Razumevanje Cyber-Kill lanca i proširena verzija Cyber-Kill lanca

Uvod:

Većina organizacija ima sredstva za otkrivanje poznatih napada, mada se neke od njih i dalje mogu dogoditi. Ono što je bilo oduvek teško je zaustaviti nepoznate napade, koji su posebno prilagođeni da se zaobiđu najnovije zaštite promenom potpisa i obrasca ponašanja.

Mnoge organizacije su napravile značajne investicije u stvaranju vlastitog „tima za lov“ i/ili su pak preneli Managed Service Providera neizbežan i kritičan zadatak kontinuiranog razvijanja svojih odbrambenih tehnika i potražnje za boljim alatima i načinima za očuvanje njihove intelektualne svojine i digitalne imovine.

Stalna promena okruženja i frekvencija, sofisticiranost i specijalizovana priroda protivnika zahteva evoluciju operativnih sigurnosnih praksi u kombinaciju prevencije, otkrivanja i reakcije na cyber napade.

Razumevanje kako ovi protivnici funkcionišu i mapu odbrambene strategije organizacije u odnosu na životnog ciklusa njihovih aktivnosti mogu pokazati kako je moguće otkriti, zaustaviti, ometati i oporaviti se od napada i gde se bezbednosne aktivnosti organizacije mogu ojačati.

Cilj ovog predavanja je da se razume model životnog ciklusa cyber napada (Cyber-Kill Chain (CKC)), njegov osnovni i prošireni model i kako Panda Adaptive Defence Service pokriva taj životni ciklus i reaguje na taj ciklus u cilju zaštite krajnjih tačaka u sistemu.

Imajte na umu da su najvrednija sredstva organizacije, a ponekad i nekontrolisana, smeštena na krajnje tačke i na serverima. Zbog toga će svi napadači želeti da dođu upravo do njih kako bi dobili pristup ovim kritičnim sredstvima. Zaustavljanje protivnika na krajnjoj tački drastično smanjuje verovatnoću uspeha bilo kojeg cyber napadača, pojednostavljujući napore za prekid lanca i značajno povećanje efikasnosti i delotvornosti sigurnosnih sistema.

Razumevanje Cyber Kill lanca

Koncept Cyber Kill-Chain-a prvobitno je objavio Lockheed Martin kao deo modela za Inteligence Driven Defense.

Model definiše ono što napadači moraju da urade kako bi postigli svoj cilj, ciljanjem mreže, eksfiltracijskim podataka i neprestanom aktivnošću u penetraciji zaštitnih sistema organizacije.

Zahvaljujući ovom modelu saznali smo da zaustavljanje protivnika u bilo kojoj fazi može da razbije lanac napada. Da bi uspeo, napadači mora sve vreme napredovati kroz sve faze dok odbrana može biti uspešna blokiranjem samo jedne od faza.

U sledećim koracima videćemo da je krajnja tačka neizbežna tačka ka kojoj svi napadi idu i stoga zaustavljanje na ovom nivou enormno povećava šansu da se prekine svaki sajber napad. Stopa uspeha će biti veća ako se zaustave u ranim fazama u lancu.

Bolje razumevanje napadača i njihovih tehnika u cilju razvoja efikasnijih sistema odbrane

Cyber-Kill navodi da za izvršenje svojih namera, protivnici moraju uvek slediti sedam osnovnih koraka:

1. ***External Reconnaissance***

Ova faza se može definisati kao faza ciljne selekcije, identifikacija detalja organizacije, industrijsko-vertikalni-zakonski zahtevi, informacije o izboru tehnologije, društvene mreže ili mailing liste. Protivnik u suštini želi da odgovori na ova pitanja: „Koje metode napada će raditi sa najvišim stepenom uspeha?“ i „Koje je najlakše primeniti u smislu ulaganja resursa?“

2. ***Weaponization and packaging***

Ovo podrazumeva mnoge forme: eksploataciju veb aplikacija, off-shelf ili prilagođeni malver (preuzet za ponovnu upotrebu ili kupljen), ranjivosti složenih dokumenata (isporučeno u PDF formatu, Office ili drugim formatima dokumenta) ili watering hole napad.

3. ***Delivery***

Prenos „sadržaja“ je pokrenut ili od strane mete (na primer, korisnik pregledava Web sa malicioznim sadržajem, što dovodi do upotrebe „expliot“-a radi isporuke zlonamernog koda ili otvara zlonamerni PDF fajl) ili od strane napadača (npr. SQL injection).

4. ***Exploitation***

Nakon isporuke korisniku, računaru ili uređaju, zlonamerni kod će „preuzeti“ platformu, čime će se stvoriti baza u kompanijskom okruženju za nastavak delovanja.

5. ***Installation***

Ovo često ima oblik nečega što aktivno komunicira sa spoljnim okruženjem. Malver je obično tajan u svom radu, šireći se na krajnjim tačkama kojima može da pristupi. Napadač onda može da kontroliše ovu aplikaciju neprimetno i bez podizanja „uzbune“ u organizaciji.

6. ***Command and Control***

U ovoj fazi, napadač ima kontrolu nad sredstvima unutar ciljne organizacije putem metoda kontrole (najčešće udaljenih), kao što su DNS, Internet Control Message Protocol (ICMP), web

stranice i društvene mreže. U ovom koraku napadač „govori“ kontrolisanoj „svojini“ šta treba dalje da uradi i koje informacije treba sakupiti.

Metode koje se koriste za prikupljanje podataka pod komandom uključuju snimanje ekrana i aktivnosti na tastaturi, otkrivanje lozinki, nadgledanje mreže radi sakupljanja akreditiva, prikupljanje osetljivih sadržaja i dokumenata. Često je u ovoj fazi definisan, na koji se kopiraju svi interni podaci, zatim se komprimuju i/ili šifriraju i spremaju se za eksfiltraciju.

7. Actions on Targets

Ova završna faza obuhvata operacije nad podacima i/ili oštećenje IT sredstva. Zatim se preduzimaju mere za identifikaciju novih ciljeva, proširenje njihovog otiska unutar organizacije i – možda najvažnije – eksfiltracija podataka.

Zatim se CKC ponavlja. Zapravo, kritična tačka sa CKC-om jeste to što je kružna, a ne linearna. Jednom kada napadač uđe u mrežu, on ponovo počinje sa CKC u mreži i to onda postaje unutrašnji CKC.

Pored toga, neophodno je imati na umu da dok je metodologija ista, napadač će koristiti druge metode za kretanje kroz unutrašnji lanac ubijanja, nasuprot onima koje je koristio dok je bio izvan okruženja.

U stvari, kada se napadač nalazi unutar mreže, postaje insajder, korisnik sa privilegijama, a to sprečava bezbednosne timove da sumnjaju u napad i shvate da je već u naprednim fazama proširenog modela Ciber-Kill Chain.

CKC je kružni i nelinearni proces, gde se napadač stalno i kontinuirano kreće unutar mreže. Faze koje se odvijaju unutar mreže su iste kao i one koje se koriste kada je cilj bio pristup mreži, iako koriste različite tehnike i taktike.

Kombinacija spoljnog i unutrašnjeg CLC se zove Prošireni CLC. To znači dodavanje više koraka, koji su u stvari isti skup aktivnosti, samo na naglaskom na „unutrašnji“, tako da CKC postaje Unutrašnji CKC sa sopstvenim fazama, unutrašnjim izviđanjem, unutrašnjim oružjem i tako dalje.

Svaka od faza napada, kada se napadač jednom nađe u mreži žrtve, može potrajati od nekoliko minuta do meseci, uključujući i konačno vreme čekanja kada je napad pripremljen i spreman za aktiviranje.

Imajte na umu da će napadač zadržati optimalno vreme za pokretanje kako bi se dobio najveći efekat.

Faze izviđanja i pripreme „oružja“ mogu trajati mesecima.

Te faze je teško prekinuti pošto se one sprovode bez povezivanja sa napadačem. Zbog toga je od ključne važnosti da mere bezbednosti na krajnjim tačkama analiziraju i nadziru sve sisteme i aplikacije koje se koriste u uređajima. To će značajno ometati rad napadača, a napad neće postati profitabilan.

Internal Reconnaissance

U ovoj fazi, protivnici imaju pristup jednoj korisničkoj radnoj stanici i istražiće je u potrazi za lokalnim datotekama, mrežnim pristupima, istoriji pregledača i pristupu Wiki i SharePointu. Cilj je da se utvrdi kako bi ta mašina mogla da mapira mrežu i omogući prelazak na više vredna sredstva.

Internal Exploitation

Koristeći nedostatak patch-eva, ranjivost web aplikacija, broadcast protokole, spoofing ili čak nečeg tako jednostavnog kao što su default kredencijali, napadač će omogućiti sebi da se premesti sa radnih stanica na servere koristeći eskalaciju privilegija, bočno kretanje unutar mreže i manipulaciju pojedinačnim ciljanim mašinama.

Napadači imaju ciljeve i spremni su da potroše određenu količinu resursa kako bi ih postigli. Ako sigurnosni mehanizam krajnjih tačaka može povećati trošak – bilo finansijski, kadrovski ili vremenski – iznad vrednosti koju napadači očekuju, onda će najčešće odlučiti da ne napadnu tu organizaciju.

Misija kompanije Panda Securiti je da se to uvek desi, a s obzirom na rezultate, upravo je to rezultat zaštite uz pomoć Panda Adaptive Defense.

Sve organizacije moraju biti spremne da pitaju šta će učiniti ako napadač ima pristup internoj korporativnoj mreži, korisničkim imenima i lozinkama, dokumentaciji i specifikacijama mrežnih uređaja, sistema, sigurnosnim kopijama i aplikacijama i spreman da odmah reaguje.

Viši cilj sigurnosne strategije treba da bude izgradnja otpornijeg sistema. To neće sprečiti sve napade, ali će ih sprečiti više i u ranijim fazama. Jedan od ciljeva je postaviti efikasni odbrambeni mehanizam na proširenom CKC, a kako bi usporili napadače, učinili skupljim i težim svako premeštanje u narednu fazu.

Ako protivnici ne mogu ostvariti svoj cilj na način koji ima ekonomski smisao, oni će ići po različitim ciljevima ili sličnim ciljevima, ali sa drugom organizacijom.

Strategija sigurnosti organizacija mora uzeti u obzir kako se napad izvršava, spolja, a posebno iznutra, jer su napadači jednom u mreži, insajderi sa pristupom krajnjim tačkama i njihovoj imovini.

Tradicionalni bezbednosni pristup treba proširiti metodama zasnovanim na razumevanju CKC i obezbeđivanju tehnologija koje mogu sprečiti napadače da dobiju pristup krajnjim tačkama, ali i da ih zaustave u bilo kojoj mogućoj fazi tokom unutrašnjeg CKC.

Mapiranje strategije odbrane u proširenom CKC modelu pokazuje kako organizacija može sprečiti, otkriti, ometati i oporaviti se kroz faze napada, uskladivši sigurnost organizacije sa istim kriterijumima uspeha kao i napadači.

To je teško postići zbog više faktora: aplikacije su povećane kako u složenosti tako i međusobnoj povezanosti, aplikacije su ugrožene, jer većina softvera nije razvijana primenom principa sigurnosti.

Zaposleni i partneri takođe ostaju glavni faktor rizika i otvorena vrata za napade zasnovane na socijalnom inženjerstvu.

Panda Adaptive Defense i Panda Adaptive Defense 360 se bave osnovnim stubovima koji se isporučuju u obliku upravljačkog servisa, sprečavaju i otkrivaju najnaprednije tehnike napada i taktike u svakoj fazi proširenog CLC i pomaže bezbednosnim timovima da dizajniraju sigurnosnu strategiju u skladu sa CLC.

Zaštita od poznatog malware-a

Traženje poznatih pretnji neće zaštititi od varijanti ili nepoznatih napada, ali proširenje sa dodatnim sigurnosnim slojevima može preventivno zaustaviti poznate pretnje kada ih isporučuju u krajnju tačku.

Panda Adaptive Defense 360 koristi ogromnu kolekciju reputacionih usluga kako bi proaktivno blokirala napadače tokom faze „Isporuke“, a koristeći podatke iz oblaka.

Napredna detekcija

Panda Adaptive Defense i Panda Adaptive Defense 360 otkrivaju i blokiraju nepoznate zlonamerne programe i ciljane napade zahvaljujući sigurnosnom modelu zasnovanom na tri načela:

- kontinuiran dubinski nadzor svih aplikacija koje se pokreću na krajnjim tačkama,
- automatska klasifikacija procesa krajnjih tačaka koristeći Big Data i
- machine learning tehnike na cloud platformi, sa mogućnošću da se proces, ako ne automatski klasifikuje, onda od strane stručnog lica.

Dynamic Expoit Detection

Tokom Exploit faze proširenog CKC, napadači koriste exploit-e da ciljaju ranjivosti na nivou koda, tako da mogu da „probiju“ aplikacije i sisteme, u cilju instaliranja i aktiviranja malvera. Preuzimanja (download) sa interneta je uobičajeni vektor za izvršavanje Exploit napada. Panda Adaptive Defense i Panda Adaptive Defense 360 pružaju dinamične anti-exploit mogućnosti za zaštitu na nivou aplikacija i memory-based napada.

Panda Adaptive Defense i Panda Adaptive Defense 360 otkrivaju i blokiraju stvarne tehnike koje koriste napadači tokom eksploatacionog stadijuma (heap spraying, stack pivots, ROP attacks and memory permitions modifications), ali osim toga dinamički otkriva nepoznate napade praćenjem svih procesa koji se pokreću na uređajima i utiču na podatke kroz algoritme mašinskog učenja u oblaku.

Adaptive Defense Anti-exploit tehnologije će zaustaviti napadača u ranoj fazi unutrašnjeg napada tako što će identifikovati čim dođe do kompromitovanja aplikacija ili procesa.

Ublažavanje (Mitigation)

Zaštita krajnje tačke sledeće generacije mora sprečiti i otkrivati napadače tokom različitih faza CKC, ali otkrivanje mora biti praćeno brzim ublažavanjem napada tokom početnih faza lansiranja.

Panda Adaptive Defense 360 automatski i blagovremeno ublažava napad, postavljanjem malvera u karantin, ubijanjem kompromitovanog procesa ili čak potpunim zatvaranjem sistema kako bi se smanjila šteta.

Remedijacija

Tokom izvršenja, malver često stvara, modifikuje ili briše sistemske datoteke i podešavanje registra i menja konfiguraciona podešavanja.

Ove promene ili ostaci koji su ostavljeni za sobom mogu da izazovu nestabilnost sistema ili čak otvorena vrata za nove napade.

Panda Adaptive Defense 360 vraća krajnje tačke na svoje pre-malvare stanje.

Forenzičari

U okviru promene okruženja i sa učestalošću, sofisticiranošću i ciljanom prirodom napadača, ne bi trebalo biti nikakve sigurnosne tehnologije koja tvrdi da je 100% efikasna i stoga je sposobnost pružanja forenzičkih podataka i vidljivosti u stvarnom vremenu neophodna.

Timovi za korporativnu sajber sigurnost treba da imaju plan za rešavanje situacija u kojima je došlo do proboja koji uključuje i kontaktiranje predstavnika zakona kao i suočavanje sa nepovoljnim publicitetom i slično.

Panda Adaptive Defense i Panda Adaptive Defense 360 pružaju jasnu i pravovremenu vidljivost zlonamerne aktivnosti u čitavoj organizaciji. Ova vidljivost omogućava timovima bezbednosti da brzo procene opseg napada i preduzmu odgovarajuće odgovore.