

OCHRAŇTE DOMÁCNOST NA INTERNETU



Ochrana routeru
a webkamery



Ochrana proti
krádeži identity



Zákaznická
podpora zdarma



Ochrana plateb
a bankovníctví



Ochrana před
hrozbami internetu



Anti-Theft: najde
ztracený notebook



ENJOY SAFER TECHNOLOGY™



30 LET
NEPŘETRŽITÝCH
INOVACÍ
IT BEZPEČNOSTI

30

30 LET NEPŘETRŽITÝCH INOVACÍ IT BEZPEČNOSTI

NOD

Miroslav Trnka a Peter Paško, pozdější zakladatelé společnosti ESET, napsali první antivirový program a nazvali jej NOD. Akronym NOD, čili Nemocnice na Okraji Disku, odkazoval na oblíbený televizní seriál.

Heuristická analýza

Heuristická analýza pomocí emulace ve virtuálním stroji testuje a monitoruje chování spouštěných aplikací v počítači, a pokud nějaká z jejich činností vykazuje známky typické pro chování malwaru, jako je replikování, přepisování souborů a snaha o utajení existence podezřelého souboru, je aplikace označena jako potenciální virus a uživatel je na tuto skutečnost upozorněn.

Pokročilá heuristika

Rozšířená heuristika se zakládá na unikátních heuristických algoritmech vyvinutých společností ESET, optimalizovaných pro detekci škodlivých kódů napsaných ve vyšších programovacích jazycích. Zavedení rozšířené heuristiky výrazně zvýšilo detekční schopnost produktů ESET.

DNA detekce

Tvůrci malwaru se pokouší škodlivý kód různými způsoby maskovat (například obfuskací). ESET DNA analýza detekuje malware na základě jeho komplexních vlastností, jako jsou chování a struktura programového kódu. Tímto způsobem je možné odhalit více variant škodlivého kódu.

Automatizace vytváření DNA vzorků

Významnou část vytváření DNA vzorků převzal ESET expertní systém, čímž detekci malwaru výrazně zrychlil a zefektivnil.

Cloudový reputační systém ESET LiveGrid

Neznámé či potenciálně škodlivé aplikace a jiné hrozby jsou monitorovány a odesílány na vyhodnocení do cloudového reputačního systému ESET. Pokud je vzorek vyhodnocen jako škodlivý, je pro něj vytvořena detekční signatura a je dána k dispozici všem uživatelům prostřednictvím reputačního systému.

1987

1995

2002

2005

2007

2011

Exploit Blocker

Exploit Blocker monitoruje často zneužívané zranitelnosti v aplikacích, jako jsou prohlížeče, čtečky dokumentů, poštovní klienti nebo doplňky Flash, Java a další. Při spuštění aplikace Exploit Blocker analyzuje její chování a při pokusu o zneužití její zranitelnosti daný proces ihned zablokuje.

Pokročilá kontrola paměti

Umožňuje lépe zachytávat malware, který se snaží maskovat svou přítomnost v operačním systému pokročilými technikami, jako je obfuskace kódu nebo šifrování. Pokročilá kontrola paměti monitoruje chování škodlivých procesů po jejich rozbalení v operační paměti.

Ochrana proti botnetu

Tato technologie chrání počítač před připojením do škodlivé sítě, která může zneužívat nakažené zařízení k rozesílání spamu či útokům na další počítače.

Síťové detekce

Technologie monitorující komunikaci nejen mezi aplikacemi uvnitř sítě, ale i mezi malwarem a řídicími servery útočníka.

Ochrana před skriptovými útoky

Detekuje skripty, které se snaží k útoku zneužít Windows PowerShell, a také škodlivé JavaScriptové útoky a skripty v prohlížečích Mozilla Firefox, Google Chrome, Microsoft Internet Explorer a Microsoft Edge.

Ochrana proti ransomware

Blokuje speciální druh malwaru, který za zpřístupnění zašifrovaných dat vyžaduje zaplacení značných finančních částek.

2012

2013

2014

2015

2016

2017



ENJOY SAFER TECHNOLOGY™

