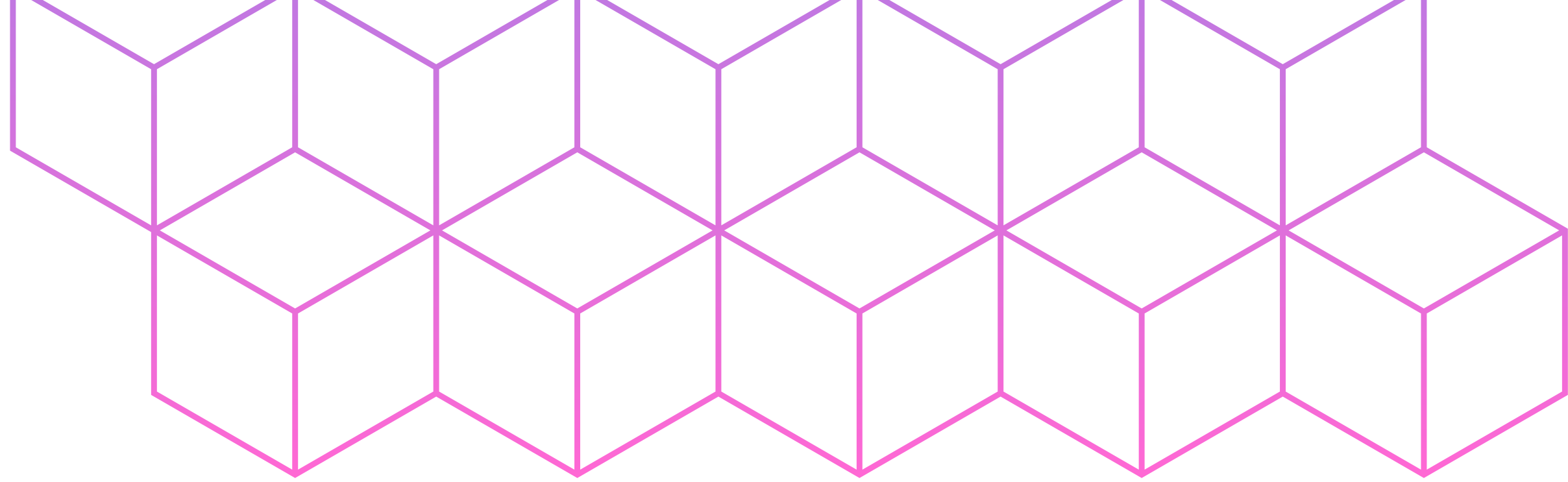
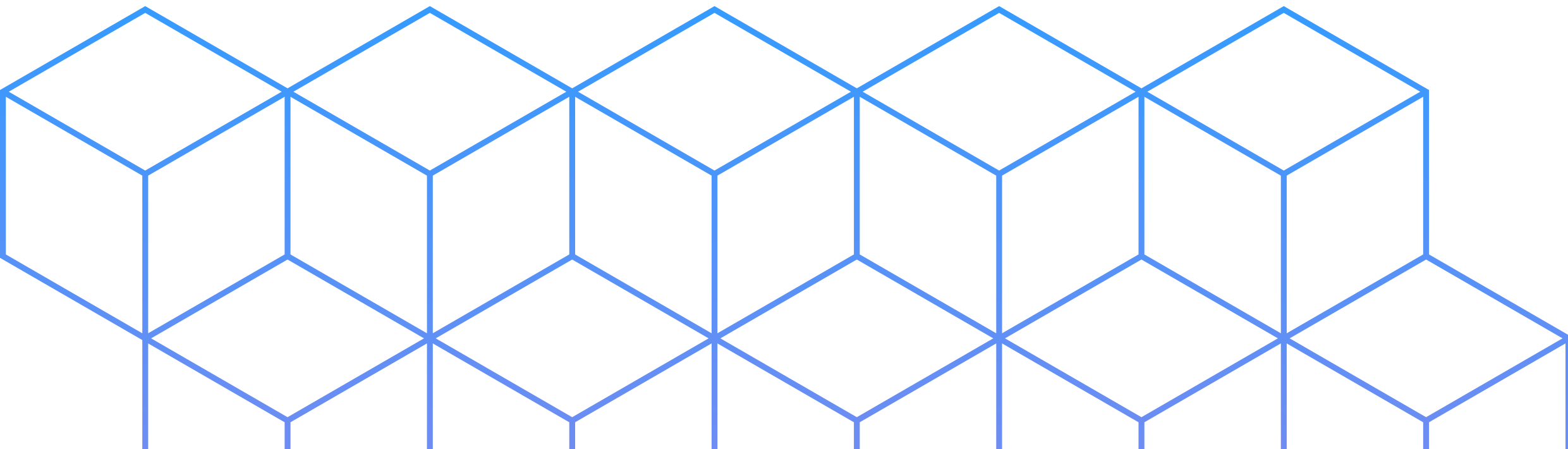


Epicode



Costrutti C - AssemblyX86

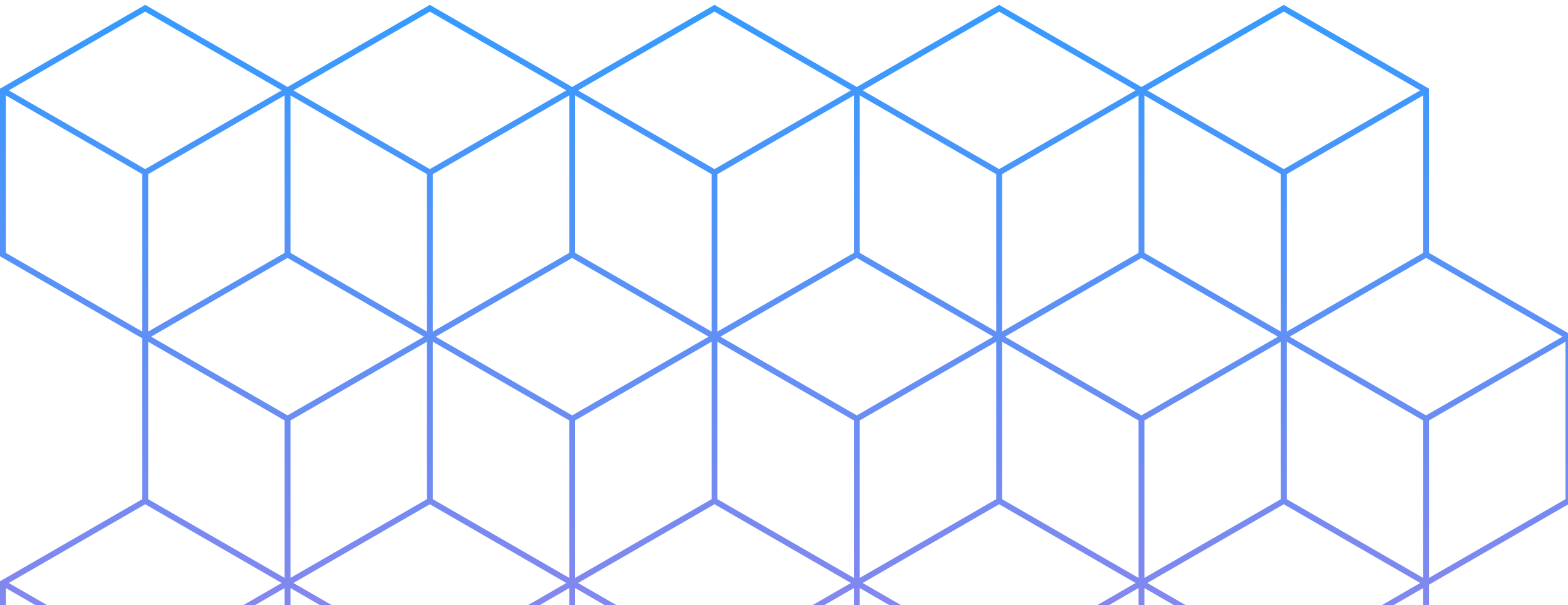
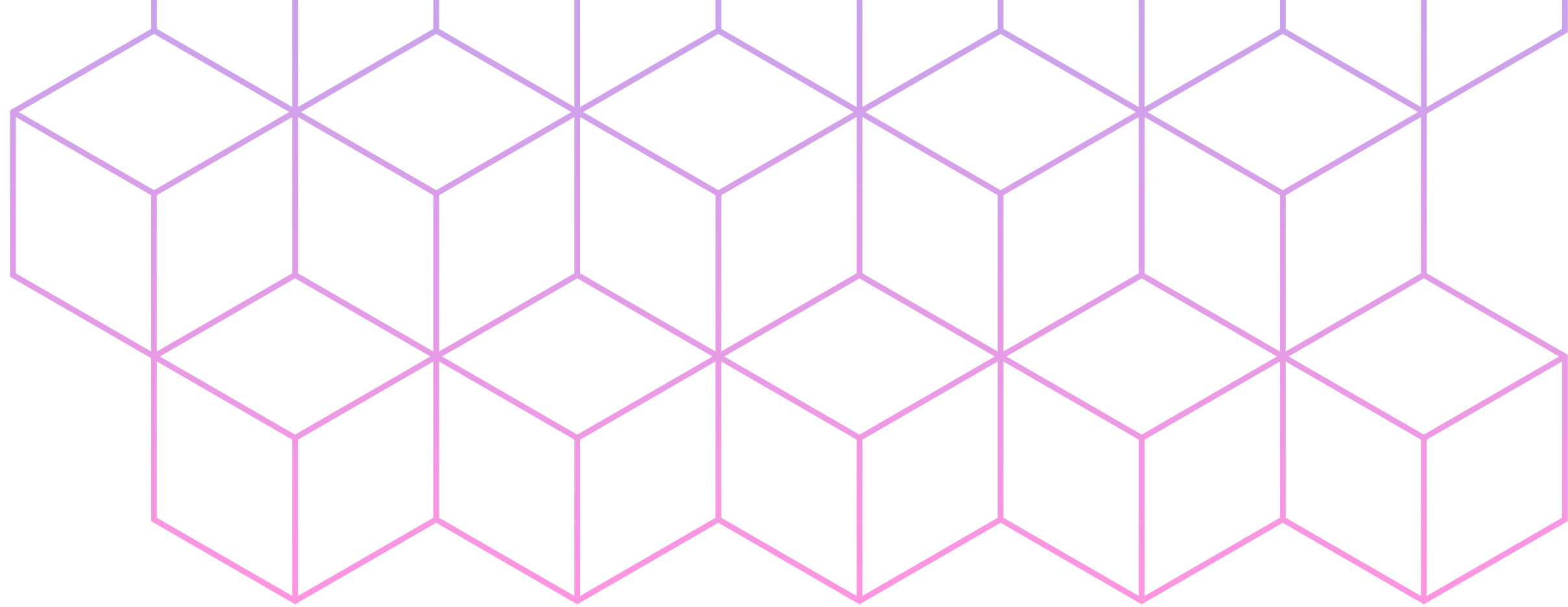


Traccia

Istruzioni

Analisi Codice

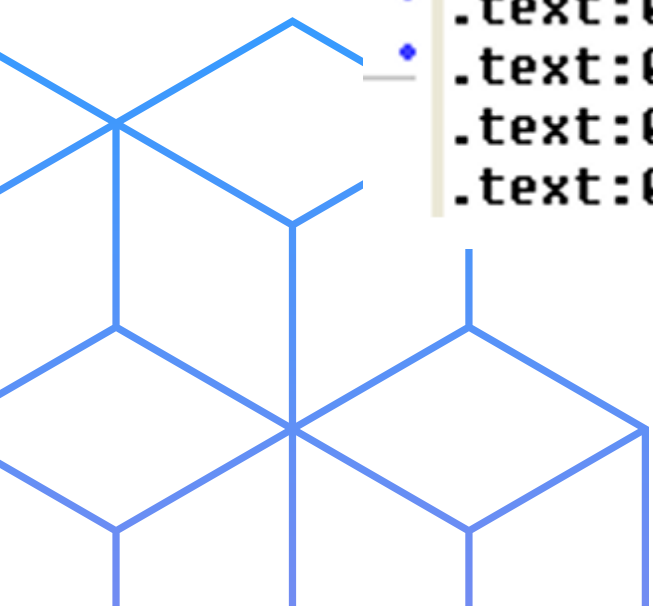
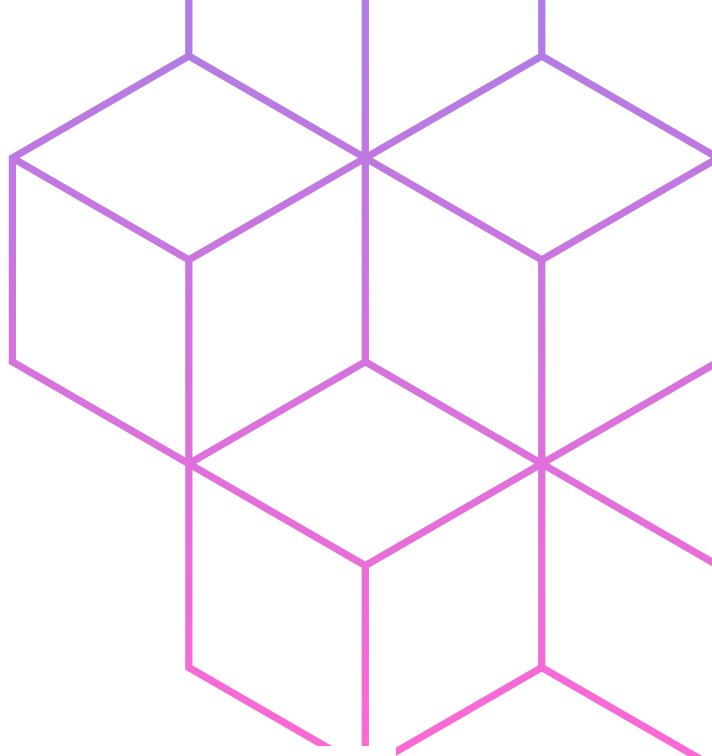
Tabella



Indice

Traccia

La figura seguente mostra un estratto del codice di un malware.
Identificare i costrutti noti visti durante la lezione teorica.



```
♦ .text:00401000
♦ .text:00401001
♦ .text:00401003
♦ .text:00401004
♦ .text:00401006
♦ .text:00401008
♦ .text:0040100E
♦ .text:00401011
♦ .text:00401015
- .text:00401017
♦ .text:0040101C
♦ .text:00401021
♦ .text:00401024
♦ .text:00401029
- .text:0040102B ; -----
♦ .text:0040102B

push    ebp
mov     ebp, esp
push    ecx
push    0          ; dwReserved
push    0          ; lpdwFlags
call    ds:InternetGetConnectedState
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jz      short loc_40102B
push    offset aSuccessInterne ; "Success: Internet Connection\n"
call    sub_40105F
add     esp, 4
mov     eax, 1
jmp     short loc_40103A
```

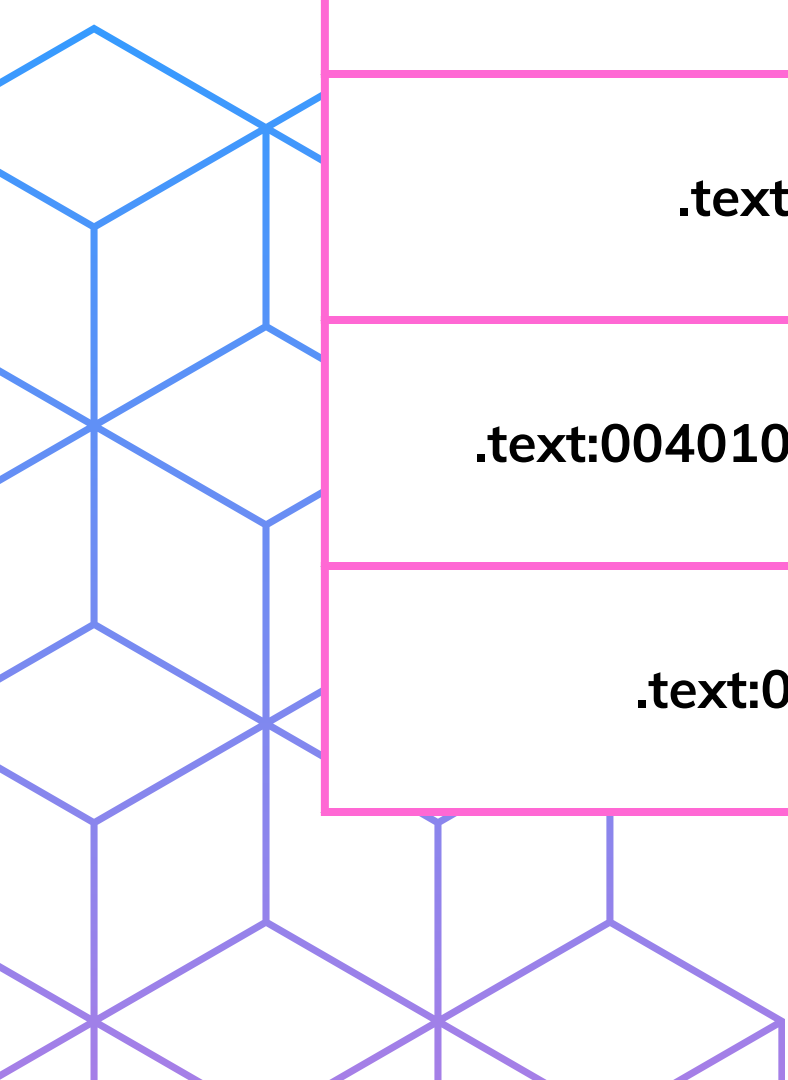
Istruzioni

MOV	ADD	CMP	JMP	CALL	PUSH
<p>spostare una variabile o un dato da una locazione ad un'altra. La sintassi di «mov» è: mov destinazione, sorgente</p>	<p>si utilizza l'istruzione «add» con la sintassi «add a,b» per sommare b al valore di a e salvare/aggiornare il valore di a con il nuovo valore dopo l'addizione</p>	<p>l'istruzione «cmp» è simile all'istruzione «sub», ma a differenza di «sub» non modifica gli operandi. l'operazione «cmp» modifica i flag ZF (Zero Flag) e CF (CarryFlag). La sintassi di cmp è «cmp destinazione, sorgente»</p>	<p>Salta incondizionatamente all'istruzione associata all'operando. I salti condizionali utilizzano il contenuto dei flags per determinare se «saltare» o meno ad una data locazione che viene specificata come operando dell'istruzione jump.</p>	<p>L'istruzione call passa l'esecuzione del programma alla funzione chiamata per la quale verrà creato un nuovo stack.</p>	<p>Push: spingere un valore vuol dire scriverlo nello stack. L'operazione per aggiungere un piatto è «push» mentre l'operazione per rimuovere un piatto è «pop».</p>

Analisi codice

Questo codice dovrebbe verificare se - sulla macchina nella quale viene eseguito - possiamo trovare una connessione Internet attiva: Se il valore di ritorno della funzione è diverso da zero, indica che la connessione è attiva

♦ .text:00401000	push	ebp	→ Crea lo stack
♦ .text:00401001	mov	ebp, esp	
♦ .text:00401003	push	ecx	
♦ .text:00401004	push	0	; dwReserved
♦ .text:00401006	push	0	; lpdwFlags
♦ .text:00401008	call	ds:InternetGetConnectedState	→ Chiamata della funzione dallo Stack tramite il push
♦ .text:0040100E	mov	[ebp+var_4], eax	
♦ .text:00401011	cmp	[ebp+var_4], 0	
♦ .text:00401015	jz	short loc_40102B	→ IF-Style: assembly di un costrutto switch compilato come un costrutto IF.
♦ .text:00401017	push	offset aSuccessInterne	; "Success: Internet Connection\n"
♦ .text:0040101C	call	sub_40105F	
♦ .text:00401021	add	esp, 4	
♦ .text:00401024	mov	eax, 1	→ Chiamata della funzione dallo Stack tramite il push
♦ .text:00401029	jmp	short loc_40103A	
♦ .text:0040102B	; -----		
♦ .text:0040102B			



ISTRUZIONE	DESCRIZIONE
.text:00401000 push ebp	Mette il valore attuale del registro EBP nello stack
.text:00401001 mov ebp, esp	Copia il valore dello stack di ESP in EBP.
.text:00401003 push ecx	Mette il valore di ECX nello stack
.text:00401004 push 0; dwReserved:	Mette il valore 0 nello stack. E lo passa come argomento dwReserved alla funzione.
.text:00401006 push 0 ; lpdwFlags	Mette il valore 0 nello stack. E lo passa come argomento lpdwFlags alla funzione.
.text:00401008 call ds:InternetGetConnectedState:	Chiama la funzione InternetGetConnectedState che controlla lo stato della connessione a Internet.
.text:0040100E mov [ebp+var_4], eax:	Copia il valore restituito dalla funzione InternetGetConnectedState in [ebp+var_4].

ISTRUZIONE	DESCRIZIONE
.text:00401011 cmp [ebp+var_4], 0:	Confronta il valore memorizzato con 0.
.text:00401015 jz short loc_40102B:	Passa ad loc_40102B se il valore nella variabile è zero. Quindi se non c'è connessione a Internet, il programma salta a loc_40102B.
.text:00401017 push offset asuccessInterne:	Mette l'indirizzo della stringa asuccessInterne nello stack. Sembra essere un messaggio che indica la corretta connessione a internet.
.text:0040101C call sub_40105F:	Chiama una subroutine a sub_40105F, per stampare il messaggio di successo sulla connessione.
.text:00401021 add esp, 4:	Ripristina lo stack dopo la chiamata alla funzione.
.text:00401024 mov eax, 1:	copia 1 nel registro EAX.
.text:00401029 jmp short loc_40103A:	Passa a loc_40103A. Questa azione viene eseguita a prescindere se è presente una connessione a internet.