MOBIL QURILMALARDA XAVFLI URL'LARNI KO'P QATLAMLI SANDBOX TAHLILI: OFFLINE EVRISTIKA, URLHAUS, GOOGLE SAFE BROWSING VA VIRUSTOTAL INTEGRATSIYASI

Erkinov Shohjahon Sherali o'g'li
Axmatov Bekzod Nurali o'g'li
Ramazonova Marjona Ikrom qizi
Saidov O'lmasbek Azamatovich
Muhammad al-Xorazmiy nomidagi TATU talabasi

Annotatsiya. Tezis mobil qurilmalarda foydalanuvchiga kelayotgan URL havolalarni avtomatik xavfsizlik bahosi orqali aniqlashning ko'p qatlamli sandbox arxitekturasiga bag'ishlangan. Yondashuv to'rt mustaqil tahlil qatlamini birlashtiradi: offline evristika, URLhaus bazasi, Google Safe Browsing API v4 va VirusTotal ko'plab antivirus mexanizmlari orqali tekshirish. Tizim qisqartirilgan havolalarni haqiqiy manzilga ochib beradi, qatlamlar natijasini kombinatsion bonus bilan birlashtiradi va 24 soatlik LRU keshda saqlaydi. Foydalanuvchi xabar mazmuni tashqariga uzatilmaydi, faqat URL'ning o'zi uchinchi tomon API'lariga jo'natiladi. To'liq sinov natijalari 97% F1-score va 1.2% false-positive nisbatini ko'rsatadi.

Kalit so'zlar: URL xavfsizligi, sandbox tahlili, fishing havolalar, threat intelligence, URLhaus, Google Safe Browsing, VirusTotal, homoglyph hujumi, IDN spoofing, LRU kesh, mobil xavfsizlik, ko'p qatlamli aniqlash.

Aksariyat zamonaviy kiber-hujumlar bitta umumiy boshlanish nuqtasiga ega — foydalanuvchiga yuborilgan xavfli URL havola. MITRE ATT&CK matritsasidagi T1566 "Phishing" texnikasi ostida URL'lar credential harvesting yoki malware tarqatishning birinchi bo'g'inini ta'minlaydi. APWG hisobotlariga ko'ra, har chorakda yangi fishing domenlarining soni millionlab birlik hisobida o'lchanmoqda va ularning o'rtacha hayot davri bir kundan kam — bu klassik qora ro'yxat yondashuvini samarasiz qilib qo'yadi va dinamik tekshirish vositalarining zaruriyatini keltirib chiqaradi. Mobil qurilmalardagi tahlil qo'shimcha cheklovlarga ega: tarmoq pasayuvchanligi, batareya iqtisodi, API kvota chegaralari va past kechikish talabi.

Birinchi qatlam — offline evristika. Tashqi tarmoqqa murojaat qilmasdan URL strukturasini tahlil qiladi: shubhali yuqori darajadagi domenlar (.xyz, .top, .click, .gq, .tk), homoglyph hujumlari (Unicode Technical Standard #39 dagi confusables jadvali asosida), URL ichidagi IP-manzil, anormal uzunlik (200 belgidan ortiq), hamda "hxxp://" kabi obfuskatsiyalangan sxemalar. Eng arzon qatlam, ishlash vaqti — 5 millisekunddan kam.

Ikkinchi qatlam — URLhaus xavfli URL bazasi. abuse.ch tashkiloti tomonidan boshqariladigan, malware tarqatuvchi URL'larning ochiq bazasi. Har 5 daqiqada yangilanadi va malware oilasi nomini (Emotet, IcedID, AgentTesla va boshqalar) qaytaradi. Javob vaqti 100–300 ms atrofida bo'ladi. URLhaus boshqa xizmatlarga qaraganda malware kontekstida aniqroq indikatorlar taqdim etadi.

Uchinchi qatlam — Google Safe Browsing API. 2007-yildan beri faoliyat ko‘rsatayotgan eng katta xavfli URL bazasi. API v4 to‘rtta tahdid sinfini qaytaradi: MALWARE, SOCIAL_ENGINEERING, UNWANTED_SOFTWARE va POTENTIALLY_HARMFUL_APPLICATION. Bepul kvota — 10 000 ta URL/kun, javob vaqti 150–400 ms.

To‘rtinchi qatlam — VirusTotal ko‘plab antivirus mexanizmlari orqali tekshirish. URL’ni 70 dan ortiq mustaqil antivirus va xavfsizlik mexanizmida bir vaqtda tekshiradi. Public API kvotasi juda chekli (500 so‘rov/kun), shuning uchun bu qatlam faqat foydalanuvchi qo‘lda “deep scan” tugmasini bosgan paytda ishga tushiriladi. Detection ratio 5/70 dan yuqori bo‘lsa, URL aniq xavfli deb belgilanadi.

URL Expander va qatlamlarni birlashtirish. Tekshirishdan oldin URL Expander qisqartirilgan havolalarni (t.me, bit.ly, tinyurl, goo.gl) HTTP HEAD so‘rovlari ketma-ketligi orqali oxirgi manzilga ochib beradi. Yakuniy bal formulasi: yakuniy_bal = max(barcha qatlam ballari) + kombinatsion_bonus, bunda ikkitadan ortiq qatlam tahdid topgan bo‘lsa +8 ball, uchtadan ortiq bo‘lsa qo‘shimcha +5 ball qo‘shiladi. Tasnif uch darajaga ajratiladi: 0–39 XAVFSIZ, 40–69 SHUBHALI, 70–100 XAVFLI.

LRU kesh va privatsiya kafolatlari. URL’lar takror tahlilini oldini olish uchun tizim 100 ta yozuv sig‘imli 24 soatlik LRU keshni saqlaydi. Amaliyotda keshning samaradorligi 60–70% atrofida bo‘ladi va API kvotalarini sezilarli darajada tejaydi. Privatsiya invariantiga binoan, uchinchi tomon API’lariga faqat URL’ning o‘zi uzatiladi — xabar matni, telefon raqami yoki qurilma identifikatori hech qachon jo‘natilmaydi. Mahalliy kesh foydalanuvchi qurilmasidan tashqariga chiqmaydi va backup’lardan istisno qilinadi.

Amaliy natijalar. 5 000 ta URL’dan iborat aralash test korpusi (PhishTank, OpenPhish, URLhaus va Tranco Top sites) ustida sinovlar o‘tkazildi. Faqat offline evristika 78% F1-score ko‘rsatdi, URLhaus va Safe Browsing kombinatsiyasi 91% F1 ga yetdi, to‘liq to‘rt qatlamli tahlil (deep scan rejimida) 97% F1-score va 1.2% false-positive nisbatini ko‘rsatdi. Umumiy kechikish ketma-ket rejimda 350–600 ms, parallel rejimda esa 200–350 ms gacha qisqaradi — bu foydalanuvchi tajribasiga sezilarli ta’sir qilmaydi.

Xulosa qilib aytganda, ko‘p qatlamli URL sandbox arxitekturasi mobil qurilmalarda foydalanuvchini fishing va malware havolalardan himoya qilishning amaliy va kvota-samarali yo‘lidir. Yondashuvning asosiy ustunligi har bir qatlamning o‘ziga xos kuchli tomonini birlashtirish va bir-birining zaif tomonini qoplashidir: offline evristika tezkor va arzon, URLhaus malware kontekstida aniq, Safe Browsing keng qamrov beradi, VirusTotal esa ko‘p mustaqil mexanizm xulosasi orqali ishonchni mustahkamlaydi. Kelajakda DNS-over-HTTPS integratsiyasi, mahalliy ML modelni offline qatlamga qo‘shish va Certificate Transparency loglarini kuzatish yo‘nalishlari ko‘rib chiqilishi mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. MITRE ATT&CK Framework: Initial Access -- Phishing (T1566). -- The MITRE Corporation, 2024. -- URL: https://attack.mitre.org/techniques/T1566/
2. URLhaus -- abuse.ch threat intelligence platform. -- abuse.ch, 2024. -- URL: https://urlhaus.abuse.ch/

3. Google Safe Browsing API v4 Reference. -- Google Developers, 2024. -- URL: https://developers.google.com/safe-browsing/v4
4. VirusTotal Public API v3 Documentation. -- VirusTotal (Google), 2024. -- URL: https://docs.virustotal.com/
5. Unicode Technical Standard #39: Unicode Security Mechanisms. -- Unicode Consortium, 2023. -- URL: https://www.unicode.org/reports/tr39/
6. APWG Phishing Activity Trends Report. -- Anti-Phishing Working Group, 2024. -- URL: https://apwg.org/trendsreports/
7. Pochat V. L. et al. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. // NDSS Symposium. -- 2019.