Lateralno kretanje – Replikacija putem prenosivog medija

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Ograničite pristup kritičnim sredstvima po potrebi
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Ograničite upotrebu USB uređaja i prenosivih medija unutar mreže
- Blokirajte pokretanje nepouzdanih izvršnih datoteka sa prenosivih medija

(I) Identifikacija

- Pratite:

a. Neobičan pristup datotekama na prenosivim medijama
b. Procese koji se izvršavaju sa prenosivog medija nakon što je postavljen
c. Mrežne veze sa komandnim i kontrolnim serverima
d. Procese koji neobično otkrivanje informacija o sistemu i mreži

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada

(E) Eliminacija

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme (P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu
- kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružatelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Izvršenje - Eksploatacija za izvršenje klijenta

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Ograničite pristup kritičnim sredstvima po potrebi
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Razmislite o pokretanju aplikacija na virtualnim mašinama

(I) Identifikacija

- Pratite:

a. Nenormalno ponašanje pregledača ili Office procesa
b. Sumnjive datoteke zapisane na disk
c. Izmjene evidencije
d. Neobičan mrežni saobraćaj

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski provjerite evidencije firewall-a, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Držati pod kontrolom eventualne DLL-ove koji su učitani procesom kojim ne bi trebalo da budu

(E) Eliminacija

- Zatvorite vektor napada primenom gore navedenih koraka
- Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Lateralno kretanje – Kompromitovan dijeljeni sadržaj

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno proveravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Ograničite pristup kritičnim sredstvima po potrebi
- Sprovedite obuku o bezbednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Ograničite pristup deljenim diskovima samo zaposlenima kojima je potreban pristup

(I) Identifikacija

- Pratite:

a. Sumnjive procese upisivanja ili prepisivanja nekih datoteka na dijeljeni disk
b. Sumnjive procese koji pristupaju dijeljenim diskovima bez ovlaštenja
c. Mrežnu komunikaciju sa C2 serverima
d. Procese koji se izvršavaju sa prenosivog medija

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada

(E) Eliminacija

- Zatvorite vektor napada primenom gore navedenih koraka Pripreme(P)
- Privremeno uklonite pristup deljenom disku da biste ograničili dalje širenje
- Skenirajte dijeljeni disk u potrazi za zlonamernim datotekama ili drugim datotekama kojima nije mesto u deljenom disku
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromizovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Proverite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada pre oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Vratite pristup deljenom disku u samo zaposlenima kojima je potreban pristup
- Adresirajte eventualnu kolateralnu štetu pregledom i procenom izloženih tehnologija
- Rešite sve povezane bezbednosne incidente
- Vratite pogođene sisteme na njihovu poslednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružatelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Eskalacija privilegija – Kreiranje ili izmjena procesa sistema

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Ograničite pristup kritičnim sredstvima po potrebi
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Koristite alate za nadgledanje koji su sposobni da otkriju mogućnosti za zloupotrebu privilegija i usluga na sistemima unutar preduzeća i da ih isprave

(I) Identifikacija

- Pratite:

a. Promjene sistemskh procesa koje nisu u korelaciji sa poznatim softverom
b. Abnormalni proces poziva iz poznatih usluga
c. Abnormalne promjene datoteka povezanih sa sistemskim nivoima procesa

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Držati pod kontrolom eventualne DLL-ove koji su učitani procesom kojim ne bi trebalo da budu

(E) Eliminacija

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Izbegavanje odbrane - Podrivanje kontrola pouzdanosti

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Ograničite pristup kritičnim sredstvima po potrebi
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Koristite kontrolu aplikacije i/ili blokiranje skripti da biste blokirali neodobrene aplikacije
- Uvjerite se da su "Hide Microsoft Entries" i "Hide Windows Entries" izabrane u “Autoruns-u”
- Koristite smjernice Windows grupe za upravljanje *root* certifikatima

(I) Identifikacija

- Pratite:

a. Abnormalne pokušaje izmjene proširenih atributa datoteke pomoću programa kao što je “xattr”
b. Odstupanja u očekivanoj aktivnosti “Autoruns”
c. Neočekivane certifikate koji su instalirani na sistemu
d. Odstupanja kod registrovanih SIP-a i provajderima od povjerenja
e. Odstupanja u metapodacima certifikata za potpisivanje

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski provjerite evidencije firewall-a, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Držati pod kontrolom eventualne DLL-ove koji su učitani procesom kojim ne bi trebalo da budu

(E) Eliminacija

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada pre oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Izbjegavanje odbrane – Izmjena smjernica domena

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Ograničite pristup kritičnim sredstvima po potrebi
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Identifikujte i ispravite mogućnosti zloupotrebe GPO (*group policy object*) dozvola
- Razmislite o implementaciji bezbjednosnog filtriranja

(I) Identifikacija

- Pratite:

a. Zlonamjerne zakazane zadatke
b. Lažne upravljače domena
c. Sumnjive promjene GPO (*group policy object*)
d. Komande i komandne linije koje mogu biti korisne za izmjenu postavke politike domena

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Držati pod kontrolom eventualne DLL-ove koji su učitani procesom kojim ne bi trebalo da budu

(E) Eliminacija

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu
- kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Pristup kredencijalima – Nasilan upad

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Ograničite pristup kritičnim sredstvima po potrebi
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Podesite smjernice za zaključavanje naloga nakon određenog broja neuspjelih pokušaja prijavljivanja
- Omogućite potvrdu identiteta sa više faktora gdje god je to moguće
- Koristite jake smjernice za lozinke na svim nalozima

(I) Identifikacija

- Nadgledajte veliki broj grešaka u autentifikaciji pomoću bilo koje od sljedećih metoda:

a. Pogađanje lozinke
b. Razbijanje lozinke
c. Iskorištavanje iste lozinke na više naloga iz neke baze (Password Spraying)
d. Iskorištavanje kompromitovanih kredencijala (Credential Stuffing)

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada

(E) Eliminacija

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa
- Odmah resetujte naloge koji su provaljeni

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Udar – Otmica resursa

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okruženja
- Ograničite pristup kritičnim sredstvima po potrebi
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Pregledajte AUP (Acceptable Use Policy) i BYOD (Bring Your Own
- Device) smjernice

(I) Identifikacija

- Pratite:

a. Neuobičajeno korišćenje procesa za utvrđivanje anomalne aktivnosti povezane sa zlonamjernom otmicom računarskih resursa kao što su CPU, memorija i resursi za obradu grafike
b. Sumnjivo korišćenje mrežnih resursa povezanih sa softverom za rudarenje kriptovaluta
c. Uobičajeni nazivi procesa i datoteka softvera za kripto rudarenje na lokalnim sistemima koji mogu ukazivati na kompromis i korištenje resursa

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski proverite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Držati pod kontrolom eventualne DLL-ove koji su učitani procesom kojim ne bi trebalo da budu

(E) Eliminacija

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružatelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Udar – Otmica resursa

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okruženja
- Ograničite pristup kritičnim sredstvima po potrebi
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Pregledajte AUP (Acceptable Use Policy) i BYOD (Bring Your Own
- Device) smjernice

(I) Identifikacija

- Pratite:

a. Neuobičajeno korišćenje procesa za utvrđivanje anomalne aktivnosti povezane sa zlonamjernom otmicom računarskih resursa kao što su CPU, memorija i resursi za obradu grafike
b. Sumnjivo korišćenje mrežnih resursa povezanih sa softverom za rudarenje kriptovaluta
c. Uobičajeni nazivi procesa i datoteka softvera za kripto rudarenje na lokalnim sistemima koji mogu ukazivati na kompromis i korištenje resursa

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski proverite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Držati pod kontrolom eventualne DLL-ove koji su učitani procesom kojim ne bi trebalo da budu

(E) Eliminacija

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružatelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Početni pristup – Hardverski dodaci

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Ograničite pristup kritičnim sredstvima po potrebi
- Zabranite svaki pristup prenosivim medijima ako to nije potrebno za poslovne operacije

(I) Identifikacija

- Pratite:

a. Neovlašćeno korištenje spoljnih komunikacionih portova uključujući USB uređaje
b. Neovlašteno dodavanje sistemskog hardvera
c. Sva sredstva koja ne bi trebalo da postoje na mreži

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada

(E) Eliminacija

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa
- Odmah resetujte naloge koji su provaljeni
- Uklonite sve neodobrene prenosive medije iz okruženja

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Eksfiltracija – Eksfiltracija preko fizičkog medija

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Ograničite pristup kritičnim sredstvima po potrebi
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Primjenite strategije za sprečavanje gubitka podataka
- Onemogućite automatsko pokretanje ako je nepotrebno
- Ograničite upotrebu USB uređaja i prenosivih medija unutar mreže

(I) Identifikacija

- Pratite:

a. Izvršene komande koje mogu pokušati eksfiltrirati podatke preko fizičkog medijuma
b. Novo dodjeljeni diskovi ili tačke pristupa na uređaj za skladištenje podataka
c. Neovlaštene pristupe datotekama na prenosivom medijumu
d. Novoizvršeni procesi u trenutku montiranja prenosivog medija

- Istražite i obrišite sva upozorenja povezana sa pogođenim sredstvima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Zaustavljanje

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara | Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada

(E) Eliminacija

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa
- Odmah resetujte naloge koji su provaljeni
- Uklonite sve neodobrene prenosive medije iz okruženja

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Izbjegavanje odbrane – Odbrana oštećenja

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Uvjerite se da postoje dozvole za ograničavanje neovlaštenih korisnika da ne ometaju bezbjednosne usluge

(I) Identifikacija

- Nadgledajte za:

a. Neovlaštene izmjene Windows registratora
b. Neovlaštene izmjene zaštitnog zida
c. Neovlašteno izvršavanje komande ili skripte
d. Neovlašteno kreiranje ili prekid procesa
e. Neovlašteni pristup ili modifikacija bezbjednosnih alata/oružja

- Istražite i obrišite sva obavještenja povezana sa pogođenim sredstvima
- Rutinski provjerite da li u evidencijama zaštitnog zida, IDS-a, IPS-a i SIEM-a postoji bilo kakva neobična aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada

(E) Iskorjenjivanje/Uništavanje

- Zatvorite vektor napada primenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Provjerite sva sredstva i aktivnost korisnika za MOK u skladu sa profilom napada
- Provjerite rezervne kopije za MOK u skladu sa napadačkim profilom prije oporavka sistema
- Zakrpa ranjivosti sredstava
- Uspostavite početne vrijednosti naloga koji su odmah probijani

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Početni pristup – Iskorištavanje aplikacije okrenute ka javnosti

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Implementiraj zaštitne zidove Web aplikacija (WAFs)
- Segment spoljno okrenut serverima i uslugama iz ostatka mreže sa DMZ-om ili korištenjem zasebne hosting infrastrukture

(I) Identifikacija

- Nadgledajte po:

a. Korištenje dubinske inspekcije paketa za traženje artefakata uobičajenog eksploatacionog saobraćaja, kao što su SQL niske za ubrizgavanje, poznati tovari i drugi pokazatelji kompromisa

- Istražite i obrišite sva obavještenja povezana sa pogođenim sredstvima
- Rutinski provjerite da li u evidencijama zaštitnog zida, IDS-a, IPS-a i SIEM-a postoji bilo kakva neobična aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada

(E) Iskorjenjivanje/Uništavanje

- Zatvorite vektor napada primenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Provjerite sva sredstva i aktivnost korisnika za MOK u skladu sa profilom napada
- Provjerite rezervne kopije za MOK u skladu sa napadačkim profilom prije oporavka sistema
- Zakrpa ranjivosti sredstava
- Resetujte nalog koji je probijen, odmah
- Uklanjanje svih neodobrenih prenosivih medija iz okruženja

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Otkrivanje - otkrivanje smjernica lozinke

(P) Priprema

- Popravite (zakrpite) ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Uvjerite se da je antivirusni/zaštitni softver instaliran na radnim stanicama i laptop računarima
- Utvrdite da se serveri i radne stanice prijavljuju na centralnu lokaciju
- Redovno provjeravati pravila firewall-a, IDS-a i IPS-a i ažurirajte ih prema potrebama okuženja
- Sprovedite obuku o bezbjednosti zaposlenih
- Ograničite korisnike na minimalne privilegije koje su im potrebne
- Postavljanje i primjena smjernica bezbjedne lozinke za sve naloge
- Pogledajte smjernice NIST-a prilikom kreiranja smjernica za lozinke
- Uvjerite se da svi nalozi sa punim dozvolama imaju lozinke koje su jedinstvene, složene i potrebne za periodično mijenjanje

(I) Identifikacija

- Nadgledajte za:

a. Pristup detaljnim informacijama o smjernicama lokalne lozinke organizacije
b. Pristup smjernicama za lozinke zasnovane na oblaku kao što je AWS
c. Više neuspjelih pokušaja potvrde identiteta na jednom ili različitom nalogu
d. Pokušaji korisničkog naloga da dobiju pristup neobičnim ili neovlaštenim sistemima ili mrežama
e. Greške pri prijavljivanju sa neobičnih lokacija ili ponovljenih MFA neuspjeha

- Istražite i obrišite sva obavještenja povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada

(E) Iskorjenjivanje/Uništavanje

- Zatvorite vektor napada primjenom gore navedenih koraka pripreme
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije za MOK u skladu sa napadačkim profilom prije oporavka sistema
- Zakrpa ranjivosti sredstava
- Uspostavite početne vrijednosti naloga koji su odmah probijani

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Zapamtite da podatke i događaje ne treba posmatrati izolovano, već kao dio lanca ponašanja koji može dovesti do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Izviđanje - Web lokacije u vlasništvu žrtvi

(P) Priprema

- Zakrpa ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Održavanje ispravki antivirusne/EDR aplikacije
- Kreiranje segmentacije mreže
- Evidentirajte saobraćaj između mrežnih segmenata
- Uključite obavještajne podatke o prijetnjama
- Izvršite rutinsku inspekciju rezervnih kopija imovine
- Sprovodite *phishing* simulacije
- Sprovesti obuku za bezbjednost korisnika
- Sprovoditi Response training- Trening za pravovremeni odgovor na prijetnju (PBC)
- Fokusirajte se na minimiziranje količine i osjetljivosti podataka dostupnih spoljnim stranama

(I) Identifikacija

- Nadgledajte po:

a. Sumnjiv mrežni saobraćaj koji bi mogao biti pokazatelj izviđanja protivnika
b. Brze sukcesije zahtjeva koji ukazuju na web popisivanje
c. Velike količine zahtjeva koje potiču iz jednog izvora
d. Web metapodaci koji također mogu otkriti artefakte koji se mogu pripisati potencijalno zlonamernoj aktivnosti, kao što su referentna ili niska korisničkog agenta HTTP/S polja

- Istražite i obrišite sva obavještenja povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite da li u evidencijama zaštitnog zida, IDS-a, IPS-a i SIEM-a postoji bilo kakva neobična aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Utvrđivanje kritičnih sredstava koja nisu pogođena

(E) Iskorjenjivanje/Uništavanje

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Izbjegavajte otvaranje e-pošte i priloga nepoznatih pošiljalaca
- Izbjegavajte otvaranje priloga e-pošte od pošiljalaca koji obično ne uključuju priloge
- Ne zaboravite da podatke i događaje ne treba posmatrati u izolaciji već kao dio lanca ponašanja koji bi mogao da dovede do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Izviđanje - Prikupljanje informacija o hostu žrtve

(P) Priprema

- Zakrpa ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Održavanje ispravki antivirusne/EDR aplikacije
- Kreiranje segmentacije mreže
- Evidentirajte saobraćaj između mrežnih segmenata
- Uključite obavještajne podatke o prijetnjama
- Izvršite rutinsku inspekciju rezervnih kopija imovine
- Sprovodite *phishing* simulacije
- Sprovesti obuku za bezbjednost korisnika
- Sprovoditi Response training- Trening za pravovremeni odgovor na prijetnju (PBC)
- Fokusirajte se na minimiziranje količine i osjetljivosti podataka dostupnih spoljnim stranama

(I) Identifikacija

- 1.Nadgledajte za:

a. Evidentiran mrežni saobraćaj kao odgovor na skeniranje koje prikazuje vrijednosti zaglavlja i tijela protokola koje mogu da kupe i/ili ukradu SSL/TLS sertifikate koji se mogu koristiti tokom ciljanja
b. Kontekstualni podaci o resursu okrenutom ka Internetu prikupljenom iz skeniranja, kao što su usluge pokretanja ili portovi koji mogu da kupuju, iznajmljuju, ili kompromituju infrastrukturu koja bi mogla da se koristi tokom ciljanja

- Istražite i obrišite sva obavještenja povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Utvrđivanje kritičnih sredstava koja nisu pogođena

(E) Iskorjenjivanje/Uništavanje

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Izbjegavajte otvaranje e-pošte i priloga nepoznatih pošiljalaca
- Izbjegavajte otvaranje priloga e-pošte od pošiljalaca koji obično ne uključuju priloge
- Ne zaboravite da podatke i događaje ne treba posmatrati u izolaciji već kao dio lanca ponašanja koji bi mogao da dovede do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Izbjegavanje odbrane – Važeći nalozi

(P) Priprema

- Zakrpa ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Održavanje ispravki antivirusne/EDR aplikacije
- Kreirajte segmentaciju mreže i evidentirajte se između segmenata
- Uključite obavještajne podatke o prijetnjama
- Izvršite rutinsku inspekciju rezervnih kopija imovine
- Sprovesti obuku za bezbjednost korisnika (sa fokusom na sumnjivu svijest o MFA aktivnostima)
- Sprovesti obuku za reagovanje (PBC)
- Uvjerite se da aplikacije skladište akreditive na bezbjedan način i sprovode ispravke akreditiva u pravilnim intervalima
- Odmah promijenite podrazumjevane akreditive naloga
- Pridržavanje principa najmanje privilegije
- Obavlja redovne pretrage za neaktivne korisničke naloge i provjeriti da li su očišćeni iz okruženja

(I) Identifikacija

- 1.Nadgledajte za:

a. Abnormalnosti ili potencijalna zloupotreba postojećih korisničkih akreditiva
b. Sumnjivo ponašanje naloga u sistemima koji dijele naloge
c. Novokreirani nalozi dobijaju pristup neovlaštenim sistemima ili softveru

- Istražite i obrišite sva obavještenja povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Utvrđivanje kritičnih sredstava koja nisu pogođena

(E) Iskorjenjivanje/Uništavanje

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Popravite ranjivosti resursa

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Redovno sprovodite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Izbjegavajte otvaranje e-pošte i priloga nepoznatih pošiljalaca
- Izbjegavajte otvaranje priloga e-pošte od pošiljalaca koji obično ne uključuju priloge

CSEC
Cyber Security Excellence Centre

Upornost - Izmjena procesa potvrde identiteta

(P) Priprema

- Zakrpite ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Održavajte ispravke antivirusne/EDR aplikacije
- Kreirajte segmentaciju mreže
- Evidentirajte saobraćaj između mrežnih segmenata
- Uključite obavještajne podatke o prijetnjama
- Izvršite rutinsku inspekciju rezervnih kopija imovine
- Sprovodite *phishing* simulacije
- Sprovesti obuku za bezbjednost korisnika
- Sprovoditi Response training- Trening za pravovremeni odgovor na prijetnju (PBC)
- Omogućite potvrdu identiteta sa više faktora na svim interfejsima za potvrdu identiteta
- Onemogućavanje skladišta lozinki pomoću reverzibilnog šifrovanja

(I) Identifikacija

- 1.Nadgledajte za:

a. Abnormalnosti ili potencijalna zloupotreba postojećih korisničkih akreditiva
b. Sumnjivo ponašanje naloga u sistemima koji dijele naloge
c. Novokreirani nalozi dobijaju pristup neovlaštenim sistemima ili softveru

- Istražite i obrišite sva obavještenja povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Utvrđivanje kritičnih sredstava koja nisu pogođena

(E) Iskorjenjivanje/Uništavanje

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Zakrpa ranjivosti sredstava

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Izvršite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novodobijene potpise prijetnji
- Izbjegavajte otvaranje e-pošte i priloga nepoznatih pošiljalaca
- Izbjegavajte otvaranje priloga e-pošte od pošiljalaca koji obično ne uključuju priloge
- Ne zaboravite da podatke i događaje ne treba posmatrati u izolaciji već kao dio lanca ponašanja koji bi mogao da dovede do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Otkriće - Otkrivanje obilježivača pregledača

(P) Priprema

- Zakrpite ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Održavajte ispravke antivirusne/EDR aplikacije
- Kreirajte segmentaciju mreže
- Evidentirajte saobraćaj između mrežnih segmenata
- Uključite obavještajne podatke o prijetnjama
- Izvršite rutinsku inspekciju rezervnih kopija imovine
- Sprovodite *phishing* simulacije
- Sprovesti obuku za bezbednost korisnika
- Sprovoditi Response training- Trening za pravovremeni odgovor na prijetnju (PBC)

(I) Identifikacija

- 1.Nadgledajte za:

a. Izvršene komande ili radnje preduzete za prikupljanje informacija o obilježivaču pregledača putem alatki za daljinski pristup, alatki za upravljanje sistemom ili Powershell-a
b. Neočekivani pristup ili prikazivanje obilježivača pregledača
c. Prikupljanje ili izostavljanje podataka obilježivača pregledača
d. Novi procesi neočekivano prikupljanje ličnih korisničkih podataka

- Istražite i obrišite sva obavještenja povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Utvrđivanje kritičnih sredstava koja nisu pogođena
- Onemogućite privilegije za račune za koje se sumnja da su kompromitovani

(E) Iskorjenjivanje/Uništavanje

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Resetujte sve kompromitovane lozinke
- Pregledajte sva sredstva i aktivnosti korisnika u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada
- Provjerite rezervne kopije u potrazi za indikatorima kompromitacije koji odgovaraju profilu napada prije oporavka sistema
- Zakrpa ranjivosti sredstava

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Izvršite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novododate potpise prijetnji
- Izbjegavajte otvaranje e-pošte i priloga nepoznatih pošiljalaca
- Ne zaboravite da podatke i događaje ne treba posmatrati u izolaciji već kao dio lanca ponašanja koji bi mogao da dovede do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Lateralno kretanje – Unutrašnji spirpišing (spear phishing)

(P) Priprema

- Zakrpite ranjivosti sredstava
- Izvršite rutinsku inspekciju kontrola/oružja
- Održavajte ispravke antivirusne/EDR aplikacije
- Kreirajte segmentaciju mreže
- Evidentirajte saobraćaj između mrežnih segmenata
- Uključite obavještajne podatke o prijetnjama
- Izvršite rutinsku inspekciju rezervnih kopija imovine
- Sprovodite *phishing* simulacije
- Sprovesti obuku za bezbednost korisnika
- Sprovoditi Response training- Trening za pravovremeni odgovor na prijetnju (PBC)

(I) Identifikacija

- 1.Nadgledajte za:

a. Usluge preslikavanja e-pošte koje skeniraju kopije e-poruka u potrazi za zlonamernim sadržajem
b. Obrasci saobraćaja i sadržaj paketa, posebno traženje neobične upotrebe protokola interno
c. Mrežni podaci za neuobičajene tokove podataka. Procesi korištenja mreže koji inače nemaju mrežnu komunikaciju ili nikada ranije nisu viđeni su sumnjivi

- Istražite i obrišite sva obavještenja povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Arhivirajte artefakte u vezi sa skeniranjem kao što su IP adrese, korisnički agenti i zahtjevi
- Utvrdite izvor i putanju napada
- Utvrđivanje kritičnih sredstava koja nisu pogođena

(E) Iskorjenjivanje/Uništavanje

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Poništite sve kompromitovane lozinke
- Provjerite sva sredstva i aktivnost korisnika za MOK u skladu sa profilom napada
- Provjerite rezervne kopije za MOK u skladu sa napadačkim profilom prije oporavka sistema
- Zakrpa ranjivosti sredstava

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Izvršite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novododate potpise prijetnji
- Izbjegavajte otvaranje e-pošte i priloga nepoznatih pošiljalaca
- Izbjegavajte otvaranje priloga e-pošte od pošiljalaca koji obično ne uključuju priloge
- Obratite pažnju na neobično ponašanje koje ispoljavaju stranke od povjerenja
- Ne zaboravite da podatke i događaje ne treba posmatrati u izolaciji već kao dio lanca ponašanja koji bi mogao da dovede do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Izviđanje – Prikupljanje informacija o identitetu žrtve

(P) Priprema

- Pečovanje ranjivosti aseta
- Obaviti rutinsku inspekciju i kontrolu
- Održavati apdejtovanje Antivirus/EDR aplikacija
- Kreirati segmentaciju mreže
- Praćenje logova mrežnog saobraćaja između mrežnih segmenata
- Uključiti obavještajnu prijetnju
- Obavljati rutinsku inspekciju i bekapovanja aseta
- Sprovoditi *phishing* simulacije
- Sprovoditi bezbjednosne treninge sa korisnicima
- Sprovoditi Response training- Trening za pravovremeni odgovor na prijetnju (PBC)
- Minimalizacija količine povjerljivih podataka koja je dostupna za eksterne partije

(I) Identifikacija

- Nadgledajte za:

a. Mrežni saobraćaj koji može da otkrije probing (proces ispitivanja ili testiranja sistema)
b. Analiza Web metadata artefakata kao što su korisnički agenti HTTPS/S polja

- Istražite i obrišite sve alertove povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Skeniranje relevantnih artefakata kao što su IP adrese, korisnički agenti i zahtjevi
- Otkrivanje izvora i puta napada
- Identifikovati neobuhvaćene kritične asete

(E) Uklanjanje

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Poništite sve kompromitovane lozinke
- Inspekcija svih aseta i aktivnosti korisnika za IOC sa profilom napada
- Inspekcija bekapa za IOC konzistentnosti sa profilom napada prije oporavka sistema
- Ažuriranje ranjivosti aseta

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Vratite pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Izvršite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novododate potpise prijetnji
- Izbjegavajte otvaranje e-pošte i priloga nepoznatih pošiljalaca
- Izbjegavajte otvaranje priloga e-pošte od pošiljalaca koji obično ne uključuju priloge
- Obratite pažnju na neobično ponašanje koje ispoljavaju stranke od povjerenja
- Ne zaboravite da podatke i događaje ne treba posmatrati u izolaciji već kao dio lanca ponašanja koji bi mogao da dovede do drugih aktivnosti

Reference: https://attack.mitre.org/techniques/T1589/

CSEC
Cyber Security Excellence Centre

Command and Control – Protokol aplikativnog sloja

(P) Priprema

- Pečovanje ranjivosti aseta
- Obaviti rutinsku inspekciju i kontrolu
- Održavati apdejtovanje Antivirus/EDR aplikacija
- Kreirati segmentaciju mreže
- Praćenje logova mrežnog saobraćaja između mrežnih segmenata
- Uključiti obavještajnu prijetnju
- Obavljati rutinsku inspekciju i bekapovanja aseta
- Sprovoditi *phishing* simulacije
- Sprovoditi bezbjednosne treninge sa korisnicima
- Sprovoditi Response training- Trening za pravovremeni odgovor na prijetnju (PBC)
- Implementacija signature-based mrežnih detekcija upada i preventivnih sistema

(I) Identifikacija

- Nadgledajte za:

a. Novoformirane mrežne konekcije koje su poslane ili primljene od nepoznatih hostova

b. Mrežni procesi koji nemaju normalnu mrežnu komunikaciju ili procesi koji nisu prije detektovani u mreži

- Istražite i obrišite sve alertove povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Skeniranje relevantnih artefakata kao što su IP adrese, korisnički agenti i zahtjevi
- Otkrivanje izvora i puta napada
- Identifikovati neobuhvaćene kritične asete

(E) Uklanjanje

- Zatvorite vektor napada primjenom gore navedenih koraka Pripreme(P)
- Izvršite skeniranje krajnjih tačaka/AV na pogođenim sistemima
- Poništite sve kompromitovane lozinke
- Inspekcija svih aseta i aktivnosti korisnika za IOC sa profilom napada
- Inspekcija bekapa za IOC konzistentnosti sa profilom napada prije oporavka sistema
- Ažuriranje ranjivosti aseta

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Obnoviti obuhvaćene sisteme do zadnjeg clean backupa

(L) Lekcije/Mogućnosti

- Izvršite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novododate potpise prijetnji
- Izbjegavajte otvaranje e-pošte i priloga nepoznatih pošiljalaca
- Izbjegavajte otvaranje priloga e-pošte od pošiljalaca koji obično ne uključuju priloge
- Obratite pažnju na neobično ponašanje koje ispoljavaju stranke od povjerenja
- Ne zaboravite da podatke i događaje ne treba posmatrati u izolaciji već kao dio lanca ponašanja koji bi mogao da dovede do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Reference: https://attack.mitre.org/techniques/T1071/ 2. https://attack.mitre.org/mitigations/M1031/ 3. https://attack.mitre.org/datasources/DS0029/

Istrajnost - Event trigerovana egzekucija

(P) Priprema

- Pečovanje ranjivosti aseta
- Obaviti rutinsku inspekciju i kontrolu
- Održavati apdejtovanje Antivirus/EDR aplikacija
- Kreirati segmentaciju mreže
- Praćenje logova mrežnog saobraćaja između mrežnih segmenata
- Uključiti obavještajnu prijetnju
- Obavljati rutinsku inspekciju i bekapovanja aseta
- Sprovoditi *phishing* simulacije
- Sprovoditi bezbjednosne treninge sa korisnicima
- Sprovoditi Response training- Trening za pravovremeni odgovor na prijetnju (PBC)

(I) Identifikacija

- Nadgledajte za:

a. Sumnjivu konfiguraciju na lokalalnom sistemu kao što su novi kreirani fajlovi ili WMI objekti, modifikovani ključevi ili neprepoznate DLL aktivnosti
b. Kreiranje i modifikovanje cloud-based funkcija i workflow-ova za monitoring servisa
c. Nestandardni protokoli i mrežni protok

- Istražite i obrišite sve alertove povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Izdajte ojačanje perimetra za poznate lokacije aktera prijetnji
- Skeniranje relevantnih artefakata kao što su IP adrese, korisnički agenti i zahtjevi
- Otkrivanje izvora i puta napada
- Identifikovati neobuhvaćene kritične asete

(E) Uklanjanje

- Zatvoriti vektor napada primjenjujući pripremne korake koji su označeni u pripremnoj fazi
- Provoditi skeniranje endpoint i anti virus uređaja na targetiranim sistemima
- Resetovanje svih kompromitovanih passworda
- Inspekcija svih aseta i aktivnosti korisnika za IOC sa profilom napada
- Analiza ranjivosti path aseta

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Obnoviti obuhvaćene sisteme do zadnjeg clean backupa

(L) Lekcije/Mogućnosti

- Izvršite rutinske mjere sajber higijene
- Angažujte eksterne pružitelje usluga sajber bezbjednosti i stručnjake za odgovor na incidente
- Sprovedite promjene politike radi smanjenja budućeg rizika
- Koristite novododate potpise prijetnji
- Izbjegavajte otvaranje e-pošte i priloga nepoznatih pošiljalaca
- Izbjegavajte otvaranje priloga e-pošte od pošiljalaca koji obično ne uključuju priloge
- Obratite pažnju na neobično ponašanje koje ispoljavaju stranke od povjerenja
- Ne zaboravite da podatke i događaje ne treba posmatrati u izolaciji već kao dio lanca ponašanja koji bi mogao da dovede do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Reference: https://attack.mitre.org/techniques/T1071/ 2. https://attack.mitre.org/mitigations/M1031/ 3. https://attack.mitre.org/datasources/DS0029/

Eskalacija privilegija – Boot i logon skripte

(P) Priprema

- Pečovanje ranjivosti aseta
- Obaviti rutinsku inspekciju i kontrolu
- Održavati apdejtovanje Antivirus/EDR aplikacija
- Kreirati segmentaciju mreže
- Praćenje logova mrežnog saobraćaja između mrežnih segmenata
- Uključiti obavještajnu prijetnju
- Obavljati rutinsku inspekciju i bekapovanja aseta
- Sprovoditi bezbjednosne treninge sa korisnicima
- Sprovoditi Response training- Trening za pravovremeni odgovor na prijetnju (PBC)
- Ograničiti pristup logon skiptama, pristup dati samo administratorima

(I) Identifikacija

- Nadgledajte za:

a. Neovlaštene promjene za aktivne direktorije startap skripti
b. Egzekucija logon skripti sa neobičnih naloga ili u neobično vrijeme
c. Novi fajlovi, skripte ili ključevi koji pokreću automatski boot up ili logon

- Istražite i obrišite sve alertove povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Ustanoviti perimetar za poznate lokacije prijetnji
- Skeniranje relevantnih artefakata kao što su IP adrese, korisnički agenti i zahtjevi
- Otkrivanje izvora i puta napada
- Zaštita nezaraženih kritičnih aseta

(E) Uklanjanje

- Zatvoriti vektor napada primjenjujući pripremne korake koji su označeni u pripremnoj fazi
- Provoditi skeniranje endpoint i anti virus uređaja na targetiranim sistemima
- Resetovanje svih kompromitovanih passworda
- Inspekcija svih aseta i aktivnosti korisnika za IOC sa profilom napada
- Analiza ranjivosti path aseta
- Ažurirajte ranjivosti aseta

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Obnoviti obuhvaćene sisteme do zadnjeg clean backupa

(L) Lekcije/Mogućnosti

- Redovno obavljanje provjere bezbjednosti i održavanje sajber higijene
- Uključiti eksterne stručnjake za odgovor na incidente i provajdere sajber bezbjednosti
- Implementirati promjene u polisama da se smanji budući rizik
- Primjeniti najnovije bezbjednosne potpise
- Ne zaboravite da podatke i događaje ne treba posmatrati u izolaciji već kao dio lanca ponašanja koji bi mogao da dovede do drugih aktivnosti

CSEC
Cyber Security Excellence Centre

Reference: https://attack.mitre.org/techniques/T1071/ 2. https://attack.mitre.org/mitigations/M1031/ 3. https://attack.mitre.org/datasources/DS0029/

Inicijalni pristup – Replikacija kroz prenosne medije

(P) Priprema

- Pečovanje ranjivosti aseta
- Obaviti rutinsku inspekciju i kontrolu
- Održavati apdejtovanje Antivirus/EDR aplikacija
- Kreirati segmentaciju mreže
- Praćenje logovi mrežnog saobraćaja između mrežnih segmenata
- Uključiti obavještajnu prijetnju
- Sprovoditi *phishing* simulacije
- Obavljati rutinsku inspekciju i bekapovanja aseta
- Sprovoditi bezbjednosne treninge sa korisnicima
- Sprovoditi trening kako pravovremeno reagovati (PBC)
- Uključiti Attack surface reduction pravila za blokiranje neprovjerenih/neovlaštenih egzekjutivnih fajlova
- Isključiti autoran ukoliko je nepotrebno

(I) Identifikacija

- Nadgledajte za:

a. Novokonstruisane *drive letters* ili *mount points* za prenosivu medije

b. Neočekivane ili novokonstruisane fajlove na prenosivim medijima

c. Egzekjutivne procese koji originalno potiču sa prenosivih medija

- Istražite i obrišite sve alertove povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Ustanoviti perimetar za poznate lokacije prijetnji
- Skeniranje relevantnih artefakata kao što su IP adrese, korisnički agenti i zahtjevi
- Otkrivanje izvora i puta napada
- Zaštita nezaraženih kritičnih aseta

(E) Uklanjanje

- Zatvoriti vektor napada primjenjujući pripremne korake koji su označeni u pripremnoj fazi
- Provoditi skeniranje endpoint i anti virus uređaja na targetiranim sistemima
- Resetovanje svih kompromitovanih passworda
- Inspekcija svih aseta i aktivnosti korisnika za IOC sa profilom napada
- Analiza ranjivosti path aseta
- Ažurirajte ranjivosti aseta

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Obnoviti obuhvaćene sisteme do zadnjeg clean backupa

(L) Lekcije/Mogućnosti

- Redovno obavljanje provjere bezbjednosti i održavanje sajber higijene
- Uključiti eksterne stručnjake za odgovor na incidente i provajdere sajber bezbjednosti
- Implementirati promjene u polisama da se smanji budući rizik
- Primjeniti najnovije bezbjednosne potpise
- Ograničiti korištenje USB uređaja i prenosivih uređaja u mrežnom sistemu

- References:

https://attack.mitre.org/datasources/DS0016/
https://attack.mitre.org/datasources/DS0022/
https://attack.mitre.org/datasources/DS0009/
https://attack.mitre.org/mitigations/M1040/
https://attack.mitre.org/mitigations/M1042/
https://attack.mitre.org/mitigations/M1034/

CSEC
Cyber Security Excellence Centre

Istrajanost – Raspoređeni task ili posao

(P) Priprema

- Pečovanje ranjivosti aseta // Obaviti rutinsku inspekciju i kontrolu
- Održavati apdejtovanje Antivirus/EDR aplikacija
- Kreirati segmentaciju mreže // Praćenje logovi mrežnog saobraćaja između mrežnih segmenata // Uključiti obavještajnu prijetnju
- Obavljati rutinsku inspekciju i bekapovanja aseta
- Konfigurisati podešavanja za zakazane taskove kako biste prisilili taskove da se izvode u kontekstu autentifikovanih računa umjesto da im se omogući pokretanje kao SISTEM.
- Ključ registra se nalazi: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl.
- The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled
- Konfigurišite opciju povećanje raspoređenog prioriteta da se dopusti samo administratorima da raspoređuju proiritetni proces. Ovo se može konfigurisati kroz: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority
- Sprovoditi bezbjednosne treninge sa korisnicima
- Sprovoditi trening kako pravovremeno reagovati (PBC)

(I) Identifikacija

- Pratite aktivnosti:

a. Izvršene naredbe i argumenti i novokonstruisani kontejneri koji mogu zloupotrijebiti funkciju funkciju planiranja zadatka kako bi olakšali ponavljajuće izvršenje malicioznog koda

b. Novokonstruisani fajlovi i promjene napravljene na fajlovima koje mogu zloupotrijebiti zadatak funkcionalnog planiranja kako bi se olakšalo početno ili ponavljajuće izvršenje zlonamjernog koda

- Istražiti i očistiti sve alertove povezane sa pogođenim asetima i nalozima
- Grupe prijetnji kao što su Eart Lusca poznate su po tome da uspostavljaju prisustvo i postojanost koristeći sledeću komandu schtasks /Create /SC ONLOgon/TN Windows UpdateCheck /TR "[filepath]"/ru
- Rutinski provjeravati firewall, IDS, IPS i SIEM logove za detekciju sumnjivih aktivnosti

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Ustanoviti perimetar za poznate lokacije prijetnji
- Skeniranje relevantnih artefakata kao što su IP adrese, korisnički agenti i zahtjevi
- Otkrivanje izvora i puta napada
- Zaštita nezaraženih kritičnih aseta

(E) Uklanjanje

- Zatvoriti vektor napada primjenjujući pripremne korake koji su označeni u pripremnoj fazi
- Provoditi skeniranje endpoint i anti virus uređaja na targetiranim sistemima
- Resetovanje svih kompromitovanih passworda
- Inspekcija svih aseta i aktivnosti korisnika za IOC sa profilom napada
- Ažurirajte ranjivosti aseta

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Obnoviti obuhvaćene sisteme do zadnjeg clean backupa

(L) Lekcije/Mogućnosti

- Redovno obavljanje provjere bezbjednosti i održavanje sajber higijene
- Uključiti eksterne stručnjake za odgovor na incidente i provajdere sajber bezbjednosti
- Implementirati promjene u polisama da se smanji budući rizik
- Primjeniti najnovije bezbjednosne potpise
- Upamtiti da podatke i događaje ne treba posmatrati izolovano već kao dio lanca ponašanja koji bi mogao dovesti do drugih aktivnosti
- Kompleti alata poput okvira Powersploit sadrže powerup module koji se mogu koristiti istražiti sisteme za nedostatak dozvola u planiranim zadacima koji bi mogli koristiti za eskalaciju privilegija
- References:
- https://attack.mitre.org/datasources/DS0017/
- https://attack.mitre.org/datasources/DS0032/
- https://attack.mitre.org/mitigations/M1047/
- https://attack.mitre.org/mitigations/M1028/
- https://attack.mitre.org/mitigations/M1026/
- https://attack.mitre.org/groups/G1006/

CSEC
Cyber Security
Excellence Centre

Pristup kredencijalima – Sniffing mreža

(P) Priprema

- Pečovanje ranjivosti aseta
- Obaviti rutinsku inspekciju i kontrolu
- Održavati apdejtovanje Antivirus/EDR aplikacija
- Kreirati segmentaciju mreže
- Praćenje logovi mrežnog saobraćaja između mrežnih segmenata
- Uključiti obavještajnu prijetnju
- Obavljati rutinsku inspekciju i backup aseta
- Sprovoditi bezbjednosne treninge sa korisnicima
- Sprovoditi trening kako pravovremeno reagovati (PBC)
- Osigurati da sav mrežni (žičani i wireles) saobraćaj je pravilno enkriptovan. Koristiti najbolje prakse za protokole o autentifikaciju, kao što je Kerberos i osigurajte da je mrežni saobraćaj koji koristi kredencijale je zaštićen od SSL/TLS
- Koristiti multi faktor autentifikaciju kad god je moguće
- U korištenju cloud okruženja, osigurajte da se korisnicima ne dodijele dozvole za kreiranje i modifikovanje ogledala mrežnog saobraćaja osim ako to nije izričito potrebno

(I) Identifikacija

- Nadgledajte za:

a. Izvršene komande i argumenti za akcije koje pomažu u sniffing-u mrežnog saobraćaja za hvatanje informacija u okruženju, uključujući autentifikovani materijal proslijeđen mrežom
b. Novoizvršeni procesi koji mogu pomoći u sniffing-u mrežnog saobraćaja radi hvatanja infirmacija o mrežnom okruženju, uključujući autentifikacioni materijal proslijeđen mrežom

- Istražite i obrišite sve alertove povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Ustanoviti perimetar za poznate lokacije prijetnji
- Skeniranje relevantnih artefakata kao što su IP adrese, korisnički agenti i zahtjevi
- Otkrivanje izvora i puta napada
- Zaštita nezaraženih kritičnih aseta

(E) Uklanjanje

- Zatvoriti vektor napada primjenjujući pripremne korake koji su označeni u pripremnoj fazi
- Provoditi skeniranje endpoint i anti virus uređaja na targetiranim sistemima
- Resetovanje svih kompromitovanih passworda
- Inspekcija svih aseta i aktivnosti korisnika za IOC sa profilom napada
- Inspekcija svih aktivnosti aseta i korisnika za IOC sa profilom napadača
- Ažurirajte ranjivosti aseta

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Obnoviti obuhvaćene sisteme do zadnjeg clean backupa

(L) Lekcije/Mogućnosti

- Redovno obavljanje provjere bezbjednosti i održavanje sajber higijene
- Uključiti eksterne stručnjake za odgovor na incidente i provajdere sajber bezbjednosti
- Implementirati promjene u polisama da se smanji budući rizik
- Primjeniti najnovije bezbjednosne potpise
- Upamtiti da podatke i događaje ne treba posmatrati izolovano već kao dio lanca ponašanja koji bi mogao dovesti do drugih aktivnosti

- https://attack.mitre.org/mitigations/M1041/
- https://attack.mitre.org/mitigations/M1032/
- https://attack.mitre.org/mitigations/M1018/
- https://attack.mitre.org/datasources/DS0017/
- https://attack.mitre.org/datasources/DS0009/

CSEC
Cyber Security Excellence Centre

Command and Control – Komunikacija kroz prenosive medije

(P) Priprema

- Pečovanje ranjivosti aseta
- Obaviti rutinsku inspekciju i kontrolu
- Održavati apdejtovanje Antivirus/EDR aplikacija
- Kreirati segmentaciju mreže
- Praćenje logova mrežnog saobraćaja između mrežnih segmenata
- Uključiti obavještajnu prijetnju
- Obavljati rutinsku inspekciju i backup aseta
- Sprovoditi bezbjednosne treninge sa korisnicima - Security awareness
- Sprovoditi trening kako pravovremeno reagovati (PBC)
- Isključiti autoran ukoliko je potrebno
- Podesiti polise za ograničenje korištenja prenosivih medija na organizacionom nivou

(I) Identifikacija

- Nadgledajte za:

a. Neočekivan pristup fajlovima na prenosivim medijima
b. Novoizvršeni procesi kad su prenovi mediji montirani

- Istražite i obrišite sve alertove povezana sa pogođenim sredstvima ili računima
- Rutinski provjerite evidencije zaštitnog zida, IDS-a, IPS-a i SIEM-a za bilo koju neobičnu aktivnost

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Ustanoviti perimetar za poznate lokacije prijetnji
- Skeniranje relevantnih artefakata kao što su IP adrese, korisnički agenti i zahtjevi
- Otkrivanje izvora i puta napada
- Zaštita nezaraženih kritičnih aseta
- Isključiti pristup internetu ako je aset pod sumnjom C2 komunikacije

(E) Uklanjanje

- Zatvoriti vektor napada primjenjujući pripremne korake koji su označeni gore u pripremnoj fazi
- Provoditi skeniranje endpoint i anti virus uređaja na targetiranim sistemima
- Resetovanje svih kompromitovanih passworda
- Inspekcija svih aseta i aktivnosti korisnika za IOC sa profilom napada
- Inspekcija svih aktivnosti aseta i korisnika za IOC sa profilom napadača
- Ažurirati ranjivosti aseta

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Adresirajte eventualnu kolateralnu štetu pregledom i procjenom izloženih tehnologija
- Riješite sve povezane bezbjednosne incidente
- Obnoviti obuhvaćene sisteme do zadnjeg clean backupa

(L) Lekcije/Mogućnosti

- Redovno obavljanje provjere bezbjednosti i održavanje sajber higijene
- Uključiti eksterne stručnjake za odgovor na incidente i provajdere sajber bezbjednosti
- Implementirati promjene u polisama da se smanji budući rizik
- Primjeniti najnovije bezbjednosne potpise
- Upamtiti da podatke i događaje ne treba posmatrati izolovano već kao dio lanca ponašanja koji bi mogao dovesti do drugih aktivnosti

- References:
- https://attack.mitre.org/techniques/T1092/
- https://attack.mitre.org/mitigations/M1042/
- https://attack.mitre.org/mitigations/M1028/
- https://attack.mitre.org/datasources/DS0016/#Drive%20Access
- https://attack.mitre.org/datasources/DS0016/#Drive%20Creation

CSEC
Cyber Security Excellence Centre

Device Theft – Device Loss

(P) Priprema

- Ažurirati ranjivosti aseta
- Izvršiti redovne inspekcije kontrole/oružja
- Održavati ažurnu evidenciju elektronskih uređaja
- Postaviti tagove na asete u vlasništvu kompanije
- Koristiti enkripciju celokupnog diska
- Postaviti pravila za lozinke/pin kodove na uređajima
- Održavati mogućnost daljinskog brisanja podataka sa uređaja
- Biti upoznat sa zakonima ili ugovornim obavezama koje zahtevaju obaveštenje o gubitku podataka

(I) Identifikacija

- Nadgledajte za:

a. Prijava zaposlenih o krađi/gubitku uređaja

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Utvrditi:

a. Koji podaci su bili sačuvani na uređaju
b. Kako su podaci na uređaju zaštićeni
c. Koji udaljeni podaci i usluge su dostupni sa uređaja

- Promeniti lozinke svih naloga koji su korišćeni na uređaju
- Pregledati logove o neovlaštenoj aktivnosti sa ukradenog/izgubljenog uređaja ili naloga koji su sa njim povezani
- Primjeniti mjere zaštite perimetra za poznate lokacije sa kojih dolaze pretnje

(E) Uklanjanje

- Izvršiti daljinsko brisanje podataka/sistema sa uređaja

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Obavijestiti treću stranu o gubitku podataka ako to u skladu sa pravilima
- Obavijestiti nadležne organe ukoliko je to u skladu sa pravilima
- Obratiti pažnju / Riješiti eventualnu kolateralnu štetu

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Mitigation M1027: https://attack.mitre.org/mitigations/M1027/
- MITRE ATT&CK Mitigation M1041: https://attack.mitre.org/mitigations/M1041/

CSEC
Cyber Security Excellence Centre

Initial Access – Drive By Compromise

(P) Priprema

- Redovno ažurirati pretraživače i ostale softvere
- Izvršiti redovne inspekcije kontrole/oružja
- Osigurati da je Antivirusni / Endpoint Protection softver instaliran na svim radnim stanicama
- Osigurati da su radne stanice spojene sa centralnom lokacijom i da beleže logove
- Evidentirati mrežni saobraćaj
- Postaviti proksi za web saobraćaj
- Koristiti Group Policy za upravljanje sigurnosnim postavkama pretraživača
- Staviti u upotrebu Windows Defender Exploit Guard ili druge alate za ublažavanje ranjivosti i eksploatacije

(I) Identifikacija

- Pratiti aktivnosti:

a. Neuobičajene DNS aktivnosti
b. Upozorenja Antivirusnog/Endpoint softvera
c. Upozorenja IDS/IPS sistema
d. Prijava korisnika o neočekivanom ponašanju uređaja

- Istražiti i otklonite sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Primijeniti mjere zaštite perimetra za poznate lokacije sa kojih dolaze pretnje
- Sistemi za koje se vjeruju da su kompromitovani ukloniti sa mreže

(E) Uklanjanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Ažurirati ranjivosti aseta
- Izvršiti antivirusna skeniranja pogođenog sistema
- Pregledati logove i mrežni saobraćaj kako biste identifikovali svaku povezanu zlonamjernu aktivnost

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Obratiti pažnju / Riješite eventualnu kolateralnu štetu
- Reset lozinke svih naloga koji se koriste na kompromitovanom sistemu
- Riješiti povezane sigurnosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1189: https://attack.mitre.org/techniques/T1189/

CSEC
Cyber Security Excellence Centre

Initial Access – External Remote Services – Unauthorised VPN and VDI Access

(P) Priprema

- Redovno ažurirati pretraživače i ostale softvere
- Izvršiti redovne inspekcije kontrole/oružja
- Osigurati da je Antivirusni / Endpoint Protection softver instaliran na svim radnim stanicama
- Onemogućiti pristup kompanijskim uređajima osobama koje nisu zaposlene u kompaniji
- Osigurati da su radne stanice spojene sa centralnom lokacijom i da beleže logove
- Omogućiti obuke o sajber bezbednosti za zaposlene
- Koristiti višestruku autentifikaciju gde god je to moguće
- Osigurti da se uvedu odgovarajuća pravila za firewall za udaljene korisnike i odradi odgovarajuća segmentacija mreže
- Redovno proveravati pristup udaljenim sistemima

(I) Identifikacija

- Pratiti aktivnosti:

a. Udaljeni pristup tokom neuobičajenih sati/dana
b. Udaljeni pristup sa neuobičajenih izvora (npr. geografskih lokacija, IP adresa)
c. Prekomjerne neuspjele pokušaje prijave
d. Upozorenja IDS/IPS sistema
e. Upozorenja Antivirusnog/Endpoint sistema

- Istražiti i otklonite sva upozorenja povezana sa pogođenim resursima
- Kontaktirati korisnika na drugi način kako biste utvrdili verodostojnost uočene aktivnosti

(Z) Obuzdavanje/Kontrola

- Inventar (popišite i procijenite)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Prevara| Uništavanje
- Posmatrajte -> Orijentišite se -> Odlučite -> Djelujte
- Primijeniti mjere zaštite perimetra za poznate lokacije sa kojih dolaze pretnje
- Blokirati pristup sistemima od strane kompromitovanog korisnika
- Zaključati naloge povezane sa kompromitovanim korisnikom
- Inspekcija svih potencijalno kompromitovanih sistema u potrazi za indikatorima kompromitacije (IOC - Indikator kompromitacije)

(E) Uklanjanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Ažurirati ranjivosti aseta
- Izvršiti antivirusna skeniranja pogođenog sistema
- Pregledati logove i mrežni saobraćaj kako biste identifikovali svaku povezanu zlonamjernu aktivnost

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Obratiti pažnju / Riješite eventualnu kolateralnu štetu
- Riješiti povezane sigurnosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1133: https://attack.mitre.org/techniques/T1133/

CSEC
Cyber Security Excellence Centre

Impact - Defacement

(P) Priprema

- Ažurirati ranjivosti aseta
- Izvršiti redovne inspekcije kontrole/oružja
- Osigurati da su radne stanice spojene sa centralnom lokacijom i da bilježe logove
- Provjeriti da li serveri vrše redovan backup

(I) Identifikacija

- Pratiti aktivnosti:

a. Nepredviđene promjene na web sajtovima
b. Neuobičajene poruke o greškama u logovima
c. Neuobičajeni uzorci mrežnog saobraćaja
d. Upozorenja IDS/IPS sistema
e. Upozorenje antivirusnih programa

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Privremeno ukloniti oštećenu web stranicu
- Sprovesti primjenu perimetarskih mijera za poznate lokacije prijetnji

(E) Uklanjanje

- Pregledati logove kako biste utvrdili uzrok narušavanja bezbjednosti
- Izvršiti antivirusna skeniranja na pogođenim sistemima
- Pregledati web servere i druge sisteme radi pronalaženja dokaza o postojanju backdoor pristupa ili lateralnog kretanja
- Verifikovati integritet svih podataka kojima su napadači imali pristup
- Resetovati sve potencijalno kompromitovane lozinke
- Ažurirati ranjivosti aseta

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Obratiti pažnju / Riješite eventualnu kolateralnu štetu
- Riješiti povezane sigurnosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1491: https://attack.mitre.org/techniques/T1491

CSEC
Cyber Security Excellence Centre

Impact – Inhibit System Recovery – Disabling Volume Shadow Service

(P) Priprema

- Ažurirati ranjivosti aseta
- Izvršiti redovne inspekcije kontrole/oružja
- Osigurati da su radne stanice spojene sa centralnom lokacijom i da bilježe logove
- Osigurati da je Antivirusni / Endpoint Protection softver instaliran na svim radnim stanicama
- Proveriti da li se važni podaci redovno rade backup
- Osigurati da se nalozi sa administrativnim privilegijama koriste samo kada je to neophodno

(I) Identifikacija

- Pratiti aktivnosti:

a. Upozorenja Antivirusnog/Endpoint sistema
b. Logove vezane za promene ili onemogućavanje servisa za oporavak sistema

- Istražiti i otkloniti sva upozorenja povezana

sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Ukloniti sa mreže sisteme za koje se veruje da su kompromitovani

(E) Uklanjanje

- Izvršiti skeniranje antivirusnim programima na pogođenim sistemima
- Pregledati logove kako biste utvrdili uzrok otkrivene aktivnosti
- Utvrditi da li su kompromitovani i drugi sistemi ili korisnički nalozi
- Provjeriti izmjenjene i obrisane fajlove na sistemu i dijeljenim mrežnim resursima
- Resetovati sve potencijalno kompromitovane lozinke
- Ažurirati ranjivosti aseta

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Obratiti pažnju / Riješite eventualnu kolateralnu štetu
- Utvrditi osnovni uzrok probijanja sigurnosnih mijera
- Riješiti povezane sigurnosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1490:

https://attack.mitre.org/techniques/T1490/

CSEC
Cyber Security Excellence Centre

Defense Evasion – Disabling Security Software

(P) Priprema

- Ažurirati ranjivosti aseta
- Izvršiti redovne inspekcije kontrole/oružja
- Osigurati da su radne stanice spojene sa centralnom lokacijom i da bilježe logove
- Osigurati da je Antivirusni / Endpoint Protection softver instaliran na svim radnim stanicama
- Osigurati da su serveri spojeni sa centralnom lokacijom i da bilježe logove
- Provjeriti da redovni korisnici nemaju prekomjerne permisije

(I) Identifikacija

- Pratiti aktivnosti:

a. Neuobičajene DNS aktivnosti
b. Upozorenja Antivirusnog/Endpoint softvera
c. Upozorenja IDS/IPS sistema
d. Neuobičajno odsustvo logova iz sigurnosnog softvera

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Primijeniti mjere zaštite perimetra za poznate lokacije sa kojih dolaze prijetnje
- Ukloniti sisteme za koje se vjeruje da su kompromitovani sa mreže

(E) Uklanjanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Ažurirati ranjivosti aseta
- Izvršiti skeniranje antivirusnim programima na pogođenim sistemima
- Pregledati logove kako biste utvrdili da li je još neki sistem zaražen

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Obratiti pažnju / Riješite eventualnu kolateralnu štetu
- Utvrditi osnovni uzrok probijanja sigurnosnih mijera
- Riješiti povezane sigurnosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1562 Sub-technique 001: https://attack.mitre.org/techniques/T1562/001/

CSEC
Cyber Security Excellence Centre

Defense Evasion – Install Root Certificate

(P) Priprema

- Ažurirati ranjivosti aseta
- Izvršiti redovne inspekcije kontrole/oružja
- Osigurati da su radne stanice spojene sa centralnom lokacijom i da bilježe logove
- Osigurati da je Antivirusni / Endpoint Protection softver instaliran na svim radnim stanicama
- Održavati listu poznatih ispravnih root certifikata
- Provjeriti prethodno instalirane root certifikate na novim uređajima

(I) Identifikacija

- Pratiti aktivnosti:

a. Neuobičajene DNS aktivnosti
b. Upozorenja Antivirusnog/Endpoint softvera
c. Upozorenja IDS/IPS sistema
d. Neuobičajno odsustvo logova iz sigurnosnog softvera

- Periodično provjeriti root certifikate na uređajima i utvrditi da li su se desile promjene
- Istražiti i otkloniti sva upozorenja povezana sa pogođenim asetima

(Z) Obuzdavanje/Kontrola

- Evidentirati (popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Sisteme za koje se vjeruje da su kompromitovani ukloniti sa mreže
- Provjeriti prisustvo root certifikata na ostalim sistemima

(E) Uklanjanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Ažurirati ranjivosti aseta
- Identifikovati porijeklo potencijalno zlonamjernog root certifikata
- Izvršiti skeniranje antivirusnim programima na pogođenim sistemima

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Obratiti pažnju / Riješite eventualnu kolateralnu štetu
- Utvrditi osnovni uzrok probijanja sigurnosnih mijera
- Riješiti povezane sigurnosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1553 Sub-technique 004: https://attack.mitre.org/techniques/T1553/004/

CSEC
Cyber Security Excellence Centre

Credential Access - Password Spraying

(P) Priprema

- Ažurirati ranjivosti aseta
- Izvršiti redovne inspekcije kontrole/oružja
- Osigurati da su radne stanice spojene sa centralnom lokacijom i da bilježe logove
- Osigurati da je Antivirusni / Endpoint Protection softver instaliran na svim radnim stanicama
- Podesiti segmentaciju mreže i firewall-ove da ograničite pristup sistemima i uslugama
- Koristiti višestruku autentifikaciju gde god je to moguće
- Uspostaviti i sprovesti politiku sigurnosti lozinki

(I) Identifikacija

- Pratiti aktivnosti:

a. Neuspjeli pokušaji prijave za podrazumijevana i česta korisnička imena
b. Neuspjeli pokušaji prijave za isti nalog na više sistema
c. Neuspjeli pokušaji prijave na više sistema sa istog izvora

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim asetima

(Z) Obuzdavanje/Kontrola

- Evidentirati (popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Sisteme za koje se vjeruje da su kompromitovani ukloniti sa mreže
- Pregledati logove da biste utvrdili da li je napadač uspješno prijavljen na bilo koji nalog
- Zaključati sve kompromitovane naloge
- Primeniti mere zaštite perimetra za poznate lokacije sa kojih dolaze pretnje

(E) Uklanjanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Resetovati pristupne podatke za sve kompromitovane naloge
- Pregledati sve potencijalno kompromitovane asete

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Obratiti pažnju / Riješite eventualnu kolateralnu štetu
- Riješiti povezane sigurnosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1110 Sub-technique 003: https://attack.mitre.org/techniques/T1110/003/
- NIST Digital Identity Guidelines: https://pages.nist.gov/800-63- 3/sp800-63-3.html
- Microsoft Password Guidance: Microsoft_Password_Guidance-1.pdf

CSEC
Cyber Security Excellence Centre

Collection – Email Collection – Cloud Email Compromise

(P) Priprema

- Osigurati da je klijentski softver potpuno ažuriran
- Izvršiti redovne inspekcije kontrole/oružja
- Potvrditi da su logovi i upozorenja omogućeni i konfigurisani
- Koristiti pravila pristupa na osnovu rizika
- Redovno obučavati i testirati zaposlene za prepoznavanje *phishing* napada
- Upoznati se sa sigurnosnim mogućnostima koje su vam na raspolaganju u okviru vaše kompanije
- Redovno generisati izvještaje o prijavljivanju i vršiti njihov pregled
- Zabraniti upotrebu lozinki koje sadrže ime vaše kompanije ili imena proizvoda ako je to moguće
- Koristiti usluge treće strane za nadzor nad curenjem podataka

(I) Identifikacija

- Pratiti aktivnosti:

a. Neuobičajene aktivnosti prijavljivanja
b. Promjene pravila o prosljeđivanju email-ova
c. Onemogućavanje sigurnosnih funkcija

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Pregledati logove kako biste utvrdili da li je napadač uspješno pristupio drugim nalozima
- Zaključati sve kompromitovane naloge
- Primijeniti mjere zaštite perimetra za poznate lokacije sa kojih dolaze prijetnje

(E) Uklanjanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Resetovati pristupne podatke za sve kompromitovane naloge
- Pregledati sve potencijalno kompromitovane asete

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Obratiti pažnju / Riješite eventualnu kolateralnu štetu
- Riješiti povezane sigurnosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1114:

https://attack.mitre.org/techniques/T1114/

CSEC
Cyber Security Excellence Centre

Persistence - BITS Jobs

(P) Priprema

- Ažurirati ranjivosti aseta
- Izvršiti redovne inspekcije kontrole/oružja
- Osigurati da je Antivirusni / Endpoint
- Protection softver instaliran na svim radnim stanicama
- Osigurati da su radne stanice spojene sa centralnom lokacijom i da bilježe logove
- Bilježiti mrežni saobraćaj

(I) Identifikacija

- Pratiti aktivnosti:

a. Neuobičajene DNS aktivnosti
b. Upozorenja Antivirusnog/Endpoint softvera
c. Upozorenja IDS sistema
d. Iniciranje novih BITS radnji

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Primijeniti mjere zaštite perimetra za poznate lokacije sa kojih dolaze prijetnje
- Pregledati sumnjive BITS radnje
- Zaključati sve potencijalno kompromitovane naloge
- Sistemi za koje se sumnja da imaju malware ukloniti sa mreže

(E) Uklanjanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Ažurirati ranjivosti aseta
- Izvršiti skeniranje antivirusnim programima na pogođenim sistemima
- Pregledati logove da biste utvrdili da li su drugi sistemi pogođeni
- Provjeriti da li postoji još procesa koji se pokreću iznova i ukloniti ih

(O) Oporavak

- Vratite se na tačku oporavka (RPO – Recovery Point Objective) unutar vremena za oporavak (RTO – Recovery Time Objective)
- Obratiti pažnju / Riješite eventualnu kolateralnu štetu
- Istražiti kako su BITS procesi kreirani
- Riješiti povezane sigurnosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1197:

https://attack.mitre.org/techniques/T1197/

CSEC
Cyber Security Excellence Centre

Persistence – Pre-OS Boot

(P) Priprema

- Ažurirati ranjivosti aseta
- Izvršiti redovne inspekcije kontrole/oružja
- Osigurati da je Antivirusni / Endpoint Protection softver instaliran na svim radnim stanicama
- Osigurati da su radne stanice spojene sa centralnom lokacijom i da bilježe logove
- Postaviti BIOS ili UEFI lozinke na relevantne resurse
- Koristiti TPM tehnologiju i pouzdan boot proces
- Osigurati lokalne administratorske naloge
- Evidentirati sve promjene na boot zapisima, BIOS-u i EFI-ju
- Napraviti rezervne kopije particije bootloadera

(I) Identifikacija

- Pratiti aktivnosti:

a. Sumnjive promjene na boot fajlovima
b. Neuobičajene DNS aktivnosti
c. Upozorenja Antivirusnog/Endpoint softvera
d. Upozorenja IDS/IPS sistema

- Odraditi provjeru boot fajlova, konfiguracionih fajlova i firmware fajlove sa verifikovanim ispravnim fajlovima
- Odraditi provjeru integriteta za pre-OS boot mehanizme
- Koristiti provjere diska, forenzičke alate i podatke iz drajvera uređaja kako biste identifikovali nepravilnosti
- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Primijeniti mjere zaštite perimetra za poznate lokacije sa kojih dolaze prijetnje
- Ukloniti pogođeni sistem sa mreže
- Provjeriti integritet boot fajlova na svim asetima koji su rizični
- Provjeriti mrežne logove radi sumnjivog izlaznog saobraćaja

(E) Uklanjanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Ažurirati ranjivosti aseta
- Kreirati forenzičke rezervne kopije pogođenih sistema
- Zamijeniti firmware i boot fajlove iz rezervnih kopija ili pouzdanih izvora
- Izvršiti skeniranje antivirusnim programima na pogođenim sistemima

(O) Oporavak

- Vratiti se na tačku oporavka RPO unutar vremenskog okvira oporavka RTO
- Obratiti pažnju / Riješiti eventualnu kolateralnu štetu
- Otkriti korijen problema, nastanka incidenta
- Riješiti povezane sigurnosne incidente
- Vratiti pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1542: https://attack.mitre.org/techniques/T1542/

CSEC
Cyber Security Excellence Centre

Privilege Escalation – Group Policy Modification

(P) Priprema

- Ažurirati ranjivosti aseta
- Izvršiti redovne inspekcije kontrole/oružja
- Osigurati da su radne stanice spojene sa centralnom lokacijom i da bilježe logove
- Periodično provjeravati dozvole za Group Policy Object (GPO) putem revizije
- Koristiti WMI i filtriranje sigurnosnih grupa kako biste ograničili na koje sisteme i korisnike će se primjenjivati GPO-ovi

(I) Identifikacija

- Pratiti aktivnosti:

a. Neuobičajene DNS aktivnosti
b. Upozorenja Antivirusnog/Endpoint softvera
c. Upozorenja IDS/IPS sistema
d. Kreiranje, brisanje ili izmjena GPO-a
e. Kreiranje zakazanih zadataka i servisa

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Primijeniti mjere zaštite perimetra za poznate lokacije sa kojih dolaze prijetnje
- Ukloniti pogođeni sistem sa mreže
- Provjeriti integritet boot fajlova na svim asetima koji su rizični
- Provjeriti mrežne logove radi sumnjivog izlaznog saobraćaja

(E) Uklanjanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Ažurirati ranjivosti aseta
- Kreirati forenzičke rezervne kopije pogođenih sistema
- Izvršiti skeniranje antivirusnim programima na pogođenim sistemima
- Odraditi reviziju Group Policy pravila i permisija

(O) Oporavak

- Vratiti se na tačku oporavka RPO unutar vremenskog okvira oporavka RTO
- Obratiti pažnju / Riješiti eventualnu kolateralnu štetu
- Otkriti korijen problema, nastanka incidenta
- Riješiti povezane sigurnosne incidente
- Vratiti pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1484 Sub- technique 001: https://attack.mitre.org/techniques/T1484/001/

CSEC
Cyber Security Excellence Centre

Uticaj - Podaci enkriptovani za uticaj - Ransomware

(P) Priprema

- Ispraviti ranjivosti aseta
- Izvršiti redovne inspekcije kontrola/oružja
- Potvrditi da su rezervne kopije bez zlonamjernog softvera
- Uspostaviti mogućnost plaćanja otkupnina sa kriptovalutom
- Prikupiti ključeve za dešifrovanje različitih varijanti ransomware-a
- Potvrditi pokriće osiguranja za sajber bezbjednost
- Sprovesti simulacije ransomware napada
- Sprovesti simulacije *phishing* napada
- Sprovesti obuku korisnika o bezbjednosti
- Sprovesti obuku za odgovor u slučaju napada (PBC)
- Pregledati dijeljenje fajlova radi otkrivanja labavih/otvorenih privilegija
- Održavati ažuriranja antivirusnog/EDR softvera
- Kreirati segmentaciju mreže
- Logovati saobraćaj između segmenata mreže
- Uključiti obavještajne informacije o prijetnjama
- Uključiti tehnologiju obmane
- Izvršiti redovne inspekcije rezervnih kopija aseta
- Potvrditi ispravno funkcionisanje

(I) Identifikacija

- Pratiti:

a. Poruke/obaveštenja o ransomware-u
b. Neobične ekstenzije fajlova ili zlonamjerne ekstenzije
c. Prijave korisnika o oštećenim ili nečitljivim fajlovima
d. E-mejlove sa sumnjivim prilozima
e. Neobičan DNS saobraćaj
f. Brzo preimenovanje fajlova
g. Skokovi u korištenju CPU-a na sistemima za dijeljenje fajlova
h. Neobični izvršni binarni fajlovi
i. Anomalne mrežne veze na računarima
j. Odbijanja firewall-a na poznatim portovima za dijeljenje fajlova
k. Mrežne veze ka poznatim C2 (Command and Control) i eksploit kit lokacijama
l. Korišćenje TOR ili I2P mreže

- 2. Istražiti i ukloniti SVA upozorenja mogućeg ransomware-a:

a. IDS/IPS (sistem za otkrivanje i sprečavanje napada)
b. Antivirusni/EDR softver
c. Obavještajne informacije o pretnjama
d. Tehnologija obmane

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Locirati i izolovati asete odgovorne za enkripciju fajlova
- Izolovati pogođene sisteme za dijeljenje fajlova
- Zatvoriti vektor napada
- Ojačati sisteme za dijeljenje fajlova koji nisu pogođeni
- Ojačati kritične resurse koji nisu pogođeni
- Uspostaviti kontrolu pristupa za poznate lokacije prijetnji
- Implementirati EDR (Endpoint Detection and Response) agente za otkrivanje i uklanjanje štetnih procesa

(E) Iskorjenjivanje/Uništavanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Ažurirati ranjivosti aseta
- Ponovno kreirati pogođene resurse
- Inspekcija svih aseta u potrazi za IOC (Indicators of Compromise) koji su u skladu s profilom napada
- Pregled korisničke aktivnosti u potrazi za IOC koji su u skladu s profilom napada
- Pregled rezervnih kopija u potrazi za IOC koji su PRIOR za oporavka sistema
- Implementirati novo dobijene potpise prijetnji

(O) Oporavak

- Vratiti se na tačku oporavka RPO unutar vremenskog okvira oporavka RTO
- Obratiti pažnju / Riješiti eventualnu kolateralnu štetu
- Riješiti povezane sigurnosne incidente
- Vratiti pogođene sisteme na njihovu posljednju čistu rezervnu kopiju

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost
- Izbjegavati otvaranje e-mejlova i priloga od nepoznatih pošiljalaca
- Izbjegavati otvaranje e-mejl priloga od pošiljaoca koji obično ne šalju priloge

- Reference:
- MITRE ATT&CK Technique T1486: https://attack.mitre.org/techniques/T1486/
- Plaćanje otkupnina se ne preporučuje, ali trebalo bi biti dostupno kao mogućnost za izvršne direktore u slučaju potrebe (vidjeti Priprema #4 i #6).

CSEC
Cyber Security Excellence Centre

Početni pristup - Iskorištavanje resursa preduzeća - Napadi na SIM kartice mobilnih uređaja

(P) Priprema

- Dajte prednost korištenju aplikacija za autentifikaciju umjesto SMS poruka
- Kreirajte snažan PIN ili lozinku za nalog
- Koristite poseban broj za račune visoke vrijednosti

a. Alternativa: Koristite besplatan Google Voice broj

- Koristite menadžer lozinki
- Nikada ne čuvajte lozinke, metode plaćanja itd. u pregledaču na telefonu
- Pripremite rezervne komunikacijske mogućnosti kako biste brže reagovali na kompromis

a. Hangouts, GVoice, Skype, Line itd.

- Sprovodite obuku korisnika o svesti o bezbjednosti
- Sprovodite obuku za reagovanje na incidente (PBC)

(I) Identifikacija

- Pratiti:

a. Neobjašnjiv, dugotrajan gubitak mobilne usluge
b. Neočekivani pozivi korisničke službe koji kažu: "Žao nam je, izgubili smo vezu..."
c. Upozorenja o promjenama lozinke/autentifikacije na vašim nalozima
d. Upozorenja na vašem telefonu da li pokušavate da se prijavite sa adrese <Grad>, <Država>?

(Z) Obuzdavanje/Kontrola

- Odmah obavijestite svog mobilnog operatera
- Objasnite situaciju:

a. "Ja sam osoba od visoke vrijednosti i moj broj telefona je prebačen na novu SIM karticu prije otprilike 3 sata, kojom ja ne upravljam..."

- Zatražite da se broj potpuno onemogući:

a. "Pošto je ovo aktuelna situacija, molim vas da odmah uklonite moj broj telefona sa te SIM kartice, što znači da niko ne može primati pozive ili poruke na moj broj..."

- Zatražite da se vaš broj vrati na vašu SIM karticu:

a. Ovo može biti teže nego onemogućavanje broja

- Zabilježite ime/broj zaposlenog i datume
- Zabilježite sve brojeve slučaja ili podrške
- Zatražite da se sačuvaju svi zapisi o vašem IMEI broju
- Promijenite sve lozinke sa pouzdanog uređaja koji nije kompromitovan:
- a. Prvo promijenite lozinke za važnije e-mail naloge
- b. Prioritet: od najvrijednijeg do najmanje vrijednog.
- c. Dokumentujte vaše radnje kako ih sprovodite, uključujući vreme i snimke ekrana

(E) Iskorjenjivanje/Uništavanje

- Zatražite od svog mobilnog operatera da blokira sve pokušaje zamijene SIM kartica tokom jedne nedjelje
- Pogledajte dodatne korake u "Obuzdavanje/Kontaminiranje".

(O) Oporavak

- Zadržite pravnu pomoć i savjetovanje
- Kontaktirajte odgovarajuće agencije za sprovođenje zakona
- Kontaktirajte pogođene poslovne partnere

a. Pratite savjete svog pravnog savjetnika

- Angažujte usluge stručnjaka za bezbjednost
- Ponovo preuzmite kontrolu nad kompromitovanim nalogom

a. Svaki pružalac usluga će biti drugačiji
b. Zabilježite datume, vrijeme, imena i korake koje preduzimate

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Budite svjesni svih opcija za dvofaktornu autentifikaciju prilikom postavljanja novih naloga, onemogućavajući sve slabije opcije zasnovane na SMS porukama
- Budite svesni da je ranjivost povezana sa vašim mobilnim operaterom i da imate ograničenu kontrolu nad tim

a. Fokusirajte se na ono što možete kontrolisati
b. Primijenite odbranu u dubini i kompartmentalizaciju vaših naloga

- Reference:
- 1. MITRE ATT&CK Technique T1451:
- https://attack.mitre.org/techniques/T1451/

CSEC
Cyber Security Excellence Centre

Pristup podacima za pristup - Spearphishing - Phishing

(P) Priprema

- Popraviti ranjivosti sistema
- Redovno vršiti inspekcije kontrola/oružja
- Redovno sprovoditi obuke o prepoznavanju i zaštiti od *phishinga*
- Sprovoditi simulacije *phishing* napada
- Voditi evidenciju o mrežnom saobraćaju
- Voditi evidenciju dolaznih i odlaznih e-mailova
- Ustanoviti mehanizam za prijavljivanje sumnjivih e-mailova od strane korisnika
- Uključiti obavještajne podatke o prijetnjama

(I) Identifikacija

- Pratiti aktivnosti:

a. Neuobičajene DNS aktivnosti
b. E-mailove sa sumnjivim prilozima
c. Više identičnih e-mailova poslatih sa nepoznatih izvora
d. E-mailove poslate sa domenima koji sadrže greške u kucanju
e. E-mailove koji ne prolaze SPF i/ili DKIM provjere

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Implementirati zaštitu perimetra za poznate lokacije prijetnji
- Zaključati ili resetovati lozinku pogođenih korisnika ukoliko su njihovi podaci za prijavu otkriveni

(E) Iskorjenjivanje/Uništavanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Ažurirati ranjivosti aseta
- Pregledati sve priloge koji su uključeni u e-mailove
- Izvršiti skeniranje krajnjih tačaka/antivirus skeniranje na sistemima pogođenih korisnika
- Pregledati logove kako biste identifikovali druge pogođene korisnike

(O) Oporavak

- Provjeriti da li su promijenjeni svi kompromitovani podaci za prijavu
- Vratiti ili ponovo kreirati sisteme sa prisustvom malvera
- Staviti na crnu listu izvore phishing e-mailova

a. Pojedinačne adrese pošiljalaca e-mailova
b. Cijeli domen pošiljaoca, ako je potrebno

- Riješiti posljedice štete

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1566: https://attack.mitre.org/techniques/T1566/

CSEC
Cyber Security Excellence Centre

Izvlačenje podataka - Automatizovano izvlačenje - Krađa podataka

(P) Priprema

- Popraviti ranjivosti sistema
- Redovno vršiti inspekcije kontrola/oružja
- Osigurati da je instaliran antivirus/endpoint zaštita na radnim stanicama
- Pružiti obuku o bezbjednosti zaposlenima kako bi bili svjesni bezbjednosnih rizika

(I) Identifikacija

- Pratiti aktivnosti:

a. Neuobičajene DNS aktivnosti
b. Neobičnu aktivnost fajl sistema
c. Neobičnu mrežnu aktivnost
d. Upozorenja antivirus/endpoint sistema

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Implementirati zaštitu perimetra za poznate lokacije prijetnji
- Privremeno ukloniti pogođene sisteme sa mreže

(E) Iskorjenjivanje/Uništavanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Popraviti ranjivosti sistema
- Izvršiti skeniranje krajnjih tačaka/antivirus skeniranje na sistemima pogođenih korisnika

(O) Oporavak

- Identifikovati vrstu malvera koji je korišten
- Utvrditi koje podatke su možda prenijeli
- Provjeriti da li su promijenjene sve kompromitovane akreditacije
- Vratiti ili ponovo kreirati sisteme sa prisustvom malvera
- Skenirati druge sisteme i logove za poznate indikatore kompromitacije.
- Blokirati IP adrese povezane sa malverom na perimetru firewall-a

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1020: https://attack.mitre.org/techniques/T1020/

CSEC
Cyber Security Excellence Centre

Lateralni pokret - Zaobići Hash

(P) Priprema

- Popraviti ranjivosti sistema
- Redovno vršiti inspekcije kontrola/oružja
- Osigurati da je instaliran antivirus/endpoint zaštita na radnim stanicama
- Osigurati da serveri i radne stanice bilježe logove na centralnoj lokaciji.
- Mrežna segmentacija i firewall-ovi mogu pomoći u smanjenju uticaja
- Onemogućiti NTLM autentifikaciju gdje je moguće

a. SMB
b. HTTP
c. SMTP

(I) Identifikacija

- Pratiti aktivnosti:

a. Neobičnu aktivnost korisnika
b. Neočekivane prijave korištenjem NTLM autentifikacije

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Implementirati zaštitu perimetra za poznate lokacije prijetnji
- Blokirati naloge za koje se sumnja da su kompromitovani
- Sistemi za koje se vjeruje da imaju malver trebaju biti uklonjeni sa mreže

(E) Iskorjenjivanje/Uništavanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Popraviti ranjivosti sistema
- Izvršiti skeniranje krajnjih tačaka/antivirus skeniranje na sistemima pogođenih korisnika
- Pregledati logove kako bi se identifikovali drugi potencijalni slučajevi "pass the hash"

(O) Oporavak

- Vratiti se na RPO (Recovery Point Objective) unutar RTO (Recovery Time Objective)
- Riješiti eventualnu prateću štetu
- Promijeniti lozinke svih potencijalno kompromitovanih naloga
- Utvrditi niz događaja koji su doveli do incidenta "pass the hash"
- Riješiti sve povezane bezbjednosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1550 Sub-technique 002: https://attack.mitre.org/techniques/T1550/002/

CSEC
Cyber Security Excellence Centre

Upornost - Kreirajte nalog - Backdoor korisnički nalozi

(P) Priprema

- Popraviti ranjivosti sistema
- Redovno vršiti inspekcije kontrola/oružja
- Osigurati da je instaliran antivirus/endpoint zaštita na radnim stanicama
- Osigurati da serveri i radne stanice bilježe logove na centralnoj lokaciji
- Provjeriti da li bezbjednosni softver generiše upozorenja kada se kreiraju privilegovani nalozi
- Ukloniti neaktivne/neiskorištene naloge

(I) Identifikacija

- Pratiti aktivnosti:

a. Neobičnu DNS aktivnost
b. Kreiranje privilegovanih naloga
c. Neočekivane promjene dozvola za naloge

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima
- Pregledati logove aktivnosti novokreiranog naloga i naloga koji je korišćen za njegovo kreiranje
- Kontaktirati korisnike izvan opsega komunikacije kako biste se informisali o novom nalogu

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Implementirati zaštitu perimetra za poznate lokacije prijetnji
- Blokirati naloge za koje se sumnja da su kompromitovani
- Sistemi za koje se vjeruje da imaju malver trebaju biti uklonjeni sa mreže

(E) Iskorjenjivanje/Uništavanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Popraviti ranjivosti sistema
- Izvršiti skeniranje krajnjih tačaka/antivirus skeniranje na sistemima pogođenih korisnika
- Potvrditi da su uklonjeni svi dodatni mehanizmi za trajno prisustvo

(O) Oporavak

- Vratiti se na RPO (Recovery Point Objective) unutar RTO (Recovery Time Objective)
- Riješiti eventualnu prateću štetu
- Ukoliko napadač stekne pristup kao Domain Admin, resetovati lozinku korisničkog naloga "krbtgt"

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITER ATT&CK Technique T1136: https://attack.mitre.org/techniques/T1136/

CSEC
Cyber Security Excellence Centre

Početni pristup - Pouzdani odnos - Pristup dobavljača infrastrukturi

(P) Priprema

- Popraviti ranjivosti sistema
- Redovno vršiti inspekcije kontrola/oružja
- Održavati listu dobavljača sa pristupom sistemima ili mreži.
- Verifikovati da dobavljači imaju pristup samo neophodnim sistemima i mrežama
- Izolovati sisteme koji su dostupni dobavljačima od ostatka mreže koliko je moguće
- Redovno auditovati pristup dobavljača mreži i sistemskim nalozima
- Zahtijevati od dobavljača da koriste multifaktorsku autentifikaciju gde je to moguće
- Osigurati da svi sistemi i mrežni uređaji bilježi logove na centralnoj lokaciji

(I) Identifikacija

- Pratiti aktivnosti:

a. Pristup dobavljača tokom neobičnih sati/dana
b. Pristup dobavljača sa neobičnih izvora (npr. geografske lokacije, IP adrese, itd.)
c. Pokušaji dobavljačkih naloga da pristupe drugim sistemima/mrežama

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima
- Redovno pregledati aktivnosti dobavljača

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Implementirati zaštitu perimetra za poznate lokacije prijetnji
- Blokirati pristup od strane kompromitovanog dobavljača
- Zaključati naloge povezane sa kompromitovanim dobavljačem
- Informisati dobavljača o detektovanoj aktivnosti
- Inspektovati sve potencijalno kompromitovane sisteme kako bi se identifikovali indikatori kompromitacije (IOC)

(E) Iskorjenjivanje/Uništavanje

- Zatvoriti vektor (metoda ili put kojim se izvodi napad na računarski sistem) napada
- Izvršiti skeniranje krajnjih tačaka/antivirus skeniranje na sistemima pogođenih korisnika
- Pregledati logove kako bi se utvrdio obim neovlaštene aktivnosti

(O) Oporavak

- Vratiti se na RPO (Recovery Point Objective) unutar RTO (Recovery Time Objective)
- Riješiti eventualnu prateću štetu
- Resetovati lozinke za naloge dobavljača
- Vratiti neophodan pristup dobavljačima kada je sigurno

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1199: https://attack.mitre.org/techniques/T1199/

CSEC
Cyber Security Excellence Centre

Postojanost - Proširenja pretraživača - Zlonamjerna proširenja pretraživača

(P) Priprema

- Popraviti ranjivosti sistema
- Redovno vršiti inspekcije kontrola/oružja
- Osigurati da je instaliran antivirus/endpoint zaštita na radnim
- stanicama
- Osigurati da radne stanice bilježe logove na centralnoj lokaciji
- Bilježiti mrežni saobraćaj
- Koristiti Group Policy za dozvolu samo odobrenih ekstenzija pregledača

(I) Identifikacija

- Pratiti aktivnosti:

a. Neobičnu DNS aktivnost
b. Upozorenja antivirus/endpoint sistema
c. Upozorenja IDS/IPS sistema

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Identifikovati zlonamjernu ekstenziju
- Implementirati zaštitu perimetra za poznate lokacije prijetnji
- Ukloniti pogođeni sistem sa mreže ako je potrebno

(E) Iskorjenjivanje/Uništavanje

- Zatvoriti vektor napada
- Popraviti ranjivosti sistema
- Provjeriti sistem za druge zlonamerne/nedozvoljene ekstenzije
- Ukloniti zlonamjernu ekstenziju sa sistema
- Izvršiti antivirus skeniranje pogođenog sistema

(O) Oporavak

- Vratiti se na RPO (Recovery Point Objective) unutar RTO (Recovery Time Objective)
- Riješiti eventualnu prateću štetu
- Utvrditi kako i zašto je ekstenzija instalirana
- Riješiti sve povezane bezbjednosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1176: https://attack.mitre.org/techniques/T1176/

CSEC
Cyber Security Excellence Centre

Money Mule prevare - Prevara izvršnog direktora

(P) Priprema

- Redovno vršiti inspekcije kontrola/oružja
- Redovno sprovoditi obuke o prepoznavanju *phishing* napada
- Sprovoditi simulacije *phishing* napada
- Uspostaviti procedure za proveru finansijskih transakcija putem drugog kanala komunikacije
- Bilježiti dolazne i odlazne e-mail poruke
- Uspostaviti metodu za korisnike da prijave sumnjive e-mail poruke

(I) Identifikacija

- Pratiti aktivnosti:

a. E-mail poruke sa sumnjivim prilozima
b. Višestruke identične e-mail poruke poslate sa nepoznatih izvora
c. E-mail poruke poslate sa domenima sa greškama u kucanju
d. E-mail poruke koje ne prolaze SPF i/ili DKIM provjere

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Implementirati zaštitu perimetra za poznate lokacije prijetnji
- Pregledati logove e-maila kako bi se identifikovali drugi pogođeni korisnici
- Pregledati relevantne finansijske transakcije

(E) Iskorjenjivanje/Uništavanje

- Kontaktirajte finansijske institucije kako biste zaustavili/poništili transakcije

(O) Oporavak

- Dodajte izvore *phishing* e-mail poruka na crnu listu

a. Individualne adrese pošiljaoca e-maila
b. Cijeli domen pošiljaoca, ako je to prikladno

- 2. Prijavite incident odgovarajućem organu za sprovođenje zakona

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1566: https://attack.mitre.org/techniques/T1566/

CSEC
Cyber Security Excellence Centre

Postojanost - Web Shells

(P) Priprema

- Popraviti ranjivosti sistema.
- Redovno vršiti inspekcije kontrola/oružja
- Osigurati da serveri bilježe logove na centralnoj lokaciji
- Onemogućiti izvršavanje skripti u direktorijumima gde nije potrebno
- Verifikovati da veb aplikacije na serveru ne rade sa prekomjernim privilegijama
- Koristiti AppArmor, SELinux ili druge mitige gde je to prikladno

(I) Identifikacija

- Pratiti aktivnosti:

a. Neobične poruke o greškama u logovima
b. Neobične obrasce web saobraćaja
c. Neočekivane promjene u osnovnim direktorijumima web sajtova
d. Upozorenja IPS/IDS sistema
e. Upozorenja antivirus sistema

- Istražiti i otkloniti sva upozorenja povezana sa pogođenim resursima

(Z) Obuzdavanje/Kontrola

- Evidentirati (Popisivanje i procjena)
- Otkrivanje | Odbijanje | Ometanje | Oštećenje | Obmanjivanje | Uništavanje
- Posmatranje -> Orijentacija -> Odlučivanje -> Djelovanje
- Implementirati zaštitu perimetra za poznate lokacije prijetnji
- Pregledati web logove kako bi se identifikovali slučajevi pristupa web shell-u
- Implementirati zaštitu perimetra za poznate lokacije pretnji

(E) Iskorjenjivanje/Uništavanje

- Zatvoriti vektor napada
- Popraviti ranjivosti sistema
- Skenirati veb servere u potrazi za drugim instancama web shell-ova
- Utvrditi kako je web shell postavljen na sistem.
- Resetovati sve potencijalno kompromitovane lozinke.
- Pregledati logove svih sistema koje je napadač mogao da pristupi
- Skenirati pogođene sisteme antivirus/endpoint softverom

(O) Oporavak

- Vratiti se na Recovery Point Objective (RPO) unutar Recovery Time Objective (RTO)
- Riješiti eventualnu prateću štetu
- Utvrditi osnovni uzrok incidenata
- Riješiti sve povezane bezbjednosne incidente

(L) Lekcije/Mogućnosti

- Vršiti rutinsku provjeru sajber higijene
- Angažovati eksterne stručnjake za odgovor na incidente i provajdere usluga za sajber bezbjednost

- Reference:
- MITRE ATT&CK Technique T1505 Sub-technique 003: https://attack.mitre.org/techniques/T1505/003/

CSEC
Cyber Security Excellence Centre