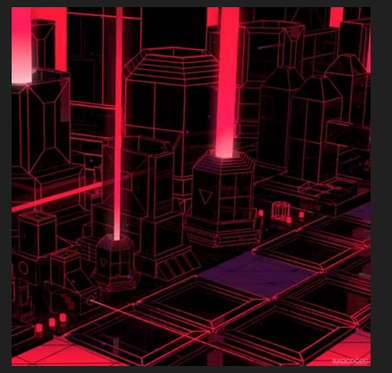
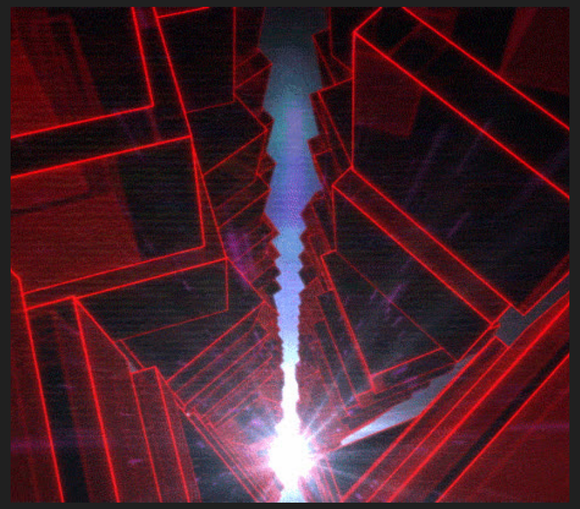
WIRUSY

TYPY I ZAPOBIEGANIE



BLANKA,
WIKA,
MARTYNA

SPIS TREŚCI



TEMATY PRZEPROWADZANE

- MALWARE
- RANSOMWARE
- SPYWARE
- ZAPOBIEGANIE

MALWARE

WIRUS ZŁOŚLIWY

Ogół programów o szkodliwym działaniu w stosunku do systemu komputerowego lub jego użytkownika.
Mianem malware określa się wyłącznie oprogramowanie, które zostało przeznaczone do złych celów i działa wbrew oczekiwaniom użytkownika; określenie to nie obejmuje aplikacji, które mogą wyrządzić niezamierzoną szkodę z powodu jakiejś niedoskonałości.
Polski Komitet Normalizacyjny jako polski odpowiednik terminu malware usankcjonował określenie „program złośliwy”.
Do szkodliwego oprogramowania zalicza się:

- wirusy (pasożytnicze, wieloczęściowe, towarzyszące, gnieżdżące się, makrowirusy)
- konie trojańskie
- fork-bomba (program rezydentny nie powielający się przez sieć)
- backdoory (przejmują kontrolę nad zainfekowanym komputerem, umożliwiając wykonywanie na nim czynności administracyjnych, łącznie z usuwaniem i zapisem danych)
- rejestratory klawiszy (odczytują i zapisują wszystkie naciśnięcia klawiszy użytkownika)

Jak zapobiegać malware?

- instalacja oprogramowania antywirusowego,
- włączona zapora sieciowa z modułem HIPS, która zapobiega uruchamianiu zagrożeń typu zero day
- czytanie okien instalacyjnych aplikacji, a także ich licencji

regularne skanowanie systemu programem antywirusowym i skanerami wykrywającymi szkodliwe oprogramowanie

- stałe aktualizowanie oprogramowania

SPYWARE

CZYM TAK NAPRAWDĘ JEST?

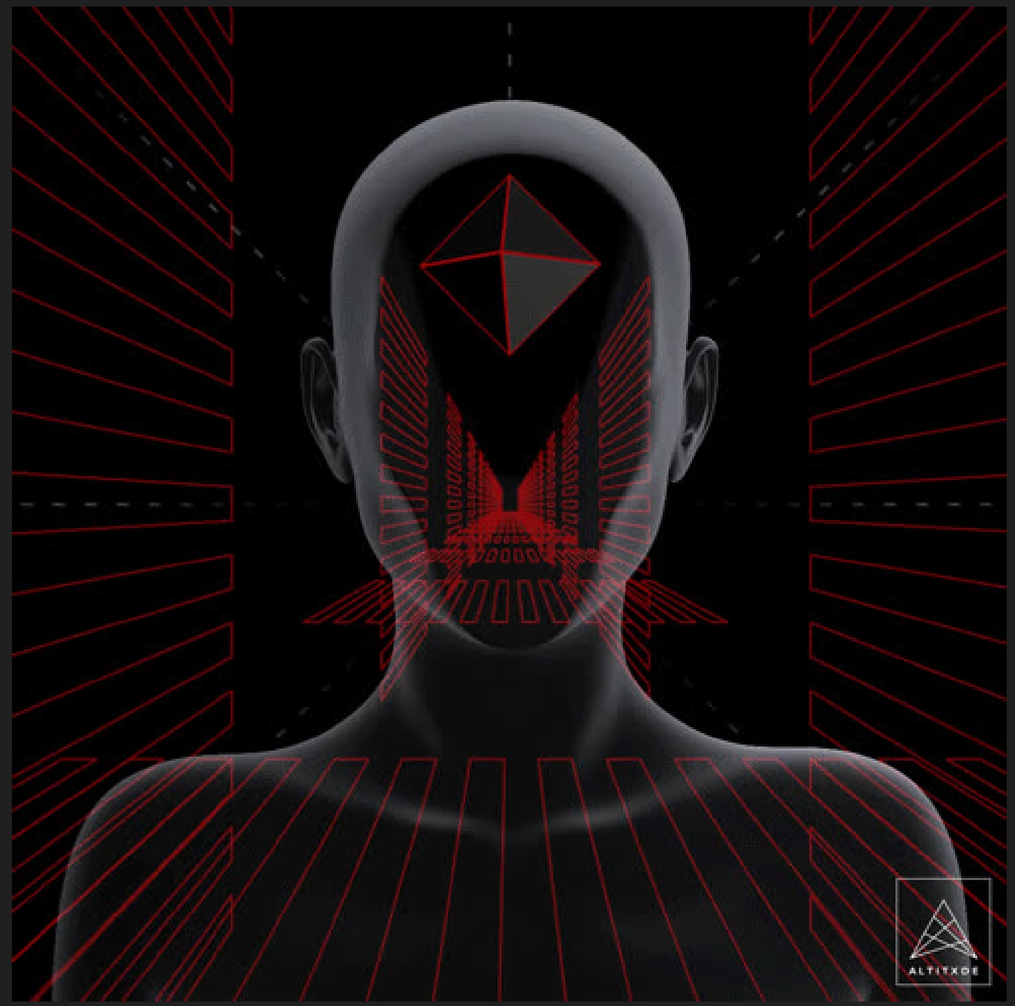
Jest to szkodliwe oprogramowanie, którego celem jest gromadzenie informacji o użytkowniku, a także ich przesyłanie bez jego wiedzy innym osobom.
Programy te mogą również wyświetlać reklamy lub rozsyłać niechcianą pocztę elektroniczną.
Do takich informacji należą:

- adresy WWW stron internetowych
- dane osobowe
- numery kart płatniczych
- hasła
- adresy poczty elektronicznej
- archiwum

Do najbardziej znanych programów tego typu należą Aureate, Cydoor, Gator, Promulgate, SaveNow.
Oprogramowanie takie zaliczane jest do kategorii złośliwego. Funkcjonuje ono niemal wyłącznie w środowisku Microsoft Windows.
Do jego wykrywania, usuwania i zwalczania służą różne skanery antyszpiegowskie, w tym:

- Ad-Aware
- Spyboy Search & Destroy
- Spy Sweeper
- Windows Defender

Oprogramowanie szpiegujące jest rozpowszechniane przy wykorzystaniu nieświadomości samych użytkowników poprzez scam.



74921 59300 4 18863 70782 0

0012 7482901 2744103 0592346 8774510 7255

RANSOMWARE

Oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego.

JAK MOŻNA DOSTAĆ RANSOMWARE?

Istnieją różne metody infekowania komputerów przez oprogramowanie ransomware. Jedną z najpopularniejszych jest rozsyłanie złośliwego spamu. Takie wiadomości e-mail mogą zawierać zainfekowane pliki (np. dokumenty PDF lub Word) lub odnośniki do złośliwych stron. Inną popularną metodą infekcji są złośliwe reklamy. Korzystanie z tej techniki pozwala przestępcom rozpowszechniać oprogramowanie za pośrednictwem reklam internetowych, co w wielu przypadkach wymaga bardzo niewielkiego (lub zerowego) udziału potencjalnej ofiary.

JAK ZAPOBIEGAĆ?

Kopie zapasowe stanowią najbardziej skuteczną metodę zniwelowania skutków ataku typu ransomware.
Zabezpiecz swoje urządzenia programami antywirusowymi, regularnie aktualizuj oprogramowanie – część ataków wykorzystuje istniejące luki w oprogramowaniu, zachowaj czujność podczas korzystania z Internetu i ostrożnie korzystaj z publicznych sieci Wi-Fi.

Back to Agenda Page

DZIĘKUJEMY ZA UWAGĘ!