TRIBUNAL DE CONTAS DA UNIÃO

TCU
Federal Court of Accounts - Brazil

Information Security Assessment Division (Dasi)

Diretoria de Avaliação de Segurança da Informação

Segecex/SecexEstado
Unidade de Auditoria Especializada em Tecnologia da Informação – AudTI
Diretoria de Avaliação de Segurança da Informação – Dasi

whoami

TCU

Since 2003

CIA Certified Internal Auditor

CGAP Certified Government Auditing Professional

CCSA Certification in Control Self-Assessment

CRMA Certification in Risk Management Assurance

Association of Certified Fraud Examiners · CFE ·

IBGC Conselheiro Certificado

CISA

EXIN Information Security Management ISO/IEC 27001 FOUNDATION Certified by EXIN

EXIN Privacy & Data Protection FOUNDATION Certified by EXIN

EXIN Privacy & Data Protection PROFESSIONAL Certified by EXIN

EXIN Data Protection Officer EXIN CERTIFIED

CompTIA Security+ CERTIFIED · CE

CompTIA CySA+ CERTIFIED · CE

Certified AppSec Practitioner · The SecOps Group

ICCA INE

eJPTv2 Dynamic Exam

Certified Red Team Professional

Offensive Security OSWP

Carnegie Mellon University · Software Engineering Institute

CERT
Incident Response Process Professional
Certificate Holder

whoami

CompTIA CSIE Secure Infrastructure EXPERT

CompTIA CSAE Security Analytics EXPERT

CompTIA CNSP Network Security PROFESSIONAL

CompTIA CNVP Network Vulnerability Assessment PROFESSIONAL

CompTIA CSAP Security Analytics PROFESSIONAL

TCM SECURITY CERTIFIED Practical Network Penetration Tester PNPT

CompTIA CASP+ CERTIFIED · CE

CompTIA PenTest+ CERTIFIED · CE

CompTIA CySA+ CERTIFIED · CE

CompTIA Security+ CERTIFIED · CE

CompTIA Linux+ POWERED BY LPI CERTIFIED

CERTIFIED RED TEAM PROFESSIONAL

CERTIFIED RED TEAM EXPERT

CERTIFIED ENTERPRISE SECURITY PROFESSIONAL (CESP - ADCS)

eJPT

eWPT V1

eCPPT V2

CERTIFIED NETWORK SECURITY PRACTITIONER · THE SECOPS GROUP

CERTIFIED APPSEC PRACTITIONER · THE SECOPS GROUP

Microsoft CERTIFIED AZURE FUNDAMENTALS

CARNEGIE MELLON UNIVERSITY · SOFTWARE ENGINEERING INSTITUTE

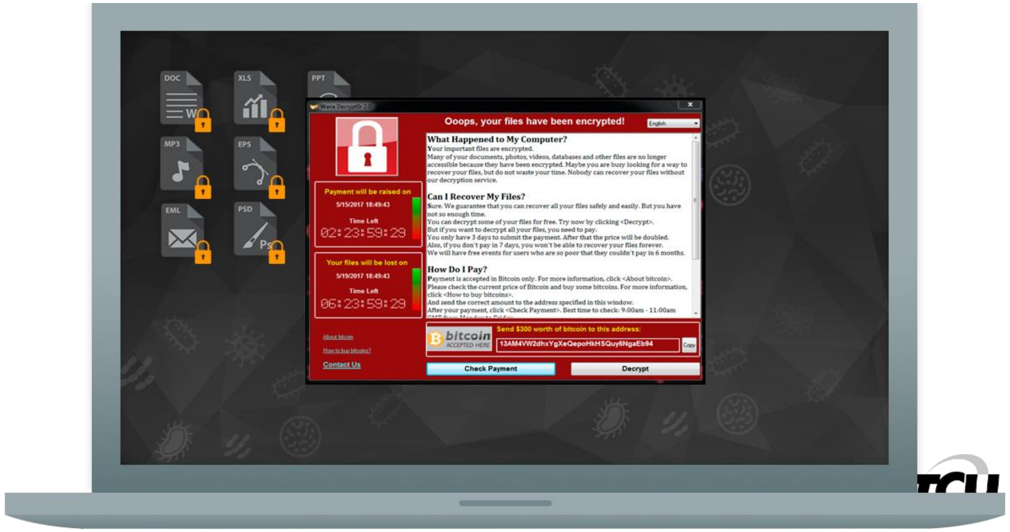
CERT
Incident Response Process Professional
Certificate Holder

TCU

Since 2010

What is ransomware?

- Malicious software (*malware*) that encrypts data, blocks its access and demands a ransom ($) to obtain the decrypting key
  - When there is no payment, sensitive data is exposed
- Evolution to a RaaS model (*ransomware as-a-service*)
- Data loss, business operation interruption, financial and reputation damage



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 18:49:43
Time Left
02:23:59:29

Your files will be lost on
5/19/2017 18:49:43
Time Left
06:23:59:29

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

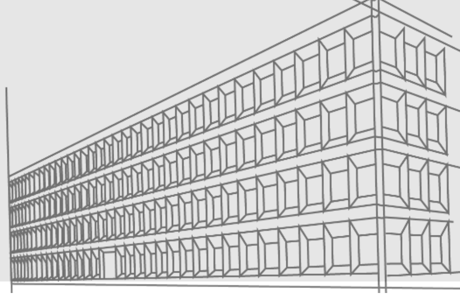
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

What is ransomware?

- Initial infection
- File encryption
- Ransomware notification message
- Payment using cryptocurrencies
- Getting data back (or not?)

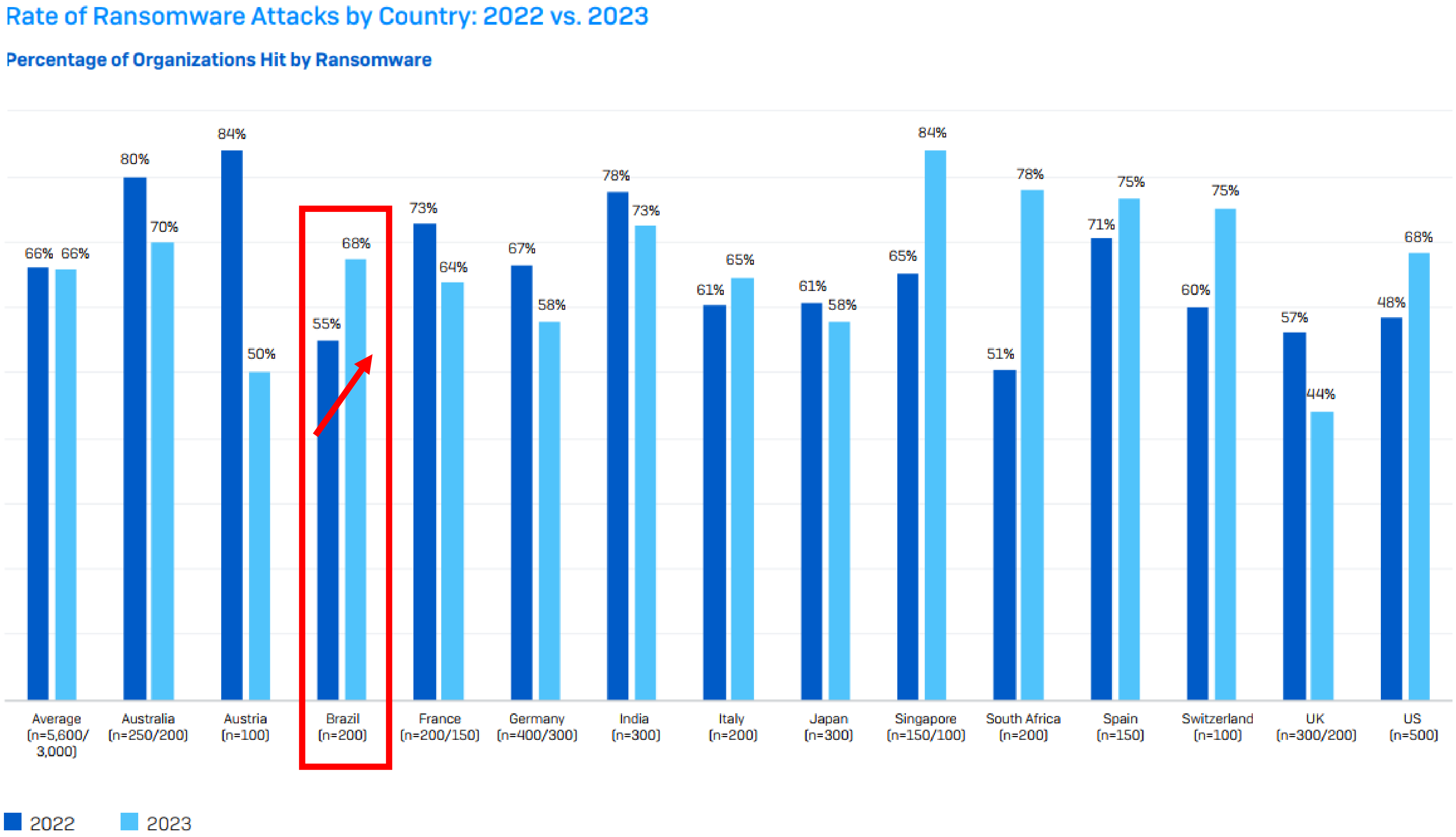
Current cybersecurity landscape



The State of Ransomware 2023

Findings from an independent, vendor-agnostic survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries, conducted in January-March 2023.

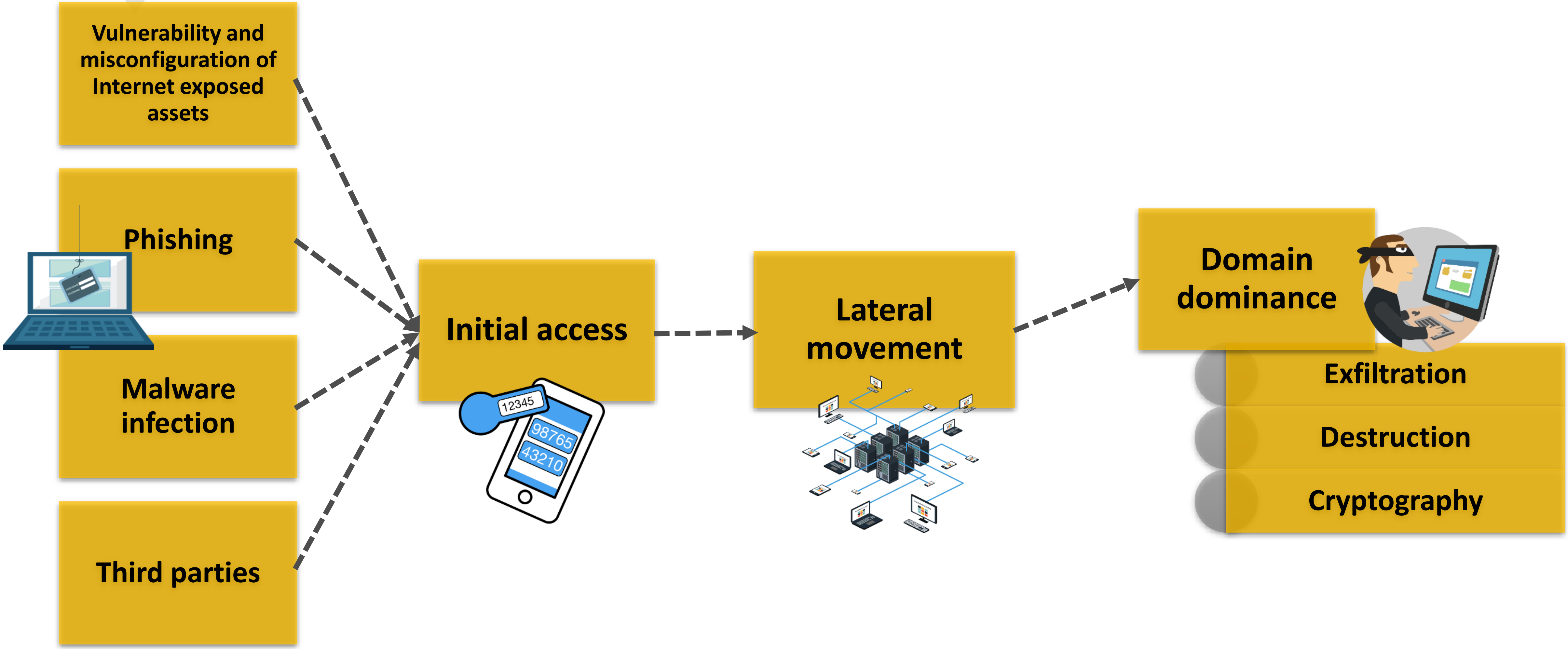
SOPHOS



In the last year, has your organization been hit by ransomware? Base numbers in chart

Fonte: The State of Ransomware 2023

Ransomware attack anatomy



Vulnerability and misconfiguration of Internet exposed assets

Phishing

Malware infection

Third parties

Initial access

Lateral movement

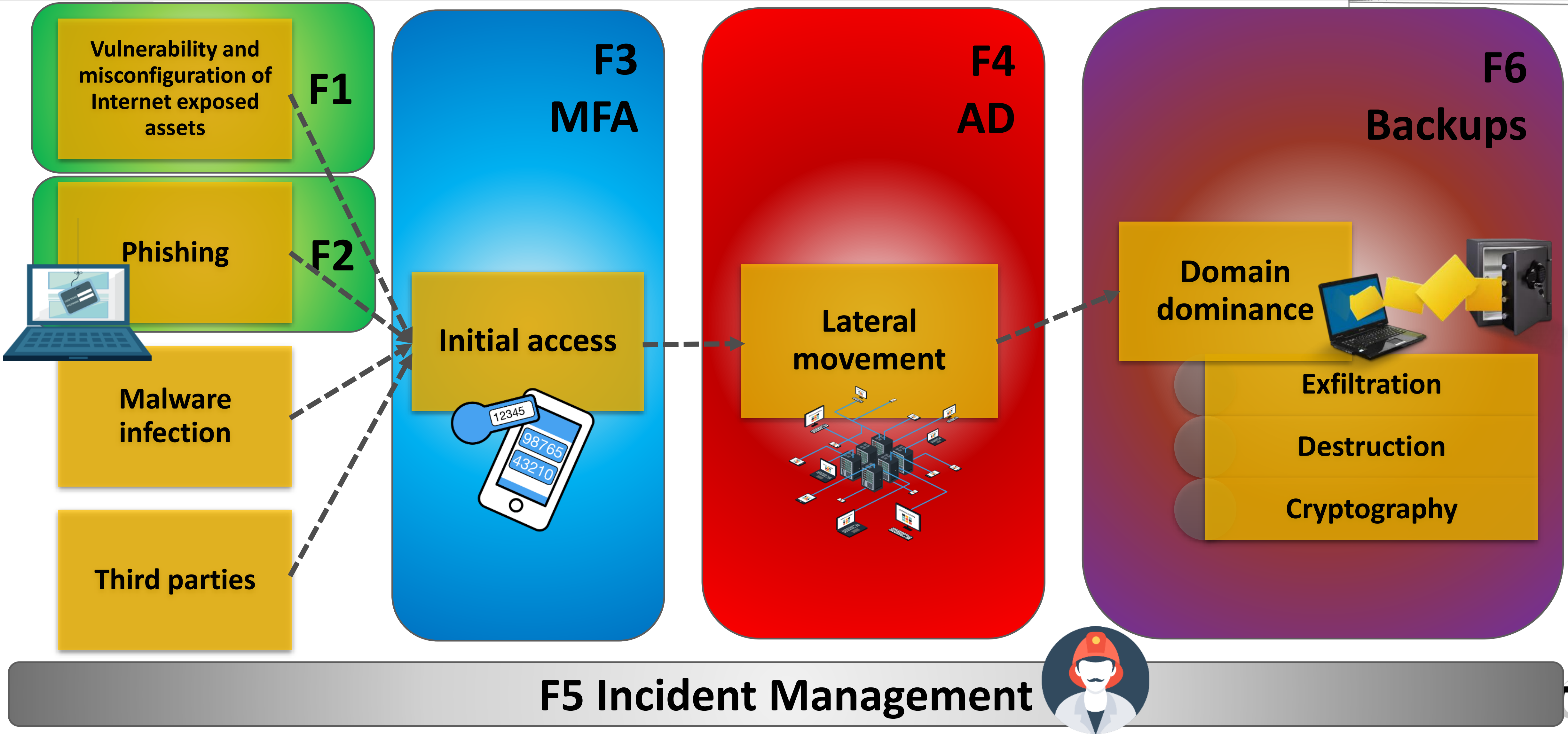
Domain dominance

Exfiltration

Destruction

Cryptography

Ransomware attack anatomy



Vulnerability and misconfiguration of Internet exposed assets

F1

Phishing

F2

Malware infection

Third parties

F3

MFA

Initial access

F4

AD

Lateral movement

F6

Backups

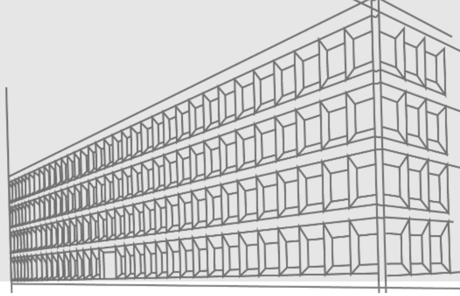
Domain dominance

Exfiltration

Destruction

Cryptography

F5 Incident Management



Methodology

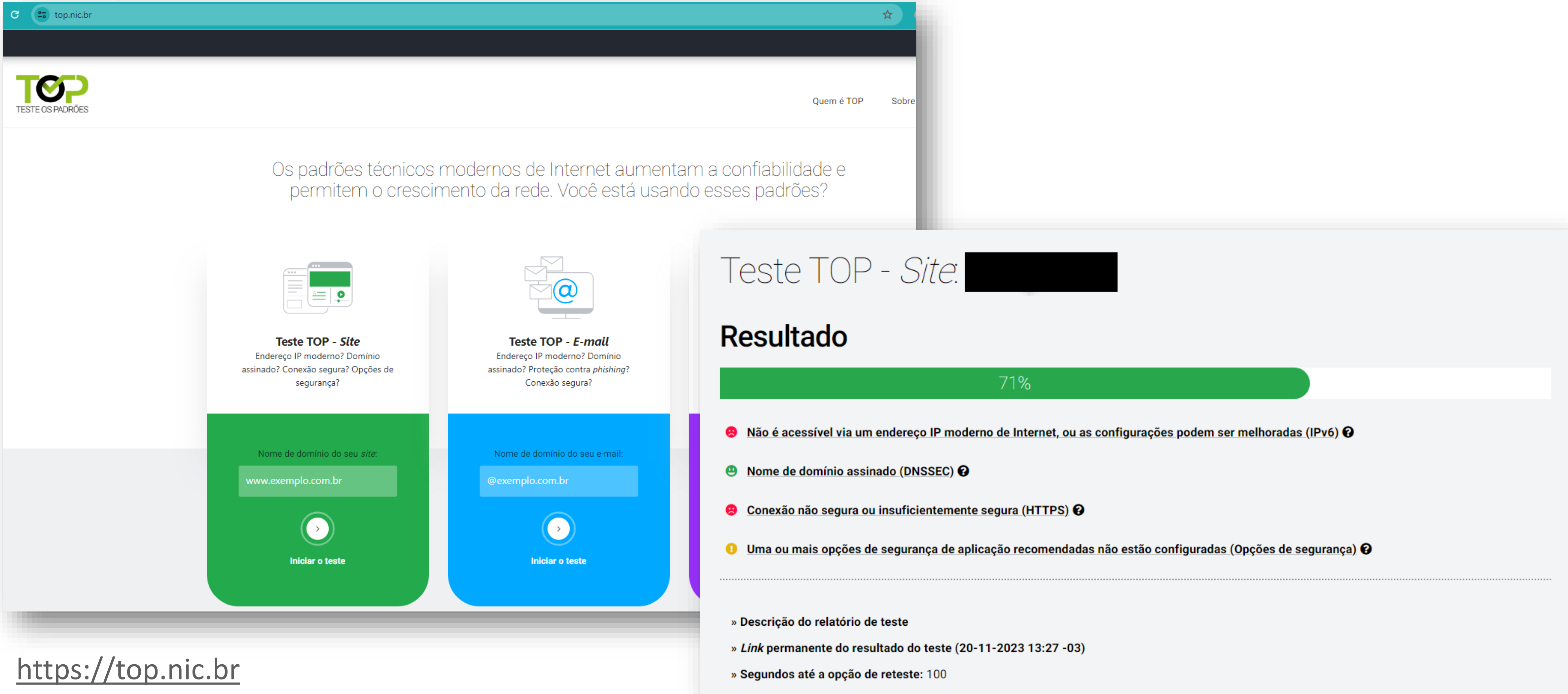
- Operational audits
- Share procedures with auditee before their execution
- Plan from attacker's point of view
- Use attacker's tools for reconnaissance, enumeration, vulnerability assessment

What we do ✓

- Pentest
- Access auditee's assets without their knowledgement
- Act as a read team
- Use attacker's tools for exploitation, post-exploitation

What we don't do ✗

F1: Vulnerability and misconfiguration of Internet exposed assets



top.nic.br

TOP TESTE OS PADRÕES

Quem é TOP Sobre

Os padrões técnicos modernos de Internet aumentam a confiabilidade e permitem o crescimento da rede. Você está usando esses padrões?

Teste TOP - *Site*
Endereço IP moderno? Domínio assinado? Conexão segura? Opções de segurança?

Nome de domínio do seu *site*:
www.exemplo.com.br

Iniciar o teste

Teste TOP - *E-mail*
Endereço IP moderno? Domínio assinado? Proteção contra *phishing*? Conexão segura?

Nome de domínio do seu e-mail:
@exemplo.com.br

Iniciar o teste

Teste TOP - *Site*: [redacted]

Resultado

71%

- ☹ Não é acessível via um endereço IP moderno de Internet, ou as configurações podem ser melhoradas (IPv6) ?
- ☺ Nome de domínio assinado (DNSSEC) ?
- ☹ Conexão não segura ou insuficientemente segura (HTTPS) ?
- ! Uma ou mais opções de segurança de aplicação recomendadas não estão configuradas (Opções de segurança) ?

» Descrição do relatório de teste

» *Link* permanente do resultado do teste (20-11-2023 13:27 -03)

» Segundos até a opção de reteste: 100

https://top.nic.br

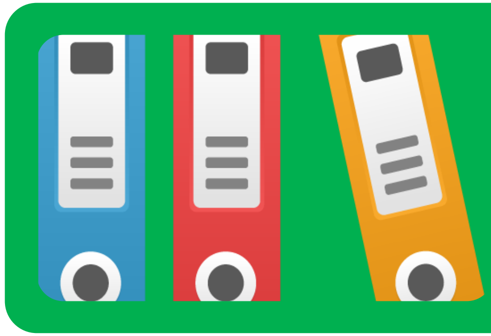
(Project based on https://internet.nl/)

F1: Vulnerability and misconfiguration of Internet exposed assets

Around 14K URLs

ALL federal, state, district and municipal public organizations that have web, email and DNS services in URL located by the engagement team

F2: Phishing



1st Layer (administrative)

- Internal standards (AUP) and related processes
- Use of corporate email by users

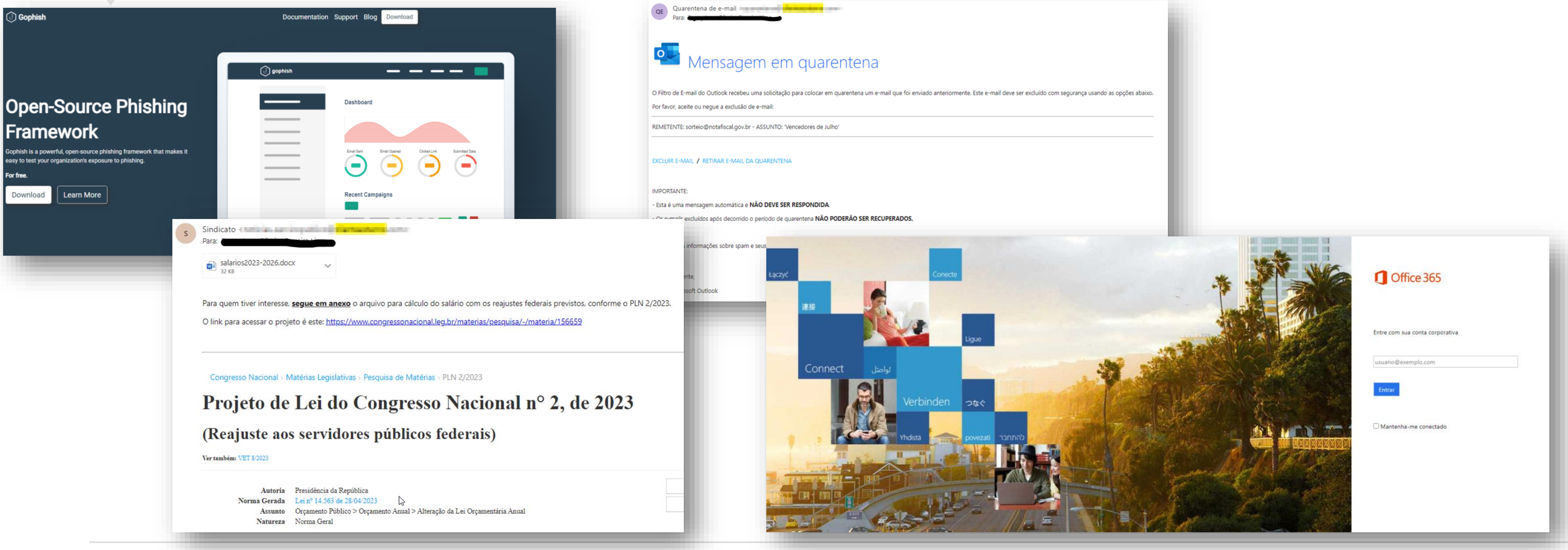
2nd Layer (technical)

- Email server controls (SPF, DKIM, DMARC)
- Support solutions

3rd Layer (User awareness)

- User Awareness Program
- Phishing simulation

F2: Phishing



Open-Source Phishing Framework

Gophish is a powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing.

For free.

Quarantena de e-mail [redacted]
Para: [redacted]

Mensagem em quarentena

O Filtro de E-mail do Outlook recebeu uma solicitação para colocar em quarentena um e-mail que foi enviado anteriormente. Este e-mail deve ser excluído com segurança usando as opções abaixo.

Por favor, aceite ou negue a exclusão de e-mail:

REMETENTE: sorteio@notafiscal.gov.br - ASSUNTO: 'Vencedores de Julho'

EXCLUIR E-MAIL / RETIRAR E-MAIL DA QUARENTENA

IMPORTANTE:

- Esta é uma mensagem automática e **NÃO DEVE SER RESPONDIDA**.

- Os e-mails excluídos após decorrido o período de quarentena **NÃO PODERÃO SER RECUPERADOS.**

informações sobre spam e seus

nte,

soft Outlook

Sindicato [redacted]
Para: [redacted]

salarios2023-2026.docx
32 KB

Para quem tiver interesse, **segue em anexo** o arquivo para cálculo do salário com os reajustes federais previstos, conforme o PLN 2/2023.

O link para acessar o projeto é este: https://www.congressonacional.leg.br/materias/pesquisa/-/materia/156659

Congresso Nacional › Matérias Legislativas › Pesquisa de Matérias › PLN 2/2023

Projeto de Lei do Congresso Nacional n° 2, de 2023

(Reajuste aos servidores públicos federais)

Ver também: VET 8/2023

Autoria	Presidência da República
Norma Gerada	Lei nº 14.563 de 28/04/2023
Assunto	Orçamento Público > Orçamento Anual > Alteração da Lei Orçamentária Anual
Natureza	Norma Geral

Office 365

Entre com sua conta corporativa

usuario@exemplo.com

Entrar

□ Mantenha-me conectado

Phishing templates

2 templates measuring if user **clicked** on a malicious link

2 templates measuring if user **accessed** a malicious webpage and **inserted** personal information

2 templates with **attached files**, measuring if user opened file and enabled macro execution

F3: MFA (multi-factor authentication)

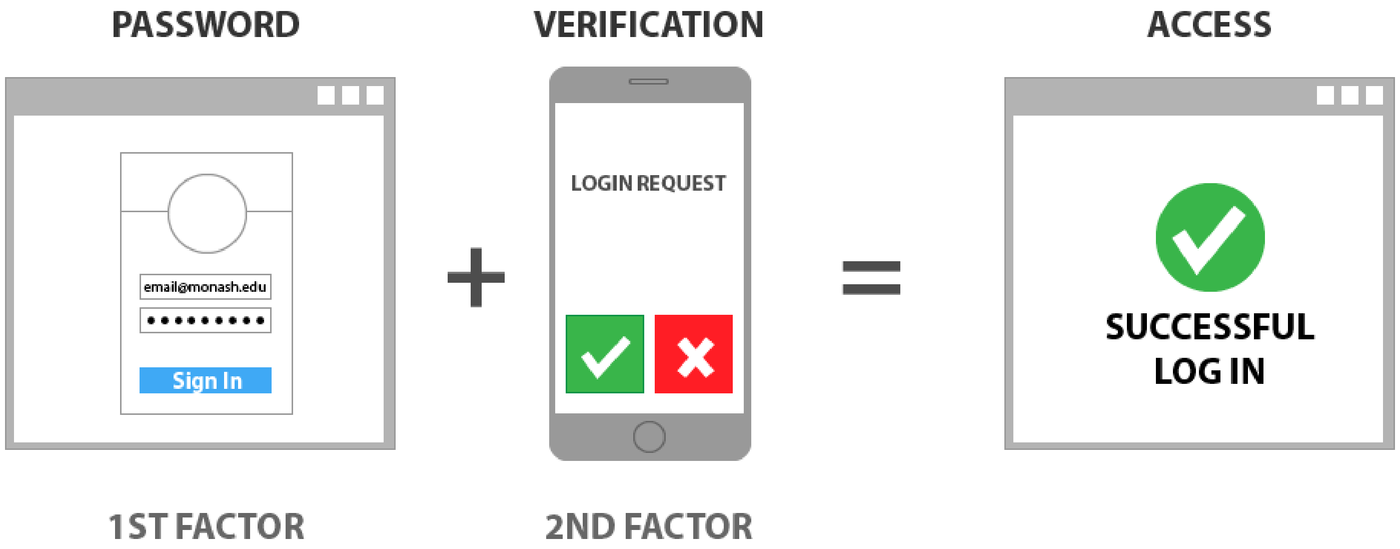


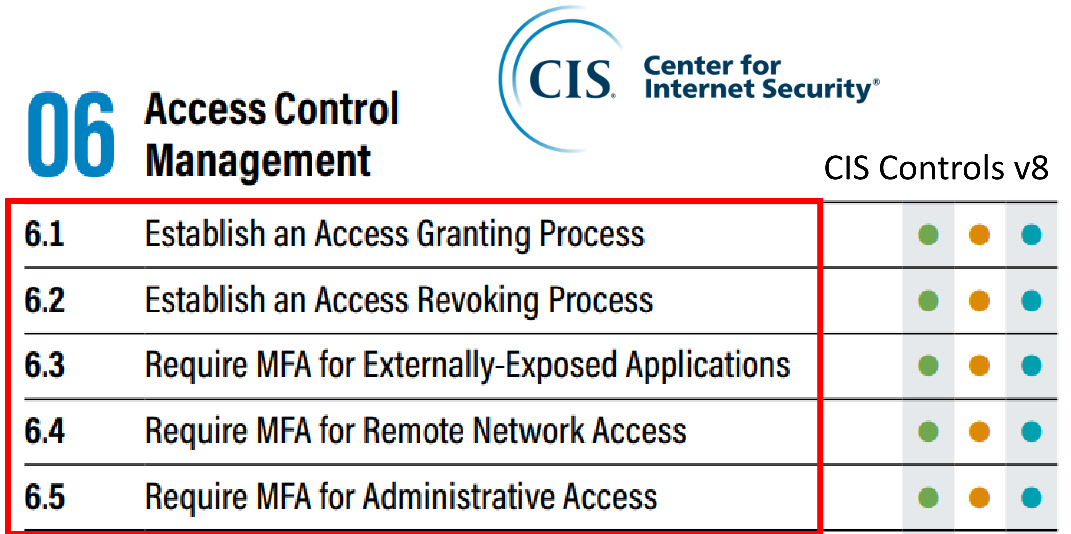
Image source: Monash University

MFA

Type of technology in use

Grant, revocation and recovery

Application, remote network and administrative acess



06 Access Control Management

CIS Center for Internet Security®

CIS Controls v8

6.1	Establish an Access Granting Process	●	●	●
6.2	Establish an Access Revoking Process	●	●	●
6.3	Require MFA for Externally-Exposed Applications	●	●	●
6.4	Require MFA for Remote Network Access	●	●	●
6.5	Require MFA for Administrative Access	●	●	●

F4: Active Directory

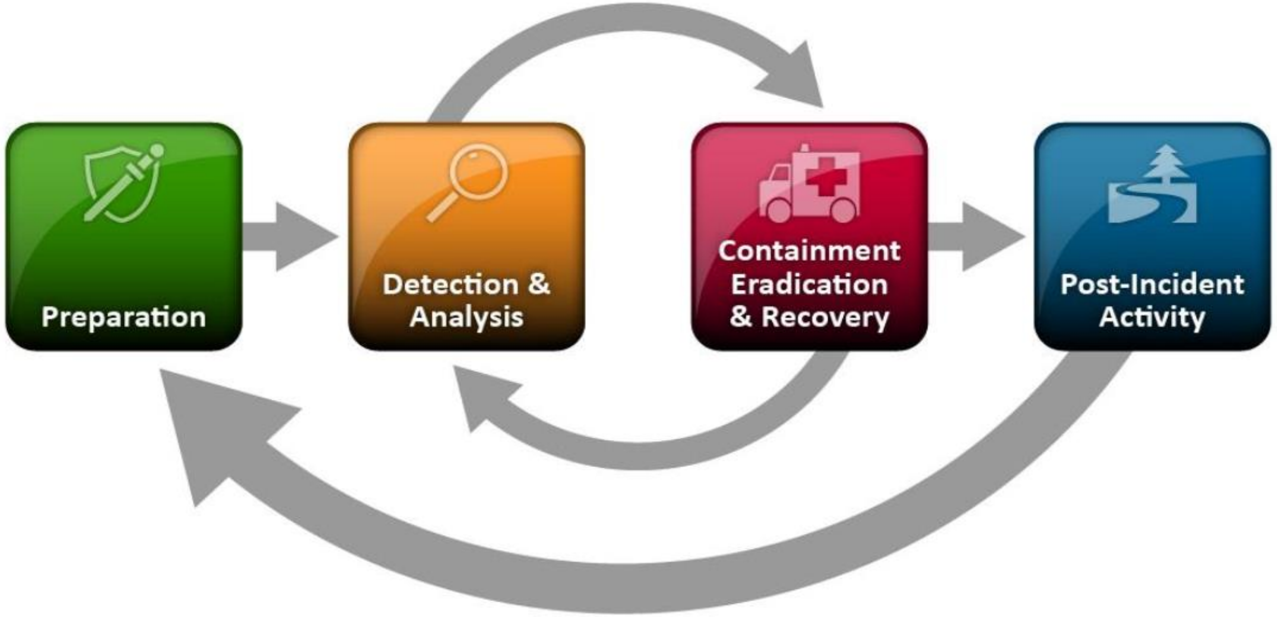
People, processes and roles

Active Directory configuration

Active Directory Monitoring (focus on security alerts)

Active Directory backup & recovery

F5: Incident Management



Audit Criteria

NIST 800-61 rev. 2

Security Incident Response Guide – SGD

F5: Backups

Audit Criteria

ABNT NBR ISO/IEC 27002

CIS Controls v8 - 11 Data Recovery

Backup Policy Model – SGD

Information Security Assessment Division (Dasi)

Diretoria de Avaliação de Segurança da Informação

dasi at tcu dot gov dot br

Segecex/SecexEstado
Unidade de Auditoria Especializada em Tecnologia da Informação – AudTI
Diretoria de Avaliação de Segurança da Informação – Dasi

https://www.linkedin.com/in/andretorresbr/