**Złośliwe aplikacje mogą nas szpiegować – nowy rodzaj ataku na urządzenia z Androidem**

**Kraków, 12 stycznia 2021 –** Badacze firmy **Sophos** zidentyfikowali nowy rodzaj atakuna użytkowników urządzeń z systemem **Android**. Cyberprzestępcy stworzyli **fałszywe wersje** m.in. oficjalnej aplikacji rządowej Pakistanu, aplikacji firmy ubezpieczeniowej oraz porównywarki cen operatorów telefonicznych. Złośliwe wersje programów **przechwytują** z urządzeń **kontakty**, treść **wiadomości SMS**, dane z dokumentów tożsamości, informacje o lokalizacji czy **zdjęcia**, a następnie przesyłają je na serwery przestępców. Dotychczas celem były aplikacje dla użytkowników w Pakistanie, jednak atak może zostać łatwo powtórzony w każdym miejscu na świecie.

**Telefony na podsłuchu**

Fałszywe aplikacje są **identyczne jak ich legalne odpowiedniki** dostępne w Google Play Store, umożliwiają też korzystanie z tych samych funkcji. Przestępcy wybrali pięć programów działających w Pakistanie: oficjalną **aplikację rządową** Pakistan Citizen Portal, muzułmański zegar modlitewny, aplikację do porównywania ofert operatorów telefonicznych, narzędzie do sprawdzania ważności karty SIM oraz program firmy ubezpieczeniowej.

Złośliwe narzędzia po uruchomieniu przechwytują unikalny identyfikator IMEI urządzenia, informacje o lokalizacji, pełną listę kontaktów, treść wiadomości tekstowych, zestawienie połączeń czy katalogi karty SD. Aplikacja Pakistan Citizen Portal skłania też użytkowników do **podania** swojego **numeru dowodu osobistego**, danych paszportowych, **haseł** do Facebooka i innych serwisów. Niektóre ze sfałszowanych aplikacji zawierają mechanizm umożliwiający **nagrywanie rozmów telefonicznych i dźwięków** rejestrowanych przez urządzenie. Funkcje te nie zostały jednak jeszcze aktywowane przez przestępców.

**„Czerwona lampka” dla wszystkich użytkowników**

Fałszywe wersje aplikacji nie są dostępne w oficjalnym sklepie Google Play Store, ale na stronach imitujących m.in. pakistański serwis rządowy. Użytkownicy mogli otrzymać **linki** z instrukcją pobrania programów m.in. **SMS-em** lub **mailem**. Cyberprzestępcy szyfrują przy tym stworzony przez siebie kod, instalowana aplikacja **nie jest** więc **identyfikowana jako złośliwa** podczas wstępnego skanowania przez urządzenie.

Odkryte programy szpiegujące to **sygnał ostrzegawczy** dla użytkowników nie tylko w Pakistanie, ale i **na całym świecie**.Przestępcy coraz częściej przeprowadzają bowiem ataki na telefony komórkowe, aby przechwycić wrażliwe dane i uzyskać **dostęp w czasie rzeczywistym** do lokalizacji zainfekowanego urządzenia, a nawet rozmów odbywających się w jego zasięgu.

**–** *Każdy, kto korzysta z telefonu komórkowego, powinien pamiętać o podstawowych zasadach ochrony: nieklikaniu w linki otrzymywane mailem czy SMS-em i pobieraniu aplikacji tylko z oficjalnych źródeł. Ważne jest także zwracanie uwagi na uprawnienia, o które prosi instalowany program. Jeśli zegar czy porównywarka ofert żąda dostępu do wiadomości, listy kontaktów czy zdjęć, powinno to wzbudzić czujność. Warto też rozważyć instalację na urządzeniu mobilnym programu antywirusowego, który będzie chronił dane przed podobnymi zagrożeniami –* wskazuje **Łukasz Formas, kierownik zespołu inżynierów w firmie Sophos.**

**Informacje o firmie**

Jako światowy lider zabezpieczeń nowej generacji, Sophos chroni przed najbardziej zaawansowanymi cyberzagrożeniami ponad 400 tys. firm różnej wielkości w ponad 150 krajach. Rozwiązania Sophos wykorzystują chmurę i sztuczną inteligencję, aby zabezpieczać urządzenia końcowe (laptopy, serwery i urządzenia mobilne) oraz sieci przed ewoluującymi metodami cyberprzestępców. Przy wsparciu SophosLabs – globalnego zespołu badającego zagrożenia – firma odpowiada na zagrożenia takie jak ransomware, malware, exploity, eksfiltracja danych, phishing czy indywidualnie dokonywane włamania przez cyberprzestępców. Platforma do zarządzania w chmurze Sophos Central integruje całe portfolio produktów nowej generacji Sophos w jeden system „zsynchronizowanej ochrony”, dostępny przez zestaw interfejsów API i obejmujący m.in. rozwiązanie Intercept X dla urządzeń końcowych oraz zaporę sieciową nowej generacji z rodziny XG Firewall. Firma oferuje również usługi łączące posiadaną technologię oraz aktywne przeciwdziałanie zagrożeniom (Managed Threat Response), szczególnie istotne w zmieniającym się dynamicznie świecie.

Sophos dąży do rozwijania i oferowania rozwiązań nowej generacji, aby zapewnić każdemu przedsiębiorstwu najwyższej klasy ochronę, zachowując jednocześnie prostotę zarządzania i umożliwiając redukcję kosztów. Wykorzystuje do tego m.in. zaawansowane funkcje infrastruktury chmurowej, uczenie maszynowe, interfejsy API, automatyzację i zarządzanie sposobami reagowania na zagrożenia. Firma sprzedaje swoje produkty i usługi za pośrednictwem globalnej sieci ponad 53 tys. partnerów i dostawców usług zarządzanych (MSP). Z innowacyjnych technologii Sophos mogą skorzystać także konsumenci indywidualni dzięki rodzinie rozwiązań Sophos Home. Firma ma siedzibę w Oksfordzie w Wielkiej Brytanii.

Więcej informacji można znaleźć na stronie www.sophos.com.