black hat® europe
DIGITAL SELF DEFENSE
+2010 BARCELONA, SPAIN
HOTEL REY JUAN CARLOS

welcome

Welcome to the Black Hat Briefings Europe! As Black Hat heads into its 13th year, I see this as a pivotal time for the entire industry. With the attention on our industry after the public announcement of the "Aurora" Google attacks it seems our profession is starting to enter the world stage. It is dawning on politicians that there are larger issues besides p2p and copyright infringement to deal with. Attribution is the byword of military and intelligence organizations, it's hard to respond if you don't know who just attacked you, and the research in this area as gotten a renewed purpose in life. At the same time there is a growing sense that policy makers are getting involved with legislation from Cyberspace security acts and mandatory disclosure laws to more potential controls on ISPs to help track and contain botnets. Things seem to be speeding up!

I am excited for this year's conference for a number of reasons. First is the new location, Barcelona! You might not believe me, but for the past three years in Amsterdam we had maxed out the available space at the Movenpick, with no easy way to grow the conference. I kept hoping a new hotel would be built with the appropriate space, but no such luck. The second reason is that this move has let us grow from two tracks to three, a long-time personal goal of mine. I think the only way Black Hat will grow is by staying focused on technical security content and research and by adding more of it. This third track is the first major step in that direction!

This year's three tracks will feature over 25 speakers discussing their latest research. In addition we have selected a wider range of topics, instead of being forced to only have one presenter on a given topic there is now be some overlap. The Big Picture track is meant to help orient you and highlight the larger world we operate in, as well as some of the bigger battles currently raging.

In 2010 you will see Black Hat in more places, as I try to expand the reach of Black Hat speakers and trainers. In late 2009 we held a joint Virtual Event with Dark Reading that was a success, and so in Q4 2010 we are planning a full stand-alone Virtual Black Hat Briefings. Think of it as a regular Briefings with a Call for Papers, keynote address and multiple tracks. Same great content delivered at Black Hat, just all on-line.

Also in 2010 will the first Black Hat Abu Dhabi, bringing the Black Hat way of thinking about security to a different region of the world. With three tracks and training it will be the full Black Hat experience! I hope it inspires the security experts in the region to participate. I'm really interested to learn what's going on in their security community.

If you are interested in participating at the next Black Hat, think about submitting a paper. The CFP is now open, as is registration for our big conference Black Hat USA at the end of July in Las Vegas, Nevada.

Jeff Moss

Jeff Moss
Director, Black Hat

contents

SUSTAINING sponsors

QUALYS®
Microsoft®
CORE SECURITY TECHNOLOGIES
IOActive™ COMPREHENSIVE COMPUTER SECURITY SERVICES
nitrosecurity
Trustwave® Information Security & Compliance

WWW.BLACKHAT.COM

presentations

MISUSING WIRELESS ISPS FOR ANONYMOUS COMMUNICATION

Andre Adelsbach

In this presentation we will present several insider attacks, which break the unicast communication imposed by the carrier of the infrastructure. The most striking example of highly asymmetric resources are satellite ISPs: here the user normally has a terrestrial link to the carrier and no means to broadcast data at all. On the other side, the carrier can broadcast its signals over huge footprints, covering thousands of kilometers. Therefore, we will illustrate our attacks mainly in terms of satellite ISPs, but also discuss other examples such as WIMAX. Our strongest insider attack allows any end-user to make the satellite ISP broadcast data as clear text, even if the downlink (data sent from the satellite to the user) is properly encrypted by the satellite ISP, thereby breaking the unicast communication structure imposed by the satellite ISP. Finally, we discuss how the presented findings can be used to set up communication channels, achieving perfect receiver anonymity.

CYBER [CRIME | WAR] CHARTING DANGEROUS WATERS

Iftach Ian Amit

CyberWar has been a controversial topic in the past few years. Some say the the mere term is an error. CyberCrime on the other hand has been a major source of concern, as lack of jurisdiction and law enforcement have made it one of organizaed crime's best sources of income. In this talk we will explore the uncharted waters between CyberCrime and CyberWarfare, while mapping out the key players (mostly on the state side) and how past events can be linked to the use of syndicated CyberCrime organization when carrying out attacks on the opposition. We will discuss the connections between standard warfare (kinetic) and how modern campaigns use cybersecurity to its advantage and as an integral part of it.

BINDING THE DAEMON: FREEBSD KERNEL STACK AND HEAP EXPLOITATION

Patroklos Argyroudis

FreeBSD is widely accepted as one of the most reliable and performance-driven operating systems currently available in both the open source and proprietary worlds. While the exploitation of kernel vulnerabilities has been researched in the context of the Windows and Linux operating systems, FreeBSD, and BSD systems in general, have not received the same attention. This presentation will initially examine the exploitation of kernel stack overflow vulnerabilities on FreeBSD. The development process of a privilege escalation kernel stack smashing exploit will be documented for vulnerability CVE-2008-3531. The second part of the presentation will present a detailed security analysis of the Universal Memory Allocator (UMA), the FreeBSD kernel's memory allocator.

SCADA AND ICS FOR SECURITY EXPERTS: HOW TO AVOID BEING A CYBER IDIOT

James Arlen

The traditional security industry has somehow decided that they are the white knights who are going to save everyone from the horror of insecure powergrids, pipelines, chemical plants, and cookie factories.Suddenly, every consultant is an expert and every product is loudly advertising how it solves SCADA SECURITY AND COMPLIANCY ISSUES! And because they don't know what the hell they're talking about – 'fake it till ya make it' doesn't work – they're making all of us look stupid.

Let's sit down for a little fireside chat and discuss all things SCADA and ICS with an eye towards increasing our knowledge to the point where we can confidently say: "I'm not an expert at everything, I can help some, may we work together on a solution?" It's time to stop being a Cyber Idiot and start being a positive contributor. Learn some truth, look behind the curtain, bust some FUD, Oh – and make government agents have kittens. That's fun for everyone.

VIRTUAL FORENSICS

Christiaan Beek

This presentation will be about the problems we are facing when forensic research has to be done on environments which are virtualized. What are the differences between 'traditional' system forensics, what techniques & tools can be used? Which files are important when performing forensic research on Citrix and VMWare environments? What about the VMDK file system and what do we need for future research?

SURVIVING YOUR PHONE: PROTECTING MOBILE COMMUNICATIONS WITH TOR

Marco Bonetti

Tor is a software project that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security. Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Unfortunately, with the new features of HTML5 and browser built-in geolocation being pushed into the Web2.0 world and on mobile phones and browser, it's becoming harder and harder to keep the users' privacy safe. This presentation will describe the problems which are arising around the use of these new technologies and how they can be (ab)used to attack Tor users. It will also describe where the development is going to protect mobile phone users privacy and let them survive their own devices.

FIRESHARK, A TOOL TO LINK THE MALICIOUS WEB

Stephan Chenette

Thousands of legitimate web sites serve malicious content to millions of visitors each and every day. Trying to piece all the research together to confirm any similarities between possible common group patterns within these websites, such as redirectors that belong to the same IP, IP range, or ASN, and reconstructing the final deobfuscated code can be time consuming and sometimes impossible given many of the freely available tools. I will present a web security research project called FireShark that is capable of visiting large collections of websites at a time, executing, storing and analyzing the content, and from it identifying hundreds of malicious ecosystems of which the data, such as the normalized, deobfuscated content within them can easily be analyzed.

TARGETED ATTACKS: FROM BEING A VICTIM TO COUNTER ATTACKING

Andrzej Dereszowski

This presentation is an analysis of a common sort of targeted attacks performed nowadays against many organizations. As it turns out, publicly available remote access tools – RAT (which we usually call trojans) are frequently used to maintain control over the victim after a successful penetration. The presentation and the white paper do not focus on a particular exploitation techniques used in these attacks. Instead, they aim to get a closer look at one of the most popular remote access trojans. The presentation describes a way to figure out which particular trojan has been used. It shows the architecture, capabilities and techniques employed by developers of the identified trojan, including mechanisms to hide its presence in the system, and to cover its network trace. It speaks about tools and techniques used to perform this analysis. Finally, it presents a vulnerability analysis and a proof of concept exploit to show that the intruders could also be an object of an attack.

SAP BACKDOORS: A GHOST AT THE HEART OF YOUR BUSINESS

Mariano Nuñez Di Croce

In any company, the ERP (Enterprise Resource Planning) is the heart of the business technological platform. These systems handle the key business processes of the organization, such as procurement, invoicing, human resources management, billing, stock management and financial planning. Among all the ERPs, SAP is by far the most widely deployed one, having more than 90.000 customers in more than 120 countries and running in Fortune 100 companies, governmental and defense organizations.

This talk will present an old concept applied to a new paradigm: SAP Backdoors. We will discuss different novel techniques that can be deployed by malicious intruders in order to create and install backdoors in SAP systems, allowing them to retain access or install malicious components that would result in imperceptible-and-ongoing financial frauds.

After the description of these techniques, we will present the countermeasures that should be applied in order to avoid these attacks and protect the business information, effectively reducing financial fraud risks and enforcing compliance.

Furthermore, we will release a new Onapsis free tool that will help security managers to automatically detect unauthorized modifications to SAP systems.

VERIFYING EMRTD SECURITY CONTROLS

Raoul D'Costa

With the transition to RFID enabled travel documents (including the ePassport and the eID) in Europe, a correct implementation of the authentication and verification of passport technologies is necessary. The complexity if the technology can cause a myriad of security issues in the identification.

Our presentation examines the eMRTD security controls and suggests correct implementations to enable identification as a mechanism. We also examine the dangers of incorrect implementations and the resulting consequences.

PRACTICAL CRYPTO ATTACKS AGAINST WEB APPLICATIONS

Thai Duong & Juliano Rizzo

In 2009, we released a paper on MD5 extension attack ([1]), and described how attackers can use the attack to exploit popular web sites such as Flickr, Vimeo, Scribd, etc. The attack has been well-received by the community, and made the Top Ten Web Hacking Techniques of 2009 ([2]). In the conclusion of that paper, we stated that we have bexen carrying out a research in which we test-run a number of identified practical crypto attacks on random widely-used software systems. To our surprise, most, if not all, can be attacked by one or more of well-known crypto bugs. In this talk, we present the latest result of that research, where we choose another powerful crypto attack, and turn it into a new set of practical web hacking techniques.

CONTINUED //

We show that widely used web development frameworks and web sites are using encryption wrongly that allow attackers to read and modify data that should be protected. It has been known for years in cryptography community that encryption is not authentication. If encrypted messages are not authenticated, data integrity cannot be guaranteed which makes systems vulnerable to practical and dangerous chosen-ciphertext attacks. Finally, we list several popular web development frameworks and web sites that are vulnerable to Padding Oracle attacks, including, but not limited to, eBay Latin America, Apache MyFaces, SUN Mojarra, Ruby On Rails, etc. These are all 0-day vulnerabilities. We show that even OWASP folks can't get it right, how can an average Joe survive this new class of vulnerabilities? We strongly believe that this is just the tip of the iceberg, and the techniques we describe in this research would uncover many more vulnerabilities for years to come.

HOW TO OPERATIONALLY DETECT AND BREAK MISUSE OF WEAK STREAM CIPHERS

Eric Filiol

Despite the evergrowing use of block ciphers, stream ciphers are still widely used: satellite communications (military, diplomatic...), civilian telecommunications, software... If their intrinsic security can be considered as strong, the main drwaback lies in the high risk of key misuse wich introduces severe weaknesses, even for unconditionnally secure ciphers like the Vernam system. Such misuses are still very frequent, more than we could expect.

In this talk we explain how to detect such misuses, to identify ciphertexts that are relevant to this misuse (among a huge amount of ciphertexts) and finally how to recover the underlying plaintext within minutes. This may also apply to (intendly or not) badly implemented block ciphers. To illustrate this technique, this talk will also deal with the technical cryptanalysis of encryption used in Office up to the 2003 version (RC4 based). We will focus on Word and Excel applications. The cryptanalysis has been successfully and we manage to recover more than 90% of the encrypted texts in a few seconds. The attack is based both on a pure mathematical effort AND a few basic forensic approach. In a more general cases (e.g. satellite communications), we just need to intercept ciphertexts.

In the Office case, we will explain in our sense that the attack does not rely on particular weakness but in a setting that can be seriously considered and described as a possible intended trap. We will develop this concept to explain how in a more general way such trap can be built.

DEFENDING THE POOR

FX

The talk presents a simple but effective approach for securing Rich Internet Application (RIA) content before using it. Focusing on Adobe Flash content, the security threats presented by Flash movies are discussed, as well as their inner workings that allow such attacks to happen. Some of those details will make you laugh, some will make you wince. Based on the properties discussed, the idea behind the defense approach will be presented, as well as the code implementing it and the results of using it in the real world.

WEAPONIZING WIRELESS NETWORKS: AN ATTACK TOOL AGAINST SENSOR NETWORKS

Thanassis Giannetsos

The pervasive interconnection of autonomous sensor devices has given birth to a broad class of exciting new applications. At the same time, however, the unattended nature and the limited resources of sensor nodes have created an equal number of vulnerabilities that attackers can exploit in order to gain access in the network and the information transferred within. While much work has been done on trying to defend these networks, little has been done on suggesting sophisticated tools for proving how vulnerable sensor networks are. This work demonstrates a tool that allows both passive monitoring of transactional data in sensor networks, such as message rate, mote frequency, message routing, etc., but also discharge of various attacks against them.

HARDWARE IS THE NEW SOFTWARE

Joe Grand

Society thrives on an ever increasing use of technology. Electronics are embedded into nearly everything we touch. Hardware products are being relied on for security-related applications and are inherently trusted, though many are completely susceptible to compromise with simple classes of attacks that have been known for decades.

Bolstered by the flourishing hobbyist electronics/do-it-yourself movement, easy access to equipment, and realtime information sharing courtesy of the internet, hardware is an area of computer security that can no longer be overlooked. In this session, Joe will explore the hardware hacking process and share some recent high-profile attacks against electronic devices.

0-KNOWLEDGE FUZZING

Vincenzo Iozzo

Fuzzing is a pretty common technique used both by attackers and software developers. Currently known techniques usually involve knowing the protocol/format that needs to be fuzzed and having a basic understanding of how the user input is processed inside the binary. In the past, fuzzing was little-used obtaining good results with a small amount of effort was possible. Today finding bugs requires digging a lot inside the code and the user-input as common vulnerabilities are already identified and fixed by developers.

This talk will present an idea on how to effectively fuzz with no knowledge of the user-input and the binary. Specifically the talk will demonstrate how techniques like code coverage, data tainting and in-memory fuzzing allow to build a smart fuzzer with no need to instrument it in any way.

ADOBE READER'S CUSTOM MEMORY MANAGEMENT: A HEAP OF TROUBLE

Haifei Li & Guillaume Lovet

PDF vulnerabilities are hot. Several AV and security companies, in their 2010 predictions, cited an increase in PDF vulnerabilities volume, possibly driven by demand from Cybercriminals, eager to leverage them in focused and large-scale attacks alike.

But how serious could it really be, and what's the share of casual marketing FUD spreading here? After all, many PDF vulnerabilities out there are structure (i.e. file format) based ones, and essentially result in heap corruption situations. And everybody knows that leveraging a heap corruption bug into actual exploitation, with execution of attacker-supplied code, is no piece of cake. Indeed, MS Windows' heap is hardly predictable, and is armoured with protection mechanisms such as safe-unlinking.

Yet, the main PDF reader software out there, called Adobe Reader, has a specificity that may lead us to revise our beliefs: for performance purpose, it implements its own heap management system, on top of the Operating System's one. And it turns out that, performance sometimes (often? nah...) being the enemy of security, this custom heap management system makes it significantly easier to exploit heap corruption flaws in a solid and reliable way. Coupled with the very recent developments in DEP protection bypass in Flash (eg: JIT spraying [1]), which we will briefly show to be also valid in PDF context, this makes heap corruption exploitation potentially consistent across a very large amount of setups (a very interesting characteristic for the Cybercriminal, either for "blind-shooting" at a targeted system, or for compromising a large amount of systems at once).

This paper introduces Adobe's Reader custom heap management system, dissects its mechanisms, and points out its weaknesses in order to shed light and awareness on the PDF vulnerabilities issue. In addition, limitations will be discussed and possible mitigation leads evoked.

[1] Interpreter Exploitation: Pointer Inference and JIT Spraying, Dion Blazakis

UNIVERSAL XSS VIA IE8S XSS FILTERS

David Lindsay & Eduardo Vela Nava

Internet Explorer 8 has built in cross-site scripting (XSS) detection and prevention filters. We will explore the details of how the filters detect attacks, the neutering method, and discuss the filters' general strengths and weaknesses. We will demonstrate several ways in which the filters can be abused (not just bypassed) in order to enable XSS on sites that would not otherwise be vulnerable. We will then show how this vulnerability makes most every major website vulnerable to XSS in affected versions of Internet Explorer 8.

CHANGING THREATS TO PRIVACY: FROM TIA TO GOOGLE

Moxie Marlinspike

We won the war for strong cryptography, anonymous darknets exist in the wild today, and decentralized communication networks have emerged to become reality. These strategies for communicating online were conceived of in anticipation of a dystopian future, but somehow these original efforts have fallen short of delivering us from the most pernicious threats to privacy that we're now facing.

Rather than a centralized state-based database of all our communication and movements, modern threats to privacy have become something much more subtle, and perhaps all the more sinister. This talk will explore these evolving trends and discuss some interesting solutions in the works.

ORACLE, INTERRUPTED: STEALING SESSIONS AND CREDENTIALS

Steve Ocepek & Wendel G. Henrique

In a world of free, ever-present encryption libraries, many penetration testers still find a lot of great stuff on the wire. Database traffic is a common favorite, and with good reason: when the data includes PAN, Track, and CVV, it makes you stop and wonder why this stuff isn't encrypted by default. However, despite this weakness, we still need someone to issue queries before we see the data. Or maybe not… after all, it's just plaintext.

CONTINUED //

presentations

Wendel G. Henrique and Steve Ocepek of Trustwave's SpiderLabs division offer a closer look at the world's most popular relational database: Oracle. Through a combination of downgrade attacks and session take-over exploits, this talk introduces a unique approach to database account hijacking. Using a new tool, thicknet, released at Black Hat Europe, the team will demonstrate how deadly injection attacks can be to database security.

ABUSING JBOSS
Christian Papathanasiou

JBoss Application Server is the open source implementation of the Java EE suite of services. It's easy-to-use server architecture and high flexibility makes JBoss the ideal choice for users just starting out with J2EE, as well as senior architects looking for a customizable middleware platform. The pervasiveness of JBoss in enterprise JSP deployments is second to none meaning there is an abundance of targets both for the blackhat or the pentester alike. JBoss is usually invoked as root/SYSTEM meaning that any potential exploitation usually results in immediate super user privileges. A tool has been developed that is able to compromise an unprotected JBoss instance. The current state of the art in published literature involves having the JBoss instance connect back to the attacker to obtain a war file that is subsequently deployed. The tool that will be presented at Black Hat does this in-situ and ultimately uploads a Metasploit payload resulting in interactive command execution on the JBoss instance. On Windows platforms, through the Metasploit framework a fully interactive reverse VNC shell can also be obtained and shall be demonstrated.

HACKING CISCO ENTERPRISE WLANS
Enno Rey & Daniel Mende

The world of "Enterprise WLAN solutions" is full of obscure and "non-standard" elements and technologies. Cisco's solutions, from the early Structured Wireless-Aware Network (SWAN) to the current Cisco Wireless Unified Networking (CUWN) architectures, only partly differ here. In this talk we describe the inner workings of these solutions, dissect the vulnerable parts and discuss theoretical and practical attacks, with some nice demos. A new tool automating a number of attacks (incl. taking over the WDS master role, extracting WPA pairwise master keys from intra-AP communication etc) will be released at Black Hat Europe.

ATTACKING JAVA SERIALIZED COMMUNICATION
Manish Saindane

Many applications written in JAVA make use of Object Serialization to transfer full blown objects across the network via byte streams or to store them on the file system. While Penetration Testing applications communicating via Serialized Objects, current tools/application interception proxies allow very limited functionality to intercept and modify the requests and responses like in typical web applications. I'm trying to introduce a new technique to intercept such Serialized communication and modify it to perform penetration testing with almost the same ease as testing regular web applications. For achieving this I have developed a plug-in for Burp Suite as a proof-of-concept. What makes this technique unique is that it is completely seamless and gives the penetration tester the same control and power that an application developer has.

STATE OF MALWARE: FAMILY TIES
Peter Silberman & Ero Carrera

Over the last few years malware has gravitated towards a few major families rather than the single or small-sized families of the past. Families of hundreds or even thousands are not uncommon. These families grouped together demonstrate the evolution of malware over time. This evolution may originate in simple bugfixes and small enhancements or entirely new sets of functionality added over an existing code base. Studying the ties between families, both within and across families, provides us with a context in which to study the development pace and technical improvements as they appear. We will examine how families grow and change amongst the mass malware and targeted attack malware. While examining how families grow and change we will attempt to identify features across all families that are both common and implemented in the same way. This could lead to quick static identification of malware features as well as signaturing these features. We hope to show how multiple families are derived from one code base, we will not just address mass malware, targeted malware but also rootkits and code sharing amongst them.

NEXT GENERATION CLICKJACKING
Paul Stone

Clickjacking is a technique that can be used to trick users into performing unintended actions on a website by formatting a web page so that the victim clicks on concealed links, typically hidden within an IFRAME. However, in comparison to other browser-based attacks such as XSS (Cross-site Scripting) and CSRF (Cross-site Request Forgery), Clickjacking has hitherto been regarded as a limited attack technique in terms of consequences for the victim and the scenarios in which it can be used. During this talk I intend to demonstrate that this assumption is incorrect, and that today's Clickjacking techniques can be extended to perform powerful new attacks that can affect any web application.

This talk will cover the basics of Clickjacking, quickly moving on to more powerful, and newly developed, techniques. The presentation will explore further ways in which a user can be tricked into interacting with a victim site and how these can lead to attacks such as injecting data into an application (bypassing all current CSRF protections) and the extraction of data from websites without the user's knowledge. The demo will show several cross-browser techniques, and newly released browser-specific vulnerabilities in Internet Explorer, Firefox and Safari/Chrome which can be used to take full control of a web application. I will also be demonstrating and releasing a new tool that allows for easy point-and-click creation of multi-step Clickjacking attacks on any web application, by visually selecting the links, buttons, fields and data to be targeted. The tool will highlight the need for improved Clickjacking defences in both browsers and web applications.

HACKING THE SMARTCARD CHIP
Christopher Tarnovsky

From start to finish, we will walk through how a current generation smartcard was successfully compromised. The talk will discuss everything that was required in the order the events took place. We will cram several months into an hour, will be very technical, mixed hardware and software.

UNVEILING MALTEGO 3.0
Roelof Temmingh

For a year the Paterva team has been quietly working on Maltego 3 with no new releases since March 2009. For the first time since Black Hat 2009, Paterva will be showing you what they have been up to - revealing an all new Maltego version, built from the ground up. Expect Hollywood quality graphing and animation, endless possibilities of extensions, new analytic views that will make you weep, and brand new transforms that will blow your mind.

SECURITY IN DEPTH FOR LINUX SOFTWARE
Julien Tinnes & Chris Evans

In many designs, the slightest error in the source code may become an exploitable vulnerability granting an attacker barely or not at all restricted access to a system. In this talk, using vsftpd and Google Chrome Linux as examples, we will firstly show how to design your code to be more robust to well-known classes of vulnerabilities and secondly, how to generically mitigate the consequences of such a vulnerability by dropping privileges and reducing attack surfaces.

While Mandatory Access Control systems are readily available, three of them being merged in the current Linux kernel tree, the ability to drop privileges in a "discretionary" way has to often rely on ancient mechanisms (which may not have been designed for security). We will show the state of the art on Linux and how well-known mechanisms, such as switching to an unprivileged uid, using chroot() and capabilities may or may not be suitable to achieve decent privilege dropping. We will discuss their drawbacks, availabilities to non-root processes and how an incorrect usage could be exploited by an attacker to circumvent security measures.

HIDING IN THE FAMILIAR: STEGANOGRAPHY AND VULNERABILITIES IN POPULAR ARCHIVES FORMATS
Mario Vuksan, Tomislav Pericin & Brian Karney

Exploiting archive formats can lead to steganographic data hiding and to processing errors with serious forensic consequences. These formats are very interesting as they are commonly found on every PC, Apple or Linux machine, and it is popularly believed that they are well understood and trusted. Can exploits ever be present in file formats that have been in use for over ten or even twenty years?

Through deep format analysis, beyond fuzzing, we look at what goes wrong when the format specifications are interpreted differently. Can you trust programs that work with archives? Can you even trust your antivirus? We will answer these questions and disclose for the first time 15 newly discovered vulnerabilities in ZIP, 7ZIP, RAR, CAB and GZIP file formats revealing the impact they have on anti-malware scanners, digital forensic, security gateways and IPS appliances. This talk will include demo of ArchiveInsider, a new forensics tool that detects and extracts hidden data and fully validates vulnerable file formats. We will demonstrate file format steganography, file malformation, and even data "self destruction," all with tools that you use and trust.

PROTOCOL, MECHANISM AND ENCRYPTION OF PUSHDO/CUTWAIL/WEBWAIL BOTNET
Kyle Yang

After several months efforts, the pushdo/cutwail botnet author(s) finally released a new pushdo advanced installer(codename "revolution") which not only changed the protocol and encryption totally but also implemented "Services" mechanism. Moreover, a new spam engine was in the experimental phase. In this presentation, I will examine pushdo's brand new protocol and encryption, reveal their "Cyber Crime Services" vendors mapping and disclose the debug version of the new spam engine's protocol and encryption.

speakers

Andre Adelsbach: Telindus S.A.

Iftach Ian Amit: With over 10 years of experience in the information security industry, Iftach Ian brings a mixture of Software development, OS, Network and web security to the Strategic consulting firm Security & Innovation.

Patroklos Argyroudis: is an IT security researcher at Census, Inc (www.census-labs.com), a company that builds on strong research foundations to offer specialized IT security services to customers worldwide. His current focus is on vulnerability research, exploit development, reverse engineering, source code auditing and malware analysis.

James Arlen is a security consultant most recently engaged as the CISO of a mid-market publicly traded financial institution. He has been involved with implementing a practical level of information security in Fortune 500, TSE 100, and major public-sector corporations for more than a decade.

Christiaan Beek has been working in the security field for several years. Working for national and international companies, he gained knowledge of hacking techniques, forensic analysis and incident response. Currently he is working as a security consultant/ethical hacker and trainer for a Dutch company, TenICT.

Marco Bonetti is a Computer Science engineer interested in privacy and security themes, following the emerging platforms for the protection of privacy in hostile environments. Created Slackintosh, the unofficial PowerPC port of the famous Slackware Linux distribution, currently a security consultant for CutAway.

Ero Carrera is currently a reverse engineering automation researcher at Zynamics. Ero spent several years as a Virus Researcher at F-Secure where his main duties ranged from reverse engineering of malware to research in analysis automation methods.

Stephan Chenette is a Principal Security Researcher for Websense Security Labs working on malcode detection techniques. Stephen specializes in research tools and next generation emerging threats, releasing public analyses on various vulnerabilities and malware.

Andrzej Dereszowski is a security consultant and researcher, now focused on analysing targeted threats. He has 6 years of experience as a forensic analyst and incident handler. He works for his own security consulting firm, SIGNAL 11.

Mariano Nuñez Di Croce is the Director of Research and Development at ONAPSIS. Mariano has a long experience as a Senior Security Consultant, involved in security assessments and vulnerability research. He has discovered critical vulnerabilities in SAP, Microsoft, Oracle and IBM applications.

Raoul D'Costa is a Technical Manager at 3M's Security and Safety Systems Division and is responsible for the development and management of the PKI range of products for inspecting biometric passports. Professional interests include PKI, usability and security, RFID enabled ID cards and biometrics.

Thai Duong is a hacker from Vietnam, currently working as the Chief Security Officer at one of Vietnam's leading commercial banks where he leads the Information Security Department to protect more than 3.5 million customers.

Chris Evans is the author of vsftpd and is a vulnerability researcher. His work includes vulnerabilities in all the major browsers (Firefox, Safari, Internet Explorer, Opera, Chrome); the Linux and OpenBSD kernels; Sun's JDK; and lots of open source packages. He now leads security for Google Chrome.

Eric Filiol is the Head Scientist Officer of the Operational Cryptology and Operational Computer Virology Lab at the French Army Signals Academy in Rennes and at the ESIEA Engineer Academy in Laval, France.

FX runs Recurity Labs, a security consulting and research company in Berlin, Germany. FX has over 11 years experience in the computer industry, nine of them in consulting for large enterprise and telecommunication customers.

Thanassis Giannetsos has been working with Algorithms and Security group in Athens Information Technology (AIT), Greece, as a research engineer since 2008; his research interests include wireless security and privacy, design of intrusion detection and routing protocols of sensor networks, embedded systems and distributed computing.

Joe Grand is an electrical engineer, hardware hacker, and president of Grand Idea Studio, Inc. (www.grandideastudio.com), where he specializes in the invention, design, and licensing of consumer products and modules for electronics hobbyists, and has spent over a decade finding security flaws in hardware devices and educating engineers on how to increase the security of their designs.

Wendel G. Henrique is a Security Consultant at Trustwave's SpiderLabs, the advanced security team within Trustwave focused on forensics, ethical hacking, and application security testing for premier clients. He has worked with IT since 1997, with a specific focus on security for the last 8 years.

Vincenzo Iozzo is a student at the Politecnico di Milano where he does some research regarding malware and IDS. He is involved in a number of open source projects, including FreeBSD due to Google Summer of Code. He works as a reverse engineer for Zynamics GmbH.

Brian Karney: COO of AccessData Corporation, his technical expertise and broad-based business knowledge in forensics, incident response, enterprise security management, and eDiscovery make him an integral part of the AccessData team.

Max Kelly joined facebook in 2005 where he built the security organization from the ground up and served as CSO until January 2010. Currently, as director of security strategy, he now spends his time breaking facebook and catching those that try.

Haifei Li is a Senior Vulnerability Researcher at Fortinet (Canada) Inc. He mainly focuses on researching new technologies for vulnerability exploitation and discovery (has discovered 30+ major vulnerabilities so far).

David Lindsay is a Security Consultant with Cigital. His primary areas of interest include web application vulnerabilities, cryptography and web standards. His primary area of disinterest is writing bios.

Guillaume Lovet is currently the Sr Manager of Fortinet's EMEA Threat Response Center, based in Sophia Antipolis, France. Involved in research activities and member of antivirus, threats, and incidents information exchange networks.

Moxie Marlinspike does research with the Institute For Disruptive Studies. He holds a 50 Ton Master Mariner's license.

Daniel Mende is a German security researcher specialized on network protocols and technologies. He's well known for his Layer2 extensions of the SPIKE and Sulley fuzzing frameworks and has presented on protocol security at many occasions including Troopers08, CCC Easterhegg, IT Underground/Prague and ShmooCon.

Steve Ocepek is a Senior Security Consultant at Trustwave's SpiderLabs, the advanced security team within Trustwave focused on forensics, ethical hacking, and application security testing for premier clients.

Christian Papathanasiou is a Information Security consultant for Trustwave Spiderlabs. SpiderLabs is the advanced security team at Trustwave responsible for incident response, penetration testing and application security tests for Trustwave's clients.

Tomislav Pericin has been analyzing and developing software packing and protection methods for the last 7 years. He is author of the book "the Art of Reversing" and founder of the commercial software protection project RLPack. Recently he spoke at Black Hat and TechnoSecurity Conferences.

Enno Rey is a long time network geek with extensive knowledge in the protocol and device security space. Some people like to play with model railways, some with toys from Cupertino... likes to play with high end network equipment.

Juliano Rizzo: For more than a decade Juliano has been working on vulnerability research, reverse engineering and development of high quality exploits. As a researcher he has published various security advisories, papers and proof of concept tools. He is one of the founders and designers of Netifera, an open source platform for network security tools.

Manish Saindane is a security evangelist with over 6 years experience in Application Security. He has been actively involved in designing application security processes and secure SLDC for major companies across all verticals. Saindane is currently working for a well know international Telecom Software/Service provider. In his free time he likes to research new techniques in performing application security assessments.

Peter Silberman works at MANDIANT on the product development team. For a number of years, Peter has specialized in offensive and defensive kernel technologies, reverse engineering, and vulnerability discovery. He enjoys automating solutions to problems both in the domain of reverse engineering and rootkit analysis.

Paul Stone is a Security Consultant, currently working at Context Information Security in the UK, where he performs penetration testing, tool development and security research. He has five years experience in software development and now specializes on web application and browser security.

Christopher Tarnovsky runs Flylogic Engineering, LLC and specializes in analysis of semiconductors from a security "how strong is it really" standpoint. Flylogic offers detailed reports on substrate attacks which define if a problem exists.

Roelof Temmingh has been working in the security industry for 15 years. In 2000 he co-founded SensePost as technical director and later headed up the research and development section. During this time he developed many successful security assessment tools (such as Wikto and Suru), contributed to several books (such as Aggressive Network Self-Defense, How to own a continent, Nessus Network Auditing).

Julien Tinnes enjoys both designing and breaking the security aspects of complex systems, and before joining Google, worked for one of the biggest telecoms company as a security engineer and technical project manager.

Eduardo Vela Nava: By day, Eduardo worked for a couple of the biggest internet companies as a security engineer. By night, he discovered (and reported... mostly) all types of vulnerabilities, for Symantec, Oracle, Microsoft, Google, Mozilla, and some others (for fun, and learning purposes).

Mario Vuksan is an independent security researcher. He was the Director of Research at a leading provider of application and device control solutions, where he has founded and built the world's largest collection of actionable intelligence about software.

Xu (Kyle) Yang (CCIE#19065) is a senior reversing engineer/malware researcher at Fortinet Technologies for 6 years. He's currently focused on Malware Custom Packer Researching, Botnet Researching, Malware Behavior Researching, Reverse Engineering, and Network Security.

day1: APRIL 14

08:00 - 08:50	REGISTRATION & CONTINENTAL BREAKFAST - *PALAU DE CONGRESSOS DE CATALUNYA, HALL 1*		
08:50 - 09:00	INTRODUCTION: *Jeff Moss, Founder & Director, Black Hat* - *PALAU DE CONGRESSOS DE CATALUNYA, H3+J*		
09:00 - 09:50	INTRODUCTION: *Max Kelly, CSO - Facebook // Security: The Facebook Way* - *PALAU DE CONGRESSOS DE CATALUNYA, H3+J*		
TRACK	BIG PICTURE 1	APPLICATION SECURITY 2	HARDWARE 3
LOCATION	PALAU DE CONGRESSOS DE CATALUNYA: H3+J	PALAU DE CONGRESSOS DE CATALUNYA: H2	PALAU DE CONGRESSOS DE CATALUNYA: H1
09:50 - 10:00	+ break		
10:00 - 11:15	CYBER [CRIME | WAR]: *Charting Dangerous Waters* ***Iftach Ian Amit***	DEFENDING THE POOR ***FX***	HARDWARE IS THE NEW SOFTWARE ***Joe Grand***
11:15 - 11:30	+ coffee service		
11:30 - 12:45	UNVEILING MALTEGO 3.0 ***Roelof Temmingh***	SECURITY IN DEPTH FOR LINUX SOFTWARE ***Julien Tinnes & Chris Evans***	HACKING THE SMARTCARD CHIP ***Christopher Tarnovsky***
12:45 - 13:45	+ lunch // HOTEL REY JUAN CARLOS - JARDIN ROOM		
13:45 - 15:00	FIRESHARK - A TOOL TO LINK THE MALICIOUS WEB ***Stephan Chenette***	NEXT GENERATION CLICKJACKING ***Paul Stone***	VERIFYING EMRTD SECURITY CONTROLS ***Raoul D'Costa***
15:00 - 15:15	+ break		
15:15 - 16:30	PROTOCOL, MECHANISM & ENCRYPTION OF PUSHDO/CUTWAIL/ WEBWAIL BOTNET ***Kyle Yang***	SAP BACKDOORS: *A Ghost At The Heart Of Your Business* ***Mariano Nuñez Di Croce***	SCADA AND ICS FOR SECURITY EXPERTS: *How to Avoid Being a Cyber Idiot* ***James Arlen***
16:30 - 16:45	+ coffee service		
16:45 - 18:00	STATE OF MALWARE: *Family Ties* ***Peter Silberman & Ero Carrera***	ATTACKING JAVA SERIALIZED COMMUNICATION ***Manish Saindane***	HACKING CISCO ENTERPRISE WLANS ***Enno Rey & Daniel Mende***
18:00 - 19:30	+ reception // PALAU DE CONGRESSOS DE CATALUNYA - HALL 1		

day2: APRIL 15

TRACK	EXPLOIT 1	APPLICATION SECURITY 2	FORENSICS / PRIVACY 3
LOCATION	HOTEL REY JUAN CARLOS MARE NOSTRUM: A+B	HOTEL REY JUAN CARLOS MARE NOSTRUM: C	HOTEL REY JUAN CARLOS MARE NOSTRUM: D
09:00 - 10:00	REGISTRATION & CONTINENTAL BREAKFAST - *HOTEL REY JUAN CARLOS, MEZZANINE LEVEL*		
10:00 - 11:15	BINDING THE DAEMON: *FreeBSD Kernel Stack & Heap Exploitation* ***Patroklos Argyroudis***	PRACTICAL CRYPTO ATTACKS AGAINST WEB APPLICATIONS ***Thai Duong & Juliano Rizzo***	MISUSING WIRELESS ISPS FOR ANONYMOUS COMMUNICATION ***Andre Adelsbach***
11:15 - 11:30	+ coffee service		
11:30 - 12:45	ACCEPTING ADOBE READER'S CUSTOM MEMORY MANAGEMENT: *A Heap Of Trouble* ***Haifei Li & Guillaume Lovet***	ABUSING JBOSS ***Christian Papathanasiou***	HIDING IN THE FAMILIAR: *Steganography and Vulnerabilities in Popular Archives Formats* ***Mario Vuksan, Tomislav Pericin & Brian Karney***
12:45 - 13:45	+ lunch // HOTEL REY JUAN CARLOS - JARDIN ROOM		
13:45 - 15:00	ORACLE, INTERRUPTED: *Stealing Sessions and Credentials* ***Steve Ocepek & Wendel G. Henrique***	HOW TO OPERATIONALLY DETECT AND BREAK MISUSE OF WEAK STREAM CIPHERS *(And Even Block Ciphers Sometimes)* ***Eric Filiol***	TARGETED ATTACKS: *From Being a Victim To Counter Attacking* ***Andrzej Dereszowski***
15:00 - 15:15	+ break		
15:15 - 16:30	0-KNOWLEDGE FUZZING ***Vincenzo Iozzo***	UNIVERSAL XSS VIA IE8S XSS FILTERS ***David Lindsay & Eduardo Vela Nava***	SURVIVING YOUR PHONE: *Protecting mobile communications with Tor* ***Marco Bonetti***
16:30 - 16:45	+ coffee service		
16:45 - 18:00	WEAPONIZING WIRELESS NETWORKS: *An Attack Tool for Launching Attacks Against Sensor Networks* ***Thanassis Giannetsos***	CHANGING THREATS TO PRIVACY: *From TIA to Google* ***Moxie Marlinspike***	VIRTUAL FORENSICS ***Christiaan Beek***

stay connected

RSS:
blackhat.com/BlackHatRSS.xml

TWITTER:
@BlackHatEvents *(real time event updates)*
@BlackHatHQ *(the staff at Black Hat)*

FACEBOOK:
facebook.com/blackhat

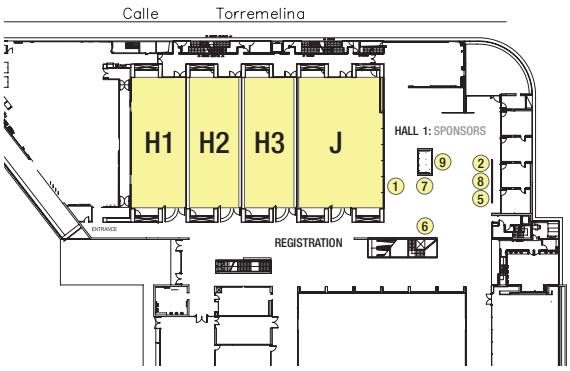
LINKED.IN:
search groups, Black Hat

upcoming events

briefings & training: **las vegas**
CAESARS PALACE LAS VEGAS, NEVADA
July 24 - 29, 2010

briefings & training: **dc**
HYATT REGENCY CRYSTAL CITY
Jan 16 - 19, 2010

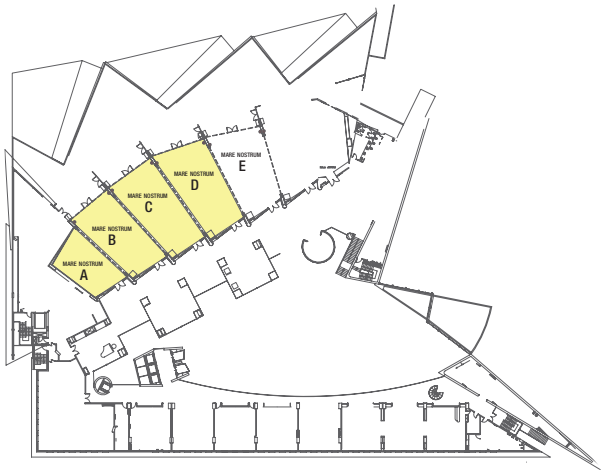
briefings floorplan



PALAU DE CONGRESSOS DE CATALUNYA

SPONSOR TABLE LOCATIONS

1	Core Security Technologies
2	Imperva
5	Norman
6	Qualys
7	SecureWorks
8	Trustwave
9	NetWitness



HOTEL REY JUAN CARLOS – MEZZANINE

SPONSORS

GOLD

CORE SECURITY TECHNOLOGIES
NORMAN
IMPERVA
QUALYS
intel
SecureWorks
Microsoft
Trustwave Information Security & Compliance
NETWITNESS

DAY 1 & 2

LUNCH	Hotel Rey Juan Carlos - Jardin Room

DAY 1 ONLY

THE BIG PICTURE	Palau de Congressos de Catalunya - H3+J
APPLICATION SECURITY	Palau de Congressos de Catalunya - H2
HARDWARE	Palau de Congressos de Catalunya - H1
RECEPTION	Palau de Congressos de Catalunya - Hall 1
SPONSORS	Sponsor Area - Hall 1
BREAKFAST	Palau de Congressos de Catalunya - Hall 1
COFFEE SERVICE	Palau de Congressos de Catalunya - Hall 1

DAY 2 ONLY

EXPLOIT	Hotel Rey Juan Carlos - Mare Nostrum A+B
APPLICATION SECURITY	Hotel Rey Juan Carlos - Mare Nostrum C
FORENSICS / PRIVACY	Hotel Rey Juan Carlos - Mare Nostrum D
BREAKFAST	Hotel Rey Juan Carlos - Mezzanine