

CAIS-Resumo: Setembro a Dezembro de 2013

Alertas, vulnerabilidades e incidentes de segurança

[RNP, 28.01.2013-, revisão 01]

Publicação quadrimestral do Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa

Setembro a dezembro de 2013

Disponível em: <http://www.rnp.br/cais/alertas/2013/cais-res-2013-3.html>

Neste CAIS Resumo, são abordados os alertas, as vulnerabilidades e os demais acontecimentos que se destacaram na área de segurança no terceiro quadrimestre de 2013.

- 1. Destaques**
- 2. Alertas**
- 3. CAIS na Mídia**
- 4. Estatísticas**
- 5. Notas**

1. Destaques

- De setembro a dezembro de 2013, o CAIS tratou 30.033 incidentes de segurança identificados na rede da RNP, com parciais de 5.338 em setembro, 5.836 em outubro, 6.572 em novembro e 12.287 em dezembro.
- A quantidade de incidentes tratados durante o terceiro quadrimestre de 2013 diminuiu 7.58% em relação ao período de maio a agosto de 2013.
- Os casos de máquinas infectadas com Worm/Bot diminuíram de 34.437 para 29.492, representando 70,33% dos incidentes tratados no período de maio a agosto de 2012.
- Os incidentes de envio de spam no backbone acadêmico aumentaram em relação ao quadrimestre anterior, com parciais de 985 em maio, 891 em junho, 741 em julho e 686 em agosto, representando 7,88% do total de incidentes tratados neste período.
- A utilização de páginas web falsas em ataques de fraude contra instituições financeiras e a tentativa de exploração de vulnerabilidades em servidores DNS apresentaram um aumento. Nesse quadrimestre, o CAIS notificou 8.891 incidentes de tentativa de exploração de vulnerabilidades contra 1.263 notificações realizadas no quadrimestre anterior.

- Os casos de máquinas infectadas com Worm/Bot tiveram um queda, representando 58.77% dos incidentes tratados no período de setembro a dezembro de 2013.
- Também diminuiu o número de incidentes de spam neste quadrimestre. Houve uma queda de 59.84% (de 2.981 para 1.197 incidentes nos quatro últimos meses de 2013).
- De setembro a dezembro, foram cadastradas 370 novas fraudes no [Catálogo de Fraudes do CAIS](#), totalizando 5391 fraudes desde o lançamento do serviço, em março de 2008.

2. Alertas

Neste quadrimestre, o CAIS divulgou sete (7) alertas de segurança através da lista CAIS-Alerta. Abaixo, segue uma relação dos alertas do período.

[CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Dezembro/2013](#)

Microsoft Security Bulletin Summary for December 2013
[RNP, 11.12.2013]

[CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Novembro/2013](#)

Microsoft Security Bulletin Summary for November 2013
[RNP, 14.11.2013]

[CAIS-Alerta: vulnerabilidade no plugin PHP Weathermap para CACTI](#)

[RNP, 08.11.2013]

[CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Outubro/2013](#)

Microsoft Security Bulletin Summary for October 2013
[RNP, 11.07.2012]

[CAIS-Resumo: Maio a Agosto de 2013](#)

Alertas, vulnerabilidades e incidentes de segurança
[RNP, 27.09.2013]

[CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Setembro/2013](#)

Microsoft Security Bulletin Summary for September 2013
[RNP, 19.09.2013]

3. CAIS na Mídia

A seguir estão relacionadas as matérias e entrevistas que contaram com a participação da equipe do CAIS.

- [Encontro sobre Segurança em Informática acontece na UFBA](#)
- [Workshop de tecnologia em redes do PoP-SC](#)

4. Estatísticas

Apresentamos uma análise comparativa das estatísticas de incidentes reportados ao CAIS no terceiro quadrimestre de 2013 em relação a dados do período correspondente em anos anteriores.

Mês	2011	2012	2013
set	23.798	9.889	5.338
out	25.505	12.143	5.836
nov	21.407	9.472	6.572
dez	12.195	13.632	12.287
TOTAL	82.905	45.136	30.033

No terceiro quadrimestre de 2013, o CAIS tratou 30.033 incidentes de segurança. Foi observado uma redução de 33.46% no total de incidentes tratados de setembro a dezembro em comparação com o mesmo período de 2012 e uma redução de 63.77% em relação ao mesmo período de 2011.

Quadrimestre anterior	#incidentes	Quadrimestre atual	#incidentes
Mai/2013	8.208	Set/2013	5.338
Jun/2013	7.487	Out/2013	5.836
Jul/2013	7.481	Nov/2013	6.572
Ago/2013	9.321	Dez/2013	12.287
TOTAL	32.497		30.033
Média	8.124		7.508

A média de incidentes no terceiro quadrimestre de 2013 diminuiu 2464 em relação ao quadrimestre anterior. Ainda neste quadrimestre, a quantidade de incidentes em dezembro superou os demais meses, principalmente por conta de incidentes relacionados à Intrusão (comprometimento de aplicação envolvendo servidores DNS).

Média mensal de incidentes (nos últimos anos)	
Ano	#incidentes
2013	8.893
2012	11.120

2011	26.611
2010	8.753

A média mensal de incidentes tratados em 2013 é de 8.893 incidentes ao mês, valor 20.02% menor que a média mensal de 2012.

5. Notas

O CAIS ressalta que manter os sistemas e aplicativos atualizados, seguir uma política de segurança e orientar os usuários são algumas das práticas recomendadas para diminuir os riscos de comprometimento de sua rede, além de contribuir para o aumento da segurança da Internet como um todo.

Assim, o CAIS recomenda aos administradores que se mantenham cientes e conscientes dos alertas, correções e atualizações disponibilizados pelos fabricantes e órgãos de renome na área de segurança.

CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)

Rede Nacional de Ensino e Pesquisa (RNP)

cais@cais.rnp.br

<http://www.cais.rnp.br>

Tel. 019-37873300 Fax. 019-37873301

Chave PGP disponível: <http://www.rnp.br/cais/cais-pgp.key>