DYNAMIC THREAT DEFENSE

CZYM JEST ESET DYNAMIC THREAT DEFENSE (EDTD)?

ESET Dynamic Threat Defense to dodatkowa warstwa zabezpieczeń produktów ESET, w tym Mail Security i produktów Endpoint oparta na technologii sandboxingu w chmurze, która pozwala na wykrywanie nowych i nieznanych dotąd rodzajów zagrożeń.

Sandbox w chmurze to bezpieczne i odizolowane środowisko testowe, pozwalające na wykonywanie podejrzanych plików i programów, obserwowanie ich zachowania analizę działania oraz automatyczne raportowanie obserwacji.

NIEZRÓWNANA SZYBKOŚĆ

Sandboxing w chmurze umożliwia analizę większości nowych próbek w czasie **krótszym niż 5 minut**.

ZALETA WYKRYWANIA

EDTD ON

EDTD OFF

+ 135min

Średnia przewaga

POJAWIAJĄCE SIĘ ZAGROŻENIA WYKRYTE PRZEZ EDTD

Downloadery

Smoke Loader

Smoke Loader to złośliwy bot często dystrybuowany za pośrednictwem zhakowanych witryn internetowych. Pobiera kolejne złośliwe oprogramowanie na zaatakowany komputer i używa wtyczek do wykonywania różnych złośliwych działań, takich jak kradzież poufnych informacji, przeprowadzanie ataków DDoS i kopanie kryptowalut.

Emotet

Emotet jest znanym trojanem modułowym, używanym głównie do pobierania kolejnych złośliwych programów na komputery ofiar, takich jak trojany bankowe, infostealery i oprogramowanie ransomware. Przed jego usunięciem w styczniu 2021 r. Emotet utworzył jeden z największych i najprężniej działających botnetów, uruchamiając kampanie spamowe na dużą skalę zawierające złośliwe dokumenty Office i PDF oraz wykorzystujące chwytliwych tematów jako przynęt.

Infekcje wykradające dane

Agent Tesla

Agent Tesla jest szeroko stosowanym, potężnym złodziejem haseł. Jego możliwości obejmują zbieranie danych logowania z różnych aplikacji przechowujących dane uwierzytelniające, rejestrowanie klawiszy i robienie zrzutów ekranu pulpit ofiary. Jest rozpowszechniany przez malware spam, nadużywający legalnych, zhakowanych kont e-mail. Wykorzystuje wyrafinowane techniki, aby uniknąć wykrycia.

Formbook

Formbook to szeroko rozpowszechniony trojan, który wykorzystuje techniki przechwytywania formularzy do kradzieży wrażliwych informacje z różnych aplikacji, takich jak przeglądarki, skrzynki poczty e-mail i FTP. Jest dystrybuowany przez złośliwe załączniki do wiadomości e-mail i wykorzystuje innowacyjne sztuczki w celu uniknięcia wykrycia i udaremnienia analizy.

Fareit

Fareit to szeroko rozpowszechniony trojan kradnący hasła, łatwo dostępny dla cyberprzestępców na podziemnych forach internetowych. Kradnie dane logowania z różnych przeglądarek i innych aplikacji do przechowywania danych uwierzytelniających. Fareit jest dystrybuowany za pośrednictwem złośliwych załączników w dobrze ukierunkowanych kampaniach z malspamem, wykorzystujących różnego rodzaju przynęty, od motywów finansowych i przesyłek po tematykę związaną z pandemią Covid-19.

Zagrożenia bankowe

Dridex

Dridex to ewoluujący, wyrafinowany trojan bankowy skierowany do sektora usług finansowych. Rozprzestrzenia się głównie za pośrednictwem złośliwych załączników do wiadomości e-mail. Dridex kradnie dane bankowe i inne dane wrażliwe swoich ofiar, ułatwiając nieuczciwe transakcje. Poza obszernymi szkodami finansowymi jakie wyrządza, trojan zyskał rozgłos za zastosowanie techniki „bombardowania atomowego" i wykorzystanie exploita zero-day MS Word do dystrybucji.

Infekcje usuwające dane

KillDisk

Złośliwe oprogramowanie, wykryte pod nazwą KillDisk, którego celem jest wyczyszczenie dysku twardego komputera, który infekuje. Może usunąć MBR ofiary i uszkodzić bootloader, a także skutecznie uniemożliwić rozruch systemu. W niektórych konkretnych, ukierunkowanych przypadkach ma również żądać okupu.