasticity by component and establish a best-case state, given the enterprise's business and functional requirements, and a path to get you there.

KUIITY's SotariA™ has reduced the risk of costly embedded hardware and software malware by up to 45%. KUIITY arms organizations with all of the tools and services needed in the information assurance arsenal to assess and reduce this insidious threat that steals organizations' prized intellectual assets. SotariA is a dynamic solution, providing ongoing threat assessment and mitigation guidance. With SotariA, executives gain both the metrics and the oversight of the process to confidently and consistently make better specification, procurement, and deployment decisions for hardware, software, and peripheral devices.

KUITY MALWARE RISK REDUCTION CASE EXAMPLE

KUITY recently completed an embedded malware assessment for a Fortune 500 technology company. KUITY identified a **45% risk reduction** opportunity, and using the component and system-level risk reduction elasticity data identified, KUITY delivered a best-case path and schedule to significantly reduce embedded malware risk.

ABOUT KUITY CORP

KUITY is an advanced analytics company that provides operational risk management solutions and services. KUITY's analytic solutions, simulation tools, and services provide organizations with deeper visibility into the drivers of financial and operational results, identify and reduce risk and volatility, and predict future outcomes based on specific actions. KUITY delivers accurate, predictive insight to help clients make better-informed investment and risk management decisions and optimize performance.

Targeted KUITY solutions address specific needs in key application areas, including: financial analytics, total ownership cost, predictive performance management, sustainable resource planning, government and defense operations, and information assurance. With headquarters in San Diego, KUITY serves a diverse customer base of governmental agencies and Fortune 2000 companies that use our solutions to make informed, rational decisions that reduce risk and improve performance. For more information, please visit www.kuitycorp.com.

PART OF A DEFENSE-IN-DEPTH STRATEGY

Defense-in-Depth is an information assurance and cyber-security strategy in which multiple layers of defense are placed throughout an information technology system to address all facets of security vulnerability from personnel to technology and operations policy and practices for the duration of a system's life cycle.

A defense-in-depth approach defends a system against any particular attack using several varying methods as a layering tactic to provide a comprehensive approach to information security.

The placement of multiple protection mechanisms, procedures, and policies is intended to increase the dependability of an IT system where multiple layers of defense prevent espionage and direct attacks against critical systems.

