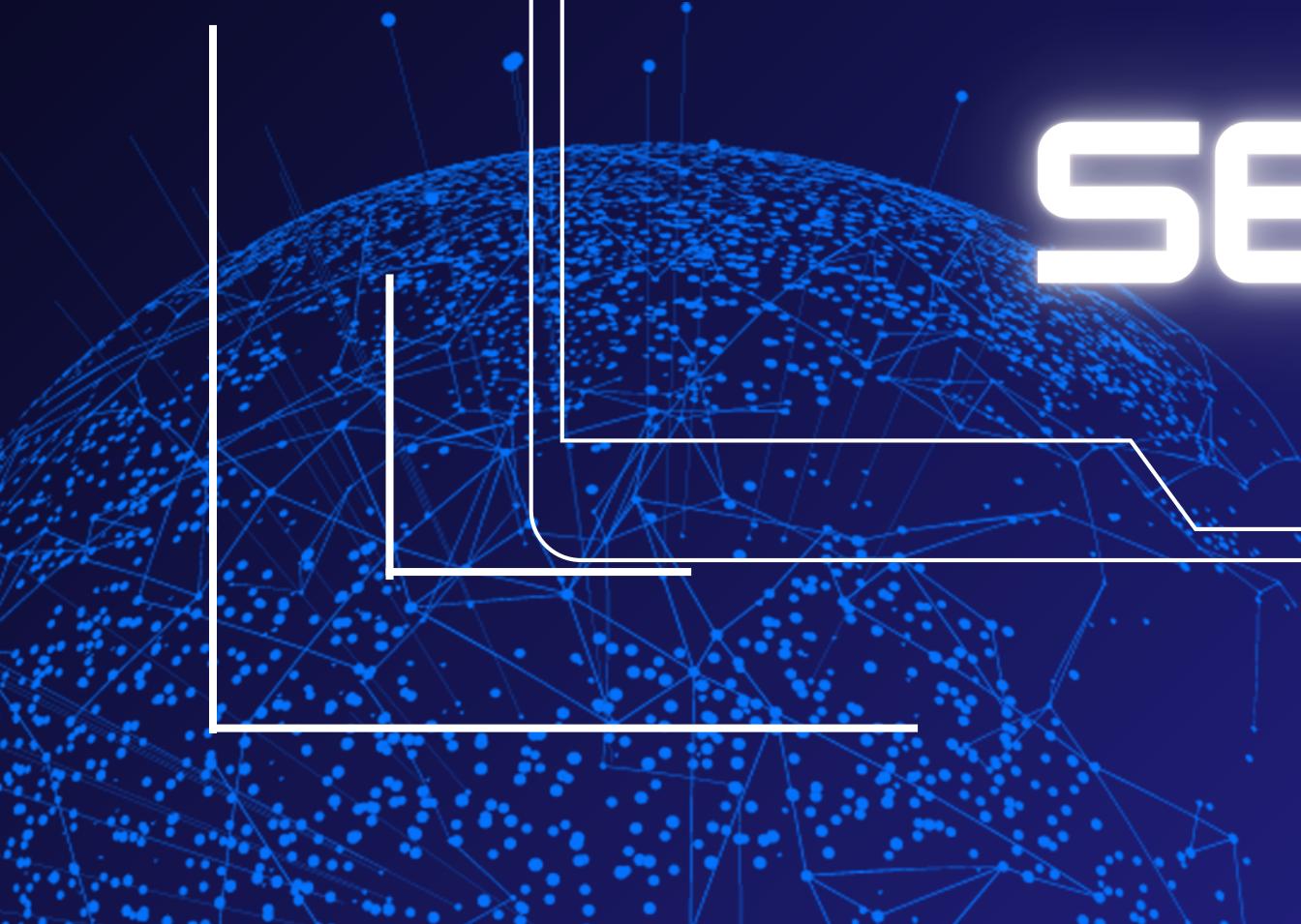


SISTEMAS COMPUTACIONAIS E SEGURANÇA



VULNERABILIDADES

fragilidade ou falha de segurança que pode ser explorada por ameaças maliciosas, comprometendo a segurança e integridade de dados.



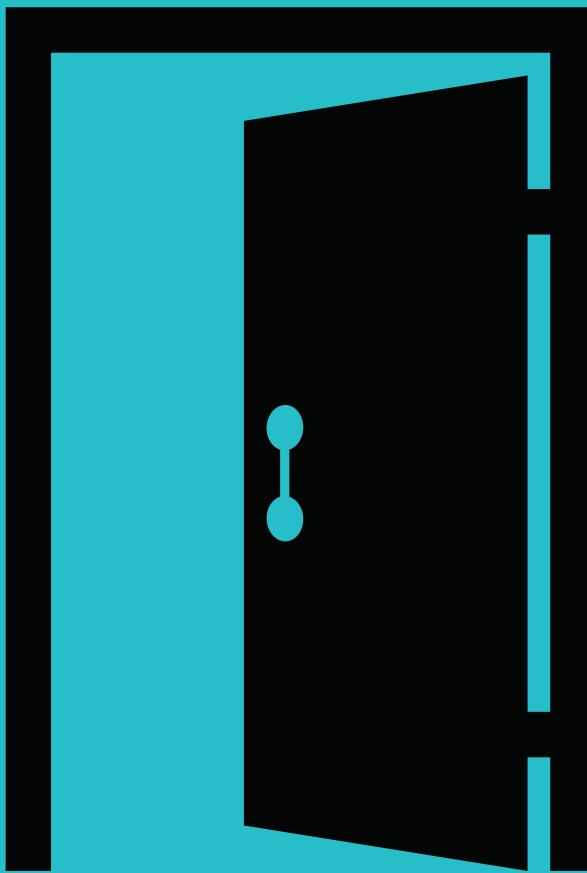
ATAQUE CIBERNÉTICO

■ O que é?

A definição de um ataque cibernético é “qualquer tentativa de expor, alterar, desativar, destruir, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um dispositivo.”



VULNERABILIDADE NA API DA SOLARWINDS



Em dezembro de 2020 o software de monitoramento Orion da SolarWinds foi comprometido quando em um ataque de cadeia de suprimentos conseguiu inserir um backdoor em uma atualização legítima, o que deu acesso a várias redes corporativas e governamentais



BACKDOOR



Nada mais é do que uma tecnica que permite um invasor (ou usuario não autorizado) acessar uma rede um sistema ou um dispositivo





ATAQUE DE CADEIA DE SUPRIMENTOS

Um ataque à cadeia de suprimentos usa ferramentas ou serviços de terceiros — coletivamente chamados de "cadeia de suprimentos" — para se infiltrar no sistema ou na rede de um alvo. Esses ataques às vezes são chamados de “ataques de cadeia de valor” ou “ataques de terceiros”.



```
module foo_bar(data_out, data_in, incoming_id, address, clk, rst_n);
output [31:0] data_out;
input [31:0] data_in, incoming_id, address;
input clk, rst_n;
wire write_auth, addr_auth;
reg [31:0] data_out, acl_oh_allowlist, q;
assign write_auth = |(incoming_id & acl_oh_allowlist) ? 1 : 0;
always @*
acl_oh_allowlist <= 32'h8312;
assign addr_auth = (address == 32'hFOO) ? 1: 0;
always @ (posedge clk or negedge rst_n)
if (!rst_n)
begin
q <= 32'h0;
data_out <= 32'h0;
end
else
begin
q <= (addr_auth & write_auth) ? data_in: q;
data_out <= q;
end
end
endmodule
```

Parte do código usado
CVE-2020-10148

algumas das empresas e organizações afetadas pelo ataque

- Departamento de Justiça (DOJ)
- Departamento do Tesouro
- Departamento de Segurança Interna (DHS)
- Administração Nacional de Telecomunicações e Informação (NTIA)
- Administração Nacional de Segurança Nuclear (NNSA)
- Microsoft
- FireEye
- Cisco
- Intel

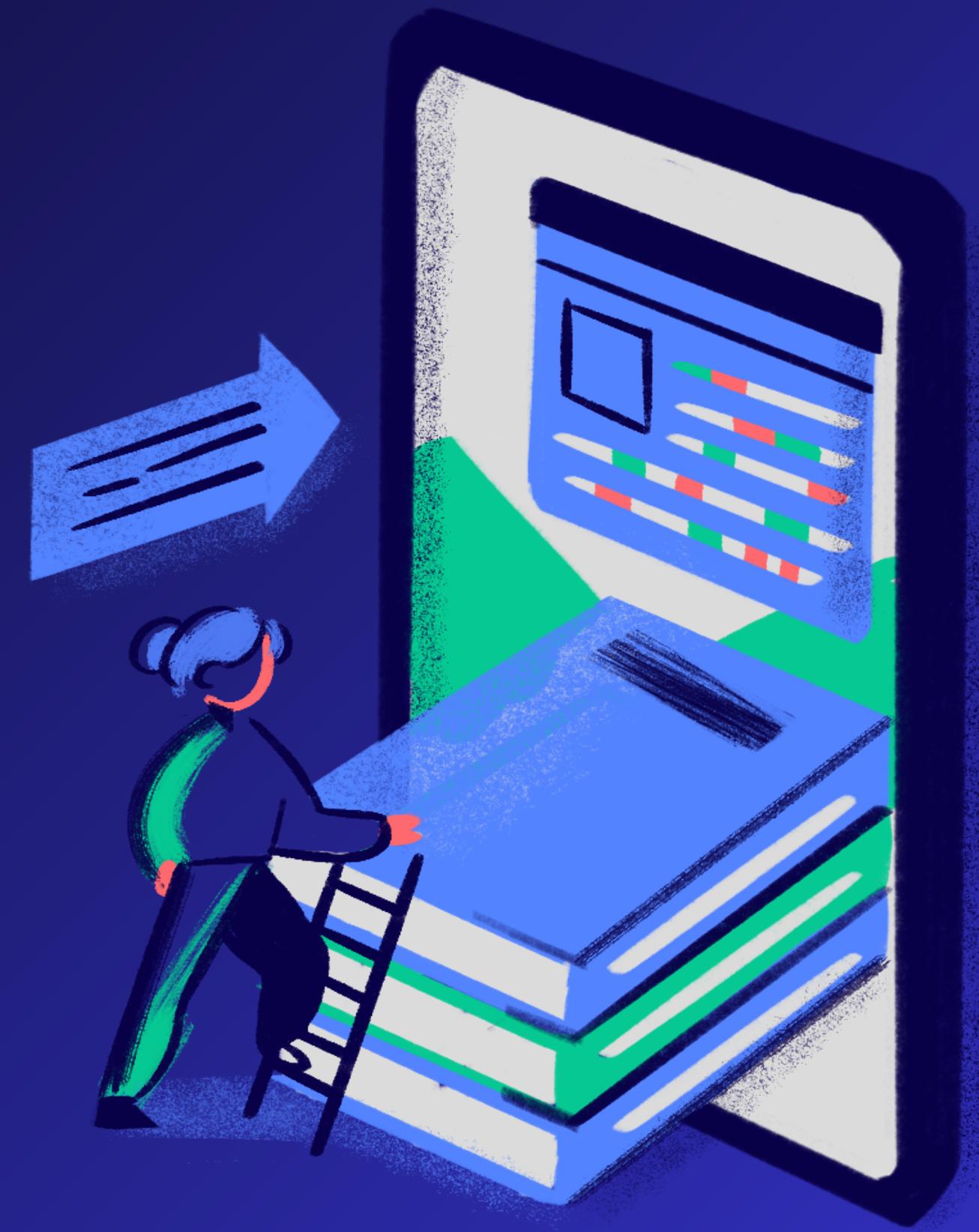
SOLUÇÃO

A solução veio através de uma atualização de software que corrigiu o problema que permitia que os criminosos adicionassem conteúdo ao código fonte da API.

PRESENTED BY SANDRA HARO

ATAQUE DE CREDENTIAL STUFFING

TWITTER



PRESENTED BY SANDRA HARO

Em junho de 2020 Twitter sofreu um ataque de credential stuffing que consiste em pegar as autorizações que certas pessoas tem para poder usar como quiser



A Twitter divulgou que
aproximadamente 130
contas foram
comprometidas

Muitas pessoas caíram
em golpes fazendo
com que os criminosos
conseguissem cerca
de 130 mil Dólares





MUITO
OBRIGADO

MURILO PASSOS
824217071

