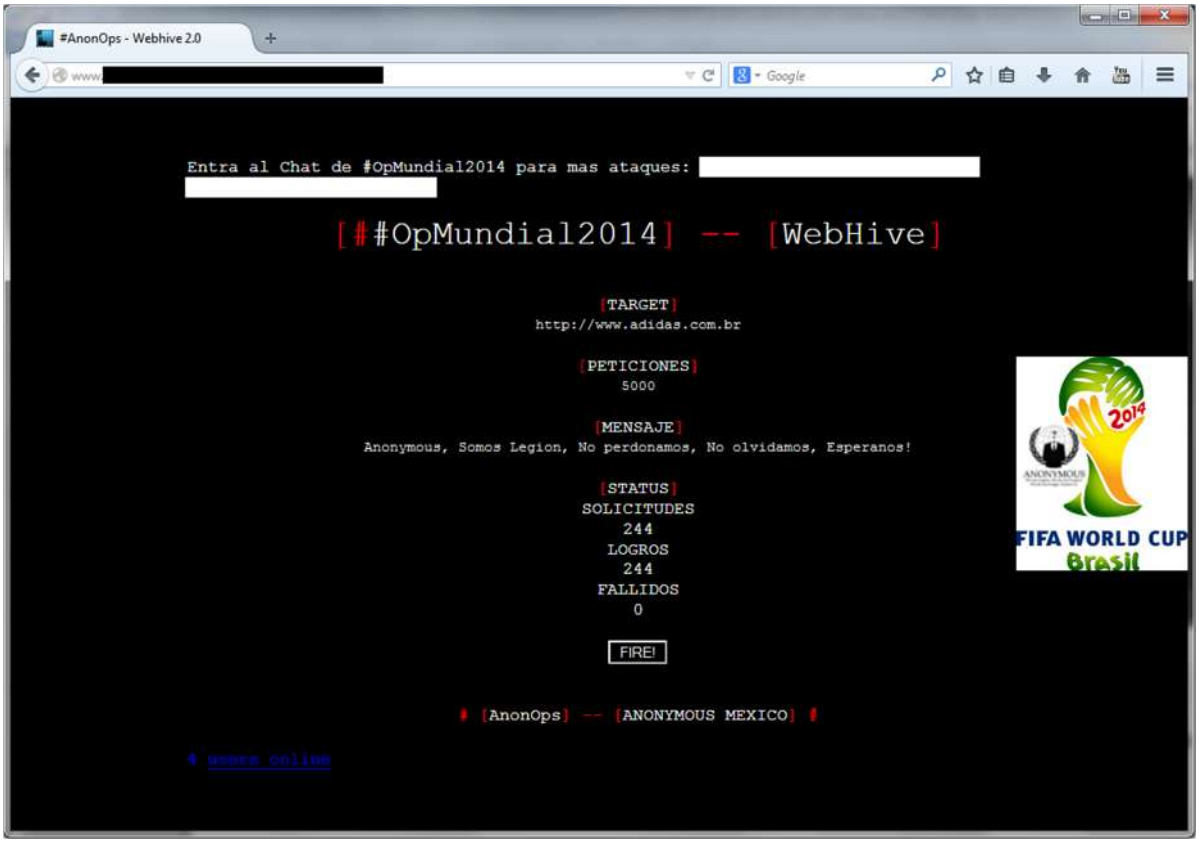
Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

Alerta nº 03/2014 – Uso de ferramentas LOIC.

1. Descrição do Problema

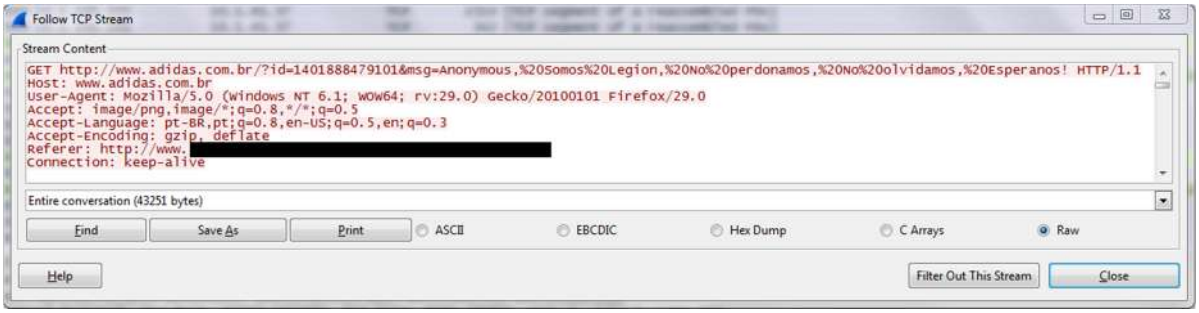
Está sendo divulgado em mídias sociais, a hospedagem de uma ferramenta de LOIC, usada para ataques de Negação de Serviço, associado a Copa do Mundo FIFA 2014.

A ferramenta identificada está configurada para atacar um dos patrocinadores da Copa do Mundo FIFA 2014. Podendo existir outras ainda não identificadas.



Da análise dos pacotes enviados pela ferramenta identificada, verificou-se a existência de uma mensagem fixa, em métodos GET ao site do patrocinador:

msg=Anonymous,%20Somos%20Legion,%20No%20perdonamos,%20No%20olvidamos,%20Esperanos!



Pacotes com essas características podem ser bloqueados com o intuito de evitar a participação de máquinas da comunidade em ataques de Negação de Serviço, visto a facilidade de utilização da ferramenta.

2. Possíveis Riscos

Participação de máquinas da Instituição em ataques de Negação de Serviço, com consequente dano a Imagem da Instituição e da Admistração Pública;

Maculação do nome da instituição.

3. Sugestões para Mitigação do Problema

Sugerimos que criem regras nos equipamentos de segurança dessa instituição, para que pacotes com as características apresentadas não saiam de suas redes. Evitando-se assim a participação de máquinas da instituição no ataque e possibilitando a identificação de funcionários simpatizantes ao evento.

Sugerimos ainda que as regras criadas possibilitem a detecção da mensagem em outras línguas, como inglês e português, com o objetivo de ampliar a defesa.

Atenção deve ser dada para utilizar combinações de palavras da mensagem, ao invés da mensagem completa, também com o objetivo de ampliar a defesa e evitar que pequenas modificações façam o pacote não coincidir com a regra.

Pode-se ainda verificar a possibilidade de criação de regras, baseado nas características dos pacotes da ferramenta, para defender a instituição de ataques de Negação de Serviço.

Referências:

- http://pt.wikipedia.org/wiki/LOIC
- http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html
- http://www.simpleweb.org/reports/loic-report.pdf

Brasília-DF, 05 de Junho de 2014

Atenciosamente,

Equipe do CTIR Gov