

## **Sukces międzynarodowego zespołu policji – strona NetWire RAT została przejęta**

13.03.2023

Połączone wysiłki kilku międzynarodowych organów ścigania przerwały znaną akcję hakerską polegającą na dystrybucji trojana NetWire RAT. Władze USA współpracowały z Chorwacją, Szwajcarią, australijską policją federalną i Europejskim Centrum ds. Cyberprzestępczości Europolu w celu przeprowadzenia dochodzenia i przejęcia strony internetowej hakerów.

### **Śmiała akcja międzynarodowego zespołu policji – strona NetWire RAT została przejęta**

7 marca br. chorwackie władze aresztowały domniemanego administratora strony internetowej „worldwiredlabs”, na której przez lata sprzedawano trojana zdalnego dostępu (RAT) NetWire.

W tym samym czasie amerykański sędzia podpisał nakaz zezwalający władzom szwajcarskim na konfiskatę infrastruktury serwera NetWire RAT, a władzom federalnym Los Angeles – na przejęcie złośliwej domeny.

„Chociaż hakerzy reklamowali NetWire jako legalne narzędzie biznesowe do utrzymania infrastruktury komputerowej, specjaliści do spraw bezpieczeństwa stwierdzili, że NetWire jest wrogim oprogramowaniem wykorzystywanym do złośliwych celów” – powiedział rzecznik prasowy biura prokuratora USA. „Oprogramowanie było reklamowane na forach hakerskich, a liczne firmy zajmujące się bezpieczeństwem cybernetycznym i agencje rządowe udokumentowały przypadki wykorzystania NetWire RAT w działalności przestępczej”.

## **W jaki sposób działa trojan NetWire RAT?**

Podobnie jak inne RAT, NetWire zapewnia sprawcom zdalny dostęp do maszyny ofiary, umożliwiając im wykonywanie szkodliwych działań w zaatakowanych systemach. Operatorzy RAT mogą szpiegować poszkodowanych, sterować urządzeniami z podwyższonymi uprawnieniami oraz wykonywać zdalnie zadania, takie jak wdrażanie backdoorów w celu zachowania trwałości, eksfiltracja danych.

W rozpoczętym w 2020 roku śledztwie „worldwidelabs” tajni agencji FBI utworzyli konto na złośliwej stronie, płacąc za abonament. Konto zapewniało dostęp do narzędzia Builder, które umożliwiało agentom tworzenie dopasowanej pochodnej NetWire RAT.

„Globalne partnerstwo nie tylko doprowadziło do aresztowania sprawców w Chorwacji. Usunęło również popularne narzędzie służące do przejmowania kontroli nad komputerami w celu utrwalania globalnych oszustw, naruszeń danych i włamań do sieci ” – mówi zastępca dyrektora FBI w Los Angeles.

Sukces międzynarodowego zespołu policji – strona  
NetWire RAT została przejęta

**Bitdefender**<sup>®</sup>

Chociaż władze nie ustaliły jeszcze, ile pieniędzy zarobili nielegalni operatorzy NetWire RAT, wiadome jest, że sprawcy sprzedawali złośliwe oprogramowanie za kwoty od 10 do 1200 dolarów.

„Trojany to niezwykle niebezpieczny rodzaj złośliwego oprogramowania. Przy ich pomocy cyberprzestępcy są w stanie przejąć pełną kontrolę nad całą infrastrukturą sieciową każdej korporacji. W ten sposób mogą wykraść wszystkie dane niezbędne do płynnej pracy firmy. Aby obronić się przed tego typu zagrożeniami, należy wyedukować pracowników w zakresie podstaw cyberbezpieczeństwa oraz korzystać z odpowiednich zabezpieczeń, takich jak EDR i XDR” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: <https://bitdefender.pl/strona-netwire-rat-zostala-przejeta/>

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 13.03.2023

Z pozdrowieniami Piotr Rozmiarok

E-mail: [piotr.r@marken.com.pl](mailto: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

Sukces międzynarodowego zespołu policji – strona **Bitdefender**  
NetWire RAT została przejęta

instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.