kaspersky

# Szkodnik Rovnix powraca z nowymi funkcjami kradzieży danych

23 czerwca 2020 r.

**W kwietniu 2020 r. badacze z firmy Kaspersky zaobserwowali powrót znanego bootkita Rovinx w kampanii wykorzystującej obecną pandemię. Bootkity to wyrafinowane narzędzia mające na celu ładowanie szkodliwego kodu na jak najwcześniejszym etapie uruchamiania systemu operacyjnego, jeszcze przed aktywacją funkcji bezpieczeństwa. Uaktualniony bootkit Rovnix dostarczał na komputery ofiar trojana wyposażonego w funkcje szpiegowskie.**

Bootkit Rovnix był bardzo popularny do czasu, gdy w 2013 r. jego kod źródłowy stał się wskutek wycieku dostępny dla wszystkich producentów rozwiązań bezpieczeństwa i innych zainteresowanych stron. Jednak w połowie kwietnia 2020 r. systemy monitorowania zagrożeń firmy Kaspersky ponownie wykryły szkodliwe pliki zawierające tego sławnego bootkita. Był on rozprzestrzeniany w rosyjskojęzycznym pliku wykonywalnym o nazwie, którą można przetłumaczyć tak: „Na temat inicjatywy Światowego Banku w związku z pandemią koronawirusa".

Nowa wersja bootkita zawierała kilka usprawnień, takich jak możliwość obchodzenia mechanizmu kontroli konta użytkownika i podnoszenia uprawnień na urządzeniu, a także moduł ładujący, który zwykle nie jest kojarzony z tym konkretnym bootkitem. Analiza wykrytych plików wykazała, że szkodliwą funkcję stanowił trojan otwierający tylną furtkę (tzw. backdoor) i pozwalający na szpiegowanie ofiar. To oznacza, że po instalacji szkodnika na zainfekowanym sprzęcie atakujący miałby dostęp do urządzenia i mógłby gromadzić różnego rodzaju informacje.

Bootkit był rozprzestrzeniany za pośrednictwem samorozpakowującego się archiwum, które zawierało dokument Worda oraz wykonywalny szkodliwy kod. Dla większej wiarygodności dokument rzeczywiście zawierał informacje na temat nowej inicjatywy Światowego Banku, a w metadanych podano jako jego autorów rzeczywiste osoby związane z tą organizacją. Jednak po otwarciu plik ładował bootkita i rozpoczynał proces infekcji.

*Opisany przykład zwraca uwagę na dwie kwestie. Po pierwsze, nigdy nie ma pewności, czy stare zagrożenie nie powróci. Po drugie, cyberprzestępcy szybko dostosowują się do sytuacji – są bardziej elastyczni w wykorzystywaniu swoich narzędzi i bez wahania żerują na „gorących" tematach. Z naszej analizy wynika, że po upublicznieniu kodu źródłowego zagrożenia mogą zdarzyć się niespodziewane rzeczy, jak w przypadku bootkita Rovnix. Nie musząc rozwijać od zera własnych narzędzi obchodzenia ochrony, cyberprzestępcy mogą skoncentrować się na możliwościach własnego szkodnika, dodając do istniejącego kodu źródłowego dodatkowe możliwości* – powiedział **Aleksander Jeremin**, analityk ds. cyberbezpieczeństwa z firmy Kaspersky.

Szczegóły techniczne dotyczące bootkita Rovnix są dostępne na stronie https://r.kaspersky.pl/UbXme.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky jako źródła.

Wszystkie informacje prasowe są dostępne na stronie https://www.kaspersky.pl/nowosci.

## Dalszych informacji udziela

Piotr Kupczyk
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kupczyk@kaspersky.pl
Tel. bezpośredni: 22 206 59 61
Tel. kom.: 518 935 846

## Informacje o firmie Kaspersky

Kaspersky jest globalną firmą z branży cyberbezpieczeństwa założoną w 1997 r. Dzięki doświadczeniu i zdobywanej latami eksperckiej wiedzy firma tworzy rozwiązania bezpieczeństwa chroniące firmy, infrastrukturę krytyczną, rządy i konsumentów na całym świecie. Obszerny wachlarz produktów firmy Kaspersky obejmuje technologie ochrony punktów końcowych oraz wyspecjalizowane rozwiązania i usługi pozwalające na walkę z zaawansowanymi, nieustannie ewoluującymi cyberzagrożeniami. Technologie Kaspersky chronią ponad 400 milionów użytkowników oraz 270 000 klientów korporacyjnych na całym świecie. Polskie przedstawicielstwo firmy aktywnie działa od 2001 r. Informacje o bezpieczeństwie przygotowywane przez ekspertów z firmy Kaspersky są dostępne w serwisie SecureList.pl oraz na oficjalnym blogu – Kaspersky Daily. Więcej informacji można uzyskać na stronie https://kaspersky.pl.