SYSTÉM PRO ROZPOZNÁVÁNÍ APT ÚTOKŮ

APT útoky

APT je zkratka Advanced Persistent Threat, tedy pokročilého profesionálně vedeného útoku, který se vyznačuje dlouhou dobou trvání, zpravidla v řádu měsíců až roků. APT útoky nejsou příležitostné či náhodné, ale cíl útoku je předem velice pečlivě nastudován.Útoky nejsou příležitostné či náhodné, ale cíl útoku je předem velice pečlivě nastudován. Co přesně APT útok je a čím se odlišuje od jiných typů sofistikovaných útoků, ještě není zcela ustáleno. Někteří považují APT útok pouze za poslední článek ve vývoji útoků, jiní je považují za úplně nový přístup. Základní definice společnosti ISACA je definuje jednoduše jako hrozbu, která je pokročilá a trvalá. Pokročilostí hrozby je myšleno použití netriviálních technik pro provedení útoku, trvalostí pak to, že APT útoky nejsou jednorázové akce, ale vyznačují se určitou delší dobou trvání. Útočníci se snaží dostat do cílového prostředí, kde setrvávají delší dobu a monitorují citlivé informace, nebo provádí jiné akce k dosažení svých cílů.

Cílem APT útoků se stávají nejčastěji velké organizace, kde mohou útočníci získat nejvíce ceněná data a nejčastější motivací je průmyslová či politická špionáž. Cílem však nemusí být jen data, ale také napadení nějaké služby a dokonce může také během probíhajícího útoku dojít ke změně cílů útočníka. Například může útočník usilovat o citlivé informace, po jejich získání je zneužije a dále sabotuje systémy napadeného. Pro zjištění cílů útočníků je potřeba vzít v úvahu kým útočníci jsou, nebo kým jsou sponzorováni, a o jaká aktiva mohou mít zájem. Útočníků může být celá škála od organizovaných skupin, kterým jde o finanční obohacení, až po armády a rozvědky nepřátelských států, kterým jde o strategické informace.

Klíčové charakteristiky útoku

Jednou z věcí, kterou se APT útoky odlišují, je míra jejich zacílení. Tyto útoky nebývají náhodné a ani nenapadají plošně příliš mnoho zařízení. Jsou zamířeny na předem důsledně vytipované cíle s úmyslem získat přístup k určitým informacím nebo zdrojům (například v případě počítačového červa The Stuxnet Worm tento obsahoval omezení, kterými limitoval své rozšíření na cílové systémy). Útočník nejdříve detailně zmapuje zamýšlený cíl, což mu umožňuje vytipovat si slabá místa pro průnik do cílového systému a prová- dět i útoky typu social engineering, při kterém se zaměřuje na osoby a spoléhá na selhání lidského faktoru. Velmi často jsou APT útoky vícevektorové, tedy využívají více způsobů kompromitace za účelem získání přístupu, přičemž se snaží využít více slabin v cílovém systému.

APT útoky jsou prováděny zkušenými odborníky s velmi dobrou znalostí dnešních tech-nologií a představují většinou velmi pokročilé typy útoků využívající často zatím neznámých zranitelností (tzv. zero day), které útočníkům umožňují kompromitaci systémů a téměř se nedají odhalit pomocí tradičních postupů. Tradiční postupy založené na rozpoznávání signatur, tedy určitých sekvencí známých škodlivých programů, nemohou pro nově vyvinutý malware fungovat. Při úspěšné kompromitaci útočníci nasazují komplexní, často modulární, škodlivý software, který je schopen dále provádět velmi rozličné útočné akce v cílovém systému. Instalovaný software také může disponovat umělou inteligencí a často se snaží uniknout detekci, například přesouváním umístění škodlivého kódu nebo jeho šifrováním. Útočníci jsou schopni napadnout širokou škálu zařízení, o čemž svědčí například již zmíněný The Stuxnet Worm, který byl schopen infikovat i průmyslové počítače (PLC).

Zásadním rozdílem oproti běžným typům útoků je délka trvání útoku. Běžné útoky většinou po průniku do systému provedou požadovanou akci, jako je například získání informací, omezení funkčnosti služby, nebo nainstalování škodlivého programu a dále již útok neprobíhá. V případě instalace škodlivého programu může dojít k začlenění napadeného stroje do tzv. botnetu který může být útočníkem využit i později, ale zpravidla bývá napadený počítač konečným cílem a dále již k útoku nedochází. Naopak u APT útoků dochází v případě kompromitace k instalaci programů, které jsou pak vstupní branou pro automatizované i manuální útoky v cílovém systému. APT útoky jsou často velice dlouhodobě probíhající útoky, které kladou velký důraz na minimální riziko odhalení. Proto mohou APT útoky postupovat relativně pomalu a vyhnout se detekci pomocí skrývání komunikace v běžném provozu. Jako příklad si můžeme vzít napadení amerického úřadu pro personální management z června minulého roku, které probíhalo minimálně rok (od července 2014). U APT útoků se většinou jen velice obtížně zjišťuje doba, kdy byl systém infikován. Organizace jsou z kapacitních důvodů nuceny starší logy mazat a stává se tak, že detekovaný APT útok je vystopován až do počátku uložených logů a nelze stanovit dobu, kdy došlo k infikaci systému. Také rozsah útoku se vzhledem k jeho době trvání a velkým možnostem variability určuje jen ztěžka.

Životní cyklus útoku

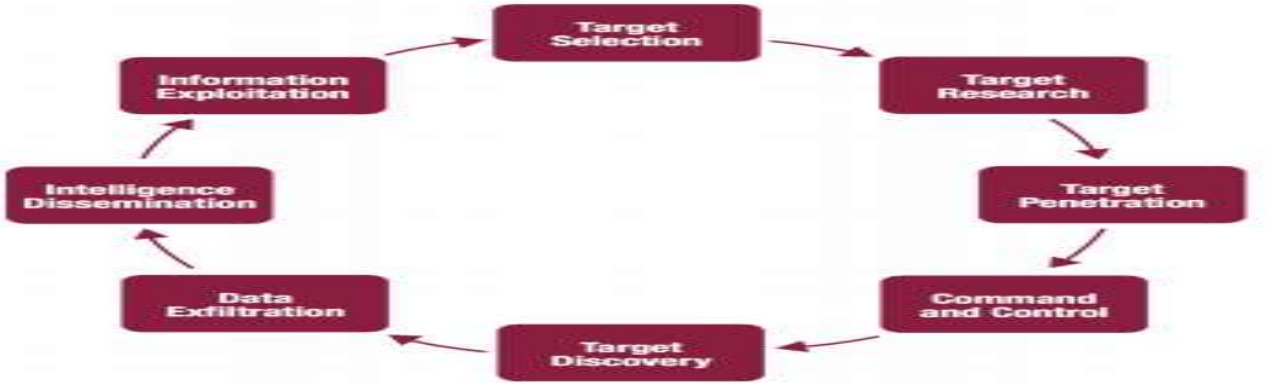
Na obrázku 2.1 je znázorněn životní cyklus APT útoku s vyznačenými fázemi. Jak lze na první pohled vidět, je životní cyklus kruhový, protože po úspěšně provedeném primárním cíli útoku často nedochází k ukončení útoku, ale k vytipování dalších cílů s využitím znalostí získaných v předchozích krocích.

Fáze životního cyklu APT útoku

Výběr cíle (Target Selection) Výběr cílů bývá důkladný a jako cíl nejsou určeny pouze nějaká aktiva, ale mohou to být i podružné cíle, které útočníkům následně umožní další postup. Pokud se během probíhajícího útoku změní priority nebo se vyskytnou nové informace není neobvyklé, že se plán útoku, nebo i výběr cíle, změní.

Vnější zmapování cíle (Target Research) Před samotným APT útokem dochází k co nejúplnějšímu zmapování cíle s důrazem na infrastrukturu, identifikací vhodných zdrojů informací a hledání zranitelností, které by mohly sloužit k napadení cíle.

Kompromitace (Target Penetration) Kompromitace je první přímou fází útoku, kdy se útočníci pomocí informací získaných v předchozí fázi dostávají do systému. K tomu většinou nedochází na místech, které mají pro útočníky přímou hodnotu, jako jsou počítače vrcholových managerů organizace nebo přímo datová centra obsahující chtěné informace, protože ty bývají dobře zabezpečeny a přímý útok by byl velice nesnadný. Prvotní kompromitace se většinou vydává cestou nejmenšího odporu a zasahuje stroje zaměstnanců na nižších pozicích, nebo dokonce externích spolupracovníků. Přes tyto body se pak útočníci dostávají do systému, který pak mohou lépe prozkoumat zevnitř a postupně napadnout cílová zařízení.



Zavedení trvalého spojení (Command and Control) Když jsou útočníci v systému, instalují malware, který jim umožní přístup do vnitřní sítě a provádění útoků zevnitř. Malware se po instalaci typicky spojí s útočníky a zahájí monitorování, nebo čeká na případné další instrukce, přičemž se snaží zůstat nedetekován. Často bývá modulární a po úspěšné infiltraci si stáhne dodatečné moduly, které rozšíří mož- nosti monitorování sítě a provádění útoků. Tento malware může fungovat do značné míry autonomně a odesílat citlivé informace útočníkům.

Zmapování vnitřní sítě (Target Discovery) Když má útočník k dispozici spojení do vnitřní sítě napadeného, dochází k automatickému či manuálnímu zmapování vnitř- ních struktur a instalaci dalších malwarů pro zajištění připojení i v případě odhalení a neutralizování původního spojení. S detailní znalostí vnitřních struktur a informací z vnitřní sítě (které mohou obsahovat samy o sobě citlivé informace, a dokonce i přístupové údaje) je možné detailně naplánovat další postup.

Filtrování informací (Data Exfiltration) Po zmapování vnitřní sítě lze účinně získat požadované informace. Tyto se většinou shromažďují na některém napadeném zařízení v síti oběti a jsou dále komprimovány a šifrovány.

Distribuce informací (Intelligence Dissemination) Jsou-li požadované informace k dispozici a připraveny na odeslání, nastává samotné odeslání těchto dat útočníkům. Pro minimalizaci pravděpodobnosti detekce jsou přenášená data obvykle skryta mezi legitimní komunikaci a pro případ odhalení nejsou data zasílána přímo útočníkům, ale cestují přes několik proxy serverů, které slouží ke skrytí útočníků.

Zneužití informací (Information Exploitation) Po získání informací je mohou útoč- níci využít ihned, nebo je pouze archivují pro vlastní potřebu. Pokud zjištěné informace vedou ke změně priorit či cílů, může být hned zahájen další útok, který bude nyní již operovat s mnohem detailnějšími informacemi o cílovém systému. Případem informace, která je pouze archivována, může být průmyslová, či politická špionáž, která nemá okamžité uplatnění, ale až v budoucnosti, po provedení určité akce (uvedení produktu na trh, válka).

Současné způsoby obrany

Jak již bylo zmíněno, je obrana proti APT útokům značně komplikovaná a organizace nejsou na tento typ útoků připraveny, což je výsledkem velkého počtu úspěšných útoků v poslední době. K bezpečnosti v oblasti IT se příliš dlouhou dobu přistupovalo velmi benevoletně a finanční prostředky vynakládané na zajištění bezpečnosti byly směšné v porovnání s prostředky vynakládanými na rozvoj software. Až kolem roku 2005 dochází ke zlomu, kdy se začaly organizace, v důsledku nárustu kyberkriminality, více zajímat o bezpečnost a více do ní investovat. V roce 2010 mělo 86% obětí kyberůtoků k dispozici důkazy o napadení, přesto pouze 61% z nich odhalilo kompromitaci vlastním přičiněním, zatímco ostatní byly upozorněny třetí stranou . Vzhledem k tomu, že dnes existuje obrovské množství malware, a v APT útocích jsou navíc často používány zcela nové a na míru vyrobené programy, je detekce APT útoku velmi obtížná. Navíc vzhledem k dlouhé době trvání odhalení APT útoků je pravděpodobné, že nyní detekované způsoby jsou již zastaralé a útočníci využijí zkušeností z úspěšných útoků pro tvorbu nových, sofistikovanějších a ještě hůře detekovatelných postupů. V současné době nedochází k žádným speciálním akcím, kterými by organizace předchá- zely, nebo se bránily, APT útokům. Pro prevenci před těmito útoky jsou využity konvenční způsoby obrany, které zřídka bývají doplněny o určité heuristiky pro odhalování nových způsobů útoku nebo o nějakou formu umělé inteligence.

Jako první bývají nasazovány antivirové programy pro rozpoznávání nevyžádaných programů na jednotlivých počítačích. Tyto programy jsou schopny dobře rozpoznat známý malware a často nabízejí i doprovodné funkce pro předcházení kompromitace systému, jako je skenování souborů v sandboxovaném prostředí při stahování, varování uživatelů při pří- stupu na známé podvodné stránky a hlídání bezpečnostních aktualizací pro nainstalované programy. Mohou se snažit detekovat nové hrozby podle sledování chování procesů a sdílení veškerých poznatků v komunitě uživatelů.

Základní síťovou bezpečnost zajišťuje rozdělení sítě do logických celků a hlídání perimetru pomocí firewallu. Firewallů existuje více typů, jak hardwarové, tak i softwarové a jejich úkolem je podle nastavených pravidel povolit či zahodit síťovou komunikaci. Dříve jednoduché bezestavové systémy mohou dnes být dynamicky konfigurovány, udržují si svůj stav a dovolují relativně komplexní nastavení pravidel.

Pro monitorování síťového provozu se většinou používají systémy IDS (Intrusion Detection System) a IPS (Intrusion Prevention System). Tyto systémy analyzují události a hledají v nich hrozby porušující nastavené bezpečnostní politiky. Zatímco systémy IDS jsou pasivní a případné porušení pouze hlásí pověřeným osobám, IPS systémy umožňují na nalezené hrozby automaticky reagovat např. nastavením nových pravidel firewallu. Tyto systémy se většinou nasazují na sledování síťového provozu (tzv. network-based), mohou však být nasazeny na stanicích (tzv. host-based) a sledovat tak události nastávající na dané stanici, jako je například vytížení procesoru RAM .

IDS a IPS systémy většinou fungují na principu hloubkové analýzy paketů a popisu pravidel - signatur, podle kterých odhalují hrozby podobně, jako antivirové programy. Mohou být schopny detekovat přenášené soubory a odhalovat náhodné útoky na přihlašovací údaje (např. podle přihlašovacího jména guest, které bývá u méně sofistikovaných útoků často zkoušeno). Tyto systémy jsou relativně jednoduché na vytvoření a výkonné, ale trpí již dříve popsanými problémy s detekcí nových typů útoků, pro které zatím nebyly vytvořeny signatury.

gnatury. Jiným typem IDS a IPS systémů jsou ty, které využívají principů behaviorální analýzy a snaží se tak rozpoznat útočníka od legitimního uživatele podle anomálií v chování. Většina systémů hledá tyto anomálie v síťovém toku, ale dají se sledovat i anomálie dat obsažených v hlavičkách paketů [30]. Do tohoto typu systémů spadají i systémy založené na stavové analýze protokolů, která používá modely chování jednotlivých protokolů specifikovaných tvůrci těchto protokolů a hlásí události v případě použití protokolu jiným způsobem. Velkým problémem IDS systémů fungujících na principu behaviorální analýzy je velké množství tzv. false positives, tedy upozornění na podezřelou aktivitu, která je však zcela nezávadná.

Vzhledem k velkému množství zdrojů bezpečnostních informací, jako jsou různé logy (systémové, aplikační) rozličných hlášení z firewallů a IDS/IPS, se ukázalo nezbytné zavést systém, který by je dokázal shromažďovat na jednom místě, agregovat a umožnit bezpečnostním analytikům zjednodušený pohled na celou síť. Takovým systémem je Security Information and Event Management (SIEM), který vznikl spojením Security Event Managementu (SEM), který se staral o shromažďování logů a jejich analýzu a Security Information Managementu (SIM), který analyzoval trendy a poskytoval analytikům vyšší abstrakci. Shromažďováním těchto informací na jednom místě a jejich korelací se dají rozpoznat vzory, které se odlišují od běžného provozu a tak rychle identifikovat, analyzovat a reagovat na bezpečnostní incidenty. Přestože v teorii by měly být tyto systémy schopny detekovat hrozby téměř v reálném čase i v rozsáhlých sítích, v praxi to selhává kvůli velkému množství dat, se kterými musí pracovat. Navíc tyto systémy nedetekují útoky, které se maskují v běžném provozu a nejsou tedy zachyceny žádnou sondou a proto se neobjeví v logu.

Návrh systému pro rozpoznání APT útoku

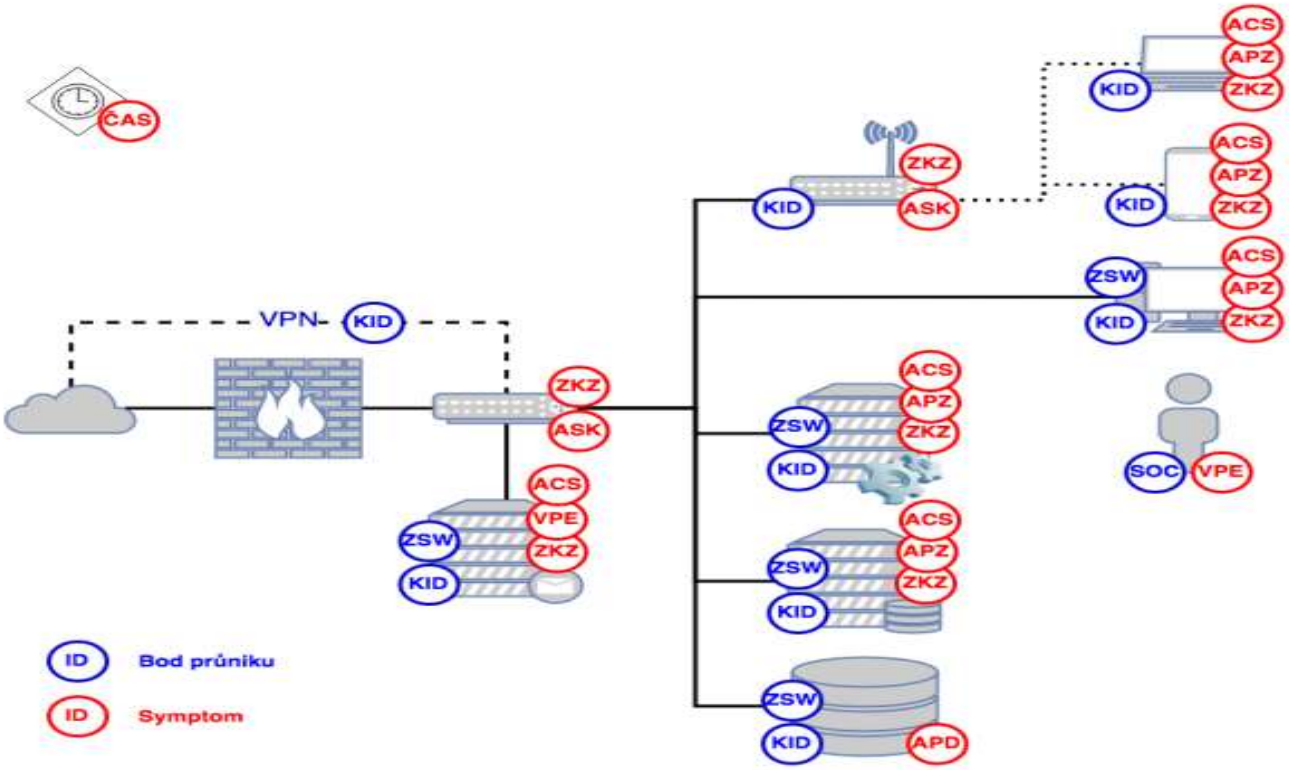
V rámci této kapitoly je navržen systém, který je po implementaci v cílovém prostředí schopen detekovat pokročilé ICT útoky včetně APT útoků. Nejprve je třeba identifikovat symptomy, které provází APT útoky, abychom byli schopni rozhodnout, které oblasti je třeba sledovat a pomocí čeho lze detekovat, jestli se organizace nachází pod APT útokem. Symptomem se v práci rozumí příznak či průvodní jev obtížně pozorovatelného děje, stavu nebo procesu, který slouží k rozpoznání útoku. U každého

nalezeného symptomu je dále rozebráno, jak jej lze detekovat a nakonec je navržen obecný systém, který na základě sledování symptomů určí, zda se organizace nachází pod APT útokem.

Identifikace symptomů APT útoku

Na obrázku 3.1 je ilustrativně vyobrazeno typické prostředí organizace, ve kterém hrozí APT útok, s bezpečnostními aktivy, které se v daném prostředí vyskytují. Modrá kolečka identifikují body průniku, které jsou dále přiblíženy v tabulce 3.1, červená pak znázorňují výskyt symptomů, podle kterých lze rozpoznat APT útok. Přehled symptomů je pak uveden v tabulce 3.2. V následujícím odstavci je popsán obrázek z pohledu bezpečnostních aktiv na něm uvedených.

Vlevo na obrázku 3.1 je uvedena ikona oblaku, která symbolizuje vnější síť, ke které je organizace připojena. Kromě fyzického připojení firewallu lze pozorovat virtuální VPN spojení, které směřuje přímo do vnitřní sítě. Toto VPN spojení je podstatné, protože obchází firewall, kterým proteče jako šifrovaný kanál a v poslední době bývají VPN připojení velmi častým bodem průniku APT útoků. Pro zobrazení demilitarizované zóny (DMZ) byl zvolen třícestný firewall kvůli jednoduchosti jeho znázornění, přestože v praxi je DMZ obvykle řešena pomocí dvou firewallů. V DMZ je umístěn poštovní server, který reprezentuje různé servery nacházející se v DMZ. Velmi často využívají útočníci pro získání přístupu do sítě spear phishing, který přes tento server proudí, a pokud se útočníkům podaří kompromitovat poštovní server, mohou číst nešifrovanou firemní komunikaci. Směrem do vnitřní sítě je umístěn switch, který reprezentuje síťové prvky a na který směřuje VPN, která je tím zavedena přímo do vnitřní sítě.



Obrázek 3.1: Typické prostředí APT útoků

Do switche jsou pak zapojena další zařízení nacházející se ve vnitřní síti. Nahoře na obrázku je znázorněn bezdrátový přístupový bod (AP), pod ním běžná pracovní stanice, aplikační server, databázový server a datové úložiště. AP jsou důle-žitá místa v síti, protože umožňují bezdrátový přístup do vnitřní sítě, který mohou útočníci zneužít. Významným problémem jsou v podnikových sítích zejména nepovolené AP, které si uživatelé nainstalují sami bez vědomí síťového administrátora. Aplikační servery obsahují většinou podpůrné nástroje pro fungování organizace. Jejich napadením může útočník získat přístup k datům se kterými aplikace pracuje a také může sabotovat organizaci pomocí odepření služeb daného serveru, nebo dezinformacemi které danou aplikací šíří. Databázový server se stará o správu veškerých dat a jeho napadením získá útočník moc nad všemi daty, která jsou obsažena v celé databázi. Přímým přístupem do úložiště dat získá útočník veškerá surová data organizace, některá data je ale nutné správně interpretovat, což nemusí být triviální (např. datové soubory databází, vnitřní soubory aplikací). V nejpravějším sloupci jsou zobrazena zařízení, se kterými přímo pracuje uživatel, který je reprezentován ikonou nejníže. Uživatel sám o sobě může být jak terčem útoku (např. již zmíněný phishing nebo sociální inženýrství), tak i zdrojem útoku. Nezanedbatelná část útoků je vedena z vnitřní sítě pomocí zaměstnanců, kteří vědomě z osobních důvodů, např. kvůli vydírání či finanční odměně, kompromitují systémy a data zaměstnavatele. S uživatelem je spojena pevná pracovní stanice, mobilní zařízení a přenosný počítač, které jsou na obrázku znázorněny nad ikonou uživatele. S pevnou pracovní stanicí uživatel v kanceláři pracuje nejčastěji, tato stanice je zpravidla pod správou IT oddělení organizace, přesto může být napadena a využita pro potřeby útočníka. Přenosná zařízení představují vyšší formu rizika, jelikož jsou často pod správou jednotlivých uživatelů a mohou být snáze odcizena. Při odcizení či zneužití mobilního telefonu získá útočník relativně málo hodnotných údajů, může však zneužít zařízení pro ukradení identity uživatele a přihlášení se do podnikové sítě. U přenosných počítačů je rizikem kromě krádeže identity i krádež dat na daném zařízení, opět však platí, že není tolik důležitá jako krádež identity. Pokud útočník získá přenosný počítač s důvěrnými daty, jedná se většinou o několik málo dokumentů, jejichž zcizení může pro organizaci představovat citelnou finanční ztrátu, krádež identity ale může útočníka oprávnit ke všem důvěrným datům v organizaci, což je likvidační.

V dalších sekcích jsou blíže popsány jednotlivé symptomy, které indikují, že je organizace pod APT útokem.

identifikátor	název	popis
KID	Krádež identity	Ukradené přihlašovací údaje, sezení, či jiný způsob vydávání se za legitimního uživatele.
SOC	Sociální inženýrství	Zneužití lidského faktoru k získání citlivých informací, popřípadě přímo k vykonání záškodnické akce.
ZSW	Zneužití software	Využití zranitelností v software pro získání přístupu či informací z napadeného prostředí.

Tabulka 3.1: Přehled bodů průniku při APT útoku

identifikátor	název	popis
ACS	Abnormální chování software	Přístup na jiná místa v paměti, data, nebo vytěžování systému.
APD	Abnormální přístup k datům	Přístup na nezvyklá data, přístup mimo běžné cesty.
APZ	Abnormální použití zařízení	Podezřelá aktivita zařízení (přihlašování, vytížení, paměť).
ASK	Abnormální síťová komunikace	Změna v síťovém provozu uživatele nebo jeho trendech.
ČAS	Dlouhodobý průběh	Délka přítomnosti identifikovaného symptomu v prostředí.
VPE	Výskyt phishingových e-mailů	Kvalitní podvodné e-maily jsou často součástí prvních fází APT útoku.
ZKZ	Změna konfigurace zařízení	Jakákoli změna nastavení spravovaných zařízení.

Tabulka 3.2: Přehled symptomů APT útoku

Abnormální chování software

Pro získání přístupu do prostředí mohou být využity známé, ale i dosud neobjevené (takzvané zero-day) zranitelnosti v software, a to jak v aplikačním, tak i v serverovém software, či dokonce v nějaké součásti operačního systému. Nejčastěji dochází k napadení pomocí speciálního uživatelského vstupu, který není řádně ošetřen. Útočník pak může software využít například pro eskalaci svých práv a k získání kontroly nad cílovým zařízením. Kromě využití zranitelností pro přímý průnik lze zneužít software také ke sběru informací, kdy je útočník schopen přinutit software, aby mu zpřístupnil informace, na které nemá právo, nebo jej může dokonce útočník modifikovat tak, aby tyto informace sám sbíral a útočníkovi předal (například sledování bankovních údajů zadávaných ve webovém prohlížeči). Pokud se útočníkovi podaří upravit aplikaci tak, aby přijmala příkazy, které jí nějakým způsobem doručí, zajistí si útočník trvalý přístup k cílovému zařízení a může jej použít pro další průniky.

Abnormální přístup k datům

V dnešním informačním světě představují firemní data hodnotu, a proto se stávají terčem APT útoků téměř vždy. APT útoky, jejichž cílem není krádež citlivých dat jsou spíše vý- jimkou. Získání citlivých údajů poskytuje útočníkovi kromě kompetitivní výhody také nové informace o cíli, které umožňují přesnější postup při dalším pokračování útoku. Vzhledem k důležitosti dat je nutné věnovat vyšší úsilí kontrole přístupu k nim a detekovat nejen pokusy o přístup k tajným datům, ale kontrolovat veškeré operace s těmito daty. Je důležité od sebe oddělit tajná data od dat veřejných a to jak logicky, tak i fyzicky. Tajná data by neměla nikdy opustit vnitřní síť organizace.

Abnormální použití zařízení

Po získání přístupu k zařízení na něm útočník zpravidla provádí operace odlišné od běžného chování uživatele. Velmi často se útočník pokouší převzít kontrolu nad zařízením, aby získal přístup ke všem informacím dostupným na daném zařízení a dalších zařízení, které napadenému zařízení důvěřují. Proto se na zařízení objevují pokusy o eskalaci práv, kterého je zpravidla dosaženo zneužitím zranitelnosti v software, jak bylo zmíněno výše. Abnormální použití zařízení lze rozpoznat změnami v přihlašování uživatele. Útočník nepřistupuje k zařízení stejným způsobem a lze tedy detekovat vzdálené přihlašování z neobvyklých adres, nebo dvojí přihlášení uživatele - lokálně a vzdáleně. Kromě způsobu přihlašování lze také pozorovat změny v době přihlášení, pokud je zařízení aktivní mimo standardní časový rámec, lze indikovat pravděpodobné napadení zařízení. Pokročilé APT útoky se však snaží skrýt své aktivity v běžném provozu zařízení a nezpůsobují tak výrazné změny, jako je připojení k zařízení v nestandardní době. Přes to však lze detekovat více menších symptomů, včetně vyššího vytížení zařízení, zaplňování paměti nebo zaplňování pevného disku.

Abnormální síťová komunikace

Naprostá většina útoků využívá toho, že jsou dnes počítače propojeny internetovou sítí. Ta poskytuje útočníkům způsob, jak vynést informace z napadené organizace a také, jak vzdá- leně útok řídit. Po prvotní kompromitaci systému je většinou instalován v cílovém prostředí software umožňující vzdálené ovládání a tento software se přihlásí do útočníkovy řídící sítě. V poslední době také často dochází ke zneužití stávající VPN linky organizace, což umožní útočníkům nerušený a šifrovaný přístup do vnitřní sítě. Útočník z počátku často nezná strukturu sítě v prostředí a tak je nucen ji nějakým způsobem odhalit, což se často skládá z různého skenování sítě. Skenování portů jako takové je pro APT útoky méně časté, jelikož je velice snadno odhalitelné. Pokud je však rozloženo v dostatečném časovém rozpětí, může klasické detekci uniknout. Protože je u APT útoků kladen velký důraz na skrytí všech aktivit, je obvykle komunikace s řídící sítí útočníka šifrovaná a odesílání nasbíraných dat probíhá po malých částech během delšího období, čímž se skryje v normální komunikaci. Je tedy zřejmé, že sledování síťového provozu a jeho analyzování je zásadní a nedílnou součástní jakéhokoli systému, který se zabývá detekcí moderních útoků v ICT prostředí.

Dlouhodobý průběh

Již v názvu APT je zmíněna perzistence a v kapitole 2.1 je popsáno, že se tyto útoky vyznačují dlouhou dobou trvání. Přes to, že se rozhodně jedná o určující prvek APT útoku, není samostatně měřitelný. Dlouhodobou povahu útoku lze detekovat pouze zpětně a je měřena pomocí ostatních symptomů. Pokud tedy výskyt symptomů indikuje podezření na APT útok, lze až zpětně pomocí analýzy zjistit délku trvání daného symptomu a podle ní indikovat, že se s pravděpodobností jedná o APT útok. Dlouhodobý průběh tedy můžeme chápat nikoli jako samostatný symptom APT útoku, ale jako charakteristiku u ostatních symptomů.

Výskyt phishingových e-mailů

Přesto, že podvodné e-maily nejsou specifikem pouze APT útoků a jsou jimi dnes zahlceny téměř všechny e-mailové schránky, velice se liší v důmyslnosti a zůstávají nejčastěji využívaným bodem pro průnik do cílového prostředí. Pokročilé útoky stylu APT používají velice kvalitně vypadající podvodné e-maily, které jsou téměř nerozpoznatelné od regulérní pošty. Tento typ podvodných e-mailů se nazývá spear phishing a útočník pro jejich vytvoření používá často detailní informace o napadeném

prostředí a uživateli. Tato pošta pak snadno projde automatickými filtry a uživatel, který nepozná rozdíl od podnikové pošty, může nevědomky nainstalovat malware, nebo je přesměrován na podvodný web, který útočník nastražil.

Změna konfigurace zařízení

V podnikovém prostředí bývají zařízení pod správou IT oddělení, v poslední době se však rozmáhá princip BYOD (Bring Your Own Device). U zařízení, které spravuje IT oddělení, se předpokládá stabilní konfigurace, která se nemění. Jakákoli změna, jako je například instalace nového programu nebo otevření portu, indikuje narušení bezpečnosti. U pracovních stanic se může jednat o běžný virus, ale pokud se změní konfigurace síťových prvků, dá se předpokládat pokročilejší útok.

Po napadení zařízení často útočník instaluje backdoor, který mu umožní vzdálený pří- stup k systému, nebo modifikuje stávající aplikaci, aby plnila tento účel. Tyto změny se mohou projevit naslouchán̆ím na novém síťovém portu, nebo přesměrováním běžné komunikace. Kromě pasivního čekání na pokyny dochází u těchto typů malware ke kontaktování útočníka a předání informace o úspěšné kompromitaci systému . Útočník však nemusí napadené zařízení kompromitovat pouze kvůli přístupu do sítě. Napadené zařízení může také pro útočníka po kompromitaci autonomně sbírat informace. Například má-li napadené zařízení vhodnou síťovou kartu, může sledovat veškerý provoz proudící přes ni i pokud není určen pro dané zařízení. V případě bezdrátové sítě se pak jedná o veškerý provoz v okolí. Jiným příkladem je sbírání informací z okolí napadeného zařízení pomocí jeho senzorů, jako je mikrofon, kamera nebo i GPS.

Kromě softwarové změny konfigurace je možná i změna konfigurace HW. Útočník může oběti nainstalovat přídavný hardware, nebo nahradit stávající tak, aby nepozorovaně plnil i jinou funkci. Nejznámějším využitím změny HW konfigurace je instalace keyloggeru, který zaznamenává veškeré stisky klávesnice a útočník je schopen pomocí něj zjistit hesla a jiné citlivé údaje o oběti.

Možnosti detekce jednotlivých symptomů

Jak vyplývá z kapitoly 2 je detekce APT útoků značně komplexní problém vzhledem k tomu, že jsou APT útoky vedeny profesionálně odborníky a s důrazem na skrývání svých aktivit. Přes to, že APT útoky lze teoreticky detekovat stejnými způsoby jako jakékoli jiné ICT útoky, profesionálně vedené APT útoky často zůstávají pod rozlišovacími schopnostmi stávajících bezpečnostních řešení. APT útoky nelze detekovat jednoduchým systémem či za- řízením, které by stačilo přidat do stávajícího systému v organizaci (jako např. IDS), pro umožnění detekce tohoto typu útoků je nutné zahrnout bezpečnost již do návrhu struktury systémů organizace. Pro identifikaci kritických míst je vhodné použít analýzu rizik, jejímž výstupem je seřazení zkoumaných prvků (aktiv) podle kritičnosti a pravděpodobnosti, že se útočník zaměří právě na toto místo. Návrh struktury s oddělením kritických prvků od méně kritických umožňuje zaměřit se při obraně na důležitá místa a neplýtvat energií a financemi jinde.

Mnoho symptomů sleduje abnormality v použití jednotlivých elementů, ať už se jedná o software, data nebo komunikaci. Sledování těchto informací lze abstrahovat do sledování množiny trojic použití, kde trojice použití je definována jako [Subjekt, Metoda, Objekt]. Subjekt je ta entita, která provádí nějakou akci s objektem a metoda pak popisuje způsob a typ prováděné akce. V případě přístupu k datům pak může být subjektem uživatel, popří- padě proces vyžadující data, metodou je pak volání nějakého rozhraní, nebo přímý přístup a objektem jsou ovlivněná data. V následujících sekcích jsou přiblíženy způsoby detekce jednotlivých symptomů.

Abnormální chování software

Pro sledování chování software jsou používány antivirové programy. Tyto programy prochází soubory přítomné na počítači a ověřují podle signatur, nejedná-li se o známý škodlivý software. V tomto základním pojetí jsou tyto programy schopny detekovat pouze ten malware, který je již znám a je pro něj vytvořena signatura a nejsou schopny odhalit nové hrozby a modifikaci či zneužití software. Pokročilejší antivirové programy jsou schopny detekovat podezřelé chování i podle pří- stupů aplikace k některým funkcím operačního systému nebo zdrojům, které nejsou běžně používány. Díky tomu jsou schopny rozpoznat i některé hrozby, pro které zatím není vytvo- řena signatura, pokud je jejich chování při těchto přístupech dostatečně podobné známému vzorci.

Pro detekci změn v software lze využít techniku podepisování, kdy je pro aplikaci spočten její otisk pomocí nějaké hashovací funkce a tento otisk je pak zašifrován soukromým klíčem vydavatele. Pomocí tohoto otisku pak lze detekovat nejen změny v software, protože dojde ke změně otisku, ale pokud máme ověřený veřejný klíč vydavatele, lze ověřit, že nainstalovaný software nebyl dodatečně modifikován. Toto ověřování je rozšířeno zejména u mobilních aplikací a Linuxových repozitářů, u aplikací pro Windows dochází k podepisování důležitých součástí systému, jako jsou ovladače, také. Problémem stále zůstává bezpečná distribuce veřejných klíčů vydavatelů, která bývá řešena pomocí centralizované správy software, jako jsou Linuxové repozitáře, Google Play store a úložiště ovladačů pro Windows. Pokud je software spravován centrálně, lze jej podepsat pomocí jednotného klíče a uživateli pak stačí mít k dispozici pouze jeden veřejný klíč.

Uzavírání aplikací do kontrolovaného prostředí, tzv. sandboxing, umožňuje kromě omezení přístupu aplikace také detekovat změny v chování. Aplikace je uzavřena ve svém prostředí, kde má přístup k datům a prostředkům, které potřebuje pro svůj běh, a všechny ostatní prostředky jsou jí skryty. Pokud detekujeme pokus aplikace přistoupit k datům mimo toto prostředí, je zde podezření, že byla napadena, protože při standardním použití by k podobným událostem nemělo docházet.

Abnormální přístup k datům

Pro detekci abnormalit přístupu k datům je nutné sledovat veškeré pokusy o načtení dat i jejich změny. Pro sledování těchto údajů však nestačí ukládat si informace v obslužném software, ale je potřeba součinnost operačního systému, který data spravuje. To z toho důvodu, že útočník může kromě přístupu pomocí standardních rozhraní využít i přímého přístupu k datům a zcela tak obejít obslužný software.

Protože sledování všech přístupů k datům je náročné, je potřeba data kategorizovat a oddělit od sebe citlivá data od těch, jejichž případný únik by neznamenal vážné bezpečnostní riziko. Kromě logického oddělení dat podle míry tajnosti je vhodné oddělit tato data i fyzicky. To umožňuje lepší správu přístupu k tajným datům a nasazení jiných politik pro přístupový systém. Pokud budou tajná data přístupná pouze přes dedikovaný přístupový server, je snažší nasadit na tento server bezpečný systém, který bude uchovávat větší množství informací o veškerých přístupech. Naproti tomu data, která jsou veřejná, budou umístěna na jiném zařízení, které nebude zbytečně zatíženo sbíráním informací o přístupu. Neoprávněné pokusy o přístup na tajná data jsou jednoznačným varováním, že by se mohlo jednat o útok. Kromě zamítnutých přístupů lze také sledovat způsob přístupu na data, jelikož útočníci se mohou často pokusit obejít standartní rozhraní ve snaze vyhnout se obranným mechanismům. Měla by tedy být kontrolována i integrita dat a ověřováno nejen kdo na data přistupuje, ale i jakým způsobem. Také lze detekovat, ke kterým datům uživatel přistupuje a sledovat, jestli se jeho chování nezmění a nezačne číst i data, která standartně nepotřebuje. Dobrou praktikou je povolit uživateli přístup pouze na ta data, která reálně potřebuje ke své činnosti.

Abnormální použití zařízení

Pro sledování používání zařízení je nutné uchovávat provozní informace o využití zařízení. Pro získávání těchto informací je nutná plná podpora operačního systému, který musí generovat auditní události. V Unixovém prostředí probíhá toto nastavení přes auditního démona auditd, v prostředí MS Windows je pak toto nastavení součástí služeb operačního systému pod názvem Security Auditing.

Mezi vhodné události, které by měl audit sledovat, patří přihlašování uživatelů. To umožní identifikovat přihlášení nestandartního uživatele, jako je například nepoužívaný účet guest, přihlášení nestandartním způsobem, což může být například vzdálené přihlášení k pracovní stanici, ke které se uživatel vždy přihlašuje lokálně, nebo přihlášení v nestandardní době. Jiným vhodným ukazatelem jsou běžící procesy a jejich nároky na RAM a vytížení CPU, které odhalí, zdali nedošlo ke spouštění neznámých procesů nebo nedošlo ke kompromitaci stávajících. Audit operačního systému umožňuje generovat i události související s prací se soubory a lze tedy detekovat vytváření, modifikace i čtení souborů. Pomocí sběru a sledování těchto dat lze vytvořit model popisující běžnou činnost zaří- zení, který může být pak použit pro porovnávání s aktuálním stavem a rozhodnutí, zdali je aktuální použití zařízení normální či nikoli.

Abnormální síťová komunikace

K detekci abnormální síťové komunikace lze přistoupit ze dvou zcela odlišných směrů. Prvním je sledování jednotlivých komunikačních toků a detekce podezřelého obsahu komunikace (například pokus o navázání spojení na neexistující uzel). Druhým přístupem je sledování chování jednotlivých účastníků, jejich komunikačních partnerů a vzorů chování a detekování podezřelého chování. Běžné firewally a IDS/IPS systémy používají první způsob. Firewally sledují, kdo se snaží komunikovat a jaký kanál (port) pro to chce využít a na základě sady pravidel rozhoduje, zda je komunikace povolená, či nikoli. IDS/IPS systémy často fungují na principu hloubkové analýzy paketů, kdy se snaží zjistit obsah komunikace a reagují na takový obsah, který mají označen jako nežádoucí. Tyto systémy jsou schopny velmi efektivně rozpoznávat známé typy útoků podle komunikačních partnerů (skenování portů, přístupy na neaktivní adresy) nebo podle známého obsahu nebezpečných paketů. Nejsou však schopny rozpoznat novátorské přístupy a skrytí před těmito systémy nepředstavuje pro zkušeného útočníka příliš velký problém.

Druhým způsobem lze odhalit útočníka podle chování, které nějakým způsobem vybo- čuje z normálního vzoru komunikace. Sledujeme-li chování jednoho uživatele v síti a jsme-li schopni vysledovat vzory v jeho komunikaci, lze rozeznávat změny v těchto vzorech nebo detekovat podezřelé aktivity podle známých vzorů chování. Systémy založené na detekci chování jsou teoreticky schopny odhalit i zcela nové a zatím neznámé útoky a skrytí před nimi je složité. Proto je tento způsob detekce vhodnější pro APT útoky. Chceme-li sledovat chování uživatele v síti pro detekci APT útoků, je nutné analyzovat veškerou jeho komunikaci. Pokud sledujeme chování uživatelů, stačí nám analyzovat odchozí komunikaci, podle ní totiž jsme schopni pozorovat akce uživatele, příchozí zprávy jsou většinou pouze reakcí na ty odchozí. Útočníci mohou sice zasílat do sítě příkazy nainstalovanému malware, což je příchozí komunikace, ale tyto příkazy se jen velmi těžko detekují a navíc pokročilý malware používaný při APT útocích může pracovat do značné míry autonomně, bez nutnosti příchozí komunikace. Nejsnadněji lze odhalit odchozí komunikaci po infikaci, kdy se malware přihlašuje do řídící sítě anebo když malware odesílá útočníkům nasbíraná data. Útočník však také může obranné mechanismy postupem času naučit komunikaci mezi řídící sítí a malware považovat za normální, pokud dostatečně pomalu rozšiřuje normální chování uživatele o svou komunikaci tak, aby zůstal pod rozlišovací schopností detekčního mechanismu. Proto je vhodné kromě změn v chování na síti sledovat také dlouhodobější trendy například porovnáním aktuálního normálního chování uživatele s tím, jaké bylo před měsícem, či rokem.

Výskyt phishingových e-mailů

Odhalování spear phishingových e-mailů je velmi náročný až téměř nemožný úkol vzhledem k důmyslnosti, se kterou jsou vytvořeny. Standardní součástí každého e-mailového serveru by měl být antiphishingový filtr. Tyto filtry jsou nejčastěji založeny na metodách strojového učení a rozpoznávají podvodné e-maily podle jejich struktury, zpracování přirozeného jazyka, kontrolou zpětného DNS záznamu zdrojového serveru a vznikají i protokoly pro ověřování autentičnosti e-mailů.

Pro napadení zařízení bývají v podvodných e-mailech nejčastěji využívány infikované přílohy, alternativně se útočníci snaží uživatele pomocí falešného odkazu přinutit navštívit podvrženou webovou stránku a malware si nevědomky nainstalovat. Malware připojený k e-mailu má zřídka formu spustitelného souboru, který bývá téměř vždy odhalen, ale častěji dochází k infikování ZIP či RAR archivu nebo souborů běžně používaných v organizaci (jako jsou tabulky v programu Excel nebo PDF soubory). Mnoho antivirů umožňuje prozkoumat přílohy e-mailů a pokusit se detekovat přítomný malware.

Protože však spear phishingové e-maily často díky své důmyslnosti překonají antiphishingové filtry, nezbývá než upozornit na tato rizika uživatele a před otevřením příloh podezřelých e-mailů vždy ověřovat nezávisle jejich autentičnost a na případné nesrovnalosti upozornit. Pokud se v organizaci vyskytnou kvalitní spear phishingové e-maily, které obsahují firemní informace, je riziko, že se organizace nachází pod APT útokem, velmi vysoké. Pokud se však podaří odhalit APT útok díky detekci phishingových e-mailů, došlo tak v prvních fázích útoku a útok tedy zatím pravděpodobně nezpůsobil velké ztráty.

Změna konfigurace zařízení

Pro sledování změn konfigurace zařízení je nutné vytvořit systém, který bude sledovat vybrané konfigurace a upozorní na jejich změnu. V případě zařízení firmy Cisco s operačním systémem IOS stačí sledovat dva konfigurační soubory - startup-config a running-config. U počítačů je ale situace komplikovanější, vzhledem k jejich komplexitě totiž neexistuje jednotný konfigurační soubor. Je tedy nutné pomocí nějakého nástroje sledovat důležitá konfigurační nastavení a ověřovat, jestli nedošlo v běžícím systému k dynamické změně konfigurace. Pro sledování integrity systému lze také použít TPM čip (Trusted Platform Module). Tento čip byl vyvinut jako bezpečnostní modul pro počítače a jednou z jeho funkcí může být i sledování, zda nedošlo k porušení integrity operačního systému [3]. Na základě podpisů jednotlivých konfiguračních souborů a hardwarové konfigurace by tento čip měl být schopen detekovat neoprávněné změny.