



SANS Top-20 Internet Security Attack Targets Atualização Anual de 2006

Versão 7.0 15 de Novembro de 2006

Copyright © 2006, SANS Institute

Questões / comentários podem ser direcionados para top20@sans.org.

Para links para a lista Top 20 use o logo "SANS Top 20 List" logo

Introdução

Há seis anos atrás SANS Institute e National Infrastructure Protection Center (NIPC) do FBI lançaram um documento resumando as Dez Vulnerabilidades de Segurança Mais Críticas da Internet. Milhares de organizações confiaram naquela lista e nas listas expandidas Top-20 que seguiram nos anos seguintes para priorizar seus esforços de maneira que eles pudessem fechar primeiro os buracos de segurança mais perigosos. Os serviços vulneráveis que levaram a worms como Blaster, Slammer e Code Red estiveram nas listas SANS.

A lista SANS Top-20 não é "acumulativa." Nós listamos apenas vulnerabilidades críticas do último ano. Se você não aplicou "patches" em seus sistemas por muito tempo é altamente recomendado que você também elimine as vulnerabilidades listadas no Top-20 2005 assim como as listadas na lista de 2006. Ao final deste documento você encontrará um curto FAQ (Frequently Asked Questions) do SANS Top-20 que responde a perguntas que você pode ter sobre o projeto e sobre a maneira como a lista é criada.

O SANS Top-20 2006 é uma lista de consenso de vulnerabilidades que requerem correção imediata. Ela é o resultado de um processo que reuniu diversos dos principais especialistas em segurança. Elas vem das agências governamentais mais conscientes sobre segurança do Reino Unido, Estados Unidos e Cingapura; dos principais fornecedores de software de segurança e empresas de consultoria em segurança; dos maiores programas de segurança de universidades; do Internet Storm Center e de muitas outras organizações de usuários. Uma lista de participantes está ao final deste documento.

A lista SANS Top-20 é um documento vivo. Ela inclui instruções passo a passo e apontadores para informações adicionais que são úteis na correção de falhas de segurança. Vamos atualizar a lista e as instruções à medida que mais ameaças críticas e métodos de proteção forem identificados, sua contribuição é bem-vinda. Este é um documento que é resultado do consenso da comunidade -- sua experiência em lutar contra os atacantes e em eliminar as vulnerabilidades pode ajudar outros no futuro. Por favor envie sugestões por e-mail para top20@sans.org

Sistemas Operacionais

- W1. Internet Explorer
- W2. Bibliotecas Windows
- W3. Microsoft Office
- W4. Serviços Windows
- W5. Fraquezas de Configuração do Windows
- M1. Mac OS X
- U1. Fraquezas de Configuração do UNIX

Aplicações de Múltiplas Plataformas

- C1 Aplicações Web
- C2. Software de Base de Dados
- C3. Aplicações de Compartilhamento de Arquivos P2P
- C4. Mensagens Instantâneas
- C5. Tocadores Multimídia
- C6. Servidores DNS
- C7. Software de Backup
- C8. Servidores de Segurança, Corporativos e de Gerenciamento de Diretório

Dispositivos de Rede

- N1. Servidores e Telefones VoIP
- N2. Fraquezas de Configuração de Dispositivos de Rede e Outros Dispositivos Comuns

Política de Segurança e Pessoal

- H1. Direitos Excessivos de Usuário e Dispositivos Não Autorizados
- H2. Usuários (Phishing/Phishing Direcionado)

Seção Especial

- Z1. Ataques Zero Day Attacks e Estratégias de Prevenção

W1. Internet Explorer

W1.1 Descrição

Microsoft Internet Explorer é o navegador mais popular usado para navegar na Web e é instalado por padrão em cada sistema Windows. Versões sem correção ou mais antigas do Internet Explorer contém múltiplas vulnerabilidades que podem levar a memória corrompida, forjamento e execução de scripts arbitrários. Os problemas mais críticos são aqueles que levam à execução remota de código sem a necessidade de qualquer interação do usuário quando este visita uma webpage maliciosa ou lê uma mensagem. Código para exploração (exploit) de muitas das falhas críticas do Internet Explorer são disponíveis publicamente. Além disso, Internet Explorer tem sido usado para explorar vulnerabilidades em outros componentes do núcleo do Windows, tais como HTML Help e Graphics Rendering Engine. Vulnerabilidades em controles ActiveX instalados pela Microsoft ou por outros fornecedores de software também estão sendo exploradas por meio do Internet Explorer.

Estas falhas tem sido amplamente exploradas para a instalação de spyware, adware e outros malware em sistemas de usuários. As falhas de forjamento tem sido alavancadas para na condução de ataques de phishing. Em muitos casos, as vulnerabilidades foram zero-days, ou seja, nenhuma correção estava disponível no momento em que as vulnerabilidades foram divulgadas publicamente. A vulnerabilidade **zero-day** no VML, corrigida pela Microsoft na correção MS06-055, foi amplamente explorada por websites maliciosos antes que o patch estivesse disponível.

Durante o último ano a Microsoft lançou múltiplas atualizações para Internet Explorer.

- Vulnerability in Vector Markup Language Could Allow Remote Code Execution ([MS06-055](#))
- Cumulative Security Update for Internet Explorer ([MS06-042](#))
- Vulnerability in Microsoft JScript Could Allow Remote Code Execution ([MS06-023](#))
- Cumulative Security Update for Internet Explorer ([MS06-021](#))
- Cumulative Security Update for Internet Explorer ([MS06-013](#))
- Cumulative Security Update for Internet Explorer ([MS06-004](#))
- Cumulative Security Update for Internet Explorer ([MS05-054](#))

Observe que a atualização acumulativa mais recente para o Internet Explorer inclui todas as atualizações acumulativas anteriores.

Embora [MS06-051](#) seja um patch para o kernel do Windows ele é importante para o Internet Explorer; sem este patch, uma vulnerabilidade de negação de serviço no Internet Explorer pode ser explorada para a execução de código arbitrário.

W1.2 Sistemas Operacionais Afetados

Internet Explorer 5.x e 6.x rodando em Windows 98/ME/SE, Windows NT Workstation e Server, Windows 2000 Workstation e Server, Windows XP Home e Professional e Windows 2003 são todos potencialmente vulneráveis.

W1.3 Entradas CVE

[CVE-2005-2831](#), [CVE-2006-0020](#), [CVE-2006-1185](#), [CVE-2006-1186](#), [CVE-2006-1188](#), [CVE-2006-1189](#), [CVE-2006-1245](#), [CVE-2006-1303](#), [CVE-2006-1313](#), [CVE-2006-1359](#), [CVE-2006-1388](#), [CVE-2006-2218](#), [CVE-2006-2382](#), [CVE-2006-2383](#), [CVE-2006-3450](#), [CVE-2006-3451](#), [CVE-2006-3637](#), [CVE-2006-3638](#), [CVE-2006-3639](#), [CVE-2006-3873](#), [CVE-2006-4868](#)

W1.4 Como Determinar Se Você Está em Risco

Use qualquer vulnerability scanner para verificar se seus sistemas sofreram correção contra estas vulnerabilidades. Você também pode considerar usar Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) ou Systems Management Server ([SMS](#)) para verificar o estado da aplicação de correções em seus sistemas.

W1.5 Como se Proteger Contra Estas Vulnerabilidades

- Se você está usando Internet Explorer em seu sistema a melhor maneira de permanecer seguro é o upgrade para Windows XP Service Pack 2. A melhor segurança do sistema operacional e o Windows Firewall ajudarão a mitigar riscos. Para aqueles impossibilitados de usar Windows XP com Service Pack 2 é fortemente recomendado que se use outro navegador.
- Também é recomendado o upgrade para a versão 7 do Internet Explorer, que fornece segurança melhorada em comparação com versões anteriores. A versão mais recente do Internet Explorer, IE7, está sendo distribuída pela Microsoft como uma Atualização Crítica ([KB926874](#))
- Mantenha os sistemas atualizados com todos os patches mais recentes e service packs. Se possível habilite [Atualizações Automáticas](#) em todos os sistemas.
- Estar sempre alerta a [Microsoft Security Advisories](#) e implementar as mitigações sugeridas antes que a correção esteja disponível pode aliviar a exposição a ataques zero day.
- Para prevenir a exploração de vulnerabilidades de execução de código remoto ao nível de usuário Administrator ferramentas como Microsoft [DropMyRights](#) podem ser usadas para implementar "mínimo de privilégios" para o Internet Explorer.
- Previna a execução de componentes ActiveX vulneráveis dentro do Internet Explorer através do mecanismo "killbit".
- Muitos programas spyware são instalados como Browser Helper Objects. Um Browser Helper Object ou BHO é um pequeno programa que roda automaticamente sempre que o Internet Explorer é iniciado e estende suas funcionalidades. Browser Helper Objects podem ser detectados com scanners Antispyware.
- Use Sistemas de Detecção/Prevenção de Intrusões, Anti-virus, Anti-Spyware e Malware Detection Software para bloquear scripts HTML maliciosos.
- Windows 98/ME/NT não são mais suportados para atualizações. Usuários destes sistemas deveriam considerar o upgrade para Windows XP.
- Considere usar outros navegadores, tais como Mozilla Firefox, que não oferecem suporte à tecnologia ActiveX.

W1.6 Como tornar o Internet Explorer Seguro

Para configuras as definições de Segurança no Internet Explorer:

-
- Selecione "Internet Options", no menu "Tools".
 - Selecione a aba "Security" e depois clique em "Custom Level for the Internet zone".
 - A maioria das falhas no IE são exploradas por Active Scripting e controles ActiveX.
 - Em "Scripting", selecione "Disable for Allow paste operations via script" para prevenir a exposição do seu clipboard (área de transferência). Nota: Desabilitar Active Scripting pode fazer com que alguns web sites não funcionem de maneira apropriada. Controles ActiveX não são tão populares, mas são potencialmente mais perigosos uma vez que permitem maior acesso ao sistema.
 - Selecione "Disable" para "Download signed and unsigned ActiveX Controls". Selecione também "Disable" para "Initialize and script ActiveX Controls not marked as safe".
 - Applets Java normalmente tem mais funcionalidades do que scripts. Sob Microsoft VM, selecione "High safety for Java permissions" para prevenir o acesso privilegiado de applets Java ao seu sistema.
 - Em "Miscellaneous" selecione "Disable" para "Access to data sources across domains" para evitar ataques de Cross-site scripting.
 - Garanta que nenhum site não confiável esteja em "Trusted sites" ou "Local intranet zones", uma vez que estas zonas tem definições de segurança mais fracas que as demais zonas.

W1.7 Referências

Atualizações de Segurança do Internet Explorer

- <http://www.microsoft.com/technet/security/Bulletin/MS06-055.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=38#widely1>
- <http://www.microsoft.com/technet/security/Bulletin/MS06-042.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=32#widely2>
- <http://www.microsoft.com/technet/security/bulletin/MS06-023.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=24#widely5>
- <http://www.microsoft.com/technet/security/bulletin/MS06-021.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=24#widely1>
- <http://www.microsoft.com/technet/security/Bulletin/MS06-013.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=12#widely1>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=11#widely4>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=12#widely1>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=15#widely1>
- <http://www.microsoft.com/technet/security/Bulletin/MS06-004.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=6#widely1>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely2>
- <http://www.microsoft.com/technet/security/Bulletin/MS05-054.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=50#widely1>

US-CERT Securing Web Browser Information

- http://www.us-cert.gov/reading_room/securing_browser/browser_security.html

[top^](#)

W2. Bibliotecas Windows

W2.1 Descrição

As bibliotecas do Windows são módulos que contêm funções e dados que podem ser usados por outros módulos, tais como aplicações Windows. Aplicações Windows normalmente fazem uso de um grande número destas bibliotecas, freqüentemente empacotadas como arquivos dynamic-link library (DLL) para conduzir suas funções. Estas bibliotecas normalmente tem a extensão de arquivo DLL ou OCX (para bibliotecas contendo controles ActiveX).

DLLs fornecem uma maneira de modularizar as aplicações de modo que suas funcionalidades podem ser atualizadas e reutilizadas facilmente. DLLs também ajudam a reduzir o overhead de memória quando muitas aplicações usam a mesma funcionalidade ao mesmo tempo. Estas bibliotecas são usadas para muitas tarefas comuns tais como verificação de código HTML, decodificação de formatos de imagem e decodificação de protocolos. Tanto aplicações locais quanto remotas usam estas bibliotecas. Assim, uma vulnerabilidade crítica em uma biblioteca geralmente causa impacto em uma grande gama de aplicações da Microsoft e de terceiros que fazem uso daquela biblioteca. Freqüentemente a exploração é possível por meio de múltiplos vetores de ataque. Por exemplo, falhas em bibliotecas de processamento de imagens podem ser exploradas por meio do Internet Explorer, Office e visualizadores de imagens. Na maioria dos casos as bibliotecas são usadas por todos os sabores de sistemas operacionais Windows, o que aumenta o número de sistemas disponíveis para ataques.

Durante o último ano muitas bibliotecas Windows foram reportadas como portadoras de vulnerabilidades críticas. Em diversos casos códigos de exploração (exploits) foram descobertos antes que correções estivessem disponíveis (**zero-day**).

Em Dezembro de 2005 uma vulnerabilidade (CVE-2005-4560) foi reportada na Graphics Rendering Engine: ao manipular imagens Windows Metafile (WMF) especialmente montadas é possível fazer com que código arbitrário seja executado. Muitos exploits maliciosos e malware foram descobertos se espalhando pela Internet logo depois da descoberta da vulnerabilidade. Uma vez que esta vulnerabilidade pode ser explorada pela simples visualização de um arquivo de imagem WMF malicioso (por websites ou arquivos anexos), muitas aplicações foram reportadas como afetadas. Até algumas das versões de Lotus Notes foram reportadas como afetadas por este exploit zero-day no WMF. Não havia patch disponível até meados de Janeiro de 2006. Detalhes sobre esta vulnerabilidade podem ser encontrados em: <http://isc.sans.org/diary.php?storyid=993>.

Uma vez que vulnerabilidades em bibliotecas do Windows podem ser exploradas por diversos vetores, em muitos casos um atacante remoto precisará apenas persuadir um usuário a acessar um website especialmente preparado, imagem, ícone ou arquivo de ponteiro de mouse e o atacante seria capaz de executar código arbitrário on sistema daquele usuário, com seus privilégios.

As bibliotecas críticas afetadas durante os últimos anos incluem:

- Vulnerability in Windows Explorer Could Allow Remote Execution ([MS06-057](#), [MS06-015](#)).
- Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution ([MS06-050](#))
- Vulnerability in HTML Help Could Allow Remote Code Execution ([MS06-046](#))
- Vulnerability in Microsoft Windows Could Allow Remote Code Execution ([MS06-043](#))
- Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution ([MS06-026](#), [MS06-001](#))

-
- Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution ([MS06-002](#))

W2.2. Sistemas Operacionais Afetados

Windows NT, Windows 2000, Windows XP, Windows 2003

W2.3. Entradas CVE

[CVE-2005-4560](#), [CVE-2006-0010](#), [CVE-2006-0012](#), [CVE-2006-2376](#), [CVE-2006-2766](#), [CVE-2006-3086](#), [CVE-2006-3357](#), [CVE-2006-3438](#), [CVE-2006-3730](#), [CVE-2006-4868](#)

W2.4. Como Determinar Se Você Está em Risco

- Use qualquer software que faça varredura por vulnerabilidades (vulnerability scanner) para verificar se seus sistemas estão corrigidos contra estas vulnerabilidades. Você pode também considerar o uso do Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) ou Systems Management Server ([SMS](#)) para verificar o estado da aplicação de correções de segurança em seus sistemas.
- Você pode também verificar a presença de um patch pela verificação da chave de registro mencionada na seção "Registry Key Verification" do alerta de segurança correspondente. Além disso, é recomendável também se assegurar de que as versões atualizadas de arquivo mencionadas no alerta estejam instaladas no sistema.

W2.5. Como se Proteger Contra Estas Vulnerabilidades

- Garanta que seus sistemas Windows tenham todas as atualizações de segurança instaladas.
- Bloquear as portas 135-139/tcp, 445/tcp e outras portas usadas por sistemas Windows systems no perímetro de rede. Isto evita que um atacante remoto explore as vulnerabilidades por meio de sistemas de arquivos compartilhados.
- Use a filtragem TCP/IP disponível no Windows 2000 e XP, Windows Firewall em sistemas Windows XP ou qualquer outro firewall pessoal de terceiros para bloquear acessos às portas afetadas partindo de fora do host. É importante que o firewall esteja configurado de maneira apropriada para que o bloqueio contra ataques externos aconteça de maneira efetiva.
- Sistemas de Prevenção/Detecção de Intrusões assim como anti-vírus e softwares de detecção de malware são muito úteis para prover proteção adicional contra malware e exploits que estejam explorando estas vulnerabilidades.
- Se você está executando aplicações de terceiros em plataformas Windows 2000/XP customizadas assegure-se que uma correção apropriada do fornecedor tenha sido aplicada.
- Siga o princípio "Menor Privilégio" (Least Privilege) para limitar o acesso de worms e Trojans em qualquer sistema. Mais detalhes sobre como limitar o acesso a certas chaves do registro, executáveis e diretórios estão disponíveis nos guias NSA em <http://www.nsa.gov/snac/index.cfm?MenuID=scg10.3.1>.
- Use orientações de reforço na segurança de sistemas (tais como aquelas de [CISecurity](#)) para tornar os sistemas mais resistentes a ataques remotos e locais.

-
- Mantenha-se atualizado a respeito de notícias e patches de segurança Microsoft (<http://www.microsoft.com/security/default.aspx>).
 - Devido ao grande número de vetores de ataque seja vigilante ao receber arquivos anexos em e-mail não solicitado e ao navegar em websites desconhecidos. Não clique em links recebidos em e-mail não solicitado, mensagens instantâneas, fóruns web ou canais IRC.
 - Windows NT não é mais suportado. Usuários deveriam realizar upgrade para Windows XP/2003.

W2.6. Referências

Vulnerability in Windows Explorer Could Allow Remote Execution

<http://www.microsoft.com/technet/security/Bulletin/MS06-057.msp>

<http://www.microsoft.com/technet/security/Bulletin/MS06-015.msp>

Vulnerability in Vector Markup Language Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/Bulletin/MS06-055.msp>

Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/bulletin/MS06-050.msp>

<http://www.microsoft.com/technet/security/bulletin/MS05-015.msp>

Vulnerability in HTML Help Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/Bulletin/MS06-046.msp>

<http://www.microsoft.com/technet/security/bulletin/MS05-026.asp>

<http://www.microsoft.com/technet/security/bulletin/MS05-001.asp>

Vulnerability in Microsoft Windows Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/bulletin/MS06-043.asp>

Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/bulletin/MS06-026.asp>

<http://www.microsoft.com/technet/security/bulletin/MS06-001.asp>

<http://www.microsoft.com/technet/security/bulletin/MS05-053.asp>

Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution

<http://www.microsoft.com/technet/security/bulletin/MS06-002.asp>

[top^](#)

W3. Microsoft Office

W3.1 Descrição

Microsoft Office é o suíte de e-mail e produtividade mais utilizado no mundo. As aplicações incluem Outlook, Word, PowerPoint, Excel, Visio, FrontPage e Access. Vulnerabilities nestes produtos podem ser exploradas pelos seguintes vetores de ataque:

- O atacante envia o documento Office malicioso em uma mensagem de e-mail. Virus podem explorar este vetor de ataque.

-
- O atacante hospeda o documento em um servidor web ou pasta compartilhada e induz um usuário a visitar a webpage ou a pasta compartilhada. Note que o Internet Explorer abre documentos Office automaticamente. Assim, visitar uma webpage ou pasta maliciosa é suficiente para a exploração da vulnerabilidade.
 - O atacante executa um servidor de notícias ou seqüestra um feed RSS que envia documentos maliciosos para clientes de e-mail.

Um grande número de falhas críticas em aplicações MS Office foram reportadas no último ano. Além disso, algumas delas ([CVE-2006-5296](#), [CVE-2006-4694](#), [CVE-2006-4534](#), [CVE-2006-3649](#), [CVE-2006-3590](#), [CVE-2006-3059](#), [CVE-2006-2492](#), [CVE-2006-1540](#), [CVE-2006-1301](#)) foram exploradas em estágio **zero-day** quando nenhuma correção do fornecedor estava disponível, o que representa uma tendência em crescimento. Código de exploração e detalhes técnicos são publicamente disponíveis para algumas destas vulnerabilidades.

As falhas críticas no Office e Outlook Express que foram reportadas no último ano são:

- PowerPoint Remote Code Execution Vulnerability ([CVE-2006-5296](#))
- Word Malformed Stack Vulnerability ([MS06-060](#))
- Office and PowerPoint Mso.dll Vulnerability ([MS06-062](#), [MS06-048](#))
- Excel Multiple Remote Code Execution Vulnerabilities ([MS06-059](#))
- PowerPoint Malformed Record Vulnerability ([MS06-058](#))
- Visio, Works and Projects VBA Vulnerability ([MS06-047](#))
- Office Malformed String Parsing Vulnerability ([MS06-038](#))
- Excel Malformed SELECTION record Vulnerability ([MS06-037](#))
- Word Malformed Object Pointer Vulnerability ([MS06-027](#))
- Outlook and Exchange TNEF Decoding Remote Code Execution ([MS06-003](#))

W3.2 Sistemas Operacionais Afetados

Windows 9x, Windows 2000, Windows XP, Windows 2003 são todos vulneráveis dependendo da versão do software Office instalada.

W3.3 Entradas CVE

[CVE-2006-5296](#), [CVE-2006-4694](#), [CVE-2006-4534](#), [CVE-2006-3649](#), [CVE-2006-3590](#), [CVE-2006-3059](#), [CVE-2006-2492](#), [CVE-2006-1540](#), [CVE-2006-1301](#), [CVE-2006-0002](#)

W3.4 Como Determinar Se Você Está em Risco

As instalações de MS Office sem as correções de segurança referenciadas nos Boletins de Segurança listados das entradas NVD (National Vulnerability Database) são vulneráveis. Use qualquer software de varredura de vulnerabilidades (vulnerability scanner) para verificar se seus sistemas estão protegidos contra estas vulnerabilidades. Você pode também considerar usar os serviços do Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) ou Systems Management Server ([SMS](#)) para verificar o nível de aplicação de correções de segurança de seus sistemas.

W3.5 Como se Proteger Contra Vulnerabilidades do Microsoft Office

- Mantenha os sistemas atualizados com todas as correções de segurança mais recentes e service packs. Se possível habilite [Atualizações Automáticas](#) em todos os sistemas.
- [Desabilite](#) o recurso do Internet Explorer que automaticamente abre documentos Office.
- Configure Outlook e Outlook Express com [segurança](#) melhorada.
- Use Sistemas de Prevenção/Detecção de Intrusões e Anti-virus e Software de Detecção de Malware para prevenir a resposta de servidores maliciosos e que documentos maliciosos cheguem a usuários finais.
- Use sistemas de filtragem de mensagens e web no perímetro da rede para prevenir a chegada de documentos Office maliciosos aos sistemas de usuários finais.

W3.6 Referências

Discussões sobre vulnerabilidades Zero-Day no Microsoft Office

<http://blogs.technet.com/msrc/archive/2006/10/12/poc-published-for-ms-office-2003-powerpoint.aspx>

<http://blogs.securiteam.com/?p=508>

http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-081616-2104-99

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FMDROPPER%2EBI&Vsect=T>

<http://blogs.securiteam.com/?p=451>

http://www.symantec.com/security_response/writeup.jsp?docid=2006-051911-0706-99

http://www.symantec.com/security_response/writeup.jsp?docid=2006-051914-5151-99

[top^](#)

W4. Serviços Windows

W4.1 Descrição

A família de sistemas operacionais Windows oferece suporte a uma grande variedade de serviços, métodos e tecnologias de rede. Muitos destes componentes são implementados como Service Control Programs (SCP), sob o controle do Service Control Manager (SCM), que roda como Services.exe. Vulnerabilidades nesses serviços que implementam estas funções do Sistema Operacional são uma das principais avenidas para exploração.

Diversos destes serviços essenciais do sistema oferecem interfaces remotas para componentes de cliente por Remote Procedure Calls (RPC). Eles são em sua maioria expostos por endpoints named, acessíveis pelo protocolo Common Internet File System (CIFS), portas TCP/UDP conhecidas e, em certos casos, portas efêmeras TCP/UDP. Historicamente houve muitas vulnerabilidades em serviços que podem ser explorados por usuários anônimos. Quando exploradas, estas vulnerabilidades dão ao atacante os mesmos privilégios que o serviço tem no host.

Versões anteriores do sistema operacional, especialmente Windows NT e Windows 2000, habilitaram diversos destes serviços por padrão para uma melhor experiência do usuário ao instalar o produto. Estes serviços não essenciais aumentam a superfície de exploração significativamente.

As vulnerabilidades críticas foram reportadas nos seguintes serviços Windows no último ano:

-
- Server Service ([MS06-040](#), [MS06-035](#))
 - iRouting and Remote Access Service ([MS06-025](#))
 - Exchange Service ([MS06-019](#))

Código de exploit está disponível para estas vulnerabilidades. Por exemplo, a vulnerabilidade corrigida pelo hotfix [MS06-040](#) foi explorada pelos worms [W32.Dasher.G](#) e [W32.Spybot.AKNO](#).

W4.2 Sistemas Operacionais Afetados

Windows 2000 Workstation e Server, Windows XP Home e Professional e Windows 2003 são todos potencialmente vulneráveis.

W4.3 Entradas CVE

[CVE-2006-0027](#), [CVE-2006-1314](#), [CVE-2006-2370](#), [CVE-2006-2371](#), [CVE-2006-3439](#)

W4.4 Como Determinar Se Você Está em Risco

- Use qualquer software de varredura de vulnerabilidades (vulnerability scanner) para verificar se seus sistemas estão corrigidos contra estas vulnerabilidades. Você pode também considerar usar os serviços Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) ou Systems Management Server ([SMS](#)) para verificar o estado da aplicação de correções de segurança de seus sistemas.
- Você pode também verificar a presença de uma correção verificando a chave de registro mencionada na seção "Registry Key Verification" do alerta de segurança correspondente. Além disso, é também recomendável ter certeza de que as versões atualizadas dos arquivos mencionados no alerta estejam instaladas no sistema.
- Para verificar se seu sistema está vulnerável a um problema em serviço opcional você precisa determinar se o serviço está habilitado. Isto pode ser feito pela interface "Gerenciador de Serviços", que pode ser chamada de **Serviços** em Ferramentas Administrativas.

W4.5 Como se Proteger Contra Vulnerabilidades nos Serviços Windows

- Mantenha o sistema atualizado com todas as últimas correções e service packs. Se possível habilite [Atualizações Automáticas](#) em todos os sistemas.
- Use Sistemas de Prevenção/Deteção de Intrusões para prevenir/detectar ataques explorando estas vulnerabilidades.
- Em alguns casos a exposição à vulnerabilidade pode ser removida pela desativação do serviço correspondente. Por exemplo, o serviço Windows Routing and Remote Access pode ser desativado na maioria dos ambientes que usam Windows 2000. Para tal, inicie a interface gerenciador de serviço. Localize o serviço requerido e clique com o botão direito do mouse. Chame a opção propriedades no menu popup. O "Startup Type" do serviço pode ser modificado para desabilitar o respectivo serviço.
- Em alguns casos o acesso por sessões nulas (null session) à interface vulnerável pode ser removido como maneira de se contornar o problema. É uma boa prática revisar sua atual

configuração RestrictAnonymous e mantê-la o mais keep it as estrita possível baseado em seu ambiente. <http://www.securityfocus.com/infocus/1352>

- Muitas destas vulnerabilidades são encontradas em interfaces oferecidas pelo CIFS e bloquear as portas 139/tcp e 445/tcp no perímetro é essencial para prevenir ataques remotos. Também é uma boa prática bloquear requisições RPC provenientes da Internet para portas acima de 1024 para bloquear ataques para outras vulnerabilidades baseadas em RPC usando [firewalls](#).
- XP SP2 e Windows 2003 SP1 e R2 vem com várias melhorias de segurança, incluindo o Windows firewall e Security Configuration Wizard (Windows 2003 SP1 e R2 apenas). É altamente recomendável realizar upgrade para estes service packs, habilitar o Windows firewall e reduzir a superfície de ataque com o Security Configuration Wizard.

W4.6 Referências

Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP
<http://www.microsoft.com/technet/security/topics/serversecurity/tcg/tcgch00.msp>

Windows XP Security Guide
<http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.msp>

Windows Server 2003 Security Guide
<http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.msp>

Using Windows Firewall
<http://www.microsoft.com/windowsxp/using/networking/security/winfirewall.msp>

Security Configuration Wizard for Windows Server 2003
<http://www.microsoft.com/windowsserver2003/technologies/security/configwiz/default.msp>

How to use IPSec IP filter lists in Windows 2000
<http://support.microsoft.com/kb/313190>

How to block specific network protocols and ports by using IPSec
<http://support.microsoft.com/kb/813878>

How to configure TCP/IP filtering in Windows 2000
<http://support.microsoft.com/kb/309798>

[top^](#)

W5 Fraquezas de Configuração do Windows

W5.1 Descrição

1. Fraquezas em Senhas Configuradas pelo Usuário

Fraquezas em configurações de senha ganharam importância nos últimos anos com a proliferação de worms, bots e outros malware que melhoraram sua capacidade de propagar a si mesmos pelo abuso de senhas inadequadas. O reforço de senhas complexas é um dos problemas mais antigos que com que os administradores de segurança de TI se deparam mas continua a ser uma praga em empresas ao redor do mundo. Estas fraquezas podem existir tanto no nível do Active Directory quanto no nível local, cada qual

pode ser explorado de maneira efetiva tanto por malware quanto por ameaças internas. Além disso, com o aumento da autenticação centralizada em diversas plataformas o comprometimento de credenciais Windows pode frequentemente levar diretamente ao comprometimento de outras plataformas (UNIX e RACF/ACF2/Top Secret por exemplo). Mesmo que senhas complexas sejam implantadas na vasta maioria de contas da rede uma senha fraca pode levar a um comprometimento muito maior.

2. Senhas de Contas de Serviço

Contas de serviço precisam de senha em Windows. Infelizmente é muito comum usar senhas curtas, imprimíveis para estas contas. Isto é particularmente problemático uma vez que elas são freqüentemente usadas em muitas máquinas, tem alto nível de privilégios e mudam raramente.

3. Log-on Nulo

Credenciais nulas tem sido um problema em ambientes Windows com domínio há muito tempo. Desde a introdução da arquitetura de domínio com Windows NT sessões nulas (null sessions) têm permitido que usuários anônimos enumerem sistemas, compartilhamentos e contas de usuários. Windows 2000 introduziu dois níveis de controle sobre o acesso anônimo; entretanto, este controle foi desabilitado por padrão. Com a introdução do Windows 2003 a Microsoft adicionou diversos controles sobre o acesso anônimo e habilitou algumas restrições por padrão. Entretanto, sistemas legados forçaram muitos ambientes a continuar a oferecer suporte a conexões anônimas.

W5.2 Como se Proteger Contra Fraquezas de Configuração

Senhas Fracas:

- Implante uma política de senhas rígida para todos os usuários do domínio. Esta política deve incluir requerimentos de complexidade e expiração da senha. Considere usar uma ferramenta de terceiros para o gerenciamento das senhas de contas locais, garantindo que as senhas sejam únicas.
- Previna o Windows de armazenar o hash LM hash no Active Directory ou base de dados SAM seguindo as [instruções](#) postadas pela Microsoft.
- Implemente uma política para testar periodicamente as senhas na empresa. Este teste deve incluir o uso de ferramentas automatizadas como [THC Hydra](#), [LophtCrack](#) e [John the Ripper](#) para verificar a existência de senhas em branco e simples/comuns. O teste deve ser realizado em todas as plataformas e não deve ser limitado a senhas de AD (Active Directory).

Null Log-on:

- Restrinja o acesso anônimo a sistemas do domínio. Veja a seção "Referências" para detalhes a respeito do impacto de restrições de sessões nulas e as definições disponíveis em vários cenários.

W5.3 Referências

The Administrator Accounts Security Planning Guide

<http://www.microsoft.com/technet/security/topics/serversecurity/administratoraccounts/default.msp>

Guias de Segurança Windows

<http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.msp>

<http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en>

How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases

<http://support.microsoft.com/kb/299656>

MSRPC NULL sessions - exploitation and protection

http://www.hsc.fr/ressources/presentations/null_sessions/null_sessions_explained.html

Restricting Anonymous Access

<http://technet2.microsoft.com/WindowsServer/en/library/2c82586e-bd58-42b7-9976-228a23721e351033.mspx?mfr=true>

Client, service, and program incompatibilities that may occur when you modify security settings and user rights assignments

<http://support.microsoft.com/kb/823659>

Microsoft policy on third-party security configuration guidance support

<http://support.microsoft.com/kb/885409/en-us>

[top^](#)

M1. Mac OS X

M1.1 Descrição

O Mac OS X é um sistema operacional baseado em BSD da Apple para sua linha de computadores PowerPC- e baseados em Intel.

Para mais informações sobre Mac OS X, veja: <http://www.apple.com/macosex>

O Mac OS X é composto por diversos componentes diferentes. Cada um destes componentes pode potencialmente possuir falhas de segurança. A maioria das falhas críticas descobertas no ano passado enquadraram-se em seis categorias diferentes:

- Safari - O navegador web Safari da Apple é o navegador padrão nas versões recentes do Mac OS X. Vulnerabilidades nesta aplicação podem potencialmente resultar no controle completo do navegador ou na sessão de login do usuário.
- ImageIO - A base do gerenciamento de imagens utilizado pelo sistema e pela maioria das aplicações. Vulnerabilidades neste conjunto de ferramentas pode potencialmente afetar muitas aplicações diferentes. Arquivos de imagens são geralmente considerados arquivos "seguros" por várias aplicações, e por padrão são abertas sem questionamentos.
- Unix - O Mac OS X é baseado e incorpora grandes quantidades de código dos sistemas operacionais Unix-like anteriores. Muitas aplicações escritas para vários sistemas operacionais Unix e Unix-like rodam em Mac OS X e algumas destas aplicações são inseridas como parte do sistema operacional da Apple. Falhas nestas aplicações podem ser corrigidas no Mac OS X com considerável atraso em relação ao fabricante original.
- Wireless - Relatos sobre vulnerabilidades críticas no sub-sistema de rede wireless do Mac OS X capazes de permitir aos atacantes próximos fisicamente obterem o controle completo sobre um

sistema foram recebidos com surpresa por muitos na comunidade de segurança. A natureza da falha permitiu aos atacantes atacarem sistemas mesmo que estes não fossem parte da mesma rede lógica onde o atacante se encontrava. Falhas adicionais foram descobertas no sub-sistema da interface wireless Bluetooth, com resultados similares.

- Vírus/Trojan - Os primeiros vírus e trojans para a plataforma Mac OS X foram descobertos no ano passado.
- Outros - As demais vulnerabilidades não se enquadram em uma categoria bem definida.

Observe que a Apple normalmente distribui correções e atualizações como atualizações de forma geral; uma dada Atualização de Segurança irá incluir tanto atualizações de baixa severidade como atualizações críticas.

M1.2 Indicadores do CVE

Vulnerabilidades no Safari (incluindo zero-days)

HTML Rendering Vulnerabilities - [CVE-2005-3705](#), [CVE-2006-1987](#), [CVE-2006-3505](#), [CVE-2006-3946](#)
Security Bypass Vulnerabilities - [CVE-2005-2516](#), [CVE-2006-0399](#), [CVE-2006-0397](#), [CVE-2006-0398](#).

Vulnerabilidades no ImageIO

Image Format Vulnerabilities - [CVE-2006-1469](#), [CVE-2006-1982](#), [CVE-2005-2747](#)

Vulnerabilidades em Produtos de Terceiros

Inherited Vulnerabilities - [CVE-2006-0384](#)

Vulnerabilidades no Driver Wireless

WiFi Driver Vulnerabilities - [CVE-2006-3509](#), [CVE-2006-3508](#), [CVE-2006-3507](#)

Vírus e Trojans

Viruses and Trojans - [OSX/Leap-A](#) trojan.

Outras Vulnerabilidades

[CVE-2006-3498](#), [CVE-2006-1450](#), [CVE-2006-1449](#), [CVE-2006-0848](#), [CVE-2005-2518](#), [CVE-2006-4394](#)

M 1.3 Como Determinar se Você Está em Risco

Qualquer instalação de Mac OS X padrão ou sem as correções de segurança devem ser presumidas como vulneráveis.

O seguinte procedimento irá checar se existem novos pacotes disponíveis.

1. Escolha System Preferences no Menu da Apple.
2. Escolha Software Update no menu View.
3. Clique em Update Now.
4. Marque os itens disponíveis.

Para auxiliar o processo de descoberta de vulnerabilidades, você pode utilizar um scanner de vulnerabilidades.

M1.4 Como se Proteger Contra Estas Vulnerabilidades

- Tenha certeza de estar atualizado e de ter todas as correções de segurança para os produtos da Apple aplicadas, configurando o Sistema de Atualização de Software (Software Update System) para automaticamente checar por atualizações lançadas pela Apple. Embora diferentes programações sejam possíveis, nós recomendamos que você configure-o para checar por atualizações pelo menos a cada semana. Para mais informações sobre como checar e rodar o Sistema de Atualização de Software, veja a página do Sistema de Atualização de Software (Software Update System) - <http://www.apple.com/macosx/upgrade/softwareupdates.html>
- Para evitar acessos não autorizados à sua máquina, ative o firewall pessoal incluso. Se você possui na sua máquina serviços autorizados rodando que necessitam de acesso externo, certifique-se de permiti-los explicitamente.
- Existem disponíveis muitos guias excelentes para aumentar a segurança do Mac OS X. O [CIS Benchmark](#) para Mac OS X enumera configurações de segurança úteis para aumentar a segurança do Sistema Operacional. As ações sugeridas pelos documentos do CIS Level-1 benchmarks não devem causar nenhuma interrupção nos serviços ou aplicações e são altamente recomendadas a serem aplicadas no sistema. Também, o relatório [Securing Mac OS X 10.4 Tiger](#) examina as funcionalidades e as configurações de segurança do Mac OS X.

[top^](#)

U1. Fraquezas de Configuração do UNIX

U1.1 Descrição

A maioria dos sistemas Unix/Linux inclui um número de serviços padrões em sua instalação original. Estes serviços, mesmo que completamente atualizados, podem ser a causa de comprometimentos não-intencionais. Administradores de segurança conscientes refinam os sistemas desligando serviços desnecessários e/ou ativando um firewall em conexões com a Internet.

Por exemplo uma instalação padrão do Red Hat Enterprise Linux terá serviços como o cups (Common Unix Printing System), portmap (RPC support), sendmail (Mail Transport Agent), e sshd (OpenSSH server) que devem ser desativados se não forem necessários.

De particular interesse temos os **ataques de força bruta contra acessos por comando de linha como SSH, FTP, e telnet**. Estes serviços são frequentemente alvos de ataques devido à prevalescência deles para o acesso remoto. Entretanto, nos dois últimos anos um esforço conjunto tem sido feito pelos atacantes para atacar com força bruta as senhas utilizadas nestas aplicações. De modo crescente, worms e bots têm motores de ataques de força bruta contra senhas incluídas neles. Sistemas com senhas fracas para contas de usuários são comprometidas rapidamente; a escalação de privilégios é utilizada frequentemente para obter o acesso de root, e rootkits são instalados para ocultar o comprometimento. É importante lembrar que ataques de força bruta podem ser usados como uma técnica para comprometer mesmo um sistema completamente atualizado.

Administradores de segurança atentos utilizam SSH como seu método de acesso remoto interativo. Se a versão do SSH é a atual e está completamente corrigida, o serviço é geralmente tido como seguro. Entretanto, independente de quão atualizado e corrigido esteja, ele ainda pode ser comprometido via

ataques de força bruta capazes de adivinhar a senha. Para o SSH é recomendado utilizar o mecanismo de autenticação por chave pública para impedir este tipo de ataque. Para outros serviços interativos, audite as senhas para garantir que elas sejam de complexidade suficiente para resistir a ataques de força bruta.

U1.2 Versões Afetadas

Todas as versões de UNIX/Linux estão potencialmente em risco devido à configurações impróprias ou padrão. Todas as versões de UNIX/Linux podem ser afetadas devido à contas possuindo senhas fracas ou baseadas em palavras de dicionário para a autenticação.

U1.3 Como determinar se você está vulnerável

As instalações padrão (feitas tanto pelos fabricantes quanto por administradores) de sistemas operacionais ou de softwares de rede podem habilitar uma vasta quantidade de serviços desnecessários e inúteis. Em muitos casos, a incerteza sobre as necessidades de um sistema operacional ou uma aplicação leva muitos fabricantes ou administradores a instalar todos os programas no caso deles serem necessários no futuro. Isto simplifica significativamente o processo de instalação, mas também introduz uma grande variedade de serviços não necessários e contas que possuem senhas padrão/fracas ou conhecidas.

O uso de um scanner de vulnerabilidades atualizado ou um scanner de portas pode ser altamente eficaz no diagnóstico de quaisquer vulnerabilidades em potencial deixadas pelas instalações padrão, como serviços e aplicações desnecessárias ou desatualizadas. Da mesma forma, uma ferramenta para quebrar senhas pode ajudá-lo a evitar o uso de senhas fracas, o que dificultaria a adivinhação no caso de ataques de força bruta em serviços remotos.

Atenção: Nunca execute uma ferramenta de quebra de senhas/scanner de vulnerabilidades mesmo em sistemas nos quais você possui acesso root sem uma permissão explícita e preferencialmente por escrito de seu empregador. Administradores com as intenções mais benevolentes possíveis têm sido demitidos por utilizar ferramentas de quebra de senhas sem a devida autorização para fazê-lo.

U1.4 Como se Proteger Contra Estas Vulnerabilidades

Serviços Desnecessários

- Verifique o servidor com um scanner de portas ou ferramenta de análise de vulnerabilidades para determinar quais serviços desnecessários estão rodando no sistema. Desabilite os serviços que não são cruciais às aplicações necessárias.
- Instale regularmente as correções de segurança mais recentes do fabricante para mitigar as vulnerabilidades em serviços expostos. O gerenciamento da aplicação de correções é uma parte crítica do processo de gerenciamento de riscos.
- Utilize as avaliações do "The Center for Internet Security" presentes em www.cisecurity.org para seu SO e serviços que você utiliza. Também considere a utilização do Bastille presente em www.bastille-linux.org para refinar a segurança de hosts baseados em Linux e HP-UX.
- Considere a troca da porta padrão de serviços quando possível. Scanners automáticos tendem a varrer somente as portas padrão.
- Utilize um firewall por hardware ou software para proteger serviços necessários.

-
- Garanta que os serviços estão protegidos por mecanismos de segurança fornecidos pelo fabricante (por exemplo SELinux ou a aleatoriedade do espaço de endereçamento).

Ataques de Força Bruta

- Não utilize senhas padrão em nenhuma conta.
- Imponha uma política de senhas fortes. Não permita senhas fracas ou senhas baseadas em palavras encontradas em dicionários.
- Audite para garantir que sua política de senhas está sendo seguida.
- Limite o número de falhas de tentativas de login aos serviços expostos.
- Limite as contas que podem registrar-se através da rede; a conta de root não deve ser uma delas.
- Empregue as regras do firewall de forma a limitar as origens de logins remotos.
- Proíba contas compartilhadas e não utilize nomes genéricos em contas, como tester, guest, sysadmin, admin, etc.
- Registre as falhas nas tentativas de login. Um grande número de falhas no login em um sistema pode requerer uma checagem futura, para analisar se o sistema foi comprometido.
- Considere a utilização de autenticação baseada em certificados.
- Se seu sistema UNIX permite a utilização de módulos de autenticação PAM, implemente estes módulos de forma a checar a qualidade das senhas.
- Filtre através do firewall serviços que não necessitem de acesso à Internet.

U1.5 Referências

Ataques de Força Bruta contra SSH e Contramedidas

- <http://isc.sans.org/diary.php?storyid=1541>
- <http://isc.sans.org/diary.php?storyid=1491>
- <http://isc.sans.org/diary.php?date=2006-08-01>
- http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1094140,00.html

Fontes Diversas de Segurança em UNIX

- <http://www.cisecurity.org>
- <http://www.bastille-linux.org>
- <http://www.puschitz.com/SecuringLinux.shtml>

[top^](#)

C1 Aplicações Web

C1.1 Descrição

Aplicações como Sistemas de Gerenciamento de Conteúdo (CMS), Wikis, Portais, Bulletin Boards e fóruns de discussão estão sendo utilizados por organizações de grande e pequeno porte. Toda semana, **centenas** de vulnerabilidades nestas aplicações estão sendo reportadas, e estão sendo continuamente exploradas. O número diário de tentativas de ataques em alguns dos grandes centros de hospedagem alcança de **centenas de milhares até milhões de ataques**.

Todos os pacotes de ferramentas de desenvolvimento para web (PHP, .NET, J2EE, Ruby on Rails, ColdFusion, Perl, etc) e todos os tipos de aplicações web possuem o risco de falhas de segurança nas aplicações, que vão desde a validação insuficiente até erros lógicos na aplicação. As vulnerabilidades mais exploradas são:

- **Inclusão remota de arquivos em PHP:** O PHP é a linguagem de aplicação e base de desenvolvimento mais utilizada na web atualmente. Por padrão, o PHP permite às funções de arquivos acessarem recursos na Internet através da funcionalidade chamada "allow_url_fopen". Quando os scripts em PHP permitem aos usuários entrarem com dados que modifiquem nomes de arquivos, podemos ter como resultado a inclusão remota de arquivos. Este ataque permite (mas não é limitado) a :
 - Execução remota de código
 - Instalação remota de rootkits
 - Em Windows, o comprometimento interno do sistema pode ser possível através do uso de arquivos de wrapper SMB do PHP.
- **SQL Injection:** Inserções de código, particularmente de códigos SQL, são muito comuns em aplicações web. As inserções são possíveis devido à mistura de dados fornecidos pelo usuário dentro de consultas dinâmicas ou dentro de procedimentos de armazenamento construídos de forma simplista. As inserções de código SQL permitem aos atacantes:
 - Criar, ler, atualizar ou apagar qualquer dado arbitrário disponível à aplicação
 - No pior cenário, comprometer completamente o sistema de banco de dados e os sistemas próximos a ele
- **Cross-Site Scripting (XSS):** Cross site scripting, também conhecido como XSS, é a falha de segurança mais nociva e facilmente encontrada em aplicações web. O XSS permite aos atacante desfigurarem páginas web, inserirem conteúdo hostil, executarem ataques de phishing, obterem o controle sobre o navegador do usuário através de códigos maliciosos escritos em JavaScript, e forçar os usuários a executar comandos que eles não solicitaram - um ataque conhecido como cross-site request forgeries, também conhecido como CSRF.
- **Cross-site request forgeries (CSRF):** O ataque por CSRF obriga usuários legítimos a executarem comandos sem seu consentimento. A prevenção contra este tipo de ataque é extremamente difícil de ocorrer, a menos que a aplicação esteja livre de vetores de cross-site scripting, incluindo inserções DOM (DOM injections). Com o aumento de técnicas Ajax, e um melhor conhecimento de como explorar corretamente os ataques XSS, os ataques por CSRF estão se tornando extremamente sofisticados, tanto em um ataque individual como em um worm automatizado, como o Samy MySpace Worm.
- **Directory Traversal:** Directory traversal (acesso a arquivos através de ".." ou muitas variantes codificadas) permite aos atacantes acessarem recursos controlados, como arquivos de senhas, arquivos de configuração, credenciais a bancos de dados ou outros arquivos da escolha do atacante.

C1.2 Como Determinar se Você Está em Risco

Ferramentas de scan de páginas web podem ajudá-lo a encontrar estas vulnerabilidades, particularmente se elas possuem erros conhecidos. Entretanto, para encontrar todas as potenciais vulnerabilidades é

necessário proceder com uma revisão no código fonte. Isto deve ser realizado pelos desenvolvedores anteriormente ao lançamento do produto.

Inspecione a configuração de sua base de desenvolvimento web e refine-a apropriadamente.

Os administradores de sistemas devem considerar a execução de análises (scans) periódicas em seus servidores web com ferramentas de análise de vulnerabilidades, particularmente caso eles executem uma grande diversidade de scripts fornecidos por usuários, como uma empresa de hospedagem. É impraticável aos administradores de sistemas executarem testes de penetração detalhados.

C1.3 Como Proteger-se contra Vulnerabilidades em Aplicações Web

Da perspectiva de administradores de sistemas PHP e da hospedagem:

- Atualize para o PHP 5.2 pois ele elimina muitas das falhas de segurança latentes do PHP e permite APIs mais seguras, como a PDO
- Sempre teste e instale as correções e novas versões do PHP conforme forem sendo lançadas
- A freqüente auditoria em servidores web é recomendada em ambientes nos quais uma grande quantidade de aplicações PHP estão em uso
- Considere a utilização das seguinte configuração para o PHP:
 - register_globals (deve estar como off, vai gerar falhas em aplicativos inseguros)
 - allow_url_fopen (deve estar como off, vai gerar falhas em aplicativos que necessitam desta funcionalidade, mas vai proteger contra um vetor de exploração bastante ativo)
 - magic_quotes_gpc (deve estar como off, vai gerar falhas em aplicativos inseguros mais antigos)
 - open_basedir (deve estar ativo e corretamente configurado)
 - Considere a utilização de funcionalidades que permitam a execução com menores privilégios como PHPsuexec ou suPHP
 - Considere a utilização do Suhosin para controlar o ambiente de execução de scripts em PHP
- Utilize Sistemas de Detecção/Prevenção de Intrusão para bloquear/alertar no caso de solicitações HTTP maliciosas. Considere a utilização do mod_security do PHP para bloquear ataques conhecidos contra o PHP
- Como último recurso, considere a proibição de aplicativos que possuam histórico de exploração em curso, e reduza o tempo de resposta para a correção de falhas de segurança.

Da perspectiva do desenvolvedor:

- Se você utiliza PHP, migre sua aplicação para PHP 5.2 em caráter de urgência.
- Para evitar os problemas na codificação acima descritos:
 - Desenvolva com a última versão do PHP e com uma configuração reforçada (veja acima)
 - Valide todas as entradas de dados apropriadamente
 - Codifique todas as saídas de dados utilizando htmlentities() ou um mecanismo similar para evitar ataques de XSS
 - Migre sua camada de dados (data layer) para PDO - não utilize a velha forma com funções mysql_*() que são consideradas falhas
 - Não utilize dados fornecidos por usuários em funções de arquivos para evitar ataques de inclusão remota de arquivos

-
- Afilie-se a organizações com fins de codificação segura, como a OWASP (veja referências) para melhorar sua técnica e aprender sobre programação segura
 - Teste seus aplicativos utilizando o "OWASP Testing Guide" com ferramentas como WebScarab, Firefox's Web Developer Toolbar, Greasemonkey e o XSS Assistant

C1.4 Referências

OWASP - Open Web Application Security Project

<http://www.owasp.org>

OWASP Testing Guide

http://www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents

OWASP Guide - a compendium of secure coding

http://www.owasp.org/index.php/Category:OWASP_Guide_Project

OWASP Top 10 - Top 10 web application security weaknesses

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Suhosin, a Hardened PHP project to control the execution environment of PHP applications

<http://www.hardened-php.net/suhosin/>

PHP Security Features

<http://php.net/features.safe-mode>

[top^](#)

C2. Software de Bases de Dados

C2.1 Descrição

Bases de dados são um elemento chave em muitos sistemas de armazenagem, procura ou manipulação de grandes quantidades de dados. Elas são encontradas em praticamente todos os segmentos de negócios, finanças, bancos, relacionamento com clientes e aplicações de monitoração de sistemas.

Devido ao valor da informação que elas armazenam como dados pessoais ou financeiros, as bases de dados são frequentemente alvos de ataque e são de interesse peculiar aos ladrões de identidade. Os sistemas de banco de dados são frequentemente bastante complexos, combinando a base de dados com um conjunto de aplicações; algumas fornecidas pelo fabricante da base de dados, outras escritas pela própria equipe (como aplicações web). Uma falha em qualquer um destes componentes pode comprometer todos os dados armazenados. As vulnerabilidades mais comuns em sistemas de bancos de dados podem ser classificadas como:

- O uso de configurações padrão com nomes de usuários e senha padrão
- Buffer overflows em processos que escutam portas TCP/UDP bem conhecidas.
- SQL Injection via ferramentas da própria base de dados ou por personalizações na interface web inseridas pelos próprios usuários.
- Uso de senhas fracas em contas privilegiadas.

Existem muitos diferentes sistemas de bases de dados disponíveis. Alguns dos mais comuns são Microsoft SQL Server (proprietário, roda em Windows), Oracle (proprietário, roda em diversas plataformas), IBM DB2 e IBM Informix (ambos proprietários, rodam em diversas plataformas), Sybase (proprietário, roda em diversas plataformas), MySQL e PostgreSQL (ambos de código aberto e disponíveis para diversas plataformas).

Todos os sistemas de banco de dados relacionais modernos são endereçáveis através de portas, o que significa que qualquer pessoa com ferramentas de consultas em bancos prontas pode tentar se conectar diretamente à base de dados, transpondo os mecanismos de segurança utilizados pelo sistema operacional. As conexões padrão frequentemente utilizadas são: Microsoft SQL via TCP porta 1433 e UDP porta 1434, Oracle via TCP porta 1521, IBM DB2 via portas 523 e da 50000 em diante, IBM Informix via TCP portas 9088 e 9099, MySQL via TCP porta 3306, e PostgreSQL via TCP porta 5432.

Exploits na forma Prova de Conceito (Proof of concept) para muitas falhas em bases de dados são rapidamente disponibilizados na Internet. Devido às conexões de rede que eles permitem, os bancos de dados podem sofrer com worms. O mais infame destes foi o [SQL Slammer worm](#), em 2003. Em 2005 vimos a aparição do primeiro worm para Oracle: "[Voyager](#)". Enquanto este não trazia uma carga capaz de causar muitos danos, ele demonstrou o que poderia ser feito caso uma base de dados Oracle não estivesse protegida.

Além do relato das vulnerabilidades específicas mencionadas aqui, os administradores preocupados com a segurança dos bancos de dados deveriam considerar:

- O impacto de padrões como o [Payment Card Industry Data Security Standard](#) que pode exigir a encriptação de algumas informações, como números de cartões de crédito.
- Os riscos de transferir grandes quantidades de dados em equipamentos móveis: no último ano houve inúmeros casos de dados pessoais sendo perdidos devido ao roubo de laptops.

C2.2 Sistemas Operacionais Afetados

A maioria das bases de dados, comerciais e de código aberto, rodam em plataformas múltiplas. As falhas se aplicam a todas as plataformas suportadas.

C2.3 Entradas CVE

Estes são os indicadores divulgados desde Outubro de 2005. Vulnerabilidades anteriores podem ser encontradas em edições anteriores das listas de vulnerabilidades do SANS. Em muitos casos os problemas notificados não são falhas nos bancos de dados propriamente ditos, mas em aplicações desenvolvidas ao seu redor, por exemplo, inserção de código SQL em interfaces web; estes não foram incluídos aqui.

Oracle

[CVE-2005-3641](#), [CVE-2006-0256](#), [CVE-2006-0257](#), [CVE-2006-0258](#), [CVE-2006-0259](#), [CVE-2006-0260](#), [CVE-2006-0261](#), [CVE-2006-0262](#), [CVE-2006-0263](#), [CVE-2006-0265](#), [CVE-2006-0266](#), [CVE-2006-0267](#), [CVE-2006-0268](#), [CVE-2006-0269](#), [CVE-2006-0270](#), [CVE-2006-0271](#), [CVE-2006-0272](#), [CVE-2006-0282](#), [CVE-2006-0283](#), [CVE-2006-0285](#), [CVE-2006-0286](#), [CVE-2006-0287](#), [CVE-2006-0290](#), [CVE-2006-0291](#), [CVE-2006-0435](#), [CVE-2006-0547](#), [CVE-2006-0548](#), [CVE-2006-0549](#), [CVE-2006-0551](#), [CVE-2006-0552](#),

[CVE-2006-0586](#), [CVE-2006-1868](#), [CVE-2006-1871](#), [CVE-2006-1872](#), [CVE-2006-1873](#), [CVE-2006-1874](#), [CVE-2006-3698](#).

Note: Esta lista se baseia nos programas base da base de dados Oracle. Existem vulnerabilidades em outras aplicações que são parte do pacote Oracle. A Oracle divulga quadrimestralmente Atualizações com Correções Críticas (Critical Patch Updates - CPU) cobrindo um grande número de falhas nas bases de dados e aplicações associadas. A recomendação padrão é trabalhar com estas CPUs. Devido à maneira como a Oracle divulga as informações durante este período de notificações, muitos indicadores CVE podem estar relacionados a um mesmo problema.

MySQL

[CVE-2006-2753](#).

PostgreSQL

[CVE-2006-2313](#), [CVE-2006-2314](#).

IBM DB2

[CVE-2005-3643](#), [CVE-2005-4737](#).

IBM Informix

[CVE-2005-3642](#), [CVE-2006-3854](#), [CVE-2006-3860](#), [CVE-2006-3862](#).

Microsoft SQL Server

Nenhum indicador durante o período deste relatório.

Sybase

Nenhum indicador durante o período deste relatório.

C2.4 Como Determinar se Você Está Vulnerável

Uma verificação simples, com listas das aplicações que você possui instaladas mantida manualmente não é suficiente! Como os bancos de dados são frequentemente distribuídos como componentes parte de outras aplicações, é possível que uma base de dados tenha sido instalada sem mesmo os administradores o perceberem. Além disso, os bancos de dados podem permanecer desatualizados ou com configurações padrão vulneráveis. Isto foi graficamente demonstrado quando o worm SQL Slammer atacou o Microsoft Data Access Component (MDAC), que é incluído em muitas aplicações.

Execute uma varredura em busca de vulnerabilidades nos sistemas para determinar qual o Sistema de Gerenciamento de Banco de Dados (DBMS) está instalado, é acessível e está vulnerável. Você pode utilizar scanners comuns de vulnerabilidades ou ferramentas distribuídas por fabricantes como [MySQL Network Scanner](#), [Microsoft SQL server tool](#). O [Microsoft Baseline Security Analyzer](#) é também para ser utilizado no Microsoft SQL Server.

C2.5 Como se Proteger Contra Vulnerabilidades em Bancos de Dados

- Certifique-se que todos os Sistemas de Gerenciamento de Banco de Dados (DBMS) estão atualizados. Versões não corrigidas ou desatualizadas costumam possuir vulnerabilidades. Consulte o website dos fabricantes em busca de informações para a correção dos sistemas. Mantenha-se a par das vulnerabilidades e alertas anunciados pelos fabricantes:

-
- alertas de Segurança da Oracle
(<http://www.oracle.com/technology/deploy/security/alerts.htm>)
 - MySQL (<http://lists.mysql.com/>)
 - PostgreSQL (<http://www.postgresql.org/support/security>)
 - Microsoft SQL (<http://www.microsoft.com/technet/security/bulletin/notify.msp>)
 - IBM DB2 (<http://www-306.ibm.com/software/data/db2/udb/support/>)
 - IBM Informix (<http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg24009130>)
- Certifique-se que todos os DBMS e aplicações estão seguras:
 - Remova/modifique as senhas padrão das contas privilegiadas do banco de dados e do sistema antes de colocar o sistema na rede. Listas das contas padrão estão prontamente disponíveis na Internet.
 - Utilize os mínimos privilégios possíveis.
 - Utilize os procedimentos existentes (stored procedures) onde for possível.
 - Remova/desabilite os procedimentos existentes (stored procedures) desnecessários.
 - Configure o comprimento limite de quaisquer campos de formulários.
 - Veja a seção de referências abaixo que traz diversas fontes úteis para auxiliá-lo na segurança do DBMS.
 - Utilize firewall ou outro equipamento de segurança de rede para restringir o acesso através da rede às portas associadas a estes serviços das bases de dados.
 - Não confie nas entradas de dados de usuários! Garanta que as aplicações que utilizam o banco de dados tratem todas as entradas de usuários no lado do servidor, para evitar ataques como a inserção de código SQL (SQL injection) (veja <http://www.sans.org/rr/whitepapers/securecode/23.php>)

C2.6 Referências

Fontes genéricas e de diversas bases de dados

- Artigos do SANS reading room sobre segurança em bases de dados:
http://www.sans.org/rr/catindex.php?cat_id=3
- DoD database security technical implementation guide: <http://iase.disa.mil/stigs/stig/database-stig-v7r2.pdf>
- <http://www.databasesecurity.com/>

Oracle

- Checklist de Segurança abrangente do SANS para Oracle:
<http://www.sans.org/score/oraclechecklist.php>
- https://store.sans.org/store_item.php?item=80
- http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
- CIS benchmark tool: http://www.cisecurity.org/bench_oracle.html
- <http://www.petefinnigan.com/orasec.htm>
- <http://otn.oracle.com/deploy/security/index.html>
- <http://www.red-database-security.com>

MySQL

- SecurityFocus step-by-step guide to securing MySQL:
<http://www.securityfocus.com/infocus/1726>
- <http://dev.mysql.com/doc/mysql/en/Security.html>

PostgreSQL Security Guide

- <http://www.postgresql.org/support/security>
- <http://www.postgresql.org/docs/techdocs.53>

Microsoft SQL Security

- <http://www.microsoft.com/sql/techinfo/administration/2000/security/default.mspx>
- <http://www.sqlsecurity.com/>
- CIS SQL Server Benchmark Tool: http://www.cisecurity.org/bench_sqlserver.html

IBM DB2

- http://www.net-security.org/dl/articles/Securing_IBM_DB2.pdf

IBM Informix

- <http://www.databasesecurity.com/informix.htm>
- <http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.admin.doc/admin197.htm>

Sybase

- Guide to Sybase security: <http://www.niiconsulting.com/innovation/Sybase.pdf>

[top^](#)

C3. Aplicações de Compartilhamento de Arquivos P2P

C3.1 Descrição

Redes Peer to Peer (P2P) consiste em coleções dos computadores ou "nós" que funcionam simultaneamente como "clientes" e "usuários" para conseguir uma finalidade comum. Os nós podem trocar dados, compartilhar recursos, fornecer serviços de diretórios, suportar comunicações e fornecer ferramentas de colaboração em tempo real.

Um número de arquiteturas do controle e comunicação são utilizadas. Servidores indexadores centralizados podem fornecer serviços de diretório para a disponibilidade de dados e de serviços. Em redes inteiramente distribuídas cada nó ajuda com os serviços de indexação e de diretório e é inteiramente equivalente. As arquiteturas híbridas combinam as características de ambos para diferentes graus e grupos dos nós podem eleger/promover determinados nós para agir como servidores regionais de indexação/diretório.

Muitas aplicações legítimas utilizam P2P. Empresas de Software, incluindo Microsoft e Sun, fornecem uma

variedade das ferramentas e incentivam o desenvolvimento de aplicações P2P. Entretanto, como toda a ferramenta de transferência de dados, as aplicações P2P podem ser empregadas mal ou explorado para compartilhar ilegal do material proprietário, para obter dados confidenciais, expor usuários a pornografia não desejada, violência ou propaganda, para distribuir e executar malware (vírus, spyware, bots, etc.), para sobrecarregar a rede, encontrar dados de uso e comportamento e controlar bots, que podem criar uma responsabilidade legal. A responsabilidade e o processo legal não podem ser limitados ao perpetrador e podem ser estendidos ao patrocinador da rede, apoiadores ou membros.

As próprias redes P2P podem ser atacadas modificando arquivos legítimos com malware, espalhando arquivos de malware em diretórios compartilhados, explorando vulnerabilidades no protocolo ou nos erros no código, obstruindo (filtrar) o protocolo, negação de serviço fazendo a rede funcionar lentamente, Enviando Spam e ataques da identidade que identificam os usuários da rede e os importunam. Ações legais foram usadas com sucesso fechar algumas redes populares que eram culpados de infringir copyright.

Os conceitos e as técnicas do P2P estão evoluindo e podem ser encontrados em:

- Redes de compartilhamento de arquivos – cujo objetivo principal é compartilhar de recursos tais como o armazenamento e a largura de banda. Operam através de uma rede distribuída dos clientes, compartilhando diretórios de arquivos ou discos rígidos inteiros de dados. Os clientes participam fazendo download de arquivos de outros usuários, fazendo seus dados disponíveis a outros e coordenando buscas de arquivos para outros usuários.
- Computação em Nuvem –(chamado também de processamento distribuído, computação de grade, redes distribuídas) onde as "nuvens" de computadores são montadas para fornecer um ambiente computacional virtual para realizar uma tarefa dada distribuindo a carga de processamento e dados. Computação em Nuvem inclui servidores em linha quando necessitados, e o usuário final não sabe onde os dados residem ou executam durante o processo. Em alguns casos, a aplicação funciona em uma combinação de servidores e no PC do usuário. Nuvens de servidores podem residir fisicamente em grandes estruturas controladas por uma organização ou podem também residir toda sobre a Internet. Porque a capacidade computacional redimensionável é baseada em servidores virtuais o proprietário dos dados não sabe realmente onde seus programas e dados residem fisicamente.

A maioria dos programas do P2P usa um conjunto de portas padrão, mas elas podem automaticamente ou manualmente ser alteradas para usar portas diferentes se necessário para evitar a detecção, os firewalls, ou filtros de saída (egress). A tendência parece mover-se para o uso de invólucros (wrapps) HTTP e de criptografia para contornar facilmente restrições impostas.

C3.2 Sistemas Operacionais Afetados

Existem versões de software P2P disponíveis para todos os sistemas operacionais Microsoft Windows atualmente em uso, junto com versões para Linux, MacOS e a maioria de sistemas operacionais Unix.

C3.3 Detectando a atividade P2P

Detectar atividade P2P na rede pode provar ser desafiante. É possível detectar aplicações P2P funcionando na sua rede através:

-
- Monitorar o tráfego para portas comumente usadas por aplicativos P2P; funciona com alguns programas mais antigos. Entretanto, alguns programas migraram para usar o HTTP, o https e para outras portas que necessitam geralmente ter passagem livre pelo firewall e pelo proxies.
 - Monitoramento da camada de aplicação para protocolos P2P pode identificar os programas que usam as portas geralmente permitidas (53, 80). Entretanto, falha quando programas maliciosos cifram o conteúdo.
 - O uso de algum software local de prevenção de intrusão e de auditoria de mudança de sistema pode prevenir a instalação ou execução de aplicativos P2P assim como de malware diversos.
 - Testes de padrão / sistemas de detecção de intrusão por comportamento podem identificar membros potenciais de P2P. Os padrões observados incluem a frequência, tempo e o tamanho de avalanches de comunicação.
 - Varredura da rede e do armazenamento de PC para o conteúdo geralmente baixado pelos usuários de P2P, incluindo *.mp3, *.wma, *.avi, *.mpg, *.mpeg, *.jpg, *.gif, *.zip, *.torrent, e *.exe.
 - Mudanças no desempenho da rede podem indicar o uso em larga escala de P2P, ou de infecções por malware.
 - Alguns firewalls e produtos de Detecção/Prevenção de Intrusão combinam técnicas de detecção/prevenção de tráfego P2P de entrar ou sair da rede.
 - Para máquinas Microsoft Windows, SMS pode ser utilizado para fazer a varredura para os executáveis que estão instalados em estações de trabalho. Além disso, administradores devem limitar permissões a fim impedir que os usuários instalem tais aplicativos em suas estações de trabalho.
 - Sistemas comprometidos que tiveram o malware instalado através de compartilhamento de arquivos via P2P possuirão os mesmos sintomas vistos quando são infectados com sucesso por outros meios de distribuição de malware.

C3.4 Como se Proteger Contra Vulnerabilidades de Software P2P

- Usuários padrão não devem possuir permissão para instalar software. Restringir privilégios administrativos e de usuários poderosos (power users) para apoiar o pessoal que atua no suporte aos sistemas. Se um usuário deve ter privilégios de administrador ou de usuário poderoso, devem-se criar uma conta separada a ser utilizada para suas funções diárias do escritório, navegação na Internet e comunicação ao vivo.
- Usar ferramentas tais como o Microsoft DropMyRights para aumentar a segurança dos navegadores Web e clientes de correio.
- Em ambientes com Active Directory, Software Restriction Group Policies podem ser utilizadas a fim evitar que tipos sabidos de arquivos sejam executados.
- Educar os usuários sobre redes P2P, os perigos do compartilhamento de arquivos e a política da empresa.
- Habilite regras de filtro egress para restringir todas as portas não necessárias para as finalidades da empresa, embora como as aplicações P2P migram para o HTTP e para a encriptação, esta ação está se tornando menos eficaz.
- Monitore os registros (logs) do Firewall e IDS.
- Para reduzir as infecções por malware que podem ser espalhadas através de inúmeras aplicações, utilize soluções corporativas de produtos antivírus e de antispymware assegurando de que as atualizações estejam sendo executadas diariamente.
- Utilize firewalls locais em adição a firewalls de perímetro. Windows XP e Windows 2003 possuem o Windows firewall, o qual prove proteção adequada se configurado adequadamente. Uma

variedade de firewalls produzidos por terceiros (ZoneAlarm, Sygate, Outpost) prove funcionalidades adicionais e flexibilidade. Sistemas Windows 2000, XP e 2003 podem utilizar políticas IPSec como forma de prover filtragem de portas de tráfego de rede desnecessários via VPN. Em ambientes Active Directory, políticas IPSec e a configuração do Windows Firewall (para Windows XP SP2 e Windows 2003 SP1) podem ser gerenciadas de forma centralizada através do Group Policies.

- Desabilite a funcionalidade de Simple File Sharing (compartilhamento simples) do Windows XP se não for requerido explicitamente. [Start - Settings - Control Panel - Folder Options - Tab View - Disable (uncheck) setting Use Simple File Sharing - Apply - OK.]
- Monitorar sistemas para a presença de executáveis desconhecidos e de modificações desautorizada de arquivos do sistema. Soluções como o Tripwire ou AIDE (existem versões comerciais e de código aberto do produto) podem ser utilizados para detectar mudanças em arquivos.
- Compartilhamentos baseados em Samba podem ser configurados para executar um filtro quando da abertura ou da gravação de arquivos. Um detector de tipo de arquivo e um sistema de alerta podem se provar úteis para evitar o mau uso dos compartilhamentos.

C3.5 Referências

Wikipedia Peer-to-peer

<http://en.wikipedia.org/wiki/Peer-to-peer>

Web site de Cybercrime do Departamento de Justiça dos EUA

<http://www.usdoj.gov/criminal/cybercrime>

Outros fornecedores de software podem ser responsabilizados por violação de direito autoral.

[http://www.usdoj.gov/criminal/cybercrime/2006IPTFProgressReport\(6-19-06\).pdf](http://www.usdoj.gov/criminal/cybercrime/2006IPTFProgressReport(6-19-06).pdf) FBI Education initiative

<http://www.fbi.gov/cyberinvest/cyberedletter.htm>

The Information Factories

http://www.wired.com/wired/archive/14.10/cloudware_pr.html

Mobile Service Clouds: A Self-managing Infrastructure for Autonomic Mobile Computing Services

<http://www.cse.msu.edu/~farshad/publications/conferences/samimi06msc.pdf>

Cyber Security Tip ST05-007 - Risks of File-Sharing Technology

<http://www.us-cert.gov/cas/tips/ST05-007.html>

Risks of P2P File Sharing (Apresentação)

<http://www.ftc.gov/bcp/workshops/filessharing/presentations/hale.pdf>

Securing Windows XP Professional in a Peer-to-Peer Networking Environment

http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/sec_winxp_pro_p2p.mspx

Identifying P2P users using traffic analysis - Yiming Gong - 2005-07-21

<http://www.securityfocus.com/infocus/1843>

Bot software looks to improve peerage
<http://www.securityfocus.com/news/11390>

Stop the bots
<http://www.securityfocus.com/columnists/398/1>

How to block specific network protocols and ports by using IPSec (MS KB article 813878)
<http://support.microsoft.com/kb/813878>

Using Software Restriction Policies to Protect Against Unauthorized Software
<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx>

Availability and description of the Port Reporter tool (MS KB article 837243)
<http://support.microsoft.com/kb/837243>

New features and functionality in PortQry version 2.0 (MS KB article 832919)
<http://support.microsoft.com/default.aspx?kbid=832919>

Log Parser 2.2
<http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspx>

Browsing the Web and Reading E-mail Safely as an Administrator (DropMyRights)
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure11152004.asp>

Amazon Cloud Computing goes beta
<http://www.amazon.com/gp/browse.html?node=201590011>

Checkpoint Application Intelligence
http://www.checkpoint.com/products/downloads/applicationintelligence_whitepaper.pdf

Site de busca da Microsoft para peer-to-peer
<http://search.msdn.microsoft.com/search/default.aspx?siteId=0&tab=0&query=peer-to-peer>

Instant-Messaging-and-P2P-Vulnerabilities-for-Health-Organizations
<http://ezinearticles.com/?Instant-Messaging-and-P2P-Vulnerabilities-for-Health-Organizations&id=232800>

Detecting and Understanding Rootkits
<http://www.buanzo.com.ar/sec/Rootkits.html>

Classificador de pacote de camada de aplicação para Linux
<http://l7-filter.sourceforge.net/>

[top^](#)

C4. Mensagens Instantâneas

C4.1 Descrição

O uso difundido de mensagens instantâneas (MI) continua a aumentar os riscos da segurança para

organizações e usuários individuais. Quando o uso de mensagens instantâneas pode ser uma ferramenta muito útil para a comunicação; é ao mesmo tempo sujeito a muitas preocupações com a segurança. Os ataques recentes incluem novas variações no estabelecimento e a propagação de botnets, e o uso de contas comprometidas de mensagens instantâneas para ludibriar usuários a revelar informações sensíveis. Variantes de e-mail worms (tais como a família Mytob) foram espalhados também com o uso de mensagens instantâneas. As áreas de risco relacionadas a mensagens instantâneas são:

- Malware -- Worms, vírus, e Trojans transferidos com o uso de mensagens instantâneas. Muitos bots são controlados através de canais IRC.
- Confidencialidade da informação -- a informação transferida através de mensagens instantâneas pode estar sujeita à divulgação ao longo de qualquer parte do processo.
- Rede -- ataques de negação de serviço; utilização excessiva da capacidade da rede, mesmo que decorrente de uso legítimo.
- Aplicativos vulneráveis -- Aplicativos de mensagens instantâneas contêm vulnerabilidades que podem ser explorados para comprometer sistemas afetados.

Aplicativos de mensagens instantâneas populares incluem: AOL Instant Messenger (AIM), Gaim, ICQ, Jabber Messenger, Lotus Sametime, Skype, QQ, Windows Live Messenger (WLM), Google Talk, Trillian e Yahoo! Messenger. Protocolos de mensagens instantâneas incluem: IRC, MSNP, OSCAR, SIMPLE, XMPP e YMSG.

C4.2 Sistemas Operacionais Afetados

Aplicações de mensagens instantânea são disponíveis para todos os sistemas operacionais populares.

C4.3 Entradas CVE

[CVE-2006-0992](#), [CVE-2006-4662](#), [CVE-2006-5084](#)

C4.4 Como se Proteger Contra Vulnerabilidades em IM e seu uso não autorizado

- Estabelecer políticas para o uso aceitável de mensagens instantâneas e assegurar-se de que todos os usuários estejam cientes daquelas políticas e compreendam claramente os riscos potenciais.
- Usuários padrão não devem possuir permissão para instalar software. Restringir privilégios administrativos e de usuários poderosos (power users) para apoiar o pessoal que atua no suporte aos sistemas. Se um usuário dever ter privilégios de administrador ou de usuário poderoso, devem-se criar uma conta separada a ser utilizada para suas funções diárias do escritório, navegação na Internet e comunicação ao vivo.
- Assegure-se de que as correções do vendedor sejam aplicadas prontamente ao software de mensagens instantâneas, aplicações relacionadas, e ao sistema operacional subjacente.
- Empregar produtos do antivírus e antispymware.
- Não confiar em servidores de MI externos para o uso interno de mensagens; Providencie um proxy comercial de MI ou um servidor interno.
- Crie rotas de comunicação seguras ao usar mensagens instantâneas com parceiros comerciais de confiança.

-
- Configure de forma apropriada sistemas de detecção/prevenção de intrusão. Compreenda que muitos aplicativos de mensagens instantâneas são capazes de permitir associar comunicações para mascarar como um tráfego legítimo qualquer (por exemplo HTTP).
 - Considere implementar produtos projetados especificamente para a segurança em mensagens instantâneas.
 - Filtrar todo o tráfego HTTP através de um servidor proxy com autenticação para fornecer capacidades adicionais de filtragem/monitoramento do tráfego de mensagens instantâneas.
 - Bloquear o acesso aos servidores públicos conhecidos de mensagens instantâneas que não foram autorizados explicitamente. (nota: Oferece proteção parcial devido ao número de potenciais servidores externos.)
 - Bloquear portas popularmente utilizadas por mensagens instantâneas. (nota: Oferece proteção parcial, devido ao potencial número de protocolos e de portas associadas, e da habilidade dos aplicativos de contornar as limitações de portas.)
 - Monitorar utilizando um sistema de detecção/prevenção de intrusão contra usuários que criam túneis para IM ou que contornem proxies.

C4.5 Referências

Phishers hijack IM accounts

http://news.com.com/Phishers+hijack+IM+accounts/2100-7349_3-6126367.html

Rich presence: a new user communications experience

http://www.alcatel.com/doctypes/articlepaperlibrary/html/ATR2005Q1/ATR2005Q1A17_EN.jhtml

Instant messaging: a new target for hackers

http://www.leavcom.com/ieee_july05.htm

AIM bot creates "fight combos" to spread

<http://www.securityfocus.com/brief/305>

Secure Instant Messaging in the Enterprise

http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1199405,00.html

[top^](#)

C5. Tocadores Multimídia

C5.1 Descrição

Tocadores multimídias são popularmente utilizados e possuem um parque instalado de milhões de sistemas. Conteúdo é baixado em forma de arquivos multimídia como filmes, vídeo ou música. Este conteúdo é encaixado em páginas Web, apresentações, ou integrado em aplicações multimídia.

Tocadores multimídias podem fazer parte de sistemas através de instalações padrão ou empacotados com outro software. Tipicamente os navegadores são ajustados para realizar "convenientemente" o download e abrirem arquivos multimídia sem requer a interação do usuário. São também baixados por usuários em redes corporativas para facilitar a transferência de conteúdo multimídia para dispositivos móveis.

Um grande número de vulnerabilidades foi descoberto em vários tocadores multimídias ao longo do ano

passado. Muitos destas vulnerabilidades permitem uma página Web maliciosa ou a um arquivo multimídia comprometer completamente o sistema de um usuário sem requer muita interação do usuário. O sistema do usuário pode ser comprometido simplesmente ao se visitar uma página Web maliciosa. Daqui, estas vulnerabilidades podem ser exploradas para instalar software malicioso como spyware, Trojans, adware ou keyloggers nos sistemas dos usuários. Exemplos de código de exploração estão disponíveis publicamente.

Alguns dos tocadores multimídias mais populares incluem:

- Windows: Windows Media Player, RealPlayer, Apple Quicktime, Winamp, iTunes
- Mac OS: RealPlayer, Quicktime, iTunes
- Linux/Unix: RealPlayer, Helix Player

C5.2 Sistemas Operacionais Afetados

- Microsoft Windows
- Linux/UNIX
- Mac OS X

C5.3 Entradas CVE

RealPlayer and Helix Player

[CVE-2006-1370](#), [CVE-2006-0323](#), [CVE-2005-2922](#), [CVE-2005-4130](#), [CVE-2005-4126](#), [CVE-2005-3677](#), [CVE-2005-2936](#)

iTunes

[CVE-2006-1249](#), [CVE-2005-4092](#), [CVE-2005-2938](#)

Winamp

[CVE-2006-0708](#), [CVE-2005-3188](#), [CVE-2005-2310](#)

Quicktime

[CVE-2006-2238](#), [CVE-2006-1456](#), [CVE-2006-1249](#), [CVE-2005-3713](#), [CVE-2005-3711](#), [CVE-2005-3710](#), [CVE-2005-3709](#), [CVE-2005-3708](#), [CVE-2005-3707](#), [CVE-2005-2340](#), [CVE-2005-4092](#), [CVE-2005-2743](#)

Windows Media Player

[CVE-2006-0025](#), [CVE-2006-0006](#), [CVE-2005-3591](#)

Macromedia Flash Player

[CVE-2005-3591](#), [CVE-2005-2628](#)

C5.4 Como Determinar Se Você Está Vulnerável

Se você executa alguns destes tocadores, e se você não estiver utilizando a versão mais recente com todas as correções aplicadas, você é vulnerável aos ataques associados. Revisões periódicas do sistema de

software instalado podem ser utilizadas para identificar instalações não desejadas de tocadores multimídia assim como instalações não autorizadas por usuários.

C5.5 Como se Proteger Contra Vulnerabilidades em Tocadores Multimídia

Seguem algumas abordagens comuns para proteger contra estas vulnerabilidades:

- Manter os tocadores multimídia atualizados com todas as últimas correções. A maioria dos tocadores multimídia permite atualizar através dos menus de ajuda ou de ferramentas.
- Revise com cuidado as instalações padrão dos sistemas operacionais e de outros produtos para assegurar que não incluam tocadores multimídia não desejados. Configurar sistemas operacionais e navegadores para impedir instalação involuntária.
- Usar sistemas de prevenção/detecção de intrusão e antivírus e software de detecção de malware para bloquear arquivos multimídia maliciosos.
- Em estações corporativas limitar a instalação de software baixado pelo usuário sempre que possível. Isto irá permitir uma melhor gerência de correções e gerência de vulnerabilidades.
- Não instalar tocadores multimídia em sistemas onde arquivos multimídia não devem ser executados (servidores, por exemplo)

C5.6 Referências

Página de Produtos Tocadores de Multimídia da RealNetworks

http://www.realnetworks.com/products/media_players.html

Relatórios de Segurança

<http://service.real.com/help/faq/security/>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=40#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=39#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=25#widely2>

Página do Tocador Helix

<https://player.helixcommunity.org/>

Notícias, Incluindo anúncios de segurança

<https://helixcommunity.org/news/>

Relatórios de Segurança

<http://www.sans.org/newsletters/risk/display.php?v=4&i=40#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=39#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=25#widely2>

Página do QuickTime da Apple

<http://www.apple.com/quicktime/>

Página do iTunes da Apple

<http://www.apple.com/itunes/>

Atualizações de Segurança da Apple

<http://docs.info.apple.com/article.html?artnum=61798>

Suporte do QuickTime

<http://www.apple.com/support/quicktime/>

Relatórios de Segurança

<http://www.sans.org/newsletters/risk/display.php?v=5&i=39#06.39.25>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=37#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=27#06.27.34>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=26#widely4>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=19#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=11#06.11.28>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=2#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=49#05.49.24>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely2>

Nullsoft Winamp

<http://www.winamp.com/>

<http://www.winamp.com/about/news.php>

Relatórios de Segurança

<http://www.sans.org/newsletters/risk/display.php?v=5&i=25#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=8#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely4>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=5#widely1>

Página do Microsoft Windows Media Player

<http://www.microsoft.com/windows/windowsmedia/default.aspx>

Segurança do Windows Media Player 10

<http://www.microsoft.com/windows/windowsmedia/mp10/security.aspx>

Busca do Boletim de Segurança da Microsoft

<http://www.microsoft.com/technet/security/current.aspx>

Relatórios de Segurança

<http://www.sans.org/newsletters/risk/display.php?v=5&i=24#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely3>

Página do Macromedia Flash Player

<http://www.macromedia.com/software/flashplayer>

Relatórios de Segurança

<http://www.sans.org/newsletters/risk/display.php?v=5&i=42&rss=Y#06.42.23>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=37#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=28#widely8>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=19#widely5>
<http://www.sans.org/newsletters/risk/display.php?v=5&i=11#06.11.27>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=46#05.46.29>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely3>

[top^](#)

C6. Servidores DNS

C6.1 Descrição

O Sistema de Nomes de Domínio - The Domain Name System (DNS) - é um mecanismo da Internet crítico que primariamente facilita a conversão de nomes de host globalmente únicos em endereços do Protocolo da Internet - Internet Protocol - globalmente únicos correspondentes usando um esquema de base de dados distribuída. O DNS é baseado em um modelo de confiança desenvolvido em uma era de confiança mútua que é vastamente diferente da Internet de hoje, em geral hostil. Por causa desta mudança na natureza da Internet o sistema DNS é sujeito a muitos tipos de ataques de transação que tiram vantagem daquela confiança, incluído cache poisoning, seqüestro de domínio e redirecionamento man-in-the-middle.

Ao longo do último ano os seguintes tipos de ataque foram conduzidos por botnets contra servidores DNS.

- 1. Ataques de Negação de Serviço de Recursão:** Um Botmaster publica um grande registro DNS em um servidor DNS comprometido ou em um servidor DNS configurado para este propósito. O botmaster então orienta a botnet a enviar pequenas consultas UDP/53 para servidores públicos recursivos com um endereço de origem forjado, apontado para a vítima alvo do ataque. Como resultado, os servidores DNS recursivos, ao invés dos bots, atacam diretamente a vítima. Este efeito pode ser amplificado mais ainda ao se fazer registros DNS maiores que um pacote de resposta UDP/53 típico e por isso forçando uma transação TCP/53.
- 2. Forjamento de Respostas de zona Autoritativa:** O botmaster cria um web site falso (site phishing) em um servidor web comprometido. O botmaster então orienta a botnet a escutar por requisições e forjar respostas DNS para uma zona em especial com uma resposta apontando para o servidor web comprometido. Uma variação deste ataque é agir localmente no computador infectado por bot e modificar o arquivo de hosts local com entradas apontando para o web site falso.

C6.2 Como Determinar Se Você Está em Risco

Todos os usuários de Internet estão sob risco de ter dados incorretos retornando de consultas DNS. Se a varredura de servidores DNS sob seu controle mostra que a atual versão ou correções de segurança divulgados pelo fornecedor do DNS não foram instalados então seu servidor(s) DNS está em risco. Uma abordagem pró-ativa para manter a segurança de qualquer servidor DNS é assinar um dos boletins de alerta e vulnerabilidade, tais como aqueles oferecidos por SANS, Secunia e outros, ou se mantendo atualizado com relação às vulnerabilidades postadas no Open Source Vulnerability Database (<http://www.osvdb.org>). Além de alertas de segurança, um varredor de vulnerabilidades (vulnerability scanner) atualizado pode ser altamente efetivo no diagnóstico de quaisquer vulnerabilidades em servidores DNS. A configuração do servidor DNS também deve ser revisada e testada para garantir que recursão inapropriada ou atualizações não sejam permitidos.

C6.3 Como se Proteger Contra Vulnerabilidades DNS

Assim como qualquer pacote de software atualizações e correções para software servidor DNS devem ser aplicadas tão logo estejam disponíveis e testadas contra qualquer impacto nas operações da rede local.

Para se proteger contra vulnerabilidades DNS:

- Aplique todas as correções de segurança ou instale a versão mais recente do servidor DNS. Para mais informações sobre como reforçar um DNS já instalado veja os artigos sobre como tornar seguros serviços de nome, como referenciado nos comparativos do [Center for Internet Security DNS BIND](#) e nos comparativos CIS para a plataforma de SO.
- Aplique regras apropriadas de firewall para quaisquer servidores DNS dentro de uma rede que não precisem ser consultados da Internet.
- Para tornar as zonas de transferência entre um servidor DNS primário e um secundário seguras de uma maneira criptográfica configure os servidores para usar DNS Transaction Signatures (TSIG).
- Para evitar que um serviço DNS comprometido exponha todo o sistema restrinja o serviço de forma que ele seja executado por um usuário sem privilégio, em um diretório chroot()ed (jail).
- Não permita que seus servidores DNS recursivos sejam usados por blocos de rede que não sejam os seus a menos que isto seja requerido. Firewalls ou arquivos de configuração DNS podem prevenir isto na maioria dos casos. Desabilitar a recursão e "glue fetching" auxilia na defesa contra envenenamento de cache DNS.
- Considere assinar toda sua zona usando DNS Security Extensions (DNSSEC).
- Na maioria dos sistemas que rodam BIND o comando "named -v" mostrará a versão instalada enumerada como X.Y.Z, onde X é a versão maior (major), Y é a versão menor (minor) e Z é o nível de patch. Atualmente as duas versões "major" para BIND são 8 e 9. O Internet Systems Consortium recomenda que todos os usuários de BIND migrem para a versão 9 assim que possível.
- Servidores DNS são integrados em muitos produtos comuns como firewalls, servidores de rede corporativos e appliances de segurança. Todos os servidores em contato direto com a Internet, appliances e sistemas devem ser verificados para que se garanta que qualquer software DNS embutido esteja atualizado e mantido como recomendado pelo fornecedor.
- Servidores que não são especificamente projetados para oferecer suporte a transações DNS (mail, web ou servidores de arquivo por exemplo) não devem estar rodando uma aplicação ou daemon DNS a menos que seja absolutamente necessário.

C6.6 Referências

Vulnerabilidades DNS

- <http://www.sans.org/newsletters/risk/display.php?v=4&i=11>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=14#widely1>
- <http://isc.sans.org/presentations/dnspoisoning.php>
- <http://thekelleys.org.uk/dnsmasq/doc.html>
- <http://www.icir.org/vern/papers/reflectors.CCR.01/node8.html>

Pesquisa sobre versão do DNS e software do servidor

-
- <http://mydns.bboy.net/survey/>
 - <http://www.dns.net/dnsrd/servers/>

Fucionamento Interno do DNS

- <http://www.internic.net/faqs/authoritative-dns.html>
- <http://www.sans.org/rr/whitepapers/dns/>
- <http://www.cert.org/archive/pdf/dns.pdf>
- <http://www.isc.org/index.pl>
- <http://www.microsoft.com/windows2000/technologies/communications/dns/default.aspx>
- <http://www.dns.net/dnsrd/>

Implantação de DNSSEC

- <http://www.dnssec-deployment.org/>
- <http://www.dnssec.net>
- <http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf>

Melhores Práticas de Segurança em DNS

- <http://www.cymru.com/Documents/secure-bind-template.html>
- <http://www.softpanorama.org/DNS/security.shtml>
- http://cookbook.linuxsecurity.com/sp/bind_hardening8.html
- <http://www.isc.org/index.pl?sw/bind/bind-security.php>
- http://www.cisecurity.org/bench_bind.html
- http://www.cert.org/tech_tips/usc20_full.html

[top^](#)

C7. Software de Backup

C7.1 Descrição

O software de backup é um ativo valioso para qualquer organização. Este software tipicamente executa em um grande número de sistemas de uma empresa. Nos anos recentes com o crescimento do tamanho dos dados, a tendência tem sido a consolidação da funcionalidade de backup em poucos servidores, ou até em um único servidor. As máquinas que necessitam do serviço de backup se comunicam com o servidor através da rede. A forma de realização do backup pode ser do tipo “push”, onde o cliente envia os dados para o servidor, do tipo “pull” onde o servidor conecta com cada cliente por vez, ou uma combinação dos dois. Durante o último ano uma quantidade significativa de vulnerabilidades em software de backup foram descobertas. Estas vulnerabilidades podem ser exploradas de modo a comprometer completamente os servidores de backup ou os clientes de backup. Um atacante pode utilizar estas falhas para atingir um comprometimento global na empresa e obter acesso a dados sensíveis que estejam em backup. Exploits têm sido disponibilizados publicamente para algumas destas falhas, e estas vulnerabilidades estão sendo exploradas na rede.

C7.2 Sistemas Operacionais e Software de Backup Software Afetados

Todos os sistemas operacionais executando servidores ou clientes de backup são potencialmente vulneráveis. Os sistemas afetados são principalmente sistemas Windows ou UNIX.

Os softwares de backup a seguir são conhecidos por serem afetados por vulnerabilidades conhecidas:

- Symantec Veritas NetBackup/Backup Exec
- Computer Associates BrightStor ARCserve
- EMC Legato Networker

C7.3 Entradas CVE

[CVE-2005-3116](#), [CAN-2005-3659](#), [CAN-2005-3658](#), [CVE-2006-0989](#), [CVE-2006-0990](#), [CVE-2006-0991](#), [CVE-2006-5142](#), [CVE-2006-5143](#)

C7.4 Como Determinar Se Você Está Vulnerável

- Utilize um Verificador de Vulnerabilidades da sua preferência para detectar instalações de software de backup vulneráveis.
- Se você está utilizando algum destes softwares mencionados acima, é recomendável atualizá-lo para a última versão. Visite regularmente o site do vendedor da sua solução de backup e inscreva-se em listas de notificação de atualização caso existam, além de sites de segurança gerais como o [US-CERT](#), CERT, SANS ([Internet Storm Center](#)) para obter anúncios de novas vulnerabilidades relacionadas ao seu software de backup.
- Portas típicas utilizadas por software de backup:
 - Symantec Veritas Backup Exec
 - TCP/10000 TCP/8099, TCP/6106, TCP/13701, TCP/13721 and TCP/13724 (Uma listagem das portas utilizadas pelos daemons de backup do Veritas pode ser vista [aqui](#))
 - CA BrightStor ARCserve Backup Agent
 - TCP/6050, UDP/6051, TCP/6070, TCP/6503, TCP/41523, UDP/41524
 - Sun and EMC Legato Networker
 - TCP/7937-9936

C7.5 Como se Proteger Contra Estas Vulnerabilidades

- Tenha certeza que todas as últimas correções de segurança fornecidas pelo fabricante estão instaladas nos clientes e servidores.
- As portas utilizadas pelo software de backup devem ser bloqueadas de qualquer acesso de redes não confiáveis, inclusive da Internet.
- Dados devem ser criptografados quando armazenados em mídias de backup e quando estiverem sendo transportados através da rede.
- Firewalls baseados em host ou rede devem ser utilizados para limitar a visibilidade do software de backup de modo a garantir que apenas os hosts apropriados conseguem se comunicar com as portas do servidor de backup.
- Segmente a sua rede para criar uma VLAN separada para a rede de backup.

-
- Mídias de backup devem ser armazenadas, rastreadas e contabilizadas como qualquer outro ativo de TI para detectar roubo ou perda.
 - Mídias de backup devem ser apagadas de forma segura, ou destruídas fisicamente no fim da sua vida útil.

C7.6 Referências

Alertas da Computer Associates

<http://supportconnectw.ca.com/public/storage/infodocs/basbr-secnotice.asp>

<http://zerodayinitiative.com/advisories/ZDI-06-030.html>

<http://zerodayinitiative.com/advisories/ZDI-06-031.html>

Alertas da Symantec Veritas

<http://seer.support.veritas.com/docs/279553.htm>

<http://support.veritas.com/docs/281521>

<http://www.idefense.com/application/poi/display?id=336&type=vulnerabilities>

<http://www.zerodayinitiative.com/advisories/ZDI-06-005.html>

<http://www.zerodayinitiative.com/advisories/ZDI-06-006.html>

Alertas da EMC Legato e Sun

http://www.legato.com/support/websupport/product_alerts/011606_NW.htm

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0027.html>

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0028.html>

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0029.html>

[top^](#)

C8. Servidores de Segurança, Corporativos e de Gerenciamento de Diretórios

C8.1 Descrição

Aplicações como antivírus e antispam, serviços de diretório e sistemas de gerenciamento e monitoramento consistem em um desafio de segurança particular. Além de comprometer o sistema onde estão abrigados, eles provêem oportunidades para ataques a outros sistemas.

C8.2 Aplicações Afetadas

Estas aplicações podem ser divididas em múltiplas categorias:

- **Servidores de Diretório** - Utilizados para manter informação sobre usuários e sistemas. O comprometimento destas aplicações pode permitir acesso a grandes quantidades de informação, incluindo nomes de usuários e senhas (possivelmente cifradas).
- **Sistemas de Monitoramento** - Usados para monitorar diversos outros sistemas. Estas aplicações freqüentemente possuem contas de usuário nos clientes monitorados, permitindo a um atacante um acesso fácil para os sistemas clientes.

-
- **Sistemas de Configuração e Aplicação de Correções** - Estes sistemas são usados para manter as configurações dos clientes e correções. O comprometimento destes sistemas prove um caminho fácil para distribuição futura de malware.
 - **Softwares de varredura de Spam e Virus** - Vulnerabilidades nestes sistemas podem ser explorados com pouca ou nenhuma interação do usuário, através do simples envio de uma mensagem de correio eletrônico especialmente construída. Uma vez comprometido, atacantes podem facilmente enviar e-mails contendo vírus e spam. Adicionalmente, estes sistemas normalmente contem informações sensíveis, como caixas postais de usuários.

Estas aplicações costumam executar em uma variedade de sistemas operacionais, incluindo sistemas comuns como Microsoft Windows ou Solaris, até sistemas mais raros como HP-UX e Novell Netware.

C8.3 Entradas CVE

[CVE-2006-5478](#), [CVE-2006-4509](#), [CVE-2006-4510](#), [CVE-2006-4177](#), [CVE-2006-2496](#), [CVE-2006-0992](#), [CVE-2005-3653](#), [CVE-2005-1928](#), [CVE-2005-1929](#)

C8.4 Como Determinar Se Você Está em Risco

- Utilize um verificador de vulnerabilidades.
- Acompanhe anúncios de segurança do vendedor.

C8.5 Como se Proteger Contra Estas Vulnerabilidades

- Mantenha os sistemas atualizados com as últimas correções e service packs. Se possível, utilize um sistema de atualização automática.
- Utilize sistemas de prevenção e detecção de intrusos para detectar ou prevenir ataques explorando estas vulnerabilidades.
- Garanta que apenas usuários e sistemas autorizados possuam acesso aos sistemas afetados.

C8.6 Referências

Trend Micro ServerProtect Multiple Vulnerabilities

<http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0066.html>

<http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0067.html>

<http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0068.html>

Página da Trend Micro

<http://www.trendmicro.com/>

CA iTechnology iGateway Buffer Overflow

http://supportconnectw.ca.com/public/ca_common_docs/igatewaysecurity_notice.asp

Página da CA

<http://www.ca.com/>

Novell eDirectory iMonitor Remote Buffer Overflows
<http://www.zerodayinitiative.com/advisories/ZDI-06-016.html>

Página da Novell
<http://www.novell.com>

Symantec Sygate Management Server SQL Injection
<http://securityresponse.symantec.com/avcenter/security/Content/2006.02.01.html>

Página da Symantec
<http://www.symantec.com/>

HP OpenView Multiple Remote Command Execution
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00672314>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00671912>

HP OpenView Storage Data Protector Remote Code Execution
<http://archives.neohapsis.com/archives/bugtraq/2006-08/0273.html>

Página do OpenView da HP
<http://h20229.www2.hp.com/>

PatchLink Update Server Multiple Vulnerabilities
<http://archives.neohapsis.com/archives/bugtraq/2006-06/0631.html>

Página da PatchLink
<http://www.patchlink.com/>

Barracuda Spam Firewall Remote Command Injection
<http://archives.neohapsis.com/archives/bugtraq/2006-08/0093.html>

Página da Barracuda
<http://www.barracudanetworks.com/ns/?L=en>

McAfee ePolicy Orchestrator/ProtectionPilot Remote Buffer Overflow

Página da McAfee
<http://www.mcafee.com/>

[top^](#)

N1 Servidores e Telefones VoIP

N1.1 Descrição

A tecnologia VoIP tem tido rápida adoção durante o último ano. Ao mesmo tempo, tem havido um crescimento em falhas de segurança de componentes típicos de uma rede VoIP como o proxy de chamadas, servidores de mídia e os próprios telefones VoIP. Vulnerabilidades para vários produtos como o [Cisco Unified Call Manager](#) , [Asterisk](#) e diversos telefones VoIP de diversos fabricantes tem sido encontradas que podem levar à negação de serviço ao controle total sobre o dispositivo/servidor

vulnerável. Através do controle sobre servidores e telefones VoIP, um atacante pode efetuar golpes via VoIP, escutas de ligações, fraudes de tarifação ou ataques de negação de serviço.

Como muitos servidores VoIP, especialmente os gerenciados por provedores de serviço VoIP possuem interface com a rede de telefonia tradicional e as redes IP, um atacante capaz de comprometer um servidor VoIP pode inclusive manipular a sinalização da rede de telefonia convencional com o objetivo de afetar serviços na rede pública de telefonia (PSTN).

N1.2 Entradas CVE

Asterisk

[CVE-2006-2898](#), [CVE-2006-4345](#), [CVE-2006-4346](#), [CVE-2006-5444](#)

Cisco Call Manager

[CVE-2006-0368](#), [CVE-2006-3594](#)

VoIP Phones

[CVE-2005-3717](#), [CVE-2005-3722](#), [CVE-2005-3723](#), [CVE-2006-0305](#), [CVE-2006-0374](#), [CVE-2006-0834](#), [CVE-2006-5038](#)

N1.3 Como Mitigar Estas Vulnerabilidades VoIP

- Aplique as correções fornecidas pelo fabricante para servidores VoIP e software/firmware de telefones VoIP.
- Verifique que o sistema operacional do servidor VoIP esteja atualizado com as últimas correções fornecidas pelo fabricante do sistema ou do produto VoIP.
- Realize verificações nos servidores VoIP e telefones para detectar portas abertas. Bloqueie todas as portas contra tráfego da Internet que não sejam necessárias para funcionamento da infraestrutura VoIP.
- Utilize um firewall com suporte ao protocolo VoIP ou um produto de prevenção de intrusos para garantir que todas as portas UDP nos telefones VoIP não estão abertas para a Internet em comunicações RTP/RTCP.
- Desabilite todos os serviços desnecessários nos telefones e servidores (telnet, HTTP, etc.).
- Utilize ferramentas de fuzzing como a [OULU SIP PROTOS Suite](#) contra os componentes VoIP para garantir a integridade da pilha de protocolos VoIP.
- Cuidados adicionais devem ser tomados na fase de seleção dos produtos para garantir que o fabricante suporta correções de sistema operacional quando estes são lançados. Muitos fabricantes não oferecem suporte para correções não aprovadas e podem levar um tempo considerável antes de aprová-las.
- Utilize VLANs separadas para a sua rede de voz e dados na medida que a sua convergência de redes permita. Garanta que os servidores VoIP DHCP e TFTP estejam separados da sua rede de dados.
- Mude as senhas padrão nas ferramentas de administração dos telefones e proxies.

N1.4 Referências

Vulnerabilidades no Asterisk

<http://www.asterisk.org/>

<http://archives.neohapsis.com/archives/bugtraq/2006-06/0139.html>

<http://archives.neohapsis.com/archives/fulldisclosure/2006-08/0617.html>

<http://archives.neohapsis.com/archives/bugtraq/2006-10/0311.html>

Cisco Unified Call Manager Vulnerabilities

http://www.cisco.com/en/US/products/products_security_advisory09186a00805e8a55.shtml

General VoIP Security Information VoIPSA Organization

<http://www.voipsa.org>

Considerações de Segurança do NIST para Sistemas VoIP

<http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>

[top^](#)

N2. Fraquezas de Configuração de Dispositivos de Rede e outros Dispositivos Comuns

N2.1 Descrição

Dispositivos de Rede, tais como roteadores e switches, freqüentemente tem uma reputação por segurança e estabilidade. Além disso, dispositivos acessíveis por rede como impressoras e maquinas de fax são freqüentemente considerados inerentemente seguros. É muito freqüente que ambas as classes de dispositivos sejam omitidas de políticas e auditorias de segurança.

Por causa do papel único que estes dispositivos exercem na infra-estrutura de rede eles normalmente têm configurações padrão que enfatizam facilidade de uso e configuração em vez de segurança. Esta seção discute as inseguranças comuns presentes em diversas configurações padrão de dispositivos de rede e acessíveis por rede.

N2.2 Problemas Comuns de Configuração Padrão

N2.2.1 Community Strings SNMP Padrão

Community string padrão ou hard-coded continua a ser um problema em produtos de rede. Neste ano o Cisco IOS versões 12.2 a 12.4 antes de 20060920, usado por certos dispositivos da Cisco e por um switch da 3Com, foram reportados como vulneráveis a este problema.

Exemplos de CVEs: [CVE-2006-4950](#), [CVE-2006-5382](#)

N2.2.2 Contas, Senhas, Chaves de Criptografia e Tokens Padrão

Muitos dispositivos são configurados com senhas padrão e outros tokens de autenticação. Estes freqüentemente permitem acesso administrativo completo ao dispositivo. No caso de dispositivos sem fio, chaves de criptografia padrão podem fazer o monitoramento e captura (sniffing) de tráfego trivialmente fácil.

Exemplos de CVEs: [CVE-2006-0789](#), [CVE-2006-0834](#), [CVE-2006-3287](#)

N2.2.3 Serviços Desnecessários

Muitos dispositivos são configurados para executar outros serviços além dos necessários para a finalidade do mesmo na empresa. Muitas impressoras oferecem interfaces de impressão tanto HTTP como FTP, por exemplo. Estas interfaces são freqüentemente habilitadas por padrão. Serviços desnecessários criam brechas de segurança em potencial e tornam a administração e o registro de eventos mais difícil.

N2.2.4 Protocolos de Administração sem Autenticação ou Criptografia

Dispositivos são freqüentemente administrados por protocolos que não oferecem suporte a cifragem ou autenticação. Interfaces de administração HTTP e telnet transmitem toda informação em claro e TFTP transmite toda a informação em claro e não oferece suporte a autenticação. Protocolos que oferecem suporte a cifragem e autenticação, tais como HTTPS e SCP, devem ser usado sempre que possível.

N2.3 Vulnerabilidades em Impressoras

Dispositivos como impressoras, máquinas de fax e scanners muitas vezes contém as fraquezas de configuração descritas acima. Estes dispositivos freqüentemente permanecem sem correção e podem representar um risco de segurança significativo para a organização.

Exemplos de CVEs: [CVE-2006-0788](#), [CVE-2006-2108](#)

N2.4 Como se Proteger Contra Estas Vulnerabilidades

N2.4.1 Realize uma Auditoria Completa de Configuração

Armazenar configurações de dispositivos de uma maneira centralizada e examinar regularmente estas configurações pode fazer com que a descoberta de fraquezas seja fácil. Usar uma ferramenta como Cisco's CiscoWorks pode ajudar no gerenciamento de configuração.

CiscoWorks Home Page <http://www.cisco.com/en/US/products/sw/cscowork/ps2425/>

RANCID - Cisco Config Monitoring Tool <http://www.shrubbery.net/rancid>

CISecurity Network Element Benchmarks and Audit Tools <http://www.cisecurity.org>

N2.4.2 Monte um Servidor Syslog

Muitos dispositivos oferecem suporte para o registro de eventos (log) pelo protocolo syslog. Servidores Syslog são incluídos por padrão em todos os sistemas Unix, semelhantes a Unix e Linux e servidores syslog gratuitos são disponíveis para Microsoft Windows. O registro de logs devidamente configurado em um dispositivo de rede permitirá que um servidor syslog registre o log de acessos a um dispositivo, qualquer modificação na configuração assim como qualquer violação de política conduzidas pelo dispositivo.

Configuring Cisco Syslog <http://www.linuxhomenetworking.com/cisco-hn/syslog-cisco.htm>

Central Loghost Mini-HOWTO <http://www.campin.net/newlogcheck.html>

N2.4.3 Desabilite Contas Padrão e Mude Senhas Padrão

Quaisquer contas padrão devem ser desabilitadas e todas as senhas padrão e outros tokens de autenticação devem ser trocados por alternativas seguras.

Community Strings SNMP da Cisco

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

N2.4.4 Desabilite Serviços Desnecessários

Quaisquer serviços que não sejam necessários devem ser desabilitados. Quaisquer serviços necessários devem, se possível, ser restritos a usuários autenticados.

Pequenos Serviços TCP e UDP Cisco

http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a008019d97a.shtml

N2.4.5 Use Protocolos de Administração Encriptados e Autenticados

Se o dispositivo oferece suporte a administração por HTTPS ou SSH estes são preferíveis a protocolos não cifrados como HTTP ou telnet. Para transferência de arquivos SCP, HTTPS ou FTPS devem ser preferidos a TFTP ou FTP. Senhas fortes ou outros métodos fortes de autenticação devem sempre ser usados.

Configurando SSH em Dispositivos Cisco

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html

N2.4.6 Use Segurança no Nível de Porta

Se sua infra-estrutura de rede oferece suporte implemente segurança em nível de porta em switches. Isto pode ajudar a prevenir que sistemas "rogue" se conectem à rede e pode ajudar a conter e detectar ARP spoofing e outros ataques.

Configurando Segurança em Nível de Porta em Dispositivos Cisco

<http://articles.techrepublic.com.com/5100-1035-6123047-1.html>

<http://articles.techrepublic.com.com/5100-1035-6123047-2.html>

[top^](#)

H1. Direitos Excessivos de Usuário e Dispositivos Não Autorizados

H1.1 Introdução

Alguns ataques não podem ser prevenidos de maneira efetiva apenas por controles técnicos. Usuários incautos podem ser induzidos a fazer coisas inseguras. Usuários espertos podem encontrar maneiras inseguras de fazer as coisas, expondo mesmo de maneira não intencional a companhia a ataques. Para proteger contra ataques explorando estas fraquezas controles administrativos suplementam controles técnicos e físicos.

Em tempo, controles técnicos podem ser capazes de reforçar políticas que prescrevem comportamento do usuário. Ao mesmo tempo, para tornar estes controles administrativos efetivos as organizações precisam confiar, mas verificar para identificar violações da política de maneira que ações corretivas possam ser tomadas. A Aplicação da Política (o processo para trazer os sistemas de volta ao estado de conformidade coma a política tão logo violações sejam detectadas) também é essencial.

H.1a Dispositivos Não Autorizados e/ou infectados na rede

Os melhores esforços para tornar um sistema de informações seguro são fúteis se dispositivos não autorizados são capazes de conectar à rede. Um access point rogue pode ser uma porta aberta para um hacker. Um laptop pessoal que seja trazido ao escritório pode introduzir na rede corporativa qualquer tipo de malware que tenha coletado. Um laptop não protegido da companhia que tenha sido conectado a uma rede pública insegura pode finalmente trazer de volta todo o malware que tenha coletado para ser compartilhado com toda a companhia. Um roteador ou PC conectado por um visitante de maneira secreta a uma porta ethernet aberta pode lhe servir como porta das fundos (backdor) particular para dentro da rede corporativa. Um drive flash USB carregando um vírus pode infectar uma máquina pela simples conexão.

Ao mesmo tempo, administradores de rede devem tomar conta dos usuários que retornam a redes corporativas ou privadas. Políticas podem dizer o que os usuários são autorizados a fazer, mas testes e

controle de acesso pode garantir que as políticas estejam sendo seguidas.

O monitoramento contínuo do fluxo de dados pode identificar imediatamente dispositivos não autorizados. Além disso, sistemas de controle de acesso à rede podem varrer laptops da companhia em busca de vírus, trojans, spyware e adware para revelar vulnerabilidades ocultas que tenham sido trazidas para dentro da rede corporativa. Eles podem então segregar sistemas vulneráveis, corrigir o problema e depois permitir a eles direitos de acesso apropriados.

H.1b Direitos Excessivos de Usuário e Software Não Autorizado

Software não gerenciado introduz múltiplos riscos para a corporação. Este software pode conter vulnerabilidades de segurança e usuários podem não ser suficientemente diligentes sobre a aplicação de correções de segurança. Algumas vezes os usuários podem instalar software que, sem seu conhecimento, contém malware que pode comprometer toda a rede. Muitas vezes os usuários podem instalar fornecendo funcionalidades (P2P, por exemplo) que dão abertura a novas vulnerabilidades na rede. Aqueles que são responsáveis por cuidar da segurança das redes devem considerar implementar políticas e controles para detecção e correção para mitigar esta classe de vulnerabilidades.

Você está vulnerável se seus usuários podem instalar seu próprio software e você não tomou medidas para controlar aquele processo.

O controle chave que protege contra este conjunto de problemas é uma política totalmente implantada de limitação dos direitos do usuários. Se os usuários podem instalar software sem autorização então malwares que infectem estes sistemas podem também instalar software. Adicionalmente, listas de software autorizado (white lists) ajudam a limitar problemas, assim como todos os sistemas são verificados em busca da existência de software não autorizado quando eles se conectam à rede corporativa.

H1.2 Referências

<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17170&TEMPLATE=/ContentManagement/ContentDisplay.cfm>

http://www.techweb.com/wire/security/20020904_security

<http://technet2.microsoft.com/WindowsServer/en/library/e903f7a2-4def-4f5f-9480-41de6010fd291033.msp?mfr=true>

http://www.sans.org/resources/policies/Password_Policy.pdf

http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

<http://www.cerias.purdue.edu/weblogs/spaf/general/post-30/>

<http://www.csoon-line.com/caveat/062306.html>

[top^](#)

H2. Usuários (Phishing/Phishing Direcionado)

H2.1 Descrição

A palavra "phishing" foi usada pela primeira vez por volta de 1996 quando hackers começaram a roubar contas da America On-Line pelo envio de e-mail para usuários da AOL que aparentavam ter vindo da própria AOL. Ataques Phishing agora tem como alvo usuários on-line de banco, serviços de pagamento como PayPal e sites de e-commerce. Ataques Phishing estão crescendo rapidamente em número e

sofisticação. De fato, desde Agosto de 2003 a maioria dos grandes bancos dos EUA, Reino Unido e Austrália foram atingidos por ataques phishing.

Phishing de Senha/PIN

Phishers enviam e-mail para fazer com que você visite um web site onde você é enganado para expor suas informações bancárias de maneira que eles podem pegar o dinheiro de sua conta. Eles podem também usar de técnicas para obter dados de suas contas on-line tais como Hotmail, Yahoo e eBay. Uma vez em posse de seus nomes de usuário e senha os phishers tentarão obter informações de cobrança da vítima. Uma vez que alguém entra em sua conta eBay, por exemplo, eles tem acesso a suas transações do passado e atuais, informações pessoais como as informações de cobrança do PayPal e seu endereço físico.

Phishing VoIP

Uma forma mais nova de phishing substitui o web site por um número de telefone. Nesta forma de phishing um e-mail o orienta a telefonar para um número específico onde uma unidade de resposta de áudio, no outro fim de uma linha de telefone VoIP comprometida, espera para coletar seu número de conta, identificação pessoal, senha ou outros dados pessoais valiosos. A pessoa/unidade de áudio no outro fim da linha de telefone VoIP pode alegar que sua conta será fechada ou outros problemas podem ocorrer se você não responder.

Phishing Direcionado

Phishing direcionado (spear phishing) é um ataque de phishing altamente direcionado a um alvo. Spear phishers enviarão e-mail que inclui informações sobre funcionários ou problemas da organização que fazem com que a comunicação pareça genuína aos empregados ou membros de uma certa companhia, agência de governo, organização ou grupo. A mensagem pode parecer ter partido de seu empregador ou de um colega que pode enviar uma mensagem de e-mail para todos da companhia, tal como o diretor de recursos humanos ou a pessoa que gerencia os sistemas de computadores, e pode incluir pedidos de nomes de usuário ou senhas. Spear phishing se tornou uma das maneiras mais danosas de ataques em organizações militares dos EUA e outros países desenvolvidos. Os Atacantes obtêm informações de nome de usuário e senha e depois entram para ter acesso a informações militares confidenciais.

H2.1 Como Prevenir Ataques de Phishing

O método mais promissor de conter o ataque de phishing direcionado é o exercício contínuo para todos os seus usuários no qual eles tem experiência com phishing seguro. Uma criança normalmente aprende a não tocar um forno depois de queimar seus dedos. Ao fazer a experiência de phishing elucidadora, mas não dolorosa você pode obter o mesmo efeito sem causar dano real.

Uma segunda defesa é autenticação universal por dois fatores. Se sua organização não é economicamente forte para custear a autenticação por dois fatores algum outro método usado para prevenir ataques de phishing e outros tipos de comprometimento é a implementação de ferramentas de verificação como imagens secretas e ou questões de desafio e resposta. Imagens secretas funcionam da seguinte forma: um usuário seleciona uma ou mais imagens com antecedência. A imagem é conhecida apenas pelo usuário e pelo autenticador, o processo funciona pela exibição destas imagens para o usuário final, o usuário deve ser instruído de forma que quando esta imagem não está presente o site NÃO é legítimo e notificar um serviço de suporte ao usuário o mais rápido possível. Questões desafio funcionam pela seleção de questões secretas pelo usuário com antecedência de forma que apenas o usuário e o autenticador conheçam pergunta e resposta. Quando em processo de autenticação os usuários são desafiados com uma pergunta e devem responder com as respostas pré-definidas.

Métodos menos efetivos, mas ainda assim valiosos incluem

- Não envie mensagens em massa para sua base de cliente com links web direcionado para o seu site ou qualquer outro. Fazendo isso você ensina sua base de clientes a aceitar a abertura de links web e a assumi-los confiáveis. Isto dá abertura em sua organização para ataques Phishing no futuro.
- Não use suas credenciais de autenticação ou outras informações pessoais não públicas para autenticar sua base de clientes. (código de identificação ou número de Seguridade Social para o seu portal web on-line, por exemplo)
- Registre o log de informações como endereço IP, informações de localização e assinaturas do computador para rastrear qualquer dispositivo tendo acesso a dados de clientes on-line.
- Esteja certo de reportar todos os incidentes de fraude para uma agência que possa garantir o cumprimento da lei de forma que os dados possam ser correlacionados com outros ataques para a criação de padrões de ataques e incidentes.
- **Software Anti-Phishing:** Aplicações que tentam identificar conteúdo de Phishing tanto em e-mail quanto em web sites normalmente se integra com Navegadores Web e clientes de e-mail na forma de uma barra de ferramentas que exibe o verdadeiro nome de domínio do website que o navegador está prestes a visitar ou está atualmente visitando numa tentativa de prevenir atividade fraudulenta. Existem muitas opções de software, tanto na forma de recurso embutido e num software ou um plug-in para Firefox e Internet Explorer.
 - [Microsoft IE 7](#)
 - [NetCraft Toolbar](#): disponível tanto para Internet Explorer quanto para Firefox
 - [Google Safe browsing](#): disponível para Firefox
 - [Ebay Toolbar](#): disponível para Internet Explorer
 - [Earthlink Scamblocker](#): disponível tanto para Internet Explorer quanto para Firefox
 - [Geotrust Trustwatch](#) - disponível para Internet Explorer, Firefox e [Flock](#)
- **Educação de Usuários** Uma das melhores estratégias para combater Phishing é educar seus usuários sobre os métodos atuais e novos de ataques phishing, torná-los capazes de saber o que fazer no caso de um ataque phishing. Eduque seus usuários que recebem contatos sobre contas de usuário. Eduque seus usuários a entrar em contato com sua Hotline caso eles sejam solicitados a fornecer quaisquer informações pessoais. Os usuários devem ser orientados a digitar o URL direto de seu portal web na barra de endereços toda vez que visitarem seu site para reduzir o risco de seguir um link fraudulento, especialmente quando isto acontece por e-mail.
- **Autenticação de Dois Fatores / Modos:** Enquanto nenhum método de prevenção é totalmente infalível outro método tecnologicamente preferido usado para prevenir ataques phishing e outros tipos de comprometimentos é a implementação de ferramentas de verificação tais como imagens secretas e desafios pergunta-resposta. Secret Images works by having a user select one or more images in advance. As imagens secretas são conhecidas apenas pelo usuário e pelo autenticador, o processo funciona pela exibição destas imagens para o usuário final. Os usuários finais devem ser instruídos a considerar o site NÃO legítimo quando estas imagens não são exibidas e a entrar em contato com o departamento de suporte ao usuário assim que possível. Questões Desafio

funcionam ao fazer com que o usuário selecione múltiplas questões previamente, que apenas usuário e autenticador conheçam. Ao autenticar os usuários são então desafiados e respondem com as respostas pré-definidas.

H2.2 Referências

AntiPhishing Working Group

<http://www.antiphishing.org/>

<http://www.3sharp.com/projects/antiphishing/gonephishing.pdf>

VoIP Phishing Scams

<http://blogs.pcworld.com/staffblog/archives/001921.html>

[top^](#)

Z1: Seção Especial: Ataques Zero Day e Estratégias de Prevenção

Z1.1 Descrição

Enquanto os riscos de vulnerabilidades zero day em aplicações populares e sua subsequente exploração tenham sido discutidas por muitos anos, ataques zero day viram um crescimento significativo 2006. Uma vulnerabilidade zero day ocorre quando uma falha no código de um software é descoberta e exploits da falha surgem antes que uma correção seja oferecida pelo fabricante. Se um exploit que funciona da vulnerabilidade se torna disponível publicamente usuários do software afetado são expostos a ataques até que uma correção de software seja disponível ou alguma forma de mitigação é aplicada pelo usuário. Passos de mitigação e proteção são explicados mais adiante nesta seção.

Z1.2. Sistemas Operacionais Afetados

Todos os sistemas operacionais e todas as aplicações de software são vulneráveis à descoberta de uma vulnerabilidade zero day e exploração. Embora o alvo da maioria dos ataques neste tenham sido produtos Microsoft a Apple sofreu de diversos exploits zero day também. Além do OS X da Apple, nenhum outro ataque zero day foi reportado para Linux, BSD ou outros sistemas operacionais baseados em Unix.

Z1.3. Entradas CVE

Neste último ano muitas vulnerabilidades tiveram exploits tornados públicos antes que uma correção oficial ou remediação tivesse sido divulgada. Alguns exemplos de entradas CVE que refletem esta tendência são:

- Windows Graphical Device Interface Library (.wmf) [CVE-2005-4560](#)
- Microsoft Internet Explorer [CVE-2006-1245](#)
- Microsoft Internet Explorer [CVE-2006-1359](#)
- Microsoft Internet Explorer [CVE-2006-1388](#)
- Microsoft Internet Explorer [CVE-2006-3280](#)
- Microsoft Internet Explorer [CVE-2006-3281](#)
- Microsoft Internet Explorer [CVE-2006-4777](#)

-
- Apple OS X [CVE-2006-1982](#)
 - Apple OS X [CVE-2006-1983](#)
 - Apple Safari [CVE-2006-1986](#)
 - Apple Safari [CVE-2006-1987](#)
 - Microsoft Word [CVE-2006-2492](#)
 - Microsoft Excel [CVE-2006-3086](#)
 - Microsoft PowerPoint [CVE-2006-3590](#)
 - Microsoft PowerPoint [CVE-2006-4694](#)
 - Microsoft PowerPoint [CVE-2006-5296](#)
 - Microsoft Windows Help File Viewer [CVE-2006-4138](#)
 - Microsoft Internet Explorer and Outlook [CVE-2006-4868](#)
 - Microsoft Visual Studio [CVE-2006-4704](#)
 - Microsoft XML HTTP ActiveX [CVE-2006-5745](#)

Z1.4. Como se Proteger Contra as vulnerabilidades

Proteger contra a exploração de uma vulnerabilidade zero day é um problema que causa grande preocupação na maioria dos administradores de sistema. Para reduzir o impacto de um ataque zero day siga as melhores práticas de negócio, como:

- Adote negação total em firewalls e dispositivos de perímetro que protegem redes internas
- Separe servidores ligados diretamente à Internet de servidores internos
- Desative serviços desnecessários e remova aplicações de usuário que não sejam necessários operacionalmente
- Siga o princípio do menor privilégio possível quando definir controles de acesso, permissões e direitos de usuários
- Restrinja ou limite o uso de código ativo como Java script ou ActiveX em navegadores
- Eduque os usuários sobre a abertura de arquivos anexos não solicitados
- Desabilite a possibilidade de o usuário seguir links em e-mail
- Desabilite a possibilidade de download automático de imagens da web em e-mail
- Mantenha um serviço interno de alertas de segurança agressivo (ou realize outsource desta atividade) para se tornar ciente de exploits zero-day assim que eles se tornam públicos.
- Use soluções de gerenciamento para instalar correções de segurança ou medidas paliativas assim que eles se tornam públicos
- Se você usa o serviço Active Directory da Microsoft tire máximo proveito de Group Policy Objects para controlar o acesso dos usuários

-
- Não confie apenas na proteção dos anti-vírus uma vez que ataques zero-day attacks normalmente não são detectáveis até que novas assinaturas sejam publicadas
 - Use proteção contra buffer overflow oferecida por terceiros em todos os sistemas quando possível
 - Siga as recomendações do fornecedor do software sobre medidas paliativas e mitigações até que uma correção esteja disponível

[top^](#)

Os Especialistas que Ajudaram a Criar a Lista Top-20 2006

- Gerente do Projeto e Editor: Rohit Dhamankar, TippingPoint, uma divisão da 3Com
- Adam Safier, Global Systems & Strategies, Inc.
- Alan Rouse, Security Architect, TANDBERG Television
- Alexander Kotkov, UBS Investment Bank
- Amol Sarwate, Gerente do Laboratório de Vulnerabilidade, Qualys
- Andrew van der Stock, Diretor, OWASP
- Anton Chuvakin, Diretor da Gerência de Produtos @ LogLogic
- Anthony Richardson, Monash University, Australia
- Arturo "Buanzo" Busleiman - Consultor Independente de Segurança, Argentina
- Cesar Tascon Alvarez, Ernst and Young, Spain
- Christopher Bream, PricewaterhouseCoopers
- Chris Riley, Spherion
- Christopher Rowe, Guilford Technical Community College
- Ed Fisher, Ingersoll Rand
- Gerhard Eschelbeck, CTO, Webroot
- David Damato, PricewaterhouseCoopers
- Donald Smith, Qwest
- Edward Ray, Netsec Design and Consulting
- James King, TippingPoint, a division of 3Com
- Jean-Francois Legault, Deloitte & Touche LLP
- Jeff Pike, Integrated Team Solutions Facility
- John-Thomas Gaietto
- John Tannahill
- Johannes Ullrich, Internet Storm Center, SANS
- Jonathan Rubin, Dominion
- Kevin Hong, Korea Information Security Agency (KISA) e KrCERT/CC
- Koon Yaw Tan, Infocomm Development Authority of Singapore
- Leo Pastor, Advanced Consulting and Training, Argentina and Brazil
- Marcos A. Ferreira Jr., NX Security, Brazil
- Marcus Sachs, SRI International and Internet Storm Center, SANS
- Mark J Cox, RedHat
- Mark Goudie, Data Networking Services, Australia
- Matteo Shea, Senior Security Engineer, Communication Valley S.p.a
- Michel Cusin, Bell Security Solutions, Canada
- Michele Guel, Cisco Systems
- Miguel Guirao, Telcel

-
- Olivier Devaux, vulnpedia.com
 - Pedro Bueno - McAfee AvertLabs
 - Rajesh Mony, Webroot
 - Ralf Durkee, Security Consultant
 - Rhodri Davies, Vistorm, UK
 - Richard Bejtlich, Taosecurity
 - Rick Wanner, Technical Analyst, Corporate Security, SaskTel
 - Robert Baskerville, Vistorm, UK
 - Pedro Paulo Ferreira Bueno, Brasil Telecom
 - Sandeep Dhameja, Ambiron Trustwave
 - Syed Mohamed

Agências

- Department of Homeland Security (DHS)
- Computer Emergency Response Team (CERT)
- National Infrastructure Security Coordination Centre (NISCC, UK)
- Computer Emergency Response Team, Canada

Os Especialistas que Colaboraram na Tradução da Lista Top-20 2006 para o Português

- Atanaí Ticianelli
- Ivo Peixinho
- Jacomo Piccolini
- Ronaldo Vasconcellos

Todos os colaboradores são analistas de segurança do CAIS - Centro de Atendimento a Incidentes de Segurança da RNP - Rede Nacional de Ensino e Pesquisa, Brasil.

[top^](#)

SANS Top-20 2006 FAQ

Por Rohit Dhamankar, Diretor de Projeto do Top 20

Para quem a lista é escrita?

Nos últimos anos se tornou claro para mim que a lista SANS Top-20 list é usada por organizações bem diversas. Algumas organizações de grande porte usam a lista Top-20 para fazer uma verificação dupla dos seus esforços de segurança em andamento, visto que algumas organizações pequenas usam esta lista exclusivamente para guiar seu esforço de correção de vulnerabilidades como um todo. Assim, ao criar a lista nos tentamos servir as diversas audiências.

Ainda é relevante publicar este documento em 2006 para um ano inteiro de vulnerabilidades?

Examinando os seguintes fatos a resposta é um claro "sim".

-
- Dados de varredura na Internet mostra que ainda há sistemas ligados diretamente à Internet que não estão corrigidos de vulnerabilidades sendo exploradas amplamente. Eu por exemplo desistirei deste projeto quando eu não ver mais nenhum evento de Blaster ou Slammer disparando qualquer IDS/IPS das redes de clientes.
 - Mesmo que todas correções tenham sido aplicadas ainda há zero-days com que lidar! A lista deste ano inclui uma lista de defesas para zero-days.
 - Profissionais de segurança se tornam tão focados no "desafio do dia" que precisam de lembretes, de tempos em tempos, de ameaças emergentes de forma que eles possam pedir por recursos para lutar contra estas novas ameaças.

Por que vocês chamam a lista de Top 20 quando o número real de vulnerabilidades(CVE's) é bem maior do que 20?

- A vida seria muito mais simples se alguém pudesse listar 20 números CVE críticos e dizer que proteger contra ataques usando estas vulnerabilidades poderia fazer a Internet segura. A realidade, todos nós conhecemos, é bem distante disto. Se alguém simplesmente pegar as vulnerabilidades web semanais no último ano o número de vulnerabilidades críticas é bem maior do que 100! Estas são as vulnerabilidades que resultam em centenas de milhares de tentativas de ataques diariamente. A abordagem do Top-20 é ajudar as pessoas a focar em "classes" de vulnerabilidades sendo exploradas e fornecer orientação a administradores de sistema, programadores e CIOs sobre como mitigar cada classe de falhas.
- Os 20 maiores grupos de vulnerabilidades críticas em classes de forma que estratégias de mitigação comuns possam ser aplicadas para proteger toda uma classe. Por exemplo, um grande número de overflows MS-RPC pode ser prevenido pelo bloqueio das portas 139/tcp e 445/tcp no perímetro da rede.
- O Top-20 também ajuda a identificar os vetores de propagação usados por um grande número de malware. Ainda é triste ver em 2006 malware se propagando com sucesso por ataques de força bruta de senha!
- Finalmente, o desafio de identificar as classes de vulnerabilidades não é um problema de "cookie cutter". Há plataformas como Mac OS que usam uma boa quantidade de pacotes UNIX; entretanto, a Apple publica correções para os pacotes herdados de UNIS juntamente com outros problemas de Mac OS X. Como resultado, um grande número de vulnerabilidades de severidades variadas são incluídas em uma única correção da Apple. A recomendação, que pode parecer trivial, é aplicar as correções. Entretanto, ao mesmo tempo, é de muito valor apontar técnicas de exploração emergentes para tais plataformas com sua própria classe!

Se você quiser você pode começar a chamar a lista de "Top 20 SANS de Classes de Ataque Alvo" ou "Top 20 SANS de Grupos de Vulnerabilidades." Nós decidimos chamá-la de "SANS Top 20".

Se você tem quaisquer comentários por favor escreva para top20@sans.org

[top^](#)
