Miriane Aparecida Batista
Instituto Federal do Triângulo Mineiro Campus Paracatu
Tecnólogo em Análises e Desenvolvimento de Sistemas

Cert.br

PARACATU, 2016

Resumo

O Cert tem por definição: *Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores*, ou seja, seu objetivo é auxiliar o Administrador de redes na gerência e implementação de soluções de segurança, pois com ela é desenvolvido processos para aumentar o nível da segurança. Ela é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. Infelizmente não é possível impedir que ocorram tentativas de invasões ou ações maliciosas, mas com a ajuda do Cert a organização consegue detectar e solucionar um problema com mais agilidade.

Atua como um ponto central para notificações de incidentes de segurança no Brasil e é mantido pelo Comitê Gestor de Internet no Brasil (NIC.br).

Além do processo de tratamento a incidentes em si, o Cert também atua através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos CSIRTs no Brasil. A CSIRT é um grupo técnico responsável por resolver incidentes relacionados à segurança em sistemas computacionais. Pode ser um serviço prestado por uma empresa especializada ou uma unidade da própria empresa.

No Brasil, temos as seguintes CSIRTs, que estão localizadas nas cidades abaixo:

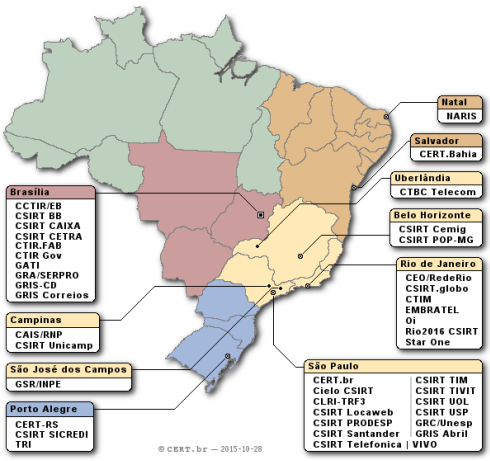


Figura 1 CSIRTs no Brasil

Tratamento de Incidentes

- Dar suporte ao processo de recuperação e análise de ataques e de sistemas comprometidos;

- Estabelecer um trabalho colaborativo com outras entidades, como outros CSIRTs, empresas, universidades, provedores de acesso e serviços Internet e backbones;

- Manter estatísticas públicas dos incidentes tratados e das reclamações de spam recebidas.

Treinamento e Conscientização

- Oferecer treinamentos na área de tratamento de incidentes de segurança, especialmente para membros de CSIRTs e para instituições que estejam criando seu próprio grupo;

- Desenvolver documentação de apoio para administradores de redes Internet e usuários;

- Realizar reuniões com setores diversos da Internet no Brasil, de modo a articular a cooperação e implantação de boas práticas de segurança.

Análise de Tendências de Ataques

- Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro, através da manutenção de uma rede de honeypots distribuídos em diversas redes do país;

- Obter, através de honeypots de baixa interatividade, dados sobre o abuso da infra-estrutura de redes conectadas à Internet para envio de spam.

O CERT.br mantém **estatísticas sobre todas as notificações de incidentes** que são reportados a eles, na qual podemos verificar quais incidentes ocorreram e os tipos de ataques, como:

- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

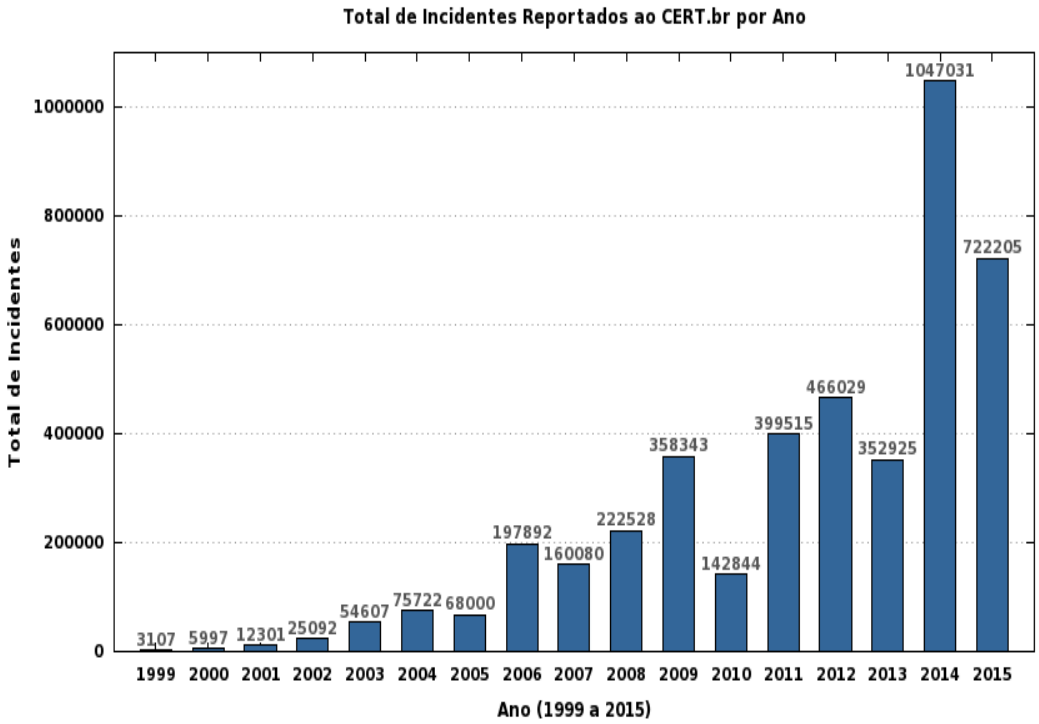
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.



Tipos dos ataques ocorridos no ano de 2015

Mês	Total	worm (%)		dos (%)		invasão (%)		web (%)		**scan** (%)		**fraude** (%)		outros (%)	
jan	**67661**	2829	4	1367	2	409	0	6547	9	36445	53	18465	27	1599	2
fev	**66700**	2682	4	2056	3	289	0	8102	12	39267	58	12513	18	1791	2
mar	**52959**	2867	5	70	0	489	0	8822	16	32351	61	6338	11	2022	3
abr	**52991**	3046	5	34	0	150	0	6297	11	31215	58	10571	19	1678	3
mai	**58322**	3122	5	374	0	177	0	5399	9	23242	39	23890	40	2118	3
jun	**81244**	3423	4	1016	1	157	0	9219	11	29593	36	36327	44	1509	1
jul	**53075**	4141	7	2763	5	160	0	4716	8	32601	61	6561	12	2133	4
ago	**65486**	3683	5	3354	5	104	0	4447	6	33446	51	18701	28	1751	2
set	**59311**	4326	7	2511	4	119	0	3993	6	29759	50	16560	27	2043	3
out	**52226**	6301	12	1702	3	140	0	4315	8	32554	62	6089	11	1125	2
nov	**64203**	5912	9	9142	14	145	0	2297	3	38482	59	6595	10	1630	2
dez	**48027**	5390	11	971	2	118	0	1493	3	32268	67	6165	12	1622	3
Total	**722205**	47722	6	25360	3	2457	0	65647	9	391223	54	168775	23	21021	2

O Cert também fornece um grande material para auxiliar na segurança, material que está disponível em seu próprio site para download, como as palestras abaixo:

- Como melhorar o cenário de ataques DDoS
- Segurança e IoT: Desafios e Expectativas

- Tratamento de Incidentes no Brasil
- Segurança em Aplicações Web: Como mitigar os riscos
- Workshop - Criptografia e Privacidade: aprendendo a usar PGP
- Workshop - Programação segura para Web
- Mitigando os Riscos de Segurança em Aplicações Web

Conclusão

À medida que uma determinada empresa, órgãos, país crescem, as chances de sofrer um ataque também aumentam. Logo, essas prevenções e táticas de segurança se tornaram hoje não mais privilégio e sim necessidade.