Cyberdefence 24

29.07.2021

# NOWY RANSOMWARE AUTOMATYZUJE SZYFROWANIE DOMEN WINDOWSA

**Nowa wersja złośliwego oprogramowania ransomware LockBit 2.0 posiada funkcję automatyzacji interakcji i późniejszego szyfrowania domen Windowsa. Żaden inny program tego typu nie miał takich możliwości - ostrzegają eksperci.**

Ransomware LockBit od czasu pojawienia się w 2019 roku był cały czas rozwijany przez cyberprzestępców, którzy w ostatnim czasie zaczęli wykorzystywać jego najnowszą wersję - LockBit 2.0.

Nowością jest fakt, że oprogramowanie zostało wzbogacone o możliwość automatycznej dystrybucji oprogramowania ransomware w domenie Windows bez używania skryptów. Inaczej niż dotychczas, kiedy to hakerzy po włamaniu się do systemu najpierw musieli zainstalować skrypty, a te dopiero uruchamiały działanie złośliwego oprogramowania na komputerach.

**Nowy sposób działania**

Specjaliści z Malware Hunter Team, portalu pomagającego ofiarom zidentyfikować ransomware, którym został zainfekowany ich komputer, odkryli, że LockBit 2.0 wykorzystuje kontroler domeny Windows Active Directory API (usługi systemu Windows stanowiącej hierarchiczną bazę danych) do wykonywania zapytań protokołu LDAP, by uzyskać listę powiązanych urządzeń.

Plik ze złośliwym oprogramowaniem może się rozprzestrzenić, dzięki automatycznemu przekopiowaniu go na pulpit każdego komputera znajdującego się na liście. Skopiowany ransomware zostaje uruchomiony po obejściu kontroli konta użytkownika, dzięki czemu działa w tle i nie może być w żaden sposób wykryty.

„Znamy przypadek, kiedy MountLocker używał interfejsów Windows Active Directory API do wykonywania zapytań LDAP. Jednakże po raz pierwszy mamy do czynienia z automatyzacją dystrybucji złośliwego oprogramowania za pomocą zasad grupy. Jest to pierwsza operacja ransomware, która zautomatyzowała ten proces i umożliwia cyberprzestępcy wyłączenie programu Microsoft Defender i uruchomienie ransomware w całej sieci za pomocą jednego polecenia” – tłumaczy Dariusz Woźniak z firmy Marken - dystrybutora oprogramowania antywirusowego.

Dodatkowo nowy ransomware posiada funkcję wydrukowania listu z żądaniem okupu na wszystkich drukarkach połączonych z zainfekowanym komputerem.

*Na podst. informacji prasowej.*

*Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.*