FCCN UNIDADE DA FCT
Tecnologia para o Conhecimento

TRAFFIC LIGHT PROTOCOL (TLP)

Louise Altvater

RCTS CERT

TRAFFIC LIGHT PROTOCOL (TLP)

TLP LABELS

TLP:RED

TLP:AMBER

TLP:GREEN

TLP:CLEAR

USO DO TLP

	RGB: font			RGB: background			CMYK: font				CMYK: background				Hex: font	Hex: background
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	0	0	100	#FF2B2B	#000000
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	0	0	100	#FFC000	#000000
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	0	0	100	#33FF00	#000000
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0	0	0	0	100	#FFFFFF	#000000

DEFINIÇÕES DO TLP

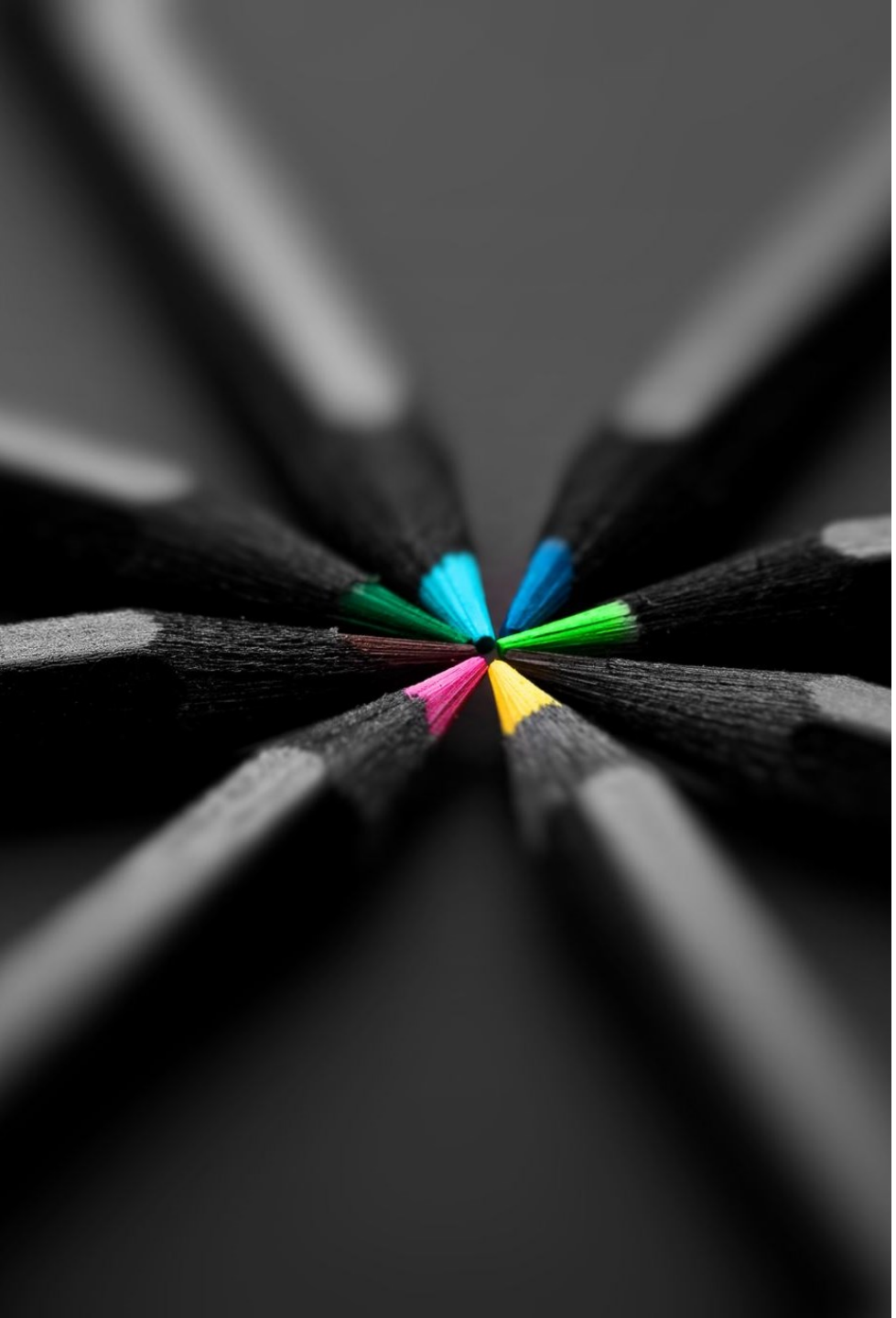
Comunidade: Grupo que partilha de práticas e objetivos em comum e mantém relações de confiança informais. Ex.: a comunidade de profissionais de cibersegurança de um país.

Organização: Grupo que partilha de uma afiliação comum através de uma filiação formal e que está conectado pelas políticas estabelecidas pela organização da qual fazem parte.

Clientes: Pessoas ou entidades que recebem serviços de cibersegurança de uma organização.

DEFINIÇÕES DO TLP

TLP:RED	Para conhecimento estrito dos recipientes individuais, informação não deve ser partilhada.
TLP:AMBER **TLP:AMBER+STRICT**	Os recipientes da informação podem partilhar a informação apenas com membros da própria organização e clientes. Se a informação for restrita apenas a membros da própria organização, o **TLP:AMBER+STRICT** deve ser usado.
TLP:GREEN	Partilha limitada, recipientes podem partilhar a informação dentro da sua comunidade. Informação pode ser partilhada com colegas e organizações parceiras dentro da sua comunidade, mas não por canais publicamente acessíveis.
TLP:CLEAR	Não existem restrições para a divulgação da informação.



ACTIVIDADE

- **Classificar Documentos de acordo com o protocolo TLP**
- **6 documentos usados pela equipa CSIRT Fantasia**
- **15 min**

Fundação
para a Ciência
e a Tecnologia

15 MINUTOS

TLP:RED	Para conhecimento estrito dos recipientes individuais, informação não deve ser partilhada.
TLP:AMBER **TLP:AMBER+STRICT**	Os recipientes da informação podem partilhar a informação apenas com membros da própria organização e clientes. Se a informação for restrita apenas a membros da própria organização, o **TLP:AMBER+STRICT** deve ser usado.
TLP:GREEN	Partilha limitada, recipientes podem partilhar a informação dentro da sua comunidade. Informação pode ser partilhada com colegas e organizações parceiras dentro da sua comunidade, mas não por canais publicamente acessíveis.
TLP:CLEAR	Não existem restrições para a divulgação da informação.

TLP:

CSIRT Fantasia

Pedido de Auditoria:

Gaivotas Inc.

Versão 1.0
Março de 2022

CSIRT Fantasia

TLP:

CSIRT Fantasia

TLP:

Entidade que solicita a auditoria:	Gaivotas Inc. (Andorinha Corp.)
Dados de Contacto (requisitante):	Otílio Salgado otilio.salgado@gaivotas.com.tk +87 356 896 471
Domínio da Entidade:	gaivotas.com.tk
Domínio a ser auditado:	test.gaivotas.com.tk
Tipo de auditoria:	Blackbox
Período da auditoria:	a definir
Data de Entrega da Auditoria:	a definir
Informações Adicionais:	

TLP:

TLP:AMBER+STRICT

CSIRT Fantasia

Pedido de Auditoria:

Gaivotas Inc.

Versão 1.0
Março de 2022

CSIRT Fantasia

TLP:AMBER+STRICT

CSIRT Fantasia

TLP:AMBER+STRICT

Entidade que solicita a auditoria:	Gaivotas Inc. (Andorinha Corp.)
Dados de Contacto (requisitante):	Otílio Salgado otilio.salgado@gaivotas.com.tk +87 356 896 471
Domínio da Entidade:	gaivotas.com.tk
Domínio a ser auditado:	test.gaivotas.com.tk
Tipo de auditoria:	Blackbox
Período da auditoria:	a definir
Data de Entrega da Auditoria:	a definir
Informações Adicionais:	

TLP:AMBER+STRICT


PHISHING WEBINAR
18 DE NOVEMBRO DE 2022
Aprenda sobre o que é phishing e boas práticas de segurança
O Link para o evento será divulgado nas páginas sociais do CSIRT Fantasia no dia do Webinar
CSIRT Fantasia
TLP:

PHISHING WEBINAR

18 DE NOVEMBRO DE 2022

Aprenda sobre o que é phishing e boas práticas de segurança

O Link para o evento será divulgado nas páginas sociais do CSIRT Fantasia no dia do Webinar

CSIRT Fantasia

TLP:CLEAR

TLP:

O grupo Hacktivista Lazarus

Trabalho apresentado na Andorinha Cyber Conference[1]

30 Fevereiro 2022

[1] Andorinha Cyber Conference é uma conferência que acontece anualmente para profissionais credenciados ligados à rede CSIRT Passeriforme. O presente documento pode ser partilhado com as listas de profissionais ligados à rede CSIRT Passeriforme.

TLP:

CSIRT
Fantasia

TLP:

Sumário

TLP:

TLP:GREEN

O grupo Hacktivista Lazarus

Trabalho apresentado na Andorinha Cyber Conference[1]®

30 Fevereiro 2022

[1] Andorinha Cyber Conference® é uma conferência que acontece anualmente para profissionais credenciados ligados à rede CSIRT Passeriforme. O presente documento pode ser partilhado com as listas de profissionais ligados à rede CSIRT Passeriforme.

TLP:GREEN

TLP:GREEN

Sumário

TLP:GREEN

TLP:

CSIRT Fantasia

Relatório

DDoS @ Andorinha Corp

2021

Versão 1.0

Armando Skemas

TLP:

TLP:

CSIRT Fantasia

ÍNDICE

TLP:

CSIRT Fantasia

TLP:

1 SUMÁRIO EXECUTIVO

O número total de ataques DDoS identificados na Andorinha Corp, durante o ano de 2021 foi de 253, o que representa uma redução de 28% face aos 352 registados em 2020.

Este número significa 21 ataques por mês, em média, e, portanto, 0,7 eventos por dia, também em média.

Os meses de maio e outubro foram os meses onde um maior número de eventos ocorreram (53 e 39, respectivamente), sendo que agosto foi o mês onde o número de eventos foi menor (4).

O peso total da Gaivotas Inc. na totalidade destes eventos foi superior a 36%.

2 INFRAESTRUTURAS DE DETECÇÃO

A Andorinha Corp dispõe de um sistema Terminator Sightline, que alimenta o SIEM utilizado pela CF.

Este sistema recebe fluxos dos routers de *backbone* interligados com a rede Flamboiant (que funciona como *upstream* da Andorinha Corp).

3 ANÁLISE DOS ENDEREÇOS IP ATACADOS

A tabela seguinte contém o TOP-10 dos Endereços IP atacados

Endereço IP	Organização	#
192.154.86.201	BANCO CORVIDAE	16
192.154.57.116	BANCO CORVIDAE	13
192.210.6.123	GAIVOTAS INC.	10
192.210.86.201	GAIVOTAS INC.	8
192.210.66.57	GAIVOTAS INC.	8
192.137.52.201	CRÉDITOS PARDAL	6
192.154.86.155	BANCO CORVIDAE	4
192.157.74.126	BÚTIO-VESPEIRO.ORG	4
192.201.58.19	CHAPIM REAL	3
192.207.19.192	APUS PALLIDUS	3

TLP:

CSIRT Fantasia

TLP:

4 ANÁLISE DAS ORGANIZAÇÕES ATACADAS

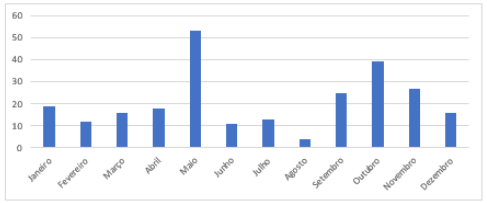
A tabela seguinte contém o TOP-5 das organizações atacadas durante o ano de 2021.

Organização	#
GAIVOTAS INC.	92
BANCO CORVIDAE	45
CRÉDITOS PARDAL	25
CHAPIM REAL	16
BÚTIO-VESPEIRO ORG.	21

A organização mais atacada, Gaivotas Inc., representa 36,36% do total de eventos de 2021, sendo que a segunda organização mais atacada (Banco Corvidae) representa 17,79% e a terceira (Créditos Pardal) apenas 9,8%.

5 DISTRIBUIÇÃO MENSAL DOS EVENTOS

O gráfico seguinte ilustra a distribuição dos eventos pelos 12 meses do ano.



6 CONCLUSÕES

A distribuição de eventos por quadrimestre foi muito assimétrica. No primeiro quadrimestre foram registados 47 eventos, 82 eventos no segundo, seguidos de 42 eventos no terceiro, e novamente 82 no último.

TLP:

CSIRT Fantasia

Relatório

DDoS @ Andorinha Corp

2021

Versão 1.0

Armando Skemas

TLP:AMBER

CSIRT Fantasia

ÍNDICE

TLP:AMBER

CSIRT Fantasia

TLP:AMBER

1 SUMÁRIO EXECUTIVO

O número total de ataques DDoS identificados na Andorinha Corp. durante o ano de 2021 foi de 253, o que representa uma redução de 28% face aos 352 registados em 2020.

Este número significa 21 ataques por mês, em média, e, portanto, 0,7 eventos por dia, também em média.

Os meses de maio e outubro foram os meses onde um maior número de eventos ocorreram (53 e 39 , respectivamente), sendo que agosto foi o mês onde o número de eventos foi menor (4).

O peso total da Gaivotas Inc. na totalidade destes eventos foi superior a 36%.

2 INFRAESTRUTURAS DE DETECÇÃO

A Andorinha Corp dispõe de um sistema Terminator Sightline, que alimenta o SIEM utilizado pela CF.

Este sistema recebe fluxos dos routers de *backbone* interligados com a rede Flamboiant (que funciona como *upstream* da Andorinha Corp) .

3 ANÁLISE DOS ENDEREÇOS IP ATACADOS

A tabela seguinte contém o TOP-10 dos Endereços IP atacados

Endereço IP	Organização	#
192.154.86.201	BANCO CORVIDAE	16
192.154.57.116	BANCO CORVIDAE	13
192.210.6.123	GAIVOTAS INC.	10
192.210.86.201	GAIVOTAS INC.	8
192.210.66.57	GAIVOTAS INC.	8
192.137.52.201	CRÉDITOS PARDAL	6
192.154.86.155	BANCO CORVIDAE	4
192.157.74.126	BÚTIO-VESPEIRO.ORG	4
192.201.58.19	CHAPIM REAL	3
192.207.19.192	APUS PALLIDUS	3

TLP:AMBER

CSIRT Fantasia

TLP:AMBER

4 ANÁLISE DAS ORGANIZAÇÕES ATACADAS

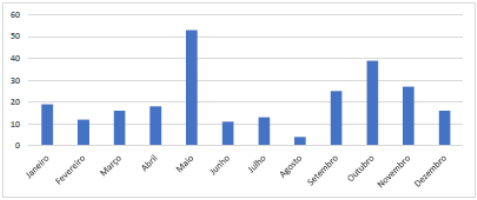
A tabela seguinte contém o TOP-5 das organizações atacadas durante o ano de 2021.

Organização	#
GAIVOTAS INC.	92
BANCO CORVIDAE	45
CRÉDITOS PARDAL	25
CHAPIM REAL	16
BÚTIO-VESPEIRO ORG.	21

A organização mais atacada, Gaivotas Inc., representa 36,36% do total de eventos de 2021, sendo que a segunda organização mais atacada (Banco Corvidae) representa 17,79% e a terceira (Créditos Pardal) apenas 9,8%.

5 DISTRIBUIÇÃO MENSAL DOS EVENTOS

O gráfico seguinte ilustra a distribuição dos eventos pelos 12 meses do ano.



6 CONCLUSÕES

A distribuição de eventos por quadrimestre foi muito assimétrica. No primeiro quadrimestre foram registados 47 eventos, 82 eventos no segundo, seguidos de 42 eventos no terceiro, e novamente 82 no último.

TLP:AMBER

CSIRT Fantasia

TLP:

INSTRUÇÕES DE ACESSO AO COFRE DA EQUIPA CSIRT Fantasia

1. Verificar que as opções Master Password e Key file/provider estão selecionadas;
2. Selecionar o key file manualmente, o qual encontra-se em \\servidor\CF\Keys\Keepass.kdbx;
3. Utilizar a senha Semseguranca99 para aceder ao cofre.

TLP:

CSIRT Fantasia

TLP:RED

INSTRUÇÕES DE ACESSO AO COFRE DA EQUIPA CSIRT Fantasia

1. Verificar que as opções Master Password e Key file/provider estão selecionadas;
2. Selecionar o key file manualmente, o qual encontra-se em \\servidor\CF\Keys\Keepass.kdbx;
3. Utilizar a senha Semseguranca99 para aceder ao cofre.

TLP:RED

CSIRT Fantasia

Código de Conduta do CSIRT Fantasia

Versão 1.2

Março 2021

TLP:

TLP:

Conteúdo

TLP:

TLP:

1 AUTORES E HISTÓRICO

1.1 CONTACTOS

Role	Name	Date	Version
Gestor	**Armando Skemas**	**2021/03/23**	**V1.2**

1.2 HISTÓRICO DE REVISÕES

Name	Description	Date	version
Armando Skemas	Criação do documento	2019/02/11	1.0
Armando Skemas	Revisão do documento	2020/04/08	1.1
Armando Skemas	Revisão do documento	2021/03/23	1.2

TLP:

TLP:

2 DESCRIÇÃO

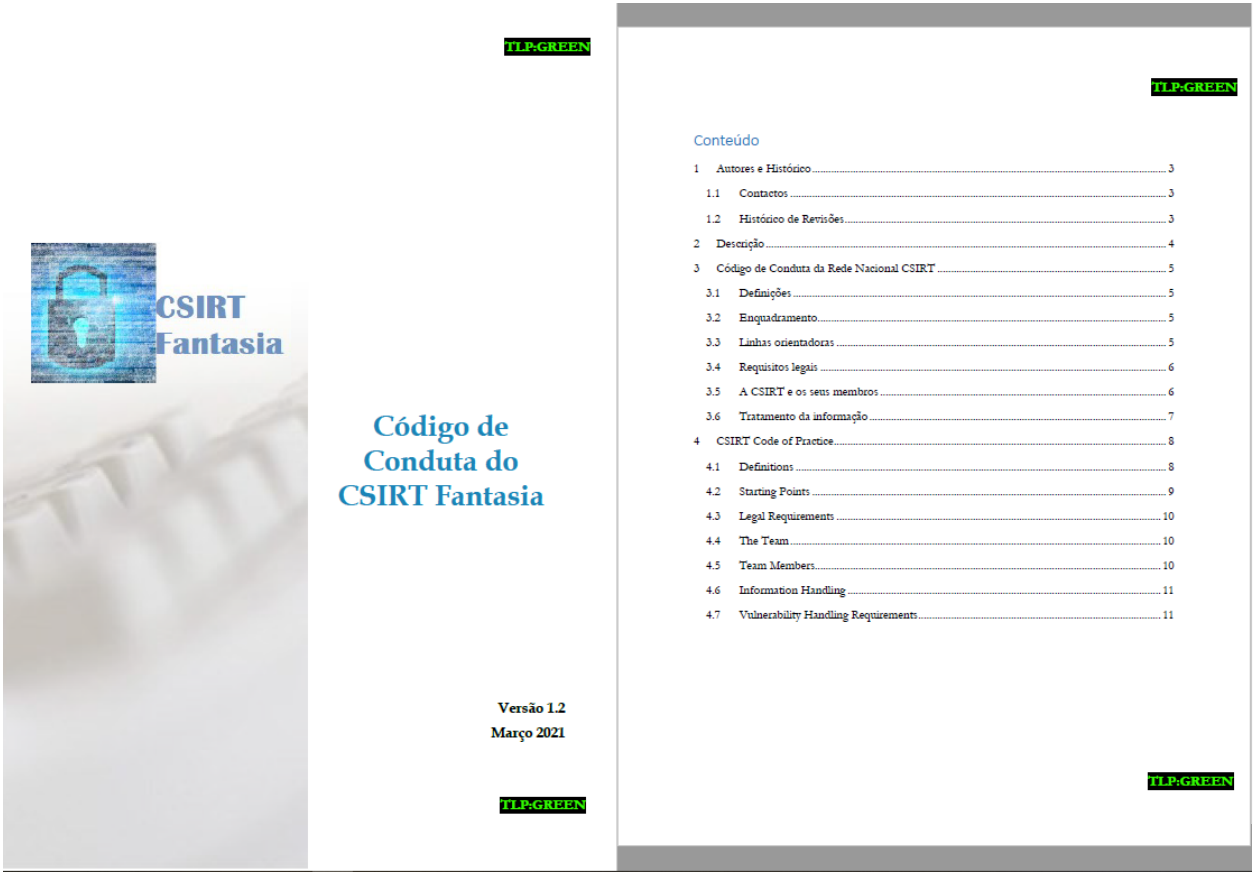
O presente documento especifica o código de conduta pelo qual os membros do CSIRT Fantasia devem reger a sua actuação. O CSIRT Fantasia adopta as disposições do código de conduta da Rede Nacional CSIRT (de 2009) e do CSIRT Code of Practice (v2.4 de 2017) do Trusted Introducer. O texto do Código de Conduta do Trusted Introducer está reproduzido na língua inglesa, conforme a língua original em que foi escrito, no capítulo 4.

As referências externas de ambos os documentos são:

- https://www.redecsirt.pt/#docs (Código de conduta dos membros da Rede)
- https://www.trusted-introducer.org/TI-CCoP.pdf

TLP:

TLP:



TLP:GREEN

CSIRT Fantasia

Código de Conduta do CSIRT Fantasia

Versão 1.2
Março 2021

TLP:GREEN

TLP:GREEN

Conteúdo

TLP:GREEN

TLP:GREEN

1 AUTORES E HISTÓRICO

1.1 CONTACTOS

Role	Name	Date	Version
Gestor	Armando Skemas	2021/03/23	V1.2

1.2 HISTÓRICO DE REVISÕES

Name	Description	Date	version
Armando Skemas	Criação do documento	2019/02/11	1.0
Armando Skemas	Revisão do documento	2020/04/08	1.1
Armando Skemas	Revisão do documento	2021/03/23	1.2

TLP:GREEN

TLP:GREEN

2 DESCRIÇÃO

O presente documento especifica o código de conduta pelo qual os membros do CSIRT Fantasia devem reger a sua actuação. O CSIRT Fantasia adopta as disposições do código de conduta da Rede Nacional CSIRT (de 2009) e do CSIRT Code of Practice (v2.4 de 2017) do Trusted Introducer. O texto do Código de Conduta do Trusted Introducer está reproduzido na língua inglesa, conforme a língua original em que foi escrito, no capítulo 4.

As referências externas de ambos os documentos são:

- https://www.redecsirt.pt/#docs (Código de conduta dos membros da Rede)
- https://www.trusted-introducer.org/TI-CCoP.pdf

TLP:GREEN

Obrigada!