



CASE STUDY

A CLASSIC LIFECYCLE RISK SCENARIO

The Zotob.A threat followed the lifecycle that VeriSign predicted in its analysis of Copa.A. Specifically, the analysis predicted that as threats escalate from a public exploit code to a tool like Copa.A, it is highly likely that Trojans, and possibly a worm, will follow. The last time events of this nature occurred was with the MS03-026 vulnerability, which led to an auto-root-type tool, several Trojans, and then the Blaster and Welchia worms.

KEY BENEFITS

Unmatched Security Intelligence

VeriSign iDefense Security Intelligence Services leverage submissions from a private, worldwide network of independent security researchers obtained through our Vulnerability Contributor Program (VCP). The program includes hundreds of researchers in more than 42 countries who provide intelligence in multiple languages. VeriSign has received thousands of submissions to the VCP in the last three years. Upon receipt of these submissions, VeriSign does thorough internal research to validate the submission, and upon validation, notifies both the affected vendor and VeriSign iDefense customers. As a result,

The VeriSign Response to ZoTob.A

The VeriSign® iDefense® Security Intelligence Services are an important component of the acclaimed suite of VeriSign® Managed Security Services (MSS). These services deliver comprehensive, actionable intelligence regarding network-based security threats and vulnerabilities to help organizations proactively protect critical data and infrastructure from attacks and manage security risk.

Utilizing an experienced team of security experts, VeriSign searches the Internet for potential cyber threats including new malicious code, zero-day exploits, and hacker groups committing cyber crime or threatening widespread cyber terror. VeriSign combines this with technical and traditional intelligence to deliver advanced warning and analysis of these threats to help protect an organization's critical infrastructure.

While VeriSign iDefense Security Intelligence Services are a critical component of any successful information security program, the expertise and intelligence provided by our iDefense offering also produces significant benefits for other Managed Security Services customers.

The following Case Study illustrates how the combined strengths of superior people, processes, technologies, and intelligence enable VeriSign to more quickly identify and respond to emerging threats to make our customers more secure.

+ Event Timeline

Day 1 - Tuesday, Aug. 9, 2005

Microsoft® releases security bulletin MS05-039 regarding a plug-and-play buffer overflow vulnerability. VeriSign quickly releases a Flash Intelligence Report, "ID# 418964: HIGH: Microsoft Plug-and-Play Buffer Overflow Vulnerability," to all VeriSign iDefense Security Intelligence Services customers and begins researching the threat.

Day 2 - Wednesday, Aug. 10, 2005

VeriSign sends multiple updates to the original report to its iDefense Security Intelligence Services customers.

Day 3 - Thursday, Aug. 11, 2005

VeriSign discovers public exploit code, greatly increasing risk in such a short period of time following the Microsoft security bulletin. As a result VeriSign sends a Flash Intelligence Report to all VeriSign iDefense Security Intelligence Services customers.



Where it all comes together.™



CASE STUDY

VeriSign has reported hundreds of unique, original vulnerabilities to customers. Most important, on average, VeriSign iDefense customers received notices regarding these vulnerabilities 68 days before they were released to the public by the vendors.

Customized Intelligence

VeriSign iDefense Security Intelligence Services offer a highly customizable set of intelligence services delivering the intelligence your organization needs, when you need it.

The Value of Intelligence

The number of vulnerabilities continues to grow exponentially, while the time elapsed between vulnerability and exploit continues to shrink. VeriSign, which tracks security events on a global basis, delivers notification of vulnerabilities and exploits as they are identified, providing timely, actionable information and guidance to help mitigate risks before they are exploited. VeriSign iDefense Security Intelligence Services enable a proactive approach to maintaining a secure environment, while saving time and money by eliminating the hours spent searching through Web sites and emails, gathering and distributing information, and following up on the results.

Security Monitoring and Risk Management

The Vulnerability Aggregation Team (VAT) monitors security events 24/7. These events are captured, analyzed, and correlated in real time by VAT, which provides primary and secondary analyses of new vulnerability exploits. Suspicious and malicious events are therefore proactively identified—helping to mitigate an organization's potential for security risk.

Additionally, the Bi-Weekly Threat Briefing goes out to our large enterprise customers warning of the new vulnerability and the appearance of some exploit code.

Day 4 - Friday, Aug. 12, 2005

VeriSign identifies additional exploit code including the HOD exploit code, created by the same actor that published the exploit code for LSASS in 2004, which lead to Sasser and other worms.

VeriSign upgrades the advisory to EXTREME due to three exploit codes and increased hacker activity, and sends notification to iDefense Security Intelligence Services customers. Further advisories include the addition of Snort™ signature information and other data to help mitigate the worm.

At the same time VeriSign MSS implements a combination of custom and public signatures across multiple platforms to help protect VeriSign Intrusion Detection Management Service (IDS) customers and VeriSign® Intrusion Prevention Management Service (IPS) customers from the MS05-039 exploitation.

Day 5 - Saturday, Aug. 13, 2005

The VeriSign iDefense Malicious Code Team monitors hacker activities related to MS05-039 exploitation. It finds that three compiled binaries are made from public exploits, and are moving towards a tool, a Trojan, and automated malicious code exploitation.

Day 6 - Sunday, Aug. 14, 2005

VeriSign identifies the first tool to emerge to help automate exploitation of vulnerable computers (an iDefense Malcode exclusive). This is a significant development in terms of lifecycle risk evolution, but a relatively simple code.

VeriSign sends a predictive Flash Intelligence Report—based upon all the factors related to the global risk and lifecycle of this threat—to all iDefense Security Intelligence Services customers.

VeriSign MSS deploys additional signatures across multiple platforms to help protect VeriSign IDS and VeriSign IPS customers from MS05-039 bots.

Day 7 - Monday, Aug. 15, 2005

Seven new bots are reported on this day. Three of these bots are first reported by the VeriSign iDefense Rapid Response Team (no other public reports on the code):

419659:RBot.BJK

419662:RBot.BJL

419691:SdBot.TPR

VeriSign validates several codes for email functionality, and exploit vectors to fully qualify the evolution of bot threats exploiting MS05-039.

Day 8 - Tuesday, Aug. 16, 2005

Over a half dozen bots emerge this day, with incidents against large companies known for the RBot.BJT variant, and others. At this point VeriSign IDS and IPS customers have been notified of the threat and have signatures deployed to identify it. In light of the onslaught of bot families and variants against MS05-039 and success of the RBot.BJT variant in particular, VeriSign releases a Flash Intelligence Report to all VeriSign iDefense Security Intelligence Services customers (419872: EXTREME: FLASH(v1): RBot.BJT Worm Exploits Microsoft Plug-and-Play Buffer Overflow Vulnerability, Aggressively

Global Network of Intelligence Contributors

The VeriSign intelligence network includes hundreds of multilingual research contributors in more than 42 countries offering early and unique insight into the cyber underground and previously unknown software vulnerabilities.

Spreading in the Wild).RBot.BJT Worm Exploits Microsoft Plug-and-Play Buffer Overflow Vulnerability, Aggressively Spreading in the Wild).

+ Conclusion

The unique combination of solutions that comprise VeriSign Managed Security Services provided for better threat detection, superior analysis, and unparalleled response to this threat. VeriSign iDefense Security Intelligence Services customers were provided the most up-to-date intelligence regarding the threat throughout its evolution. At the same time, VeriSign was able to deploy signatures to detect the exploit across multiple commercial and open-source IDS/IPS platforms, affording increased protection for VeriSign IDS and IPS customers.

+ The VeriSign Difference

Few companies match VeriSign's experience and expertise, depth and breadth of services, robust infrastructure, intelligence, and role as 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 intelligent 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, as well as the intelligence gathered by the VeriSign iDefense Security Intelligence Services 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 (more than 15 percent of revenues annually) and in infrastructure (where we continue to add Security Operations Centers (SOCs) and staff in anticipation of continued growth). The company's architecture is highly redundant 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.



DATA SHEET

- **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.

+ Learn More

For more information about VeriSign Managed Security Services and VeriSign® Global Security Consulting, please call 650-426-5310, email enterprise_security@verisign.com, or visit us at www.Verisign.com.

+ About VeriSign

VeriSign, Inc. (Nasdaq: VRSN) operates intelligent infrastructure services that enable and protect billions of interactions everyday across the world's voice and data networks. Additional news and information about the company is available at www.verisign.com.

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

©2006 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," TeraGuard, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.

00021221 04-10-2006