VENCORELABS

Zero-Day Cyber Defense Solutions

A WHITE PAPER ON VENCORE'S PROPRIETARY Z-DAY™ ENTERPRISE SECURITY SYSTEM

White paper

ABSTRACT

Z-Day Enterprise Security System (Z-Day™ ESS) from Vencore Labs (formerly Applied Communication Sciences), the transformational applied research organization of Vencore, Inc., defeats the most serious of malware-based IT attacks that foil existing security solutions. Z-Day comprehensively monitors the enterprise environment and provides the capability of detecting and responding to zero-day attacks at the time of occurrence – in real-time, not days or weeks after the fact. The novel integration of application-, host-, and enterprise-level monitoring across a spectrum of thematic, behavioral, and social activities enables extremely effective malware detection with a false positive rate of less than one per day for the enterprise. This broad and deep insight provides detailed attack sequencing and behavior information previously unavailable to security analysts in a timely and focused manner. An embedded inoculation capability permits Z-Day to improve its resilience and response time to persistent and repetitive attacks, often before an attacker strikes again, and can distribute these inoculants to other federated Z-Day systems. Z-Day is the result of 8+ years of U.S. Government sponsored research, development, and validation testing. The system has been independently tested and shown to defeat nation-state quality zero-day attacks and to limit maximal enterprise infection to less than one percent and to recover infected systems within six minutes.

DISCLAIMER

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Air Force Research Laboratory – Rome, NY, the U.S. Air Force, the Defense Advanced Research Projects Agency or the U.S. Government.

INTRODUCTION

Critical national infrastructure, financial, and Government systems are some of the most sought after networked computing targets of malicious adversaries worldwide. While much effort has been expended towards securing theses systems from intrusion and attack it has clearly been insufficient in thwarting many recent penetrations and outbreaks. The loss of data and operational capability to such systems can be devastating to the productivity and defense of the country. Zero-day attacks – those in which the attacker's methods and techniques are unknown before they are unleashed – are some of the most difficult attacks to defend against. Mass effect attacks – those attacks involving numerous systems, perhaps tens of thousands – can be the most crippling and damaging as the impact is far-reaching and extensive. Recovery to regain full operational stature may take weeks and establishment of appropriate defenses to prevent further such attacks can take days. The resulting loss of capability, period of weakness, and costs incurred should be considered unacceptable. Therefore, deploying an effective capability to quickly detect, identify and remediate zero-day, massive, and/or persistent attacks is imperative. Additional capabilities to alter the enterprise defensive posture at the speed of the attack, to acquire real-time insight into unusual application, host and enterprise activities, and the ability to provide automated assistance for attack analysis and system recovery would be considered by many a consummate achievement. The recently declassified Z-Day technology created by Vencore Labs is now available to fulfill these critical and important needs.

A vast majority of current and previous security solutions take an admittance (a onetime validation) approach towards malware detection. Virus checking, e-mail sandboxing, removable disk scanning, and qualification by certificates are some of the many security approaches that exhibit the essential property that, once scrutinized, subsequent conduct is not considered. This is exemplified by the network firewall where once a packet is approved for forwarding it is no longer considered. This has led managers and operators to employ an ever increasing obstacle-style security environment: rootkit detectors, virus scanners, network gateways, personal firewalls, restrictive web browsing, and so forth. While useful, this prophylactic approach does little to address malware sophisticated enough to bypass these barriers. A novel attack that is effectively invisible at time of scrutiny can therefore slip past undetected

and generally obtain free reign. Such sophistication is implied by attacks considered to be zero-day and/or nation-state quality. The potential for loss in revenue to corporate organizations from these attack is huge, but more importantly, such attacks can render medical, governmental, educational and civil computing systems useless – creating a very dangerous and potentially irreversible national and international threat. Current security technologies perform admirably against a constant onslaught, yet it is the admittance approach that reinforces the perspective that security is an arms race. Zero-day attacks epitomize the threat that cannot be met in advance and invites new approaches to malware detection and remediation.

Vencore Labs, under the sponsorship of DARPA's DQW (Dynamic Quarantine of Worms) program has been addressing many of these issues and is now poised to offer to interested parties the results as the Z-Day software system. Z-Day is specifically designed to detect and defend against large-scale zero-day attacks and other high-quality and pervasive computer exploitations such as botnets and advanced persistent threats. Notable achievements include limiting the impact of zero-day attacks to less than 1% of computers in a protected enterprise, recovery of infected systems within minutes, and automatic generation and deployment of inoculants to defend against subsequent such attacks in seconds. These and other important benefits are provided while generating less than one-false positive per day.

APPROACH

The Z-Day solution provides a fused hybrid detection approach, combining signature, anomaly, and specification-based algorithms operating collaboratively to provide multiple perspectives on potential malware behavior. It extends the capabilities of current intrusion detection and reaction solutions by providing a cooperative distributed sensor, detector, arbitrator, and responder (SDAR) system utilizing novel techniques and significantly improving on existing approaches. The Z-Day techniques often complement one another to strengthen the overall approach. As one example, Z-Day monitors network communication both at the host and at the network gateway. Host monitoring can take into account the application involved in the communication, while gateway monitoring does not have application context but does have the context of multiple hosts.

The Z-Day Enterprise Security System operates both within end systems (clients and servers) and at points of network ingress/egress. Four primary characteristics of an enterprise are monitored – processes, resources, content, and communications – to portray the what (thematic information), how (behavioral information), and who (social information) of any activity. These characteristics are evaluated from three different perspectives – host, network, and enterprise (Figure 1). A coordination subsystem provides the ability to correlate attacks and responses across the protected environment. Inoculants (if produced) will be generated automatically within seconds of an initial attack and will not only prevent re-infections but will also limit further spread of those attacks that continue for more than a few seconds after the initial outbreak. Inoculants alter the behavior of Z-Day, not the end systems themselves.

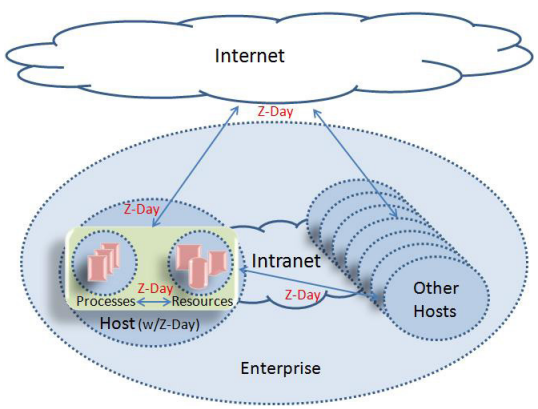

Figure 1 Z-Day Monitoring Points

The Z-Day system is problem-centered – identifying malicious activities by fusing evidential behaviors, misbehaviors and/or policy violations. Overall, it provides an effective coordinated attack discovery and mitigation capability for the enterprise, with the ability to provide a greater degree of insight into attack behaviors and identification of damaged systems, applications, and data.

The Z-Day system provides computing enterprises an attentive and continuously watchful presence that begins with the presumption an attack will

happen despite best efforts at defensive measures. Employing an innovative, comprehensive, and dispersed collection of security mechanisms, Z-Day considers the weight and presence of evidence across multiple dimensions (behavioral, compositional, and communal – analogous to the activities undertaken, how they were performed, and who was involved) against specified policies and models to identify malicious activity. Once identified, the richness of evidence informs the remediation process necessary to quarantine the attack and to inoculate against future attacks of this nature.

FEATURES

As a **zero-day attack detection system**, Z-Day augments rather than replaces existing admittance-oriented security tools (e.g., anti-virus, firewall). The focus is on detecting attacks, not just upon preventing attacks, since by definition a zero-day attack cannot be prevented. Z-Day is known to prevent many attacks, but it excels at recognizing, limiting, and stopping truly novel attacks – those that have never been experienced before. Z-Day constantly monitors the actual operational systems and the environments they exist within to detect zero-day attacks regardless of exploitation approach. This is in contrast to sandboxing and other approaches for zero-day detection that only protect the operational system at the time the data and/or processes are being examined. Z-Day distinguishes itself by providing broad and comprehensive detection to the entire enterprise. Further, as a zero day defensive system, Z-Day is agnostic towards metamorphic, polymorphic, encoded, and self-defending attacks.

A key technology objective is to provide **significant reduction to the time and resources involved in dealing with an attack**. The upper graph in Figure 2 provides an overview of the infection cycle experienced today by most organizations. Even with a rapid response time (shown here to be 6 hours) to a mass attack, significant numbers of enterprise resources can be impacted and weeks of time and resources expended to return the enterprise to pre-infection operation. Z-Day is specifically designed to minimize the impact from a mass attack to less than one percent of all protected systems, and to recover those systems infected within six minutes.

This can result in substantial operational and mission continuity related savings – several orders of magnitude in both time and resources for attack response and recovery.

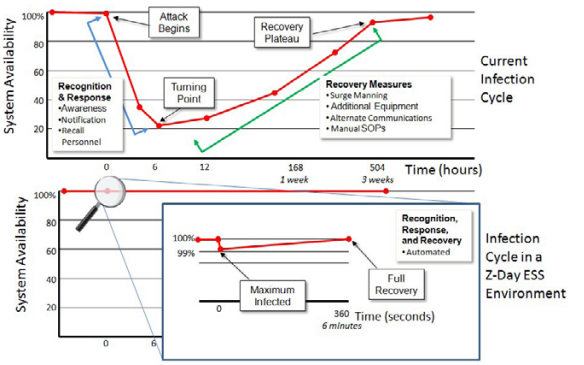

Figure 2 The impact on the enterprise infection cycle from deploying Z-Day

Z-Day c**ontinuously and collaboratively monitors** the processes, resources, and communications of the enterprise for potentially malicious activities. It detects potentially malicious actions at all possible stages of an attack: targeting, delivery, activation, exploitation, and operation. Z-Day first determines if a monitored activity is notable, and subsequently evaluates accumulated evidence to determine if there is a sufficient basis for declaring an attack. Three perspectives – host, network, and enclave – provide differing contextual basis for this evaluation. All such noted activity, even that not considered by Z-Day to warrant the declaration of an attack situation, is available in near real-time to drive activity displays and as a data set to augment long-term and forensic analysis. This enables the deployment of a continuous graphical view on the extent, type, and depth of potentially malicious activities within an enterprise. When an attack is found, Z-Day simultaneously provides the set of activities that have occurred that are related to the attack – providing immediate who, what, when, where, and how context to operational personnel. Z-Day also provides self-auditing in that all significant actions taken by the system, including software updating and policy alteration, are recorded.

Z-Day can **respond in real-time** to confine malicious actors in a manner delineated to minimize the impact to other applications and/or systems and acts to implement a rapid recovery. Automated

reaction of this nature is essential to respond to threats that propagate faster than a human's ability to react to an attack. Layers of actions may be put into place for variable amounts of time in response to an attack. Continuing attack activity can lead to additional actions and extension of existing time-limited constraints. Where such automation may be deemed inappropriate or unwise, recommended actions are presented to human operators to be verified before enacting. Automated responses of limited scope and/or duration enable the striking of a balance between rapid reaction to mitigate attack activities and the coercion of the attack process towards human time scales, thus minimizing potential for mission disruption.

Z-Day is a **highly configurable policy-driven security system**. Enterprise managers can define the types of activities that are considered notable, the degree to which these activities are tolerated, and the weight to be given in considering the activity truly malicious. They also define the type and duration of automated reactions to undertake, if any. For example, Z-Day can implement a policy where unknown applications are allowed to run on any host so long as they do not attempt to communicate over the network, and if they do the process is to be terminated and the machine quarantined from network communication. The major significance of policy as employed by Z-Day is it enables intimate alignment to enterprise specific guidelines, procedures, and objectives. Policies may be tailored on a host-by-host basis within the enterprise. Groupings of policies may also be pre-defined and named so that they may be recalled and put into action quickly, perhaps in response to changing threat postures. For example, in a high-threat situation, policies may be more restrictive to users than those generally enforced when the threat posture is less severe.

To minimize the impact of recurrent attack Z-Day is capable of **automated self-immunization** (aka "**inoculation**"). After detecting the presence of an attack, Z-Day performs a self-analysis against the characteristics of the attack to determine if a safe but effective improvement in system detection performance can be put into place. The goal of inoculation is to improve performance against future attacks of the same or similar nature. Inoculation does not occur if it appears to increase the potential for false positives. This inoculation action, when taken, occurs within seconds and rapidly improves the security defense and operational viability of the enterprise during propagating and/or persistent attacks. For example, attacks that propagate every few seconds (or days) will be completely denied moments after their initial discovery. Inoculants may be shared across federated enterprises.

To assist in **rapid recovery** of infected systems, Z-Day employs the ability to automatically rollback a system to a pre-infected state. Z-Day provides automated checkpoint of those files altered by processes on a host. When a compromise is detected, the host can be restored to its condition prior to the compromise. The detailed file alteration information in conjunction with the general malicious activity log provides a valuable forensic data contribution to aid in the analysis and/or removal of an infection. Z-Day also employs a standards-based interface for notifying other processes of those resources Z-Day identifies as potentially altered by malicious actors so that they may perform application specific recovery as necessary.

OPERATION

The Z-Day ESS is comprised of four distinct components: Master Coordinator, Enclave Coordinator, Network Protector, and Host Coordinator. The Master Repository provides managed storage for operational policies, configurations, software releases, logs, and event data. It also hosts the web service for management oversight. The Enclave Coordinator monitors the event streams of a collection of Network Protectors and Host Coordinators to provide malware detection from the perspective of group activity. A Network Protector provides monitoring and detection from the perspective of network flows and data traffic. It is typically located at network ingress/egress points. The Host Coordinator operates on a protected end system (e.g., desktop clients and servers) and coordinates the operation of the host embedded monitoring and detection capabilities.

A single enterprise typically deploys one Master Repository and several Enclave Coordinators and

Network Protectors. Z-Day software would be installed on all clients and servers in the enterprise to be protected and each would operate a Host Coordinator. Host Coordinators (e.g., clients and servers) and Network Protectors are logically assigned to an Enclave Coordinator to form a protected enclave. An enterprise may have any number of protected enclaves and any reachable system can be a member of an enclave (i.e., there are no network locality restrictions to enclave membership). Z-Day does not place a limit on the number of enclaves within an enterprise, and the size of an enclave is typically constrained only by the capabilities of the underlying hardware.

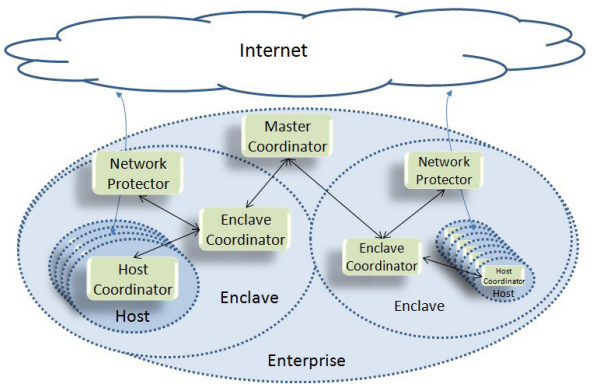

Figure 3 Z-Day distributed elements and coordination across an enterprise

The Master Repository, Enclave Coordinator, and Network Protector software all operate on standard hardware platforms (a Network Protector requires two network interfaces) provided by the enterprise. While all three components can operate on a single hardware platform, it is recommended that the Master Repository be operated independently of the other components.

TESTING AND VALIDATION

The Z-Day Enterprise Security System has undergone extensive in-house product testing and hardening equivalent to that undertaken by commercially available products. It has been demonstrated to coexist with other client security products such as anti-virus and rootkit detectors and operates on systems conforming to DISA's Security Technical Implementation Guide. It has shown itself to be stable in over one year of continuous use and robust in recovery from power failure and network instability. Z-Day has been validated for performance and effectiveness several times both internally and by multiple and independent Government sponsored test and attack teams. Evaluation against over sixty distinct zero-day attack cases and extensive testing against previously known malware types such as botnets, rootkits, worms, and advanced persistent threats reveals that Z-Day detected all attacks it has encountered and shows itself capable of meeting or exceeding its performance objectives of allowing no more than one percent of the enterprise to become infected while exhibiting a false positive rate of less than one per day.

DEPLOYMENT READINESS

A complete development cycle focused on enterprise deployment readiness provides many features generally absent from new and emerging technologies. This includes remote management via web browser, extensive policy-driven control over both permissible behavior standards and attack remediation actions, accommodation of enterprise life-cycles activities including network migration, deployment of new applications, and hardware upgrades, push-button ability to immediately invoke alternative enterprise-specific security postures, on-the-fly product upgrades, automated log management, and extensive auditing of all system and operator activities. Perhaps most importantly, Z-Day can be deployed incrementally and in a strict watch-only mode of operation. The watch-only mode allows Z-Day to monitor, detect and report attacks as it normally does but prevents any attack remediation action from taking place. Any number of roles and systems can be added as desired once the basic Master Repository and Enclave Coordinator roles (e.g., Z-Day server-based services) are established.

The Z-Day Enterprise Security System is available now to U.S Government organizations. Availability to state governmental and commercial entities is currently under consideration. It can be deployed as either a standalone application or as an integrated element of existing enterprise security management services. Z-Day is fully integrated with DoD's Host Based Security System (HBSS) and the McAfee ePolicy Orchestrator™ (ePO™) and can be easily integrated with other security management systems and consoles. Client installation can

occur directly via CD-ROM install or remotely via Microsoft Windows Server or HBSS remote install facilities. The system is immediately deployable on Windows XP and Server 2003 and can be directly ported to Windows 7/8/10. Z-Day is also available on Linux and Android platforms.directly via CD-ROM install or remotely via Microsoft Windows Server or HBSS remote install facilities. The system is immediately deployable on Windows XP and Server 2003 and can be directly ported to Windows 7 and/or Linux platforms.

SUMMARY

Vencore Labs has available the recently declassified Z-Day Enterprise Security System that defeats the most serious of malware-based IT attacks that thwart existing computer defense solutions. Z-Day provides comprehensive monitoring of the enterprise environment and is capable of detecting zero-day attacks at the time of occurrence – in real-time, not days or weeks after the fact. The novel integration of application, host, and enterprise level monitoring across a spectrum of thematic, behavioral, and social activities enables extremely effective detection capability with false positives of less than one per day. This broad and deep insight provides detailed attack sequencing and behavior information previously unavailable to security analysts in a timely and focused manner. An embedded inoculation capability permits Z-Day to improve its resilience and response time to persistent and repetitive attacks, often before an attacker strikes again, and can distribute these inoculants to other federated Z-Day systems. Z-Day is the result of 8+ years of U.S. Government sponsored research, development and validation testing. The system has been independently tested and shown to defeat nation-state quality zero-day attacks, to limit enterprise infection to less than one percent, and to recover infected systems within six minutes.

Z-Day was developed primarily under the Dynamic Quarantine of Computer-based Worm Attacks program, which was funded by the Defense Advanced Research Projects Agency, Strategic Technology Office (formerly Advanced Technology Office). Vencore Labs, d/b/a Applied Communuication Sciences, was the sole technical performer to continue beyond Phase II of this program and directed a team of many talented and dedicated individuals. The Z-Day solution for Linux and Android platforms was developed under several programs funded by U.S. Army CERDEC.

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official position or policies, either expressed or implied, of the Air Force Research Laboratory – Rome, NY, the U.S. Air Force, the Defense Advanced Research Projects Agency or the U.S. Government.

VENCORE LABS

150 MOUNT AIRY ROAD
BASKING RIDGE, NJ 07920
VENCORELABS.COM