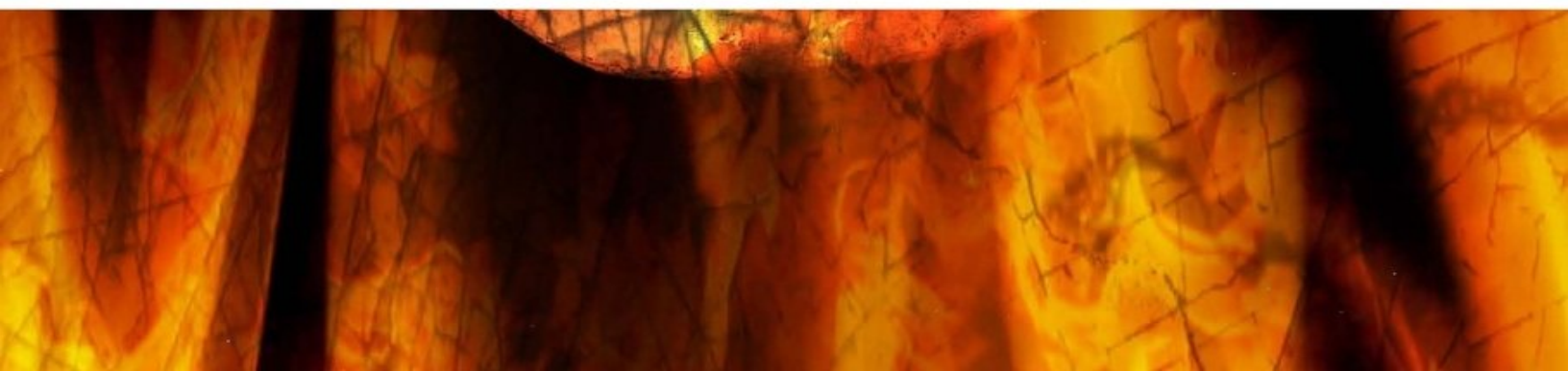




APOC@LYPSE: O FIM DO ANTIVIRUS

RODRIGO RUIZ, ROGÉRIO WINTER,
KIL PARK, FERNANDO AMATTE



Resumo de Apoc@lypse: O Fim Do AntiVirus

Quais os perigos e as opções para um mundo digital sem proteção, onde os seus escudos podem prejudicar você e o seu negócio? "Apoc@lypse o fim do antivírus" é o resultado do trabalho de 4 pesquisadores que apresenta a descoberta da primeira doença cibernética auto imune.

O que nos humanos seria equivalente ao Lupus por exemplo. Virou notícia no olhardigital do UOL, ComputerWorld, Cyber Defense Magazine, Cyber Security Review, IDG, Techmundo... A comparação dos recursos computacionais com o corpo humano nos remete ao sistema imunológico equivalente aos antivírus.

Em busca do DNA, da essência de todos os antivírus criamos uma técnica de testes de antivírus que chamamos de Apoc@lypse que mostrou após 3 anos de pesquisa que todos os antivírus possuem a mesma origem e trazem consigo uma deficiência genética dos primeiros antivírus.

Conseguimos implantar o DNA inofensivos de alguns vírus de computador em arquivos sem afetar a sua funcionalidade. Com isso os antivírus passam a combater e destruir arquivos que não representam nenhum risco.

Exatamente o que acontece em uma doença auto imune quando o sistema imunológico humano passa a atacar o próprio organismo. Nossa pesquisa indica uma falha grave do conceito de identificação de malwares (vírus, trojan, cavalo de Troia...) por assinaturas aplicado nos antivírus a quase 30 anos.

Todos os antivírus possuem um núcleo comum, um DNA primário como mostra a metáfora que escolhemos para simplificar o entendimento do público. Apesar do nome chamativo, a pesquisa promove uma renovação e chama toda a indústria de antivírus a repensar seus conceitos, evoluir e apresentar a todos nós, produtos melhores e mais seguros.

O CTI foi parceiro na divulgação da pesquisa para os entes públicos interessados convidando gestores de TI civis e militares do governo para uma palestra dia 19 passado no auditorio do CTI-Renato Archer que deu a oportunidade aos servidores públicos conhecerem o conteúdo dessa pesquisa e discutir conosco as implicações dessa vulnerabilidade.

Apoc@lypse é um vírus? NAO, Apoc@lypse é uma técnica que comprova um erro no conceito de assinaturas, que tem sido a base dos antivírus desde a sua criação até hoje.

O Apoc@lypse destrói os arquivos? NAO, quem destrói os arquivos é o próprio antivírus. O Apoc@lypse tem cura? Ainda estamos pesquisando, e demandará estudos para apresentar uma correção. Quantos antivírus são afetados?

Cerca de 150 a 180 em todo o mundo. Ilustrações de Isabela Ganzert Ruiz Sobre os autores: Rodrigo Ruiz é formado em Comércio Exterior além de Técnico em Processamento de Dados e atua na área de TI desde 1992.

Sua formação ocorreu nos softwares ERP, de programador e gerenciador de banco de dados chegou a coordenador de implantação de software na maior empresa de software da América Latina e empresário do ramo de ERP hoje é servidor público federal no CTI - Centro de Tecnologia da Informação Renato Archer e membro da SDIWC(The Society of Digital Information and Wireless Communications).

Descobriu a vulnerabilidade Apoc@lypse e como utilizar uma bactéria digital para transportar e inocular o DNA de vírus em sistemas computacionais sendo o primeiro a relatar a existência de uma doença cibernética autoimune, criou as provas de conceito, escreveu as bases deste livro e fez sua revisão.

Outras pesquisas e trabalhos publicados você pode encontrar no perfil do Researchgate.net: www.researchgate.net/profile/Rodrigo_Ruiz3 Rogério Winter e Tenente Coronel do Exército Brasileiro"

[Acesse aqui a versão completa deste livro](#)