**Emotet zmniejsza swój wpływ o połowę, ale otrzymuje nowe funkcje i ulepszenia**

**Emotet to nadal najczęściej wykorzystywane złośliwe oprogramowanie, mające wpływ na ponad 7 proc. sieci komputerowych na świecie. I pomimo iż w ostatnim miesiącu jego globalny zasięg spadł o połowę, to cyberprzestępcy uzbrajają Emoteta o nowe możliwości – donoszą eksperci Check Point Research, którzy zbadali najpowszechniejsze złośliwe programy wykorzystywane przez cyberprzestępców w Polsce i na świecie.**

Na początku 2021 roku Europol oraz organy ścigania ośmiu krajów połączyły siły, by zlikwidować rozproszoną infrastrukturę dystrybuującą malware Emotet. Przeprowadzona w ramach Europejskiej Multidyscyplinarnej Platformy Przeciwko Zagrożeniom Przestępczym (EMPACT) akcja była niezwykle skomplikowanym zadaniem, którego powodzenie uzależnione było od precyzyjnej koordynacji działań wszystkich służb. Niestety, najpopularniejsze szkodliwe oprogramowanie 2020 roku powróciło po niespełna 10 miesiącach. Dziś Emotet ponownie lokuje się na pierwszym miejscu wśród najczęściej wykrywanych rodzin złośliwego oprogramowania.

Niewykluczone, że kolejny szczyt popularności Emoteta właśnie się skończył. W okresie od czerwca do lipca eksperci Check Point Research odnotowali 50-proc. spadek ilości zainfekowanych nim urządzeń, choć nadal jest to najbardziej rozpowszechnione złośliwe oprogramowanie. Obecnie Emotet odpowiada za infekcje w ponad 7 proc. sieci komputerowych na świecie i niemal 5 proc. w Polsce. *Niemniej ciągle odkrywane są nowe funkcje i ulepszenia w możliwościach Emotetu, takie jak jego najnowszy moduł do kradzieży kart kredytowych i poprawki dokonywane w jego systemach rozprzestrzeniania.*

*- Emotet nadal dominuje na naszych comiesięcznych listach złośliwego oprogramowania. Ten botnet nieustannie ewoluuje, aby utrzymać swoją trwałość i zdolności do unikania wykrycia. Jego najnowsze funkcje obejmują moduł kradzieży kart kredytowych, co oznacza, że przedsiębiorstwa i osoby prywatne muszą zachować szczególną ostrożność podczas dokonywania zakupów online* – wyjaśnia Maya Horowitz, wiceprezes ds. badań w Check Point Software

Drugim najbardziej rozpowszechnionym szkodliwym programem jest Formbook, infostealer atakujący system operacyjny Windows. Sprzedawany jest jako Malware-as-a-Service (MaaS) na forach hakerskich internetowego podziemia. Lubiany przez cyberprzestępców ze względu na swoje techniki unikania i stosunkowo niską cenę, FormBook zbiera dane uwierzytelniające z różnych przeglądarek internetowych, zbiera zrzuty ekranu, monitoruje i rejestruje naciśnięcia klawiszy, a także może pobierać i uruchamiać pliki zgodnie z zamówieniami z centrum kontroli. Eksperci Check Point Research szacują jego wpływ na blisko 3 proc. zainfekowanych sieci na świecie i ponad 1,8 proc. w Polsce.

Światowe podium popularności zamyka XMRig, czyli oprogramowanie typu open source wykorzystujące moce obliczeniowe zainfekowanych maszyn do wydobywania kryptowaluty Monero. Przestępcy często integrują go z własnym złośliwym oprogramowaniem, aby przeprowadzać nielegalne wydobycie na urządzeniach ofiar. XMRig został ostatnio wykryty w niecałych 2 proc. sieci na świecie. W Polsce malware ten nie jest już tak popularny – odsetek zainfekowanych nim sieci oscyluje wokół 0,5 proc., natomiast trzecim najczęściej wykrywanym zagrożeniem jest AgentTesla, czyli zaawansowany trojan zdalnego dostępu. AgentTesla może monitorować i gromadzić dane wejściowe z klawiatury ofiary i schowka systemowego, a także nagrywać zrzuty ekranu i eksfiltrować dane uwierzytelniające wprowadzone do różnych programów zainstalowanych na komputerze ofiary. Obecnie jego zasięg w Polsce przekracza 1,5 proc. sieci firm i innych organizacji.

Check Point Research ujawnił również najczęściej wykorzystywaną lukę bezpieczeństwa. Jest nią ***Web Server Exposed Git Repository Information Disclosure*** dotykająca około 42 proc. organizacji na całym świecie. Tuż za nią plasuje się ***Apache Log4j Remote Code Execution*** z wpływem na 41 proc. sieci.

Pełną listę szkodliwego oprogramowania można znaleźć na [blogu Check Point.](https://blog.checkpoint.com/2022/08/10/july-2022s-most-wanted-malware-emotet-takes-summer-vacation-but-definitely-not-out-of-office/)