

Komunikat bezpieczeństwa

www.bsczechowice.com.pl

ZAGROŻENIE – RANSOMWARE PETYA

28.06.2017, źródło: www.zbp.pl

Komunikat Bankowego Centrum Cyberbezpieczeństwa ZBP z dnia 28 czerwca 2017 r.

Szanowni Państwo,

z informacji posiadanych przez Bankowe Centrum Cyberbezpieczeństwa na chwilę obecną żaden z banków - Członków ZBP nie został skutecznie zaatakowany.

Nie dotyczy to klientów banków, szczególnie firm współpracujących z firmami na Ukrainie lub prowadzących tam swoją działalność. Zagrożenie ransomware Petya posiada funkcjonalność propagowania się z wykorzystaniem luki w systemie Windows - CVE-2017-0143 MS17-010 EternalBlue SMB Remote Windows. W konsekwencji, złośliwe oprogramowanie może zagrozić wszystkim komputerom, które są podłączone w tej samej sieci.

Co zrobić, w przypadku wykrycia zagrożenia:

- niezwłocznie wyłączyć komputer, gdyż może on być źródłem dalszych infekcji innych komputerów w sieci oraz pozwoli zatrzymać proces szyfrowania plików. Podpinając dysk do innego komputera możemy próbować odzyskać niezaszyfrowane pliki. Należy szczególnie uważać podczas przenoszenia plików, aby nie doszło do ponownej infekcji poprzez złośliwy plik.
- odtworzyć system z kopii bezpieczeństwa lub ponownie zainstalować system;

Ze względu na fakt, iż podczas analizy tego zagrożenia zidentyfikowano również inne powiązane zagrożenie o nazwie LokiBot, zaleca się zmienić hasła dostępowe do usług online oraz poczty. Zmiany należy dokonać na bezpiecznym komputerze.

Jak się bronić:

- regularnie robić kopie bezpieczeństwa posiadanych zbiorów;
- aktualizować system operacyjny oraz inne oprogramowanie;
- nie otwierać podejrzanych załączników w mailach;
- nie podłączać komputerów do nieznanymi lub publicznych sieci;
- nie podłączać obcych komputerów do wewnętrznej sieci;
- nie ignorować nietypowych zdarzeń, które mogą świadczyć o trwającym procesie szyfrowania bądź ataku hakerskiego.

W przypadku zaistnienia incydentu należy go zgłosić do Rządowego Zespołu Reagowania na Incydynty Komputerowe - CERT.GOV.PL na adres mailowy: incydent@cert.gov.pl lub telefonicznie (22) 58-59-373

Bankowe Centrum Cyberbezpieczeństwa Związek Banków Polskich