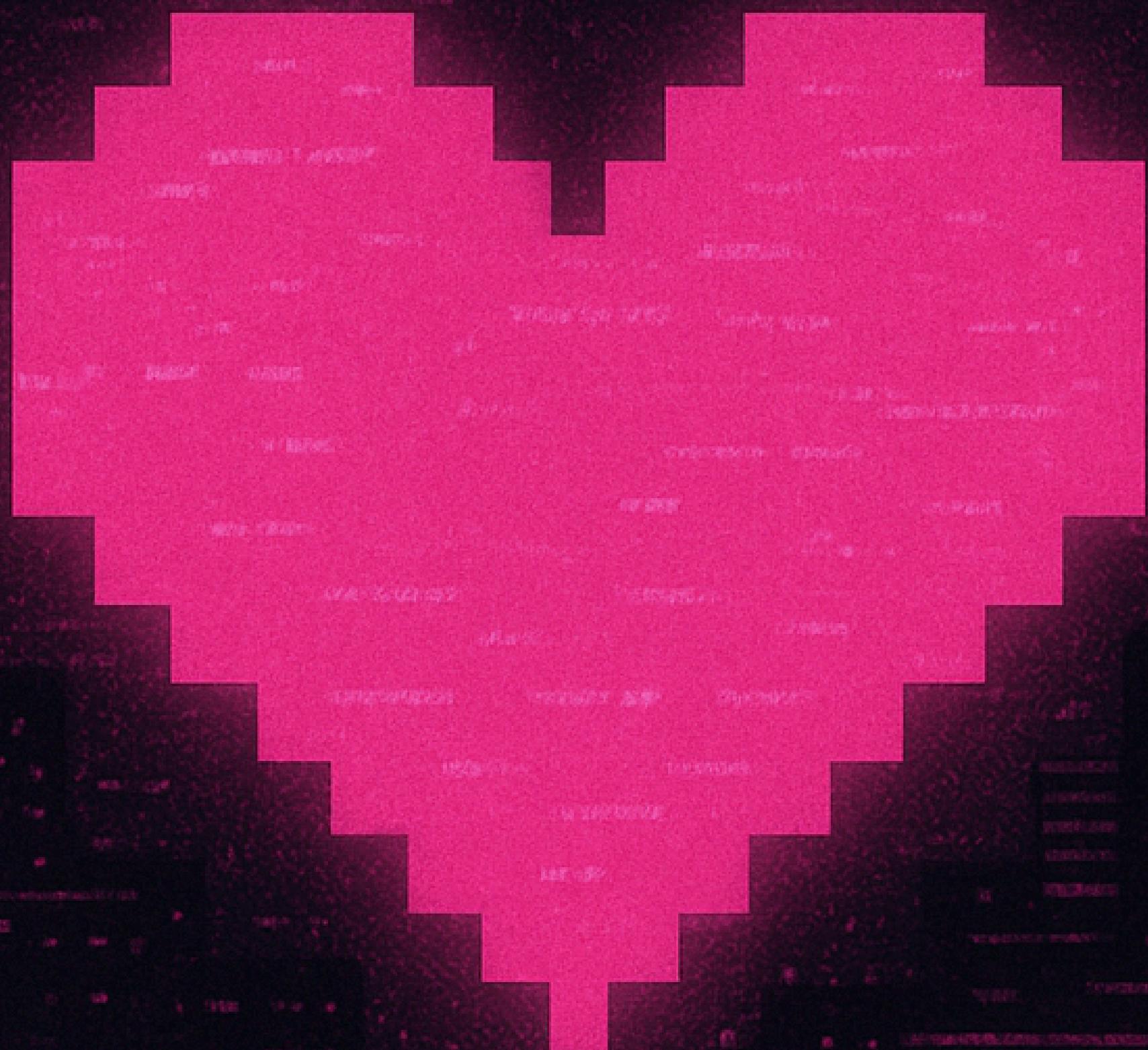
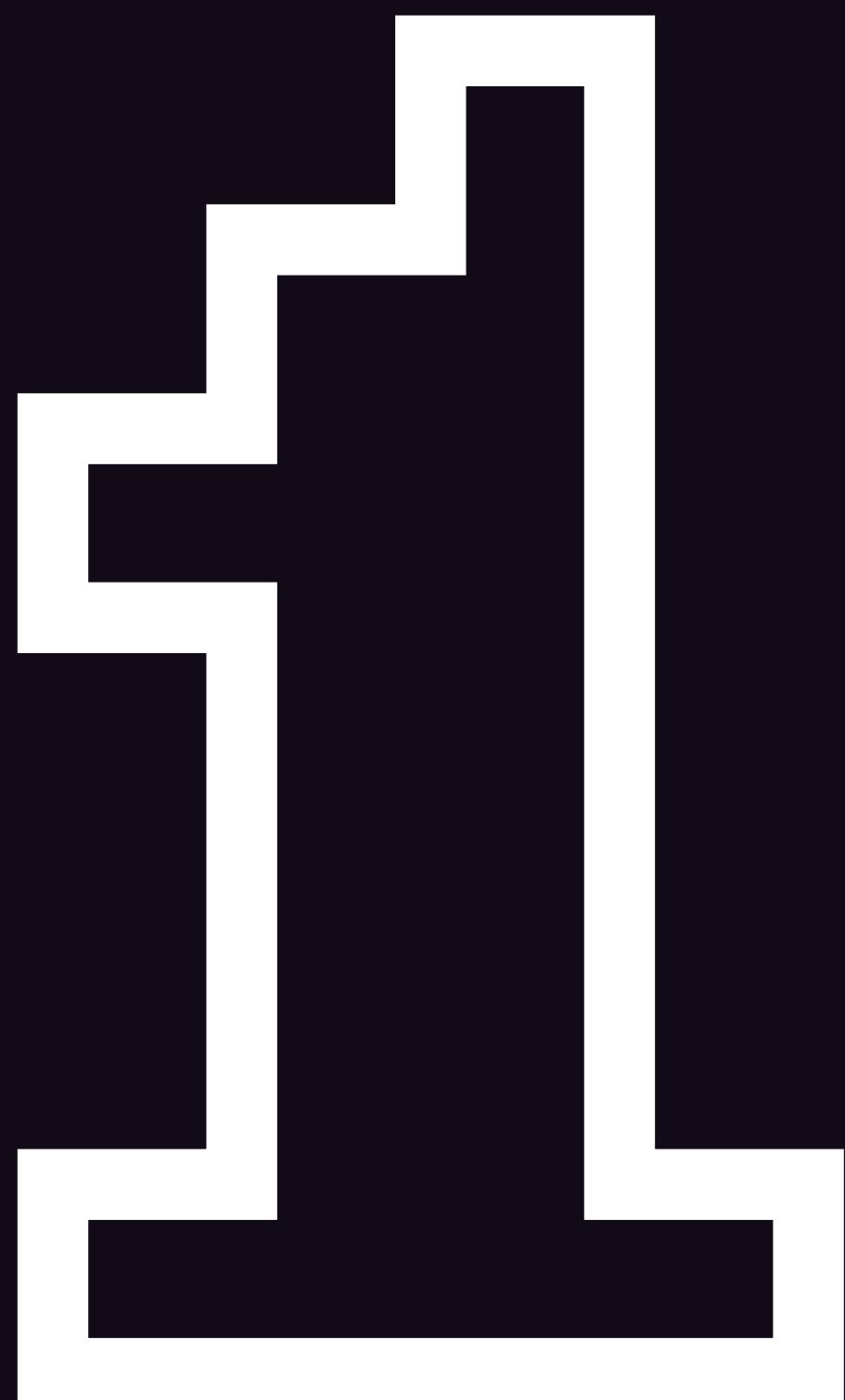


I LOVE YOU



MENTIRAS E MALWARE

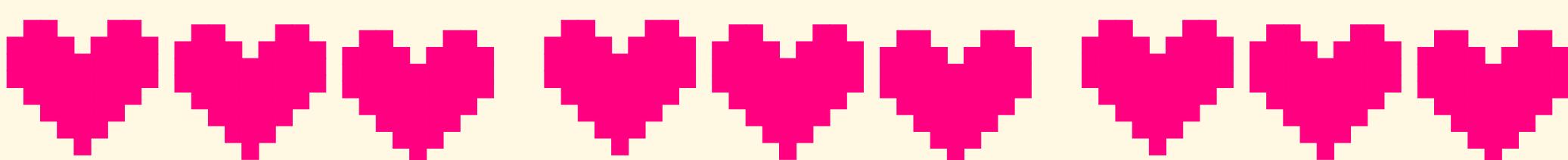


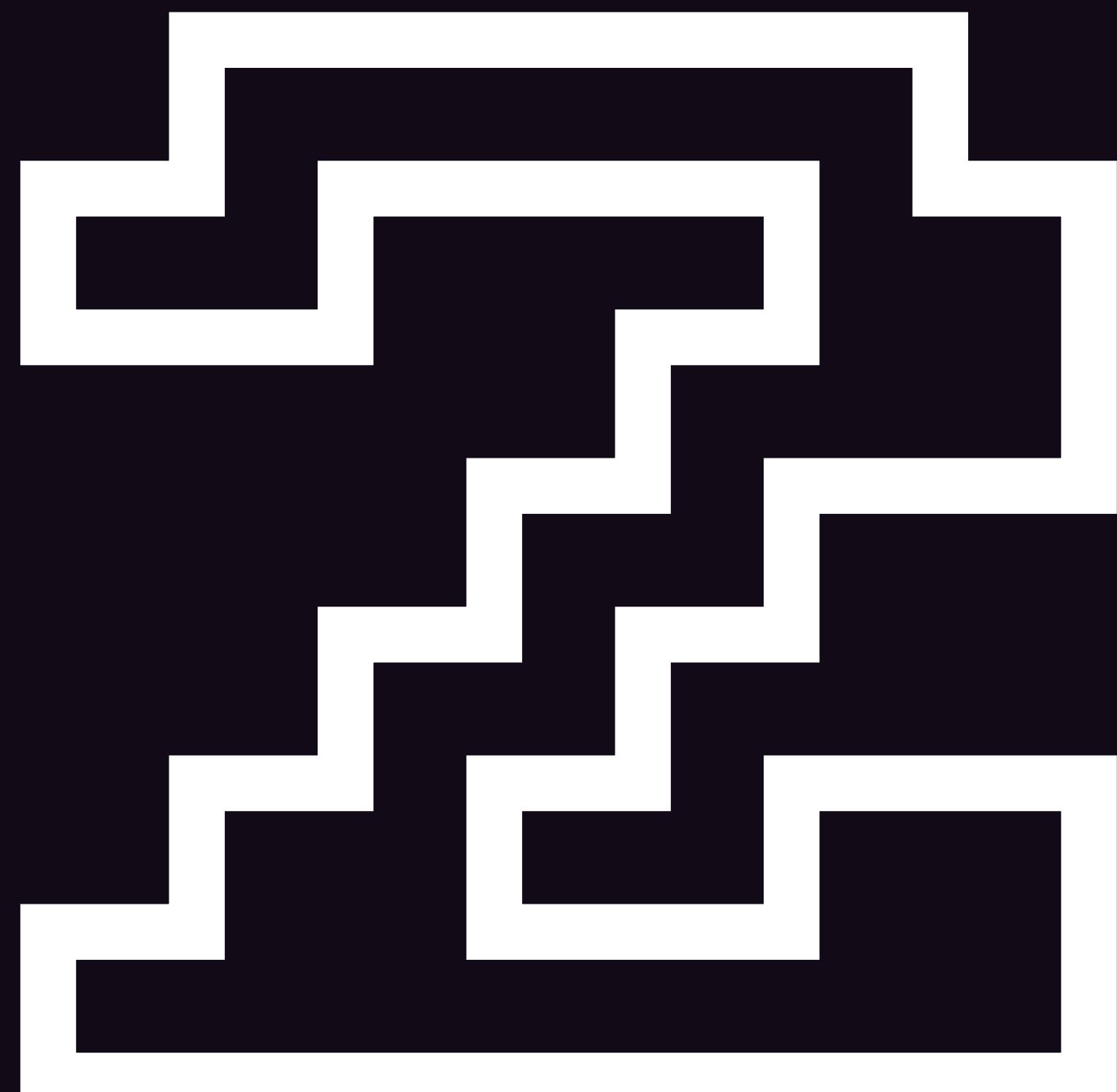
CONTEXTO

# ◆ CONTEXTO

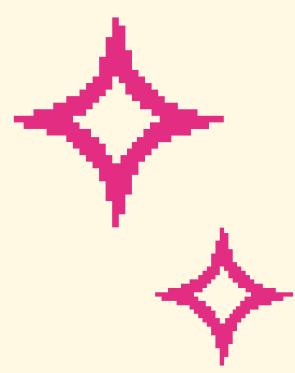
O malware pode ser definido como um software malicioso com a intenção de explorar algum dispositivo, rede ou serviços. Embora hoje sejamos capazes de reconhecer diversos tipos (como vírus, trojans, spywares ou ransomwares), nos anos 2000 a internet como conhecemos vivia seu amanhecer.

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.



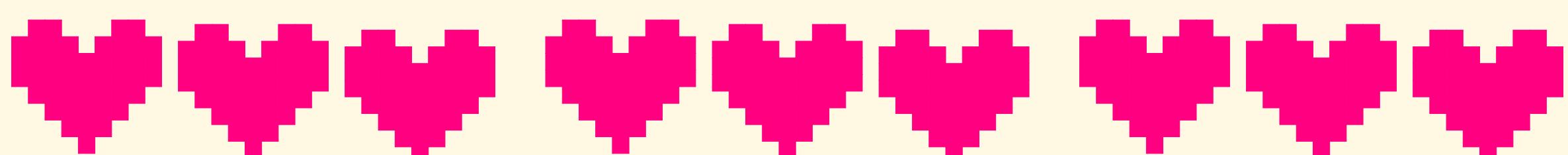
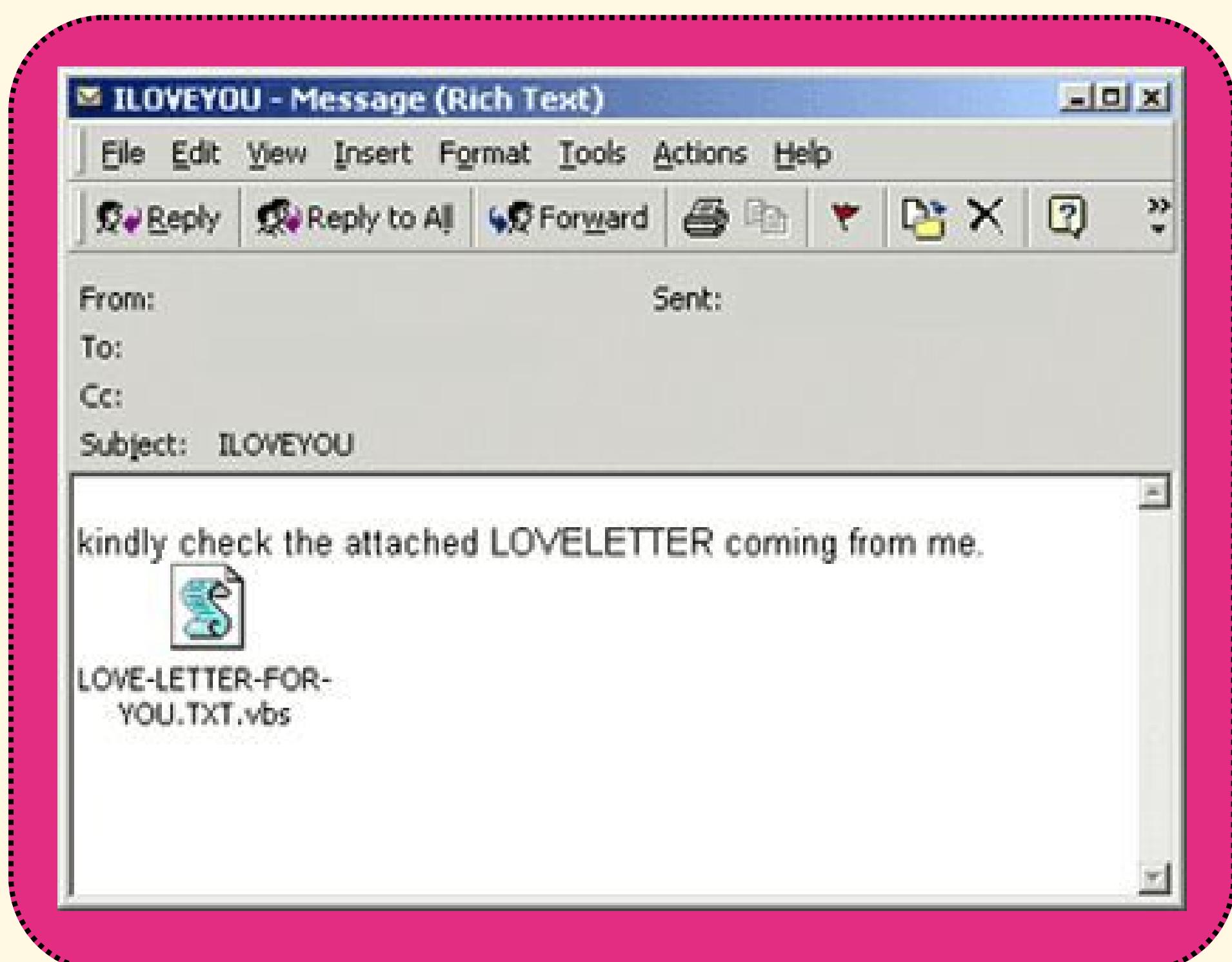


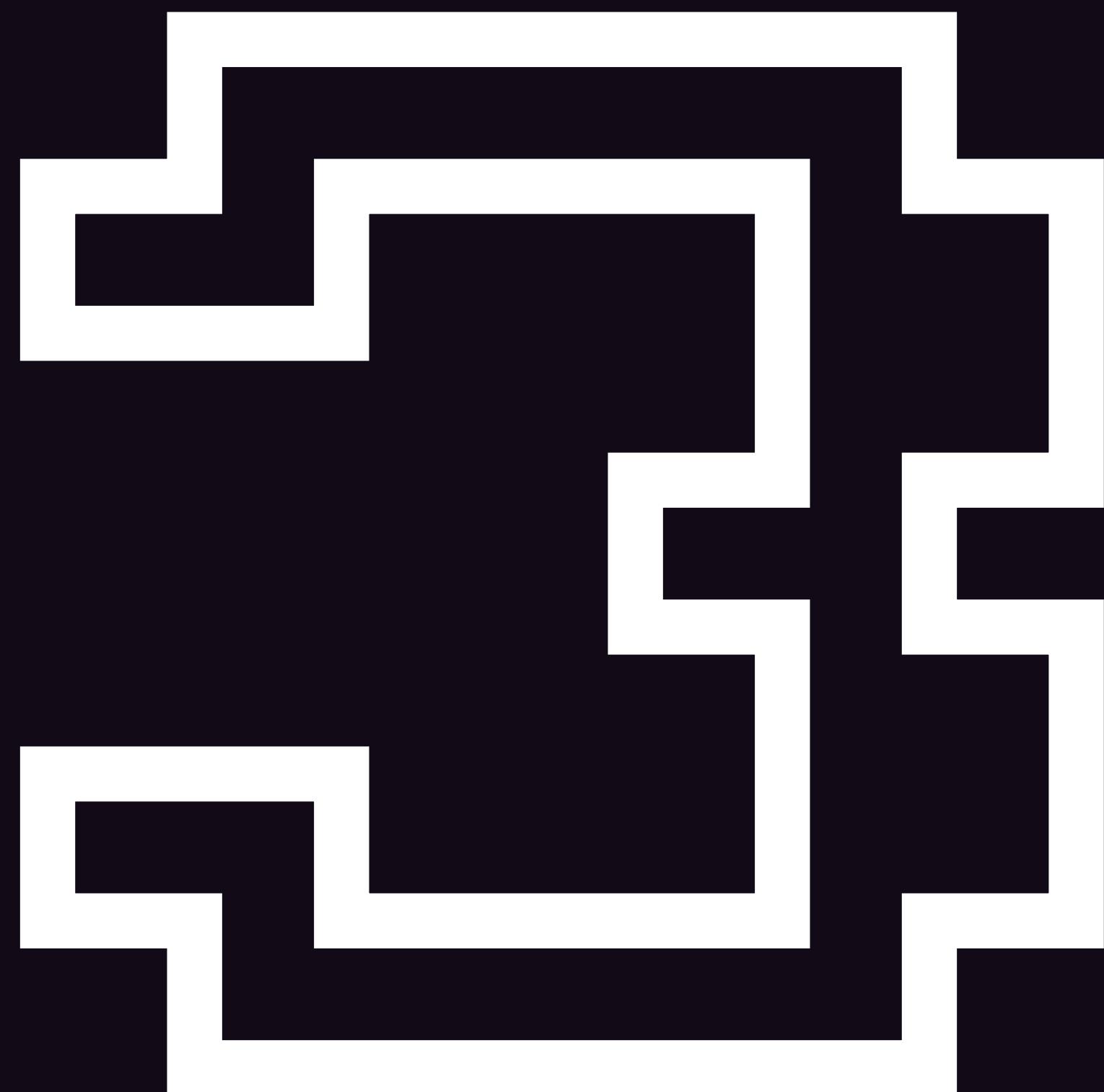
O vírus



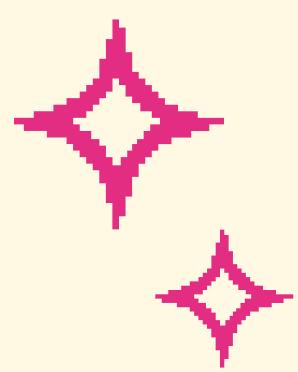
# LOVE-LETTER-FOR-YOU.TXT

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?





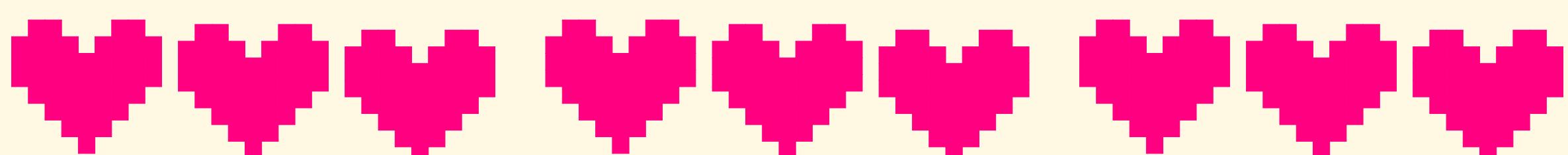
COMO FUNCIONAVA?

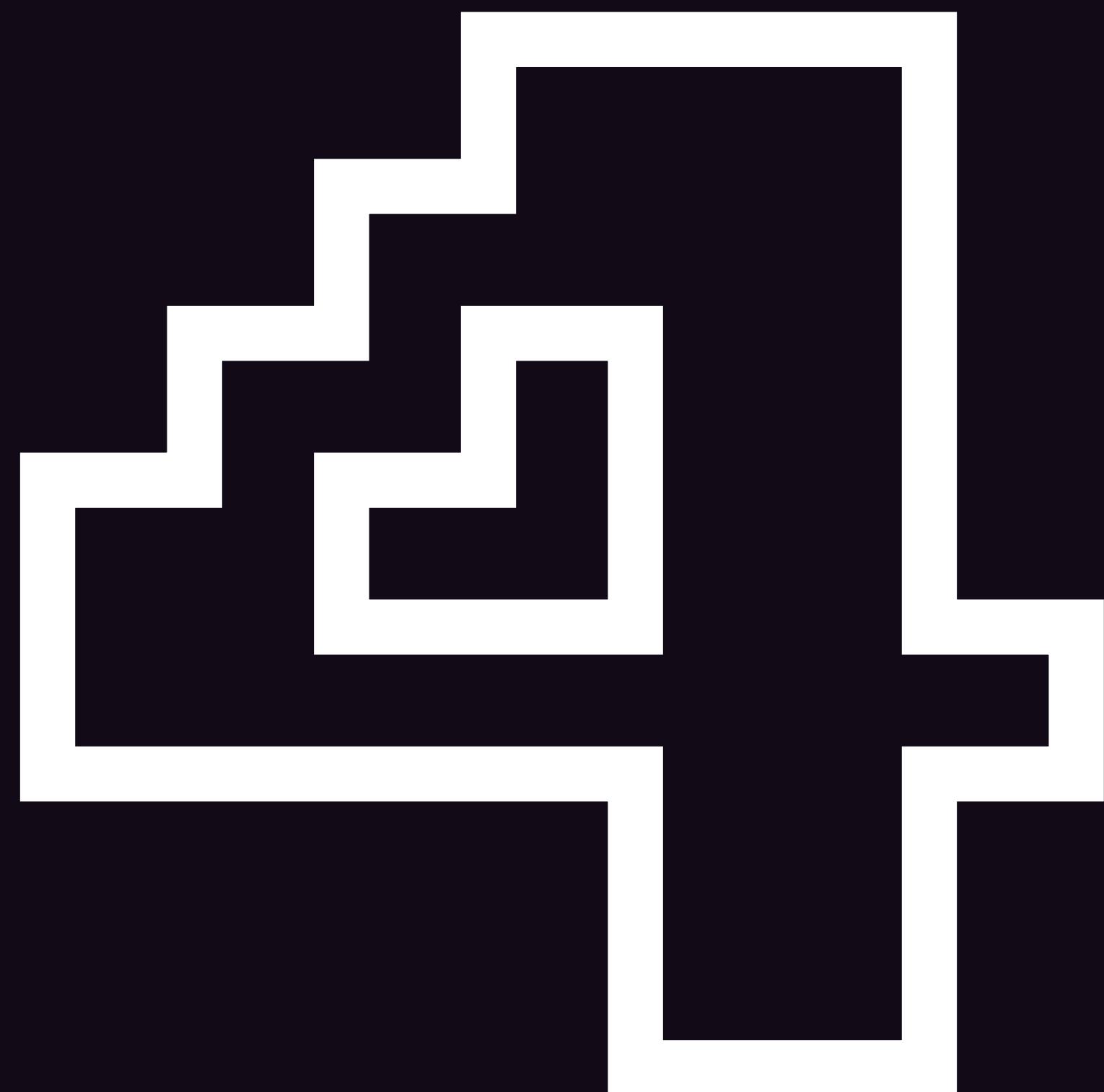


## E COMO FUNCIONAVA?

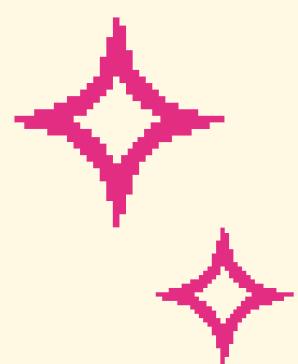
O que muita gente não sabia era que o worm se aproveitava de uma vulnerabilidade do Windows: o sistema não exibia o nome completo de um arquivo longo. Assim, o “VBS” que era a real extensão, acabava sendo omitido.

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.





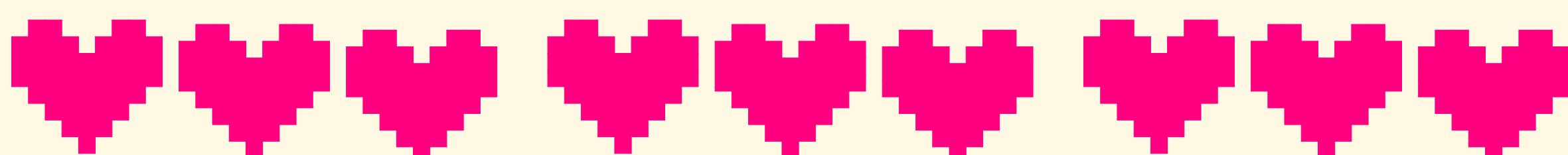
CRIADOR



## 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.



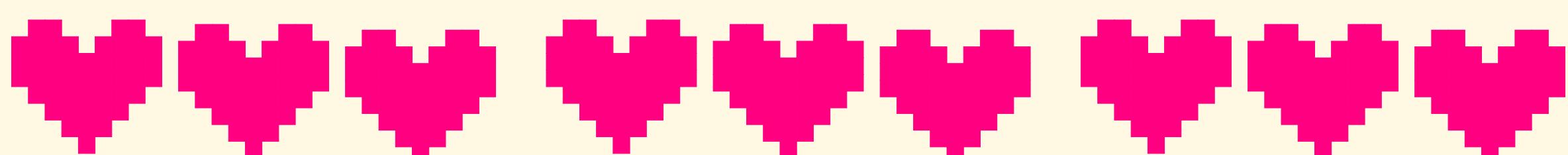


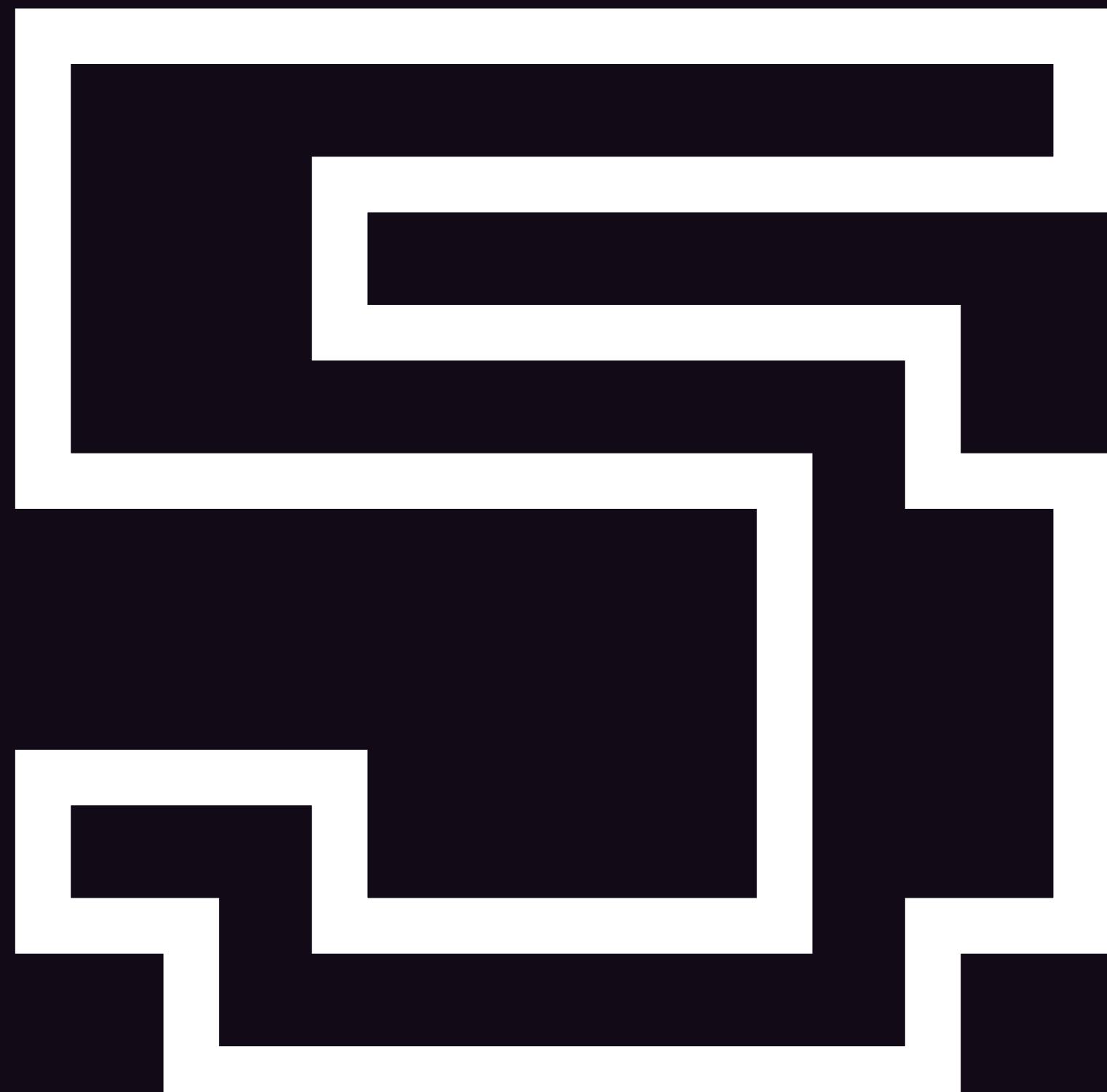
## O CRIADOR

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.

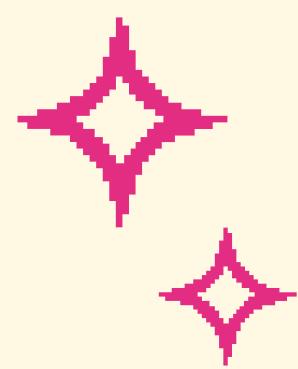
Geoff afirma que hoje em dia o rapaz, que nunca foi processado por ausência de legislações, conserta telefones em um mercado nas Filipinas.

“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

By Tomoaki Ueda

The computer virus known as a “malicious” “trojan” and “Worm” was first released about two weeks ago.

“Good Monday,” an Internet security firm and trading company in Tokyo and its office based in Seoul, Korea, originally claimed Friday that the worm was first released about three weeks ago, infecting about 1.5 million computers worldwide.

The FBI launched an inquiry into the origin of the computer bug, the agency's National Laboratories Technical Division confirmed Tuesday in a communiqué, warning of “new variants” of the virus.

Computer experts “Sugoi Tomy” and “Tomo,” working at Good Monday's office, also issued a statement.

**U.S. surveillance**

Analysts believe the United States and its allies, with more than 2.5 billion computers, may be infected,

according to Tomo.

In the United States, some 300,000 personal computers between 150,000 in Asia, 100,000 in South America, 20,000 in Australia and 10,000 in Africa, according to Good Monday, have reportedly been infected by the worm, spreading to Mexico.

The virus first appeared on “LOVE BUG” in early morning yesterday, according to Good Monday, and was spreading rapidly, according to “LOVE-LETTER-FOR-YOU.”

The worm contains a “trojan” virus that causes the user’s address book of each infected computer to automatically download information from other infected computers.

It can damage or corrupt files of various types of files, including videos, audio and word files, as well as encrypting them as a malicious effect, known as “Malware” and “Cryptography,” claims the attack would

infect about 10 million users in the United States, Philippines and the United Kingdom. “I am so sorry to inform,” reading operations that the computer virus originated in the Philippines.

Tom KF

But Philippine Airlines general of the Technical Committee Center in the Philippines, said the computer virus could have a very serious situation there next month.

Good Monday, an Internet security expert, said the virus was found in Windows, caused by a bug between operating systems that had been developed by Microsoft Corporation.

Microsoft, which is helping with the FBI investigation, said it had taken action to combat viruses possibly caused by Windows.

Computer experts of several IT companies, including the United States and Canada governments, and thousands of businesses worldwide have been warned.

In Japan, the “Love Bug” attack spread throughout offices and homes, and many local network services are still under attack.

In Italy, officials of the UN Economic and Social Commission for Europe and the European Space Agency, and the European Space Agency, were prepared to combat the virus.

“LOVE-LETTER-FOR-YOU” was initially created to cause the damage mentioned by the “Trojan” but does not contain any destructive code.

From Philip, chief editor of CNET.net, reported Wednesday that the virus was spreading rapidly that the bug could now have wider areas of infection to damage.

The bug also warned that important documents could disappear, the contents of “LOVE-LETTER-FOR-YOU” causing any unduly destructive damage.

and China, with just 2,000, remained relatively unaffected because most viruses originated in national networks.

“Most viruses”

The effects to Asia Pacific nation are said to “lose millions and billions” in all the economy’s countries.

Good Monday, chairman, Tomo stated that Good Monday’s operations of education and business funds were affected by the computer virus.

PCB.com and the “Love Bug” were first detected at about 9 AM Wednesday (Japan Standard Time) in the city of Nagoya’s business area.

In the United States, it was reported by technical companies that the virus had affected about 100,000 personal computers at 10 AM yesterday (United States’ Eastern Time).

The FBI probe was launched yesterday following complaints by Japanese consumers about the virus.

Good Monday said in a statement the bug originated in Asia around April 29 last year. It was believed that the virus was spread through e-mail messages of the virus and infected via “LOVE-LETTER-FOR-YOU.”

Good Monday, technical services division of GoodMonday, said it was believed the bug could be infected by many different ways.

As said the bug was used a trojan horse technique and had infected numerous global network services.

Customers and their families in America’s economy, noting “we are still unable to find a family that is responsible.”

“Customers said that businesses that are part of a business or small business are particularly at risk because consumers are people’s bottom priority here,”

Good Monday said it was possible that business and other people are also spreading the virus through e-mail, “using virus that is not real things.”

The virus was described as a “virus that is used to attack people and not damage with the virus itself.”

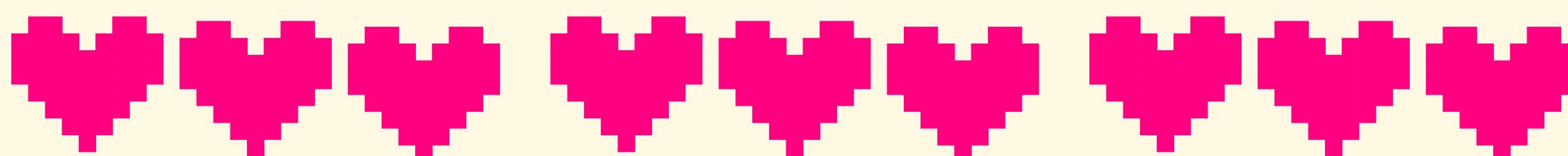
While the bug was spreading, Good Monday, said it was expected that the virus will spread to other countries.

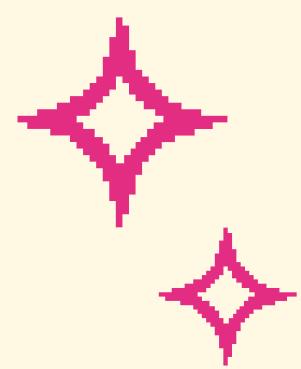
The virus was said to have a “hidden” function and would start to damage on the day.

Japanese officials said a small number of “LOVE-LETTER-FOR-YOU” were detected and checked their mail for “LOVE-LETTER-FOR-YOU.”

Good Monday service providers said to have received “LOVE-LETTER-FOR-YOU” via e-mail, but the bug was not detected.

Good Monday service providers said to have received “LOVE-LETTER-FOR-YOU” via e-mail, but the bug was not detected.

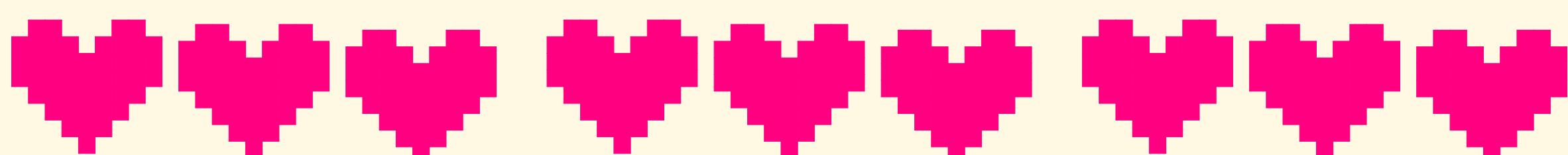


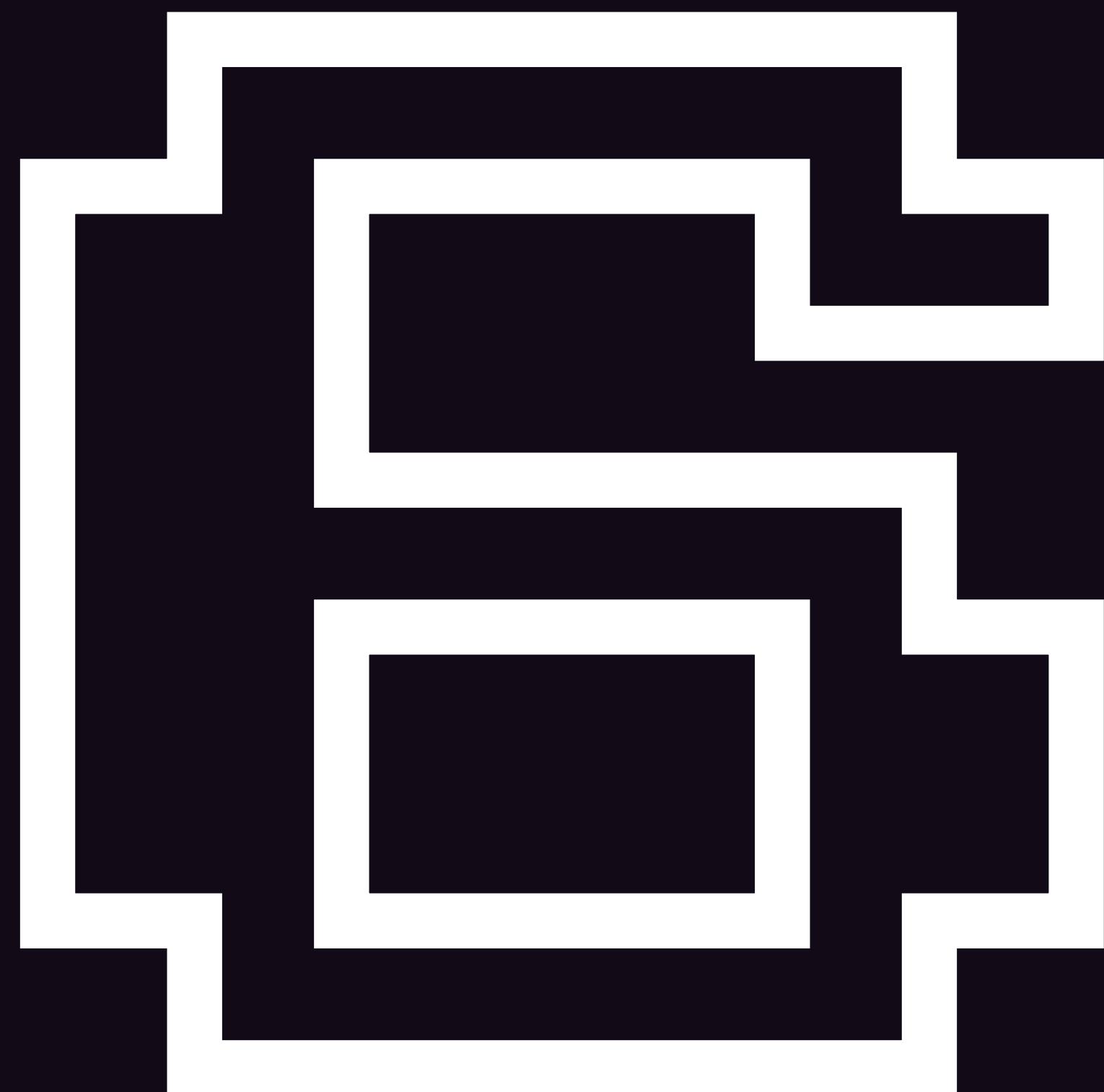


## A REPERCUSSÃO

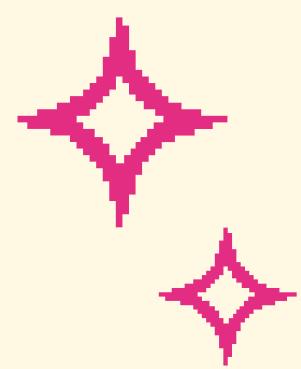
O vírus chegou a afetar empresas, governos e até instituições militares. Acredita-se que nem mesmo as redes do Pentágono e do Parlamento Britânico tenham saído ilesas da “epidemia”, o que teria forçado o desligamento de sistemas como medida de contenção. A cobertura da mídia, como era de se esperar,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





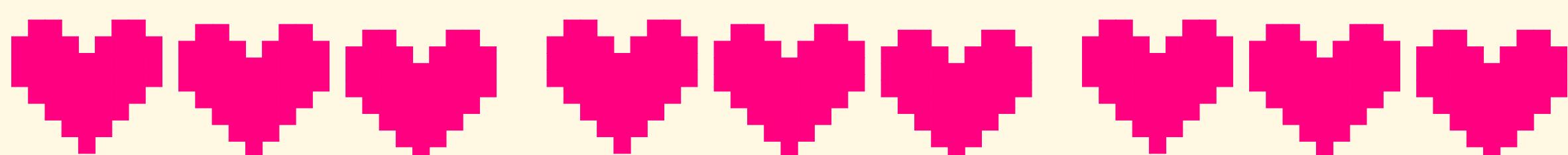
APRENDIZADO

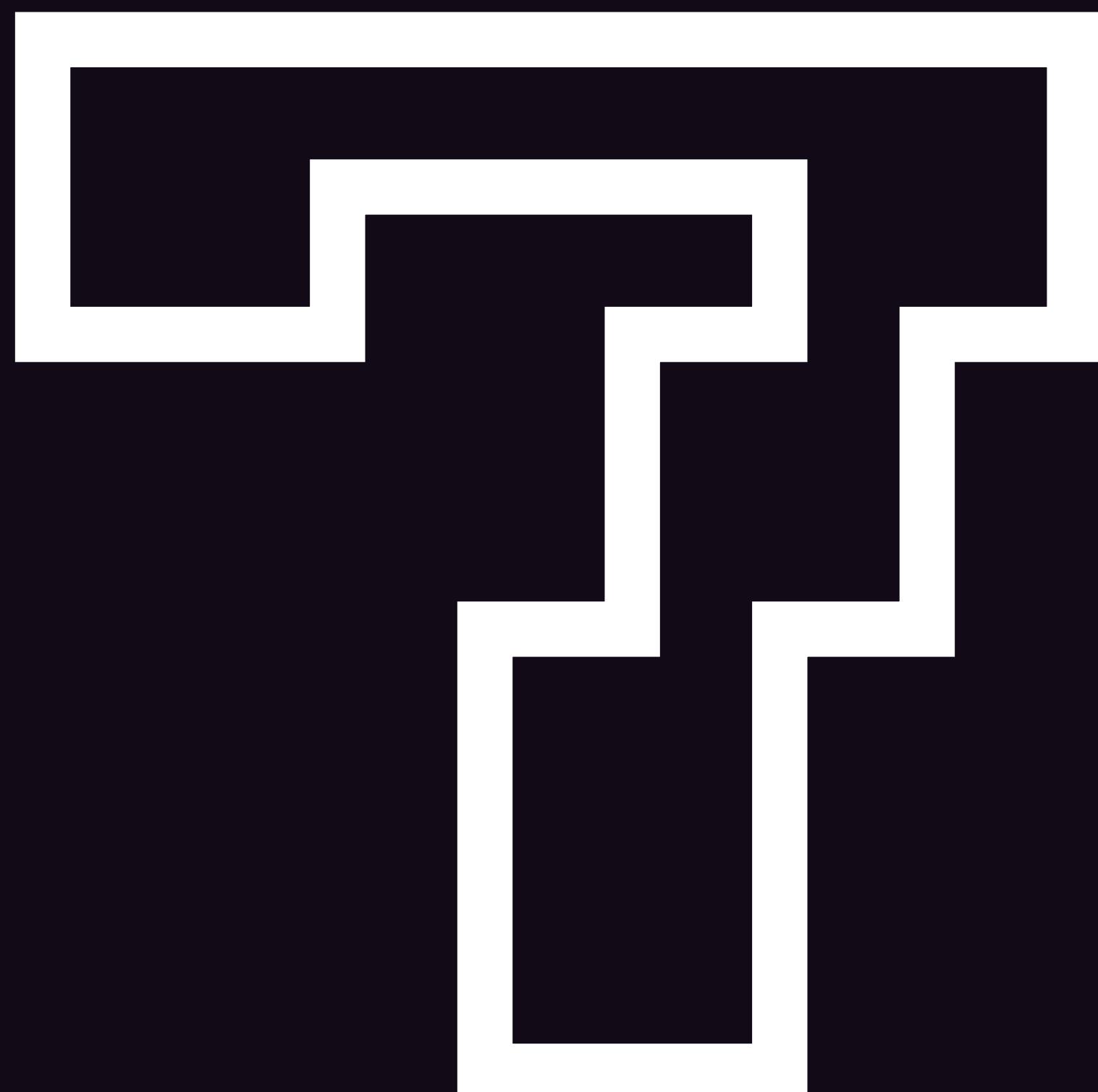


## AS LIÇÕES

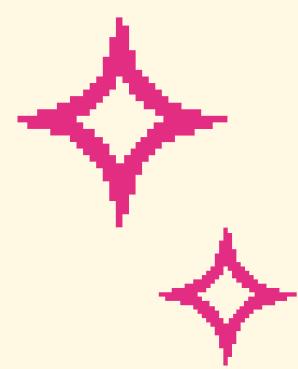
Sendo um divisor de águas para o mundo da segurança digital, ILOVEYOU foi o que fez as pessoas, empresas e entidades governamentais abrirem os olhos para ameaças virtuais. Uma simples linha de código, por mais amadora que seja, se aliada à curiosidade humana pode causar prejuízos bilionários em horas.

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.

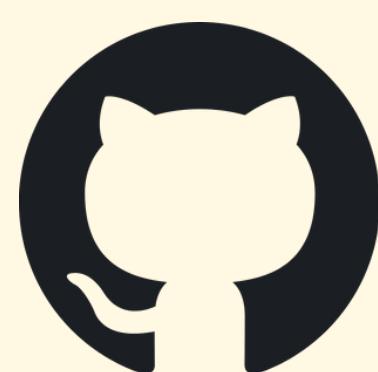
Fontes (clique no artigo para ir ao site):

**'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

