Haftalık Siber Güvenlik Haber Özeti

Son 7 gün • 2026-01-25 03:41 UTC

THE HACKER NEWS

2026-01-24 08:09 UTC

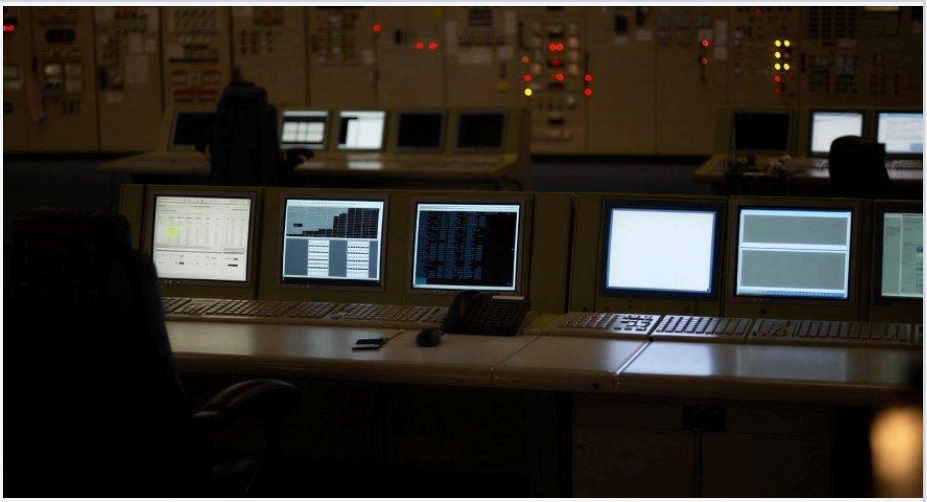
1. Multi-Stage Phishing Campaign Targets Russia with Amnesia RAT and Ransomware

Rusya'da hedef alınan yeni bir multi-derece phishing kampanyası, Amnesia RAT ve ransomware kullanılarak gerçekleştiriliyor. Bu kampanya, sosyal mühendislik lürleri aracılığıyla kullanıcıları etkiler. Fortinet FortiGuard Labs araştırmacıları, bu lürlerin, normal ve zararsız görünümlü iş belgeleri ve eşlik eden skripler olarak sunulduğunu açıkladı. Bu belgeler ve skripler, gözü dağıtmak için kullanılmakta, gerçek faaliyette sessizce çalışan kötü amaçlı faaliyetlerin arkasında çalışmaktadır. Kampanya, birkaç nedenden dolayı dikkat çekiyor. İlk olarak, farklı türdeki yüklerin dağıtımını sağlamak için birden fazla kamu bulut hizmeti kullanılmaktadır. Ayrıca, Microsoft Defender'i devre dışı bırakmak için operasyonel olarak kötü amaçlı davranış göstermektedir. Bu kampanyada, kullanıcıları etkileyen sıkıştırılmış arşivler, birden fazla decoy belge ve kötü amaçlı Windows kısayol (LNK) içeren bir dizi olarak sunulmaktadır.

THE HACKER NEWS

2026-01-24 05:21 UTC

2. New DynoWiper Malware Used in Attempted Sandworm Attack on Polish Power Sector



Polish Enerji Sektorunda Sandworm Grubu tarafından yapılan saldırı: DynoWiper Malware’nin kullanıldığı iddia ediliyor. Polonya Enerji Bakanı Milosz Motyka, geçen hafta sandworm grubunun, 2025 yılının son haftasında Polonya'nın enerji sistemine yönelik "en büyük cyber attack"ını gerçekleştirdiğini söyledi. ESET raporuna göre, saldırı DynoWiper adı verilen ve önceden belgelenmemiş wiper malware kullanılarak gerçekleştirildi. Saldırı, Polonya hükümetinin ve Slovakya'daki cybersecurity firmalarının bildirdiği gibi, iki combined heat and power (CHP) tesisi ve yenilenebilir enerji kaynaklarından elektrik üretimi için kullanılan bir sistem hedef aldı. Polonya Başbakanı Donald Tusk, saldırıyı Rus hükümetine bağlı gruplar tarafından hazırlandığını söyledi ve ek güvenlik tedbirleri alındığını bildirdi.

THE HACKER NEWS

2026-01-24 05:20 UTC

3. Who Approved This Agent? Rethinking Access, Accountability, and Risk in the Age of AI Agents

Türkçe olarak yeniden yazılan metin: İşlem Sürecinde Siber Güvenlik Sorunları: AI Ajanlarının Yetki, Sorumluluk ve Riski Yeniden Düşünülmeli AI ajanları, iş sürecini hızlandırmaya yardımcı olarak, toplantı takvimini oluşturur, veri erişimi sağlar, akışları tetikler, kod yazar ve gerçek zamanlı olarak eylemler gerçekleştirir. Ancak, güvenlik ekiplerine geldiğinde "Bu ajanı kim onayladı?" sorusu ortaya çıkar. AI ajanları, kullanıcılar veya uygulamalar gibi hızla deploy edilir, geniş bir şekilde paylaşılarak ve geniş yetki izinleri verilerek, sahipliği, onaylama ve sorumluluğu takip etmek zorlaşır. AI ajanları, geleneksel yetki modellerini bozar. Ajanlar, insanları ve geleneksel hizmet hesaplarını farklı olarak çalışır. İnsan yetki, açık niyet etrafında inşa edilir. Yetkilikler, roller ile bağlantılıdır, düzenli olarak gözden geçirilir ve zaman ve contexto tarafından kısıtlanır.

THE HACKER NEWS

2026-01-24 05:09 UTC

4. CISA Adds Actively Exploited VMware vCenter Flaw CVE-2024-37079 to KEV Catalog

Aşağıdaki metni Türkçe olarak yeniden yazarak özetini oluşturuyorum: ABD'nin Ulusal Siber Güvenlik ve İnfrastruktur Ajansı (CISA), Broadcom'un VMware vCenter Sunucusuna ilişkin kritik bir güvenlik açığını, aktif olarak işletilen KEV Kataloğu'na ekledi. Bu açığın adı CVE-2024-37079'dir ve Haziran 2024'te çözmüştür. Çinli siber güvenlik şirketi QiAnXin LegendSec'in araştırmacıları Hao Zheng ve Zibo Li, bu sorunu bulmuş ve rapor etmiştir. Araştırıcılar, DCE/RPC hizmetinde bulunan dört güvenlik açığını keşfetmişlerdir ve bu açıkların ikisi Haziran 2024'te, diğer ikisi Eylül 2024'te çözmüştür. Bu güvenlik açıklarından biri, yetkisel yükseltme açığı ile zincirlenerek, ESXi üzerinde kontrol elde edilmesine izin verir. Bu açığın şu anda nasıl işletiliyor, bilinmiyor, ancak Broadcom, bu açığın aktiv olarak işletildiğini resmi olarak onayladı.

THE HACKER NEWS

2026-01-23 12:24 UTC

5. CISA Updates KEV Catalog with Four Actively Exploited Software Vulnerabilities

Türkiye'deki Siber Güvenlik Ajansı (CISA), 24 Ocak 2026 tarihinde, aktif olarak kullanılan dört yazılım güvenlik açığını "İlgili Açıktan Bilinen Açıklar" (KEV) kataloğuna ekledi. Bu açıkların listesi şu şekilde: - CVE-2025-68645: Synacor Zimbra Collaboration Suite'ün (ZCS) uzak dosya dahil etme açığı, bir uzak saldırıya uğrayacak ve WebRoot dizini içindeki herhangi bir dosyayı olmadan kimlik doğrulama gerektirmeyecektir. (November 2025'de 10.1.13 versiyonunda fix edildi.) - CVE-2025-34026: Versa Concerto SD-WAN orchestrasyon platformunun kimlik doğrulama atlama açığı, bir saldırıya uğrayarak yönetimsel uç noktalarına erişim sağlayacak. (April 2025'de 12.2.1 GA versiyonunda fix edildi.) - CVE-2025-31125: Vite Vitejs'in yanlış erişim kontrol açığı, ?inline&import veya ?raw.

THE HACKER NEWS

2026-01-23 09:30 UTC

6. Fortinet Confirms Active FortiCloud SSO Bypass on Fully Patched FortiGate Firewalls

Here is the rewritten text in Turkish: Fortinet, tam olarak güncellenmiş FortiGate firewalllerinde aktif FortiCloud SSO atlama tespit etti. Şirket, bu atlamanın yeni saldırı yolu olduğu ve saldırıların tam olarak güncellenmiş cihazlara yönelik olduğu bildirildi. Atlama, SAML mesajları aracılığıyla FortiCloud SSO özelliği etkinleştirilen cihazlar için SSO giriş onayını atlama imkanı sunar. Şirket, bu atlamanın orijinal olarak son ayda giderilmiş olduğunu ancak yeni saldırı girişimleri olduğunu bildirdi. Şirket, saldırı aktörünün "cloud-noc@mail.io" ve "cloud-init@mail.io" adında hesaplar kullanarak giriş yaptığını ve VPN erişimini sağlamaya çalıştığını bildirdi. Şirket, saldırının önlenmesi için yerel ağ cihazına internet üzerinden erişimi kısıtlama ve FortiCloud SSO giriş onayını devre dışı bırakma önerdi.

THE HACKER NEWS

2026-01-23 08:30 UTC

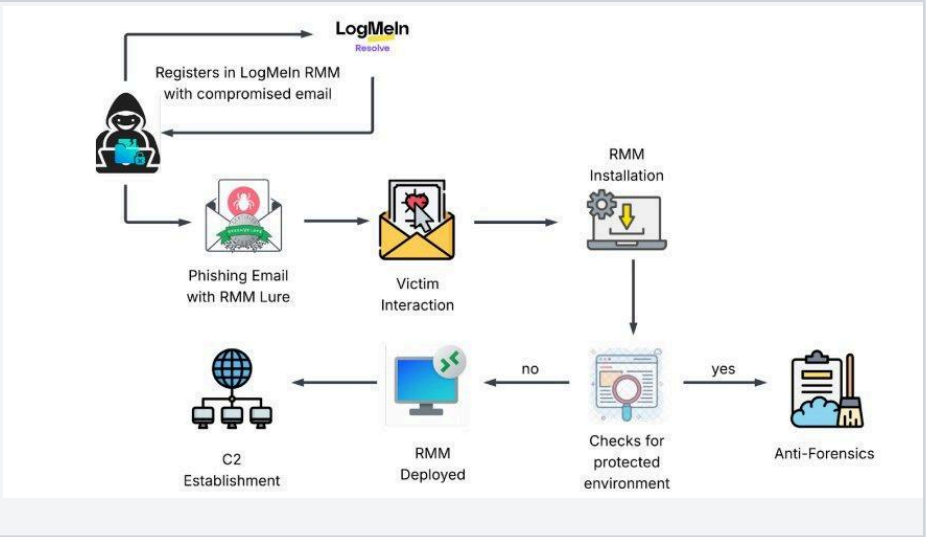
7. TikTok Forms U.S. Joint Venture to Continue Operations Under 2025 Executive Order

TikTok, popüler video paylaşım uygulaması, ABD'de 2025 tarihli başkanı Trump'un imzaladığı yürütme emrinin bir sonucu olarak ABD'de faaliyetlerini sürdürmek için bir ortak girişim kurdu. TikTok USDS Joint Venture LLC olarak adlandırılan yeni girişim, ByteDance'ın Çinli ana şirketinin, ABD'deki kullanıcı verilerini korumak için geliştirilen güvenlik tedbirlerine uyum sağlamak için kuruldu. ABD'deki kullanıcı verilerinin korunması, Oracle'ın güvenli ABD bulut ortamında sağlanacak, ayrıca TikTok'un içerik önerme algoritması ABD'deki kullanıcılar için yeniden eğitime tabi tutulacak. Ayrıca, bağımsız bir varlık, ABD'deki veri gizliliği ve siber güvenlik programını geliştirecek ve üçüncü taraf siber güvenlik uzmanlarının denetimine tabi tutulacak.

THE HACKER NEWS

2026-01-23 08:18 UTC

8. Phishing Attack Uses Stolen Credentials to Install LogMeIn RMM for Persistent Access

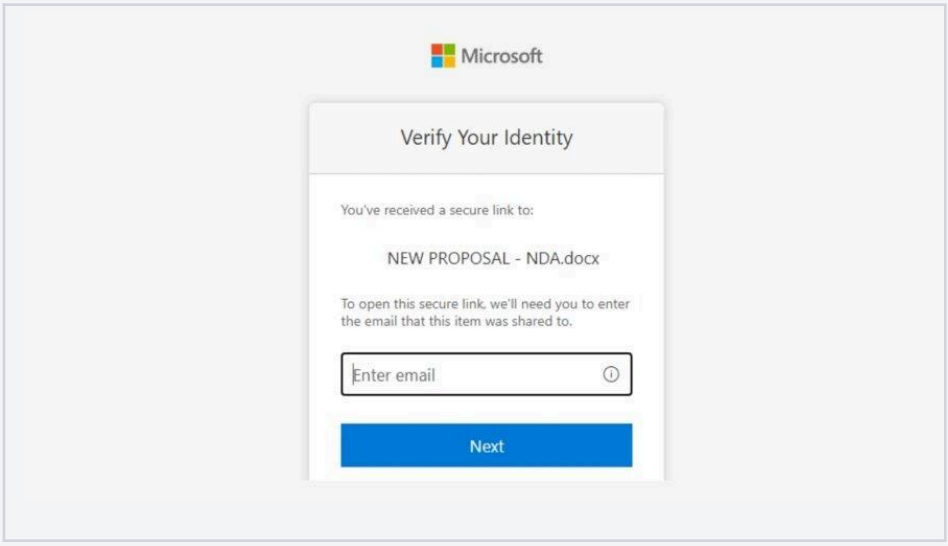


Aşağıdaki metni Türkçe olarak yeniden yazarak özetini oluşturacağım: Cybersecurity araştırmacıları, yeni bir ikili vektör kampanyası hakkında bilgi paylaştı. Bu kampanyada, çalınan kimlik bilgilerini kullanarak, meşru Uzaktan İzleme ve Yönetim (RMM) yazılımını kurarak, saldırıya uğrayan sunuculara kalıcı uzaktan erişim kuruyor. Saldırganlar, güvenlik perimetrleri etrafından dolaşarak, yöneticiyi güvenladığı IT araçlarını silahlandırıyor. Çalınan kimlik bilgilerini kullanarak, RMM araçlarını kurarak kalıcı erişim tesis ediyor. Saldırganlar, Microsoft Outlook, Yahoo!, AOL.com giriş bilgilerini çalınarak, RMM araçlarını kuruyor. Ardından, "GreenVelopeCard.exe" adlı bir yürütülebilir dosya aracılığıyla, RMM araçlarını kurarak kalıcı uzaktan erişim tesis ediyor. Bu araç, geçerli bir sertifikayla imzalanmış ve JSON konfigürasyonunu içeren bir binarydür.

THE HACKER NEWS

2026-01-23 05:25 UTC

9. Microsoft Flags Multi-Stage AitM Phishing and BEC Attacks Targeting Energy Firms

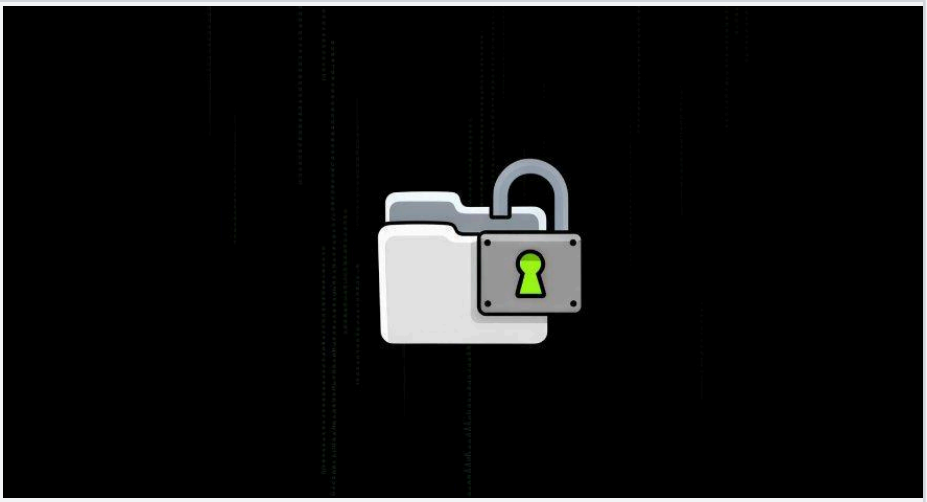


Microsoft, enerji sektöründeki şirketlere yönelik multi-şekil adversary-in-the-middle (AitM) phishing ve iş e-postası irtikâsı (BEC) kampanyasında uyarıda bulundu. Bu kampanyada, SharePoint dosya paylaşım hizmetlerini kötüye kullanarak phishing yüklemelerini teslim ettiler ve kullanıcı farkındalığına karşı kalıcı olmaya çalışarak inbox rule oluşturuldu. İlk olarak, email bir enerji şirketine ait bir email adresinden gönderildi ve ardından bir SharePoint dosya paylaşım akışı olarak sunuldu. Bu nedenle, SharePoint ve OneDrive gibi hizmetlerin işletme ortamlarında yaygın olarak kullanıldığından ve emails, bir yasal adresden gönderildiğinden, bu emails şüphe uyandırmaya uygun değil ve böylece fişin linkleri veya zararlı yüklemeleri teslim ediliyor. Bu yaklaşım, "living-off-trusted-sites" (LOTS) olarak da adlandırılıyor, çünkü böyle platformların aşikâr ve yaygın kullanımını silahlandırıyor ve email-merkezli algılamaların altını oynamaya çalışıyor.

THE HACKER NEWS

2026-01-22 15:00 UTC

10. New Osiris Ransomware Emerges as New Strain Using POORTRY Driver in BYOVD Attack

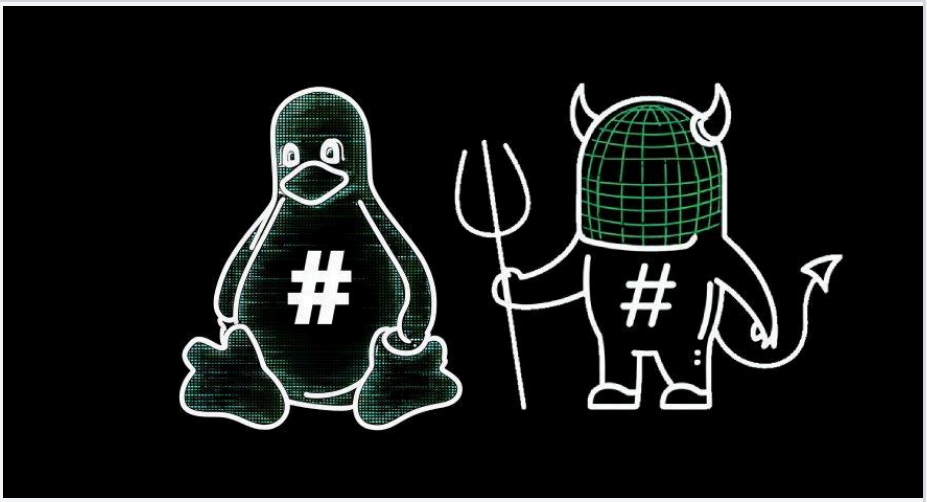


Yeni bir Osiris ransomware ailesinin ortaya çıktığı ve Kasım 2025'de Güneydoğu Asya'daki bir gıda hizmet şirketi operatörünü hedef aldığı bildirildi. Bu saldırı, bilinen bir tekniği kullanarak, güvenlik yazılımını disarman etmek için POORTRY adlı bir zararlı sürücü kullandı. Osiris, Locky ransomware'nin bir varyantı olarak Aralık 2016'da ortaya çıkan diğer bir Osiris varyantına benzemez. Şu anda, bu locker'un geliştiricilerinin kim olduklarını veya ransomware-as-a-service (RaaS) olarak pazarlandığını bilmiyoruz. Saldırı, geniş bir yelpaze yaşayan ve çift kullanımlı araçlar kullanılarak gerçekleştirildi. Bu araçlar arasında POORTRY sürücüsü, güvenlik yazılımını disarman etmek için BYOVD saldırısı olarak kullanıldı. attackers, data'sını Wasabi depolama kutularına sızdırarak ve INC ransomware'sını kullanan saldırılar ile olası bağlantılar gösterir.

THE HACKER NEWS

2026-01-22 13:30 UTC

11. Critical GNU InetUtils telnetd Flaw Lets Attackers Bypass Login and Gain Root Access



Aşağıdaki metni Türkçe olarak yeniden yazdım: GNU InetUtils telnetd'de kritik bir güvenlik açığı tespit edildi. Bu açığın, 11 yıl boyunca fark edilmeden kalmış olduğu belirtiliyor. Açığın, CVSS puanlama sisteminde 9,8/10 olarak değerlendiriliyor. Tüm GNU InetUtils sürümleri, 1.9.3'ten 2.7'ye kadar etkilendi. Açığın, telnetd sunucusunun, USER ortam değişkenini client'tan aldığı bir değer olarak işleme yapması ve bu değer "-f root" olarak ayarlanırsa, client otomatik olarak root olarak giriş yapabiliyor. Bu, telnetd sunucusunun USER ortam değişkenini temizlemeden login(1)'e göndermesi ve login(1)'in normal authentication prosedürlerini atlaması sonucu oluyor. Güvenlik araştırmacısı Kyu Neushwaistein (Carlos Cortes Alvarez olarak da bilinen), Ocak 19, 2026'da açığı keşfetmiş ve bildirmiş.

THE HACKER NEWS

2026-01-22 11:23 UTC

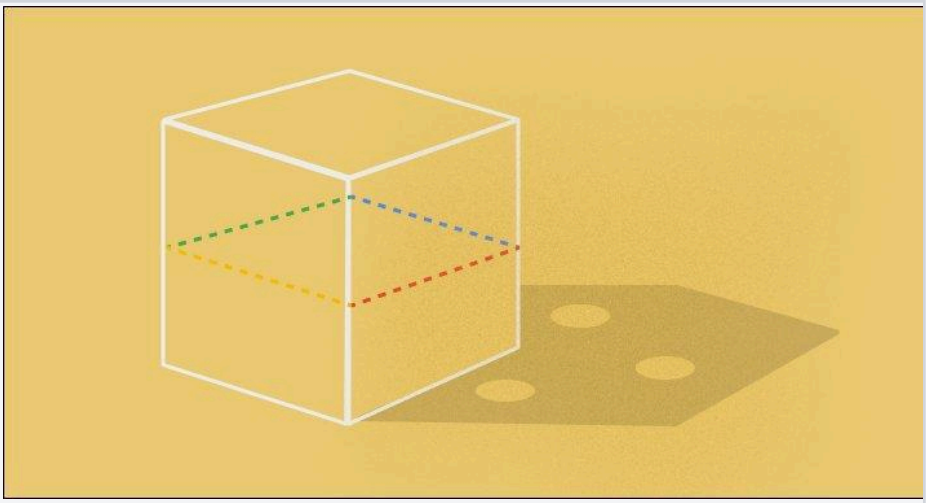
12. ThreatsDay Bulletin: Pixel Zero-Click, Redis RCE, China C2s, RAT Ads, Crypto Scams & 15+ Stories

Haber Özeti: Bu haftaın tehditleri yeni tripler yerine, bilinen sistemlerin tasarımında doğru ellerde davranmasına dayanıyordu. Normals files, routine services ve güvenilir workflow'lar, saldırıların kapılarını açmaya yeterli oldu. Attacks'in vurgusu, ölçek, sabrı ve yanlış güven sayesinde kazanılan kontroldü. Aşağıdaki haberler, bu güvenin nasıl büküldüğünü değil, nasıl kırıldığını gösterir. Her bir madde, daha büyük bir değişimin küçük bir sinyalidir ve birlikte görüldüğünde daha iyi anlaşılmaktadır. Afghanistan hükümetinin hedefi olan bir spear-phishing kampanyası, FALSECUB adlı bir backdoor'ü dağıtmaya çalıştı. Kampaınlara, GitHub'de barındırılmış ISO image dosyası aracılığıyla gerçekleştirildi. İnceleme, Aralık 2025'in sonlarında başladı. Bir başka tehdit, UK hükümetinin kritik altyapısını ve yerel hükümet organizasyonlarını hedef alan Rus-backed hacktivist gruplarının DoS saldırılarıydı.

THE HACKER NEWS

2026-01-22 08:30 UTC

13. Filling the Most Common Gaps in Google Workspace Security



Google Çalışma Alanı Güvenlik Açıklarını Doldurmak Sürdürülebilirlik olmadan hızlanan şirketlerin güvenlik ekibi, işlemini yavaşlatmadan iş güvenliğini sağlamaya çalışır. Ancak, çoğu ekibin teknoloji sağlamada değil, dayanıklılık için optimize edildiği bir geçmişe sahiptir. Google Çalışma Alanı, güvenlik temeli sağlar ancak varsayılan araçları sınırlandırır ve bunların kullanımı sakıncalıdır. Bir gerçekten dayanıklı program oluşturmak için, çalışma alanını korumaya başlamadan önce bazı ortak anlamlı ilk adımların alınması gerekir. E-posta, saldırı vektörü ve arşiv olarak en büyük hedeftir. Gmail'in varsayılan güvenliği, bazı tehditleri yakalamaya yardımcı olur, ancak hedefli tehditler, sofistike sosyal mühendislik ve yük olmadan saldırılar için genellikle başarısız olur. Google Çalışma Alanı'nı korumaya başlamadan önce, çalışma alanını inteligent bir şekilde artırarak, eksiklikler giderilmeli ve e-posta güvenliği, veri arşivinin güvenliği, multi-factor authentication (MFA) ve erişim kontrolü gibi kritik alanlarda iyileşme sağlanmalıdır.

THE HACKER NEWS

2026-01-22 07:04 UTC

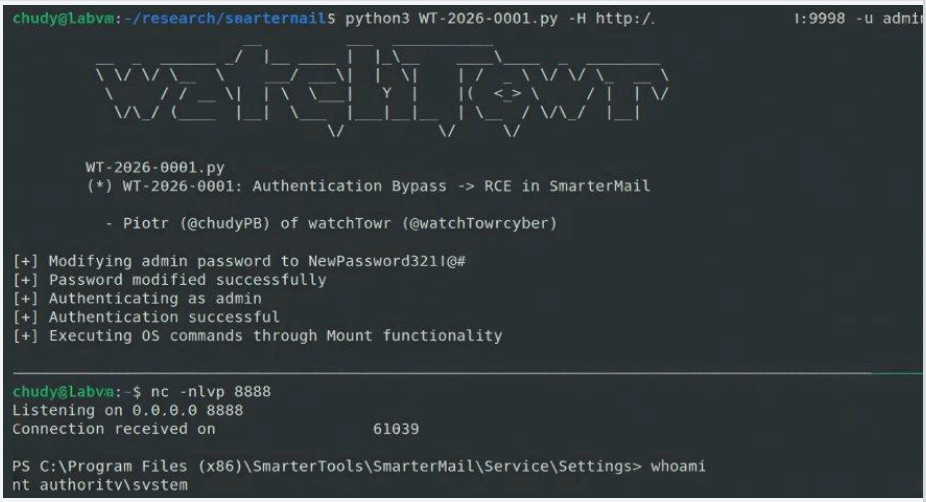
14. Malicious PyPI Package Impersonates SymPy, Deploys XMRig Miner on Linux Hosts

Aşağıdaki metni Türkçe olarak yeniden yazdım: PyPI'de bulunan bir malicious paket, Linux sunucularında XMRig madenciliği için çalışan bir miner deploy etmeye çalışmaktadır. Paket, SymPy adlı bir popüler matematiksel kütüphane tarafından imitasyon edilmektedir. "Geliştirme sürümü" olarak sunulan paket, kullanıcıları yanıltmaya çalışmaktadır. Paket, 17 Ocak 2026'dan beri 1,100'den fazla kez indirilmiştir. Bu indirme sayfası, enfeksiyon sayısını belirlemek için güvenilir bir ölçüt değildir. Paket, mevcut yazım tarihine kadar indirilebilmektedir. Paket, Socket firması tarafından analiz edildiğinde, compromised sistemlerde XMRig madenciliği için kullanılan bir downloader olarak modifiye edilmiştir. Malicious behavior, belirli polinomal işlemler çağrıldığında tetiklenmektedir.

THE HACKER NEWS

2026-01-22 06:46 UTC

15. SmarterMail Auth Bypass Exploited in the Wild Two Days After Patch Release



Aşağıdaki haber özeti Türkçe olarak yeniden yazılmıştır: SmarterMail'de bir güvenlik açığı,_patchesinin yayınlanmasından iki gün sonra aktif olarak saldırıya uğradı. Bu güvenlik açığı, SmarterTools'un SmarterMail email yazılımında yer alıyor ve şu anda bir CVE numarası yok..watchTowr Labs tarafından WT-2026-0001 olarak takip ediliyor. Güvenlik açığı, SmarterMail sistem yöneticisi parolasını resetlemek için özel olarak hazırlanmış bir HTTP isteğiyle ulaşılabilen bir kimlik doğrulama atlama açığıdır. Bu açığı kullanarak, herhangi bir kullanıcı, SmarterMail sistem yöneticisi parolasını resetleyebilir. Ayrıca, bu kullanıcı, RCE-as-a-feature fonksiyonlarını kullanarak doğrudan işletim sistemi komutlarını çalıştırabilir. Güvenlik açığı, "SmarterMail.Web.Api.AuthenticationController.ForceResetPassword" fonksiyonunda yer alıyor ve bu fonksiyon, kimlik doğrulama gerektirmeden endpoint'e ulaşılabilmesine ve bir boolean bayrak ("IsSysAdmin") kullanarak isteği işleme sürecini belirlemeye yarıyor.

KREBS ON SECURITY

2026-01-20 15:19 UTC

16. Kimwolf Botnet Lurking in Corporate, Govt. Networks

Türkiye'deki 2 milyon cihazın üzerinde IoT cihazına bulaşan yeni bir botnet, Kimwolf, 20 Ocak 2026'da meydana gelen DDoS saldırilerine katılıyor ve kötü amaçlı internet trafiğini yönlendiriyor. Kimwolf'un yerel ağlarda diğer IoT cihazlarını enfekte etmek için tarayabilmesi, kuruluşlar için ciddi bir tehdit oluşturuyor. Yeni araştırmalar, Kimwolf'un governo ve şirket ağlarında özellikle yaygın olduğunu gösteriyor. Kimwolf, Aralık 2025'de, çeşitli "residential proxy" hizmetlerini kandırmak ve bunları kötü amaçlı komutları cihazlarına göndermek için kullandı. Bu hizmetler, anonim ve yerel web trafiğini bir bölgeye yönlendirmek için satılıyor ve en büyük hizmetler, müşterilerin herhangi bir ülke veya şehirde bulunan cihazları aracılığıyla

internet aktivitesini yönlendirmelerine izin veriyor. Malware, genellikle mobil uygulamalar ve oyunlar ile birlikte saklanıyor ve enfekte edilen cihazları kötü amaçlı ve abusif trafiği yönlendirmeye zorlıyor.