Check Point®
SOFTWARE TECHNOLOGIES LTD

PROTEGENDO SEUS DISPOSITIVOS

Harmony
Mobile

Gustavo Borro – Security Engineer

Henrique Moisés – Securiy Engineer

Tipos de ataques mais recentes
Brasil x Mundo

Principais Malwares e Impactos:

Proxy	9%	0%
Trojan Bancário (TrickBot)	9%	8%
Criptominer (XMRig)	9%	3%
Glupteba	3%	2%
Formbook	3%	3%

	Mobile	Banking	Cryptominer	Botnet	InfoStealer
Média Brasil	2.5%	5.0%	7.7%	15.2%	1.6%
Média Global	1.2%	5.1%	3.8%	10%	1.7%

Em 2020-2021, as ameaças aos endpoints aumentaram

57% aumento de ataques de ransomware nos últimos 6 meses, em todo o mundo

- Uma nova vítima a cada 10 segundos
- Maze e Ryuk

Descoberto diariamente:

100,000 novos sites maliciosos

10,000 novos arquivos maliciosos

Source: Check Point Research

Ataques de ransomware têm alta na 62% na América Latina

Região foi a que registrou o maior e mais rápido aumento nas tentativas de ataque de ransomware

Da Redação
15/06/2021

Estudo da VMware detalha o aumento de ataques cibernéticos direcionados à força de trabalho remoto

Sexta, 25 Junho 2021 11:47 Crédito de Imagens:Divulgação - Escrito ou enviado por Flavia Rangel Adicionar comentario
SEGS.com.br - Categoria: Info & Ti Imprimir

Top Tecnicas MITRE, Arquivos maliciosos EXE – Ultimos 30 dias

TECNICA	TATICAS RELACIONADAS	IMPACTO BRAZIL	IMPACTO GLOBAL
Execution through API	Execution	62%	54%
System Information Discovery	Discovery	61%	51%
Virtualization / Sandbox Evasion	Defense Evasion, Discovery	60%	50%
File Deletion	Defense Evasion	55%	43%
Data Encrypted	Exfiltration	50%	40%

Cobertura técnica por contexto

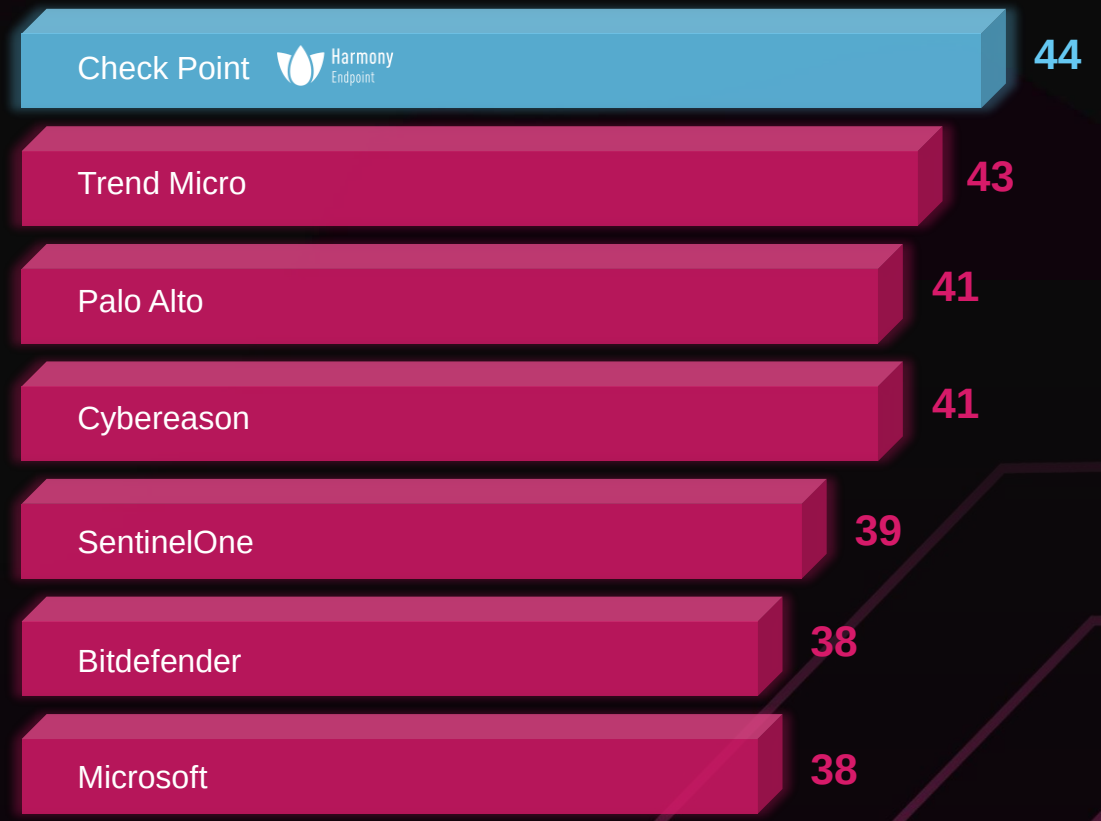
Líderes no top 7

O que foi testado?
A capacidade de fornecer o mais alto nível de contexto (categoria "técnica") para todas as técnicas testadas

Como foi testado?
Nº de técnicas com o nível mais alto de contexto (categoria "técnica")

Realizando
44/46

Harmony Endpoint



SEGURANÇA COMPLETA EM CLIENT UNIFICADO

ENDPOINT

Harmony

Threat Prevention

Anti-Ransomware

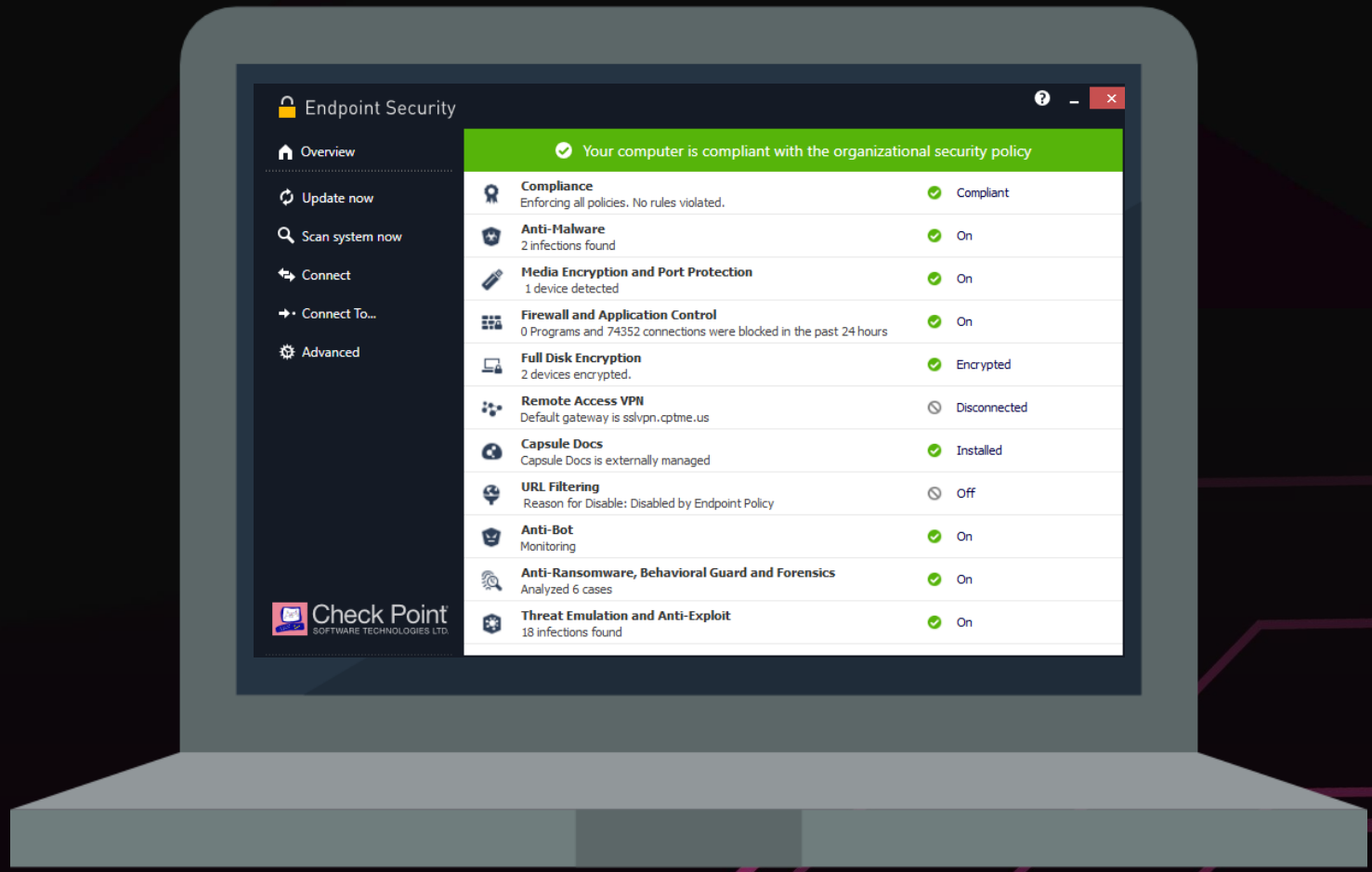
Forensics

Access/Data Security

Access Control

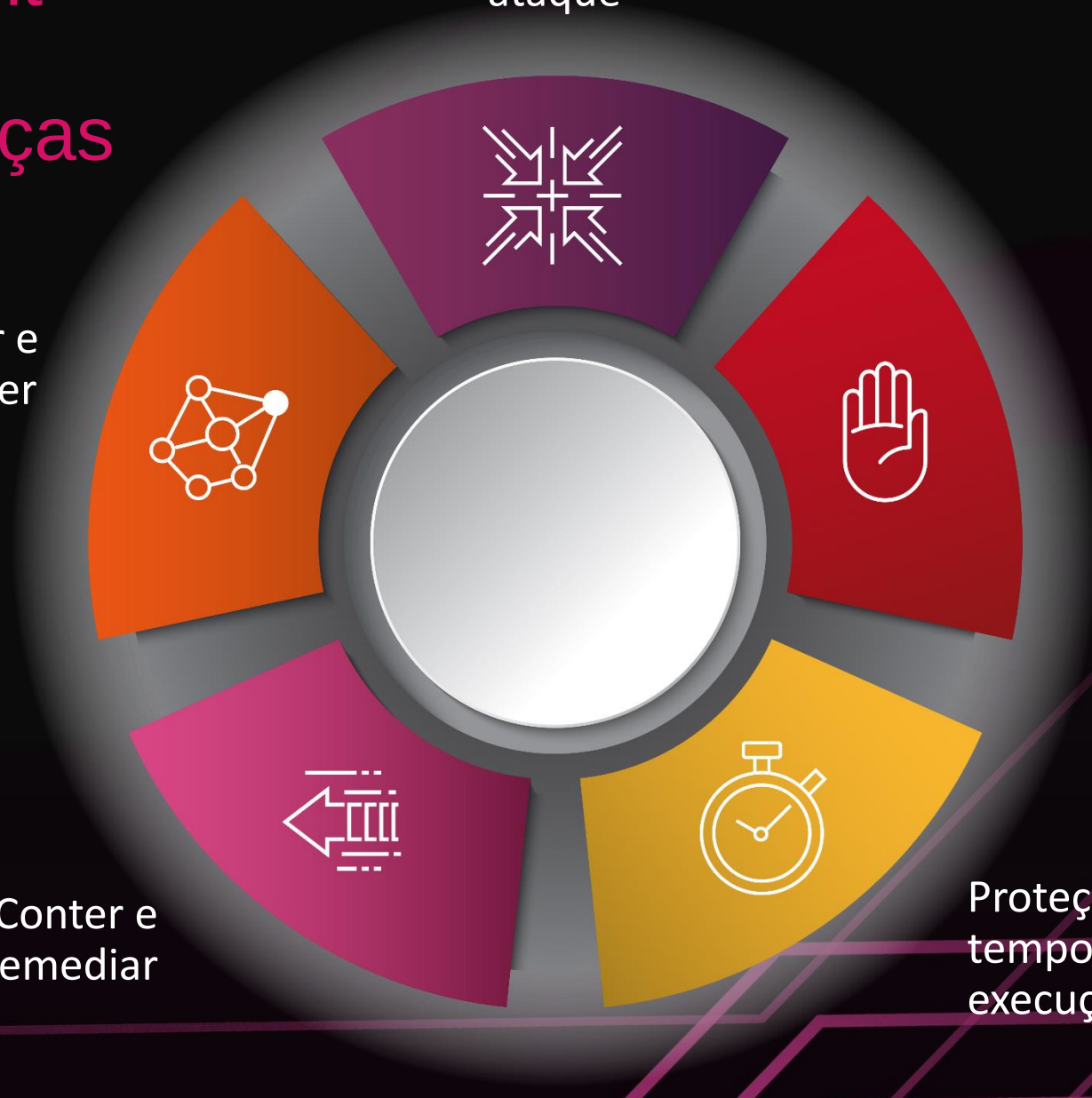
Secure Media

Secure Documents



Segurança do Endpoint

Proteção contra ameaças avançadas



DEFESA ROBUSTA E COMPLETA

ENTENDER & RESPONDER	**ENTENDER**		**RESPONDER**				
	COLETA FORENSE	EVENTOS FORENSES RELATÓRIOS ANALITICOS	IMUNIZAÇÃO CONTRA ATAQUES A SUPERFÍCES	RAPIDA TRIAGEM DE ATAQUES	CAÇA AMEAÇAS		
CONTER & REMEDIAR	**CONTER**			**REMEDIAR**			
	BLOQUEIO DE TRÁFEGO C&C	PREVENÇÃO A MOVIMENTOS LATERAIS	ISOLAMENTO DA MÁQUINA	TERMINAÇÃO DO PROCESSO	QUARENTENA DE ARQUIVO	RECUPERAÇÃO DE ARQUIVOS ENCRIPTADOS	LIMPEZA COMPLETA DO ATAQUE
PROTEÇÃO EM TEMPO DE EXECUÇÃO	ANTI-RANSOMWARE	**COMPORTAMENTAL**					ANTI-BOT
		FAMILIAS DE MALWARE	REGRAS GENERICAS	ML BASEADO EM REGRAS	ANTI-FILELESS	ANTI-EVASÃO	
PREVENIR ANTES DA EXECUÇÃO	**CONHECIDOS**		**DESCONHECIDOS**		**EXPLORAR**	**IDENTIDADE**	
	ANTI-MALWARE	REPUTAÇÃO DE URL	EMULAÇÃO E EXTRAÇÃO	ML BASEADO EM ANALISE ESTATICA	ANTI-EXPLOIT	ANTI-PHISHING	PREVENÇÃO DO REUSO DE CREDENCIAIS
REDUZIR A SUPERFICIE DE ATAQUE	**CONTROLAR**			**ENCRIPTAÇÃO**			**GARANTIR**
	PROTEÇÃO DE PORTAS	CONTROLE DE APLICAÇÃO	FIREWALL DE ENDPOINT	ACCESSO REMOTO VPN	ENCRIPTAÇÃO DE DISCO E MEDIAS	SEGURANÇA DE DOCUMENTOS	ENDPOINT COMPLIANCE

FUNCIONAMENTO DO ANTI-RANSOMWARE

EXECUTANDO

ANALISE COMPORTAMENTAL

Monitora constantemente comportamentos específicos de ransomware

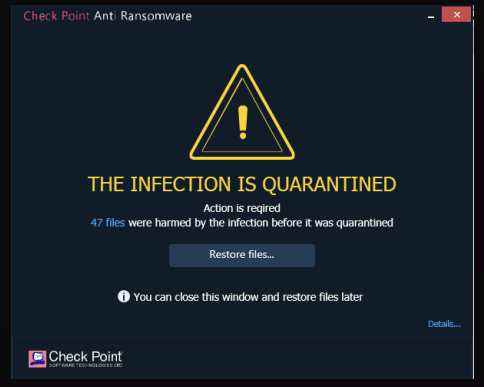
DATA SNAPSHOTS

Continuamente cria backups de curto-prazo de arquivos

APÓS DETECÇÃO

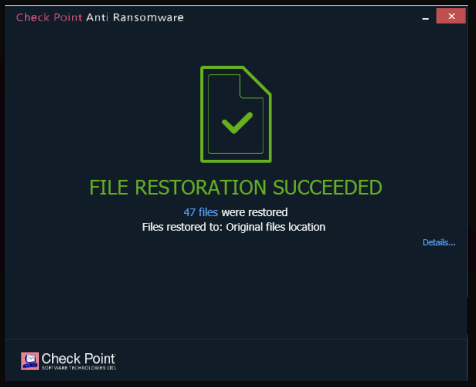
ANÁLISE

Inicia análise forense para analisar detalhes do ataque



QUARENTENA

Para e quarentena todos os elementos do ataque

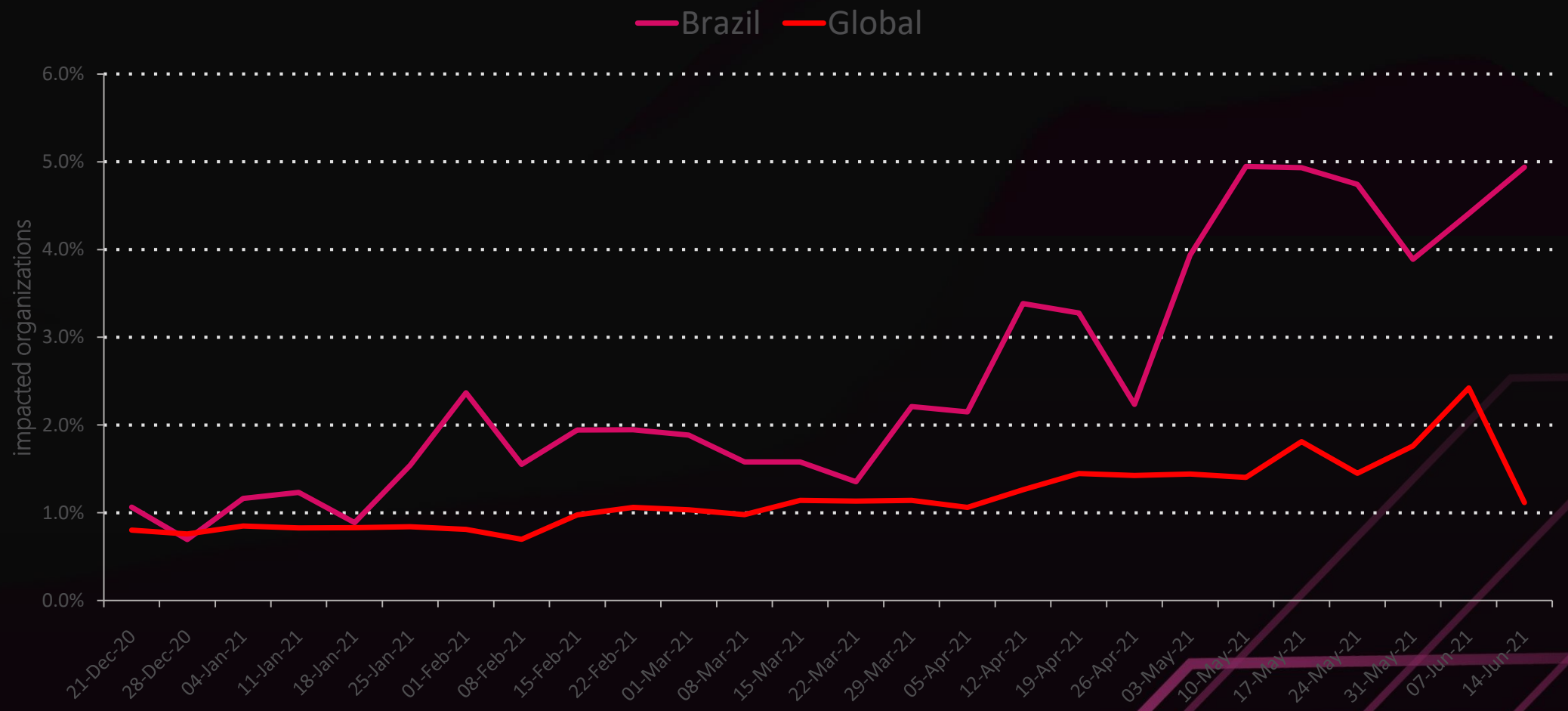


RECUPERA

Recupera arquivos criptografados de snapshots

Demo

Ataques em dispositivos móveis – últimos 6 meses



ALVOS

Interceptação de chamadas (SS7)

Rastreamento da localização

Emails

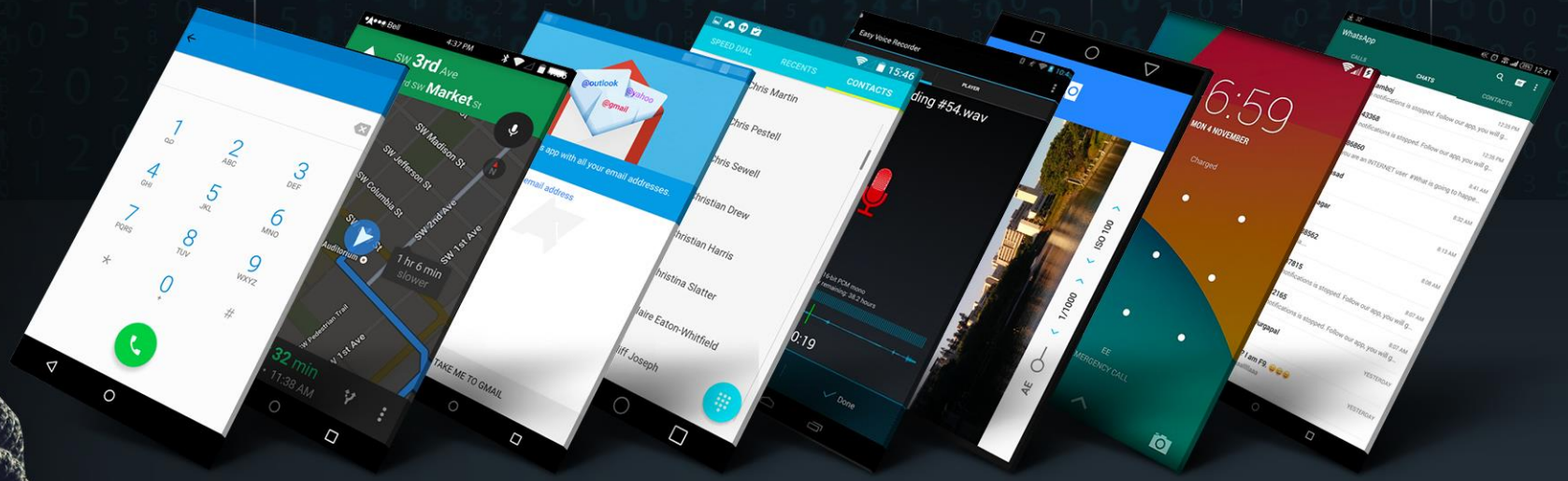
Contatos

Gravação do microfone

Fotos

Credenciais

App de mensagem



DANOS

Espionagem corporativa

Rastreamento de executivos

Spear Phishing

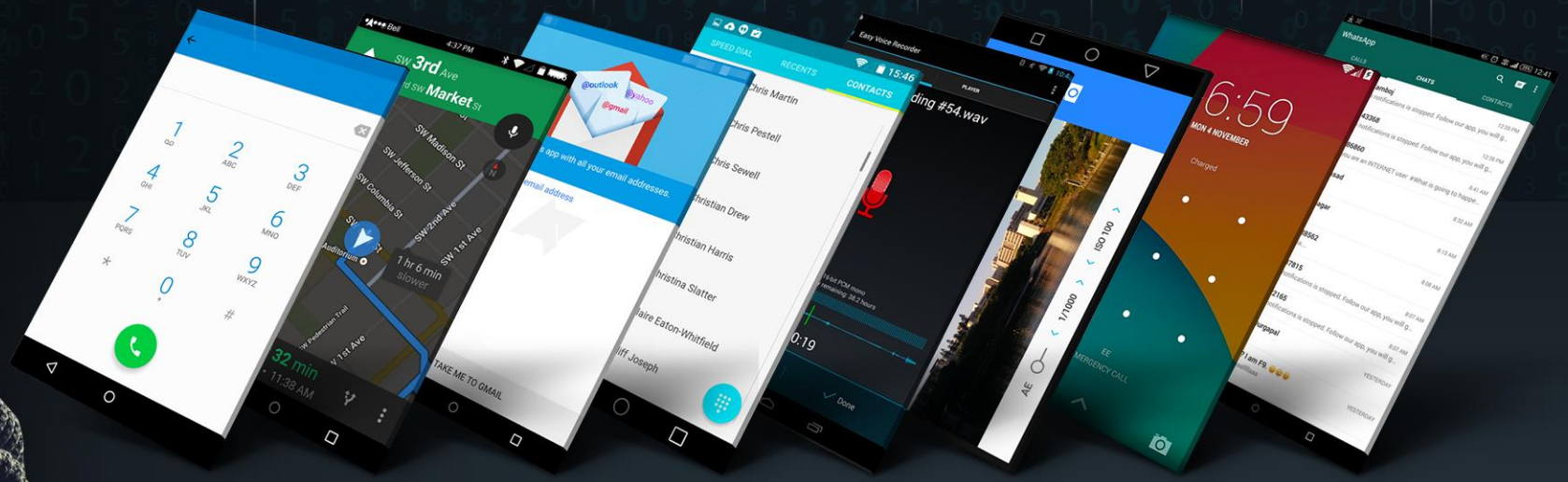
Ataque aos contatos

Escutas em reuniões

Invasão de privacidade

Roubo de contas

Interceptação de mensagens



PRINCIPAIS ATAQUES

pwn2own

40% dos dispositivos Android no mundo afetados

Execução de código Remoto

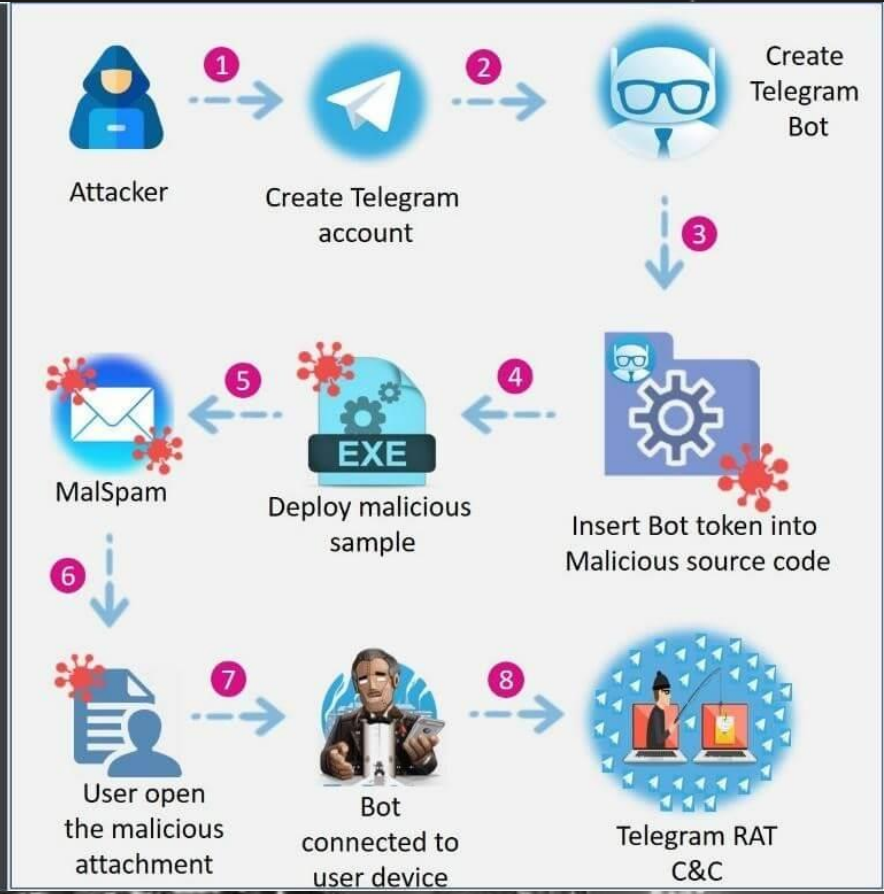
Permite acesso não autorizado à conteúdo de voz e vídeo

PRINCIPAIS ATAQUES

RAT – Trojan de Acesso Remoto via Telegram

ToxicEye

Infection Chain



Harmony Mobile

PREVENÇÃO CONTRA ATAQUES EM DISPOSITIVOS MÓVEIS

VETORES & ATAQUES

Apps

Apps infectados
Malware 0-Day
Apps vulneráveis

Rede

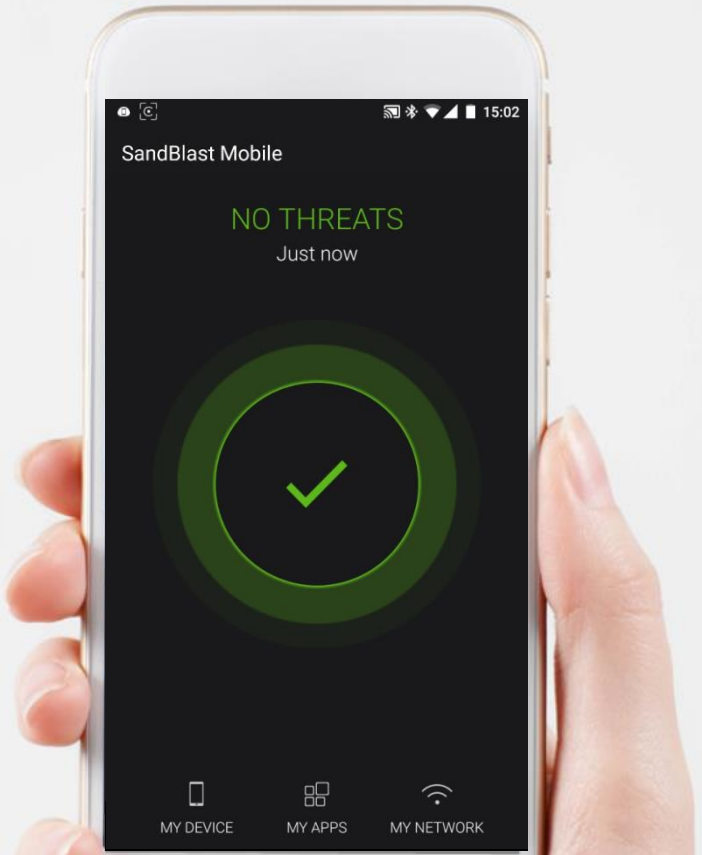
Man-in-the-Middle
URLs de Phishing
Navegação

Dispositivo

Exploits de SO
Configuração insegura
Jailbreak/Rooting

- MALWARE ZERO-DAY
- APPS INFECTADOS
- ATAQUES MitM POR Wi-Fi
- ATAQUES MitM POR CELULAR
- ANTI-PHISHING
- NAVEGAÇÃO SEGURA
- ANTI-BOT
- EXPLOITS DE SO

Harmony
Mobile



Demo

Harmony Mobile

OBRIGADO!

Gustavo Borro – Security Engineer

Henrique Moisés – Securiy Engineer