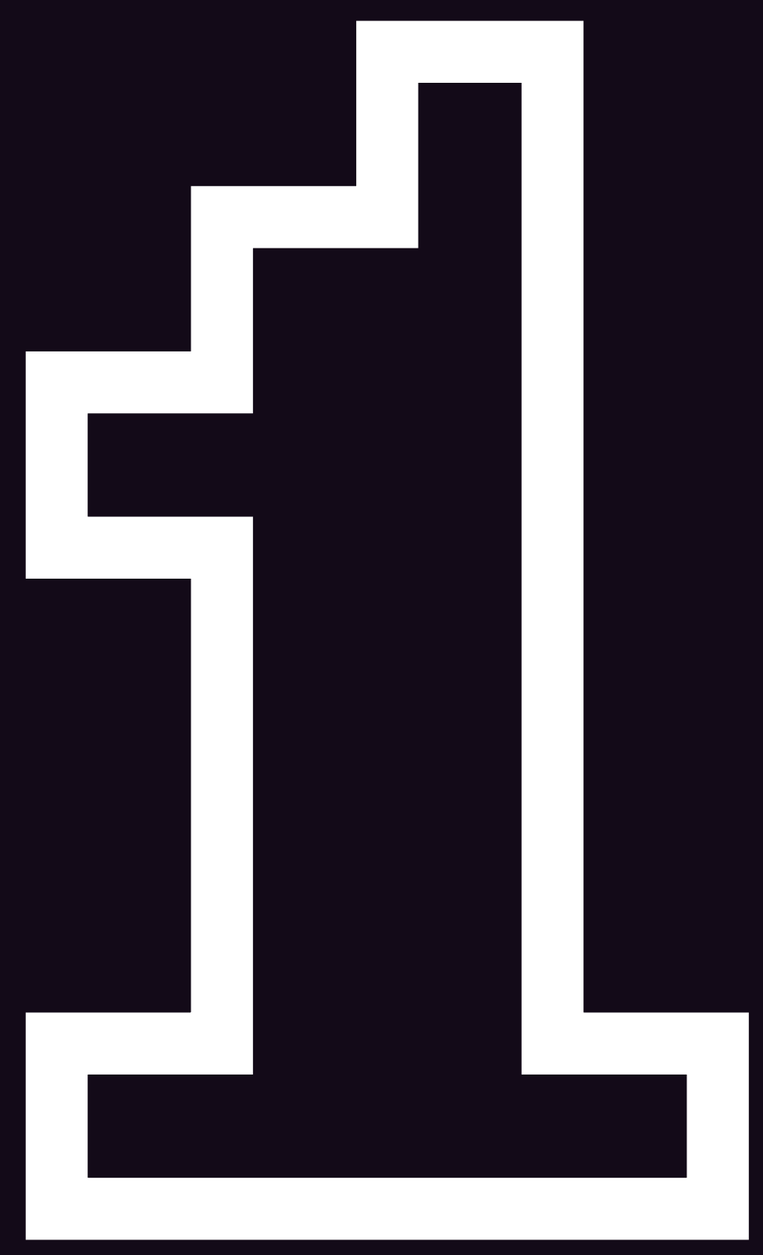
I LOVE YOU

MENTIRAS E MALWARE

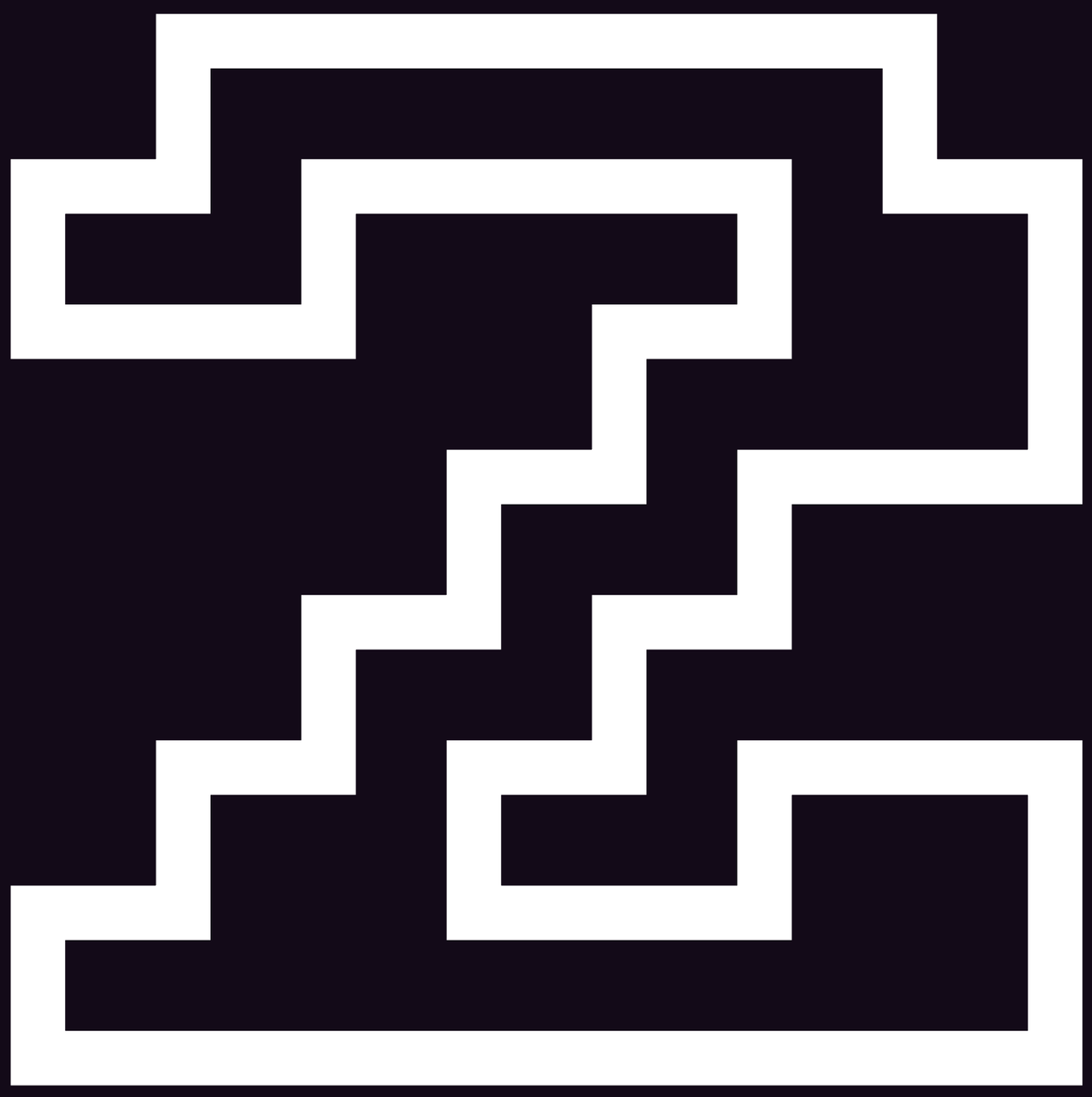


CONTEXTO

CONTEXTO

O malware pode ser definido como um software malicioso com a intenção de explorar algum dispositivo, rede ou serviços. Embora hoje sejamos capazes de reconhecer diversos tipos (como vírus, trojans, spywares ou ransomwares), nos anos 2000 a internet como conhecemos vivia seu amanhecer.

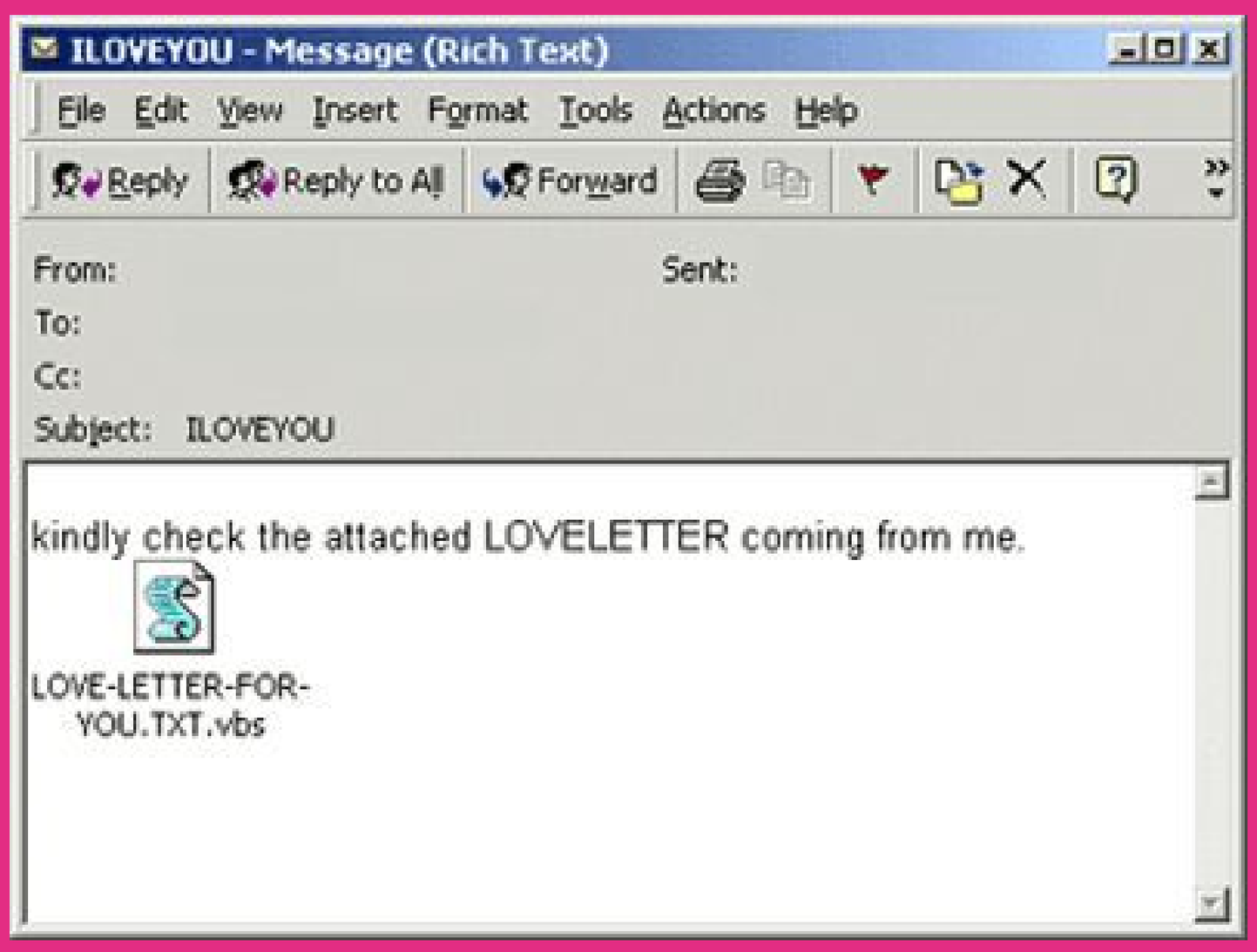
O acesso à rede se tornava cada vez mais popular e a combinação de e-mails, disquetes e falta de conhecimento sobre segurança nesse novo mundo era o solo perfeitamente fértil para ataques. Apesar da existência de programas antivírus, eles também tinham muitas limitações.

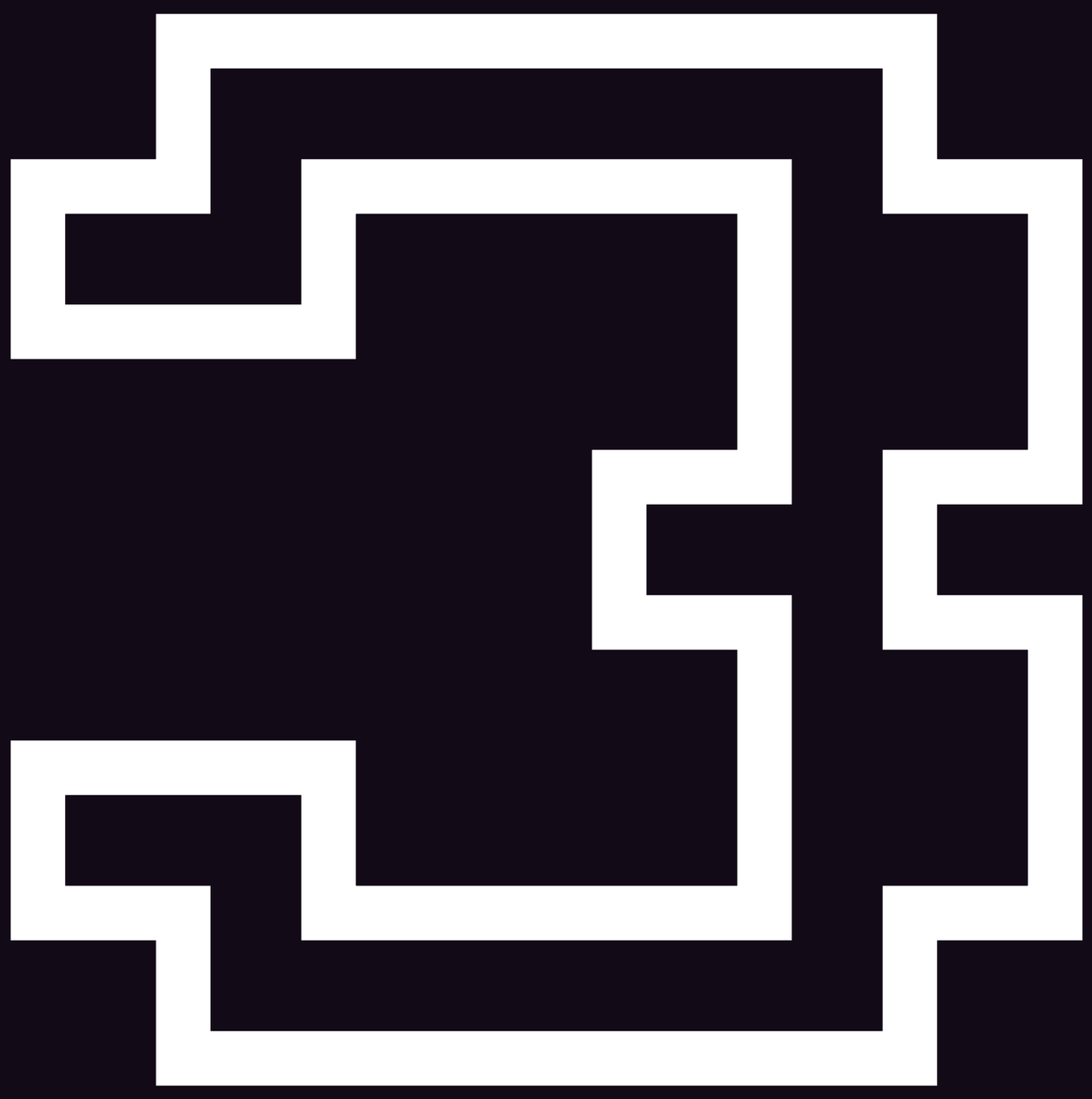


O VIRUS

LOVE-LETTER FOR-YOU.TXT

Imagine você, sentado à frente do seu computador no início do novo milênio. Você espera pela internet discada conectar, abre seu e-mail e se depara com uma mensagem de um dos seus amigos. O anexo? Era um arquivo chamado “LOVE-LETTER-FOR-YOU.TXT”. Quem não clicaria em algo assim?





COMO FUNCIONAVA?

E COMO FUNCIONAVA?

O que muita gente não sabia era que o worm se aproveitava de uma vulnerabilidade do Windows: o sistema não exibia o nome completo de um arquivo longo. Assim, o “VBS” que era a real extensão, acabava sendo omitido.

Ao clicar na suposta carta de amor, o código malicioso era executado, excluía ou corrompia os arquivos e então automaticamente se espalhava através da lista de contatos da vítima. Algumas variantes, LoveBug ou Barok, ainda conseguiam enviar uma cópia das senhas armazenadas dos afetados de volta ao criador.

CRIADOR

O CRIADOR

As autoridades começaram a rastrear o fluxo de dados, acabando por achar uma indicação de que o local de nascimento do vírus teria sido as Filipinas.Vários sinais apontavam que o vírus tenha sido criado por amadores: por exemplo, os servidores não aguentaram a quantidade de dados que recebia e acabou caindo.

“Um bocado de crianças experimentando com diversos tipos de vírus de computador”, foi como o repórter investigativo Geoff White descreveu os responsáveis. Os rastros levaram a um grupo de estudantes em Manila, uma cidade onde ainda não haviam leis que tratavam de crimes cibernéticos.

O CRIADOR

Com a pressão da mídia, um jovem chamado Onel de Guzman ficou sob o holofote. Onel teria apresentado, como projeto de tese, uma proposta para um app que roubava senhas de acesso à internet para uso gratuito que foi rejeitado por ser considerado antiético. Ele acreditava que internet era um direito básico.

Geoff afirma que hoje em dia o rapaz, que nunca foi processado por ausência de legislações, conserta telefones em um mercado nas Filipinas.

“Mas esse era o cerne da questão. Ele queria informação, queria informação de graça. Queria o que todo mundo tinha.” — Geoff White sobre Guzman.

OS RESULTADOS

OS RESULTADOS

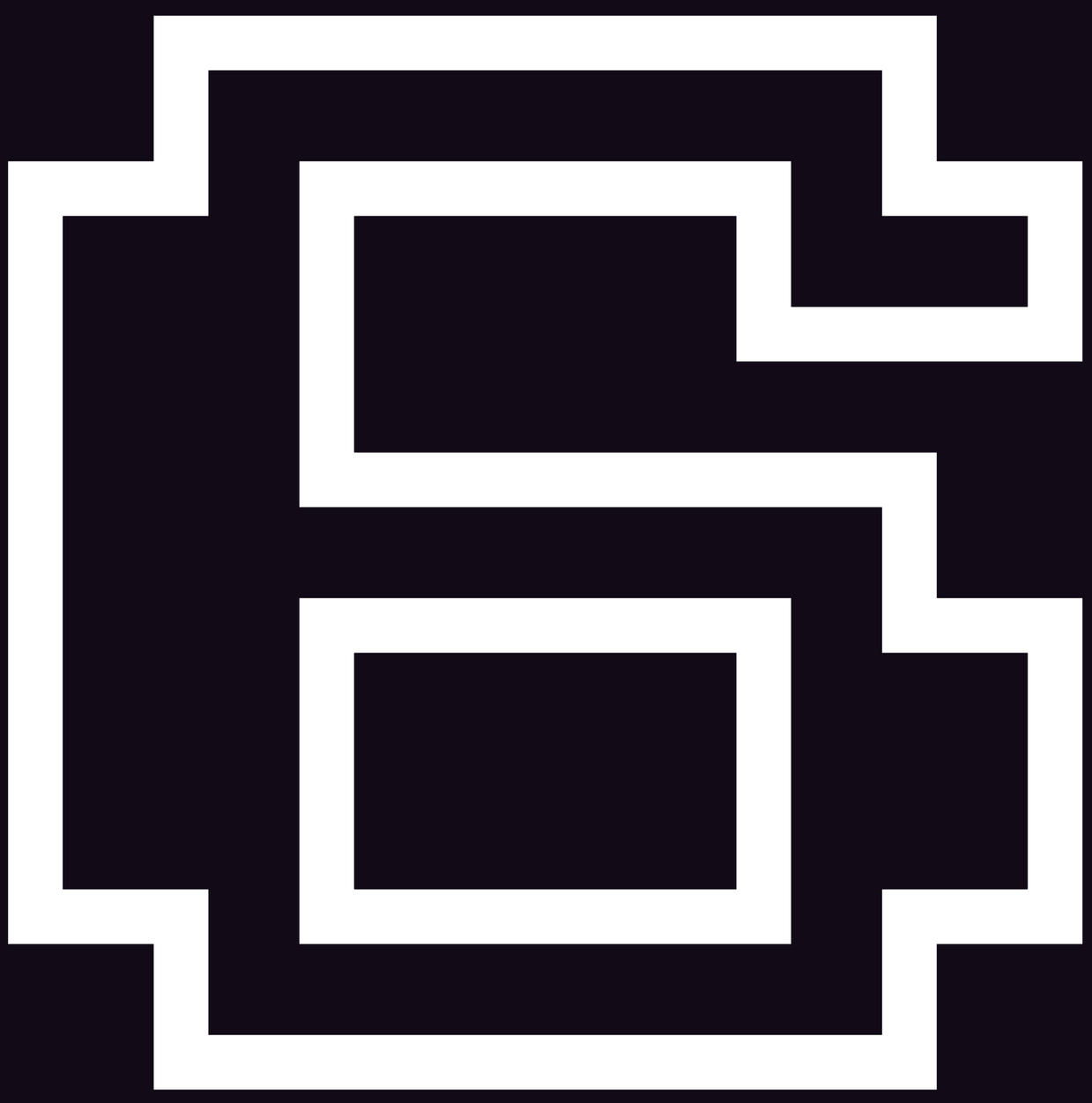
A repercussão não poderia ser menos que catastrófica. Logo no seu primeiro dia de “vida”, em 4 de maio de 2000, o worm já havia infectado milhares de computadores. Cinco dias depois, o número já havia subido para dois milhões e meio. Estima-se que cerca de 10% dos computadores conectados à internet no mundo tenham sido infectados, o que resultou em prejuízos globais avaliados entre 5,5 e 10 bilhões de dólares.

RP ‘love bug’ wreaks $1-B havoc on world’s computers

A REPERCUSSÃO

O vírus chegou a afetar empresas, governos e até instituições militares. Acredita-se que nem mesmo as redes do Pentágono e do Parlamento Britânico tenham saído ilesas da “epidemia”, o que teria forçado o desligamento de sistemas como medida de contenção. A cobertura da mídia, como era de se esperar, foi massiva e acendeu um alerta mundial sobre segurança digital.

Somente em 8 de junho, mais de um mês após o ataque, a Microsoft lançou um patch que introduziu os novos critérios de segurança no Outlook. Entre eles, o bloqueio automático de anexos considerados perigosos e restrições a programas que tentassem acessar a lista de contatos ou enviar emails. A demora só demonstra a complexidade em lidar com ameaças digitais em uma era que ainda não entendia os perigos.

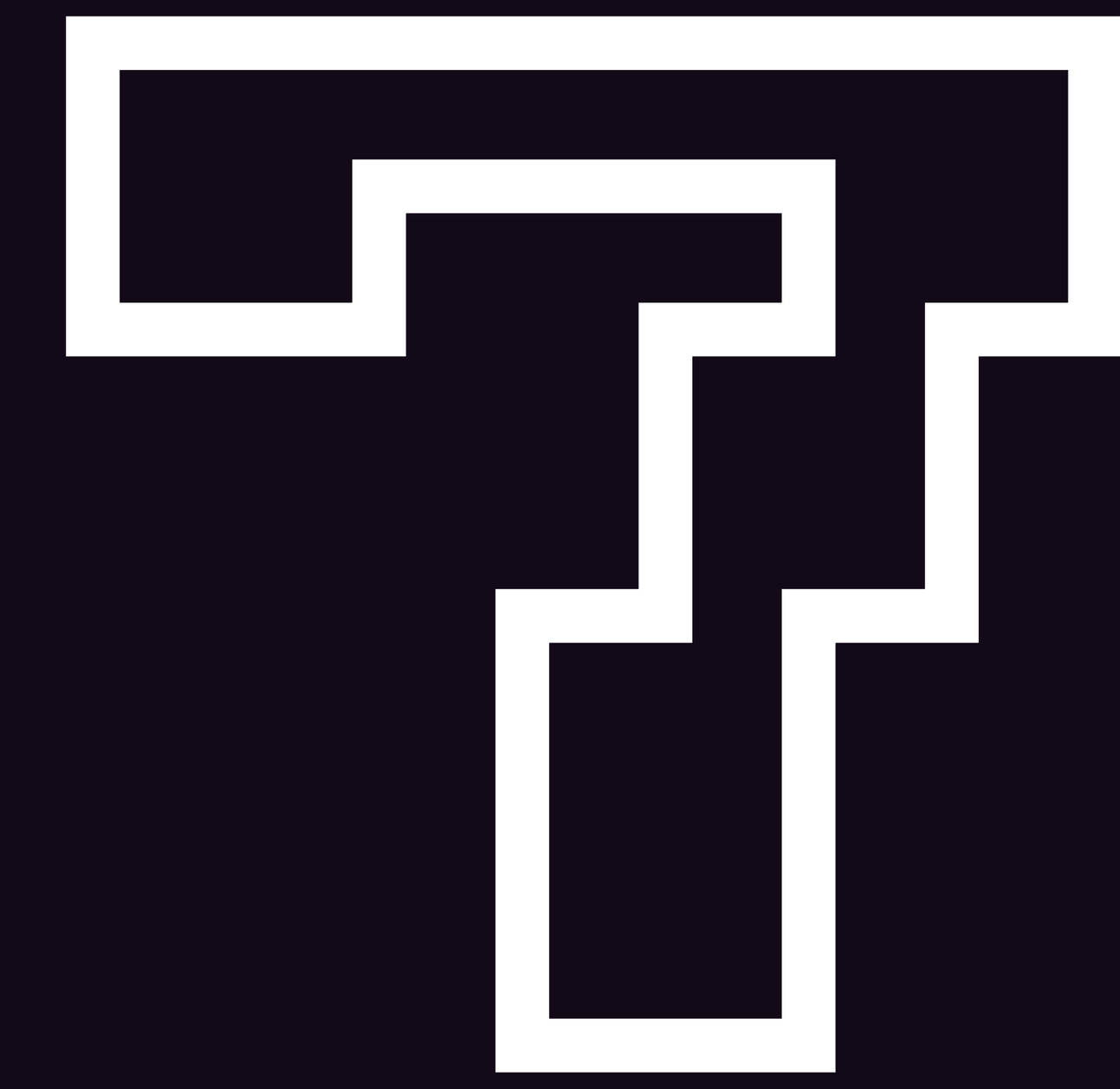


APRENDIZADO

AS LIÇÕES

Sendo um divisor de águas para o mundo da segurança digital, ILOVEYOU foi o que fez as pessoas, empresas e entidades governamentais abrirem os olhos para ameaças virtuais. Uma simples linha de código, por mais amadora que seja, se aliada à curiosidade humana pode causar prejuízos bilionários em horas.

A necessidade de leis contra crimes cibernéticos se tornou ainda mais clara, já que Onel de Guzman ficou impune pela ausência de regras contra esse tipo de crime. Empresas começaram a investir em filtros de spam e bloqueadores de anexos. Houve também uma grande conscientização por parte dos usuários sobre anexos suspeitos ou links desconhecidos.



ENCERRAMENTO

CONCLUSÃO

Foi uma experiência incrível juntar meu interesse quase compulsivo com *rabbit holes* e segurança cibernética a esse projeto. Definitivamente é algo que pretendo continuar a fazer.

Fontes (clique no artigo para ir ao site):

‘ILOVEYOU’: How a computer science student created one of the first email viruses that spread by preying on human nature

ILOVEYOU: o vírus que amou a todos

Meu LinkedIn

Meu Git