Existe vida sem email?

Como o phishing pode impactar na sua organização (e como mitigá-lo)

CADE
Conselho Administrativo de Defesa Econômica

Disclosure

Todas as opiniões aqui apresentadas são exclusivas do palestrante, apenas de caráter ilustrativo e não possuem nenhum vínculo com o Cade ou qualquer outra instituição.

Informações internas do Cade foram filtradas a fim de preservar a imagem da autarquia, bem como de sua equipe.

CADE
Conselho Administrativo de Defesa Econômica

Whoami

Giordanno Azevedo Costa Martins

Engenheiro de Computação
MBA em Segurança da Informação
CEH, ISMAS 27002
Coordenador-Geral de Tecnologia da Informação no Cade
Responsável pela ETIR-CADE

CADE
Conselho Administrativo de Defesa Econômica

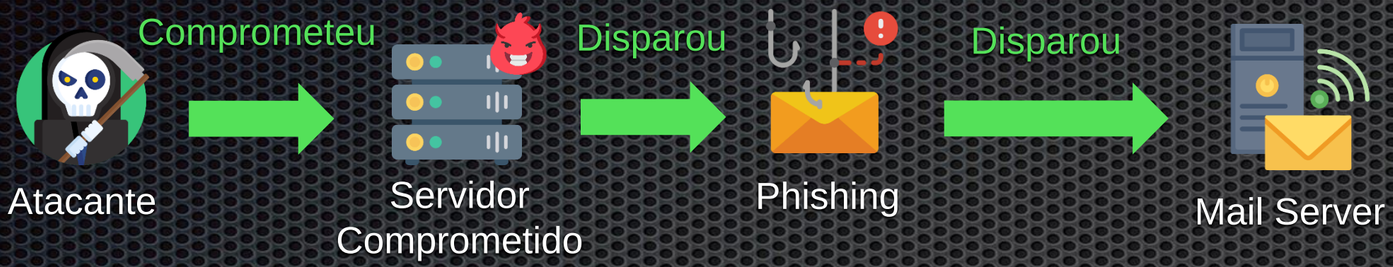
Resumo

- Estrutura do phishing recebido no Cade
- Captura de Credenciais
- Estratégia de resposta ao incidente
- Evitando entrar em blacklists
- Impacto do incidente
- Resultado das ações
- Números

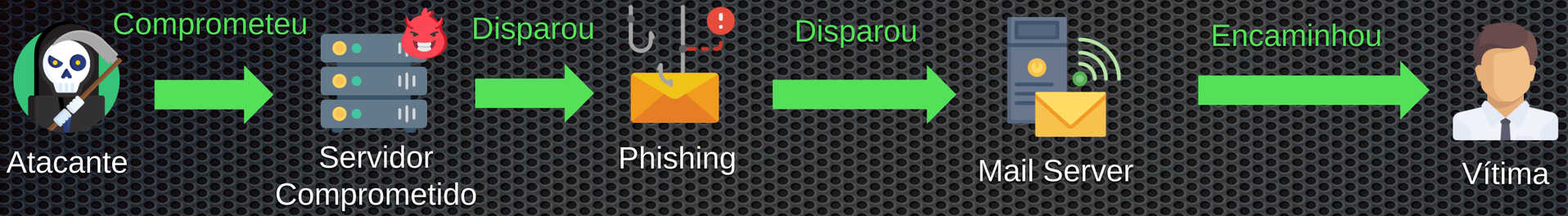
CADE
Conselho Administrativo de Defesa Econômica

Estrutura do Phishing

Estrutura do Phishing

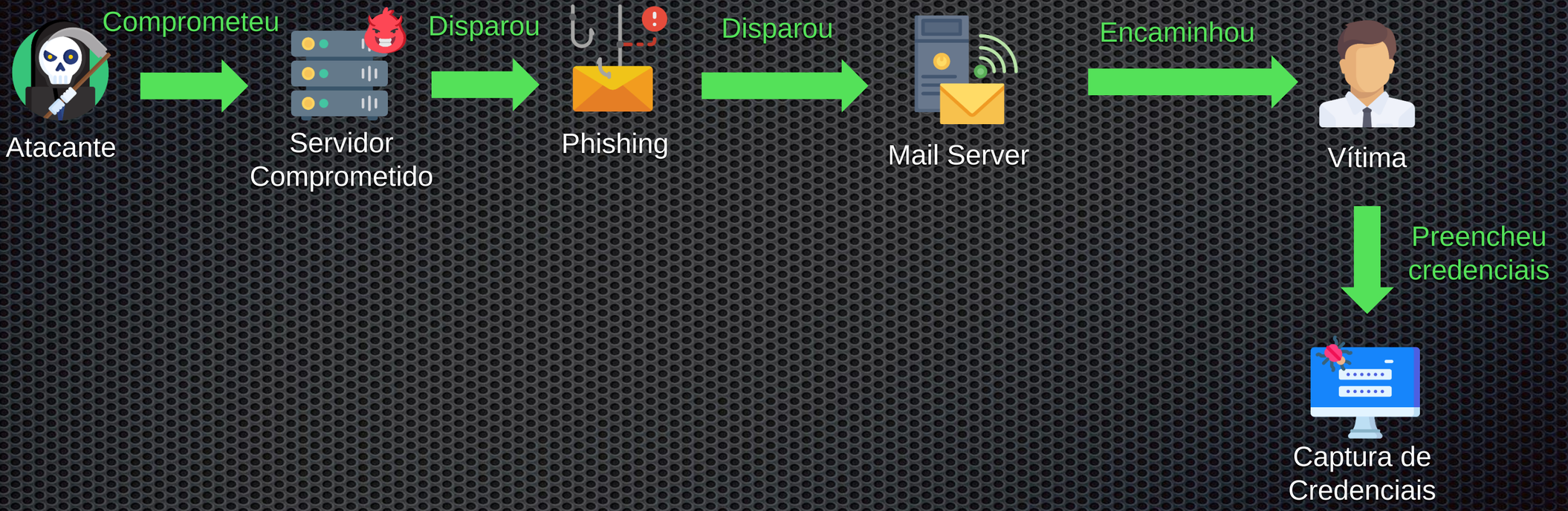


Estrutura do Phishing



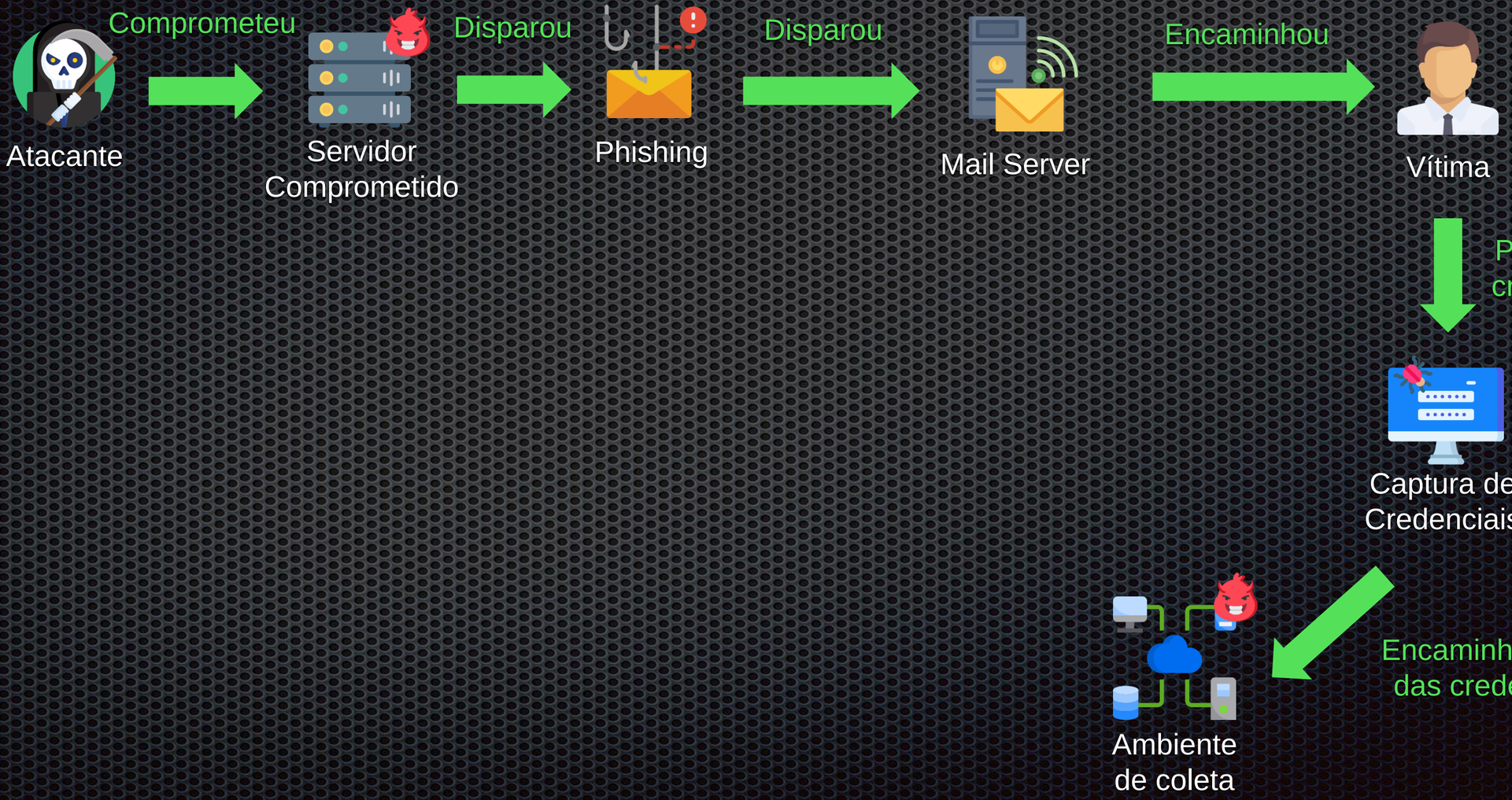
CADE
Conselho Administrativo de Defesa Econômica

Estrutura do Phishing

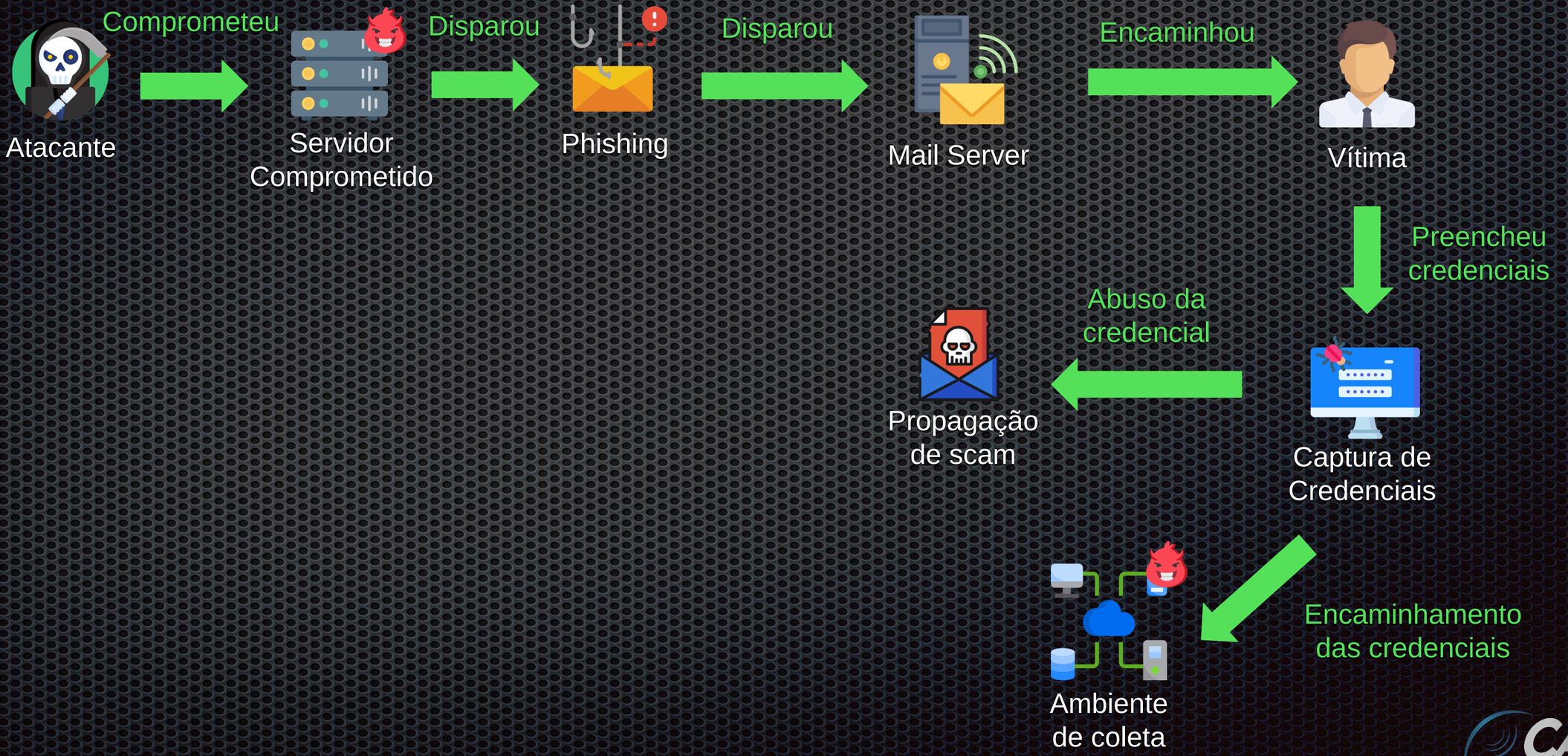


CADE
Conselho Administrativo de Defesa Econômica

Estrutura do Phishing

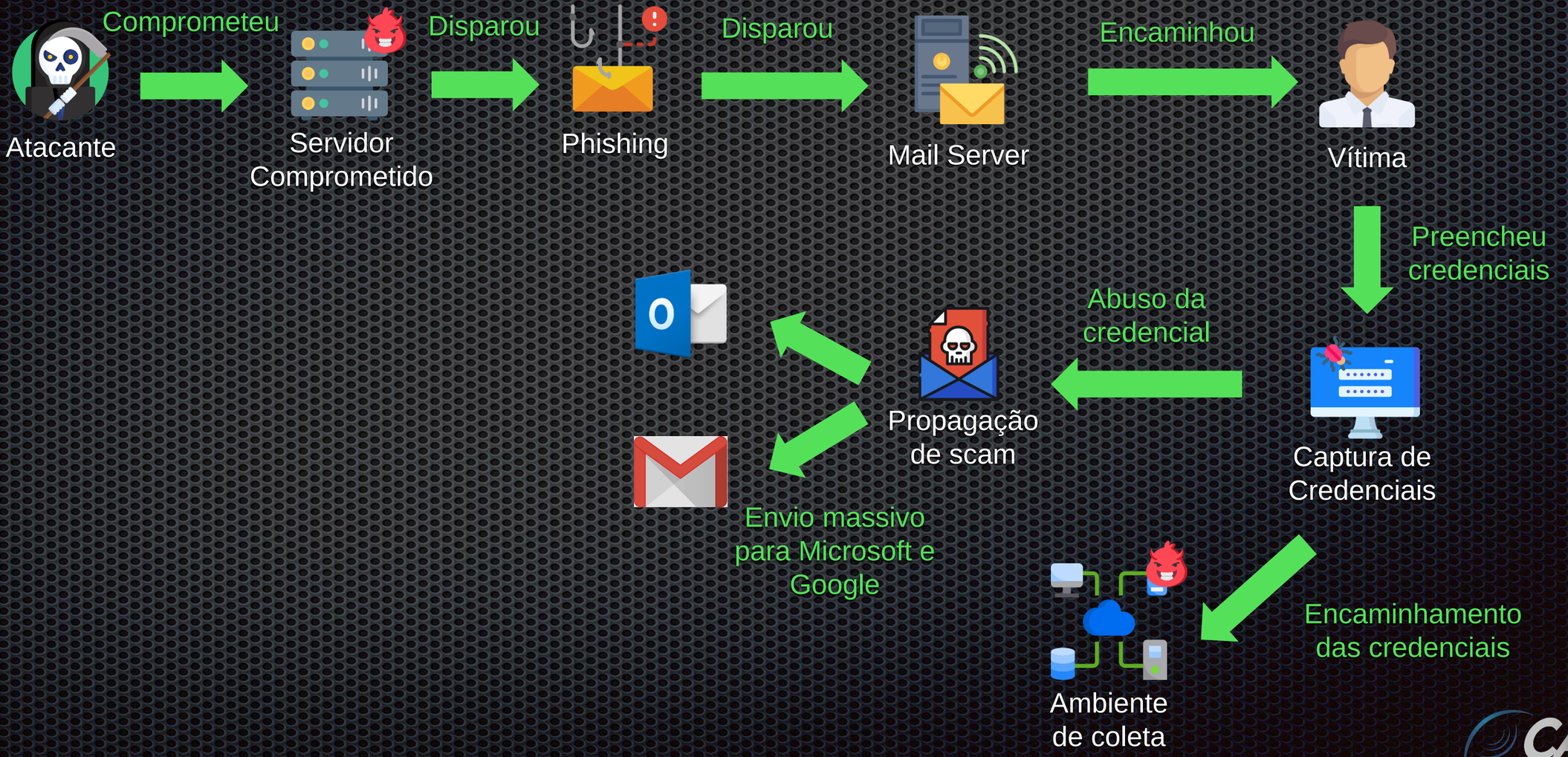


Estrutura do Phishing



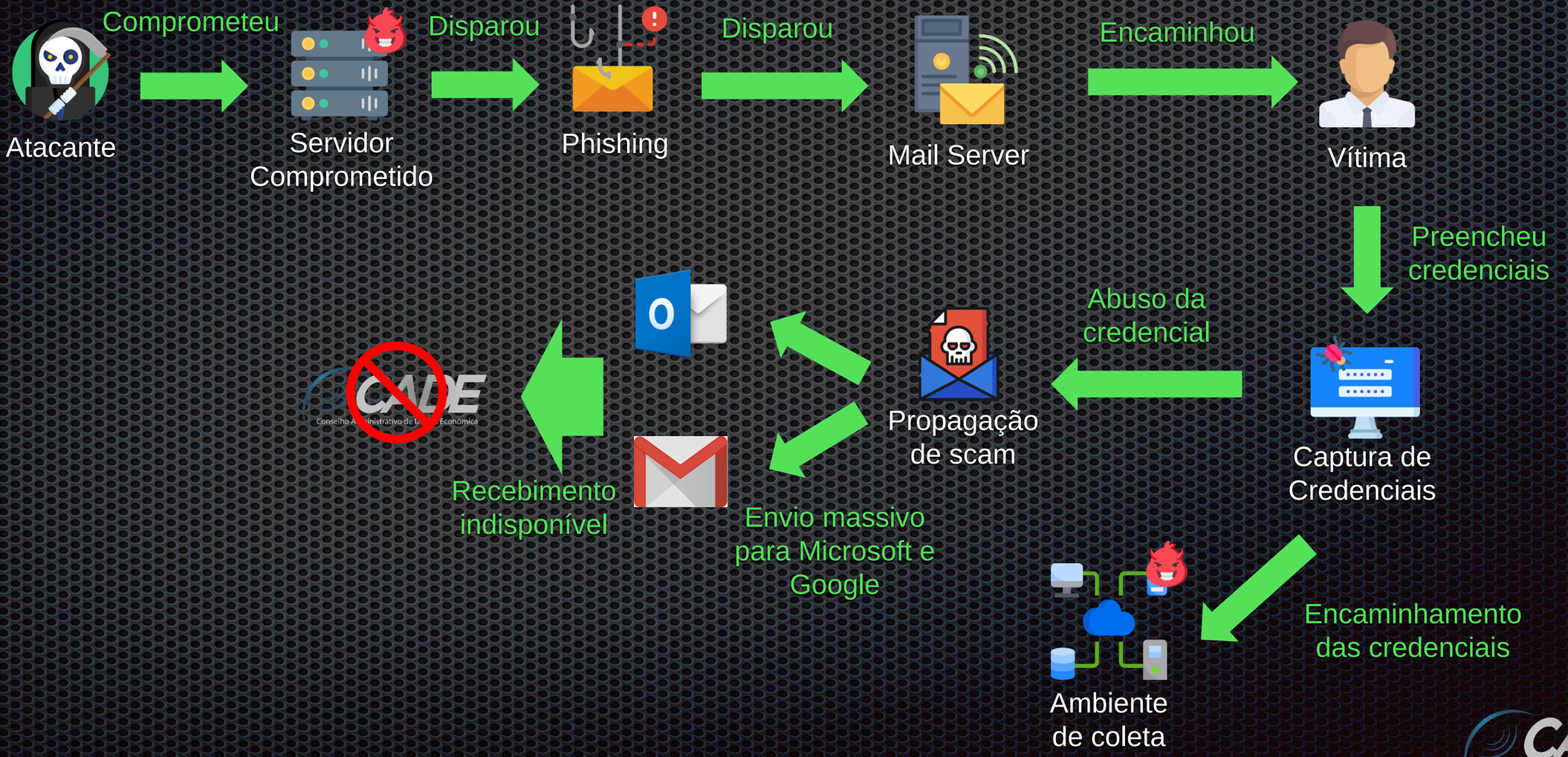
CADE
Conselho Administrativo de Defesa Econômica

Estrutura do Phishing



CADE
Conselho Administrativo de Defesa Econômica

Estrutura do Phishing



CADE
Conselho Administrativo de Defesa Econômica

Estrutura do Phishing: IOCs

- hxxp://dexcezzz.000webhostapp.com
- 145.14.144.79
- hxxp://www.unpkg.com
- 177.185.203.146
- 177.185.202.75

Estrutura do phishing: header

Received: from scmgateway.cade.gov.br (172.16.FF.FF) by SRV003B6774.cade.gov.br (10.FF.FF.FF) with Microsoft SMTP Server id 14.3.399.0; Fri, 15 Mar 2019 10:11:49 -0300
Received: from #########.CADE.GOV.BR (localhost [127.0.0.1]) by scmgateway.cade.gov.br (Postfix) with ESMTP id 1732620006; Fri, 15 Mar 2019 10:11:19 -0300 (-03)
Received: from smtp-sp203-146.hospedagem.net (smtp-sp203-146.hospedagem.net [177.185.203.146]) (using TLSv1.2 with cipher DHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (Client did not present a certificate) by scmgateway.cade.gov.br (Postfix) with ESMTPS; Fri, 15 Mar 2019 10:11:17 -0300 (-03)
Received: from webmail.bewnet.com.br (webmail-node-06-farm74.uni5.net [177.185.202.75]) (Authenticated sender: mrussoinformatica@bewnet.com.br) by smtp-sp203-146.hospedagem.net (Postfix) with ESMTPA id 38CA76001FAB;Fri, 15 Mar 2019 10:11:46 -0300 (-03)
MIME-Version: 1.0
Content-Type: multipart/alternative;
	boundary="=_9cde7a7f84cafe85a96231b766576eaa"
Date: Fri, 15 Mar 2019 10:11:46 -0300
From: admin <mrussoinformatica@bewnet.com.br>
To: undisclosed-recipients:;
Subject: =?UTF-8?Q?Querido_usu=C3=A1rio=2C?=
Message-ID: <c0d1792a598509077bb2d9f9e582c632@bewnet.com.br>
X-Sender: mrussoinformatica@bewnet.com.br
User-Agent: Roundcube Webmail/Final

CADE
Conselho Administrativo de Defesa Econômica

Estrutura do phishing: header

Received: from scmgateway.cade.gov.br (172.16.FF.FF) by SRV003B6774.cade.gov.br (10.FF.FF.FF) with Microsoft SMTP Server id 14.3.399.0; Fri, 15 Mar 2019 10:11:49 -0300
Received: from #########.CADE.GOV.BR (localhost [127.0.0.1]) by scmgateway.cade.gov.br (Postfix) with ESMTP id 1732620006; Fri, 15 Mar 2019 10:11:19 -0300 (-03)
Received: from smtp-sp203-146.hospedagem.net (smtp-sp203-146.hospedagem.net [177.185.203.146]) (using TLSv1.2 with cipher DHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (Client did not present a certificate) by scmgateway.cade.gov.br (Postfix) with ESMTPS; Fri, 15 Mar 2019 10:11:17 -0300 (-03)
Received: from webmail.bewnet.com.br (webmail-node-06-farm74.uni5.net [177.185.202.75]) (Authenticated sender: mrussoinformatica@bewnet.com.br) by smtp-sp203-146.hospedagem.net (Postfix) with ESMTPA id 38CA76001FAB;Fri, 15 Mar 2019 10:11:46 -0300 (-03)
MIME-Version: 1.0
Content-Type: multipart/alternative;
	boundary="=_9cde7a7f84cafe85a96231b766576eaa"
Date: Fri, 15 Mar 2019 10:11:46 -0300
From: admin <mrussoinformatica@bewnet.com.br>
To: undisclosed-recipients:;
Subject: =?UTF-8?Q?Querido_usu=C3=A1rio=2C?=
Message-ID: <c0d1792a598509077bb2d9f9e582c632@bewnet.com.br>
X-Sender: mrussoinformatica@bewnet.com.br
User-Agent: Roundcube Webmail/Final

CADE
Conselho Administrativo de Defesa Econômica

Estrutura do phishing: header

Received: from scmgateway.cade.gov.br (172.16.FF.FF) by SRV003B6774.cade.gov.br (10.FF.FF.FF) with Microsoft SMTP Server id 14.3.399.0; Fri, 15 Mar 2019 10:11:49 -0300
Received: from #########.CADE.GOV.BR (localhost [127.0.0.1]) by scmgateway.cade.gov.br (Postfix) with ESMTP id 1732620006; Fri, 15 Mar 2019 10:11:19 -0300 (-03)
Received: from smtp-sp203-146.hospedagem.net (smtp-sp203-146.hospedagem.net [177.185.203.146]) (using TLSv1.2 with cipher DHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (Client did not present a certificate) by scmgateway.cade.gov.br (Postfix) with ESMTPS; Fri, 15 Mar 2019 10:11:17 -0300 (-03)
Received: from webmail.bewnet.com.br (webmail-node-06-farm74.uni5.net [177.185.202.75]) (Authenticated sender: mrussoinformatica@bewnet.com.br) by smtp-sp203-146.hospedagem.net (Postfix) with ESMTPA id 38CA76001FAB; Fri, 15 Mar 2019 10:11:46 -0300 (-03)
MIME-Version: 1.0
Content-Type: multipart/alternative;
	boundary="=_9cde7a7f84cafe85a96231b766576eaa"
Date: Fri, 15 Mar 2019 10:11:46 -0300
From: admin <mrussoinformatica@bewnet.com.br>
To: undisclosed-recipients:;
Subject: =?UTF-8?Q?Querido_usu=C3=A1rio=2C?=
Message-ID: <c0d1792a598509077bb2d9f9e582c632@bewnet.com.br>
X-Sender: mrussoinformatica@bewnet.com.br
User-Agent: Roundcube Webmail/Final

CADE
Conselho Administrativo de Defesa Econômica

Estrutura do phishing: header

Received: from scmgateway.cade.gov.br (172.16.FF.FF) by SRV003B6774.cade.gov.br (10.FF.FF.FF) with Microsoft SMTP Server id 14.3.399.0; Fri, 15 Mar 2019 10:11:49 -0300
Received: from #########.CADE.GOV.BR (localhost [127.0.0.1]) by scmgateway.cade.gov.br (Postfix) with ESMTP id 1732620006; Fri, 15 Mar 2019 10:11:19 -0300 (-03)
Received: from smtp-sp203-146.hospedagem.net (smtp-sp203-146.hospedagem.net [177.185.203.146]) (using TLSv1.2 with cipher DHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (Client did not present a certificate) by scmgateway.cade.gov.br (Postfix) with ESMTPS; Fri, 15 Mar 2019 10:11:17 -0300 (-03)
Received: from webmail.bewnet.com.br (webmail-node-06-farm74.uni5.net [177.185.202.75]) (Authenticated sender: mrussoinformatica@bewnet.com.br) by smtp-sp203-146.hospedagem.net (Postfix) with ESMTPA id 38CA76001FAB; Fri, 15 Mar 2019 10:11:46 -0300 (-03)
MIME-Version: 1.0
Content-Type: multipart/alternative;
	boundary="=_9cde7a7f84cafe85a96231b766576eaa"
Date: Fri, 15 Mar 2019 10:11:46 -0300
From: admin <mrussoinformatica@bewnet.com.br>
To: undisclosed-recipients:;
Subject: =?UTF-8?Q?Querido_usu=C3=A1rio=2C?=
Message-ID: <c0d1792a598509077bb2d9f9e582c632@bewnet.com.br>
X-Sender: mrussoinformatica@bewnet.com.br
User-Agent: Roundcube Webmail/Final

CADE
Conselho Administrativo de Defesa Econômica

Estrutura do phishing: header

Received: from scmgateway.cade.gov.br (172.16.FF.FF) by SRV003B6774.cade.gov.br (10.FF.FF.FF) with Microsoft SMTP Server id 14.3.399.0; Fri, 15 Mar 2019 10:11:49 -0300
Received: from #########.CADE.GOV.BR (localhost [127.0.0.1]) by scmgateway.cade.gov.br (Postfix) with ESMTP id 1732620006; Fri, 15 Mar 2019 10:11:19 -0300 (-03)
Received: from smtp-sp203-146.hospedagem.net (smtp-sp203-146.hospedagem.net [177.185.203.146]) (using TLSv1.2 with cipher DHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (Client did not present a certificate) by scmgateway.cade.gov.br (Postfix) with ESMTPS; Fri, 15 Mar 2019 10:11:17 -0300 (-03)
Received: from webmail.bewnet.com.br (webmail-node-06-farm74.uni5.net [177.185.202.75]) (Authenticated sender: mrussoinformatica@bewnet.com.br) by smtp-sp203-146.hospedagem.net (Postfix) with ESMTPA id 38CA76001FAB; Fri, 15 Mar 2019 10:11:46 -0300 (-03)
MIME-Version: 1.0
Content-Type: multipart/alternative;
	boundary="=_9cde7a7f84cafe85a96231b766576eaa"
Date: Fri, 15 Mar 2019 10:11:46 -0300
From: admin <mrussoinformatica@bewnet.com.br>
To: undisclosed-recipients:;
Subject: =?UTF-8?Q?Querido_usu=C3=A1rio=2C?=
Message-ID: <c0d1792a598509077bb2d9f9e582c632@bewnet.com.br>
X-Sender: mrussoinformatica@bewnet.com.br
User-Agent: Roundcube Webmail/Final

CADE
Conselho Administrativo de Defesa Econômica

Estrutura do phishing: mensagem

admin <mrussoinformatica@bewnet.com.br> 0

Querido usuário,

Querido usuário,

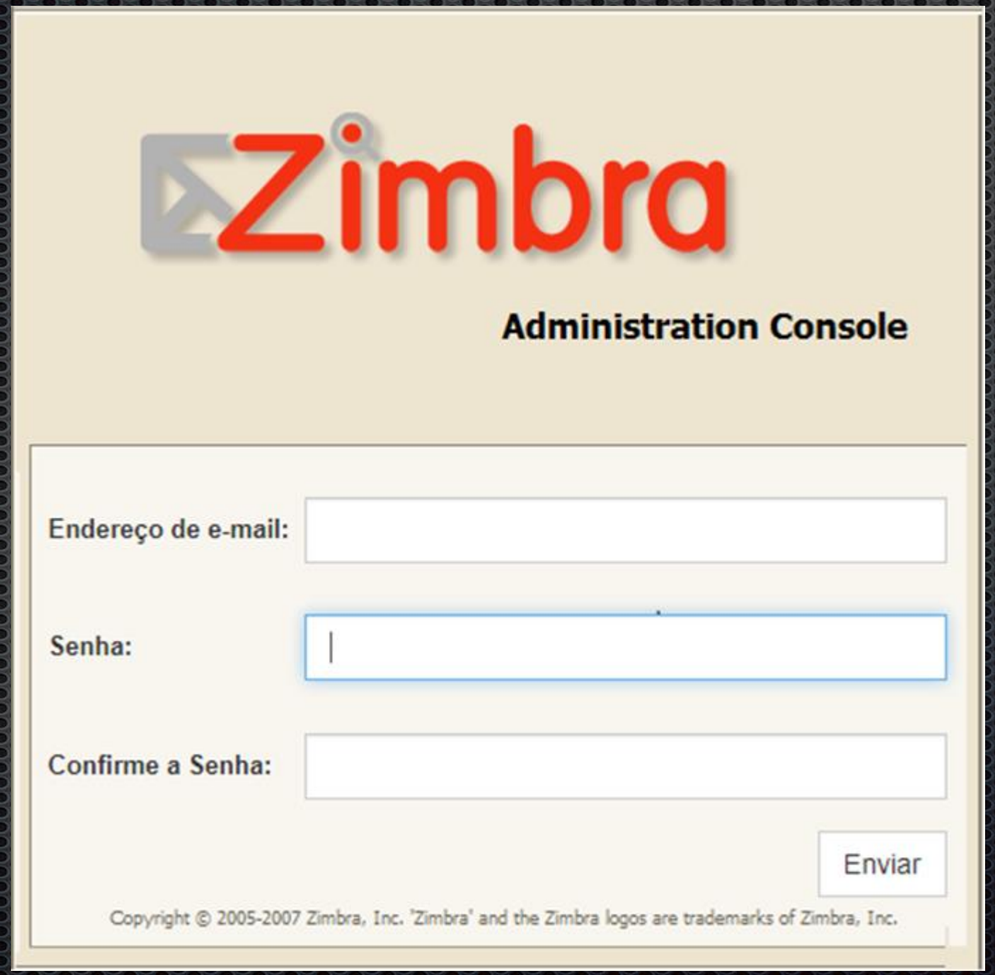
Sua caixa de correio será encerrada devido à negligência de vários e-mails. Para evitar isso, por favor clique aqui para atualizar sua conta de caixa de correio.

Pedimos desculpas por qualquer inconveniente que isso possa causar.

Administrador do sistema.

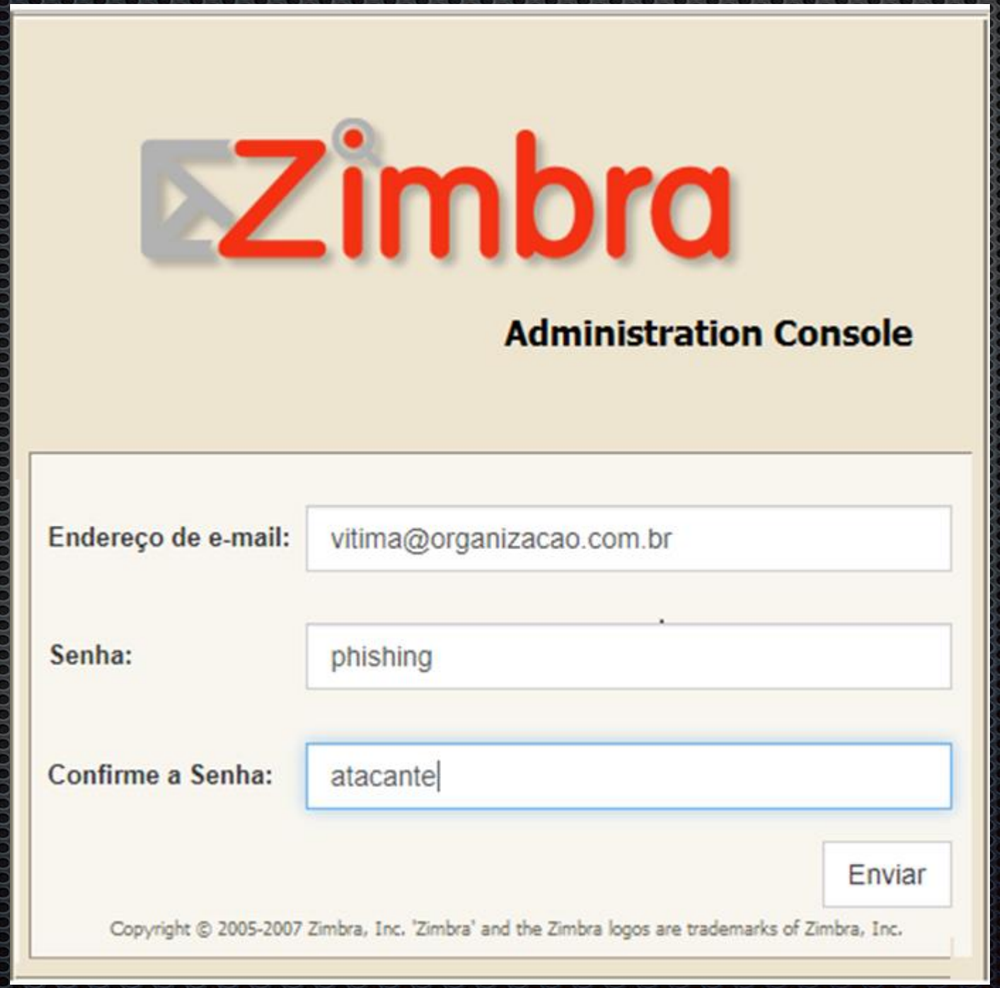
CADE
Conselho Administrativo de Defesa Econômica

Estrutura do phishing: Captura de Credenciais



CADE
Conselho Administrativo de Defesa Econômica

Estrutura do phishing: Captura de Credenciais



CADE
Conselho Administrativo de Defesa Econômica

Estrutura do phishing: Encaminhamento de Spam

Good day,

I'm Azim Hashim Premji, an Indian business tycoon, investor, and philanthropist. I'm the chairman of Wipro Limited. . I gave away 25 per cent of my personal wealth to charity. And I also pledged to give away the rest of 25% this year new 2019.. I wish to donate $700,000.00USD to every individual. Congratulation, a donation of $700,000.00 has been made to you. If you are interested in my donation, do contact me directly via:
azimpremj9@gmail.com for more info. Note: Opportunities comes, but once.

You can also read more about me via the link below

http://en.wikipedia.org/wiki/Azim_Premji

Thank You

CADE
Conselho Administrativo de Defesa Econômica

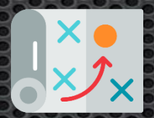
Estratégia de resposta ao incidente

Detecção

Análise

Contenção

Remediação



Recuperação

Pós incidente

Detecção

- Recebimento de chamado sobre o Outlook ter parado de funcionar

Análise

- Houve infecção nos dispositivos do paciente 0?
- Qual o alcance do ataque?
- O que os logs podem contar?
- Houve comprometimento da infraestrutura de email?
- Qual a extensão do ataque?
- Houve vazamento de dados?
- Houve impacto sobre o domínio?

CADE
Conselho Administrativo de Defesa Econômica

Contenção

- Troca da senha das vítimas
- Bloqueio de links maliciosos no firewall
- Regras mais restritivas no antispam
- Alerta para os usuários

Remediação

- Retirada do domínio de blacklists na internet
- Contato com parceiros e alerta sobre meios alternativos de manter a comunicação
- Revisão das configurações do SPF – Sender Policy Framework
- Configuração do DKIM e DMARC

Recuperação

- Abertura de chamados com a Microsoft e Google
- Preenchimento do formulário para o erro 550-5.7.1 - *O usuário ou o domínio para o qual (ou do qual) você está enviando tem uma política que proíbe o e-mail enviado. Entre em contato com o administrador do domínio para mais detalhes*

CADE
Conselho Administrativo de Defesa Econômica

Ações Pós-Incidente

- Aperfeiçoamento das regras antiphishing/spam
- Comunicação com os usuários sobre os riscos de clicar em links indevidos

Evitando entrar em *blacklists*

- Não deixar relays de email abertos
- Antispam com regras em dia
- Políticas de bloqueio de envio massivo de e-mails
- Registro PTR do DNS externo configurado
- Registro de endereços autorizados para comunicação SMTP (SPF)
- Assinatura do domínio (DKIM)
- Política de conformidade (DMARC)
- Monitoramento da reputação
- Configuração de nomes de administração de domínio (abuse, security, noc)
- Gerência da porta 25*

Evitando entrar em *blacklists*: DKIM

- Registro TXT no DNS com a chave pública do domínio
- Permite aplicação de regras
- Mecanismo de assinatura e verificação de mensagens
- Permite adoção de políticas de ferramentas antispam para bloqueio de domínios sem autenticação (indício de phishing)

Evitando entrar em *blacklists*: DKIM

- Exemplo:

Tag	TagValue	Name	Description
v	DKIM1	Version	The DKIM record version.
k	rsa	Key type	The type of the key used by tag (p).
s	email	Service Type	A colon-separated list of service types to which this record applies.
p	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA/UmFjuQMxM2p1TsgKZIzGwbRnLfZnuEDKTYrqK+HwtSUfwvmU/BHDIETVtM6tK3rutT1f0aB2W2HaW/K8AMiAe+qEfhHRWod2C+AlB1Hu/qZgVaq/YFzck7qFbqEByV7y9NIKJdi/4W9i9KdmLPOUho/xgAYXsBRnmrDkMSb3RQrbZvCz67k3kf6iCxL45rSlEYgdMMdI3CwOjkpkJU9dZSYFOtNzW56GhZ3rmTZjrm04MySO6CwZDwg5WwGvH0Jf5xnITbmVCCFJPyQssKpAjItnNktoOP2b6aslHo7m8d/qtqGVvsKUKVOOdEqgCHMF1Wsu36sfBCXfk5dVY1DdwIDAQAB	Public Key	Public-key data. The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.

	Test	Result
✓	DNS Record Published	DNS Record found
✓	DKIM Record Published	DKIM Record found
✓	DKIM Syntax Check	The record is valid
✓	DKIM Public Key Check	Public key is present

Fonte: MXToolbox

CADE
Conselho Administrativo de Defesa Econômica

Evitando entrar em *blacklists*: DMARC

- Registro TXT no DNS com as definições de política de conformidade
- Mecanismo de conformidade de boas práticas de e-mails (SPF e DKIM)
- Implementa políticas de aceite, quarentena, rejeição de mensagens
- Permite o envio de relatórios das mensagens em quarentena ou rejeição

CADE
Conselho Administrativo de Defesa Econômica

Evitando entrar em *blacklists*: DMARC

- Exemplo:

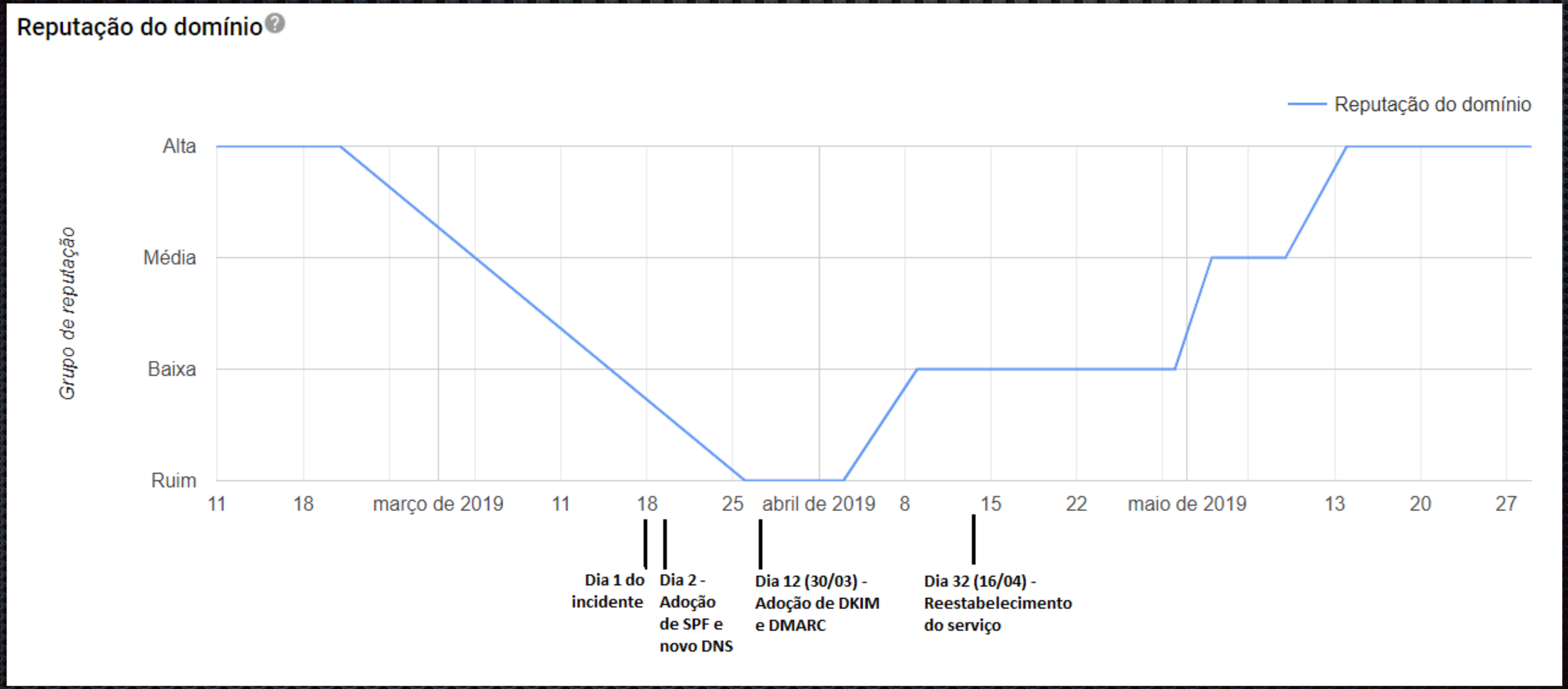
Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. TagValue can be 'none', 'quarantine', or 'reject'.
rua	mailto:abuse@cade.gov.br	Receivers	List of URIs for receivers to send XML feedback to. URIs are required to be added in the format of 'mailto:address@example.com'.
ruf	mailto:security@cade.gov.br	Forensic Receivers	List of URIs for receivers to send Forensic reports to. URIs are required to be added in the format of 'mailto:address@example.com'.

	Test	Result	
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✓	DNS Record Published	DNS Record found	
✓	DMARC Record Published	DMARC Record found	
✓	DMARC Syntax Check	The record is valid	
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	

Fonte: MXToolbox

CADE
Conselho Administrativo de Defesa Econômica

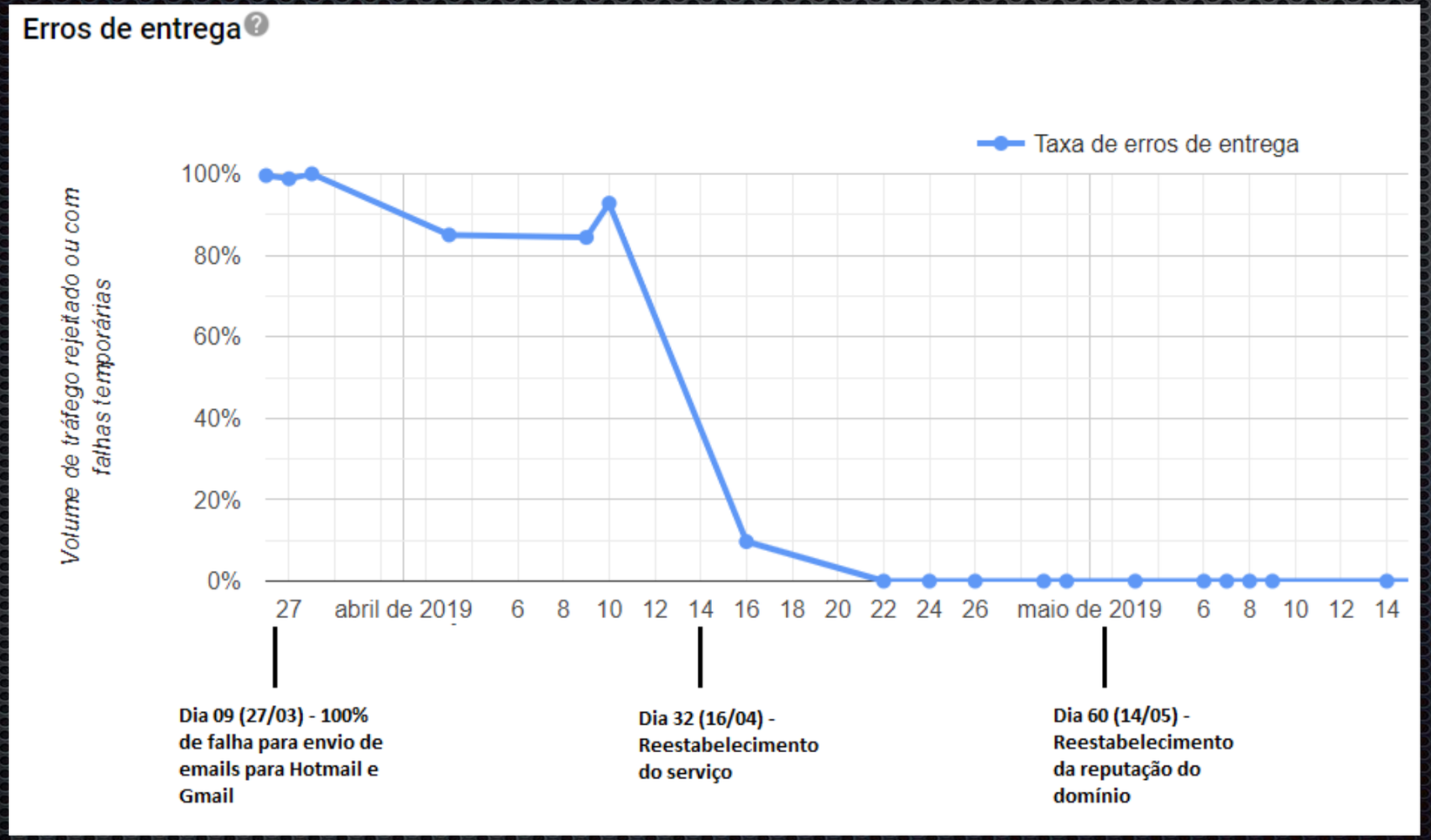
Impacto do incidente



Fonte: Google Postmaster Tools

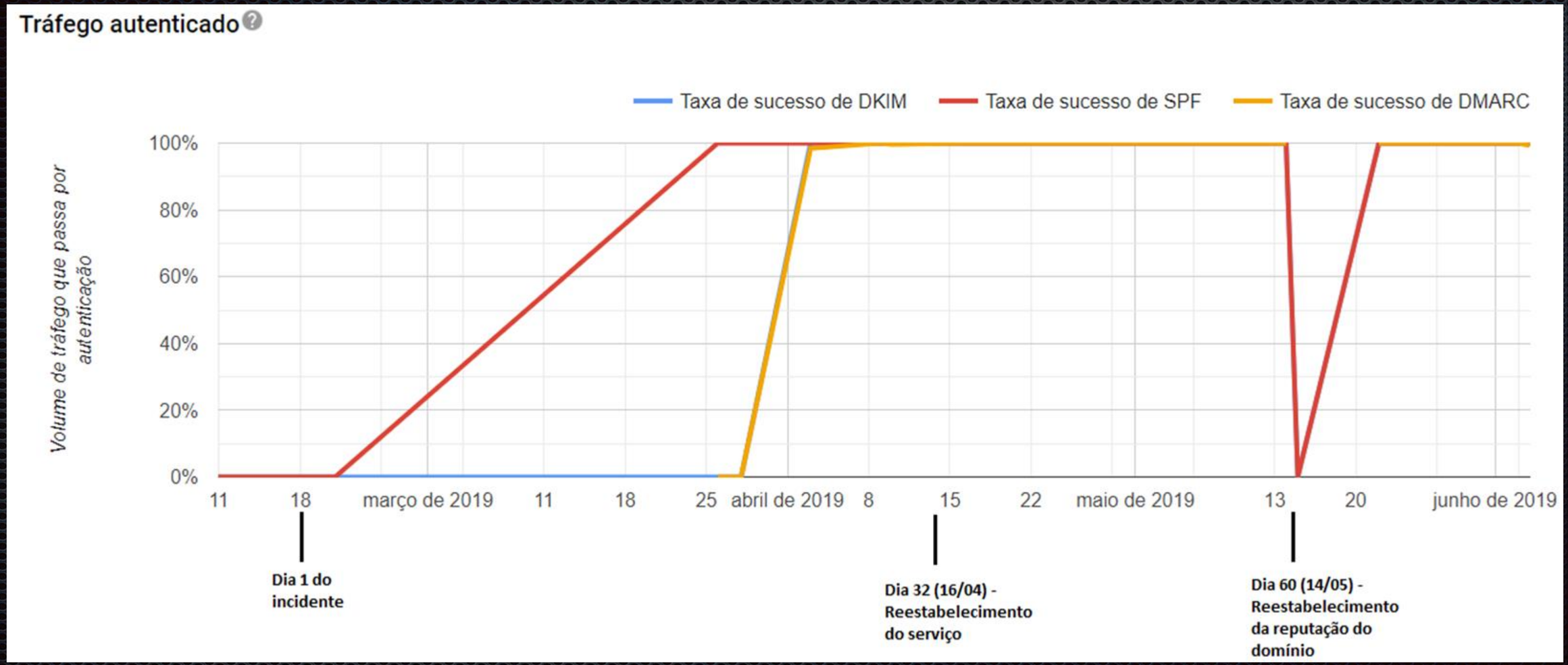
CADE
Conselho Administrativo de Defesa Econômica

Impacto do incidente



Fonte: Google Postmaster Tools

Impacto do incidente



Fonte: Google Postmaster Tools

Resultado das ações

Fonte: Mail Tester

CADE
Conselho Administrativo de Defesa Econômica

Números

- 54 usuários receberam o phishing
- 3 pessoas clicaram
- 1 conta propagou spams
- (Tentativa de) disseminação para 2059 contas de e-mail para os domínios MSN, Hotmail e Gmail
- 8 dias sem receber comunicação de e-mails do Hotmail
- 32 dias sem receber comunicação de mail servers hospedados no Google
- 60 dias para normalizar por completo o serviço
- 7 dias para implementação de novo DNS, publicação de DKIM e DMARC (modo de monitoramento)
- Prejuízo estimado na ordem de R$ 3.900.000,00*

*Valor estimado com base nas multas aplicadas pelo Cade entre 2015/2019
e quantitativo de entrada de processos de julgamento na autarquia

CADE
Conselho Administrativo de Defesa Econômica

Fontes

- Antispam.br - www.antispam.br
- RFC 7208 - tools.ietf.org/html/rfc7208
- DKIM – dkim.org
- RFC 6376 - tools.ietf.org/html/rfc6376
- RFC 2142 - www.ietf.org/rfc/rfc2142
- DMARC – dmarc.org
- Microsoft Smart Network Data Service – sendersupport.olc.protection.outlook.com/snds/index.aspx
- Google Postmaster Tools – postmaster.google.com
- MXToolbox - mxtoolbox.com
- Mail tester - www.mail-tester.com
- Formulário para reportar o erro 550-5.7.1 - support.google.com/mail/contact/msgdelivery
- Cade em números – cadenumeros.cade.gov.br

CADE
Conselho Administrativo de Defesa Econômica

Obrigado!

security@cade.gov.br