TLP:CLEAR


DEFEND
DETECT
RESPOND
RANSOMWARE x BLUE TEAMS
UMA GUERRA CIBERNÉTICA SEM FIM
ENCRYPTING
DATA LOCKED
PAY OR LOSE
NO ESCAPE
YOU HAVE BEEN HACKED
RANSOMWARE
YOUR FILES ARE ENCRYPTED
TIME LEFT:
47:59:59
PAY OR LOSE
ZOZIEL FREIRE
THREAT DETECTED
CONHECER O INIMIGO
FORTALECER DEFESAS
DETECTAR AMEAÇAS
INVESTIGAR E ANALISAR
RESPONDER RAPIDAMENTE
PROTEGER SEMPRE

TLP:CLEAR

Disclaimer

Nada do que apresento aqui representa a posição da minha empresa. Todas as opiniões e análises são de minha exclusiva responsabilidade.

TLP:CLEAR

Propósito

Apresentar um pouco da evolução dos malwares e das defesas de segurança, evidenciando a adaptação constante entre atacantes e defensores.

TLP:CLEAR

Whoami ?

Whoami ?

TLP:CLEAR

- Profissional +16 anos de experiência em TI
- Pesquisador em segurança nos ecossistemas: Windows Linux e Apple
- Apaixonado por Análise e Desenvolvimento de Malware
- Organizador Apple Red Team Village
- Fã de Chaves e Chapolin ☺

Contribuições para Comunidade

TLP:CLEAR

NerdZão

TLP:CLEAR

Tópicos

- Do Vírus ao Ransomware
- O que é um Ransomware?
- Evolução: Ataque x Defesa
- Tipos de Ataques
- Evolução dos CSIRTs
- Estudos de Casos
- Conclusão

TLP:CLEAR

Do Virus ao Ransomware

TLP:CLEAR

> DO PRIMEIRO VÍRUS AO PRIMEIRO RANSOMWARE_

// a evolução essencial do malware

01 [PoC]

1971

CREEPER

1o programa autorreplicante. Nao malicioso — exibia mensagem de alerta. Marco teorico do virus.

02 [WILD]

1982

ELK CLONER

1o virus "in the wild", via disquetes Apple II. Poema exibido a cada 50 boots.

03 [PC]

1986

BRAIN

1o virus para MS-DOS. Irmaos Alvi (Paquistao). Infectava setor de boot.

04 [NET]

1988

MORRIS WORM

1o worm em escala na internet. Explorava falhas Unix. ~10% dos hosts afetados.

05 [EXTORTION]

1989

AIDS TROJAN

1o ransomware conhecido. Disquetes via correio. Resgate de US$189 -> caixa postal no Panama.

TLP:CLEAR

O que é um ransomware?

TLP:CLEAR

O que é Ransowmare?

O ransomware é um tipo de ataque malicioso no qual os invasores criptografam os dados de uma organização, os vazam e exigem pagamento para restaurar o acesso ou impedir a exposição.

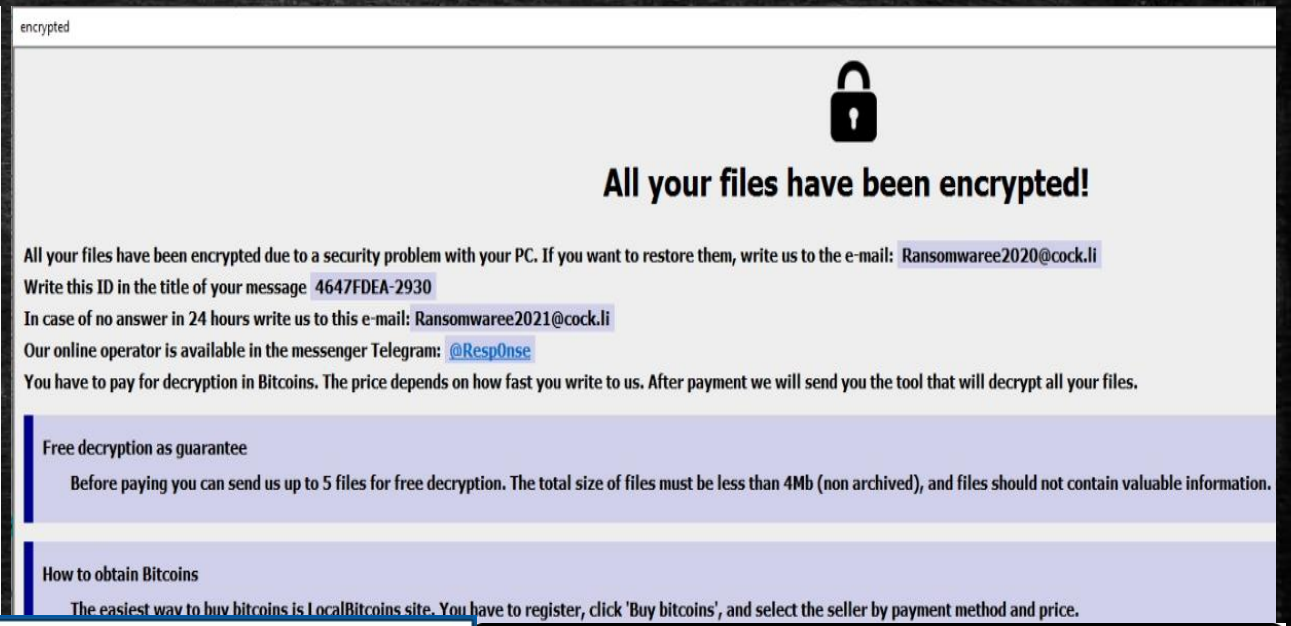
TLP:CLEAR

Modus Operandi

Modus - 1	*Modus -2*	*Modus - 3*
Criptografia	Criptografia	Criptografia
Extorsão	Extorsão	Extorsão
	Exposição	Exposição
		Notificação Regulatório

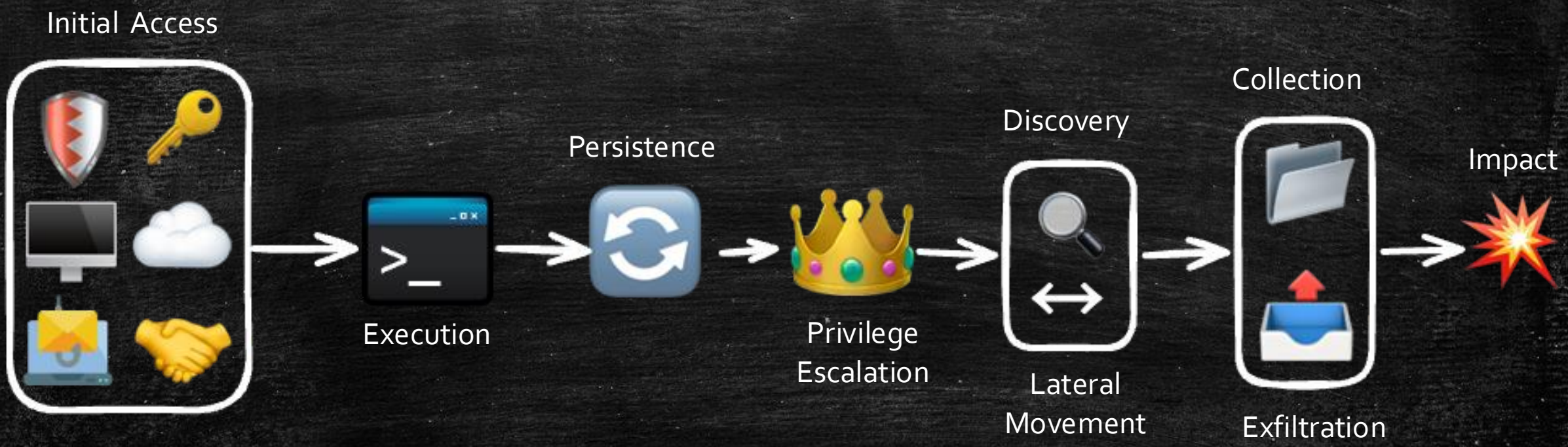
Nota de Invasão

TLP:CLEAR



Ransonware Kill Chain

TLP:CLEAR



TLP:CLEAR

Impactos

- Interrupção das operações
- Perdas financeiras
- Perda ou vazamento de dados
- Danos à reputação
- Consequências legais e regulatórias
- Redução da produtividade
- Custos de recuperação
- Impacto na continuidade do negócio

TLP:CLEAR

Evolução: Ataque x Defesa

UMA GUERRA SEM FIM

TLP:CLEAR

Evolução do ataque vs. evolução da defesa, década a década

● Marcos de ataque ● Resposta defensiva

ATÉ 1990

- Vírus de disquete (Brain, Elk Cloner)
- Worms de rede local (Morris, 1988)
- Vírus de macro embrionários
- Phreaking e acesso não autorizado
- AIDS Trojan 1º Ransomware

- Antivírus por assinatura (McAfee, Norton)
- Firewall de pacote simples
- Criptografia básica (PGP, DES)
- TCP Wrappers / controle Unix
- IDS acadêmico incipiente (Snort, 1998)

2000 – 2009

- Worms por e-mail (ILOVEYOU, Melissa)
- Worms automatizados (SQL Slammer)
- Botnets surgem (Zeus, Conficker)
- Ataques web (SQL Injection, XSS)
- Phishing bancário se populariza

- NGFW (stateful inspection)
- IDS/IPS comerciais (Snort, Sourcefire)
- SIEM surge (correlação de logs)
- VPN corporativa (IPSec/SSL)
- Pentest evolui (Nessus, Metasploit)

2010 – 2019

- Malware em infra crítica (Stuxnet)
- Ransomware moderno (CryptoLocker)
- Worm + exploit vazado (WannaCry)
- APTs e ataques direcionados
- Supply chain attacks (SolarWinds)

- EDR substitui o antivirus
- Threat Intel Platforms (IOC feeds)
- SOAR (automação de resposta)
- MITRE ATT&CK como framework
- ML/UEBA na detecção de anomalias

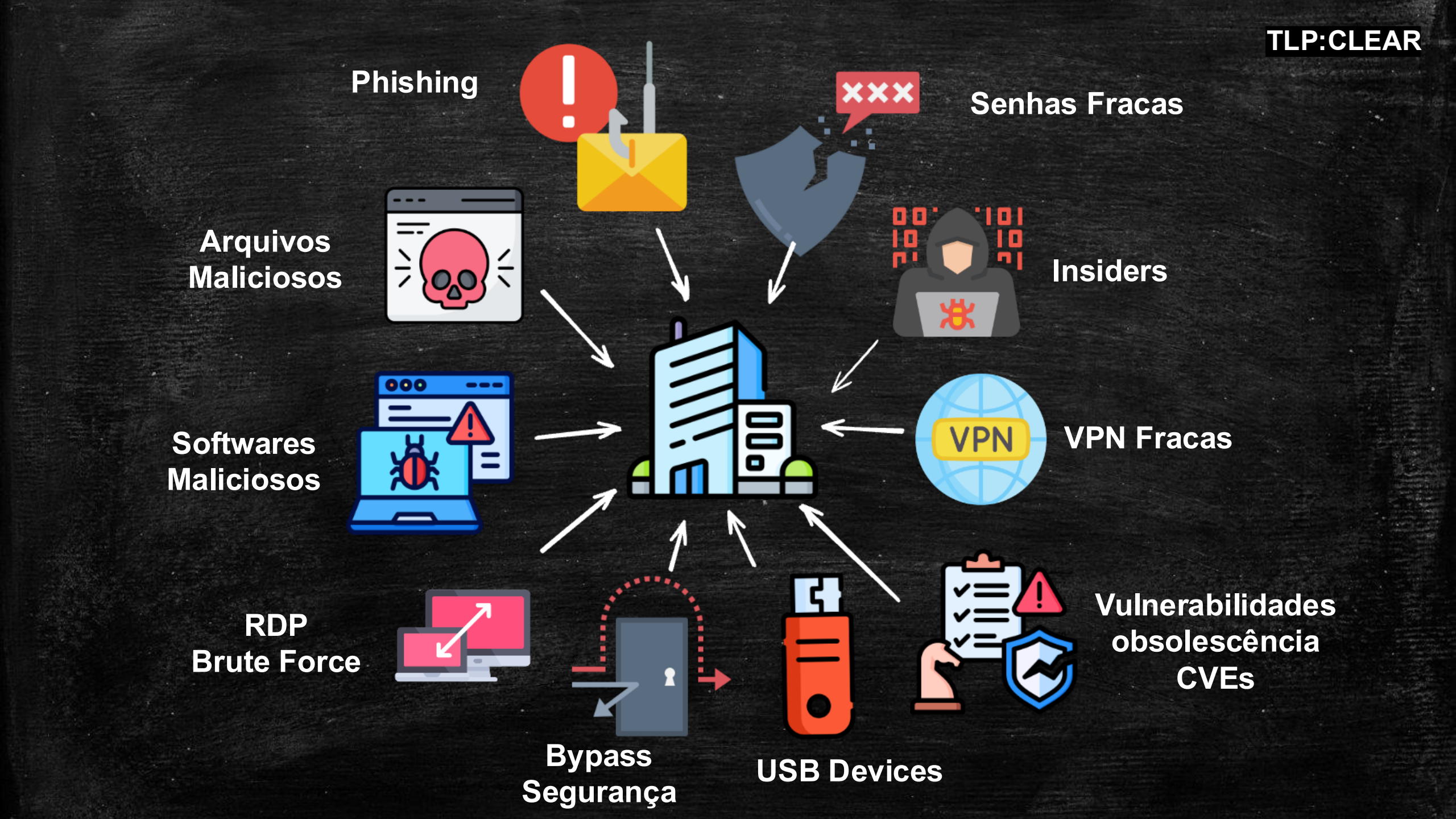
2020 – 2029

- Ransomware-as-a-Service (LockBit)
- Dupla/tripla extorsão de dados
- Ataques a identidade e nuvem
- IA generativa em phishing/deepfake
- Zero-days explorados em escala

- XDR unificado (endpoint/rede/cloud)
- Zero Trust como padrão
- IA generativa no SOC (copiloto)
- CNAPP (segurança cloud-native)
- ITDR (ameaças à identidade)


Tipos de Ataques

TLP:CLEAR


Phishing
Senhas Fracas
Arquivos Maliciosos
Insiders
Softwares Maliciosos
VPN
VPN Fracas
RDP Brute Force
Vulnerabilidades obsolescência CVEs
Bypass Segurança
USB Devices

TLP:CLEAR

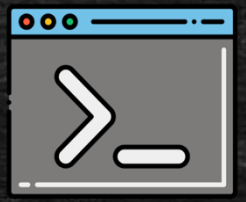
Exemplo de estágios de um Ataque

Recebimento de e-mail de phishing com documento anexado

O documento é aberto e executa macros diretamente no disco / memória

Execução de comandos via macros

Execução de PowerShell via linha de comando Memória ou Disco



Criptografia de Dados via Script

Exibição da nota de resgate

TLP:CLEAR

Evolução dos CSIRTs

Do Antivírus a Inteligência Artificial

Fluxo Tradicional

TLP:CLEAR

Security Tools

CSIRT - Tier 1

CSIRT - Tier 2

CSIRT - Tier 3

Security Rules

PlayBook

RunBook

CSIRT - Computer Security Incident Response Team

TLP:CLEAR

Fluxos Futuros

SOC: Security Operations Center
IA atua como copiloto em cada tier, não substitui o analista humano

TLP:CLEAR

CONCLUSÃO & RECOMENDAÇÕES

Controles Importantes

TLP:CLEAR

- Antivírus / EDR
- SIEM
- XDR
- Firewall NGFW
- IDS / IPS
- Scanner de Vulnerabilidades
- IAM
- PAM
- MFA
- DLP
- WAF
- Segurança de E-mail
- Backup e Recuperação
- Gestão de Patches

Controles Importantes

TLP:CLEAR

- SOAR
- CASB
- SASE
- Threat Intelligence
- Threat Hunting
- Forense Digital
- Pentest
- Criptografia e Gestão de Chaves
- GRC (Governança, Risco e Compliance)
- War Games
- Threat Simulations

Estaremos Seguros? Não!

A AI vai resolver tudo?

Não, mas vai ajudar!

Perguntas?

Contatos

Telegram: @pun1sh3rx0
linkedin.com/in/zozielfreire

Obrigado!