



* white paper

A Holistic Approach to Security Intelligence:

VeriSign® iDefense® Threat Intelligence Services





Contents

+ The Increase in Technically Sophisticated, Targeted Attacks	3
+ Problem: Ad Hoc, In-House Intelligence Gathering	4
+ Solution: Understanding Threats in Context	5
+ VeriSign iDefense - Proactive Threat Detection, Analysis, and Mitigation	6
+ The VeriSign Difference: Infrastructure, Expertise, Intelligence, Trust	9
+ Summary	10
+ Learn More	10
+ About the iDefense Team	10
+ About VeriSign	10



A Holistic Approach to Security Intelligence: VeriSign® iDefense® Threat Intelligence Services

Today's network threats are more numerous and more damaging than ever. Sophisticated attacks can seriously compromise an organization – not only in terms of lost productivity, data breaches, and possible regulatory non-compliance penalties, but also lost trust and damaged reputation. Few organizations have the intelligence-gathering and threat-analysis capabilities to address network vulnerabilities and threats in their full context. Lack of comprehensive data can delay responses to true threats, impair threat prioritization, and incur costly and unnecessary emergency responses.

To manage risk effectively, organizations must use a holistic “threats-in-context” approach that allows proactive identification of real threats to critical business systems. VeriSign® iDefense® Threat Intelligence Services leverage an extensive intelligence-gathering network, proven methodology, and highly skilled professionals to deliver comprehensive, actionable intelligence that does not merely look at the “what” and “how” of network-based security threats and vulnerabilities, but also the “who” and “why.” Using this intelligence, organizations can gauge risk more accurately and respond rapidly and appropriately to protect business-critical data and systems.

This guide provides an overview of today's threat environment; discusses three critical components of a defense-in-context security intelligence strategy; and explains how VeriSign incorporates all three of these components into its services offering.

+ The Increase in Technically Sophisticated, Targeted Attacks

Hackers and the attacks they wage have changed significantly over the past few years. Hackers are developing malicious code more quickly, and they are becoming more technically sophisticated in circumventing network controls such as anti-virus software and firewalls. Their attacks are more targeted, affecting specific industries, organizations, groups, and people. And, whereas the chance for notoriety once motivated them, today's hackers often seek financial gain or revenge. According to VeriSign intelligence, espionage will likely prove one of the largest threats to networks this year, especially from insiders and direct competitors.

The VeriSign iDefense team identified 11,543 unique malicious codes in 2006, a significantly lower number than the more than 16,000 malicious codes discovered in 2005. This drop can be attributed to the decline in creation and distribution of malicious code for notoriety and the increase in more precise and engineered targeted attacks.

MeTAPHISHer : NoT Your Nor MAI BoT

Throughout 2006, VeriSign iDefense malicious code researchers tracked and infiltrated one of the most sophisticated botnets to date. This bot was called metaphisher. Metaphisher was seeded into the wild for several months where it stole credentials so criminals could exploit bank accounts, eBay accounts, and other similar targets for financial gain.

What made this bot different was its ability to defeat two-factor authentication and communicate encrypted over HTTP rather than traditional IRC ports. The redundant command and control centers and drop points for stolen data also added to the sophistication of this threat. Finally, the number of malicious actors working on the bot and the way they worked mirrored a professionally developed project with output that maximized profitability for the malicious group.

Metaphisher was just one of several emerging attacks involving multiple fraud rings that the iDefense team saw in 2006. Metaphisher successfully undermines SSL and the TAN system to steal thousands of accounts to leverage for other attacks, spam, and fraud.

+ Problem: Ad Hoc, In-House Intelligence Gathering

The goal in obtaining accurate and actionable intelligence is to identify and effectively mitigate risk for critical business systems. Many organizations believe that they have good intelligence-gathering capabilities if their in-house staff – as part of its other security duties – simply monitors threat and vulnerability information ad hoc, and then reacts to the threat at hand. But it is virtually impossible to gather high-level intelligence in house, and even if it were possible, vulnerability data alone is not enough to ensure an appropriate response to a perceived vulnerability. Organizations must also be able to verify and prioritize risk.

The Ad Hoc Collection of Vulnerability Data

In many organizations, intelligence gathering amounts to little more than monitoring free, publicly available vulnerability data (e.g., from Bugtraq, The Open-Source Vulnerability Database, and the SANS™ Internet Storm Center). These sources, while helpful, make up a small percentage of overall vulnerability information. In addition, none of these sources provides detailed analysis or workaround information, but merely high-level facts. Besides leaving gaps in data collection and omitting detailed vulnerability analysis, this ad hoc approach leaves out two key ingredients of comprehensive intelligence gathering—malicious code tracking and threat analysis. The absence of these critical components forces organizations to rely on incomplete data to make decisions. This poor decision-making capability can come at a high price, both in terms of risk management and misallocated resources.

Reliance on In-House Resources

Intelligence gathering is a complex discipline that relies not only on hard data, but also on skill, experience, trust, and an understanding of human behavior. It involves a number of highly specialized tasks: identifying and verifying original vulnerabilities; aggregating vulnerability data from numerous sources; discovering malicious code related to vulnerabilities; tracking hackers who may potentially exploit the vulnerabilities; and prioritizing risk and responding appropriately. To implement a comprehensive intelligence-gathering strategy, an organization would need a dedicated team of experts devoted 24/7 to each of these tasks.

Finally, an important key to mitigating risk is identifying new vulnerabilities as quickly as possible. This capability requires tapping into global intelligence networks for threat trends and patterns, and contracting with security researchers to discover vulnerabilities before the bad guys do. Most organizations do not have a track record with these researchers, which can pose problems for both parties. The organization may not have sufficient visibility or trust as an intelligence gatherer to attract qualified contributors. And, it may not have the processes or experience to identify unreliable contributions.

THE FINANCIAL IMPACT OF RELEVANT INFORMATION

"We see this all the time. You have a real vulnerability that could be taken advantage of to compromise critical business systems. But there's nobody out there—no known players—writing malicious code to take advantage of it. Now if you look at only the vulnerability, you would say 'Wow, I need to patch the system right away. Maybe I should go into emergency patching,' which can cost millions of dollars. But if you look at the whole picture—to see whether there are any known exploits, or hackers trading information on the vulnerability—and you don't find anything, you can determine that you don't need to patch right away."

*—VeriSign iDefense
Threat Analyst*

+ Solution: understanding Threats in Context

To protect critical business systems from legitimate threats and prioritize resources, organizations must be able to identify vulnerabilities as soon as possible, and then examine each threat in its full context. Having vulnerability data alone is not enough.

To understand the big picture, organizations must perform three levels of intelligence gathering:

- + Collecting and Analyzing Vulnerability Data
- + Tracking Malicious Code
- + Identifying, understanding, and Monitoring the Key Players

Strict processes must govern these activities, and human intelligence must be an integral part of effective analysis. When organizations base their threat assessment on data gleaned from all three of these activities, they can more accurately determine the severity of a threat and prioritize actions accordingly. This capability allows organizations to manage resources appropriately and address true threats more rapidly. Without this multi-level strategy, every threat must be treated as critical, placing an undue burden on personnel and setting off risk management processes that can be very costly.

Collecting and Analyzing Vulnerability Data

Effective intelligence gathering requires dedicated staff that can monitor nearly 3,000 data sources 24/7; normalize, aggregate, prioritize, and analyze the data to determine its severity; and finally, to store this data in a searchable database. It is a detailed, intensive process that is not easy to replicate. Besides collecting data from traditional sources, the solution must be able to identify new vulnerabilities as quickly as possible. One way to do this is to leverage worldwide infrastructures to gain visibility into threats. Another way is to pay security researchers to discover these vulnerabilities before anyone else does. Once identified, the intelligence team must verify these threats and develop patches and workarounds for them.

Tracking Malicious Code

Once a particular vulnerability is discovered, the intelligence-gathering team must observe what types of malicious code, if any, are being created to exploit the vulnerability. This task involves various forms of reconnaissance—from visiting online hacker forums, to watching what types of code are being shared and downloaded (e.g., to create variants), to tracking other types of suspicious activity. These observations help researchers determine whether hackers or other criminals are actively trying to create code that could exploit the vulnerability. They also allow organizations to guard against all the characteristics of that code as appropriate.

Identifying, Understanding, and Monitoring the Key Players

To accurately gauge the severity of a threat, organizations must monitor the individuals and groups who develop malicious code, and they must understand their motivations and modus operandi. Today's hackers are motivated more by money and revenge than by notoriety, and they frequently work for organized criminal gangs. These hackers work all over the world and are as close as the next cubicle. To effectively monitor them, intelligence teams must have multilingual experts with global contacts in the cyber underworld, law enforcement, and security divisions of worldwide corporations, governments, and financial institutions.

+ VeriSign iDefense – Proactive Threat Detection, Analysis, and Mitigation

VeriSign, the leading provider of digital infrastructure for the networked world, is the only company that incorporates all three components of a defense-in-context strategy into its security intelligence solution. VeriSign® iDefense® Threat Intelligence Services engage a world-class team of security experts; a vast intelligence network; state-of-the-art labs and technology; and highly refined methodology to deliver advance warning and analysis of network vulnerabilities and threats. Its comprehensive intelligence services enable organizations to take into account not only vulnerability data, but also the malicious code and malevolent actors that may exist to take advantage of a particular vulnerability.

Armed with VeriSign iDefense reports, briefings, and recommendations, organizations can better prioritize risk and respond rapidly and appropriately to protect critical assets—all while eliminating the complexity and overhead associated with comprehensive data collection, analysis, and response. When combined with VeriSign® Managed Security Services, VeriSign® Global Security Consulting, and the VeriSign® Security Risk Profiling Service, VeriSign iDefense services give organizations a holistic information-security solution that allows them to optimize existing resources while comprehensively managing risk. VeriSign services are supported by a digital infrastructure that enables and protects billions of interactions every day across the world's voice, video, and data networks.

Proactive Threat Detection

The VeriSign® iDefense® team identifies and tracks security events on a global basis, and then verifies, correlates, and analyzes this data to give organizations early warning and a reliable context for evaluating and responding to risk. Hands-on analysis by skilled personnel is a unique benefit of VeriSign iDefense services.

Early Warning

As hackers become more sophisticated, the time between discovering a vulnerability and developing malicious code to exploit it shrinks. Early warning and rapid response is vital to protecting business-critical resources. The following features of the VeriSign iDefense offerings support this capability:

- 24/7 risk monitoring and management – The VeriSign iDefense team monitors security events worldwide, 24/7, and then analyzes and correlates them in real time.
- Unique intelligence – The VeriSign global intelligence network includes more than 400 multilingual vulnerability researchers in more than 46 countries. These contributors offer early and unique insight into the cyber underground and previously unknown software vulnerabilities. In addition, VeriSign operates state-of-the-art labs for discovering and verifying original vulnerabilities. These capabilities are augmented by VeriSign's digital infrastructure, which leverages and correlates data gathered from thousands of devices across multiple organizations, industries, and regions to deliver intra-enterprise, inter-enterprise, and Internet-wide security intelligence.
- Proactive vulnerability notification – The VeriSign iDefense team notifies customers of exclusive vulnerabilities that it has discovered 121 days, on average, ahead of public disclosures. It also works rapidly to provide patches or workarounds for these vulnerabilities, and thereby mitigate risk.

Context and Prioritization

When an organization has an accurate picture of the threat environment, it can more easily prioritize actions and optimize resources. This capability lends itself to knowing when to act as much as knowing when not to act (see sidebar, The Value of Defense in Context) and ultimately saves organizations money. The following features of the iDefense offerings support this capability:

- Aggregation and analysis of all data – Although many vendors help organizations automatically collect and aggregate public vulnerability data, only VeriSign combines this data with malicious code research and threat analysis, where human intelligence analyzes and prioritizes it.
- Vendor neutral, independent analysis – VeriSign's vendor-neutral stance across all its security offerings ensures that threat collection, analysis, and response activities are based entirely on the goal of mitigating customer risk. This independent analysis also provides objectivity in cases where internal constituents may have motivations or biases that do not serve the organization.

Comprehensive Threat Analysis

While the VeriSign iDefense team uses state-of-the-art technology to gather data and streamline processes, human intelligence differentiates the VeriSign iDefense offerings. Only human intelligence can provide the high-level analysis, decision-making, and response required to discern and mitigate true threats. No other solution invests as heavily in human intelligence.

The VeriSign iDefense staff is divided into separate research teams that work together to provide a complete threat picture. Team members are skilled security researchers on the cutting edge of the industry. Many have worked for Fortune 500 companies and for the U.S. Department of Defense. Their methodology is described in the following sections.

Vulnerability Contributor Program (VCP)

The Vulnerability Contributor Program (VCP) leverages a private, worldwide network of independent security researchers who provide VeriSign with exclusive advance notification of unpublished vulnerabilities and exploit code. More than 400 VCP contributors are actively working in more than 46 countries and in multiple languages. As a result of their more than 2,100 submissions over the past three years, the iDefense team has reported more than 1,100 unique, original vulnerabilities to customers, with 305 reports in 2006 alone.

Vulnerability Labs

Vulnerability Labs are responsible for the identification of original vulnerabilities and the technical verification of vulnerabilities submitted by the VCP program. The physical laboratories consist of an isolated network environment that includes a large assortment of software and hardware used by Fortune 500 corporations and various world governments, thus simulating as closely as possible real-world environments.

Vulnerability Aggregation Team (VAT)

The Vulnerability Aggregation Team aggregates raw data from more than 1,500 sources, including mailing lists, Web sites, and proprietary resources.

It is responsible for ensuring around-the-clock coverage and customer notification of emerging vulnerabilities and exploits that target any of the more than 10,000 applications, hardware, and operating systems that it monitors. Analysts regularly infiltrate hacker organizations, and are skilled in tracking underground research and gaining access to zero-day exploits. For the last two years, VeriSign iDefense customers have received, on average, 121 days advanced notice of VeriSign iDefense exclusive vulnerabilities.

Malicious Code Team

The Malicious Code Operations Team monitors threats posed by viruses, worms, Trojan horses, spyware, and adware. It reports on hundreds of new malicious code threats each month and has devised a rapid-response system to notify customers of important outbreaks. Malcode analysts have strong backgrounds in malicious code engineering, research, and reporting, and experience with a wide range of programming languages and malicious code software solutions. The Malcode Team directs cutting-edge research in the Malicious Code Lab, which has a world-class environment for reverse engineering and operational analysis of malicious code. In 2006, the Malcode Team documented and analyzed 11,543 piece of malicious code and 547 pieces of exploit code.

Threat Analysis Team

The Threat Analysis Team assesses the motivation behind cyber attacks and hacker groups worldwide. This assessment is vital to understanding the actors behind a threat and why they have launched it. The Threat Analysis Team puts analysts on the ground in countries considered hotbeds for cyber crime in an effort to better gather intelligence on malicious individuals and groups responsible for threats targeting VeriSign customers. The Threat Analysis Team also reports on related topics, including emerging threats, information warfare, cyber crime, and critical infrastructure protection.

Rapid Response Team

The Rapid Response Team is composed of incident response specialists with security expertise in all areas of malicious code, vulnerabilities, and geopolitical threats. The team focuses on risk research and reporting as it pertains to global threats and emerging technologies and trends. Team analysts and engineers work with customers as a line of first response for security incidents, and to coordinate discovery and mitigation of targeted attacks against VeriSign customers. In 2006, the team delivered 54 Rapid Response Reports to customers, helping to protect them against attacks engineered specifically against their organization.

THE RUSSIAN BUSINESS NETWORK: A GROWING THREAT

In early 2007, the VeriSign iDefense global threat research team completed the first stage of an investigation into a sophisticated group of criminals looking for financial gain based out of St. Petersburg, Russia.

This group, which calls itself the "Russian Business Network," has been behind numerous attacks stemming from illicit phishing attacks and phishing tool kits, such as "rockphish," which is responsible for approximately 50 percent of the world's phishing attacks and by some estimates made \$150 million USD in 2006.

Additionally, this group is responsible for a wide variety of malicious code that also includes Torpig and Ursnif malicious code families. The Russian Business Network hosts multiple pornography sites as seeding points to hijack browsers and deliver large payloads of malicious code, spyware and adware for additional avenues of financial gain.

The Russian Business Network is protected by family connections to the St. Petersburg government, and has accomplices in the UK, Germany, Turkey, Romania, the US and Hong Kong.

A scan of the Russian Business Network ISP and its affiliated ISP's Web space resulted in nearly 100 percent use of hosting illegal and potentially malicious files. The Russian Business Network is just one example of a recent influx of highly sophisticated financially driven groups that are being heavily investigated by VeriSign to provide customers with the most actionable security intelligence available.

+ **The VeriSign Difference: Infrastructure, expertise, Intelligence, Trust**
Few companies match VeriSign's experience and expertise, depth and breadth of services, robust digital infrastructure, intelligence, and its role as a trusted advisor. VeriSign security services leverage exceptional knowledge, training, and experience; best-of-breed solutions; a global network of proven technology; and VeriSign's history of stability and trust, to deliver cost effective solutions for proactively managing information security risk. The following characteristics distinguish and differentiate VeriSign offerings:

+ **Global Scale and unmatched Digital Infrastructure**

With a worldwide customer base and thousands of security devices under management, VeriSign has the scale to support the largest and most demanding organizations and the flexibility to support smaller enterprises where security is also a concern. The breadth of devices that VeriSign monitors affords the company a wider and deeper view of Internet activity. It leverages this unique threat intelligence, and the knowledge gathered by the VeriSign iDefense team to proactively identify—and alert customers to—emerging attack trends and cyber threats.

+ **Seasoned Practitioners**

With an average of more than ten years' experience in enterprise information security and three or more industry certifications per consultant, the VeriSign consulting team boasts one of the highest concentrations of credentialed experts in the industry. The security team's expertise, dedication, and focus on customer service help ensure that each customer not only gets a real-world solution that meets the unique requirements of its business, but also receives prompt attention when security events or other issues arise.

+ **Commitment to excellence**

As a recognized leader in managed security services, VeriSign continues to experience growth well beyond the managed security services market. As a result, VeriSign continues to invest heavily in research and development and in infrastructure, continuing to add Security Operations Centers (SOCs) and staff in anticipation of continued growth. The company's architecture supports high redundancy to ensure that customers receive 24/7 support and availability worldwide.

+ **World-class Support for Industry-leading Technology**

VeriSign delivers world-class services to enterprise customers by leveraging industry-leading technology; skilled experts; structured processes; and unique intelligence. As a services company, VeriSign focuses solely on designing and deploying security solutions that meet the specific requirements of its customers and maximize the effectiveness of their existing security investments.

+ **Trusted Partner**

VeriSign has a strong heritage in providing trusted security services, and thousands of organizations benefit from this heritage every day. Together with strong authentication, security consulting, threat intelligence, and e-commerce security, VeriSign Managed Security Services represent an unparalleled commitment to helping enterprises engage confidently in electronic commerce, communications, and collaboration.

The Value of DeFeNSe IN CoNtEXt

A few months after the Zotob (MS05-039) incident, researchers discovered a nearly identical plug-and-play (PnP) vulnerability with MS05-051. Believing that this vulnerability posed as extreme a threat as Zotob, many organizations reacted and emergency patched right away.

However, the VeriSign iDefense team chose a more methodical, less costly course. Instead of basing its response on the vulnerability data alone, it looked at the extra intelligence provided by its threat and malicious code teams to examine the vulnerability in a broader context. The threat and malicious code teams did not observe any online discussion of the vulnerability, and they did not detect any other suspicious activity (for example, individuals trading code or moving to build exploit code). In short, they did not see a threat.

For this reason, the iDefense team advised its customers that they did not need to emergency patch; they could do so during their normal patching cycle. Six-to-eight weeks later, there was still no malicious code exploiting the vulnerability.

Organizations that followed the team's advice and patched their systems during their normal patch cycles didn't waste valuable resources (\$1.4 million for one large information processing center) on emergency patching.

+ Summary

To effectively manage security risks, organizations must be able to examine network vulnerabilities and threats in a broad context that includes data collection and analysis, malicious code tracking, and threat analysis. Few organizations—and few vendors—have the resources to perform all three of these activities. In fact, only VeriSign® iDefense® Threat Intelligence Services provide all three components of this “defense in context” strategy. The VeriSign iDefense services leverage VeriSign's digital infrastructure, state-of-the-art technology, and highly trained teams of security professionals to collect and analyze vulnerability data, track malicious code, and monitor the actors who exploit vulnerabilities. Using VeriSign iDefense services, organizations gain the early warning and clear insight needed to proactively identify real threats and mitigate those threats rapidly.

+ Learn More

For more information about VeriSign® iDefense® Threat Intelligence Services, please call 650-426-5310, or email enterprise_security@verisign.com.

+ About the VeriSign iDefense Team

The VeriSign iDefense team is part of the VeriSign Managed Security Services (MSS) division. VeriSign's iDefense team helps protect the world's largest networks in government, financial, and retail markets. Its daily and weekly reports on emerging and established cyber threats—including actionable mitigation steps—are considered essential reading, and drive customers' proactive network defense strategies.

+ About VeriSign

VeriSign, Inc. (NASDAQ: VRSN) operates digital infrastructure that enables and protects billions of interactions everyday across the world's voice, video, and data networks.

Visit us at www.Verisign.com for more information.