



CASE STUDY

A CLASSIC LIFECYCLE RISK SCENARIO

The ZoTob.A threat followed the life cycle 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 Programme (VCP) which includes hundreds of researchers in over 30 countries who provide intelligence in 12 languages. VeriSign has received thousands of submissions to the VCP in the last three years. On receipt of these submissions, VeriSign does thorough internal research to validate the submission, and if confirmed, notifies both the affected vendor and iDefense Security Intelligence Service clients.

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 organisations proactively protect critical data and infrastructure from attacks.

Utilising an experienced team of security experts, VeriSign scours the Internet for potential cyber threats, including new malicious code, zero-day exploits, or 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 organisation's critical infrastructure.

While the VeriSign iDefense Security Intelligence Services are a critical component of any successful information security programme, the expertise and intelligence provided by iDefense also produce significant benefits for other VeriSign Managed Security Services clients.

The case study below provides an example of how the combined strengths of superior people, processes, technologies and intelligence enable VeriSign to more quickly identify and respond to emerging threats to make their clients 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 iDefense Flash Intelligence Report "ID 418964:HIGH:Microsoft Plug-and-Play Buffer Overflow Vulnerability" to all iDefense Security Intelligence Services clients and begins researching the threat.

Day 2 - Wednesday, Aug. 10, 2005

VeriSign sends multiple updates to the original report to their iDefense Security Intelligence Services clients.

Day 3 - Thursday, Aug. 11, 2005

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



Where it all comes together.™



CASE STUDY

VeriSign works closely with vendors such as Microsoft to help ensure that any potential vulnerabilities are identified, and ensure that vendors are able to create patches as quickly as possible. Clients are also notified of these vulnerabilities while VeriSign works with the vendor. As a result, VeriSign has reported hundreds of iDefense unique, original vulnerability reports to clients. Most important, on average, iDefense Security Intelligence Service clients received notices regarding these vulnerabilities 45 days in advance of their release to the public by the vendors.

Customised Intelligence

VeriSign iDefense Security Intelligence Services offers a highly-customisable set of intelligence services delivering the intelligence your organisation needs, when you need it.

The Value of Intelligence

The cost of a security breach in terms of loss of time, data and brand equity has grown dramatically over the last few years. At the same time, the number of vulnerabilities has grown exponentially, while the time elapsed between vulnerability and exploit continues to shrink. As a result, it is increasingly critical for enterprises to proactively protect themselves. VeriSign, tracks security events on a global basis, and delivers notification of vulnerabilities and exploits as soon 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.

In addition, the VeriSign MSS Bi-Weekly Threat Report goes out to our large corporate clients warning them 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, the same actor who published the exploit code for LSASS in 2004 leading to Sasser and other worms.

VeriSign upgrades the advisory to EXTREME due to three exploit codes and much hacker activity, and sends notification to iDefense Security Intelligence clients. 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 customised and public signatures across multiple platforms to help protect Managed IDS (Intrusion Detection Service) / IPS (Intrusion Prevention Service) clients against the MS05-039 exploitation.

Day 5 - Saturday, Aug. 13, 2005

Malicious Code Team monitors hacker activities related to MS05-039 exploitation. They find 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 malware exclusive). This is a significant development in terms of life cycle risk evolution, but a relatively simple code.

VeriSign sends a predictive iDefense Flash Intelligence Report to all iDefense Security Intelligence Service clients based on all the factors related to the global risk and life cycle of this threat.

VeriSign MSS deploys additional signatures across multiple platforms to help protect Managed IDS / IPS clients against MS05-039 bots.

Day 7 - Monday, Aug. 15, 2005

Seven new bots are reported on Aug. 15, 2005. Three of those are first reported by the VeriSign® 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 exploits vectors to fully qualify the evolution of bot threats exploiting MS05-039.

Day 8 - Tuesday, Aug. 16, 2005

Over a half dozen bots emerge on this day, with incidents against large companies known for the RBot.BJT variant, and others. At this point VeriSign Managed IDS and IPS customers have been notified of the threat and have had 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 an iDefense Flash Intelligence Report to all iDefense Security Intelligence Service clients (419872:EXTREME:FLASH(v1):RBot.BJT Worm Exploits Microsoft Plug-and-Play Buffer Overflow Vulnerability, Aggressively Spreading in the Wild).



CASE STUDY

Security Monitoring and Risk Management

24/7 monitoring of security events, which are captured, analysed and correlated in real time by our Vulnerability Aggregation Team, providing primary and secondary analyses of new vulnerability exploits. Suspicious and malicious events are therefore proactively identified—helping to mitigate an organisation's risk potential.

Global Network of Intelligence Contributors

VeriSign has a multilingual network which includes hundreds of research contributors in over 30 countries offering early and unique insight into the cyber underground and previously unknown software vulnerabilities.

+ Conclusion

The unique combination of solutions that comprise VeriSign Managed Security Services provide for better threat detection, superior analysis and unparalleled response to this threat. VeriSign iDefense Security Intelligence Services clients 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 our Managed IDS/IPS clients.

+ The VeriSign Difference

Global Scale and Intelligence and Control – As a leading provider of critical Internet-infrastructure services, VeriSign has a unique insight into security patterns, trends and threats by extracting and assimilating information from its worldwide client base and network of security devices under management. Leveraging this information and intelligence, VeriSign can be first in providing companies with visibility, aggregation and correlation of worldwide Internet-related events, proactively identifying and alerting clients to attack trends.

Trusted Partner – VeriSign has a strong tradition in managing trusted security services, and thousands of organisations benefit from this heritage every day. Together with strong authentication, application security and e-commerce security, VeriSign® Managed Security Services represent an unparalleled commitment to providing services which enable organisations to engage confidently in electronic commerce, communications and collaborative computing.

Seasoned Practitioners – The VeriSign security consulting team includes one of the highest concentrations of credentialed experts in the industry. With an average of ten years experience in business information security and three or more industry certifications per consultant, VeriSign boasts expertise across the entire information-security and information-privacy spectrum. The VeriSign team has worked with entities of all sizes worldwide, from government agencies and Fortune 1000 companies to small start-ups. VeriSign clients include local, regional, local and national government agencies, financial institutions, healthcare organisations, telecoms and online retailers.

Best-of-Breed Solutions – As a vendor-neutral provider of security services, VeriSign evaluates, certifies, and supports best-of-breed security products. It is a leading proponent of open standards-based technology for identity authentication and other security solutions. The company designs and deploys security solutions based on the specific needs and requirements of its clients and regularly evaluates and enhances its service offerings and support for third-party security products.

+ Get Started Today

For more information about VeriSign® iDefense® Security Intelligence Services, please call 0800 032 2101 or email: sales@verisign.co.uk

Visit us at www.verisign.co.uk for more information.

©2006 VeriSign UK Ltd. 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. All other registered and unregistered trademarks and trade names are the property of their respective owners.

00021897 11-01-2006