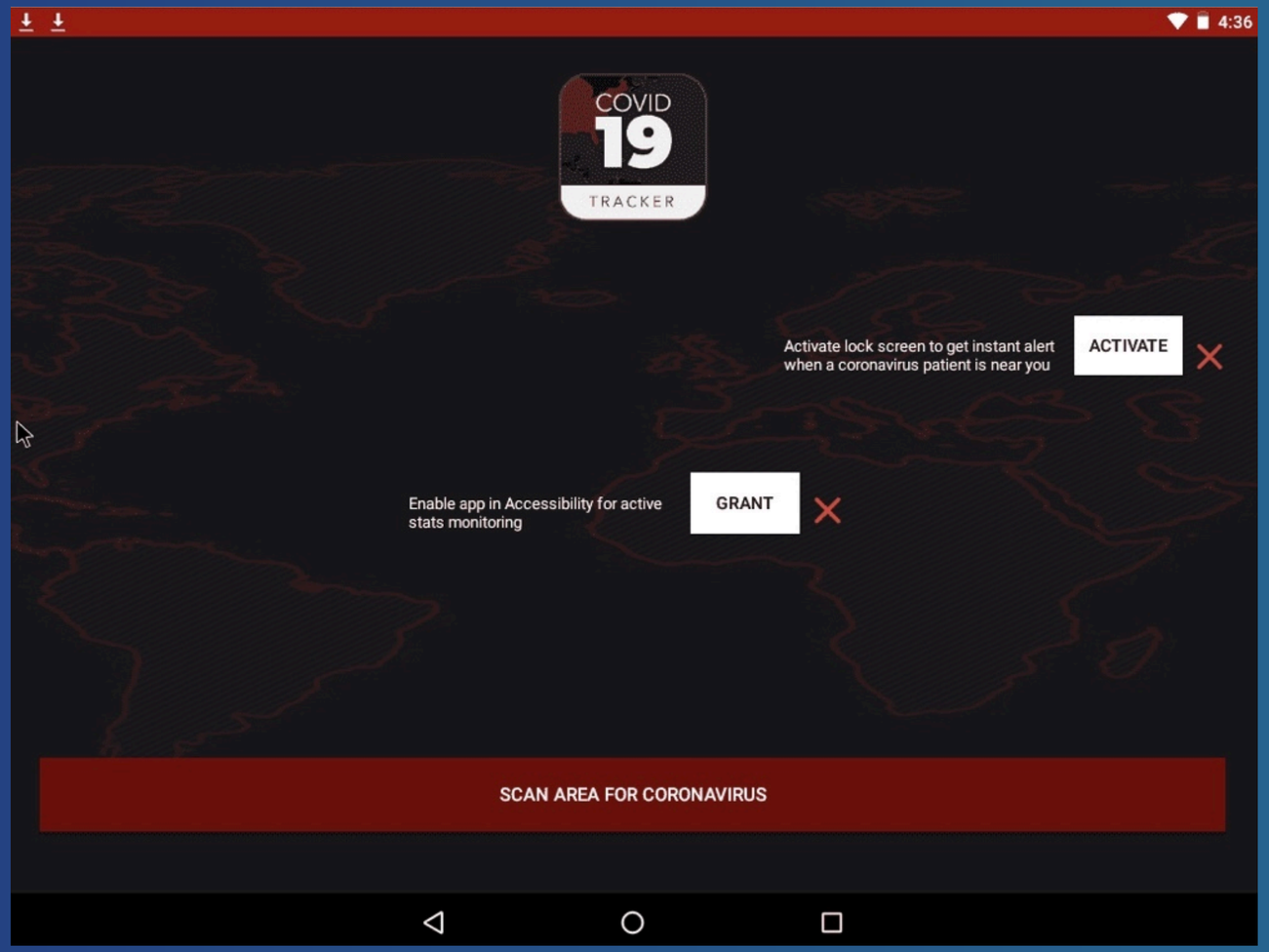
CYBER SEGURANÇA

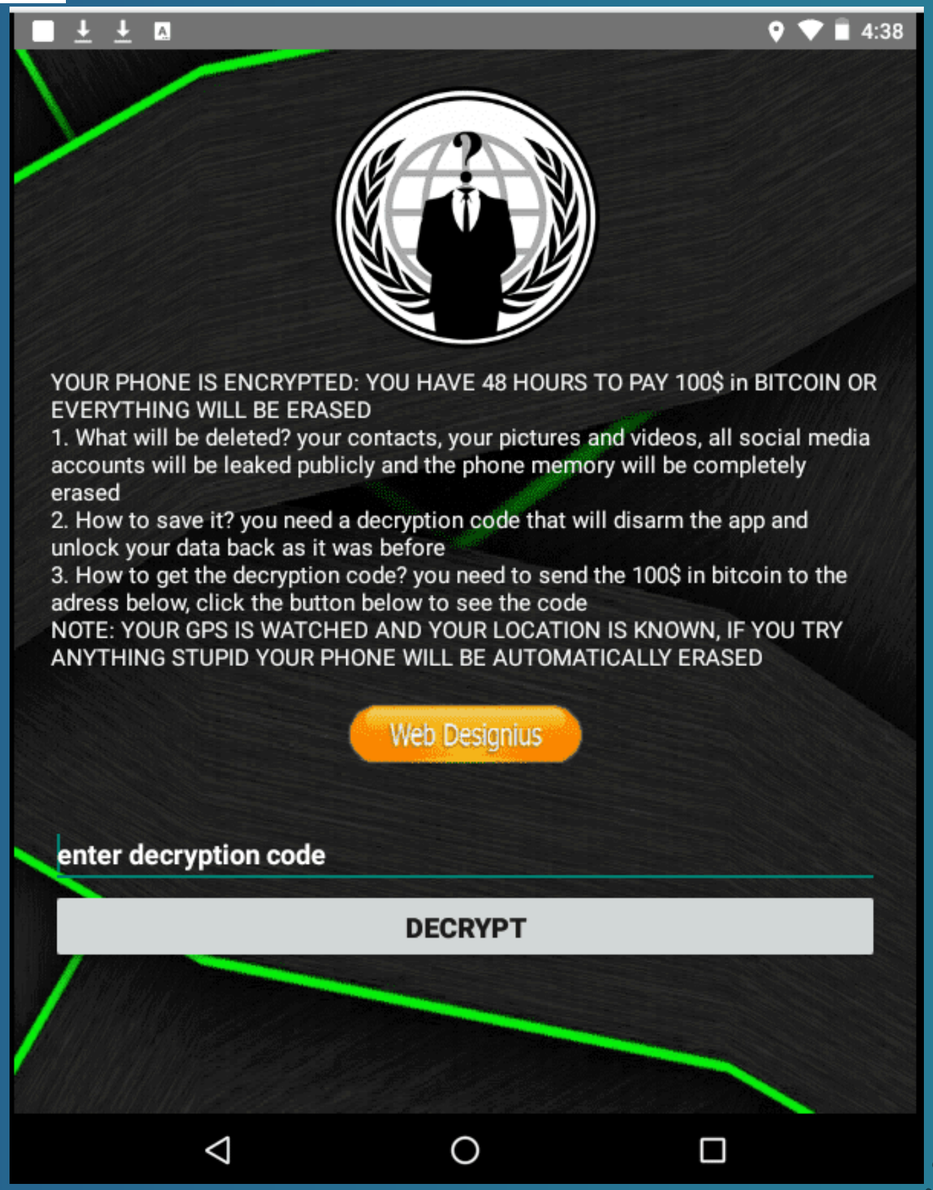
Heloísa Gabrielly Paixão Nº09 2ºano B

Caso 1 - Ransomware CovidLock

- **Quando aconteceu:** Ocorreu em 2020 e foi descoberto empresa de segurança Domain Tools;
- **Como aconteceu:** Apresenta como um aplicativo de rastreamento do coronavírus que oferece estatísticas sobre a pandemia da COVID-19 e um mapa calor que rastreia pontos críticos do surto. Após instalado, para que o usuário possa verificar casos de infecção do coronavírus nas localidades, são solicitadas permissões de acesso e de tela de bloqueio. Após o usuário baixar o aplicativo e conceder as permissões necessárias, o ransomware bloqueia a tela de seu smartphone adicionando uma senha de acesso ao dispositivo. Os criminosos induzem a vítima a pagar US$ 100 em Bitcoin dentro de 48 horas para recuperar o acesso, informando ao usuário que seus contatos, fotos e outros conteúdo serão excluídos e as contas de mídias sociais serão vazadas.

Caso 1 - Ransomware CovidLock





Caso 2 - Botnet Mariposa

- **Descoberta:** 2008, Espanha
- **Número estimado de máquinas infectadas:** Consistia em até 12 milhões de endereços IP exclusivos ou até 1 milhão de computadores zumbis individuais infectados.
- **Impacto:** Foram diversos, em parte porque partes da botnet podiam ser alugadas por terceiros, indivíduos e organizações. As atividades confirmadas incluem ataques de negação de serviço , spam de e-mail , roubo de informações pessoais e alteração dos resultados de pesquisa que um navegador exibiria para mostrar anúncios e pop-ups.
- **Situação atual:** Em 23 de dezembro de 2009, o Grupo de Trabalho Mariposa (forças de segurança espanholas, Defense Tech e Panda Security) conseguiu assumir o controle da Botnet Mariposa.

Caso 3 - Phishing Banco Central do Brasil

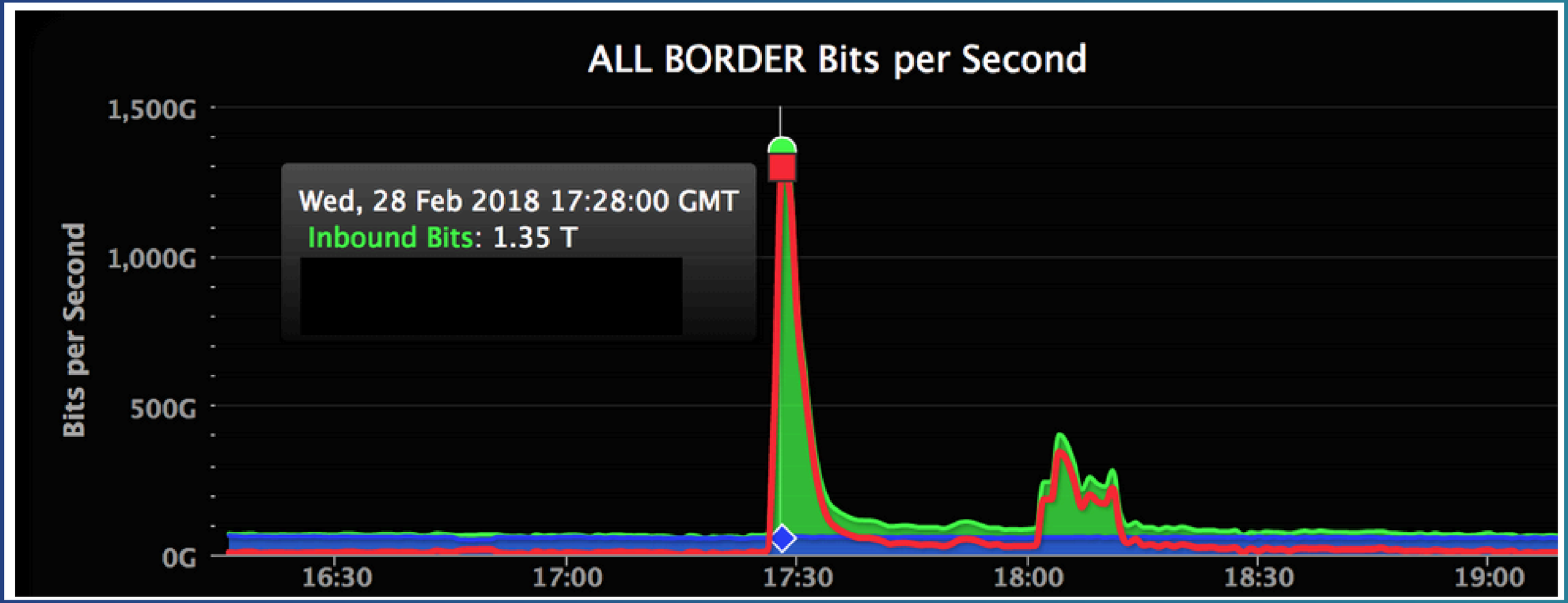
- **Quando aconteceu:** Em 2020, o Banco Central do Brasil foi alvo de ataque de phishing;
- **Como aconteceu:** Os golpistas enviaram e-mails falsos para funcionários do banco, solicitando a atualização de informações de login em um sistema interno. Ao clicarem no link fornecido no e-mail, os funcionários foram direcionados para um site falso que se assemelhava à página de login do sistema interno do banco. Ao inserir suas informações de login, os golpistas conseguiram obter acesso às contas dos funcionários e realizar transferências fraudulentas.
- **Impactos:** Resultou na transferência de cerca de R$ 3 milhões para contas bancárias controladas pelos criminosos.

BANCO CENTRAL DO BRASIL

Caso 4 - DDoS no GitHub

- **Quando aconteceu:** Foi em 2018 e teve como alvo o GitHub.
- **Como aconteceu:** O ataque chegou a atingir 1,3 Tbps, enviando pacotes a uma taxa de 126,9 milhões por segundo. Os invasores aproveitaram o efeito de amplificação de um sistema de armazenamento em cache de banco de dados popular, conhecido como memcached. Ao inundar os servidores do memcached com solicitações falsificadas , os invasores conseguiram amplificar seu ataque cerca de 50 mil vezes.
- **Impactos:** A plataforma estava utilizando um serviço de proteção contra DDoS, que foi alertado automaticamente 10 minutos após o início do ataque. Esse alerta desencadeou o processo de mitigação e o GitHub foi capaz de deter o ataque rapidamente, que durou apenas cerca de 20 minutos.

Caso 4 - DDoS no GitHub



Depois da primeira parte do ataque, que derrubou o site por apenas seis minutos, houve um segundo pico de 400 Gbps.

Caso 5 - Injeção de SQL no Guess.com

- **Quando aconteceu:** Em fevereiro de 2002 por Jeremiah Jacks, que descobriu que o Guess.com era vulnerável a um ataque;
- **Como aconteceu:** Explorou uma falha de injeção de SQL e permitia que qualquer pessoa, por meio de URLs cuidadosamente elaboradas, acessasse informações confidenciais armazenadas no banco de dados do site, incluindo nomes, números de cartões de crédito e datas de validade de mais de 200.000 clientes.
- **Impactos:** A Comissão Federal de Comércio (FTC) resolveu um caso com a fornecedora de roupas e acessórios Guess Inc., no qual a agência acusou a empresa de não tomar medidas apropriadas para proteger seu site, causando danos à reputação da Guess, comprometimento de dados pessoais de milhares de clientes e a obrigação de reforçar segurança.

GUESS

Caso 6 - Zero-day Exploit no Zoom

- **Quando aconteceu:** Ocorreu em julho de 2020 no Zoom.
- **Como aconteceu:** Uma vulnerabilidade foi encontrada na popular plataforma de conferência por vídeo. Envolveu o acesso remoto de hackers a um PC de usuário que estava usando uma versão mais antiga do Windows. Se o alvo fosse um administrador, o hacker poderia assumir completamente a máquina e acessar todos os arquivos.
- **Impactos:** Não houve registros de ataques em larga escala, mas comprometeu a reputação da empresa, levou à desconfiança de instituições e resultou em sanções da FTC (Federal Trade Commission), que exigiu melhorias nas práticas de segurança, forçando a Zoom a adotar criptografia ponta a ponta, auditorias independentes e a rever seu programa de segurança.

zoom

FONTES:

- **Caso 1:** https://seguranca.tic.ufrj.br/alertas/covidlock-malware-para-android-disfarcado-de-aplicativo-que-rastreia-o-coronavirus/ (Acesso em 19/05/2025).
- **Caso 2:** https://www.danysoft.com/pt-pt/os-12-piores-botnets/ (Acesso em 19/05/2025);
  - https://en.wikipedia.org/wiki/Mariposa_botnet (Acesso em 19/05/2025).
- **Caso 3:** https://tisec.com.br/phishing-casos-famosos-da-vida-real/ (Acesso em 19/05/2025)
- **Caso 4:** https://seguranca.tic.ufrj.br/alertas/github-passou-pelo-maior-ataque-ddos-ja-registrado/ (Acesso em 19/05/2025)
  - https://www.cloudflare.com/pt-br/learning/ddos/famous-ddos-attacks/ (Acesso em 19/05/2025)
- **Caso 5:** https://en.wikipedia.org/wiki/SQL_injection (Acesso em 19/05/2025)
  - https://www.computerworld.com/article/1723568/ftc-settles-with-guess-on-web-vulnerabilities.html (19/05/2025)
- **Caso 6:** https://www.kaspersky.com.br/resource-center/definitions/zero-day-exploit (Acesso em 19/05/2025)
  - https://cloudsecurityalliance.org/blog/2022/03/13/an-analysis-of-the-2020-zoom-breach (Aceso em 19/05/2025)