

São Paulo, 15 de julho de 2010

CERT.br registra aumento de notificações de *phishing*

*Relatos de páginas falsas de bancos e sites de
comércio eletrônico aumenta continuamente há um ano*

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), um dos serviços disponibilizados pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), divulga os dados sobre notificações de incidentes de segurança na Internet no segundo trimestre de 2010. As estatísticas são obtidas com base nos relatos enviados espontaneamente por administradores de redes e usuários brasileiros. Os dados completos podem ser consultados em <http://www.cert.br/stats/incidentes/>.

O número total de notificações de incidentes no segundo trimestre de 2010 foi superior a 32 mil, o que corresponde a um acréscimo de 16% em relação ao trimestre anterior e decréscimo de 59% em relação ao mesmo período de 2009. Cristine Hoepers, analista de segurança do CERT.br, aponta o motivo da diminuição: “O maior responsável pela queda em relação ao segundo trimestre de 2009 foi a redução nas notificações de eventuais quebras de direitos autorais, através de distribuição de material em redes P2P”.

Tentativas de fraude

As notificações de tentativas de fraude no segundo trimestre de 2010 foram superiores a oito mil, correspondendo a um decréscimo de 4% em relação ao trimestre anterior e a um decréscimo de 87% em relação ao mesmo período de 2009.

O número de notificações de páginas falsas de bancos e *sites* de comércio eletrônico (*phishing* tradicional) sofreu um aumento de 47% em relação ao trimestre anterior e 136% em relação ao mesmo período de 2009.

As notificações sobre cavalos de tróia, utilizados para furtar informações e credenciais, reduziram 22% em relação ao primeiro trimestre de 2010, e não apresentaram evolução em relação ao mesmo período de 2009.

Ataques a servidores *Web*

As notificações sobre ataques a servidores *Web* cresceram 14% em relação ao trimestre anterior e 28% em relação ao mesmo período de 2009. Além de visarem a hospedagem de páginas falsas de instituições financeiras e de cavalos de Tróia, esses ataques, que exploram vulnerabilidades em aplicações *Web*, estão sendo

utilizados para manter repositórios de ferramentas utilizadas em ataques a outros servidores *Web* e scripts para envio de spam ou *scam*.

Varreduras e propagação de códigos maliciosos

As notificações referentes a varreduras aumentaram 62% em relação ao trimestre anterior e 28% em relação ao mesmo período de 2009.

Os serviços que podem sofrer ataque de força bruta como SSH (22/TCP), TELNET (23/TCP) e FTP (21/TCP) ainda estão sendo muito visados nas varreduras, correspondendo a, respectivamente, 46%, 11% e 2% das notificações. Além destas, notou-se um aumento nas varreduras de RDC (3389/TCP) que corresponde a 2% das notificações. Esse serviço permite administração remota de máquinas Windows.

As notificações de varreduras de SMTP (25/TCP) continuam em destaque atingindo 16% do total. As reclamações em sua maior parte foram referentes a computadores brasileiros, conectados via banda larga, que tentaram identificar *relays* abertos fora do Brasil, com intuito de posteriormente enviar *spam*. “À medida que a gerência de Porta 25 em redes de caráter residencial for adotada, a tendência será de queda neste tipo de varredura”, destaca Cristine.

As notificações de atividades relacionadas com a propagação de *worms* totalizaram quase cinco mil, correspondendo a um decréscimo de 19% em relação ao trimestre anterior e acréscimo de 36% em relação ao mesmo período de 2009.

Outros incidentes reportados

No segundo trimestre de 2010 foram recebidas 1.080 notificações que se enquadraram na categoria "outros", que correspondem a um decréscimo de 42% em relação ao primeiro trimestre de 2010. A quantidade de notificações foi similar a do mesmo período de 2009. Esta categoria está relacionada à hospedagem de *scripts* e *toolkits*, utilizados para comprometimento de *sites* de terceiros.

Sobre o CERT.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em <http://www.cert.br/>.

Sobre o Núcleo de Informação e Coordenação (NIC.br)

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (<http://www.nic.br/>) é uma entidade civil, sem fins lucrativos, que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil. São atividades permanentes do NIC.br coordenar



Núcleo de Informação
e Coordenação

o registro de nomes de domínio — Registro.br (<http://www.registro.br/>), estudar, responder e tratar incidentes de segurança no Brasil - CERT.br (<http://www.cert.br/>), estudar e pesquisar tecnologias de redes e operações — CEPTR0.br (<http://www.ceptro.br/>), produzir indicadores sobre as tecnologias da informação e da comunicação — CETIC.br (<http://www.cetic.br/>) e abrigar o escritório do W3C no Brasil (<http://www.w3c.br/>).

Sobre o Comitê Gestor da Internet no Brasil – CGI.br

O Comitê Gestor da Internet no Brasil coordena e integra todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Mais informações em <http://www.cgi.br/>.

Para mais informações, acesse: <http://www.s2.com.br> ou <http://www.cgi.br/>

Contatos para a Imprensa: S2 Comunicação Integrada

<http://www.s2.com.br>

Twitter / Flickr / Youtube: S2comunicacao

Everton Schultz - everton.schultz@s2.com.br

Juliana Gilio - juliana.gilio@s2.com.br

Assessoria de Comunicação - NIC.br

Caroline D'Avo – Assessora de Comunicação – caroline@nic.br

Everton Teles Rodrigues – Assistente de Comunicação – everton@nic.br

Flickr: <http://www.flickr.com/NICbr/>

Twitter: <http://www.twitter.com/comuNICbr/>