AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Udhëzuesi Stop Ransomware

Version: 1.0

Data: 26/05/2023

Indeksi

Hyrje

Ransomware është një malware i krijuar për të enkriptuar skedarët duke i bërë ato të papërdorshme.

Aktorët keqdashës më pas kërkojnë shpërblim në këmbim të deshifrimit të të dhënave. Gjatë viteve, sulmuesit i kanë përshtatur taktikat ransomware që të jenë më shkatërrues dhe të kenë më tepër impakt.

Këto ransomware dhe incidentet që lidhen me rrjedhjen e të dhënave (data breach) ndikojnë rëndë në proceset e biznesit.

Ky udhëzues përfshin dy burime kryesore:

- **Pjesa 1: Praktika më të mira të parandalimit të ransomware dhe data extortion,**
- **Pjesa 2: Lista kontrolluese e përgjigjes së ransomware dhe data extortion.**

Pjesa 1 ofron udhëzime për të gjitha organizatat për të reduktuar ndikimin dhe gjasat e incidenteve të ransomware dhe data extortion, duke përfshirë praktikat më të mira për të përgatitur, parandaluar dhe zbutur këto incidente. Praktikat më të mira të parandalimit grupohen sipas vektorëve të aksesit fillestar.

Pjesa 2 përfshin listën kontrolluese të praktikave më të mira për t'iu përgjigjur këtyre incidenteve. Praktikat dhe rekomandimet më të mira për parandalimin dhe reagimin e ransomware dhe data extortion bazohen në njohuritë operacionale nga CISA, MS-ISAC, etj.

Ky udhëzues është për profesionistë të teknologjisë së informacionit (IT), si edhe për persona të tjerë brenda një organizate që merret me zhvillimin e politikave dhe procedurave të reagimit ndaj incidenteve kibernetike ose në koordinimin e reagimit ndaj incidenteve kibernetike.

Pjesa 1: Praktika më të mira të përgatitjes, parandalimit dhe mitigimit të *ransomware* dhe *data extortion*

Praktikat më të mira të mitigimit

Praktikat më të mira të rekomanduara janë CPG-të (Cross-Sector Cybersecurity Performance Goal) të CISA dhe Institutit Kombëtar të Standardeve dhe Teknologjisë (NIST), të cilat ofrojnë një bashkësi minimale praktikash dhe mbrojtjesh që CISA dhe NIST rekomandojnë për t´u zbatuar nga të gjitha organizatat. CPG-të përfshijnë kornizat ekzistuese të sigurisë kibernetike dhe udhëzimet për t'u mbrojtur nga kërcënimet, taktikat, teknikat dhe procedurat më të zakonshme.

Përgatitja për Ransomware dhe Incidentet e data extortion

Referojuni praktikave dhe referencave më të mira të listuara në këtë seksion rreth menaxhimit të rreziqeve që paraqiten nga ransomware për një përgjigje të koordinuar dhe efikase nga organizatën në rast të një incidenti. Zbatoni këto praktika të mëposhteme:

- *Mbani backupe offline dhe të enkriptuara të të dhënave kritike dhe testoni rregullisht disponueshmërinë dhe integritetin e tyre*. Është e rëndësishme që backup-et të mbahen offline, pasi shumë variante të ransomware përpiqen të gjejnë dhe më pas të fshijnë ose enkriptojnë backup-e të aksesueshme, për të bërë të pamundur restaurimin nëse nuk paguhet shpërblesa.
  - Mirëmbani "templates" të imazheve që kanë një sistem operativ të parakonfiguruar (OS) dhe aplikacione softuerike për të rindërtuar një sistem makinë virtuale ose server.
    - Përdorni infrastrukturën si kod (Infrastructure as Code (IaC)) për deploy, për të përditësuar burimet cloud dhe për të mbajtur backup të skedarëve të templatëve offline për një rishpërndarje të shpejtë të burimeve. Kodit IaC duhet ti kontrollohet versioni dhe të auditohen ndryshimet e template.
    - Ruani kodin burim ose skedarët e ekzekutueshëm si backup-e offline.
  - Ruani pajisjen backup për të rindërtuar sistemet nëse nuk preferohet rindërtimi i sistemit primar.

Krijoni, mirëmbani dhe ushtroni rregullisht një plan bazë të reagimit ndaj incidenteve kibernetike (IRP) dhe plan komunikimi shoqërues që përfshin procedurat e reagimit dhe njoftimit për incidentet e ransomware dhe extortion/breach të të dhënave. Sigurohuni që të keni në dispozicion një kopje fizike dhe offline të planit.

- Sigurohuni që procedurat e njoftimit për shkeljen e të dhënave t'u përmbahen ligjeve shtetërore në fuqi.
- Për shkelje që përfshijnë informacion personal të identifikueshëm (PII), njoftoni individët e prekur që ata të ndërmarrin hapa për të zvogëluar mundësinë që informacioni i tyre të keqpërdoret. Jepni llojin e informacionit të ekspozuar, informacionin përkatës të kontaktit dhe rekomandoni veprime korrigjuese.
- Njoftoni bizneset për një shkelje nëse vidhen PII-të e ruajtura në emër të bizneseve të tjera.

- Sigurohuni që IRP dhe plani i komunikimit të rishikohen dhe miratohen me shkrim nga CEO, ose ekuivalent me të, dhe të dyja keto të rishikohen dhe kuptohen nga i gjithë drejtuesit.

Përfshini në planin e komunikimit, procedurat e komunikimit organizativ, si dhe deklaratat e mbajtjes së incidenteve kibernetike. Dakortësoni se çfarë niveli informacioni është i përshtatshëm për t'u ndarë brenda organizatës dhe me publikun dhe se si do të rrjedhë informacioni.

Zbatoni një arkitekturë zero trust (ZTA) për të parandaluar aksesin e paautorizuar në të dhëna dhe shërbime. Zbatimi i kontrollit të aksesit duhet të jetë sa më i qartë të jetë e mundur.

Parandalimi dhe zbutja e incidenteve të Ransomware dhe data extortion

Referojuni praktikave dhe referencave më të mira të listuara në këtë seksion për të ndihmuar në parandalimin dhe zbutjen e incidenteve të ransomware dhe data estortion. Praktikat më të mira të parandalimit grupohen sipas vektorëve të zakonshëm të aksesit fillestar të ransomware dhe aktorëve të data extortion.

Vektori i aksesit fillestar: Vulnerabilitetet dhe konfigurimet e gabuara në pajisjet që kanë lidhje me internetin

Kryeni skanim të rregullt për vulnerabilitete për të identifikuar dhe adresuar ato, sidomos skanim në ato pajisje që kanë lidhje me internetin, për të kufizuar sipërfaqen e sulmit.

Arnoni (Patch) dhe përditësoni rregullisht softuerin dhe sistemet operative në versionet më të fundit të disponueshme.

Sigurohuni që të gjitha pajisjet brenda ambienteve të punës, shërbimeve cloud, celularët dhe ato personale (d.m.th., pajisja juaj [BYOD]) të jenë konfiguruar siç duhet dhe të jenë aktivizuar veçoritë e sigurisë. Për shembull, çaktivizoni portat dhe protokollet që nuk përdoren për qëllime biznesi (p.sh., [RDP], [TCP] Porta 3389).

Kufizoni përdorimin e RDP dhe shërbimeve të tjera të desktopit në distancë. Nëse RDP është e nevojshme, zbatoni praktikat më të mira te tyre. Aktorët kërcënues shpesh fitojnë akses fillestar në një rrjet në distancë përmes shërbimeve të ekspozuara dhe të siguruara dobët, dhe më vonë përshkojnë rrjetin duke përdorur klientin Windows RDP.

- Kontrolloni rrjetin për sistemet që përdorin RDP, mbyllini portat RDP të papërdorura, zbatoni bllokimet e llogarisë pas një numri të caktuar përpjekjesh, aplikoni vërtetimin me shumë faktorë (MFA) dhe regjistroni përpjekjet për të hyrë në RDP.

- VPN-të, pajisjet e infrastrukturës së rrjetit dhe pajisjet që përdoren për të hyrë në mjediset e punës nga distanca, përditësojini me arnimet më të fundit të softuerit dhe konfigurimet e sigurisë. Për të rritur sigurinë implementoni MFA në të gjitha lidhjet VPN. Nëse MFA nuk implementohet, të përdoren fjalëkalime me 15 ose më shumë karaktere.

Çaktivizo versionet 1 dhe 2 të protokollit të Bllokut të Mesazheve të Serverit (SMB) dhe përmirësoje në versionin 3 (SMBv3). Për të përhapur malware nëpër organizata, aktorët keqdashës përdorin SMB:

- Në sistemet që kërkojnë akses, blloko ose kufizo trafikun e brendshëm të SMB për të kufizuar ndërhyrjet në rrjetin tuaj.
- Zbatoni nënshkrimin e SMB per te parandaluar disa sulme si adversary-in-the-middle dhe pass-the-hash.
- Blloko aksesin e jashtëm të SMB në rrjet, duke bllokuar portën TCP 445, portën TCP 139 dhe portat 137–138 të protokollit UDP.
- Regjistroni dhe monitoroni trafikun e SMB për sjelljet jonormale.

Vektori i aksesit fillestar: Kredencialet e komprometuara

- Implementoni phishing-resistant MFA, për të gjitha shërbimet, veçantërisht për email, VPN dhe llogaritë që aksesojnë sistemet kritike.
- Përdorni MFA pa fjalëkalim që zëvendësojnë fjalëkalimet me dy ose më shumë faktorë verifikimi (p.sh., një gjurmë gishti, njohje fytyre, një çelës kriptografik).
- Implementoni sistemet e menaxhimit të identitetit dhe aksesit (IAM) që administratorët të kenë mjetet dhe teknologjitë për të monitoruar dhe menaxhuar rolet dhe privilegjet e aksesit në aplikacione.
- Ndryshoni emrat e përdoruesve dhe fjalëkalimet e paracaktuar të administratorit.
- Zbatoni politikat e fjalëkalimeve që kërkojnë fjalëkalime unike me të paktën 15 karaktere.
- Siguroni dhe kufizoni aksesin e çdo menaxhuesi të fjalëkalimit që përdorni dhe aktivizoni të gjitha veçoritë e sigurisë të produktit në përdorim, si p.sh. MFA.
- Zbatoni politikat e bllokimit të llogarisë pas një numri të caktuar përpjekjesh të dështuara për akses.
- Ruani fjalëkalimet në një bazë të sigurtë të dhënash dhe përdorni algoritme të forta hashing.
- Implementoni Local Administrator Password Solution (LAPS) aty ku është e mundur nëse sistemi operativ është më i vjetër se Windows Server 2019 dhe Windows 10 pasi këto versione nuk kanë LAPS të integruar.
- Trajnoni të gjithë punonjësit për sigurinë e fjalëkalimeve për të theksuar mosruajtjen e fjalëkalimeve në skedarët lokalë.
- Përdorni Windows PowerShell Remoting, Remote Credential Guard ose RDP që kur të krijoni një lidhje në distancë të shmangni ekspozimin e drejtpërdrejtë të kredencialeve.
- Ndani llogaritë e administratorit nga llogaritë e përdoruesve.

Vektori i aksesit fillestar: Phishing

Zhvilloni një program ndërgjegjësimi dhe trajnimi për përdoruesit e sigurisë kibernetike me udhëzime se si të identifikoni dhe raportoni aktivitete të dyshimta (p.sh., phishing) ose incidente.

Vendosni filtra në portën e emailit elektronik për të filtruar emailet me tregues të njohur keqdashës, dhe bllokoni adresat e dyshimta (IP) në firewall.

Aktivizoni filtrat e zakonshëm të attachment për të kufizuar llojet e skedarëve që zakonisht përmbajnë malware dhe që nuk duhet të dërgohen me email.

Zbatoni politikën dhe verifikimin e autentifikimit, raportimit dhe konformitetit të mesazheve të bazuara në domain (DMARC).

DMARC mbron domainin nga mashtrimi, por nuk mbron nga emailet mashtruese, veçse nëse domaini dërgues zbaton gjithashtu DMARC. DMARC bazohet në Sender Policy Framework (SPF) dhe Domain Keys Identified Mail (DKIM), duke shtuar një funksion raportimi që lejon dërguesit dhe marrësit të përmirësojnë dhe monitorojnë mbrojtjen e domainit nga emailet mashtruese.

Sigurohuni që skriptet makro janë çaktivizuar për skedarët e Microsoft Office të transmetuar përmes emailit. Këto makro mund të përdoren për të ofruar ransomware.

Çaktivizo Windows Script Host (WSH).

Vektori i aksesit fillestar: Infeksioni i malware

Përdorni përditësime automatike për programet antivirus dhe anti-malware.

Sigurohuni që mjetet të jenë konfiguruar siç duhet që të përshkallëzojnë paralajmërimet dhe treguesit për të njoftuar personelin e sigurisë.

Përdorni listën e lejeve të aplikacionit dhe/ose zbulimin e pikës fundore (EDR) në të gjitha asetet, për të siguruar që ekzekutohet vetëm softueri i autorizuar dhe i gjithë softueri i paautorizuar është i bllokuar.

- Për Windows, aktivizoni Windows Defender Application Control (WDAC), AppLocker ose të dyja.
- Merrni parasysh zbatimin e EDR për burimet e bazuara në cloud.

Zbatoni një sistem Intrusion Detection System (IDS) për të zbuluar aktivitetin e komandës dhe kontrollit dhe aktivitete të tjera dashakeqe të rrjetit, të cilat ndodhin përpara se të vendoset ransomware.

Sigurohuni që IDS të monitorohet dhe menaxhohet në mënyrë qëndrore.

Bllokoni krijimin e skedarëve malware me programin Windows Sysmon. Që nga Sysmon 14, opsioni FileBlockExecutable përdoret për të bllokuar krijimin e skedarëve të ekzekutueshëm me qëllim të keq, skedarëve Dynamic Link Library (DLL) dhe skedarëve të sistemit që përputhen me vlera specifike hash.

Vektori i aksesit fillestar: Format e avancuara të inxhinierisë sociale (*social engineering*)

- Krijoni politika rreth trajnimeve të ndërgjegjësimit për sigurinë kibernetike për format e avancuara të inxhinierisë sociale për personelin. Trajnimi duhet të përfshijë këshilla rreth njohjeve të faqeve të paligjshme të internetit dhe rezultatet e kërkimit.
- Zbatoni sistemin mbrojtës të emrave të domainit (DNS). Bllokimi i aktivitetit keqdashës që në burim të tij, bën që shërbimet mbrojtëse DNS të ofrojnë siguri të lartë të rrjetit për

punonjësit në distancë. Këto shërbime sigurie analizojnë pyetjet DNS dhe ndërmarrin veprime për të zbutur kërcënimet - të tilla si malware, ransomware, sulme phishing, viruse, sajte me qëllim të keq dhe spyware - duke shfrytëzuar protokollin dhe arkitekturën ekzistuese DNS.

Vektori i aksesit fillestar: Palët e treta dhe Managed Service Providers (MSP)

- Konsideroni menaxhimin e rrezikut dhe praktikat e higjienës kibernetike të palëve të treta ose MSP ku mbështetet organizata juaj për të përmbushur misionin e saj. MSP-të janë një vektor infeksioni për ransomware me impakt të madh në organizata të shumta.
- Nëse një palë e tretë ose MSP është përgjegjëse për ruajtjen dhe sigurimin e backup të organizatës suaj, sigurohuni që ata të ndjekin praktikat më të mira të përshkruara më sipër.
- Kur përcaktoni aksesin e palëve të treta siguroni përdorimin e privilegjeve më të vogla dhe ndarjen e detyrave. Palët e treta dhe MSP-të duhet të kenë akses vetëm në pajisjet dhe serverët që janë brenda rolit ose përgjegjësive të tyre.

Udhëzime të përgjithshme për praktikat më të mira

- Organizata juaj të ketë një qasje gjithëpërfshirëse të menaxhimit të aseteve:
    - Bëni inventarin e aseteve të TI-së të organizatës suaj, logjike (p.sh., të dhëna, softuer) dhe fizike (p.sh., harduer).
    - Duhet te dini se cilat të dhëna ose sisteme janë më kritike për shëndetin dhe sigurinë, gjenerimin e të ardhurave ose shërbime të tjera kritike, dhe te kuptoni çdo lidhje ndërvarësitësie (p.sh., "lista e sistemit 'A' e përdorur për të kryer 'X' ruhet në aktivin kritik 'B'"). Kjo ndihmon në përcaktimin e prioriteteve të rikuperimit nëse ndodh një incident. Për asetet kritike zbatoni kontrolle ose masa mbrojtëse më gjithëpërfshirëse të sigurisë.

Zbatoni parimin e privilegjit më të ulët për të gjitha sistemet dhe shërbimet në mënyrë që të ketë akses vetëm ai përdorues që i duhet aksesi për të kryer punën e vet. Aktorët dashakeq përdorin shpesh llogari të privilegjuara për sulme ransomware.

- Kufizoni privilegjet e përdoruesve për të instaluar dhe ekzekutuar aplikacionet softuerike.
- Kufizoni privilegjet e përdoruesve/rolin për të aksesuar ose modifikuar burimet e bazuara në cloud.
- Përdorni Windows Defender Remote Credential Guard dhe modalitetin e kufizuar të administratorit për sesionet RDP.
- Hiqni llogaritë dhe grupet e panevojshme dhe kufizoni aksesin në root.
- Auditoni Active Directory (AD) për privilegje të tepërta në llogaritë dhe anëtarësimet në grup.
- Përdorni grupin Protected Users AD për të mbrojtur domainet e Windows-it që të sigurohen më tepër llogaritë e privilegjuara të përdoruesve kundrejt sulmeve pass-the-hash.

- Çdo tremujor kontrolloni llogaritë e përdoruesve dhe administratorëve nëse ka llogari joaktive ose të paautorizuara.

Të gjitha makinat virtuale dhe hipervizorët duhet të jenë të përditësuar. Taktikat e reja të ransomware synojnë serverët VMWare ESXi, të cilat mundësojnë kriptim të shpejtë të infrastrukturës.

Përdorni praktikat më të mira dhe aktivizoni cilësimet e sigurisë në lidhje me mjediset cloud, si Microsoft Office 365.

- Rezervoni shpesh të dhënat, offline ose përdorni backup cloud-to-cloud.
- Aktivizoni logimin në të gjitha burimet dhe vendos sinjalizime për përdorime jonormale të tyre.
- Aktivizoni mbrojtjen e fshirjes/bllokimit të objekteve në burimet e magazinimit që targetohen shpesh nga sulmet e ransomware (p.sh. magazina e objekteve, magazina e bazës së të dhënave, magazina e skedarëve, magazina e block) për të parandaluar fshirjen ose mbishkrimin e të dhënave, përkatësisht.
- Aktivizoni kontrollin e versionit për të ruajtur variante të shumta objektesh. Kjo lejon që rikuperimi i objekteve të bëhet më lehtë nga pasojat e veprimeve të paqëllimta ose dashakeqe.

Zbutja e përdorimit keqdashës të aksesit në distancë dhe softueri i monitorimit dhe menaxhimit në distancë (RMM):

- Kontrolloni mjetet e aksesit në distancë në rrjetin për të identifikuar softuerin aktual ose të autorizuar RMM.
- Rishikoni loget e ekzekutimit të softuerit RMM për të zbuluar nëse ka përdorim jonormal të tij.
- Përdorni softuerin e sigurisë për të zbuluar rastet e softuerit RMM që ngarkohen vetëm në memorie.
- Zgjidhjet e autorizuara RMM të përdoren vetëm nga brenda rrjetit tuaj përmes zgjidhjeve të miratuara të aksesit në distancë, të tilla si VPN ose ndërfaqe virtuale të desktopit (VDI).

Përdorni mjete logjike ose fizike të segmentimit të rrjetit duke zbatuar ZTA dhe duke e ndarë rrejtin në njësi të ndryshme biznesi ose burime të TI-së të departamenteve brenda organizatës dhe duke mbajtur ndarjen midis IT dhe teknologjisë operacionale.

Zhvilloni dhe përditësoni rregullisht diagram(et) gjithëpërfshirëse të rrjetit që përshkruajne sistemet dhe rrjedhjen e të dhënave brenda rrjetit(eve) të organizatës suaj (shih Figurën 1). Kjo i ndihmon reaguesit e incidentit të kuptojnë se ku t'i përqendrojnë përpjekjet e tyre. Shih Figurën 2 dhe Figurën 3 për përshkrimet e një rrjeti të pa segmentuar dhe të një rrjeti të segmentuar të praktikave më të mira.

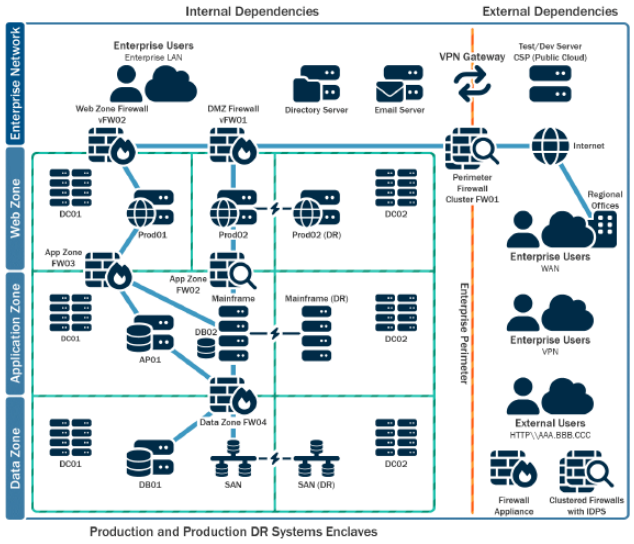

Figure 1: Example Network Diagram

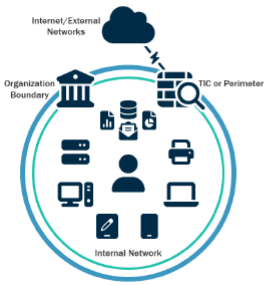

Figure 2: Flat (Unsegmented) Network

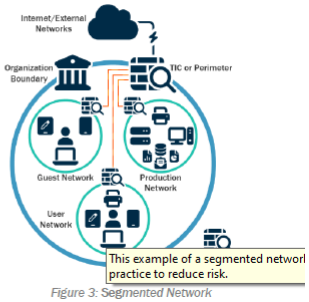

Figure 3: Segmented Network

- Të kufizohet përdorimi i Powershell vetëm nga user specifik nëpërmjet Group Policy. Përgjithësisht, vetëm user-at ose administratorët që menaxhojnë një rrjet ose Windows OS kanë privilegj përdorimi të Powershell. Powershell është një cross-platform, command-line, shell dhe gjuhë skriptimi e cila është komponent i Microsoft Windows. Hackerat e përdorin Powershell për të vendosur ransomware dhe për të fshehur aktivitetet e tyre keqdashëse.
  - Të përditësohet Windows Powershell ose Powershell Core me versionin më të fundit dhe të c'instalohen të gjithë versionet e mëparshëm të Powershell.
  - Të sigurohen që instancat e Powershell, të versionit më të fundit, kanë module, script block dhe transcripstion logging enabled. Logs nga versionet para Windows Powershell 5.0 ose janë jo ekzistent ose nuk kanë regjistruar mjaftueshëm detaje të mjaftueshme për të ndihmuar në monitorimin e ndërmarrjes së aktiviteteve të incident response.
    - Logs të Powershell përmbajnë të dhëna të rëndësishme, përfshirë ndërveprimin e regjistrit dhe historical OS dhe taktikave, teknikave dhe procedurave (TTP) të përdorimit të Powershell nga një sulmues.
    - Dy logs që regjistrojnë aktivitetin e Powershell janë "Powershell Windows Event" dhe "Powershell Operational". Organizatat autorizuese rekomandojnë që këto dy logs të vendosen me një periudhë mbajtjeje prej të paktën 180 ditë. Këto logs duhen kontrolluar në një mënyrë periodike dhe të rregullt në mënyrë që të konfirmohet në qoftë se të dhënat janë fshirë ose në qoftë se logging është fikur. Madhësia e storage e lejuar për të dyja këto logs duhet të jetë sa më e madhe të jetë e mundur.
- Sigurimi i domain controllers (DCs). Sulmuesit shpesh synojnë dhe përdorin DC si një pikë nisjeje për shpërndarjen e ransomware në një rrjet sa më të gjerë. Për të siguruar DC-të duhet:
  - Përdorur versioni më i fundit i Windows Server i suportuar nga organizata në DC, pasi versionet e reja kanë më shumë vecori sigurie, përfshirë Active Directory të integruar.
  - Rekomandohet përdorimi i Windows Server 2019 ose më i ri dhe Windows 10 ose më i ri, për shkak se kanë vecori sigurie (security features) si LSASS protections me Windows Credential Guard, Windows Defender dhe Antimalware Scan Interface (AMSI).
  - Të sigurohet që DC-të janë patched rregullisht, dhe të bëhen patched për vulnerabilitetet kritike sa më shpejt të jetë e mundur.
  - Të përdoren open-source penetration tools për të verifikuar sigurinë e DC-së.

- Të sigurohet që në DC janë të instaluar sa më pak software për shkak se software-t mund të përdoren për të ekzekutuar kod arbitrar në sistem.
- Të kufizohet aksesi i DC-ve tek grupi i Administratorëve. User-at në këtë grup duhet të jenë të limituar dhe të kenë accounts të ndarë të cilat përdoren për veprime ditore me non-administrative permissions. Account-et admin të zgjedhura duhet të përdoren vetëm për qëllime administrative, si dhe të sigurohet se hyrja në internet, kontrollimi i email-eve dhe veprime të tjera që konsiderohen me rrezikshmëri të lartë të mos bëhen në DC.
- Të konfigurohen hostet e firewall të DC që të parandalojnë aksesin në internet. Zakonisht DC-të nuk kanë nevojë për akses të drejtpërdrejtë me internetin dhe serverat e lidhur me internetin mund të përdoren për të marrë përditësimet e nevojshme për DC-të.
- Të implementohet *privileged access management* (PAM) në DC për të ndihmuar në menaxhimin dhe monitorimin e aksesit të privilegjuar. PAM gjithashtu mund të regjistrojë dhe alertojë në rast detektimi të aktivitetit të pazakonshëm.
- Të konsiderohet caktivizimi ose kufizimi i NTLM dhe WDigest Authentication, dhe të përfshihet përdorimi i tyre si kriter për priotizimin e përditësimit të legacy systems ose për segmentimin e rrjetit. Në vend të tyre të përdoren protokolle federimi moderne (OIDC, SAML ose Kerberos) për autentikim me AES-256 bit encryption. Në qoftë se është e nevojshme që NTLM të jetë e aktivizuar atëherë të aktivizohet gjithashtu dhe Extended Protection for Authentication (EPA) për të preventuar disa nga sulmet e ardhura nga NTLM (NTLM-relay attacks). Duhet që auditimi i NTLM të jetë i aktivizuar në mënyrë që të sigurohet që vetëm përgjigjet NTLMv2 dërgohen në rrjet, dhe të merren masa që përgjigjet LM dhe NTML të refuzohen.
- Të mundësohet mbrojtje shtesë për autentikimin LSA për parandalimin e code injection i cili mundëson mbledhjen e kredencialeve nga sistemi. Përpara se të aktivizohen këto mbrojtje duhet të kryhen audite për lsass.exe për të kuptuar programet që do të ndikohen nga akvizimi i kësaj mbrojtjeje shtesë.
- Të ruhen dhe sigurohet logs nga pajisjet në rrjet, local hosts dhe cloud services, pasi logs mund të analizohen për të përcaktuar impaktin e eventeve dhe të konstatojnë në qoftë se një incident ka ndodhur.
- Të mirëmbahen dhe të bëhen back up log-et e sistemeve kritike për minimumin një vit.
- Të vendoset një sistem i centralizuar i menaxhimit të logs duke përdorur një security information and event management tool, pasi kjo i mundëson një organizate që të rishikojë logs nga burime të shumta dhe të analizojë një event individual dhe të përcaktojë impaktin e saj në organizatë.

- Të krijohet një bazë sigurie e trafikut normal dhe të rregullohen pajisjet e rrjetit për të detektuar sjellje anormale, sic janë lëvizjet horizontale në rrjet dhe teknika të persistencës.
- Të kryhen vlerësime të rregullta dhe periodike për të siguruar që të gjitha proceset dhe procedurat janë të përditësuara dhe mund të ndiqen nga stafi i sigurisë dhe përdoruesit.

Pjesa 2: Lista kontrolluese e përgjigjes së ransowmare dhe data extortion.

Në qoftë se një organizatë bie viktimë e ransomware, duhet të ndjekë procedurat e aprovuara të incident response. Tre hapat e parë duhet gjithmonë të ndiqen në sekuencë.

Detection and Analysis / Detektim dhe Analizim

1. Të përcaktohen sistemet e impaktuara dhe të izolohen menjëherë. Në qoftë se një numër i madh sistemesh ose subnet-esh janë të impaktuara, atëherë rrjeti duhet të vendoset offline në nivel switch-i.
    a. Të prioritizohet izolimi i sistemve kritike që janë esenciale për veprimet ditore.
    b. Në qoftë se fikja e përkohshme e rrjetit është e pamundur, të gjendet kabëlli i rrjetit dhe të shkëputen pajisjet e impaktuara nga rrjeti.
    c. Mbas një kompromizimi fillestar, sulmuesit mund të monitorojnë aktivitetin ose komunikimet e organizatës për të kuptuar në qoftë se sulmet e tyre janë detektuar. Sistemet duhet të izolohen në një mënyrë të koordinuar dhe të përdoren metoda komunikimi si telefonatat për të mos lejuar që sulmuesit të kuptojnë që janë zbuluar dhe se hapat për zvogëlimin dhe mitigimin e dëmit janë duke u ndërmarrë.
2. Të fiken pajisjet në qoftë se shkëputja e tyre nga rrjeti është e pamundur në mënyrë që të shmanget përhapja më e gjerë e sulmit ransomware. Është e rëndësishme të theksohet se ky hap do të parandalojë organizatën nga mirëmbajtja e artifakteve të infeksionit ransomware, si dhe evidencave potenciale të ruajtuara në volatile memory.
3. Të identifikohen, prioritizohen dhe përzgjidhen sistemet e impaktuara për restaurim dhe rikuperim, në një rrjet të pastër dhe të konfirmohet natyra e të dhënave në një sistem të impaktuar. Restaurimi dhe rikuperimi i sistemeve të impaktuara duhet të bazohet në një listë të aseteve kritike, të cilat përfshijnë sistemet e informacionet për sigurinë kritike dhe shërbime të tjera kritike, së bashku me sistemet nga të cilat ato varen. Pajisjet dhe sistemet të cilat nuk janë perceptuar si të ndikuara nga sulmi, të mos vendosen si prioritare për restaurim dhe rikuperim.
4. Të kontrollohen sistemet e detektimit dhe preventimit ekzistuese në organizatë (IDS, antivirus, EDR, etj) dhe log-et. Nëpërmjet këtyre kontrolleve mund të gjenden evidenca të sistemeve ose malware-eve shtesë të përfshira në fazat fillestare të sulmit. Gjithashtu të kërkohet për evidencë të “dropper” malware sic janë Dridex, Anchor ose Bumblebee. Një rast ransomware mund të jetë evidencë e një kompromisi të mëparshëm në rrjet i cili nuk është rregulluar. Duke qënë se sulmuesit shpesh do të vendosin variante të ransomware për të turbulluar veprimaritë post-compromise, duhet kujdes i vecantë për identifikimin e dropper malware përpara rindërtimit nga backup-et.
5. Të komunikohet me ekipin e incident response për të zhvilluar dhe dokumentuar një kuptim fillestar të situatës bazuar në analizën aktuale.
6. Të iniciohen threat hunting activities,

a. Për ambjentet enterprise të kontrollohen AD accounts të krijuara së fundmi ose accounts me escalated privileges, logins anormale të pajisjeve VPN, modifikimet e pikës fundore që mund të dëmtojnë backup-et, keqpërdorimi i build-in Windows tools (bcdedit.exe, fsutil.exe, vssadmin.exe), shenja të përdorimit të papritur të remote monitoring and management software (RMM) ose të prezencës së Cobalt Strike beacon/client, ekzekutime të papritura të Powershell, shërbime të krijuara së fundmi ose software të instaluara së fundmi, si dhe shenja potenciale që të dhënat janë nxjerrë nga rrjeti.
b. Për ambientet cloud duhet të aktivizohen tools të cilat detektojnë dhe preventojnë modifikime tek IAM, burimeve të mbrojtjes së të dhënave dhe sigurisë së rrjetit. Të përdoret automatizimi për të detektuar probleme të përgjithshme dhe marrjen e masave të menjëhershme.

Reporting and Notification / Raportimi dhe Njoftimi

Të ndiqen kërkesat e njoftimit sipas planit të incident response dhe kuminikimit të organizatës për të përfshirë skuadrat e brendshme dhe të jashtme në mënyrë që të ndihmojnë për zvogëlimin, response dhe rikuperimin nga incidenti. Informacioni në dispozicion duhet të shpërndahet në mënyrë që të merret asistenca e nevojshme.

Containment and Eradication / Frenimi dhe Zhdukja

a. Në qoftë se nuk është e mundur për veprime mitigimi fillestare atëherë duhet marrë një mostër e pajisjeve të afektuara nëpërmjet memory capture dhe system image, si dhe të mblidhen logs së bashku me indikatorë të tjerë të kompromisit.
b. Të ruhet evidenca e cila është tepër e paqëndrueshme ose e limituar në mbajtje në mënyrë që të parandalohet humbja ose ngatërresa në logs etj.
c. Të studiohet për variantin e ransomware dhe të ndiqen hapa të mëtejshëm të rekomanduar për të identifikuar dhe frenuar sistemet ose rrjetet e impaktuara.
d. Të identifikohen sistemet dhe account-et e përfshira në sulmin fillestar (mund të përfshijë account-et e email), dhe bazuar në detajet e ekzaminuara të kompromisit ose sulmit, të mbidhen sistemet e asociuara të cilat mund të përdoren më tej për përdorim të vazhdueshëm të aksesit të paautorizuar. Gjithashtu të çaktivizohen VPN, remote access servers, cloud-based assets.

Në qoftë se të dhënat janë të enkriptuara në server nga një workstation i infektuar, atëherë duhet të ndiqen hapat e mëposhtëm:

e. Rishikim i Computer Management ->Sessions dhe Open Files lists. Nëpërmjet këtyre hapave mund të përcaktohet user-i ose sistemi i cili i akseson file-t e enkriptuara.
f. Rishikim i file properties i file-ve të enkriptuara për të identifikuar user-a specifik të cilët mund të jenë të asociuar më pronësinë e file-it.
g. Të rishikohet `TerminalServices-RemoteConnectionManager` event log për të kontrolluar për lidhje RDP në rrjet të suksesshme.
h. Të kontrollohen Windows Security log, SMB event logs dhe logs të tjera të cilat mund të identifikojnë evente aksesi ose autentikime të rëndësishme. Të ekzekutohen software për

packet capture, sic është Wireshark, në serverin e impaktuar, me një filter për të identifikuar adresat IP të përfshira në shkrimin dhe riemërimin e file-ve.
i. Të kryhen analiza të zgjeruara për të identifikuar mekanizma persistence outside-in dhe inside-out. Identifikimi mund të përfshijë vendosjen e EDR solutions, auditimin e local dhe domain accountsm, ekzaminimin e të dhënave të gjetura në centralized logging systems etj.
j. Outside-in përfshijnë aksesin e autentikuar tek sistemet e jashtme nëpërmjet backdoors në perimetrat e sistemit, shfrytëzimit të vulnerabiliteteve të jashtme etj.
k. Inside-out përfshinë malware implants në rrjetin e brendshëm ose një varietet të modifikimeve të ndryshme nëpërmjet përdorimit të software-ve të penetration testing, Powershell etj.
l. Të rindërtohen sistemet duke u bazuar në prioritizimin e shërbimeve kritike
m. Të vendosen passwordresets për të gjithë sistemet e impaktuara dhe të adresohet cdo vulnerabilitet ose hapësirë i asociuar, nëpërmjet përditësimit të software dhe patch application.
n. Autoriteti i sigurisë së IT deklaron në qoftë se incidenti ransomware ka përfunduar duke u bazuar në një kriter të vendosur.

Recovery and Post-Incident Activity / Rikuperim dhe veprimet post-incident

o. Rilidhja e sistemeve dhe restaurimi i të dhënave nga backups offline dhe të enkriptuara bazuar në prioritizimin e shërbimeve kritike.
p. Dokumentimi i informacionit të nxjerrë nga incidenti dhe aktivitetet e response për të përmirësuar planet, procedurat dhe politikat e organizatës.