Narzędzie do deszyfracji złośliwego oprogramowania GandCrab dostępne za darmo

Data publikacji: 9.11.2018 15:30

Biuro do Walki z Cyberprzestępczością Komendy Głównej Policji informuje, że uniwersalne narzędzie do deszyfracji złośliwego oprogramowania GandCrab zostało stworzone przez rumuńską policję przy współpracy z Europolem oraz firmy antywirusowej. Osoby, które zostały pokrzywdzone poprzez zainfekowanie ransomware GandCrab powinny odwiedzić stronę www.nomoreransom.org, gdzie dostępne jest darmowe narzędzie do odszyfrowania.

fot.: Pixabay.com

Złośliwe oprogramowanie szyfrowało pliki na komputerze, by potem żądać okupu za odszyfrowanie. Uniwersalne narzędzie do deszyfracji złośliwego oprogramowania GandCrab odszyfrowuje pliki, które zostały zaszyfrowane. Na stronie KPP w Cieszynie czytamy: - ***Oprogramowanie do odzyskiwania plików zostało stworzone przez rumuńską policję przy współpracy z Europolem oraz firmą antywirusową. Jest to oprogramowanie przeznaczone do odszyfrowania plików, które zostały zaszyfrowane ransomware o nazwie GandCrab i działa na wersje 1,2,4 oraz 5 bez względu na lokalizację ofiar. To narzędzie zostało opracowane w 5 dni po tym jak grupa przestępcza odpowiedzialna za rozsyłanie GandCrab udostępniła klucze do odszyfrowania części ofiar na terenie Syrii.***

GandCrab w skrócie

Dystrybucja GandCrab jest jednym z najbardziej agresywnych ataków w ostatnich miesiącach szyfrujących pliki. Od stycznia 2018 roku kiedy został ujawniony, zaszyfrowanych zostało 500 000 ofiar na całym świecie, w tym wiele ofiar z Polski.

GandCrab infekuje komputer ofiary i szyfruje pliki dodając do nich rozszerzenie .GDCB, a następnie żąda okupu za odszyfrowanie plików w wysokości od 300 do 6 000 dolarów. Okup musi zostać opłacony za pośrednictwem wirtualnych walut, takich jak Bitcoin i DASH, celem anonimizacji przepływu środków.

W lutym br. pierwsze narzędzie do odszyfrowania GandCrab zostało stworzone przez rumuńską policję przy współpracy z Europolem oraz firmą antywirusową. Następnie przestępcy opracowali kolejną wersję GandCrab z ulepszonym kodem źródłowym i złośliwymi komentarzami dla organów ścigania, firm bezpieczeństwa oraz No More Ransom. Trzecia wersja została opracowana dzień później.

Teraz pojawiła się już 5 wersja tego złośliwego oprogramowania i jak widać rozwijana jest w szybkim tempie. Twórcy GandCrab cały czas tworzą nowe wersje tego ransmoware aby był jeszcze bardziej agresywny i unikał silników antywirusowych.

Jak nie stać się ofiarą ransomware w przyszłości

Osoby, które zostały zainfekowane ransomware GandCrab powinny odwiedzić stronę www.nomoreransom.org, gdzie dostępne jest za darmo narzędzie do odszyfrowania. Najlepszą obroną przed atakami ransomware jest prewencja oraz świadomość zagrożeń w sieci.

Użytkownicy sieci Internet są proszeni o:

- ***Wykonywanie kopii zapasowych najważniejszych plików i trzymanie ich w osobnym miejscu (w chmurze, na zewnętrznym dysku, na pendrive lub na innym komputerze);***
- ***Używanie legalnego i zaktualizowanego oprogramowania, w tym antywirusowego;***
- ***Nie pobieranie plików z nieznanych/podejrzanych źródeł;***
- ***Nie otwieranie załączników od nieznanych nadawców, nawet jeśli email wygląda na ważny lub wiarygodny***

red./mat.pras.