ACCCF / अनुप्रयुक्त ज्ञान पुस्तकालय

13

खंड

हटाने या आरोप लगाने से पहले सुरक्षित निर्णय

स्पेनिश संस्करण · 2026

डिजिटल निगरानी का संदेह: Zero Breach Toolkit से जाँच और संरक्षण की मार्गदर्शिका

संकट, गलत संकेत, सत्यापित डाउनलोड, गोपनीयता, रिपोर्ट पढ़ना और विशेषज्ञ को सौंपना

चिंतित व्यक्ति की सरल चरणों से संकेतों की जाँच करने में सहायता करना, बिना साक्ष्य नष्ट किए या कोई और जोखिम इंस्टॉल किए; मामले की समीक्षा करने वाले के लिए पुनरुत्पाद्य अनुलग्नक सहित।

अपने फ़ोन या कंप्यूटर को लेकर चिंतित किसी भी व्यक्ति और ऐसे मामले पाने वाले फोरेंसिक विशेषज्ञों के लिए। इसके लिए घुसपैठ, भौतिक निष्कर्षण, JTAG या chip-off का ज्ञान आवश्यक नहीं है। स्थानीय जाँच वैकल्पिक है; सहायता माँगना कभी भी उसे पूरा करने पर निर्भर नहीं है।

संपादकीय समन्वय: Jocsan Laguna · अमेरिकन साइबर सुरक्षा और कंप्यूटर फोरेंसिक परिषद

सामान्य तकनीकी मार्गदर्शिका और खुली शैक्षिक सामग्री। यह कानूनी सलाह, फोरेंसिक विशेषज्ञ की राय या बिना अधिकार के सिस्टम तक पहुँचने का निर्देश नहीं है। उदाहरण और डेटा काल्पनिक हैं; आकृतियाँ संपादकीय पुनर्निर्माण हैं।

विषय-सूची

दिखाई देने वाली पृष्ठ संख्या PDF संस्करण से संबंधित है। Word दस्तावेज़ खुलने पर इस अनुक्रमणिका को अद्यतन कर सकता है; शीर्षक आंतरिक नेविगेशन बनाए रखते हैं।

1. कुछ भी छूने से पहले: सुरक्षा और संयम 3

2. सामान्य व्यवहार जो जासूसी जैसे लग सकते हैं 4

- **2.1 एक संकेत एक व्याख्या नहीं है** 4
- **2.2 फ़ॉल्स पॉज़िटिव का अर्थ कल्पना करना नहीं है** 4

3. Zero Breach क्या करता है और कब उसका उपयोग न करें 5

- **3.1 प्रकाशित संकेतकों की स्थानीय जाँच** 5
- **3.2 कब रुकें और मदद मांगें** 5

4. पैकेज डाउनलोड और सत्यापन 6

- **4.1 आधिकारिक रिपॉज़िटरी, अग्रेषित लिंक नहीं** 6
- **4.2 Windows एक्ज़ीक्यूटेबल का सत्यापन** 6
- **4.3 विकल्प: स्रोत कोड और पुनरुत्पाद्य तुलना** 6

5. निष्पादन से पहले गोपनीयता और तैयारी 7

- **5.1 स्थानीय होने का अर्थ हानिरहित होना नहीं है** 7
- **5.2 फ़ोल्डर और दायरे की तैयारी** 7
- **5.3 पूर्वावलोकन और विवरण** 8

6. चरण-दर-चरण निष्पादन 8

- **6.1 पहले: वास्तविक डिवाइस की जाँच किए बिना अभ्यास करें** 8
- **6.2 बाद में: अधिकृत स्थानीय समीक्षा** 8
- **6.3 यदि आप एक फोन चुनते हैं** 9

7. रिपोर्ट साझा करने से पहले कैसे पढ़ें 9

- **7.1 परिणाम, साक्ष्य-स्तर, दायरा और जाँच-रिक्तियाँ** 9
- **7.2 कोड और परिचालन अर्थ** 9
- **7.3 “Worth a look” कोई निर्णय नहीं है** 10

8. प्रयोगशाला के चार परिदृश्य 11

- **8.1 `spyware`: छह निष्कर्ष, कोई जल्दबाजी निष्कर्ष नहीं** 11
- **8.2 `worth-a-look`: प्रश्न पूछने के लिए, आरोप लगाने के लिए नहीं** 11
- **8.3 `clean`: चार जाँच-रिक्तियों के साथ मेल की अनुपस्थिति** 11
- **8.4 `cellebrite`: फोरेंसिक एक्सेस, स्पाइवेयर नहीं** 11

9. विशेषज्ञ या प्रतिक्रिया टीम को सुरक्षित रूप से सौंपना 15

- **9.1 पहले सारांश, फिर पूरी केस फ़ाइल** 15
- **9.2 सत्यापन योग्य डिलीवरी के लिए हैश और EML** 16
- **9.3 व्याख्या जो दूसरा संकट रोकती है** 16

अनुलग्नक A. विशेषज्ञ के लिए पुनरुत्पाद्य प्रोटोकॉल 16

- **A.1 वातावरण और उत्पत्ति का रिकॉर्ड** 16
- **A.2 वास्तविक अधिकृत निष्पादन की फ़ॉर्म** 17
- **A.3 व्याख्या की मैट्रिक्स** 17

अनुलग्नक B. कानूनी ढाँचा, गोपनीयता और अंतिम जाँच 17

1. कुछ भी छूने से पहले: सुरक्षा और संयम

यदि आपको लगता है कि कोई आपके फ़ोन या कंप्यूटर की निगरानी कर रहा है, तो पहला काम कोई प्रोग्राम डाउनलोड करना नहीं है। पहले यह रोकें कि जल्दबाजी में जानकारी नष्ट हो या कोई और समस्या पैदा हो। फ़ाइलें न हटाएँ, डिवाइस रीसेट न करें, चमत्कारी सुइट इंस्टॉल न करें और किसी अजनबी को दूरस्थ पहुँच से डिवाइस नियंत्रित न करने दें। चिंता का कारण कोई वैध स्थिति, कॉन्फ़िगरेशन या वास्तविक घटना हो सकता है। हम अभी नहीं जानते और इसी मिनट इसका निर्णय करना आवश्यक नहीं है।

यदि शारीरिक खतरा, नाबालिगों के लिए जोखिम, सक्रिय पीछा या ऐसा व्यक्ति हो जो यह जान सकता है कि आप सहायता माँग रहे हैं, तो सुरक्षा और अपने स्थान के आपातकालीन चैनलों को प्राथमिकता दें। केवल इसलिए जाँच न चलाएँ कि यह मार्गदर्शिका मौजूद है। विश्लेषण रिकॉर्ड बदल सकता है, स्थान उपयोग कर सकता है या वातावरण नियंत्रित करने वाले व्यक्ति को अप्रत्यक्ष रूप से सूचित कर सकता है। आगे बढ़ने से पहले सुरक्षित डिवाइस और चैनल से सहायता माँगें।

एक छोटी सूची बनाएँ: क्या देखा, कब शुरू हुआ, क्या बदला, क्या इंस्टॉल किया, किसके पास भौतिक पहुँच थी और किन खातों से समझौता हो सकता है। सटीक समय याद न हो तो अनुमानित समय लिखें। सहायता माँगने के लिए अंतरंग सामग्री कैप्चर या अग्रेषित न करें। संदेश, URL, कॉन्फ़िगरेशन, ऐप का नाम और तिथि प्रायः आपके निजी जीवन के पूरे फ़ोल्डर से अधिक उपयोगी होते हैं।

समय से पहले आवश्यक

सांस लें. मत हटाओ, कथित हमलावर का पीछा मत करो और पासवर्ड या कोड साझा मत करो. यदि कोई खतरा है, तो अभी मदद मांगें। यदि समय है, तब न्यूनतम रखें और बिना नाटक किए जांचें। Duriva आपको यह सवाल कई बार पूछेगाः आप क्या साबित कर सकते हैं और क्या केवल संभव लगता है?



चित्र 1. जाच करन स पहल, स्रात खान स बच. प्राथामकता यह साबत करना नहा ह कि आप सहा थ सपादकाय पुनानमाण; यह वास्तावक सबूत नहा ह।

2. सामान्य व्यवहार जो जासूसी जैसे लग सकते हैं

2.1 एक संकेत एक व्याख्या नहीं है

अलग MAC पता, डिस्कनेक्शन, तेज़ी से घटती बैटरी, अप्रत्याशित सूचना, अज्ञात ऐप या नया IP पता अपने आप में यह सिद्ध नहीं करते कि कोई आपकी निगरानी कर रहा है। इनके कारण गोपनीयता सुविधा, अद्यतन, कवरेज, सिंक्रनाइज़ेशन, वैध ऐप या साझा खाता हो सकता है। ये किसी गंभीर घटना का हिस्सा भी हो सकते हैं। स्रोत जाँचने से पहले सबसे डरावनी व्याख्या चुनना गलती है।

Apple के दस्तावेज़ के अनुसार उसके डिवाइस प्रत्येक नेटवर्क के लिए अलग निजी Wi-Fi पते उपयोग कर सकते हैं और संगत सिस्टम में Rotating मोड उन्हें हर दो सप्ताह बदल सकता है। इस सुविधा का उद्देश्य ट्रैकिंग घटाना है, जासूसी सिद्ध करना नहीं। डिस्कनेक्शन एक अलग प्रश्न है: उसमें राउटर, कवरेज, अद्यतन, संगतता, ऊर्जा, सॉफ़्टवेयर या संस्थागत कॉन्फ़िगरेशन की भूमिका हो सकती है। जाँचे बिना उसे एक ही कारण से न जोड़ें।[1]

जो आप देखते हैं	पहली रात जाँचें	समीक्षा करने के लिए क्या रखना है
MAC बदल गया	प्रत्येक नेटवर्क का निजी पता सेटिंग और मॉडल/सिस्टम जाँचें।	कॉन्फ़िगरेशन, नेटवर्क और दिनांक कैप्चर; पूरा इतिहास नहीं।
डिस्कनेक्ट होना	आवृत्ति, अन्य उपकरण, कवरेज, समय और हाल के बदलावों को नोट करें।	मॉडल, सिस्टम, राउटर, पटल और म्यूटेशन; कोई Wi-Fi पासवर्ड नहीं।
बैटरी तेज़ी से घटती है	ऐप, सिग्नल, तापमान और अपडेट के आधार पर खपत की जांच करें।	सिस्टम और अपवाद के आंकड़े; पटल सामग्री नहीं।
चेहरा बदला	सिंक्रनाइज़ेशन, अन्य डिवाइस और लिंक किए गए खाते जाँचें।	प्रोफ़ाइल, संस्करण, समय, खाता और संपर्क संबंध।
सुरक्षा अलर्ट	पढ़ें कि ठीक किस फ़ाइल या व्यवहार का पता लगाता है और उसका कौन-सा संस्करण मौजूद है।	पूर्ण पंजीकरण, मार्ग, तिथि और स्पष्टीकरण; फ़ाइल को निष्पादित न करें।
रात को गतिविधि	अद्यतन, बैकअप, फ़ोन और मौसम पहुँच को अलग करें।	रिकॉर्ड, लॉक स्थिति और किसके पास डिवाइस था।

2.2 फ़ॉल्स पॉज़िटिव का अर्थ कल्पना करना नहीं है

फ़ॉल्स पॉज़िटिव वह अलर्ट है जो डरी गई समस्या को नहीं दर्शाता, लेकिन हर असामान्य व्यवहार फ़ॉल्स पॉज़िटिव नहीं होता और बिना निष्कर्ष वाला हर परिणाम भी फ़ॉल्स पॉज़िटिव नहीं है। व्यक्ति को यह नहीं कहना चाहिए कि वह चीज़ें कल्पना कर रहा है; उसे यह जानना चाहिए कि कौन-सी जाँच व्याख्या बदल सकती है। यदि कॉन्फ़िगरेशन डेटा समझाता है तो उसे दस्तावेज़ित करें। यदि नहीं समझाता तो बिना दोषारोपण या जल्दबाज़ी के निष्कर्ष निकाले आगे जाँच करें।

> **सहायक वाक्य**
> “इसकी कोई सामान्य व्याख्या भी हो सकती है। इसे जासूसी कहने से पहले मैं उसकी जाँच करूँगा/करूँगी।” और भी: “यदि व्याख्या मेल नहीं खाती, तो मैं स्रोत संरक्षित रखूँगा/रखूँगी ताकि कोई योग्य व्यक्ति उसकी समीक्षा कर सके।”

[1] Apple Support. Use private Wi-Fi addresses on Apple devices: निजी पता नेटवर्क के अनुसार बदल सकता है और संगत सिस्टम में Rotating के साथ हर दो सप्ताह बदल सकता है। इस सुविधा का उद्देश्य ट्रैकिंग घटाना है; यह जासूसी का साक्ष्य नहीं है और सभी डिस्कनेक्शन की व्याख्या भी नहीं करती। आधिकारिक ऑनलाइन स्रोत



आकृति 2. कोई संकेत व्याख्या नहीं होता। पहले जाँच की जाती है; फिर व्याख्या की जाती है। संपादकीय पुनर्संरेखण; यह वास्तविक साक्ष्य नहीं है।

3. Zero Breach क्या करता है और कब उसका उपयोग न करें

3.1 प्रकाशित संकेतकों की स्थानीय जाँच

Zero Breach Toolkit निःशुल्क, ओपन-सोर्स टूल है जो कंप्यूटर, Android संग्रहों और iPhone बैकअप में कुछ spyware के दस्तावेज़ित संकेतक खोजता है। यह फ़ाइलों, ब्राउज़रों, पर्सिस्टेंस रिकॉर्ड और अन्य समर्थित आर्टिफैक्ट की जाँच कर सकता है। यह पूर्ण फोरेंसिक परीक्षण नहीं है, हर तरह की निगरानी का पता नहीं लगाता और कुछ न मिलने से सुरक्षा सिद्ध नहीं होती।[2][3]

यह टूल तब विशेष रूप से उपयोगी है जब आप ज्ञात संकेतकों की पहली स्थानीय समीक्षा और जाँची न जा सकी वस्तुओं की स्पष्ट सूची चाहते हैं। इसका मूल्य “कोई भूत-प्रेत नहीं” कहना नहीं, बल्कि मेल, कमज़ोर संदर्भ, जाँच-रिक्तियाँ और विशेषज्ञ के प्रश्नों को अलग करना है। नए या अज्ञात स्रोत प्रकाशित संकेतकों के आधार में स्वतः नहीं आ जाते और कुछ निशान समय के साथ गायब हो जाते हैं।

3.2 कब रुकें और मदद मांगें

यदि जाँच से आपको खतरा हो सकता है, डिवाइस या फ़ाइलों पर आपका अधिकार नहीं है, कोई दूसरा प्रक्रिया देख सकता है या रिपोर्ट सुरक्षित नहीं रख सकते, तो जाँच न चलाएँ। अपने साथी, कर्मचारी, ग्राहक या परिजन के डिवाइस की बिना अनुमति जाँच के लिए भी इसका उपयोग न करें। किसी फ़ाइल को पढ़ सकना आपको उसकी सामग्री का अधिकृत धारक नहीं बनाता।

यदि विश्वसनीय सुरक्षा सूचना, पुष्ट निष्कर्षण या लक्षित होने की चिंता पहले से है, तो अपनी समीक्षा पूरी करने की प्रतीक्षा किए बिना विशेषज्ञ सहायता लें। पत्रकार, कार्यकर्ता, मानवाधिकार रक्षक और नागरिक समाज Access Now की सहायता लाइन या Amnesty International Security Lab से संपर्क कर सकते हैं; इनके लिंक स्वयं रिपोर्ट में हैं। किसी भी अन्य व्यक्ति के लिए घटना-प्रतिक्रिया विशेषज्ञ या योग्य फोरेंसिक विशेषज्ञ उपयुक्त मार्ग है।[4]

[2] Zero Breach Toolkit, रिपॉज़िटरी interplains/Zero-Breach-Toolkit। प्रकाशित spyware संकेतकों की स्थानीय जाँचें, Apache 2.0 के अंतर्गत कोड तथा दायरे और सीमाओं का दस्तावेज़ीकरण। आधिकारिक ऑनलाइन स्रोत

[3] Zero Breach Toolkit। जाँच-परिवारों के अनुसार कवरेज और सीमाएँ: फ़ाइलें, ब्राउज़र, पर्सिस्टेंस, रजिस्टर, Android और iPhone बैकअप। यह पहचान या फ़ॉल्स पॉज़िटिव की दरें नहीं मापता। आधिकारिक ऑनलाइन स्रोत

[4] Zero Breach Toolkit। प्रशिक्षण के काल्पनिक परिदृश्यों की मार्गदर्शिका: spyware, worth-a-look, clean और cellebrite। संकेतक काल्पनिक हैं और उदाहरण डिवाइस या वास्तविक सूचियाँ नहीं पढ़ते; इनसे वास्तविक डिवाइस की स्थिति का अनुमान नहीं लगाया जा सकता। आधिकारिक ऑनलाइन स्रोत

स्थिति	सबसे पहले क्या करना है	क्या न करें
जटिल व्यवहार से जिज्ञासा	स्कैन से पहले कॉन्फ़िगरेशन और फोलिक्रम जोड़ें।	बहुत सारे उपकरण यादृच्छिक रूप से स्थापित करना।
तकनीकी सेवा और सुरक्षित वातावरण	निवारित दोषों और गोपनीयता के लाभ स्थानांतरित करें।	पूरा रिपोर्ट किसी समूह में साझा करना।
जोखिम का सक्रिय निगरानी	विशेष सहायता और सुरक्षित डिवाइस/ पैनल।	ऐसा जोर चलाना जिससे परिसर को पता चल सके।
किसी दूसरे व्यक्ति का डिवाइस	स्पष्ट अधिकार और दस्तावेज़ित दायरा।	केवल इसलिए सामग्री पढ़ना कि वह उपलब्ध है।
मालवेयर का पाठ्यक्रम का अभ्यास	जनसांख्यिकीय काल्पनिक परिदृश्य, वास्तविक डिवाइस नहीं।	प्रशिक्षण को वास्तविक पहचान के रूप में प्रस्तुत करना।

आपको हैकर बनने की जरूरत नहीं है

Test point करना, प्रोसेसर से प्रवेश या chip-off करना आवश्यक नहीं है। यदि सरल जाँच उत्तर न दे, तो साक्ष्य संरक्षित करें और मामला विशेषज्ञ को भेजें। सहायता माँगने के लिए तकनीकी जटिलता आवश्यक नहीं है।

4. पैकेज डाउनलोड और सत्यापन

4.1 आधिकारिक रिपॉज़िटरी, अग्रेषित लिंक नहीं

इस मार्गदर्शिका में उपयोग किया स्रोत `github.com/interplains/Zero-Breach-Toolkit` है। वहीं से Releases खोलकर Windows, macOS या Linux के संबंधित पैकेज या स्रोत कोड डाउनलोड करें। वीडियो, शॉर्टनर, स्क्रीनशॉट या टिप्पणी से एक जैसे नाम की फ़ाइल डाउनलोड न करें। समान नाम यह सिद्ध नहीं करता कि सामग्री भी समान है।[5]

प्रोजेक्ट के दस्तावेज़ बताते हैं कि Windows प्रोग्राम कोड प्रमाणपत्र से हस्ताक्षरित नहीं है। इसलिए SmartScreen या एंटीवायरस चेतावनी दे सकता है। सुरक्षा अक्षम न करें या अंधविश्वास से फ़ाइल स्वीकार न करें। प्रोजेक्ट बिल्ड वर्कफ़्लो का अटेस्टेशन और नए प्रोग्रामों के लिए हस्ताक्षरित SHA-256 मैनिफ़ेस्ट देता है। चलाने से पहले सत्यापित करें।[6]

4.2 Windows एक्ज़ीक्यूटेबल का सत्यापन

GitHub CLI स्थापित और वर्तमान फ़ोल्डर में डाउनलोड किए गए एक्जीक्यूटेबल के साथ, प्रलेखन इस मूल सत्यापन की पेशकश करता है:

अटेस्टेशन का सत्यापन, मालवेयर की अनुपस्थिति का नहीं

```
gh attestation verify zero-breach-toolkit-windows-x64.exe --repo interplains/Zero-Breach-Toolkit
```

सही अटेस्टेशन उन बाइट्स को सार्वजनिक बिल्ड वर्कफ़्लो और commit से जोड़ता है। यह सिद्ध नहीं करता कि प्रोग्राम में त्रुटियाँ नहीं हैं या वह आपकी स्थिति के लिए उपयुक्त है। प्रोजेक्ट द्वारा बताए गए हस्ताक्षरित SHA-256 मैनिफ़ेस्ट भी उपयोग किए जा सकते हैं। किसी दूसरे पेज पर मिले hash को अपनी फ़ाइल का न मानें: अपनी फ़ाइल का hash निकालें और उस संस्करण के संबंधित आधिकारिक स्रोत से तुलना करें।

4.3 विकल्प: स्रोत कोड और पुनरुत्पाद्य तुलना

दूसरा मार्ग रिपॉज़िटरी क्लोन करना, कोड की समीक्षा करना और उत्पन्न Python फ़ाइल की तुलना अपेक्षित संस्करण से करना है। प्रोजेक्ट एकल फ़ाइल का नियतात्मक बिल्ड और प्रकाशन सत्यापन बताता है। गैर-तकनीकी व्यक्ति के लिए कंपाइल करना अनिवार्य

[5] Zero Breach Toolkit, रिपॉज़िटरी interplains/Zero-Breach-Toolkit। प्रकाशित spyware संकेतकों की स्थानीय जाँचें, Apache 2.0 के अंतर्गत कोड तथा दायरे और सीमाओं का दस्तावेज़ीकरण। आधिकारिक ऑनलाइन स्रोत

[6] Zero Breach Toolkit। संस्करण सत्यापन मार्गदर्शिका: GitHub Actions से बने प्रोग्रामों का अटेस्टेशन, SHA-256 मैनिफ़ेस्ट और हस्ताक्षर; Windows पैकेज में Windows कोड हस्ताक्षर नहीं है। आधिकारिक ऑनलाइन स्रोत

नहीं है: पैकेज सत्यापित करने में सहायता माँग सकता है या मेनू के अभ्यास विकल्प का उपयोग कर सकता है। जल्दबाजी में स्रोत की पहचान का सत्यापन न छोड़ें।

आधिकारिक कोड प्राप्त करने का उदाहरण

```
git clone --depth 1 https://github.com/interplains/Zero-Breach-Toolkit.git
```

Durva पूछता है

वह एक्ज़ीक्यूटेबल ठीक कहाँ से आया? यदि आप रिपॉज़िटरी, संस्करण और सत्यापन के साथ उत्तर नहीं दे सकते, तो अभी उसे चलाने का समय नहीं है।

5. निष्पादन से पहले गोपनीयता और तैयारी

5.1 स्थानीय होने का अर्थ हानिरहित होना नहीं है

सामान्य विश्लेषण आपके डेटा अपलोड या संकेतकों तक पहुँच न करने के लिए डिज़ाइन किया गया है। सूचियों का अद्यतन नेटवर्क उपयोग करता है और Android अधिग्रहण सहमति से अलग कलेक्टर डाउनलोड करता है तथा फ़ोन की स्थिति बदलता है। इसके अतिरिक्त आंतरिक नेटवर्क रोक ऑपरेटिंग सिस्टम का sandbox नहीं है: नेटवर्क माउंट, अन्य ऐप और सिंक्रनाइज़ेशन बने रहते हैं। कठोर पृथक्करण चाहिए तो विशेषज्ञ के साथ तय करें।[7]

रिपोर्ट में उपयोगकर्ता नाम, प्रोफ़ाइल, पथ, इतिहास, SMS प्रेषक और संदेशों के अंश हो सकते हैं। साझा करने के सारांश में कम जानकारी होती है, लेकिन यह पूर्ण फोरेंसिक परीक्षण नहीं है और बिना समीक्षा प्रकाशित नहीं करना चाहिए। स्थानीय, गैर-सिंक्रनाइज़्ड फ़ोल्डर चुनें, OneDrive, iCloud, Dropbox और साझा फ़ोल्डर से बचें और तय करें कि रिपोर्ट कौन खोल सकेगा। रिपॉज़िटरी में कुंजियाँ, cookies, पासवर्ड या व्यक्तिगत फ़ाइलें न भेजें।

5.2 फ़ोल्डर और दायरे की तैयारी

निर्णय	क्या चुनें	क्यों
आउटपुट फ़ोल्डर	स्थानीय, गैर-सिंक्रनाइज़्ड और सीमित पहुँच वाला।	इतिहास और चैट के रिसाव से बचें।
पहला निष्पादन	जब्त पर्यावरण का सीमित दायरा।	एक वास्तविक मामले को जोखिम में डाले बिना रिपोर्ट सीखें।
सक्रिय अद्यतन	एक अलग और सचेत कदम, स्कैन के साथ मिश्रित न करें।	नेटवर्क और स्रोत बदलता है।
खुले ऐप	ब्राउज़र और मैसेजिंग को बंद कर चाय प्रक्रिया पूछता है।	अपरंपरा फ़ाइलें और समयरेखा परिवर्तन को कम करें।
अनुमति	केवल आवश्यक अनुमतियाँ, जोखिमपूर्ण अधिकार न बढ़ाएँ।	जब्त खाते को जोड़ने या सेटिंग्स बदलने से बचें।
परिणाम प्राप्त करने वाले व्यक्ति	जानलेख बनाने से पहले प्राथमिकता और सुरक्षित चैनल।	बाद में जोड़ें न साझा करने से बचें।

[7] Zero Breach Toolkit। PRIVACY: सामान्य विश्लेषण डिज़ाइन के अनुसार अपलोड नहीं करता; अद्यतन और Android अधिग्रहण अलग गतिविधियाँ हैं। रिपोर्ट में संवेदनशील डेटा हो सकता है और साझा करने का सारांश पूरी रिपोर्ट का विकल्प नहीं है। आधिकारिक ऑनलाइन स्रोत

5.3 पूर्वावलोकन और विवरण

वास्तविक डेटा का विश्लेषण करने से पहले दायरे और उपलब्ध जाँचों का पूर्वावलोकन माँग सकते हैं। `--preview` बिना स्कैन किए दायरा दिखाता है; `--describe` JSON में बताता है कि कौन-सी रीडिंग मौजूद हैं और उनकी सीमाएँ क्या हैं। इन चरणों से तय करने में सहायता मिलती है कि जाँच प्रश्न का उत्तर देती है या नहीं और कोई कम आक्रामक विकल्प है या नहीं।[8]

दायरे और रीडिंग का विवरण

```
python -X utf8 scan/zero-breach-toolkit.py --preview
python -X utf8 scan/zero-breach-toolkit.py --describe
```

> **आगे बढ़ने से पहले**
>
> यदि दायरे में ऐसा डेटा है जिसे साझा करना आवश्यक नहीं है, तो चयन घटाएँ। चिंता के लिए सहायता चाहिए तो इन चरणों को पूरा करने के लिए उसे टालें नहीं। टूल एक विकल्प है, अनिवार्यता नहीं।

6. चरण-दर-चरण निष्पादन

6.1 पहले: वास्तविक डिवाइस की जाँच किए बिना अभ्यास करें

प्रोजेक्ट में सीखने के लिए बनाए गए `spyware`, `worth-a-look`, `clean` और `cellebrite` परिदृश्य हैं। इनमें काल्पनिक फ़ोन और संकेतक तथा `.invalid` डोमेन हैं, जो वास्तविक अवसंरचना का हिस्सा नहीं हो सकते। रिपोर्ट में प्रशिक्षण की स्पष्ट चेतावनी होती है और समाप्त होने पर अस्थायी निर्देशिका हटा दी जाती है। ये साझा करने का सारांश या साक्ष्य पैकेज नहीं बनाते, ताकि कोई उन्हें वास्तविक मामला न समझे।[9]

चार अभ्यास परिदृश्य

```
python scan/zero-breach-toolkit.py --training spyware
python scan/zero-breach-toolkit.py --training worth-a-look
python scan/zero-breach-toolkit.py --training clean
python scan/zero-breach-toolkit.py --training cellebrite
```

Windows लॉन्चर उपयोग करें तो मेनू में अभ्यास विकल्प खोजें; दस्तावेज़ उसे `Practise` कहता है। स्रोत कोड उपयोग करें तो रिपॉज़िटरी के फ़ोल्डर से कमांड चलाएँ। `--training` को वास्तविक फ़ाइलों, फ़ोन, अद्यतन या सूचियों के साथ न जोड़ें: प्रोग्राम डिज़ाइन के अनुसार इसे अस्वीकार करता है। पहले जानें कि परिणाम, साक्ष्य-स्तर और जाँच-रिक्तियाँ कहाँ दिखाई देते हैं।

6.2 बाद में: अधिकृत स्थानीय समीक्षा

जब स्रोत सत्यापित हो, प्राधिकरण स्पष्ट हो और आउटपुट फ़ोल्डर संरक्षित हो, तो आप चुने गए दायरे की समीक्षा कर सकते हैं। `--quick` का उपयोग न करें यदि आप जानबूझकर अपूर्ण कवरेज से बचना चाहते हैं। यदि आप एक विशिष्ट लक्ष्य चुनते हैं, तो इसे जानबूजकर चुनें: एक विशिष्ट समीक्षा पूरे डिवाइस की समीक्षा करने के बराबर नहीं है।

रिपोर्ट, JSON और सूचनात्मक सारांश के साथ निष्पादन का उदाहरण

```
python -X utf8 scan/zero-breach-toolkit.py --report reporte.txt --json reporte.json --share-json resumen.json
```

TXT रिपोर्ट पढ़ने, JSON संरचना की समीक्षा और कम खुलाव वाली पहली बातचीत के लिए सारांश उपयोगी है। इनमें से कोई डिवाइस की प्रामाणिकता या पूरे सिस्टम की जाँच सिद्ध नहीं करता। प्रशिक्षण को `--share-json` या साक्ष्य पैकेज के साथ न जोड़ें: ये केवल वास्तविक अधिकृत समीक्षा में बनते हैं।

---

[8] Zero Breach Toolkit। परिणाम और कवरेज का अनुबंध: कोड 0, 1, 2, 3 और 4; निष्कर्ष, संदर्भ, जाँच-रिक्ति, बिना स्कैन आउटपुट और सीमित दायरे में अंतर। बिना मेल वाला परिणाम कभी सुरक्षा की गारंटी नहीं है। आधिकारिक ऑनलाइन स्रोत

[9] Zero Breach Toolkit। प्रशिक्षण के काल्पनिक परिदृश्यों की मार्गदर्शिका: spyware, worth-a-look, clean और cellebrite। संकेतक काल्पनिक हैं और उदाहरण डिवाइस या वास्तविक सूचियाँ नहीं पढ़ते; इनसे वास्तविक डिवाइस की स्थिति का अनुमान नहीं लगाया जा सकता। आधिकारिक ऑनलाइन स्रोत

6.3 यदि आप एक फोन चुनते हैं

Android संग्रह और iPhone बैकअप की समीक्षा एक जैसी नहीं है। टूल उपलब्ध आर्टिफैक्ट पढ़ता है और बताता है कि किस तक पहुँच नहीं सकता। अधिग्रहण फ़ोन की स्थिति बदलता है और निजी जानकारी रखता है; इसे स्पष्ट सहमति, सुरक्षित गंतव्य और कवरेज की समझ के बिना न करें। स्थानीय प्रतिलिपि के लिए पासवर्ड या अलग डिक्रिप्शन चाहिए हो सकता है; उसे साझा या विश्लेषण सेवाओं पर अपलोड न करें।[10][11]

> **सत्य का काई बटन नहा**
> यदि आप नहीं जानते कि अभी कौन-सा दायरा चुना है, तो रुक जाएँ। उत्तर “full” दबाना नहीं, बल्कि यह जानना है कि क्या जाँचा गया और क्या जाँचा नहीं जा सका।

7. रिपोर्ट साझा करने से पहले कैसे पढ़ें

7.1 परिणाम, साक्ष्य-स्तर, दायरा और जाँच-रिक्तियाँ

किसी भी आँकड़े से पहले चार बातें पढ़ें: परिणाम क्या कहता है, उसका साक्ष्य-स्तर क्या है, कौन-सा दायरा जाँचा गया और क्या बाहर रह गया। एक ही संख्या का अर्थ स्रोत के अनुसार बदल सकता है। छह निष्कर्ष छह संक्रमण नहीं हैं, शून्य निष्कर्ष निगरानी की अनुपस्थिति नहीं है और संदर्भ चल रही दुर्भावनापूर्ण फ़ाइल नहीं है।

तत्व	यह क्या बताता है	कौन-सी गुंजाइश रोकता है
परिणाम और कोड	पुन गए निष्पादन में क्या हुआ।	इसे निरपेक्ष लेबल बनाना।
साक्ष्य का स्तर	यह फ़ाइल, रजिस्टर, सेवन, log या अपसंदर्भ है या नहीं।	सब कुछ निष्पादन का साक्ष्य मानना।
सीमा	क्या कौन, फ़ाइल, खाते और विकल्प शामिल हैं।	पूरे डिवाइस पर सामान्यीकरण करना।
जाँच-रिक्तियाँ	क्या पढ़ा या जाँचा नहीं जा सका और क्यों।	जनपद को शुद्ध कहना।
सकतफ और तारीखें	किस स्रोत का उपयोग किया गया है और क्या वे अद्यतित हैं।	हाल की प्रतिलिपि को वर्तमान सकतफ मान लेना।
अगला कदम	मामले के अनुसार सरदात कर, जाँच-रिक्तियाँ पूरी कर या सहायता लें।	प्रतिक्रिया में हटाना या “साफ़” करना।

7.2 कोड और परिचालन अर्थ

कोड / स्थिति	सही व्याख्या	अगला निर्णय
0. कारवाइ योग्य मल या जाँच-रिक्तियाँ नहीं	उस दायरे में कारवाइ योग्य मल नहीं मिला।	इस सुरक्षित डिवाइस से कह, दायरा और चिंता का कारण दोबारा देखें।
1. त्रुटि	निष्पादन या आउटपुट विफल रहा।	इनपुट या गंतव्य ठीक कर, इसे अनुपस्थिति का प्रमाण न मानें।
2. व्यवहार संबंधी	ऐसे संकेत हैं जिनकी व्याख्या और सरदाण की आवश्यकता होती है।	मिटाना, निष्पादित करना या पीछे करना नहीं, मदद मांगना।

[10] Zero Breach Toolkit। जाँच-परिवारों के अनुसार कवरेज और सीमाएँ: फ़ाइलें, ब्राउज़र, पर्सिस्टेंस, रजिस्टर, Android और iPhone बैकअप। यह पहचान या फ़ॉल्स पॉज़िटिव की दरें नहीं मापता। आधिकारिक ऑनलाइन स्रोत

[11] Zero Breach Toolkit। PRIVACY: सामान्य विश्लेषण डिज़ाइन के अनुसार अपलोड नहीं करता; अद्यतन और Android अधिग्रहण अलग गतिविधियाँ हैं। रिपोर्ट में संवेदनशील डेटा हो सकता है और साझा करने का सारांश पूरी रिपोर्ट का विकल्प नहीं है। आधिकारिक ऑनलाइन स्रोत

कोड / स्थिति	सही व्याख्या	अगला निर्णय
3. डेटा का स्रोत अनुपलब्ध	जाँच-सीमाएँ हैं, पर clear। परिणाम नहीं है।	कवरेज पूरा कर और फिर जाँच।
4. स्कैन किए बिना आउटपुट	न तो कोई समीक्षा हुई और न ही कोई फसल।	यह दावा नहीं करना कि कोई स्पाइवेयर नहीं है।
हटाए गए सर्वर का सक्रियक	सक्रियक के स्रोत में बदलाव उसके वर्तमान जोखिम को बदलता है।	सर्वर और स्रोत जाँच, जोखिम चाहे नहीं।

तालिका के स्रोत:[12]

7.3 “Worth a look” कोई निर्णय नहीं है

ऐप स्टोर के बाहर से इंस्टॉल किया ऐप, ऐक्सेसिबिलिटी पहुँच, पुराना संस्करण या अक्षम सत्यापन कॉन्फ़िगरेशन प्रश्न पूछने का कारण हो सकता है। यह अपने आप में निष्कर्ष नहीं है। ऐक्सेसिबिलिटी टूल, स्क्रीन रीडर, पासवर्ड प्रबंधक और ऑटोमेशन ऐप वैध हो सकते हैं। डिवाइस जानने वाला व्यक्ति अतिरिक्त जानकारी से इन व्याख्याओं की पुष्टि या खंडन कर सकता है।

> **Duriva चाचा दीवार तोड़ता है**
> यदि केवल “छह मेल मिले” पढ़ें, तो यह निर्णय जैसा लग सकता है। यदि “चार जाँचें नहीं चलीं” भी पढ़ें, तो समझेंगे कि केस अब भी खुला है। यही प्रतिक्रिया देने और समीक्षा करने का अंतर है।



चित्र 3. रिपोर्ट को परतों से पढ़ा जाता है। दायरा और रिक्तियाँ अर्थ को बदलती हैं संपादकीय पुनर्लिखाण; यह वास्तविक सबूत नहीं है।

[12] Zero Breach Toolkit। परिणाम और कवरेज का अनुबंध: कोड 0, 1, 2, 3 और 4; निष्कर्ष, संदर्भ, जाँच-रिक्ति, बिना स्कैन आउटपुट और सीमित दायरे में अंतर। बिना मेल वाला परिणाम कभी सुरक्षा की गारंटी नहीं है। आधिकारिक ऑनलाइन स्रोत

8. प्रयोगशाला के चार परिदृश्य

8.1 `spyware`: छह निष्कर्ष, कोई जल्दबाजी निष्कर्ष नहीं

`spyware` काल्पनिक परिदृश्य में छह मेल मिले: डिवाइस पर पाँच साक्ष्य-वस्तुएँ और रजिस्टर में एक। इसमें ऐप, फ़ाइल-फ़ुटप्रिंट, प्रमाणपत्र, प्रॉपर्टी, पथ और काल्पनिक अवसंरचना का संदर्भ शामिल हैं। चार जाँच-रिक्तियाँ भी रहीं: फ़ाइल-फ़ुटप्रिंट नहीं, बैटरी इतिहास नहीं, क्रैश रिपोर्ट नहीं और SMS बैकअप नहीं। परिणाम `INDICATORS_FOUND`, कोड 2 और `scan_state: partial` था।[13]

यह "आपके डिवाइस में spyware है" नहीं सिखाता, बल्कि अलग-अलग वस्तुओं का समूहन और प्रत्येक की व्याख्या की आवश्यकता दिखाता है। आउटपुट स्वयं याद दिलाता है कि मेल पर जाँच करनी है, समझौता घोषित या सफ़ाई नहीं करनी। किसी फ़ाइल या कॉन्फ़िगरेशन का होना अपने आप निष्पादन सिद्ध नहीं करता और अवसंरचना का संदर्भ सफल संपर्क सिद्ध नहीं करता। पूरा फ़ोन और सभी संकेतक काल्पनिक हैं।

8.2 `worth-a-look`: प्रश्न पूछने के लिए, आरोप लगाने के लिए नहीं

`worth-a-look` परिदृश्य में ज्ञात संकेतक नहीं मिले, लेकिन प्रश्न पूछने के चार तत्व मिले: ऐक्सेसिबिलिटी पहुँच वाला सीधे इंस्टॉल किया ऐप, पुराने अद्यतन, सक्षम ऐक्सेसिबिलिटी सेवा और अक्षम ऐप सत्यापन। परिणाम `NO_KNOWN_INDICATORS_WITH_GAPS`, कोड 3 था, जिसमें वही चार कवरेज रिक्तियाँ थीं।[14]

ये तत्व संक्रमण या नकलीपन का सबूत नहीं हैं. ये एक निमंत्रण हैं पूछने के लिएः क्या आप एप्लिकेशन को पहचानते हैं? आपने इसे क्यों स्थापित किया है? क्या आप उस अनुमति की प्रतीक्षा कर रहे थे? क्या कोई अपडेट लंबित हैं? व्यवहार से पहले क्या बदल गया है? मैनुअल यह नहीं कहता है कि मालिक गलत है या सब कुछ सामान्य है। आरोप लगाने से पहले पूछना सीखना लक्ष्य है।

8.3 `clean`: चार जाँच-रिक्तियों के साथ मेल की अनुपस्थिति

`clean` परिदृश्य में ज्ञात मेल नहीं मिले, लेकिन चार जाँच-रिक्तियाँ और कोड 3 रहा। आउटपुट स्पष्ट कहता है कि यह अच्छी स्थिति का प्रमाणपत्र नहीं है। "कुछ नहीं मिला" केवल जाँचे गए दायरे और ज्ञात संकेतकों तक सीमित है। यह नए, छिपे, लक्षित या अदस्तावेज़ित spyware की अनुपस्थिति या हर स्थान की जाँच सिद्ध नहीं करता।[15]

यदि किसी व्यक्ति के पास चिंता का ठोस कारण है, तो यह परिणाम उस चिंता को समाप्त नहीं करता। अगला कदम कवरेज पूरा करना, रिकॉर्ड देखना, विशेषज्ञ से परामर्श या केवल यह दस्तावेज़ित करना हो सकता है कि पहली जाँच में कार्रवाई योग्य संकेत नहीं मिले। व्यक्ति को समझा गया दिखाने के लिए फ़ॉल्स पॉज़िटिव थोपना आवश्यक नहीं है।

8.4 `cellebrite`: फोरेंसिक एक्सेस, स्पाइवेयर नहीं

`cellebrite` परिदृश्य में USB रजिस्टर में एक मेल और कोड 2 मिला। इसका उद्देश्य दिखाना है कि टूल फोरेंसिक पहुँच के निशान को कैसे पहचानता है और सिफ़ारिशें कैसे बदलती हैं: संरक्षण करें, उस समय के आस-पास के ऐप जाँचें और संदर्भ उचित हो तो दूसरे डिवाइस से पासवर्ड बदलें। रजिस्टर और क्रम संख्या काल्पनिक हैं; पीछे कोई वास्तविक व्यक्ति या डिवाइस नहीं है।[16]

[13]स्थानीय प्रयोगशाला ACCCF. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, चार सिंथेटिक परिदृश्यों का निष्पादन। TXT/JSON में spyware, worth-a-look, clean और cellebrite फ़ाइलें। कोई व्यक्तिगत जानकारी या वास्तविक उपकरणों की जांच नहीं की गई।

[14]स्थानीय प्रयोगशाला ACCCF. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, चार सिंथेटिक परिदृश्यों का निष्पादन। TXT/JSON में spyware, worth-a-look, clean और cellebrite फ़ाइलें। कोई व्यक्तिगत जानकारी या वास्तविक उपकरणों की जांच नहीं की गई।

[15]स्थानीय प्रयोगशाला ACCCF. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, चार सिंथेटिक परिदृश्यों का निष्पादन। TXT/JSON में spyware, worth-a-look, clean और cellebrite फ़ाइलें। कोई व्यक्तिगत जानकारी या वास्तविक उपकरणों की जांच नहीं की गई।

[16]स्थानीय प्रयोगशाला ACCCF. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, चार सिंथेटिक परिदृश्यों का निष्पादन। TXT/JSON में spyware, worth-a-look, clean और cellebrite फ़ाइलें। कोई व्यक्तिगत जानकारी या वास्तविक उपकरणों की जांच नहीं की गई।

यह मामला spyware नहीं है और अपने आप पूर्ण निष्कर्षण भी सिद्ध नहीं करता। फोरेंसिक प्रश्न है कि फ़ोन तक किसने, कितने समय, किस अधिकार से पहुँच पाई और पहले तथा बाद में क्या हुआ। निष्कर्ष में कनेक्शन के निशान और संदर्भ से सिद्ध हो सकने वाले अर्थ में अंतर करना चाहिए।

> **चार अलग साख**
> मेल का अर्थ संक्रमण नहीं; जाँचने योग्य तत्वों का अर्थ फ़ॉल्स पॉज़िटिव नहीं; शून्य मेल का अर्थ सुरक्षा नहीं; और फोरेंसिक निशान का अर्थ पूर्ण निष्कर्षण का साक्ष्य नहीं है। रिपोर्ट समीक्षा की शुरुआत है, निर्णय नहीं।

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · spyware

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: spyware. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:33   Windows 11
========================================================================

========================================================================
  SUMMARY  -  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: SERIOUS FINDING - seek expert help promptly.

  WHAT WAS FOUND
    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       org.example.training.spyapp  [artifact]
          Where: app org.example.training.spyapp

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       e36c3fee5d43ffb61b91fbee792cd8b7b4ebd9076f77e9002a9eaa0ea5648a84  [sample]
          The file fingerprint of a published spyware sample (its family
          is named where the source gives one). A match here is
          conclusive, not circumstantial.
          Where: app org.example.training.spyapp (/data/app/training-spyapp/base.apk)

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       d472b7c9d957a9e55ce56bd80388b97be9e2132644c0a51cac03aa618905e6d2  [artifact]
          Where: app org.example.training.spyapp

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       persist.training.spy.flag  [artifact]
          Where: system property persist.training.spy.flag

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       /data/local/tmp/training-spy-daemon  [artifact]
          Where: /data/local/tmp/training-spy-daemon

    >> THE PHONE'S SYSTEM LOGS NAME THIS SPYWARE INFRASTRUCTURE
       training-spyware-server[.]invalid  [infrastructure]
          A server the cited researchers attribute to the named spyware
          family. Its exact role - delivering an exploit, controlling an
          implant or receiving stolen data - is not stated in the source,
          so treat contact as serious but unspecified. A domain can change
          hands after a campaign ends: compare the date of the evidence
          with the date of the research.
          the phone's own system logs name it - it may have been a
          connection, a lookup, or only text an app wrote to the log
          Where: phone log dumpsys.txt, line 1

  WHAT TO DO
    Seek expert help promptly. Preserve this report and the named
    files or registrations. Do NOT delete, move, run or try to clean
    them. A file match establishes presence; a registration
    establishes configuration. Neither alone establishes that spyware
    executed.

    Contact a qualified incident responder or your organisation's
    security team. You do not need to finish investigating first.
    Support options are at the end of this report.
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

आकृति 4. spyware नामक काल्पनिक परिदृश्य का वास्तविक प्रशिक्षण रिपोर्ट। शाब्दिक अंश; सभी डेटा काल्पनिक है। संपादकीय पुनर्मुद्रण; यह वास्तविक साक्ष्य नहीं है।

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · worth-a-look

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: worth-a-look. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:33   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: no known indicator was found in anything that could be
          checked.

  This is NOT a clean bill of health. See the two sections below for
  what was searched and, more importantly, what could not be.

  ALSO: 4 items under "WORTH A LOOK" further down. They are NOT
  a finding; each comes with its usual, ordinary explanation.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
========================================================================

Indicator set : 6 indicators, unknown age
  ** WARNING: one or more source dates are unknown; copying files does not refresh indicators. **

DETAIL  —  what was examined, and the evidence behind the summary

--- android-intrusion check  [NOT_APPLICABLE] ---
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

चित्र 5. वास्तविक worth-a-look पारदृश्य प्राशिक्षण रिपोर्ट। शाब्दिक टुकड़ा; सभी डेटा सिथांटिक है। सपादकीय पुनानमाण; वास्तविक सबूत नहीं है।

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · clean

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: clean. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:34   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: no known indicator was found in anything that could be
          checked.

  This is NOT a clean bill of health. See the two sections below for
  what was searched and, more importantly, what could not be.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
========================================================================
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

चित्र 6. वास्तावक पारदृश्य प्राशक्षण रिपाट clean. शाब्दक टुकड़ा; सभा डटा सिथाटक ह. सपादकाय पुनानमाण; वास्तावक सबूत नहा ह।

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · cellebrite

```
######################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: cellebrite. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
######################################################################
======================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:34   Windows 11
======================================================================

======================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
======================================================================
  RESULT: SERIOUS FINDING - seek expert help promptly.

  WHAT WAS FOUND
    >> SIGNS THIS PHONE WAS UNLOCKED WITH A PHONE-FORENSICS TOOL (CELLEBRITE)
       cellebrite usb 04f2:b071  [forensic]
          A trace of Cellebrite, the phone-forensics tool police and
          security services use to unlock seized phones and copy their
          contents. It is not spyware: it shows the phone was unlocked, or
          an unlock was attempted, while it was out of its owner's hands.
          the phone's own system logs name it - it may have been a
          connection, a lookup, or only text an app wrote to the log
          Where: phone log logcat.txt, line 2

  WHAT TO DO
    Someone unlocked this phone, or tried to, with Cellebrite: the
    phone-forensics tool police and security services use to copy
    everything on a seized phone. Assume what was on the phone then -
    messages, photos, contacts, saved passwords and the accounts
    signed in - was copied. Change the passwords of important accounts
    from another device, sign out other sessions, and tell the people
    whose conversations were on it. In documented cases spyware was
    installed after such an unlock, so check the apps installed around
    that time and get expert help.

    Seek expert help promptly. Preserve this report and the named
    files or registrations. Do NOT delete, move, run or try to clean
    them. A file match establishes presence; a registration
    establishes configuration. Neither alone establishes that spyware
    executed.

    Contact a qualified incident responder or your organisation's
    security team. You do not need to finish investigating first.
    Support options are at the end of this report.

    Do NOT open, visit or look up indicator addresses. Keep the [.]
    spelling when sharing them.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

चित्र 7. वास्तावक प्राशक्षण रिपाट सालाब्रटा पारदृश्य। शाब्दक टुकड़ा; सभा डटा सिथाटक ह। सपादकाय पुनानमाण; वास्तावक सबूत नहीं है।

9. विशेषज्ञ या प्रतिक्रिया टीम को सुरक्षित रूप से सौंपना

9.1 पहले सारांश, फिर पूरी केस फ़ाइल

सब कुछ भेजने से पहले मामला पाने वाले से पूछें कि उसे क्या और किस चैनल से चाहिए। पहली बातचीत चिंता के कारण, डिवाइस, दायरे, तिथि, परिणाम और जाँच-रिक्तियों तक सीमित हो सकती है। न्यूनतम सारांश से यह तय करने में सहायता मिलती है कि पूरी रिपोर्ट चाहिए या नहीं और ऐसा इतिहास या संदेश नहीं भेजे जाते जो प्रश्न में सहायक नहीं हैं।

पूरी रिपोर्ट चाहिए तो सार्वजनिक फ़ाइल के बजाय सुरक्षित चैनल से दें। कार्यकारी और साझा करने के संस्करण अलग रखें। पाने वाले को मूल वस्तुएँ चाहिए हो सकती हैं, लेकिन यह स्पष्ट रूप से तय करें। Android संग्रह, iOS बैकअप या रिपोर्ट अज्ञात सेवाओं, चैट समूहों या सामान्य विश्लेषण साइटों पर अपलोड न करें।[17]

[17] Zero Breach Toolkit। PRIVACY: सामान्य विश्लेषण डिज़ाइन के अनुसार अपलोड नहीं करता; अद्यतन और Android अधिग्रहण अलग गतिविधियाँ हैं। रिपोर्ट में संवेदनशील डेटा हो सकता है और साझा करने का सारांश पूरी रिपोर्ट का विकल्प नहीं है। आधिकारिक ऑनलाइन स्रोत

9.2 सत्यापन योग्य डिलीवरी के लिए हैश और EML

रिपोर्ट ईमेल से भेजें तो मुख्य भाग, हेडर और संलग्नकों सहित पूरा EML रखें। मुख्य भाग में प्रत्येक फ़ाइल का एल्गोरिदम और hash हो सकता है। प्राप्तकर्ता स्वयं मान निकालकर तुलना करता है। मेल उस डिलीवरी में बताई फ़ाइल के साथ समानता सिद्ध करता है, डिवाइस की प्रामाणिकता या निष्कर्षों की सत्यता नहीं। बाद में निकाला hash केवल उस समय से अखंडता सिद्ध करता है।

ईमेल एन्क्रिप्शन, हस्ताक्षर और hash अलग समस्याएँ हल करते हैं। एन्क्रिप्शन पढ़ने वालों को सीमित करता है; हस्ताक्षर उत्पत्ति और परिवर्तन की जाँच में सहायता करता है; hash वस्तुओं की तुलना करता है। इनमें से कोई यह सिद्ध नहीं करता कि संदेश लिखने वाला वही व्यक्ति है जिसका वह दावा करता है या सामग्री सत्य है। निजी कुंजी या फ़ाइल का पासवर्ड उसी संदेश में न भेजें। तय किए गए अलग चैनल का उपयोग करें।

वस्तु	क्या दर्ज किया जाता है	जो साबित नहीं करता है
डिलीवरी का EML	मुख्य भाग, हेडर, संलग्नक और प्राप्ति।	कि मानव प्रेषक ने सामग्री लिखी।
TXT / JSON रिपोर्ट	नाम, आकार, हैश, तारीख और संस्करण।	कि दावेदार पूरी या सही डिवाइस प्रामाणिक है।
साझा करने के लिए तारीखें	परिणाम, दावेदार, गोपनीयता और अगले कदम।	पूर्ण फोरेंसिक परीक्षण या जोखिम का अनुपस्थित।
फ़ुटा या पासवर्ड	अलग चैनल और पुष्टि प्राप्तकर्ता।	कि किसी ने प्राप्तकर्ता से डिलीवरी अधिकृत की थी।
मूल संग्रह	आधिकार, फॉरेंसिक, जोखिम और प्रत्येक वस्तु का hash।	कि कोई भी दूसरे से भी आर्टिफैक्ट पढ़ सकता है।

9.3 व्याख्या जो दूसरा संकट रोकती है

मामले का सारांश के लिए संक्षिप्त पाठ

चिंता का कारण: [देखा गया व्यवहार और तिथि]
उपकरण और प्राधिकरण: [प्रकार, धारक और अनुमति]
उपकरण और संस्करण: [उत्पत्ति और सत्यापन]
दायरा: [क्या चेक किया गया और क्या नहीं]
परिणाम: [संयोग, संदर्भ और रिक्तियां]
पहले से की गई कार्रवाइयाँ: [बिना हटाए या साफ़ किए]
सौंपी गई वस्तुएँ: [सारांश / रिपोर्ट / मूल वस्तुएँ]
प्रत्येक फ़ाइल का हैश: [अल्गोरिथम और मूल्य]
मुझे क्या चाहिए: [दायरे की समीक्षा, व्याख्या और अगला कदम]
जो डेटा शामिल नहीं किया: [कुंजियाँ, पासवर्ड, अंतरंग या अप्रासंगिक सामग्री]

यह बहस जीतने के बारे में नहीं है

विशेषज्ञ को यह सिद्ध कराने की आवश्यकता नहीं है कि व्यक्ति सही था। उसे स्रोत, कालक्रम और की गई कार्रवाइयों की व्याख्या चाहिए। अच्छी तरह संरक्षित अनिश्चितता बनाई गई निश्चितता से अधिक उपयोगी है।

अनुलग्नक A. विशेषज्ञ के लिए पुनरुत्पाद्य प्रोटोकॉल

A.1 वातावरण और उत्पत्ति का रिकॉर्ड

इस गाइड के उदाहरणों को बनाने के लिए इस्तेमाल किया गया रिकॉर्ड

रिपॉज़िटरी: https://github.com/interplains/Zero-Breach-Toolkit
Commit: 10ceaba497e40da1f327916a0a3fe0af0ff5994f
दिखाया गया संस्करण: Zero Breach Toolkit 2.0.6
JSON स्कीम: 1.6
फ़ाइल: scan/zero-breach-toolkit.py
SHA-256: 4f7294b0d72ae901552e3ac44f64148c0059d43d587a1638654ab00e7c80e627
परिदृश्य: spyware, worth-a-look, clean और cellebrite
डेटा प्रकार: पूरी तरह से सिंथेटिक
व्यक्तिगत जानकारी: अनजांचित
वास्तविक उपकरण: अप्रयुक्त

यह रिकॉर्ड रिपॉज़िटरी की क्लोनिंग और प्रशिक्षण निष्पादनों का विवरण है; यह Windows एक्ज़ीक्यूटेबल का अटेस्टेशन या नवीनतम संस्करण का सत्यापन नहीं है। डाउनलोड किए एक्ज़ीक्यूटेबल की जाँच उसके अपने संस्करण और बिल्ड वर्कफ़्लो से करनी चाहिए। चारों परिदृश्य चलाए गए और उन्होंने TXT तथा JSON के अतिरिक्त `--describe` का JSON आउटपुट भी दिया।

A.2 वास्तविक अधिकृत निष्पादन की फ़ॉर्म

फोरेंसिक रिकॉर्ड टेम्पलेट

मामला और अधिकार: [पहचानकर्ता, धारक, दायरा और अपवाद]
जांच का कारणः [व्यवहार और प्रश्न]
डिवाइस और प्रारंभिक स्थिति: [मॉडल, सिस्टम, तिथि, समय क्षेत्र]
पैकेज: [रिपॉज़िटरी, संस्करण, फ़ाइल और सत्यापन]
पैकेज और संकेतकों का हैशः [मान और तिथि]
वातावरण: [विश्लेषण सिस्टम, पृथक्करण और सिंक्रनाइज़ेशन]
दायरा: [default / full / targeted / browser / phone]
कमांड और पैरामीटर: [बिना रहस्यों]
समय क्षेत्र सहित प्रारंभ और समाप्ति: [मूल रूप]
आउटपुटः [TXT, JSON, सारांश, manifest और hashes]
परिणाम और कोड: [मूल रूप]
निष्कर्षः [ग्रेड, वस्तु, स्रोत और संदर्भ]
जाँच-रिक्तियाँ: [नहीं चलाई गई जाँचें और कारण]
घटनाएंः [त्रुटि, सीमाएं और अनुपलब्ध फाइलें]
संरक्षण और अभिरक्षा: [स्थान, पहुँच और स्थानांतरण]
समीक्षाः [व्यक्ति, तिथि और अगले सत्यापन]

A.3 व्याख्या की मैट्रिक्स

प्रश्न	उत्तर देने वाला स्रोत	जो नहीं कहा जा सकता है
इसने क्या पाया?	मेल, सांख्य-स्तर और वस्तु।	स्वचालित सक्रमण या हमलावर की पहचान।
इसने क्या जांच नहीं पाया?	Coverage.not_checked और scan_state।	कि छोड़ गए स्थान clean हैं।
इसने कौन-से स्रोत उपयोग किए?	सकतक, सस्करण और तारीखें।	कि एक हालिया प्रति वर्तमान साक्ष्य है।
क्या समाप्त हो सकता है?	मालिक की कॉन्फ़िगरेशन, अनुप्रयोग और सेवा।	बिना पुष्टि के झूठा सकारात्मक।
अट्रिब्यूशन के लिए क्या कमी है?	प्राधिकरण, समय, डिवाइस और समयक्रम।	IP, ऐप या MAC से सीधे मालिक व्यक्ति की पहचान।
क्या साझा किया जाता है?	जोखिमकतानुसार सारांश या पूरी रिपोर्ट।	कि रिपोर्ट प्रकाशित करना हानिरहित है।

स्वीकृति का मानदंड

रिपोर्ट से दूसरा व्यक्ति दायरा दोहरा, प्रत्येक निष्कर्ष खोज, प्रत्येक जाँच-रिक्ति समझ और जो अभी सिद्ध नहीं हुआ वह जान सके। यदि उसमें केवल “clean” या “infected” लेबल है, तो समीक्षा अब भी पूरी नहीं है।

अनुलग्नक B. कानूनी ढाँचा, गोपनीयता और अंतिम जाँच

सुरक्षा जाँच में व्यक्तिगत डेटा भी संसाधित होता है। मेक्सिको में वर्तमान LFPDPPP के उद्देश्य, समानुपातिकता, सुरक्षा, गोपनीयता और सुरक्षा उल्लंघन से संबंधित सिद्धांत लागू होते हैं। पेरू, चिली, अर्जेंटीना, कोलंबिया, इक्वाडोर और स्पेन/UE में न्यूनतमकरण, सुरक्षा, अधिकारों और प्रदाताओं से जुड़े समकक्ष, लेकिन एक जैसे नहीं, कार्य हैं। चिली में Ley 21.719 के आधुनिकीकरण का प्रारंभ

1 दिसंबर 2026 के लिए स्थगित है और इसे पूर्ण लागू ढाँचे के रूप में पहले से नहीं मानना चाहिए। किसी दूसरे के डिवाइस को पढ़ने का कोई सार्वभौमिक अधिकार नहीं है।[18]192021222324

बंद होने से पहले जाँच	उत्तर का नाम
क्या व्यक्ति सुरक्षित और जीवंत था?	कोई जाँच न जिज्ञासा के कारण चलाई गई, न बिना जनुमति के।
पकड़ा सत्यापित किया गया था?	रिपोर्टर, सत्कारण और उत्पन्न दस्तावेज़।
क्या आउटपुट सुरक्षित रहा?	स्वामित्व फ़ाइलर, एक्सेस और सिंक्रनाइज़ेशन निर्यात
क्या निष्क्रिय, संपर्क और जीव-रहित में अंतर किया गया?	यह एक लेबल के कारण संक्रमण था सुरक्षा नहीं कहा गया था।
क्या सामान्य व्याख्या को गंभीर संभावना को खारिज किए?	कॉन्फ़िगरेशन और संपर्क की जाँच की गई।
क्या रिपोर्ट स्थानीय जीवरक्षक डेटा के साथ साझा की गई?	सारांश पहले, सुरक्षित पैनल के माध्यम से पूरा दस्तावेज़।
क्या विश्लेषण इसे दोहरा सकता है?	सत्कारण, सामग्री, फ़ाइल, हश, रिकॉर्ड और रखरखाव मॉड्यूल है।

समापन

सही प्रश्न “क्या मैं आशंकावादी हूँ?” नहीं, बल्कि “मैं अपनी अधिक हानि किए बिना क्या जाँच सकता/सकती हूँ?” है। उत्तर कोई कॉन्फ़िगरेशन, मेल, जाँच-रिक्ति या पेशेवर समीक्षा हो सकता है। ये सभी बिना स्रोत के आरोप से अधिक उपयोगी हैं।

[18]मेक्सिको। Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 20-03-2025 को प्रकाशित पाठ और 14-11-2025 का संशोधन। अनुच्छेद 5–9, 18–20 और 31: सिद्धांत, सुरक्षा, गोपनीयता, सुरक्षा उल्लंघन और अधिकारों के निपटान। वर्तमान संघीय प्राधिकरण Secretaría Anticorrupción y Buen Gobierno है। आधिकारिक ऑनलाइन स्रोत

[19]पेरू। Ley 29733 और DS 016-2024-JUS द्वारा अनुमोदित उसका Reglamento। उद्देश्य, समानुपातिकता, सुरक्षा और गोपनीयता के सिद्धांत; नया Reglamento घटनाओं, निवारक मूल्यांकन और डेटा अधिकारी के क्रमिक कार्यों का विवरण देता है। आधिकारिक ऑनलाइन स्रोत

[20]चिली। Ley 21.719, जो Ley 19.628 sobre protección de datos personales में संशोधन करती है। नए ढाँचे वाले संस्करण की प्रारंभ तिथि 01-12-2026 के लिए स्थगित है; उससे पहले उस समय लागू नियम की समीक्षा करनी चाहिए और भविष्य के दायित्वों को वर्तमान में लागू नहीं मानना चाहिए। आधिकारिक ऑनलाइन स्रोत

[21]अर्जेंटीना। Ley 25.326, अद्यतन पाठ। अनुच्छेद 4–6, 9–10, 14–16 और 25: गुणवत्ता, सूचना, सुरक्षा, गोपनीयता, धारकों के अधिकार और तीसरे पक्ष की ओर से संसाधन सेवाओं का प्रावधान। आधिकारिक ऑनलाइन स्रोत

[22]कोलंबिया। Ley Estatutaria 1581 de 2012, अनुच्छेद 4, 8, 12, 17–18 और 26: सिद्धांत, अधिकार, सूचना, उत्तरदायी और संसाधकों के कर्तव्य तथा तीसरे देशों को अंतरण। आधिकारिक ऑनलाइन स्रोत

[23]इक्वाडोर। Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021। अनुच्छेद 10, 37–44: सिद्धांत, सुरक्षा उपाय, डिज़ाइन से संरक्षण, जोखिम और घटनाओं के प्रति संसाधन। आधिकारिक ऑनलाइन स्रोत

[24]यूरोपीय संघ। Reglamento (UE) 2016/679, अनुच्छेद 5, 25, 28 और 32–34: सिद्धांत, डिज़ाइन से संरक्षण, संसाधक, सुरक्षा और सुरक्षा उल्लंघनों की अधिसूचना/सूचना। स्पेन में लागू राष्ट्रीय और क्षेत्रीय कानून की भी समीक्षा आवश्यक है। आधिकारिक ऑनलाइन स्रोत