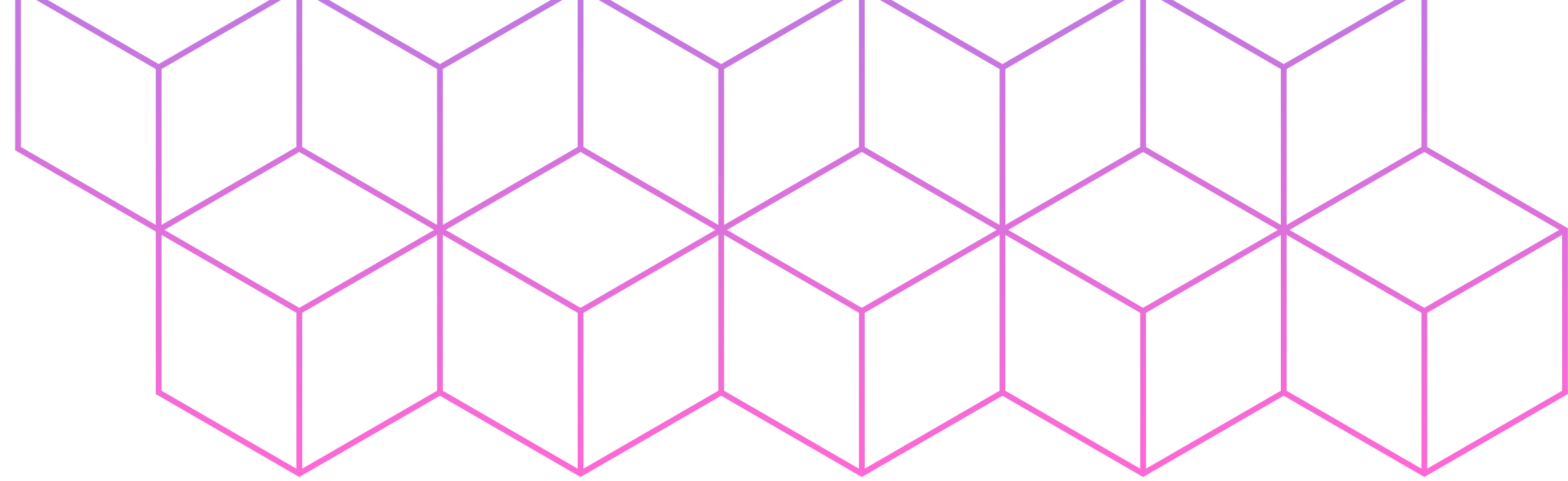
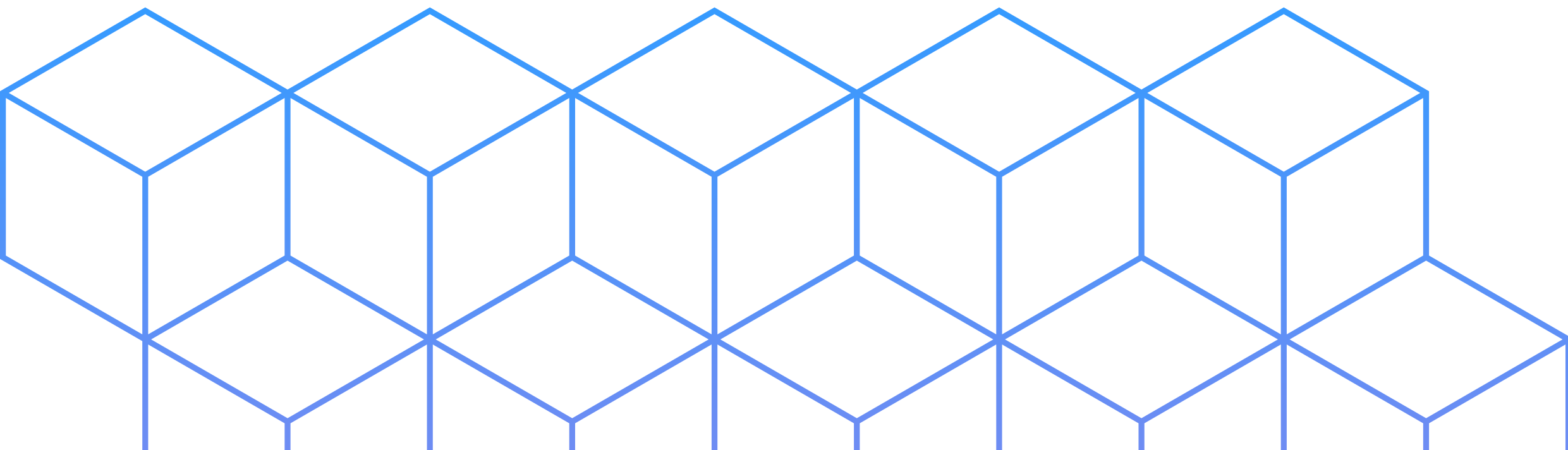
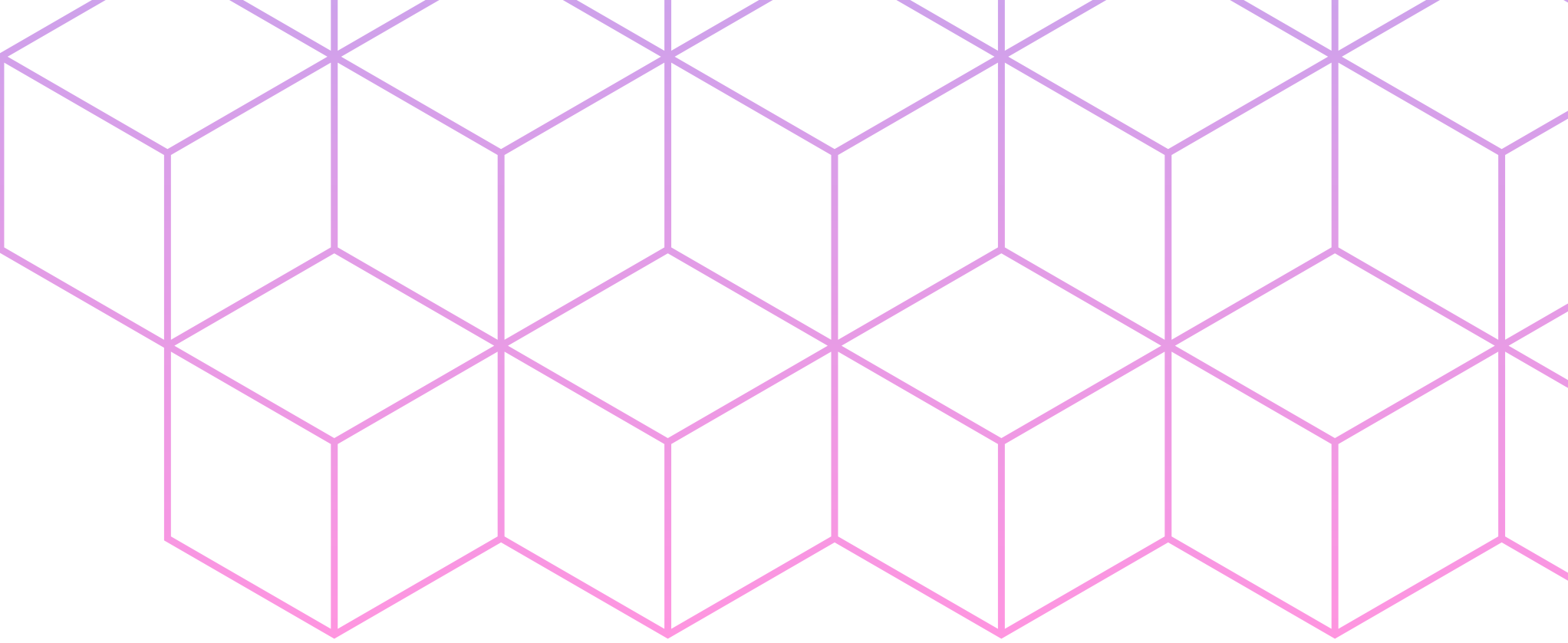
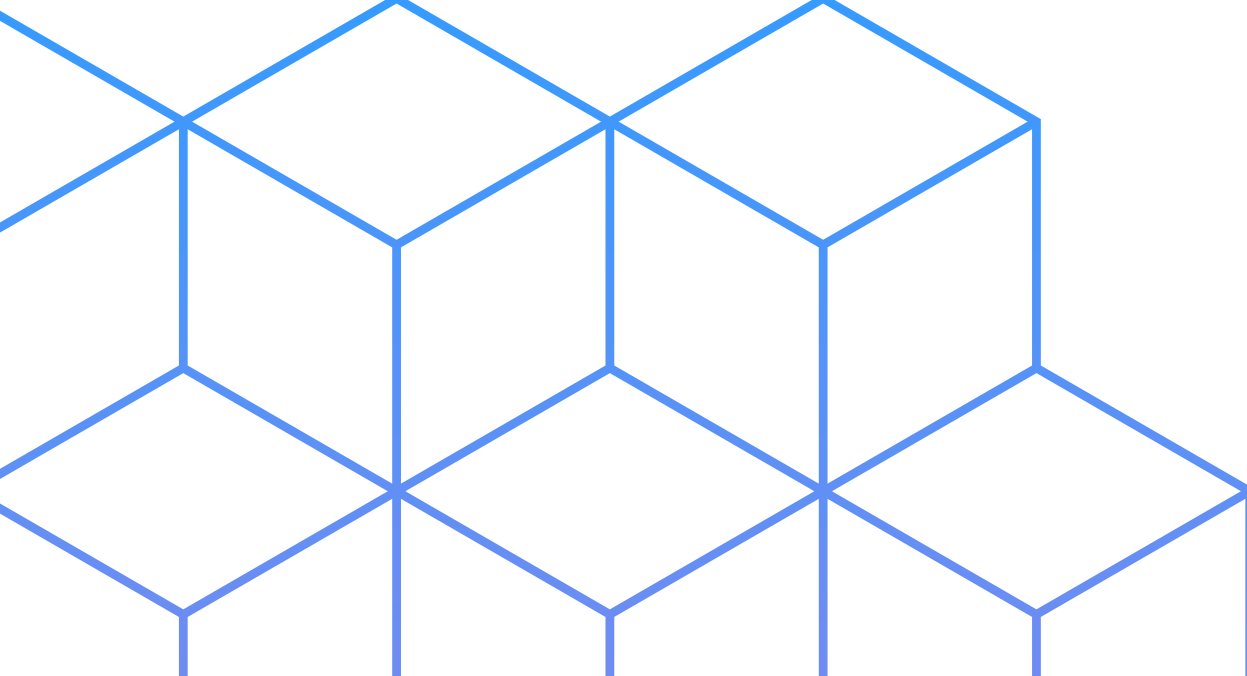


Epicode



Funzionalità dei malware



- 
- **Traccia**
 - **Tipo di Malware**
 - **Chiamate di funzione principali**
 - **Persistenza**
 - **BONUS: analisi a basso livello delle singole istruzioni**
- 

Indice

Traccia

La figura mostra un estratto del codice di un malware. Identificate:

- 1. Il tipo di Malware in base alle chiamate di funzione utilizzate.
- 2. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa
- 3. Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo
- 4. BONUS: Effettuare anche un'analisi basso livello delle singole istruzioni

.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	
.text: 00401040	XOR ECX,ECX	
.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = path_to_Malware
.text: 0040104C	push ecx	; destination folder
.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	

Tipo di Malware

.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	
.text: 00401040	XOR ECX,ECX	
.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = path_to_Malware
.text: 0040104C	push ecx	; destination folder
.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	

Questo codice potrebbe rappresentare un Keylogger, un particolare tipo di malware programmato per intercettare tutto ciò che l'utente della macchina infetta digita sulla tastiera. Le funzionalità di un keylogger sono sfruttate dai criminali informatici per rubare informazioni confidenziali quali ad esempio:

- Password dei sistemi operativi
- Credenziali di amministrazione
- Numeri di conto e informazioni circa carte di credito
- Credenziali di accesso a siti

Chiamate di funzione principali

Nel codice in figura una delle chiamate di funzione principali è sicuramente `SetWindowsHook()` che viene usata per creare proprio ciò che viene chiamato “hook”, una funzione che monitora una periferica specifica del sistema - in questo caso capiamo che si riferisce al mouse, infatti notiamo proprio il parametro `WH_Mouse`

.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	
.text: 00401040	XOR ECX,ECX	
.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = path_to_Malware
.text: 0040104C	push ecx	; destination folder
.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	

Persistenza

Il modo in cui il malware ottiene la persistenza all'interno del SO è grazie a *Startup_folder_system* evidenziato dal comando `move ecx, [EDI]`. In pratica, questo permette al malware di essere avviato automaticamente in fase di avvio del dispositivo, così da essere pronto al monitoraggio degli input provenienti proprio dal mouse; sfruttando la cartella di avvio di Windows. I dati in input vengono successivamente registrati all'interno di un file di log.

.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	
.text: 00401040	XOR ECX,ECX	
.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = path_to_Malware
.text: 0040104C	push ecx	; destination folder
.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	

BONUS: spiegare a grandi linee il funzionamento del malware

ISTRUZIONI	DESCRIZIONE
push eax, push ebx, push ecx	Qui vediamo delle istruzioni che inseriscono i valori dei registri nello stack. Questa dovrebbe essere una preparazione alla chiamata di funzione seguente, questi valori vengono quindi usati come paramenti
push WH_Mouse	Inserisce il valorente del paramento WH_Mouse nello stack. Questo è l'hook da impostare per l'intercettazione di ciò che il mouse fa
call SetWindowsHook()	Chiamata di funzione SetWindowsHook() per impostare l'intercettazione del mouse. Questo permette al malware di monitorare i movimenti del mouse.
XOR EXC, ECX, mov ecx, [EDI], move edx, [ESI]	Queste istruzione permettono operazioni di manipolazione dei registri. Preparano i paramentri necessari per la chiamata successiva alla funzione CopyFile()
push ecx, push edx	Inserisce i valori di exc e edx nello stack. Questi valori dovrebbero contenere i percorsi di destinazione e di origine per le copia del file.
call CopyFile()	Chiamata di funzione CopyFile() per copiare il malware nella nuova posizione nel sistema operativo. Questo è un comportamento tipico malware che cerca di propargarsi e nascondersi.