Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

ESTATÍSTICAS DE INCIDENTES DE REDE NA APF – ANO 2014

1. Apresentação

As informações estatísticas publicadas neste documento referem-se ao período de janeiro a dezembro de 2014 e apresentam algumas considerações sobre o trabalho de detecção, análise e resposta a incidentes de rede desenvolvido pelo Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal – CTIR Gov.

Para fins de análise, o CTIR Gov considera: (a) **Notificações**: eventos detectados e/ou reportados ao Centro para o endereço ctir@ctir.gov.br, incluindo os considerados como não incidentes, *spams*, falso-positivos, reiterações de incidentes já tratados e outras correspondências relacionadas às tarefas intermediárias da atividade de tratamento de incidentes de rede; (b) **Incidentes:** são as notificações que, após processo de triagem, são caracterizados como evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, conforme NC 05/IN01/DSIC/GSIPR; (c) **Resolvidos**: incidentes finalizados com tratamento realizado com sucesso; (d) **Pendentes**: incidentes que aguardam ação de terceiro para resolução; (e) **Não Resolvidos**: incidentes que aguardaram ação de terceiro por prazo estabelecido e não obtiveram sucesso na resolução.

2. Gráficos

2.1 – Distribuição de notificações de incidentes por status e mês de criação

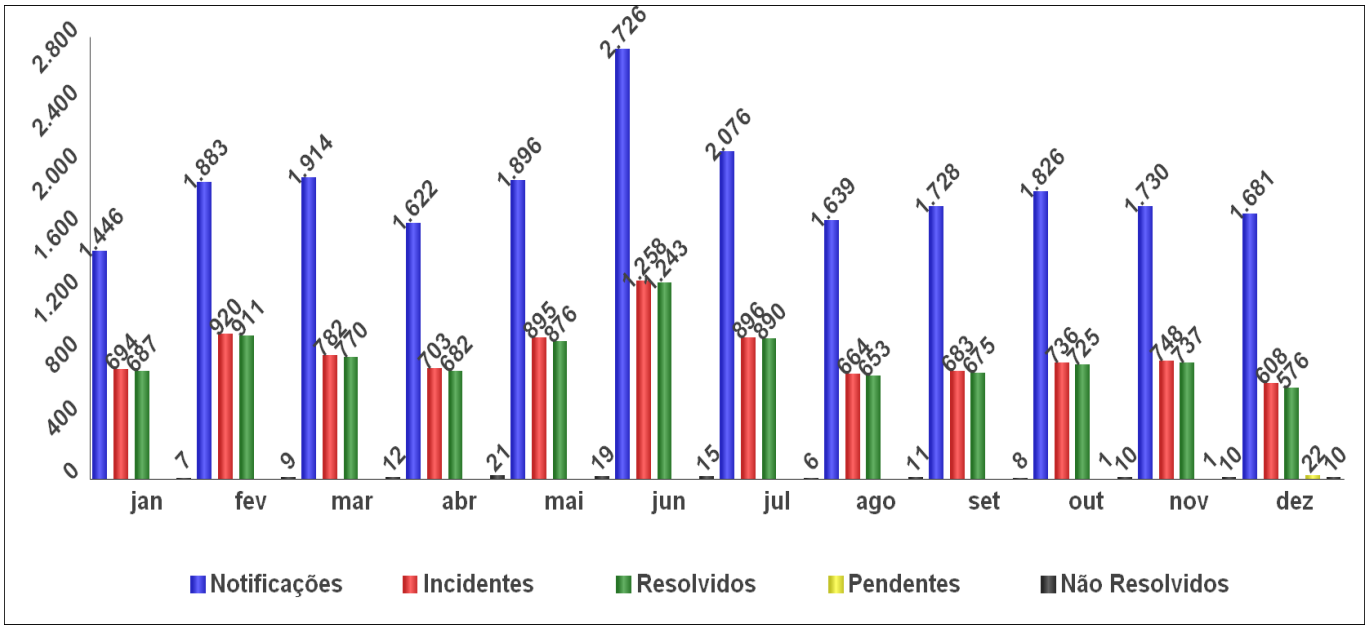

Gráfico 1 – Distribuição de notificações por status e mês de criação

2.2 – Distribuição de incidentes por categoria

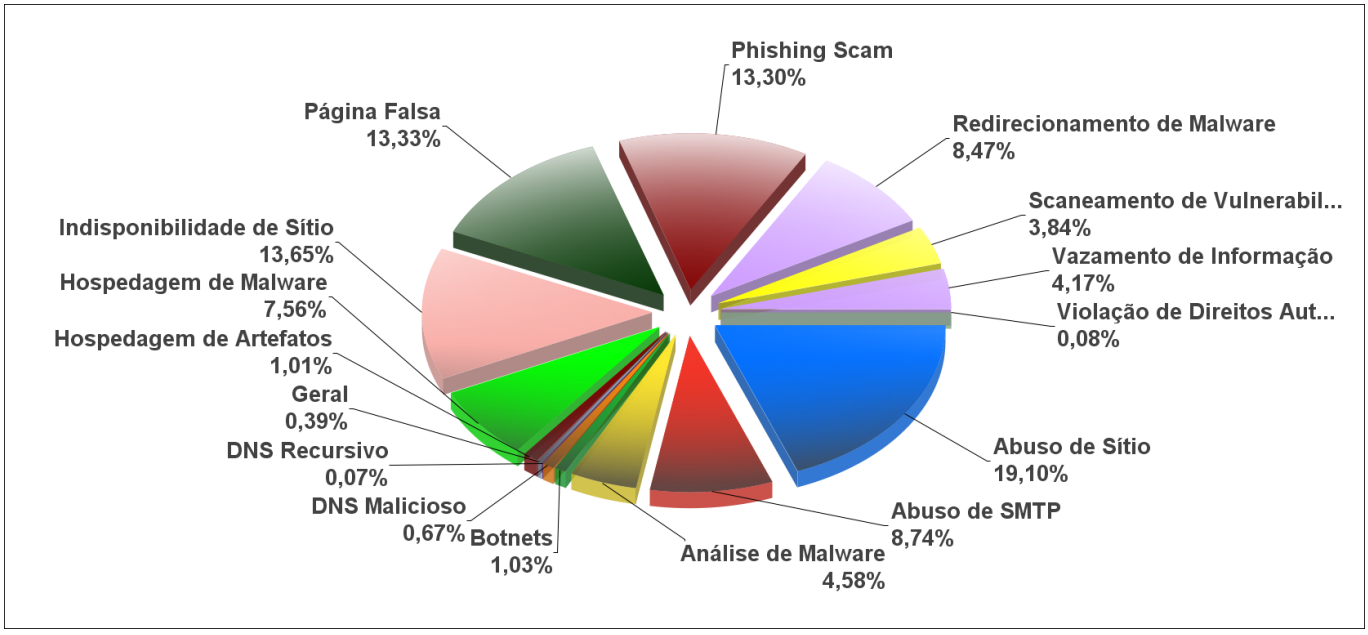

Gráfico 2 – Distribuição de incidentes por categoria

2.3 – Subtipos da categoria Abuso de Sítios

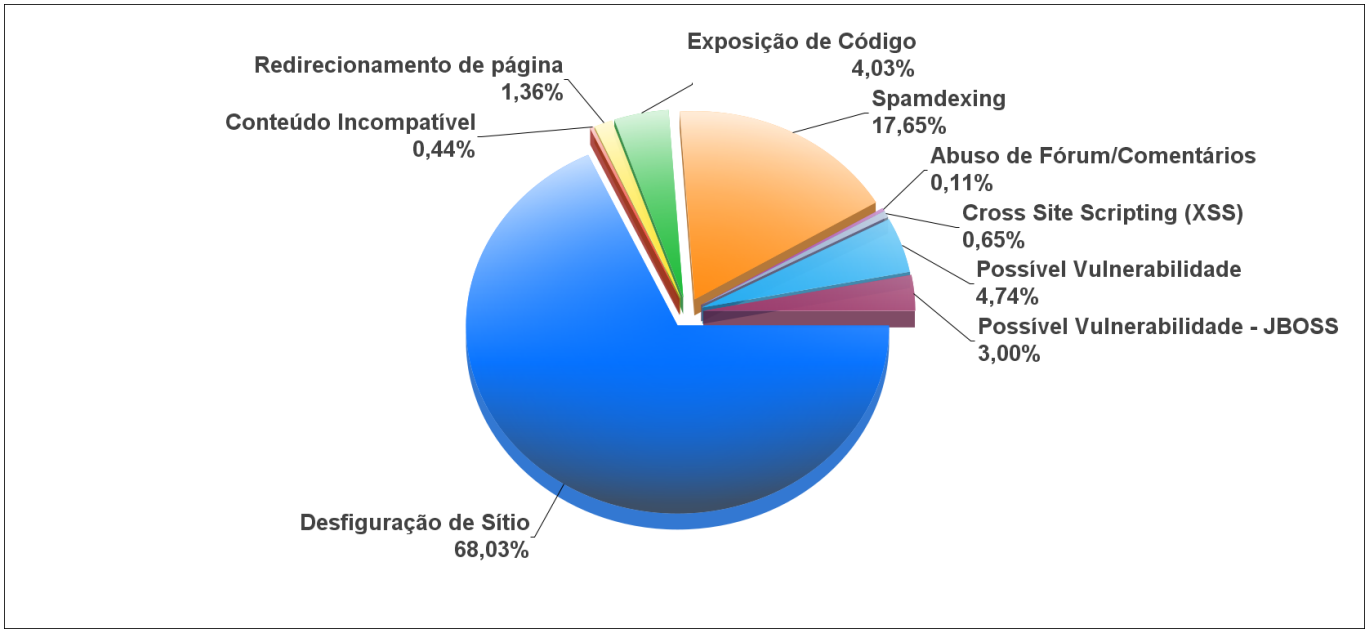

Gráfico 3 – Subtipos da categoria Abuso de Sítios

2.4 – Distribuição de notificações de Abuso de Sítios por UF

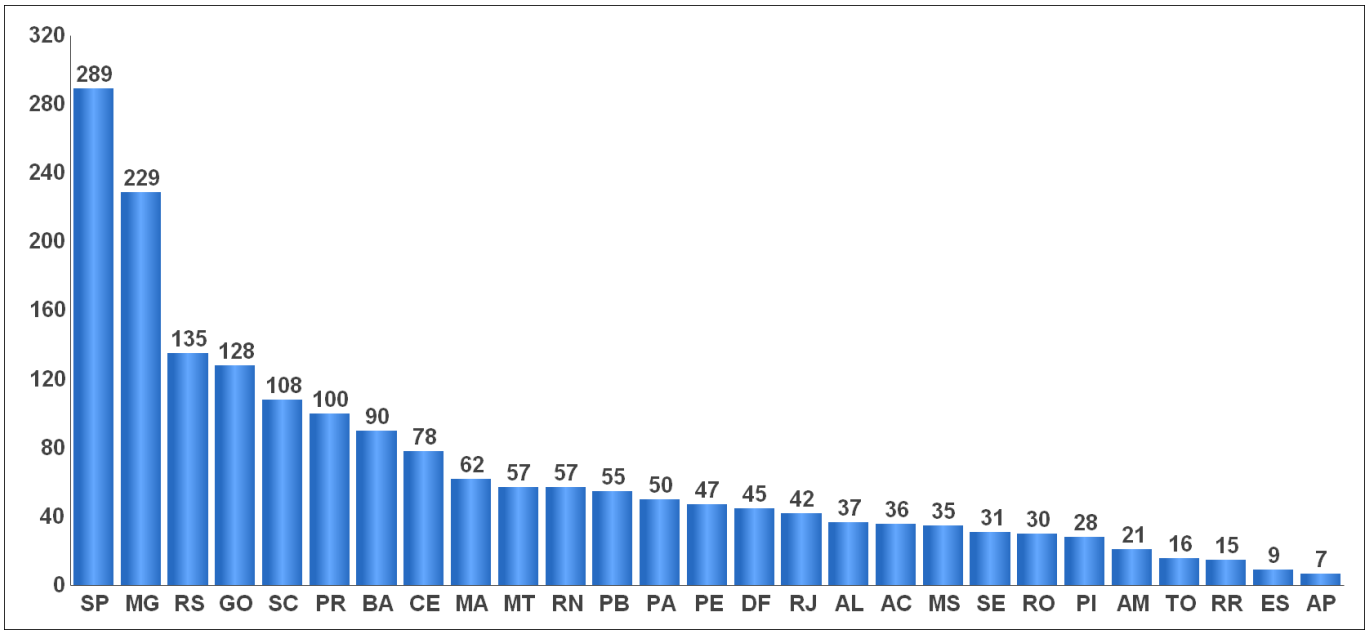

Gráfico 4 – Distribuição de notificações de Abuso de Sítios por UF

2.5– Domínios de hospedagem ou redirecionamento de *Malwares*

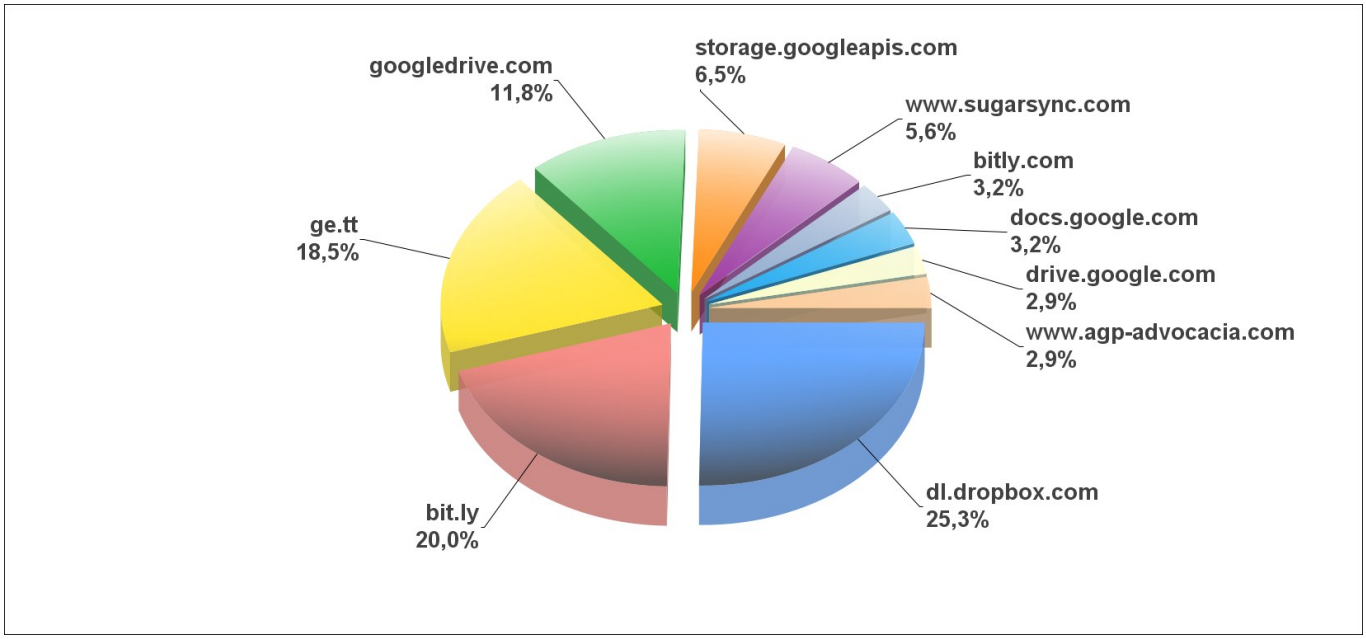

Gráfico 5 – Distribuição de domínios de hospedagem/redirecionamento de *Malwares*

2.6– Países destinatários das notificações de incidentes

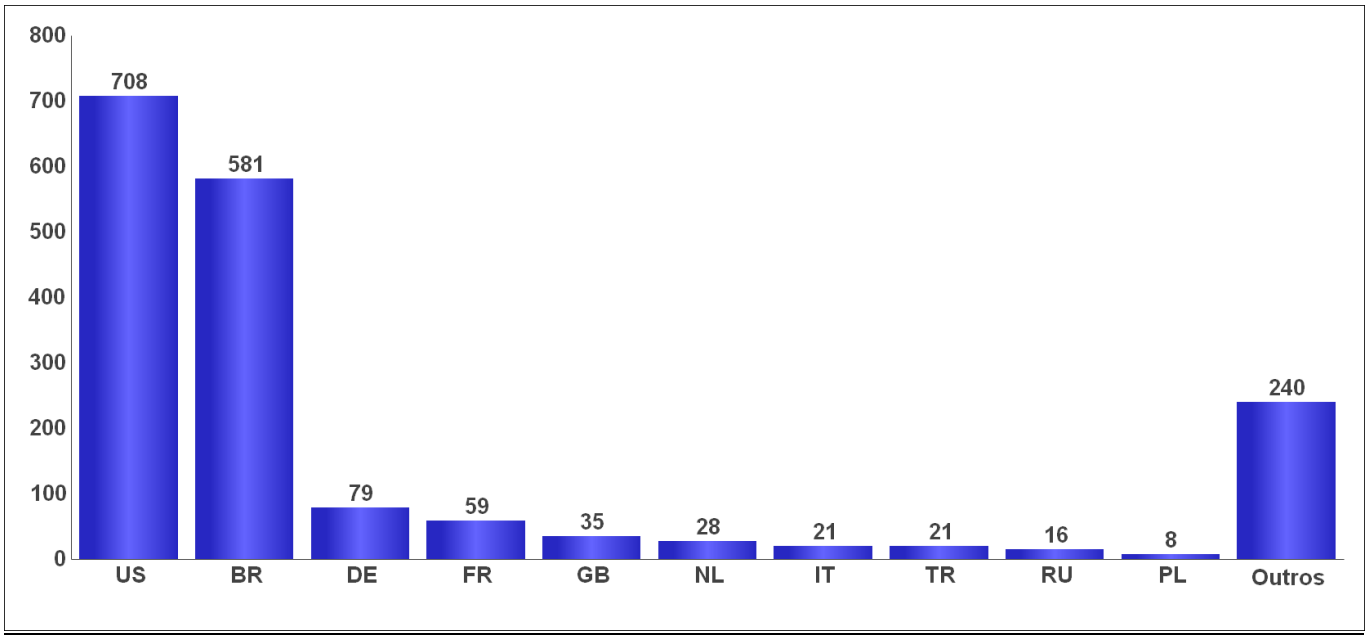

Gráfico 6 – Países destinatários das notificações de incidentes

2.7 – Tempo de resolução dos Incidentes

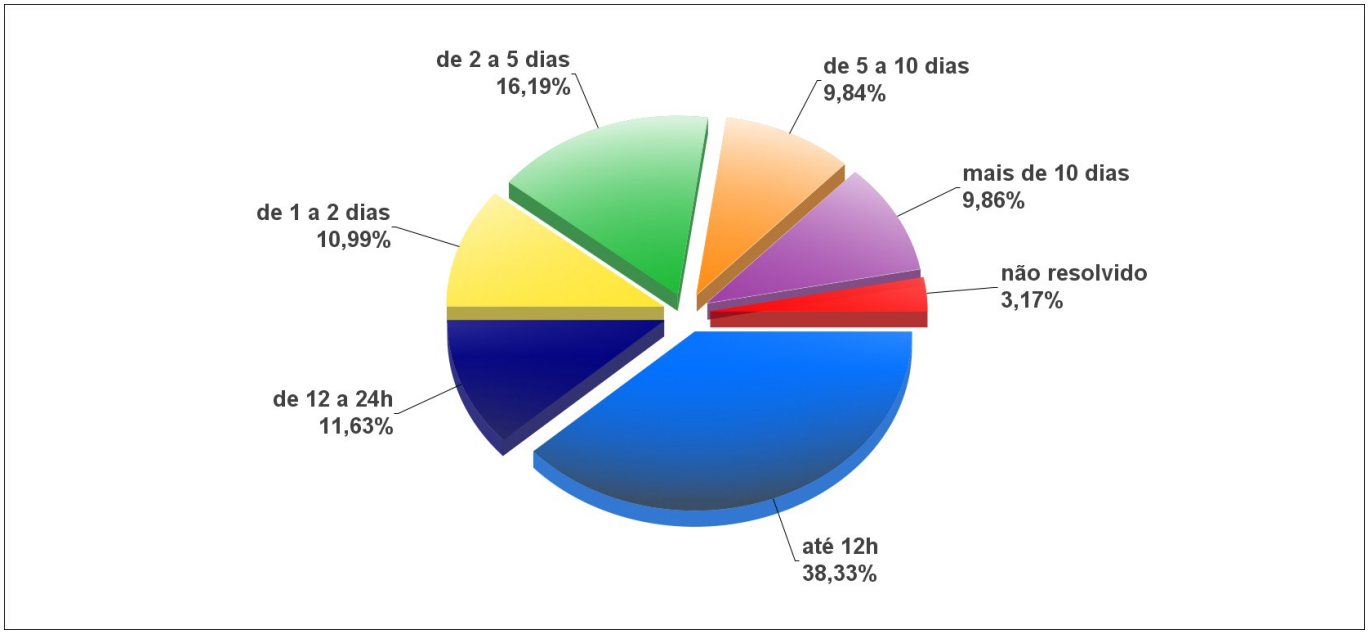

Gráfico 7 – Tempo de resolução

CTIR Gov/DSIC/GSIPR
www.ctir.gov.br