Freemindtronic

संदर्भ दस्तावेज़: APT36 (पारदर्शी जनजाति/मिथिक तेंदुआ) साइबर जासूसी समूह
अंतिम अद्यतन: 16 मई, 2025
संस्करण: 1.1
प्रारंभिक जानकारी का मुख्य स्रोत: फ्रीमाइंडट्रॉनिक एंडोरा (16/05/2025 का घटना के बाद का विश्लेषण)

परिचय

एडवांस्ड पर्सिस्टेंट थ्रेट (एपीटी) समूह जिसे एपीटी 36, ट्रांसपेरेंट ट्राइब और मिथिक लेपर्ड के नाम से जाना जाता है, कई वर्षों से एक सक्रिय साइबर जासूसी अभिनेता रहा है। मुख्य रूप से भारत पर लक्षित, APT36 सरकार, सेना और संभावित रूप से अनुसंधान और शिक्षा क्षेत्रों सहित विभिन्न संगठनों से संवेदनशील खुफिया जानकारी एकत्र करने के अपने लगातार अभियानों के लिए कुख्यात है। उनके संचालन को अक्सर परिष्कृत स्पीयरफ़िशिंग तकनीकों और बीस्पोक मैलवेयर के उपयोग की विशेषता होती है, जैसे कि पोसीडॉन, क्रिमसन आरएटी, एलिज़ारैट और कैप्रारैट। इस संदर्भ दस्तावेज़ का उद्देश्य APT36, इसकी रणनीति, तकनीकों और प्रक्रियाओं (TTPs), बुनियादी ढांचे, और अनुशंसित शमन उपायों के बारे में उपलब्ध जानकारी को संकलित और विश्लेषण करना है।

इतिहास और विकास

हालांकि फ्रीमाइंडट्रॉनिक एंडोरा द्वारा प्रदान किया गया प्रारंभिक विश्लेषण हाल के आईओसी (2023-2025) पर केंद्रित है, एपीटी 36 की गतिविधि कई वर्षों पुरानी है। अन्य सुरक्षा संगठनों की पिछली रिपोर्टों ने 2016 की शुरुआत में इसी तरह के उपकरणों का उपयोग करके और भारतीय संस्थाओं को लक्षित करने वाले अभियानों का दस्तावेजीकरण किया है। उनके TTP का विकास सुरक्षा उपायों के निरंतर अनुकूलन और लक्षित प्रणालियों तक उनकी पहुंच बनाए रखने के लिए नए उपकरणों के विकास का सुझाव देता है। उदाहरण के लिए, उनके RAT (जैसे CapraRAT) के Android संस्करणों की उपस्थिति मोबाइल उपकरणों के लिए उनके दायरे के विस्तार को इंगित करती है। C2 (ElizaRAT) के लिए टेलीग्राम जैसे प्लेटफार्मों का उपयोग संभावित रूप से कम निगरानी वाले संचार चैनलों का फायदा उठाने का प्रयास भी दिखाता है।

APT36 का सटीक श्रेय साइबर सुरक्षा समुदाय के भीतर चर्चा का विषय बना हुआ है। हालांकि मुख्य लक्ष्य भारत में हैं, लेकिन डिकॉय और लक्षित क्षेत्रों के विषयों को देखते हुए, पाकिस्तानी राज्य के हितों के संभावित लिंक के कुछ सबूत हैं। हालांकि, एक औपचारिक एट्रिब्यूशन के लिए अधिक निर्णायक साक्ष्य की आवश्यकता होती है और यह अक्सर साइबर सुरक्षा क्षेत्र में जटिल होता है।

तकनीक, रणनीति और प्रक्रियाएं (टीटीपी)

- **मान्यता:** APT36 संभवतः अपने लक्ष्यों की सावधानीपूर्वक टोह लेता है, कर्मचारियों, संगठनात्मक संरचनाओं और संवेदनशील परियोजनाओं पर सार्वजनिक रूप से उपलब्ध जानकारी (OSINT) एकत्र करता है। सोशल मीडिया प्रोफाइल और आधिकारिक वेबसाइटें सूचना के संभावित स्रोत हैं। कर्मचारियों से जानकारी प्राप्त करने के लिए सोशल इंजीनियरिंग का भी उपयोग किया जा सकता है।
- **प्रवेश का प्रारंभिक बिंदु:**
    - **स्पीयरफ़िशिंग:** यह APT36 का पसंदीदा अटैक वेक्टर है। ईमेल को वैध संचार (जैसे, सरकारी सूचनाएं, शैक्षणिक घटनाओं के लिए निमंत्रण, सुरक्षा ऐप अपडेट) की नकल करने के लिए सावधानीपूर्वक डिज़ाइन किया गया है। दुर्भावनापूर्ण अनुलग्नक (Word दस्तावेज़, PDF, निष्पादन योग्य, RTF फ़ाइलें, स्क्रीनसेवर) या समझौता की गई वेबसाइटों के लिंक का उपयोग प्रारंभिक पेलोड वितरित करने के लिए किया जाता है। पहचाने गए फ़ाइल नाम (जैसे,

Briefing_MoD_April25.docx, Alert_Kavach_Update.exe) सामयिक विषयों या संभावित पीड़ितों के लिए प्रासंगिक विषयों को लक्षित करके इस रणनीति को स्पष्ट करते हैं।

    - **कमजोरियों का शोषण:** हालांकि प्रारंभिक IOC में स्पष्ट रूप से उल्लेख नहीं किया गया है, यह संभव है कि APT36 प्रारंभिक पहुंच प्राप्त करने के लिए आमतौर पर उपयोग किए जाने वाले अनुप्रयोगों (जैसे, Microsoft Office) में ज्ञात सॉफ़्टवेयर कमजोरियों का फायदा उठा सकता है। ऐसे प्रयासों में अक्सर RTF फ़ाइलों का उपयोग किया जाता है।
    - **वेबसाइट समझौता:** यह संभव है, हालांकि IOC द्वारा सीधे सिद्ध नहीं किया गया है, कि APT36 पेलोड होस्ट करने या पीड़ितों को फ़िशिंग पृष्ठों पर पुनर्निर्देशित करने के लिए वैध वेबसाइटों से समझौता कर सकता है।

- **दृढ़ता:** एक बार सिस्टम से समझौता हो जाने के बाद, APT36 रिबूट के बाद भी पहुंच बनाए रखने के लिए तंत्र स्थापित करता है। IOCs मैलवेयर का स्वत: निष्पादन सुनिश्चित करने के लिए विशिष्ट Windows रजिस्ट्री कुंजियों (HKEY_CURRENT_USER\Software\CrimsonRAT, HKEY_LOCAL_MACHINE\SYSTEM\ElizaRAT\Persistence, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\CapraStart) के उपयोग को प्रकट करते हैं। एंड्रॉइड पर, दृढ़ता अक्सर वैध ऐप अपडेट (com.kavach.update.apk) के रूप में बहाना करके प्राप्त की जाती है।
- **पार्श्व आंदोलन:** प्रारंभिक पैर जमाने के बाद, APT36 अधिक संवेदनशील प्रणालियों तक पहुँचने के लिये पीड़ित के नेटवर्क के भीतर पार्श्व रूप से आगे बढ़ने का प्रयास करता है। इसमें नेटवर्क शेयरों का शोषण करना, चोरी किए गए क्रेडेंशियल्स (संभावित रूप से कीलॉगिंग के माध्यम से प्राप्त) का उपयोग करना और तैनात आरएटी के माध्यम से दूरस्थ कमांड निष्पादित करना शामिल हो सकता है।
- **कमांड एंड कंट्रोल (C2):** APT36 द्वारा उपयोग किया जाने वाला मैलवेयर निर्देश प्राप्त करने और डेटा को बाहर निकालने के लिए हमलावर-नियंत्रित C2 सर्वर के साथ संचार करता है। पहचाने गए IP पते (45.153.241.15, 91.215.85.21, आदि) संभावित रूप से इस C2 अवसंरचना का प्रतिनिधित्व करते हैं। एलिजारैट का टेलीग्रामबॉट का उपयोग C2 के लिए लोकप्रिय मैसेजिंग प्लेटफॉर्म का लाभ उठाने का सुझाव देता है, जो पता लगाना अधिक कठिन बना सकता है। HTTP और HTTPS का उपयोग संभवतः C2 ट्रैफ़िक के लिए किया जाता है, जो संभवतः वैध वेब ट्रैफ़िक के भीतर छिपा होता है।
- **डेटा बहिष्करण:** चूंकि APT36 का प्राथमिक फोकस जासूसी है, इसलिए डेटा एक्सफिल्ट्रेशन एक महत्वपूर्ण कदम है। लक्षित डेटा के प्रकारों में संवेदनशील दस्तावेज (सैन्य, सरकार, अनुसंधान), क्रेडेंशियल्स (उपयोगकर्ता नाम, पासवर्ड), और अन्य रणनीतिक जानकारी शामिल हैं। डेटा को स्थापित C2 चैनलों के माध्यम से बाहर निकाला जा सकता है, संभावित रूप से संकुचित, या पता लगाने से बचने के लिए एन्क्रिप्ट किया जा सकता है।
- **उपकरण और मैलवेयर:**
    - **Poseidon मैलवेयर:** व्यापक जासूसी और डेटा चोरी क्षमताओं के साथ एक परिष्कृत आरएटी। इसका हैश (3c2cfe5b94214b7fdd832e00e2451a9c3f2aaf58f6e4097f58e8e5a2a7e6fa34) इसे समझौता किए गए सिस्टम पर पहचानने की अनुमति देता है।
    - **क्रिमसन आरएटी:** एक और आरएटी जो आमतौर पर APT36 से जुड़ा होता है, जो कीलॉगिंग, स्क्रीन कैप्चर और रिमोट कमांड निष्पादन सुविधाओं की पेशकश करता है। इसका म्यूटेक्स (ग्लोबल\CrimsonRAT_Active) और रजिस्ट्री कुंजी (HKEY_CURRENT_USER\Software\CrimsonRAT) महत्वपूर्ण संकेतक हैं।

- **एलिज़ारत:** यह आरएटी सी2 संचार के लिए टेलीग्राम का उपयोग करता प्रतीत होता है, जो एक संभावित चोरी की रणनीति है। इसका लोडर (9f3a5c7b5d3f83384e2ef98347a6fcd8cde6f7e19054f640a6b52e61672dbd8f) और इसका म्यूटेक्स (Local\ElizaRATSession) प्रमुख IOC हैं।
- **CapraRAT (Android):** मोबाइल उपकरणों को लक्षित करने की APT36 की क्षमता को इंगित करता है। इसकी विशेषताओं में एसएमएस, संपर्क, ऑडियो रिकॉर्डिंग और स्थान ट्रैकिंग चोरी करना शामिल हो सकता है। इसके पैकेज नाम (com.kavach.update.apk) और म्यूटेक्स (\Sessions\BaseNamedObjects\CapraMobileMutex) विशिष्ट झंडे हैं।

- **अस्पष्टता और चोरी:** APT36 अपने मैलवेयर और संचार का पता लगाने और विश्लेषण करने के लिए अधिक कठिन बनाने के लिए कई तकनीकों का उपयोग करता है। इन रणनीति के उदाहरणों में संवेदनशील जानकारी का बेस 64 एन्कोडिंग (bXlQYXNzd29yZDEyMw==, JAB1c2VyID0gIkFkbWluIg==) और जावास्क्रिप्ट कोड का अस्पष्टता (eval(decodeURIComponent('%75%70%64%61%74%65'))) इन रणनीति के उदाहरण हैं।

अवसरंचना

APT36 के बुनियादी ढांचे में कमांड और कंट्रोल (C2) सर्वर शामिल हैं जिनका उपयोग पीड़ितों के सिस्टम पर तैनात मैलवेयर को निर्देशित करने के लिए किया जाता है। पहचाने गए आईपी पते (45.153.241.15, 91.215.85.21, 185.140.53.206, 192.241.207.45, 103.145.13.187) अवरुद्ध और निगरानी के लिए केंद्र बिंदु हैं। इन आईपी पतों के विश्लेषण से उपयोग किए गए होस्टिंग प्रदाताओं और संभावित रूप से अन्य संबंधित गतिविधियों के बारे में जानकारी मिल सकती है।

दुर्भावनापूर्ण डोमेन (kavach-app[.]कॉम, इंडियापोस्ट-जीओवी [।org, gov-inportal[.]संगठन, भारत-मंत्रालय[।कॉम, सिक्योरकवाच[.]में) का उपयोग फ़िशिंग अभियानों में नकली लॉगिन पृष्ठों को होस्ट करने या मैलवेयर वितरित करने के लिए किया जाता है। ये डोमेन अक्सर पीड़ितों को बरगलाने के लिए वैध वेबसाइटों की नकल करते हैं। इन डोमेन की पंजीकरण जानकारी का विश्लेषण करना कभी-कभी इन गतिविधियों के पीछे अभिनेताओं के बारे में सुराग प्रदान कर सकता है।

यह भी संभव है कि APT36 अपने हमलों की उत्पत्ति को छिपाने और ट्रेसिंग को और अधिक कठिन बनाने के लिए रिले के रूप में समझौता किए गए सर्वरों का उपयोग कर रहा हो।

प्रेरणा और लक्ष्य

APT36 के लिए मुख्य प्रेरणा साइबर जासूसी प्रतीत होती है, जिसमें भारत से संबंधित रणनीतिक खुफिया जानकारी इकट्ठा करने में विशेष रुचि है। विशिष्ट लक्ष्यों में शामिल हैं:

- भारत सरकार की संस्थाएं (मंत्रालय, एजेंसियां)।
- सैन्य और रक्षा संगठन।
- अनुसंधान संस्थान और विश्वविद्यालय।
- दूरसंचार कंपनियां।
- संभावित रूप से अन्य क्षेत्रों को रणनीतिक रूप से महत्वपूर्ण माना जाता है।

फ़िशिंग लालच (रक्षा, विदेशी मामलों, सरकारी अनुप्रयोगों के सुरक्षा अद्यतन) के विषय लक्ष्य और प्रेरणाओं के इस आकलन को सुदृढ़ करते हैं।

समझौते के विस्तृत संकेतक (आईओसी)

- **C2 सर्वर के IP पते (2023-2025):**
    - 45.153.241.15: APT2 मैलवेयर नमूनों से संबंधित C36 संचार में देखा गया।
    - 91.215.85.21: अक्सर क्रिमसन और एलिजा आरएटी के लिए कमांड और नियंत्रण गतिविधियों से जुड़ा हुआ है।
    - 185.140.53.206: डेटा बहिर्गमन के लिए संपर्क बिंदु के रूप में उपयोग किया जाता है।
    - 192.241.207.45: सर्वर संभावित रूप से दुर्भावनापूर्ण वेब संरचना घटकों (फ़िशिंग पृष्ठों) की मेजबानी कर रहा है।
    - 103.145.13.187: दुर्भावनापूर्ण पेलोड के वितरण में शामिल आईपी पता।
- **फ़ाइल हैश (SHA-256):**
    - 3c2cfe5b94214b7fdd832e00e2451a9c3f2aaf58f6e4097f58e8e5a2a7e6fa34 (Poseidon मैलवेयर): Poseidon RAT के एक विशिष्ट स्ट्रेन की पहचान करता है।
    - bd5602fa41e4e7ad8430fc0c6a4c5d11252c61eac768835fd9d9f4a45726c748 (क्रिमसन आरएटी) : हस्ताक्षर अद्वितीय d'une variante de Crimson RAT.
    - 9f3a5c7b5d3f83384e2ef98347a6fcd8cde6f7e19054f640a6b52e61672dbd8f (ElizaRAT लोडर): आपको प्रारंभिक ElizaRAT परिनियोजन कार्यक्रम का पता लगाने की अनुमति देता है।
    - 2d06c1488d3b8f768b9e36a1a5897cc6f87a2f37b8ea8e8d0e3e5aebf9d7c987 (CapraRAT APK) : Hash de l'application Android malveillante CapraRAT.
- **दुर्भावनापूर्ण डोमेन:**
    - कवच-अप् प[.]com: सुरक्षा अनुप्रयोग "Kavach" की नकल, संभवतः CapraRAT वितरित करने के लिए उपयोग की जाती है।
    - इंडियापोस्ट-गवर्न[.]org: भारतीय डाक सेवा साइट का प्रतिरूपण करता है, जिसका उपयोग फ़िशिंग या दुर्भावनापूर्ण अनुलग्नकों को वितरित करने के लिए किया जाता है।
    - gov-inportal[.]org: सिविल सेवकों को लक्षित करने के लिए भारत सरकार के पोर्टल की नकल करने का प्रयास।
    - भारतीय मंत्रालय[.]कॉम: भारतीय मंत्रालयों को लक्षित करने के लिए सामान्य लेकिन विश्वसनीय डोमेन नाम।
    - सिक्योरकवच[।में: "कवच" की नकल करने का एक और प्रयास, जिसका उद्देश्य भारतीय उपयोगकर्ताओं के लिए वैध दिखना है।
- **संदिग्ध URL:**
    - http://kavach-app.com/update: "Kavach" ऐप के लिए नकली अपडेट URL, CapraRAT के लिए संभावित वितरण बिंदु।
    - http://gov-inportal.org/download/defense-docs.exe: एक रक्षा दस्तावेज के रूप में प्रच्छन्न एक दुर्भावनापूर्ण निष्पादन योग्य से लिंक करें।
    - http://securekavach.in/assets/login.php: क्रेडेंशियल चोरी करने के लिए संभावित फ़िशिंग पृष्ठ।
    - https://indiapost-gov.org/track/status.aspx: एक परिष्कृत फ़िशिंग पृष्ठ, जो संवेदनशील जानकारी को मैलवेयर डालने या डाउनलोड करने के लिए प्रलोभन देने के लिए पैकेज ट्रैकिंग की नकल करता है.
- **फ़िशिंग फ़ाइल नाम:**

- Briefing_MoD_April25.docx: डिकॉय संभावित रूप से रक्षा मंत्रालय को लक्षित कर रहा है।
- Alert_Kavach_Update.exe: "कवच" के लिए झूठी अपडेट अलर्ट शायद एक आरएटी वितरित कर रही है।
- IndiaDefense2025_strategy.pdf: भारतीय रक्षा पर रणनीतिक जानकारी युक्त डिकॉय।
- MoEA_internal_memo_23.rtf: विदेश मंत्रालय से नकली आंतरिक ज्ञापन।
- academic-research-invite.scr: एक अकादमिक आमंत्रण के रूप में दुर्भावनापूर्ण स्क्रीनसेवर।

- **नकली Android अनुप्रयोग पैकेज नाम:**
  - com.kavach.update.apk: दुर्भावनापूर्ण पैकेज "कवच" के अद्यतन के रूप में मुखौटा लगा रहा है।
  - com.defensebriefing.alert.apk: रक्षा से संबंधित दुर्भावनापूर्ण एंड्रॉइड ऐप।
  - com.india.education.portal.apk: एक भारतीय एजुकेशनल पोर्टल से जुड़ा फर्जी ऐप।
- **म्यूटेक्स:**
  - ग्लोबल\CrimsonRAT_Active: विंडोज सिस्टम पर क्रिमसन आरएटी की सक्रिय उपस्थिति को इंगित करता है।
  - Local\ElizaRATSession: एक सक्रिय Eliza RAT सत्र इंगित करता है।
  - \Sessions\BaseNamedObjects\CapraMobileMutex: CapraRAT के Android संस्करण के लिए विशिष्ट म्यूटेक्स।
- **रजिस्ट्री कुंजियाँ (विंडोज़):**
  - HKEY_CURRENT_USER\Software\CrimsonRAT: क्रिमसन RAT द्वारा अपने कॉन्फ़िगरेशन को स्टोर करने के लिए उपयोग की जाने वाली कुंजी।
  - HKEY_LOCAL_MACHINE\SYSTEM\ElizaRAT\Persistence: ElizaRAT के लिए एक दृढ़ता तंत्र का संकेत देने वाली कुंजी।
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\CapraStart: CapraRAT के लिए स्वचालित स्टार्टअप कुंजी।
- **ज्ञात उपयोगकर्ता-एजेंट:**
  - मोज़िला/5.0 (विंडोज एनटी 10.0; विन64; x64) APT36Client/1.0: वापरकर्ता-एजंट संभाव्य संप्रेषण साधन किंवा APT36-विशिष्ट इम्प्लांटद्वारे वापरले जाते.
  - TelegramBot-ElizaRAT/2.5: C2 संचार के लिए एलिजा RAT द्वारा टेलीग्राम API के उपयोग को इंगित करता है।
  - CapraAndroidAgent/1.4: Android उपकरणों पर Capra दुर्भावनापूर्ण एजेंट की पहचान करने वाला उपयोगकर्ता-एजेंट।
- **पेलोड में प्रयुक्त एन्कोडेड/अस्पष्ट तार:**
  - bXlQYXNzd29yZDEyMw==: एक Base64-एन्कोडेड स्ट्रिंग, "myPassword123" के रूप में डिकोडिंग, संभावित रूप से हार्ड-कोडेड पहचानकर्ता या कॉन्फ़िगरेशन स्ट्रिंग।
  - JAB1c2VyID0gIkFkbWluIg==: एक और Base64 स्ट्रिंग, $user="व्यवस्थापक" को डिकोडिंग, दुर्भावनापूर्ण संचालन के लिए PowerShell के उपयोग का सुझाव देता है।
  - eval(decodeURIComponent('%75%70%64%61%74%65')): अस्पष्ट JavaScript कोड, जिसे जब डी-एन्कोड किया जाता है और उसका मूल्यांकन किया जाता है, तो "अपडेट" फ़ंक्शन निष्पादित होता है, जो संभावित रूप से दुर्भावनापूर्ण अपडेट या डायनामिक कोड निष्पादन सुविधा का संकेत देता है।

शमन और पता लगाने के उपाय

- **सामान्य सिफारिशें:**
    - **स्पीयरफ़िशिंग के खतरे के बारे में जागरूकता:** कर्मचारियों को संदिग्ध ईमेल की पहचान करने, प्रेषकों की प्रामाणिकता सत्यापित करने और अज्ञात या अवांछित स्रोतों से लिंक या खुले अनुलग्नकों पर क्लिक न करने के लिए प्रशिक्षित करें।
    - **मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए) लागू करें:** पासवर्ड के अलावा प्रमाणीकरण के दूसरे रूप की आवश्यकता के द्वारा खाता सुरक्षा को मजबूत करें।
    - **सिस्टम और सॉफ़्टवेयर को अद्यतित रखना:** भेद्यता शोषण के जोखिम को कम करने के लिए ऑपरेटिंग सिस्टम, एप्लिकेशन और वेब ब्राउज़र के लिए नियमित रूप से सुरक्षा पैच लागू करें।
    - **नेटवर्क विभाजन:** नेटवर्क को खंडित करके और सख्त अभिगम नियंत्रण नीतियों को लागू करके खतरों के प्रसार को सीमित करें।
    - **नेटवर्क ट्रैफ़िक और लॉग मॉनिटरिंग:** संदिग्ध नेटवर्क गतिविधि, ज्ञात IP पतों और C2 डोमेन से संचार और असामान्य एक्सेस प्रयासों का पता लगाने के लिए मॉनिटरिंग सिस्टम लागू करें। नियमित रूप से सिस्टम और एप्लिकेशन लॉग का विश्लेषण करें।
    - **मजबूत सुरक्षा समाधानों का उपयोग करें:** एंटी-वायरस समाधान, समापन बिंदु पहचान और प्रतिक्रिया (EDR) सिस्टम, और घुसपैठ की रोकथाम और पहचान (IDS/IPS) सिस्टम को तैनात और बनाए रखें।

- **IOCs पर आधारित विशिष्ट उपाय:**
    - **IOC ब्लॉकिंग:** APT36 से जुड़े संचार और मैलवेयर को ब्लॉक करने के लिए पहचाने गए IP पते, डोमेन और फ़ाइल हैश को फ़ायरवॉल, DNS सर्वर, एंटीवायरस समाधान और वेब फ़िल्टरिंग सिस्टम में एकीकृत करें।
    - **नियम-आधारित पहचान:** सिस्टम और लॉग में मैलवेयर और APT36 गतिविधियों के पैटर्न और विशेषताओं की पहचान करने के लिए यारा और सिग्मा नियम (यदि उपलब्ध हो) लागू करें।
    - **यातायात निरीक्षण:** संदिग्ध उपयोगकर्ता एजेंटों (APT36Client/1.0, TelegramBot-ElizaRAT/2.5, CapraAndroidAgent/1.4) के लिए नेटवर्क ट्रैफ़िक का निरीक्षण करने के लिए सुरक्षा प्रणालियों को कॉन्फ़िगर करें।
    - **रजिस्ट्री और म्यूटेक्स मॉनिटरिंग:** APT36 द्वारा उपयोग किए जाने वाले RATs से जुड़ी रजिस्ट्री कुंजियों और म्यूटेक्स के निर्माण का पता लगाने के लिए एंडपॉइंट मॉनिटरिंग टूल का उपयोग करें।
    - **ईमेल स्कैनिंग:** ज्ञात फ़ाइल नाम और फ़िशिंग URL वाले संदेशों को पहचानने और ब्लॉक करने के लिए स्पैम फ़िल्टर और ईमेल स्कैनिंग समाधान लागू करें।
    - **मोबाइल डिवाइस सुरक्षा:** मोबाइल सुरक्षा समाधान परिनियोजित करें और उपयोगकर्ताओं को अज्ञात स्रोतों से ऐप्स इंस्टॉल करने के जोखिमों के बारे में शिक्षित करें। दुर्भावनापूर्ण पैकेज नामों की उपस्थिति के लिए Android उपकरणों की निगरानी करें।

- **घटना प्रतिक्रिया रणनीतियाँ:**
    - **प्रतिक्रिया योजना:** APT खतरों के लिये विशिष्ट साइबर सुरक्षा घटना प्रतिक्रिया योजना विकसित करना और उसका रखरखाव करना, जिसमें APT36 से संबंधित गतिविधि का पता लगाने की स्थिति में अनुसरण करने के चरण शामिल हैं।
    - **अलगाव:** एक संदिग्ध समझौता की स्थिति में, हमले के प्रसार को रोकने के लिए प्रभावित सिस्टम को तुरंत नेटवर्क से अलग करें।

- **फोरेंसिक विश्लेषण:** उल्लंघन के दायरे को निर्धारित करने, समझौता किए गए डेटा की पहचान करने और हमलावरों द्वारा उपयोग की जाने वाली रणनीति को समझने के लिए गहन फोरेंसिक विश्लेषण करें।
- **उन्मूलन:** समझौता किए गए सिस्टम से हमलावरों द्वारा उपयोग किए जाने वाले मैलवेयर, दृढ़ता तंत्र और उपकरणों को पूरी तरह से हटा दें।
- **पुनर्स्थापित करें:** स्वच्छ, सत्यापित बैकअप से सिस्टम और डेटा पुनर्स्थापित करें।
- **सबक सीखा:** एक घटना के बाद, सुरक्षा उपायों और प्रतिक्रिया प्रक्रियाओं को बेहतर बनाने के लिए कारणों और प्रक्रियाओं का विश्लेषण करें।

संदर्भ

- https://www.zscaler.com/blogs/security-research/transparent-tribe-apt-targeting-india
- https://research.checkpoint.com/2023/transparent-tribe-evolution-of-a-cyber-espionage-threat/
- https://threatresearch.ext.hp.com/transparent-tribe-apt-group/
- यह तकनीकी संदर्भ दस्तावेज़ फ्रीमाइंडट्रॉनिक एंडोरा द्वारा प्रकाशित मूल विश्लेषण पर आधारित है, जो यहां उपलब्ध है: https://freemindtronic.com/apt36-spearphishing-india/

सुरक्षा मुद्रा को मजबूत करना: फ्रीमाइंडट्रॉनिक एचएसएम पारिस्थितिकी तंत्र

नीचे दी गई तालिका संक्षेप में बताती है कि APT36 द्वारा उपयोग किए जाने वाले प्रत्येक खतरे वेक्टर को फ्रीमाइंडट्रॉनिक के संप्रभु उपकरणों द्वारा कैसे कम किया जाता है - चाहे मोबाइल हो या डेस्कटॉप, फिक्स्ड या रिमोट, नागरिक या सैन्य-ग्रेड। यह खतरे से खतरे की तुलना करता है कि कैसे डेटाशिल्डर और पाससाइफर हमलों को कम करते हैं - चाहे मोबाइल, डेस्कटॉप या एयर-गैप्ड इन्फ्रास्ट्रक्चर पर।

APT36 रणनीति/मैलवेयर	**डेटाशिल्डर एनएफसी एचएसएम (लाइट/ऑथ/एम-ऑथ)**	**डेटाशिल्डर एचएसएम पीजीपी (विन/मैकओएस)**	**PassCypher NFC HSM (Android)**	**पाससाइफर एचएसएम पीजीपी (विन/मैकओएस)**
स्पीयरफिशिंग (इंडिया पोस्ट, कवच)	✓ क्यूआर-कोड एन्क्रिप्शन + सैंडबॉक्स	✓ हस्ताक्षर जांच + ऑफ़लाइन पीजीपी	✓ यूआरएल सैंडबॉक्स + कोई इंजेक्शन नहीं	✓ सैंडबॉक्स्ड पीजीपी कंटेनर
क्रिमसन चूहा	✓ एनएफसी संक्रमित ओएस से बचा जाता है	✓ कोई सिस्टम-संग्रहीत कुंजी नहीं	✓ रहस्य ऑफ-डिवाइस	✓ कोई मेमोरी एक्सपोजर नहीं
एलिजारैट	✓ कोई क्लाउड या रैम एक्सेस नहीं	✓ एचएसएम में पीजीपी कुंजी पृथक	कोई रैम उपयोग / कोई क्लिपबोर्ड नहीं	✓ URL मेल खाने पर ही OTP
अपोलोस्टीलर	✓ क्रेडेंशियल्स कभी उजागर नहीं हुए	✓ कुंजी सिस्टम में कभी लोड नहीं हुई	✓ क्लिपबोर्ड चोरी के लिए प्रतिरक्षा	✓ फ़िशिंग-प्रूफ लॉगिन

पोसीडॉन (लिनक्स पर नकली कवच)	✓ केवल-NFC: समझौता किए गए OS को बायपास करता है	मैं लिनक्स-संगत नहीं	मैं Android पर नहीं	✓ कोई ओएस निर्भरता नहीं
CapraRAT (एंड्रॉइड)	मैं (Android पर नहीं)	✗	✓ ऐप में कभी स्टोर नहीं हुए राज	✓ केवल डेस्कटॉप-युग्मित उपयोग
ClickFix (आदेश इंजेक्शन)	✓ कोई शेल इंटरैक्शन संभव नहीं है	✓ पीजीपी सत्यापन	✓ कोई टाइपिंग / कोई चिपकाना नहीं	✓ कोई टर्मिनल इंटरैक्शन नहीं
टेलीग्राम / क्लाउड C2 दुरुपयोग	✓ कोई क्लाउड उपयोग बिल्कुल नहीं	✓ पूरी तरह से ऑफ़लाइन	✓ 100% ऑफ़लाइन	✓ 100% ऑफ़लाइन
सीईओ फ्रॉड /	✓ Auth/M-Auth मॉड्यूल ऑर्डर एन्क्रिप्ट करते हैं	✓ डिजिटल हस्ताक्षर सुरक्षा	✓ कोई स्पूफिंग संभव नहीं है	✓ प्रतिरूपण को रोकता है

बेंचमार्किंग APT36 के परिष्कृत खतरों के खिलाफ संगठनों की सुरक्षा मुद्रा को मजबूत करने के लिए DataShielder और PassCypher सहित Freemindtronic के HSM पारिस्थितिकी तंत्र की महत्वपूर्ण क्षमता पर प्रकाश डालती है। हार्डवेयर-आधारित एन्क्रिप्शन को एकीकृत करके, संभावित रूप से समझौता किए गए ऑपरेटिंग सिस्टम वातावरण के बाहर चाबियों और रहस्यों का अलगाव, और मजबूत एंटी-फ़िशिंग सत्यापन तंत्र, ये समाधान APT36 जैसे उन्नत खिलाड़ियों द्वारा नियोजित कई डिजिटल जासूसी और विशेषाधिकार प्राप्त सूचना चोरी रणनीति के खिलाफ एक सक्रिय रक्षा बाधा प्रदान करते हैं। ऐसी एचएसएम प्रौद्योगिकियों को अपनाना लगातार खतरों के खिलाफ लचीलापन बढ़ाने की दिशा में एक महत्वपूर्ण कदम का प्रतिनिधित्व करता है।

PassCypher और DataShielder HSM NFC मॉड्यूल के बारे में अधिक जानकारी के लिए:
https://freemindtronic.com/shop/

Outlook और अगले चरण

APT36 (ट्रांसपेरेंट ट्राइब/मिथिक लेपर्ड) एक सतत और संरचित खतरे का प्रतीक है, जो मुख्य रूप से साइबर जासूसी उद्देश्यों के लिए रणनीतिक भारतीय संस्थाओं को लक्षित करता है। इसके अभियान परिष्कृत डिकॉय, कस्टम आरएटी और एक चुस्त C2 बुनियादी ढांचे पर निर्भर करते हैं।

उनकी रणनीति, तकनीकों और प्रक्रियाओं (टीटीपी) के साथ-साथ वर्तमान में ज्ञात समझौता संकेतक (आईओसी) की गहन समझ, पहचान, रक्षा और प्रतिक्रिया नीतियों का मार्गदर्शन करने के लिए एक ठोस आधार प्रदान करती है। इस समूह द्वारा उपयोग की जाने वाली तकनीकों के निरंतर विकास का सामना करते हुए, निरंतर सतर्कता की मुद्रा आवश्यक है।

यह दस्तावेज़ एक विकसित तरीके से तैयार किया गया है। हमारा मानना है कि नवीनतम उपलब्ध APT36 इंटेलिजेंस के साथ संरेखित सक्रिय सुरक्षा मुद्रा बनाए रखने के लिए इसे नए खतरों और उपकरणों के साथ अद्यतित रखना आवश्यक है।