Analiza Incydentu Bezpieczeństwa i Plan Działania: Atak na Repozytorium GitHub "LukeStriderGM/BLOX-TAK-SERVER-IUCP"

Streszczenie Zarządcze

Niniejsza analiza potwierdza, że zaobserwowana aktywność stanowi celową i aktywną próbę podszywania się (phishing/spoofing) pod legalne repozytorium GitHub LukeStriderGM/BLOX-TAK-SERVER-IUCP. Atakujący wykorzystuje infrastrukturę chmurową zlokalizowaną w Chinach, hostując złośliwą kopię strony na serwerze o adresie IP 175.178.70.242, należącym do dostawcy Tencent Cloud. Szczególnie alarmujący jest fakt, że złośliwy adres URL został pomyślnie zaindeksowany przez wyszukiwarkę Google, co znacząco zwiększa ryzyko dotarcia do nieświadomych użytkowników i potęguje zasięg ataku.
Specyfika projektu, TAK Server (Team Awareness Kit), który jest narzędziem wykorzystywanym przez służby mundurowe, agencje rządowe i zespoły reagowania kryzysowego, sugeruje, że atak jest wysoce ukierunkowany i może mieć na celu kompromitację systemów o znaczeniu krytycznym. Podnosi to wagę incydentu ponad poziom standardowej cyberprzestępczości.
Rekomendowany plan działania obejmuje trzy kluczowe filary: natychmiastowe zgłoszenie nadużycia do dostawcy hostingu (Tencent Cloud) oraz do Google w celu usunięcia złośliwej treści z publicznego dostępu; transparentną komunikację z potencjalnymi ofiarami i społecznością projektu; oraz wdrożenie długoterminowych środków wzmacniających bezpieczeństwo projektu i jego cyfrowego śladu.

1. Analiza Incydentu i Wektor Ataku

1.1. Rekonstrukcja Łańcucha Ataku (Attack Chain)

Analiza dostarczonych dowodów pozwala na zrekonstruowanie wieloetapowego łańcucha ataku, który wykorzystuje zaufanie do platformy GitHub i popularności docelowego projektu.

1. **Klonowanie i Podszywanie się (Spoofing):** Atakujący stworzył stronę internetową, która wizualnie i strukturalnie naśladuje stronę repozytorium GitHub LukeStriderGM/BLOX-TAK-SERVER-IUCP. Złośliwy adres URL, http://175.178.70.242:1111/LukeStriderGM/BLOX-TAK-SERVER-IUCP/, precyzyjnie imituje ścieżkę do legalnego projektu, co ma na celu zmylenie użytkownika.
2. **Hostowanie Złośliwej Treści (Hosting):** Fałszywa strona została umieszczona na serwerze z adresem IP 175.178.70.242. Dostęp do niej odbywa się przez niestandardowy port 1111. Wykorzystanie nietypowego portu może być celową techniką unikania podstawowych skanerów bezpieczeństwa i reguł firewall, które często monitorują wyłącznie standardowy ruch na portach 80 (HTTP) i 443 (HTTPS).
3. **Zwiększanie Wiarygodności i Zasięgu (Discovery & Delivery):** Kluczowym elementem

ataku jest pomyślne zaindeksowanie złośliwego adresu URL przez wyszukiwarkę Google [Image 3]. Ten krok przekształca pasywnie hostowaną stronę w aktywny i skalowalny wektor ataku. Użytkownicy, poszukując informacji o projekcie za pomocą popularnych wyszukiwarek, mogą nieświadomie trafić na fałszywą wersję, uznając ją za autentyczną. Ta taktyka jest charakterystyczna dla kampanii typu "repo confusion", gdzie zaufanie do znanych platform jest wykorzystywane jako broń przeciwko użytkownikom.

4. **Potencjalna Realizacja Celu (Execution):** Użytkownik, który trafia na złośliwą stronę, jest narażony na szereg zagrożeń. Celem atakującego jest najprawdopodobniej nakłonienie ofiary do pobrania zmodyfikowanego kodu źródłowego lub skompilowanej aplikacji. Taki kod może zawierać ukryte złośliwe oprogramowanie, takie jak trojany zdalnego dostępu (np. AsyncRAT, Quasar), info-stealery (np. LummaC2, RedLine Stealer) kradnące poświadczenia i dane z przeglądarek, lub backdoory umożliwiające przejęcie kontroli nad systemem ofiary. Alternatywnie, strona może służyć do klasycznego phishingu, próbując wyłudzić poświadczenia do konta GitHub lub innych usług.

1.2. Analiza Infrastruktury Adwersarza

Infrastruktura wykorzystana w ataku została zidentyfikowana i przeanalizowana przy użyciu narzędzi OSINT (Open-Source Intelligence).

- **Adres IP:** 175.178.70.242
- **Reputacja IP:** Skanery bezpieczeństwa, w tym te widoczne na dostarczonych zrzutach ekranu (VirusTotal, G-Data, Emsisoft), jednoznacznie flagują ten adres jako złośliwy, powiązany z phishingiem lub inną szkodliwą działalnością [Image 1, Image 2].
- **System Autonomiczny (ASN):** 45090
- **Właściciel ASN:** Shenzhen Tencent Computer Systems Company Limited, działający jako Tencent Cloud [Image 1].

Analiza reputacji ASN 45090 w publicznych bazach danych o zagrożeniach potwierdza, że jest on często nadużywany do celów przestępczych. Baza ThreatFox zawiera liczne wskaźniki kompromitacji (Indicators of Compromise, IOCs) z tego ASN, powiązane z serwerami Command & Control (C2) dla popularnych narzędzi ofensywnych, takich jak Cobalt Strike i GoPhish. Z kolei serwis CleanTalk wskazuje, że znaczący odsetek (blisko 8%) adresów IP w ramach tego ASN wykazuje aktywność spamerską.

Wybór dużego, globalnego dostawcy chmury, takiego jak Tencent Cloud, jest strategiczną decyzją ze strony atakującego. Pozwala mu to "ukryć się w tłumie" milionów legalnych usług, co utrudnia wykrycie. Ponadto, procesy zgłaszania nadużyć u tak dużych operatorów mogą być bardziej zbiurokratyzowane i wolniejsze, co daje atakującemu cenne okno czasowe na przeprowadzenie ataku, zanim infrastruktura zostanie zablokowana. Notoryczne wykorzystywanie tego ASN do hostowania serwerów C2 sugeruje, że atakujący może być częścią większego ekosystemu cyberprzestępczego lub po prostu korzysta z gotowych, tzw. "kuloodpornych" rozwiązań hostingowych.

1.3. Prawdopodobne Cele i Motywacje Atakującego

Nazwa repozytorium, BLOX-TAK-SERVER-IUCP, wskazuje, że projekt jest związany z oprogramowaniem **TAK Server (Team Awareness Kit)**. Jest to zaawansowana platforma geoprzestrzenna i komunikacyjna, pierwotnie opracowana na potrzeby wojska Stanów Zjednoczonych, a obecnie szeroko stosowana przez siły zbrojne, agencje rządowe, służby ratownicze i zespoły reagowania kryzysowego na całym świecie.

Ten kontekst jest kluczowy dla zrozumienia motywacji atakującego. Użytkownicy i administratorzy systemów TAK to personel o potencjalnie wysokim znaczeniu (high-value targets), a dane przetwarzane przez te systemy są niezwykle wrażliwe. W związku z tym, atak na repozytorium dostarczające narzędzia dla tej społeczności jest znacznie poważniejszy niż typowy, masowy phishing. Prawdopodobne motywacje obejmują:

1. **Szpiegostwo (Targeted Espionage):** Najbardziej prawdopodobny scenariusz. Celem jest dystrybucja zmodyfikowanej, złośliwej wersji serwera TAK, która pozwoliłaby atakującemu uzyskać dostęp do danych operacyjnych w czasie rzeczywistym, takich jak lokalizacja personelu, treść komunikacji, plany misji czy dane z sensorów. Skompromitowanie serwera TAK może dać atakującemu "oczy i uszy" wewnątrz organizacji, która go używa.
2. **Kradzież Poświadczeń (Credential Theft):** Atak może być ukierunkowany na deweloperów i administratorów systemów TAK w celu przejęcia ich poświadczeń, co mogłoby posłużyć do dalszych, bardziej zaawansowanych ataków.
3. **Atak na Łańcuch Dostaw Oprogramowania (Software Supply Chain Attack):** Autor repozytorium, jako zaufane źródło oprogramowania dla specyficznej i wrażliwej społeczności, stał się celem ataku. Kompromitując jedno źródło, atakujący ma nadzieję dotrzeć do wielu celów końcowych.

Waga incydentu przesuwa się z kategorii cyberprzestępczości finansowej w kierunku potencjalnej operacji wywiadowczej, być może sponsorowanej przez państwo (APT) lub prowadzonej przez wysoce wyspecjalizowaną grupę przestępczą.

1.4. Ocena Ryzyka i Potencjalnego Wpływu

Na podstawie powyższej analizy, poziom ryzyka związanego z incydentem jest następujący:

- **Ryzyko dla Użytkowników Końcowych: Krytyczne.** Pobranie i uruchomienie złośliwego oprogramowania z fałszywej strony może prowadzić do całkowitej kompromitacji systemów i sieci, kradzieży wysoce wrażliwych danych operacyjnych, a w skrajnych przypadkach nawet do zagrożenia bezpieczeństwa fizycznego personelu polegającego na systemie TAK.
- **Ryzyko dla Reputacji Autora i Projektu: Wysokie.** Nawet jeśli oryginalne repozytorium jest w 100% bezpieczne, istnienie złośliwego klona może podważyć zaufanie do projektu. Użytkownicy mogą zacząć go unikać z obawy przed pomyłką, co zaszkodzi jego rozwojowi i adopcji.
- **Ryzyko dla Ekosystemu GitHub: Średnie.** Incydent ten wpisuje się w szerszy, niepokojący trend wykorzystywania zaufanych platform deweloperskich do dystrybucji malware i prowadzenia kampanii phishingowych, co stopniowo podważa ogólne zaufanie do ekosystemu open-source.

Najważniejszym czynnikiem potęgującym ryzyko jest zaindeksowanie złośliwej strony przez Google. To sprawia, że atak staje się pasywny, skalowalny i nie wymaga od atakującego aktywnej dystrybucji linków. Ofiary same odnajdują złośliwą pułapkę. W związku z tym, kluczowe staje się nie tylko zablokowanie serwera, ale także jak najszybsze "oczyszczenie" publicznej przestrzeni informacyjnej, czyli wyników wyszukiwania.

2. Plan Działania: Faza Natychmiastowej Reakcji i Ograniczania Szkód (Containment & Eradication)

Poniższy plan przedstawia precyzyjne kroki, które należy podjąć w celu jak najszybszej neutralizacji bezpośredniego zagrożenia. Działania należy prowadzić równolegle na kilku frontach.

2.1. Zgłoszenie Nadużycia do Dostawcy Usług Hostingowych (Tencent Cloud)

Celem jest doprowadzenie do natychmiastowego zablokowania dostępu do adresu IP 175.178.70.242 lub usunięcia złośliwej treści przez dostawcę infrastruktury.
Procedura:

1. **Wypełnienie formularza online:** Należy skorzystać z oficjalnego formularza Tencent Cloud do zgłaszania nielegalnych treści: https://www.tencentcloud.com/report-platform/illegalcontentcomplaint. W formularzu należy precyzyjnie podać złośliwy URL, wybrać kategorię zagrożenia (np. Phishing/Malware) i w opisie szczegółowo wyjaśnić sytuację, załączając dowody (np. zrzuty ekranu).
2. **Wysłanie formalnego zgłoszenia e-mailem:** Aby zwiększyć szansę na szybką reakcję, należy wysłać zgłoszenie bezpośrednio do działów odpowiedzialnych za bezpieczeństwo i zgodność.
    - **Adresaci:** compliance@tencent.com , cloud_sec@tencent.com
    - **Sugerowany temat:** URGENT: Phishing and Malware Hosting on Tencent Cloud Infrastructure (IP: 175.178.70.242, ASN: 45090)
    - **Sugerowana treść:** W wiadomości należy zawrzeć szczegółowy opis incydentu, pełny złośliwy URL, adres IP, link do oryginalnego, legalnego repozytorium GitHub, a także wyjaśnienie, że celem ataku jest specjalistyczne oprogramowanie (TAK Server) używane przez służby, co podnosi wagę zagrożenia.

Typ Kontaktu	Adres / Link	Źródło	Uwagi
Formularz Online	https://www.tencentcloud.com/report-platform/illegalcontentcomplaint		Podstawowa i oficjalna droga zgłoszenia.
Email (Bezpieczeństwo)	cloud_sec@tencent.com		Bezpośredni kontakt do zespołu bezpieczeństwa chmury.
Email (Zgodność)	compliance@tencent.com		Kontakt do działu odpowiedzialnego za zgodność z prawem i politykami.

2.2. Zgłoszenie Złośliwego URL do Google Safe Browsing i Usunięcie z Wyników Wyszukiwania

Celem jest oflagowanie złośliwej strony jako niebezpiecznej w popularnych przeglądarkach internetowych (które korzystają z list Safe Browsing) oraz usunięcie jej z indeksu wyszukiwarki Google.
Procedura:

1. **Zgłoszenie Phishingu:** Należy użyć dedykowanego formularza Google Safe Browsing: https://safebrowsing.google.com/safebrowsing/report_phish/. Jest to najszybsza metoda

na oznaczenie strony jako wyłudzającej informacje.
2. **Zgłoszenie Malware:** Ponieważ strona może dystrybuować złośliwe oprogramowanie, należy ją również zgłosić za pomocą formularza do zgłaszania malware: https://safebrowsing.google.com/safebrowsing/report_badware/.
3. **Zgłoszenie Spamu w Wynikach Wyszukiwania:** Aby poinformować algorytmy Google o próbie manipulacji rankingiem, można dodatkowo zgłosić stronę jako spam w wynikach wyszukiwania.

Cel Zgłoszenia	Link do Formularza	Źródło
Zgłoszenie Phishingu	https://safebrowsing.google.com/safebrowsing/report_phish/	
Zgłoszenie Malware	https://safebrowsing.google.com/safebrowsing/report_badware/	
Zgłoszenie Spamu	Formularz dostępny na stronach pomocy Google Search	

2.3. Formalne Zgłoszenie Incydentu do CERT Orange Polska

Wykorzystanie nawiązanego już kontaktu z krajowym zespołem reagowania na incydenty może przyspieszyć reakcję i potencjalnie doprowadzić do zablokowania szkodliwego adresu IP na poziomie krajowych operatorów telekomunikacyjnych.
Procedura:

1. **Wysłanie e-maila na adres:** cert.opl@orange.com.
2. **Treść wiadomości:** W e-mailu należy odwołać się do publicznego posta na LinkedIn, aby nadać sprawie kontekst. Należy przekazać wszystkie zebrane dowody i analizy, w tym złośliwy URL, adres IP, zrzuty ekranu oraz informację o specyficznym celu ataku (oprogramowanie TAK). Im więcej kontekstu otrzyma zespół CERT, tym skuteczniejsza może być jego interwencja.

2.4. Komunikacja Kryzysowa i Ostrzeżenie Społeczności

Natychmiastowe i transparentne poinformowanie legalnych użytkowników o zagrożeniu jest kluczowe dla ograniczenia szkód i utrzymania zaufania.
Procedura:

1. **Edycja pliku README.md:** W autentycznym repozytorium GitHub należy na samej górze pliku dodać duży, wyraźny blok ostrzegawczy. Powinien on informować o aktywnej próbie phishingu, podawać złośliwy adres IP/URL i kategorycznie podkreślać, że jedynym oficjalnym i bezpiecznym źródłem kodu jest to konkretne repozytorium na GitHub.
2. **Utworzenie pliku SECURITY.md:** Należy stworzyć w repozytorium plik SECURITY.md, w którym opisana zostanie polityka bezpieczeństwa projektu oraz procedura zgłaszania ewentualnych luk (nawet jeśli jest to prosty adres e-mail do kontaktu). Jest to profesjonalny standard, który podnosi wiarygodność projektu.
3. **Aktualizacja w mediach społecznościowych:** Należy opublikować aktualizację do pierwotnego posta na LinkedIn, informując, że incydent został potwierdzony, a kroki zaradcze zostały podjęte. Należy ponownie podać link do bezpiecznego repozytorium i ostrzec społeczność.

Proaktywna komunikacja przekształca autora z ofiary w aktywnego obrońcę swojego projektu.

Umieszczenie ostrzeżenia bezpośrednio w pliku README.md jest niezwykle skutecznym sposobem na dotarcie do najbardziej zainteresowanych osób – deweloperów i użytkowników, którzy z największym prawdopodobieństwem odwiedzą oficjalną stronę projektu.

3. Działania Długoterminowe: Wzmacnianie Bezpieczeństwa i Monitorowanie (Post-Incident Activity)

Po opanowaniu bezpośredniego kryzysu należy wdrożyć działania, które wzmocnią bezpieczeństwo projektu i zminimalizują ryzyko podobnych incydentów w przyszłości.

3.1. Audyt Bezpieczeństwa Repozytorium i Konta GitHub

1. **Włączenie Uwierzytelniania Dwuskładnikowego (2FA):** Jest to absolutny priorytet dla zabezpieczenia dostępu do konta GitHub.
2. **Przegląd Tokenów Dostępowych (Personal Access Tokens):** Należy przejrzeć wszystkie aktywne tokeny w ustawieniach konta i unieważnić te, które nie są rozpoznawane lub nie są już używane. Atakujący często wykorzystują skradzione tokeny do uzyskania nieautoryzowanego dostępu do API GitHub i modyfikacji repozytoriów.
3. **Przegląd Kluczy SSH i Deploy Keys:** Należy zweryfikować listę kluczy SSH i kluczy wdrożeniowych powiązanych z kontem i repozytoriami, usuwając wszelkie nieautoryzowane wpisy.
4. **Podpisywanie Commitów Kluczem GPG:** Wdrożenie tej praktyki kryptograficznie potwierdza, że zmiany w kodzie pochodzą od zaufanego autora. GitHub wizualnie oznacza takie commity jako "Verified", co zwiększa zaufanie użytkowników.

3.2. Strategia Monitorowania Śladu Cyfrowego Projektu

1. **Konfiguracja Google Alerts:** Należy utworzyć automatyczne alerty na frazy kluczowe, takie jak "LukeStriderGM/BLOX-TAK-SERVER-IUCP", "BLOX-TAK-SERVER-IUCP" download oraz inne wariacje nazwy projektu. Pozwoli to na szybkie wykrycie nowych prób podszywania się, które zostaną zaindeksowane przez Google.
2. **Regularne Wyszukiwanie na GitHub:** Należy okresowo przeszukiwać platformę GitHub w poszukiwaniu repozytoriów o podobnych lub identycznych nazwach. Atakujący często tworzą fałszywe klony lub forki bezpośrednio na GitHubie, aby zwiększyć ich pozorną wiarygodność.
3. **Monitorowanie Platform Dyskusyjnych:** Jeśli projekt posiada społeczność na platformach takich jak Discord, Reddit czy specjalistyczne fora, warto je monitorować pod kątem linków do nieoficjalnych wersji oprogramowania.

3.3. Wdrożenie Dobrych Praktyk Bezpieczeństwa w Projekcie Open Source

1. **Jasne Określenie Oficjalnych Kanałów Dystrybucji:** W pliku README.md należy wyraźnie zaznaczyć, że jedynym oficjalnym źródłem kodu jest to konkretne repozytorium GitHub. Jeśli publikowane są skompilowane wersje, należy podkreślić, że powinny być

one pobierane wyłącznie z zakładki "Releases" na oficjalnej stronie projektu.
2. **Stosowanie Sum Kontrolnych (Checksums):** Dla każdej opublikowanej wersji binarnej należy podawać sumy kontrolne plików (np. SHA-256). Umożliwi to użytkownikom samodzielną weryfikację integralności pobranych archiwów i upewnienie się, że nie zostały one zmodyfikowane.
3. **Utrzymanie Polityki SECURITY.md:** Sformalizowana polityka bezpieczeństwa powinna być stałym elementem projektu.

4. Podsumowanie i Wnioski Końcowe

Analizowany incydent to nie przypadkowy phishing, lecz wysoce ukierunkowany atak na łańcuch dostaw oprogramowania, wymierzony w specyficzną i wrażliwą społeczność użytkowników systemu TAK Server. Motywacją atakującego jest najprawdopodobniej szpiegostwo i chęć uzyskania dostępu do krytycznych danych, a nie bezpośrednia korzyść finansowa.
Incydent ten jest symptomem szerszego zjawiska, w którym cyberprzestępcy i aktorzy państwowi coraz częściej nadużywają zaufanych platform deweloperskich, takich jak GitHub, oraz globalnych dostawców chmury do prowadzenia zaawansowanych kampanii. Wykorzystują one reputację i skalę tych platform do ukrywania swojej działalności i skutecznego docierania do ofiar.
Proaktywna postawa autora projektu – wczesne wykrycie podejrzanej aktywności i publiczne nagłośnienie sprawy – jest kluczowym i godnym pochwały elementem skutecznej obrony. Działania opisane w przedstawionym planie pozwolą na zneutralizowanie bezpośredniego zagrożenia i wzmocnienie odporności projektu na przyszłość. Należy jednak pamiętać, że bezpieczeństwo projektu open-source, zwłaszcza o tak wrażliwym zastosowaniu, jest procesem ciągłym, wymagającym nieustannej czujności, monitorowania i wdrażania najlepszych praktyk.

Cytowane prace

1. Attack Demo #3: Github Abuse - Delivering Malware Using Trusted Platforms | RavenMail, https://ravenmail.io/blog/github-malware-delivery 2. GitHub Repos Used for Distributing Malware - Checkmarx, https://checkmarx.com/blog/github-repos-used-for-distributing-malware/ 3. 2024 Malicious Infrastructure Report | Recorded Future, https://go.recordedfuture.com/hubfs/reports/cta-2025-0228.pdf 4. Malicious code in fake GitHub repositories | Kaspersky official blog, https://www.kaspersky.com/blog/malicious-code-in-github/53085/ 5. Malware Distribution Service Exploits Thousands of GitHub Accounts - ChannelE2E, https://www.channele2e.com/brief/malware-distribution-service-exploits-thousands-of-github-accounts 6. ThreatFox | AS45090 - Abuse.ch, https://threatfox.abuse.ch/browse/tag/AS45090/ 7. AS45090 Shenzhen Tencent Computer Systems Company Limited - CleanTalk, https://cleantalk.org/blacklists/as45090 8. TAK-SERVER 5.0 - Rocky 8 made easy - YouTube, https://m.youtube.com/watch?v=zZgb4KVKtF0&pp=0gcJCdgAo7VqN5tD 9. TAK Server install (Docker) - YouTube, https://www.youtube.com/watch?v=h4PA9NN-cDk 10. Installing TAK Server 5.x (RPM Edition) - YouTube, https://www.youtube.com/watch?v=r9HD46w1czY 11. Tencent Cloud, https://www.tencentcloud.com/report-platform/illegalcontentcomplaint 12. Integrity Policy - Tencent 腾讯, https://www.tencent.com/en-us/integrity-policy.html 13. Tencent Cloud - FIRST — Forum of Incident Response and Security Teams,

https://www.first.org/members/teams/tencent_cloud 14. Report Spam, Phishing, or Malware | Google Search Central | Support, https://developers.google.com/search/help/report-quality-issues 15. Reporting Incorrect Data | Safe Browsing APIs (v4) - Google for Developers, https://developers.google.com/safe-browsing/v4/reporting 16. reporting scam sites - Google Search Central Community, https://support.google.com/webmasters/thread/264176403/reporting-scam-sites?hl=en 17. Kontakt - CERT Orange - Orange Polska, https://cert.orange.pl/kontakt/ 18. Terminologia - CERT Orange, https://cert.orange.pl/warto-wiedziec/terminologia/