Bitdefender

Ukraińscy politycy na celowniku RomCom Threat Group

14.06.2023

Zgodnie z najnowszym raportem BlackBerry Threat Research zespół cyberprzestępców znany jako RomCom koncentruje ataki na ukraińskich politykach i amerykańskim sektorze opieki zdrowotnej w ramach nowej kampanii hakerskiej. Zgodnie z doniesieniami ekspertów ds. IT grupa ta używa wyrafinowanych technik (w tym phishingu, typosquattingu) i wdraża zmodyfikowaną wersję programu Devolutions Remote Desktop Manager.

Ukraińscy politycy na celowniku grupy hakerskiej

Sprawcy wybierają ofiary na podstawie bliskości i zaangażowania w organizacje proukraińskie, zwłaszcza te pomagające uchodźcom uciekającym przed trwającym w kraju konfliktem.

Szczegółowa kampania phishingowa wdrożona przez RomCom ma na

celu nakłonienie ofiar do pobrania złośliwego oprogramowania za pośrednictwem fałszywych stron internetowych, które imitują oryginalne legalne strony.

Hakerzy wykazali się biegłością w typosquattingu, tworząc fałszywe strony tak przekonująco podobne do prawdziwych stron internetowych, że ofiary łatwo dają się nabrać i pobierają złośliwe oprogramowanie.

Po zainstalowaniu trojan zaczyna zbierać metadane hosta i użytkownika z zaatakowanych systemów oraz przesyła je z powrotem do serwera dowodzenia i kontroli (C2) kontrolowanego przez cyberprzestępców.

„Chociaż w tym momencie nie jest jasne, jaki początkowy wektor infekcji został użyty do rozpoczęcia łańcucha wykonania, poprzednie ataki RomCom wykorzystywały ukierunkowane wiadomości e-mail typu phishing, aby skierować ofiarę na sklonowaną stronę internetową, na której znajdują się wersje popularnego oprogramowania z trojanami" – czytamy w doradztwie w zakresie bezpieczeństwa BlackBerry Research & Intelligence Team. – „Istnieje duże prawdopodobieństwo, że w tym przypadku jest tak samo, ponieważ taktyka, technika i procedury (TTP) są zgodne".

Nieoczywiste cele hakerów

Szczególnie niepokojący jest wyraźny motyw geopolityczny stojący za działaniami RomCom. W przeciwieństwie do wielu innych grup cyberprzestępczych, których celem jest przede wszystkim zysk

finansowy, RomCom wydaje się dążyć do wydobywania poufnych informacji o sytuacji wewnętrznej w Ukrainie.

Może to obejmować tajemnice wojskowe, strategie obronne i ofensywne, programy szkoleniowe, a także inne utajnione dane. Wydaje się również, że cyberprzestępcy wykorzystują wszelkie wcześniej dostępne dane na temat swoich celów, takie jak informacje dotyczące tego, z jakiego oprogramowania korzystają i ich udziału w programach społecznych lub politycznych.

Biorąc pod uwagę wyrafinowanie i oczywiste cele strategiczne grupy RomCom, oczywiste jest, że organizacje zaangażowane w działania proukraińskie, a także szerzej rozumiany sektor opieki zdrowotnej w USA, muszą zwiększyć swoje cyberbezpieczeństwo, aby chronić się przed tymi atakami.

„W trakcie naszych dochodzeń firma BlackBerry zidentyfikowała kilka ofiar, głównie w Ukrainie" — wyjaśniają badacze. – „Zgadza się to z poprzednio widzianymi geolokalizacjami, które wybierał RomCom. Zaobserwowaliśmy również dowody na to, że co najmniej jeden cel ma siedzibę w Stanach Zjednoczonych. Ofiary ataków są zaangażowane w kilka różnych branż, takich jak wojsko i opieka zdrowotna. Wspólną cechą wszystkich ofiar jest zaangażowanie w konflikt na terenie Ukrainy".

„Eksperci do spraw cyberbezpieczeństwa z firmy Bitdefender radzą, aby sprawdzać legalność i bezpieczeństwo stron internetowych przed pobraniem jakiegokolwiek oprogramowania i zachować ostrożność w

przypadku nieoczekiwanych wiadomości e-mail, nawet tych, które wydają się pochodzić od znanych kontaktów. Ponadto warto zawsze korzystać z urządzenia, które jest zabezpieczone skutecznym systemem antywirusowym wyposażonym w moduł antyphishingowy" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/ukrainscy-politycy-na-celowniku-romcom-threat-group/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 14.06.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.