VERDASYS
ENTERPRISE INFORMATION PROTECTION

APT and Cyber Attack Defense

SOLUTIONS DATASHEET

THE CYBER THREATS TO CORPORATE DATA

The rate and sophistication of malicious software ("malware") attacks continue to outpace the ability for large institutions to protect themselves from a compromising event. According to the latest figures from leading antivirus software vendors, well over 50 MILLION individual pieces of malicious code are projected to be found in 2011. Worse yet, independent research has shown the most effective antivirus software detects no better than 38%* of new, non-targeted malware initially released "in the wild."

Today's most dangerous cyber threats to businesses are those designed to target and steal their sensitive data, and are completely invisible to traditional network security technologies (i.e. "zero day" attack). Of these zero day threats, a growing number are created by world-class programmers (often funded by nation-states) who combine stealth, precision, and social engineering to remotely breach a specific company's network, "exfiltrate" targeted data, and then erase all evidence of their existence.

ADVANCED PERSISTENT THREATS (APT)

These targeted cyber attacks are collectively known as Advanced Persistent Threats (APT), a class of online threats designed to carry out stealth missions on specific corporate and classified networks. APT's are highly-sophisticated attacks which exploit user trust and system vulnerabilities to defeat the weakest links of IT security and complete a mission undetected. APT missions range from stealing data to compromising public infrastructure. Confirmed APT breaches have run the gambit of organizations with highly competitive and proprietary information, including: manufacturing; high tech; oil & gas; financial; pharmaceutical; critical infrastructure and public utilities; and, of course, military & government networks.

DETECTING, ISOLATING, AND PREVENTING APT

The most effective security model against APT's is a layered and unified approach that creates security "air gaps". The purpose of air gaps is to isolate a threat wherever it is first detected (i.e. network, workstation, or server) and prevent it from spreading by challenging its adaptability and stealth in ways it was not designed to circumvent. This type of APT defense requires enterprise-wide coordination between multiple layers of data security technologies across all possible network and system entry and exit points.

DIGITAL GUARDIAN APT DEFENSE-IN-DEPTH

Digital Guardian is a data-centric technology platform for Enterprise Information Protection (EIP) that integrates endpoint and network agents into a coordinated and multi-layered sentry to detect and stop one-off APT malware designed to steal a company's sensitive data. Digital Guardian delivers a comprehensive APT defense-in-depth security model that detects threatening events on workstations, servers, and the network simultaneously, providing an enterprise-wide overview of an attack that can be monitored and mitigated by a common management interface. When an APT event is confirmed, Digital Guardian endpoint and network agents work together to enforce complete access and control policies autonomously at the user, application, machine, file, or network session levels to prevent it from successfully exfiltrating data.

DIGITAL GUARDIAN ENDPOINT APT DEFENSE

Digital Guardian uses several policy-based methods to detect and stop a potential cyber attack, even if the APT code or methodology has not been previously seen. As workstations are often the most vulnerable entry points for APT, Digital Guardian endpoint agents use a powerful combination of root-level activity monitoring and usage controls to help to thwart APT at first contact. These capabilities include protecting users from social engineering tactics often used by APT to breach a network, such as blocking executables launched from infected websites, email attachments, or USB sticks; advanced memory scanning and forensics to detect suspicious obfuscated activities at the system memory and kernel levels; identity-based file encryption to prevent unauthorized access to sensitive files; and application monitoring, alerting and blocking to identify and block the launch of dangerous executables.

DIGITAL GUARDIAN NETWORK APT DEFENSE

Digital Guardian network agents complement endpoint agents with deep session analysis of incoming and outgoing traffic to detect suspicious activities. As APT attacks often hide malicious payloads within network traffic to bypass perimeter defenses, Digital Guardian network agents can deconstruct the entire network session at "line speed" across all ports and protocols to detect and block coordinated events like connections to suspicious IP addresses by unknown applications using secure messaging or port-hopping. By analyzing the entire session in context, Digital Guardian network agents go beyond traditional packet inspection that cannot detect payloads with embedded content (e.g. JavaScript within a PDF file) which could be used as an APT attack vector.

THE APT RISK IS REAL — MANAGE IT

APT's are the most dangerous types of online threats because they are built for a single mission against a particular target, and are undetectable by typical IT security technologies. Verdasys offers a scalable cyber defense solution that prevents the compromise of sensitive data by APT's using a layered, integrated, and tamper-resistant counter technology that combines root-level threat analysis and control on endpoint, server, and network layers simultaneously. Digital Guardian offers the only data-centric APT security that manages the risk of targeted malware by anticipating the tactical imperatives it requires to source and compromise sensitive data within a network, and enforcing user-based controls to sensitive information when access rights have been counterfeited.

*Malware Detection Rates for Leading AV Solutions:
A Cyveillance Analysis", Cyveillance.com, August 2010,
http://www.cyveillance.com/web/docs/WP_MalwareDetectionRates.pdf

WHAT ARE ADVANCED PERSISTENT THREATS?

APT attacks are designed to complete a specific mission

- Custom-made malware exploits technical vulnerabilities and/or user trust (social engineering) to compromise a machine and penetrate a targeted network
- APT code is usually undetectable by AV and IPS vendors as it is too specific to have been seen "in the wild"
- APT can be used to steal information, or to take control of a system for malicious purposes

APT can compromise machines via multiple vectors

- Infected website; O/S or application vulnerability, infected USB, targeted social engineering (i.e. "spear phishing"), DNS poisoning, etc.

APT are designed to gain privileged access to data

- Allows an "outsider" to become a privileged insider
- Creates a ***stealth*** and persistent threat with the ability to evolve, obfuscate, and communicate securely with an external "master"

A single APT attack can include multiple payloads and "objectives" to complete a mission:

- Launches sustained and evolving stealth operations from inside the network until the mission is accomplished
- An APT mission may last a day…or years
- APT code is often designed to obfuscate and erase all traces of itself to hamper post-incident investigations

MULTI-LAYERED APT DETECTION AND CONTROL CAPABILITIES

With only a single infected machine APT code can spread and embed itself quickly across the network unnoticed, quietly infecting other systems until it can complete its mission. However, in order for APT to steal data undetected it must take several predictable steps on which Digital Guardian agents and policies can be focused:

Stage 1: Initial breach

Custom malware designed for a targeted corporate or government network uses deception, system vulnerabilities, or infected media to gain administrative control of a machine and launch its mission to steal sensitive data (e.g. intellectual property).

How Digital Guardian helps:

- Digital Guardian endpoint agents forensically scan system memory to discover suspicious code undetectable by traditional antivirus software, and trigger an alert
- Digital Guardian endpoint agents can block unknown executables
- Digital Guardian network agents alert or block suspicious inbound network traffic

Stage 2: Establish command & control

If the initial breach occurs, an APT attack is typically designed to spread out across the network to compromise more secure systems; establish a secure command/control infrastructure; and potentially begin communicating with an external source.

How Digital Guardian helps:

- Digital Guardian endpoint or network agents detect suspicious or unauthorized connections to other machines or external web addresses
- Digital Guardian endpoint agents detect suspicious code execution in system memory
- Digital Guardian can take preventive actions such as blocking suspicious executables or quarantining a machine with an elevated risk profile based on system, memory, or network activity

Stage 3: Compromise target systems

Once targeted systems are identified, APT's use privileged access credentials to compromise sensitive data stored on them.

How Digital Guardian helps:

- Digital Guardian network agents can block suspicious traffic to restricted resources (e.g. data center)
- Digital Guardian server agents can block access to sensitive data by user or machine identity
- Digital Guardian servers agents can block unknown executables, OR prevent an unauthorized administrator account from accessing files (e.g. identity-based file encryption)

Stage 4: Exfiltrate data

Once sensitive data is breached, APT code attempts to securely upload it over time to an external destination without being detected.

How Digital Guardian helps:

- Digital Guardian network agents can detect and block unauthorized encrypted traffic
- Digital Guardian can apply identity-based file encryption accessible only by authorized users
- Digital Guardian endpoint agents can apply restrictions to network transfer uploads for all users regardless of privilege
- Digital Guardian network agents use continuously updated intelligence feeds to detect and automatically block connections to malicious web addresses

VERDASYS

Corporate Headquarters
404 Wyman Street
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

www.verdasys.com

ABOUT VERDASYS

Founded in 2003, Verdasys provides insider threat solutions that are the cornerstone of our customer's global data security strategy. With over a million security agents deployed at over 200 of the world's leading organizations and Federal agencies, our solutions and services provide a strategic and comprehensive approach to information risk management.