Fidelis Cybersecurity

DATASHEET

Modul Fidelis Deception

Změňte pravidla hry prostřednictvím návnady, detekce a obrany

Příležitost

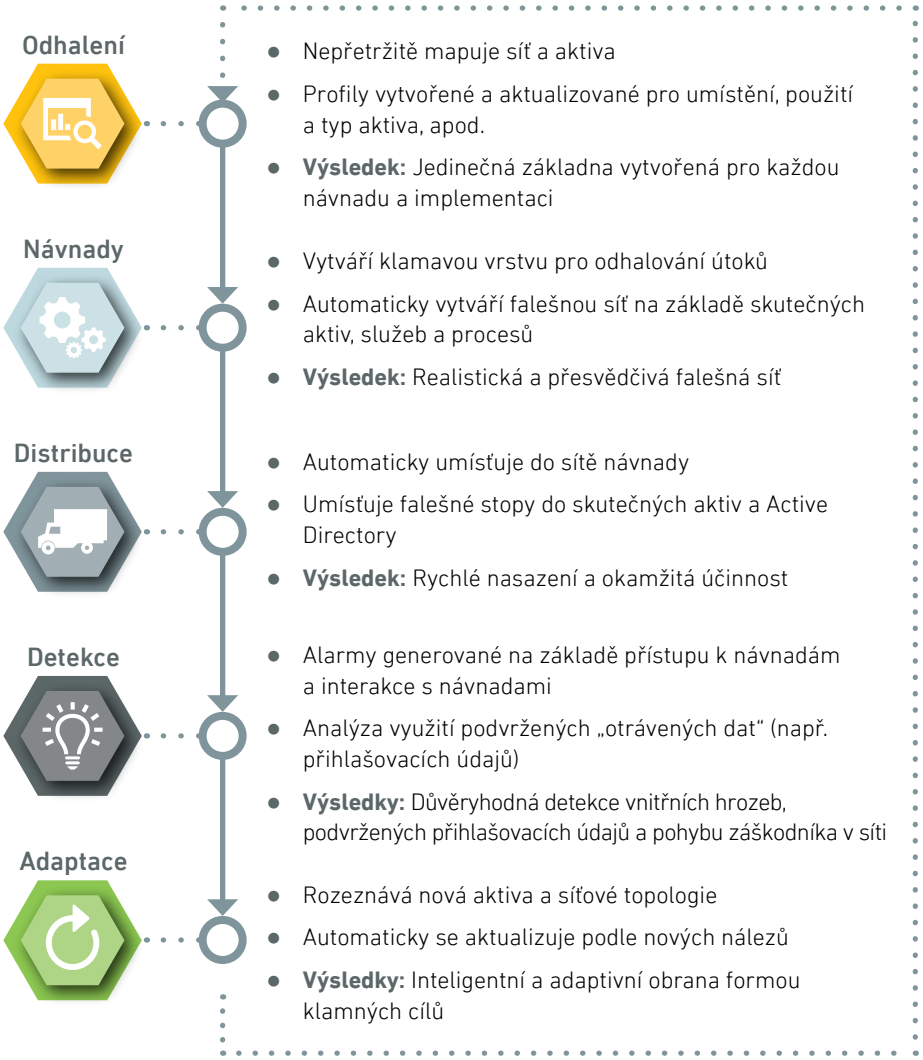
Kyberzločinci hledají hesla a přihlašovací údaje, aby mohli proniknout do sítí a aplikací, sledovat a krást data. Cvičení ve stylu boje o vlajku demonstrují, jak útočníci analyzují e-maily, soubory, dokumenty a nestrukturovaná data, aby z nich získali přihlašovací údaje. Automatický škodlivý kód se naopak soustředí převážně na strukturovaná data uložená v internetových prohlížečích a aplikacích. Útočníci se snaží získat především hesla, aby mohli proniknout do interních sítí a pohybovat se v nich. Každý úspěšný krok pomáhá útočníkovi zůstat nenápadný a vyhnout se generování digitálního „šumu", který by ho mohl prozradit. *Když víme, po čem útočníci pasou, můžeme toho využít k aktivní obraně: lákat, detekovat a bránit se.*

Úkol

- Odhalovat útočníky a škodlivý kód uvnitř sítě
- Produkovat vysoce spolehlivé alarmy s minimem či nulou falešných poplachů
- Automatizovat prošetřování a reakci
- Zvýšit účinnost a efektivitu bezpečnostních analytiků
- Zlepšit obranu mapováním strukturovaných útoků ve všech fázích jejich životního cyklu

Řešení

- Vytvářejte různé realistické návnady a falešné stopy
- Klonujte skutečná aktiva, emulujte služby i operační systémy a automaticky je aktualizujte
- Návnady v podobě aplikace lákají útočníky a připravují je o čas
- Detekce vytvářené na základě úspěšné návnady, MITM (Man In the Middle – odposlech komunikace) a analýzy síťového provozu
- Návnady skryté před skutečnými uživateli jako neznámá aktiva eliminující nechtěný přístup



„Fidelis deception se ukázal jako velmi účinný nástroj. Metoda návnad, kterou používá, je skvělým způsobem detekce anomálií bez nutnosti analyzovat velké objemy dat, jak je tomu u jiných koncepcí."

Weston Nicolls, SVP, Information Security Manager, First Midwest Bank

Jak návnady fungují

Návnady postupně přispívají k odhalení útočníka s použitím falešných stop, které vedou k pastím a lákají útočníky a automatické škodlivé kódy, které skenují stovky aplikaci. Návnady mění pravidla hry v oblasti zabezpečení. Namísto marného pátrání po falešném hráči v „oceánu" neškodných dat produkuje modul Fidelis Deception opodstatněné alarmy a události získané pomocí návnad, MITM chování a analýzy síťového provozu. Tyto alarmy mají vynikající přesnost a minimum falešných poplachů. Fidelis Deception jde ještě o krok dál a poskytuje simulované přístupové údaje včetně záznamů v Active Directory i simulovaný přístup k podnikovým aktivům. Tento simulovaný přístup k datům vytváří přesvědčivý obraz sítě (falešné) obsahující zařízení, data, vykazující chování, a to vše navržené tak, aby se útočníci sami chytili do pasti. Útočníci skočí na návnadu, takže je můžete odhalit, studovat a účinně se jim bránit.

Profily návnad

- Hardware – laptopy, servery, směrovače, přepínače, kamery, tiskárny, podniková zařízení typu IoT apod.
- Software – operační systémy, aplikace, porty, služby, aplikace a podobná data
- Návnady jsou neznámá a zamaskovaná aktiva, ke kterým nemají zaměstnanci důvod přistupovat nebo je používat
- Připravují útočníka o čas a odvádějí jeho pozornost od skutečných aktiv

Falešné profily (pasti)

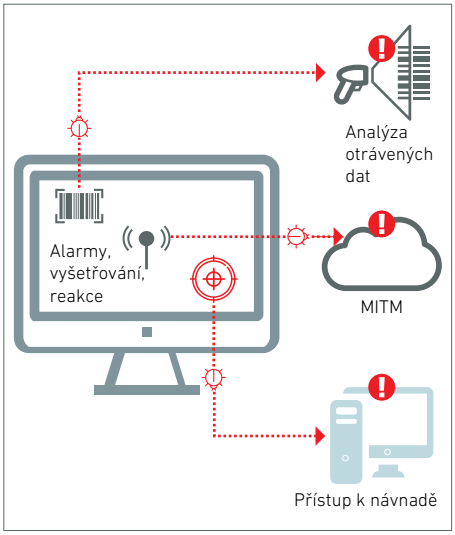
- Pasti: na bázi souboru, aplikace, sítě nebo přihlašovacích údajů
- Stopy: soubory, dokumenty, e-maily, systémové prostředky apod.
- Otrávená data, často přihlašovací údaje či profily, které útočník používá

Detekce útoků po průniku

- Přístup k návnadám jako neznámým aktivům (např. útočníci, vnitřní záškodníci)
- Analýzy dat zobrazující používání otrávených dat (např. přihlašovacích údajů)
- Monitorování činností útočníka, který pracuje s návnadami a falešnými stopami
- Síťová analýza na základě návnad a dat z alarmů

Inteligentní klamání útočníka

- Automatizuje a adaptuje rozmísťování návnad a falešných stop
- Detekuje pohyb po síti, provoz C2 a exfiltraci dat
- Vizibilita a forenzní funkce k rozpoznání taktiky, techniky, postupů a požadovaných aktiv
- Jedna konzole s kompletní telemetrií návnad pro analýzu, lov útočníků a reakci
- Žádný dopad na provoz či uživatele, žádné ohrožení dat a aktiv



Velmi přesné alarmy s minimem falešných poplachů

„DDPs (Distributed Deception Platforms) umožnily nástup nového typu detekčních funkcí využívajících návnad a pastí k rychlému posílení detekce a reakce bez ohledu na úskočnost zkušeného útočníka."

Gartner, Competitive Landscape: Distributed Deception Platforms, 2016, Lawrence Pingree, aktualizováno: 26. prosince 2017 | vydáno: 04. srpna 2016, G00310123

Proč si vybrat Fidelis?

Fidelis se nespokojuje s tradičním návnadami (honeypoty), používá inteligentní návnady, které lákají, matou a maří snahy útočníků a škodlivého kódu. Fidelis Deception pomáhá bezpečnostním týmům detekovat skryté hrozby, poznávat nové techniky útoků a bránit kritická data. Fidelis Deception Module analyzuje interní síťový provoz „z východu na západ", zatímco Fidelis Network poskytuje bezkonkurenční analýzu výstupního provozu „ze severu na jih". Fidelis automatizuje detekci a reakci v sítích a na všech koncových bodech s použitím inovativní sestavy účelně navržených a integrovaných technologií. Fidelis vybavuje novými schopnostmi bezpečnostní pracovníky v první linii a pomáhá zkušeným lovcům útočníků identifikovat, prošetřovat a ověřovat hrozby a reagovat na ně.

Obraťte se na nás ještě dnes a získejte další informace o společnosti Fidelis

Fidelis Cybersecurity | +420 222 191 918 | emea@fidelissecurity.com

Fidelis je jediná integrovaná platforma pro automatizovanou detekci a reakci na sítích i koncových bodech. Platforma Elevate™ společnosti Fidelis zvyšuje efektivitu i účinnost práce bezpečnostních týmů soustředěním dat alarmů do akčních souhrnů útoků s následnými automatickými akcemi reakce a prošetřování. Řešení Fidelis jsou vyvíjena s cílem zvýšit vizibilitu a zajistit rychlou reakci. Nabízejí automatizovanou validaci, prošetřování a prevenci útoků. Spoléhají se na ně přední světové společnosti.

