WATCHCOM
A COMBITECH COMPANY

TJENESTENEKTANGREP

WHITEPAPER V1.0 – 06.09.2022

Forfatter: Frank Haugnes, Senior Information Security Specialist, Watchcom Security Group

Innholdsfortegnelse

Den russiske "hackergruppa" Killnet varslet den 29.06.2022 på sin telegramkanal at de har til hensikt å angripe Politiet, BankID, ID-porten hos Difi, NAV, UDI, Digitaliseringsdirektoratet og flere andre norske nettsider og nettjenester. Killnet er en kjent prorussisk aktør, og disse har (sammen med flere andre russisk statsstøttede "hackergrupper") over tid stått bak en rekke tjenestenektangrep mot statlige og private virksomheter i flere land til støtte for invasjonen av Ukraina. Også i Norge har det blitt rapportert om en rekke tjenestenektangrep, men det har så langt ikke blitt rapportert om alvorlige konsekvenser. Antagelig det er bare et tidsspørsmål før kritiske systemer eller tjenester blir berørt.

"Vi anmoder forsvarere av kritisk infrastruktur til å være forberedt og forsøke å redusere muligheten for potensielle cyberangrep ved å skjerpe sitt cyberforsvar, og øke sin evne til å identifisere mistenkelig aktivitet", uttalte etterretningstjenestene til USA, Storbritannia, Canada, Australia, og New Zealand i en felles uttalelse i april. "NSM ønsker nå at virksomheter forsikrer seg om at de klarer å håndtere tjenestenektangrep." sier NSM på sin nettside om tiltak for å unngå tjenestenektangrep.

1 Hva er tjenestenekt?

Tjenestenekt (Denial of Service, DoS) er en teknikk der en trusselaktør gjør et forsøk på å forstyrre de normale aktivitetene til et bestemt angrepsmål (f.eks. nettside, server, nettverk, Internet of Things-enhet) ved å overbelaste det med forespørsler. Det overordnede målet er å gjøre angrepsmålet utilgjengelig for legitime forespørsler fra brukere. **Distribuert tjenestenekt** (Distributed Denial of Service, DDoS) legger til et kompleksitetsnivå ved å introdusere trafikkflom fra flere kilder, f.eks. fra et "botnet". Et "botnet" består av mange kompromitterte enheter på Internett som, ved bruk av skadevare, blir fjernstyrt til å iverksette angrepet. Disse enhetene kalles "zombier", og de kontrolleres fra en Command and Control (C&C) server (se Fig. 1). Denne aktiviteten, som er i større skala en DoS, gjør det mye vanskeligere å stoppe og svært vanskelig å skille legitim brukertrafikk fra ondsinnet trafikk.

Slike angrep kan koste en virksomhet både tid og penger mens ressursene og tjenestene deres er utilgjengelige.

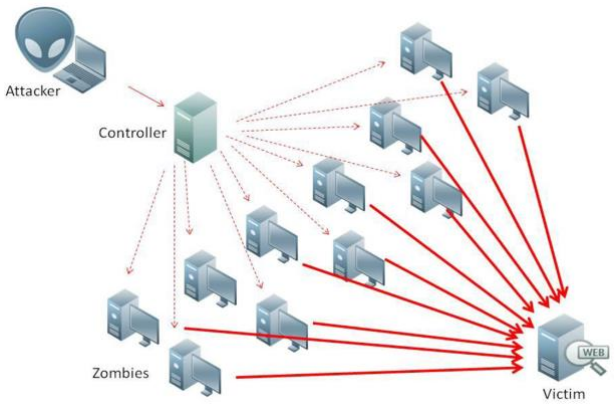

Fig. 1 – DDoS-angrep
Kilde: Wikimedia Commons

2 Teknikker for tjenestenektangrep

Det finnes mange forskjellige metoder for å utføre et tjenestenektangrep. Den vanligste angrepsmetoden er at en angriper sender flere forespørsler til målserveren, og overbelaster den med trafikk. Disse forespørslene er illegitime og har falske returadresser, noe som "villeder" serveren når den prøver å autentisere forespørselen. Siden de illegitime forespørslene behandles konstant blir serveren "overveldet", noe som forårsaker tjenestenekt for legitime forespørsler.

2.1 Ofte brukte taktikker og teknikker

Rammeverket MITRE ATT&CK ble opprettet av MITRE i 2013 som et verktøy for å dokumentere angrepstaktikker og -teknikker basert på virkelige observasjoner. Dette rammeverket har med tiden blitt en velkjent kunnskapsbase for sikkerhetsbransjen for å forstå angrepsmodeller, metoder og mottiltak. Rammeverket utvikles fortløpende med endringene i trussellandskapet.

Idéen bak rammeverket er at alle cyberangrep følger gitte faser:

Fig. 2 – Faser for cyberangrep

Rammeverket definerer hvilke teknikker angriperen benytter i hver fase, og denne informasjonen brukes som grunnlag for utvikling av spesifikke trusselmodeller og metoder. Målet med rammeverket er å bedre kunne detektere angrep eller kompromittering ved å illustrere hvilke aktiviteter en angriper kan ha gjennomført:

- Hvordan kom angriperen seg inn?
- Hvordan beveger de seg rundt i IT-systemene?

I MITRE ATT&CK er det definert to hovedteknikker av tjenestenekt - **Network Denial of Service** og **Endpoint Denial of Service**.

2.1.1 Network Denial of Service

T1498 - *Network Denial of Service (DoS)* er definert som "angrep for å forringe eller blokkere tilgjengeligheten til en utvalgt ressurs". Teknikken har to underteknikker definert:

- T1498.001 - Direct Network Flood
- T1498.002 - Reflection Amplification

Eksempler på ressurser som angripes inkluderer spesifikke nettsteder, e-posttjenester, DNS og nettbaserte applikasjoner.

Et *Network DoS* oppstår når båndbreddekapasiteten til et systems nettverkstilkoblinger er oppbrukt på grunn av volumet av illegitim trafikk rettet mot ressursen eller nettverkstilkoblingene og nettverksenhetene ressursen er avhengig av. For eksempel kan en angriper sende 10 Gbps trafikk til en server som har en 1 Gbps-tilkobling til Internett.

2.1.2 Endpoint Denial of Service

T1499 - *Endpoint Denial of Service (DoS)* er definert som "angrep for å forringe eller blokkere tilgjengeligheten til en tjeneste for brukere." Teknikken har fire underteknikker definert:

- T1499.001 - OS Exhaustion Flood
- T1499.002 - Service Exhaustion Flood
- T1499.003 - Application Exhaustion Flood
- T1499.004 - Application or System Exploitation

Et *Endpoint DoS* hindrer tilgjengeligheten til en tjeneste uten å overbelaste nettverket som tjenesten ligger på.

Angriperen kan rette angrepet mot ulike lag i systemet som brukes til å levere tjenesten. Disse lagene inkluderer operativsystemene (OS), serverapplikasjoner som webservere, DNS-servere, databaser og de (vanligvis nettbaserte) applikasjonene som ligger på toppen av dem. Hvert lag krever ulike angreps-teknikker som utnytter flaskehalser som er unike for de respektive komponentene.

Se Vedlegg 1 for en detaljert oversikt over vanlige typer tjenestenektangrep.

3 Trusselaktørene

Flere typer trusselaktører gjennomfører tjenestenektangrep for diverse formål og for å støtte andre ondsinnede aktiviteter, inkludert distraksjon, hacktivisme og utpressing.

- **Statlige trusselaktører** - er ofte motivert av geopolitisk interesser.
- **Statsstøttede trusselaktører og APT-grupper** – er ofte motivert av militære, økonomiske eller politiske interesser.
- **Organiserte kriminelle** – er ofte motivert av økonomiske interesser.
- **Hacktivister** – er ofte ideologisk motiverte.
- **Terrorgrupper** – er ofte motivert av ideologiske, religiøse eller politiske interesser.
- **Script Kiddies (thrill seekers)** – er ofte motivert av behov for tilfredsstillelse og anerkjennelse.
- **Innsidere** - er ofte motivert av misnøye.

Gjennomføring av tjenestenektangrep krever lite eller ingen kompetanse. Hvem som helst kan kjøpe slike angrep som en tjeneste gjennom en såkalt "DDoS-as-a-Service".

Det er ofte kriminelle syndikater som står bak forsyningskjeder for "cybercrime services for sale". Disse tjenestene fortsetter å modnes, og "alle" kan kjøpe de tjenestene som trengs for å utføre ondsinnet aktivitet for økonomisk vinning eller andre ondsinnede formål.

Figuren nedenfor viser gjennomsnittlig prisnivået for slike tjenester:

Fig. 3 – Gjennomsnittlig prisnivå for "cybercrime services for sale"
Kilde: Microsoft Digital Defense Report - October 2021

3.1 Statlige trusselaktører

Statlige aktører agerer for å understøtte egen stats politiske mål, og retter seg mot institusjoner i andre land for f.eks. å stjele data, forstyrre nasjonal sikkerhet eller kritiske samfunnsfunksjoner, kartlegge og hente inn informasjon, eller skade økonomien. De kan søke tilgang til militære hemmeligheter, begå industrispionasje osv.

Statlige aktører er ofte de mest sofistikerte trusselaktørene, med dedikerte ressurser og personell, og med omfattende planlegging og koordinering. Noen statlige aktører har operative forhold til enheter i privat sektor og organiserte kriminelle, og kan med det avfeie at de står bak en cyberoperasjon.

I figuren nedenfor ser vi fordelingen av angrep fra statsaktører pr. opphavsland for perioden juli 2020-Juni 2021.

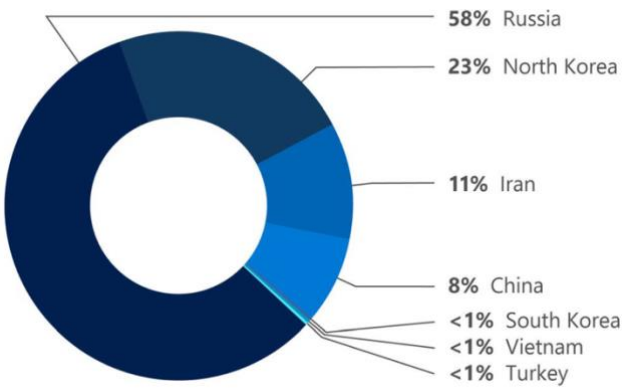

Fig. 2 – Angrep pr. opphavsland
Kilde: Microsoft Digital Defense Report - October 2021

Trusselaktører fra følgende russiske statlige organisasjoner har gjennomført ondsinnede cyberoperasjoner mot IT- og/eller OT-nettverk:

- Russian Federal Security Service (FSB), inkludert FSB's Center 16 og Center 18
- Russian Foreign Intelligence Service (SVR)
- Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS)
- GRU's Main Center for Special Technologies (GTsST)
- Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)

Vi bør være forberedt på cyberangrep også fra denne gruppen aktører, som har hensikt å skade norsk infrastruktur og norske virksomheter f.eks. som følge av hevnaksjoner etter norsk involvering i internasjonale konflikter og sanksjoner.

3.2 Statsstøttede trusselaktører og APT-grupper

Disse trusselaktørene er "kontraktører" som er oppdragsstyrt og driver cyberoperasjoner betalt av stater. Slike "hackergrupper" tar side i en konflikt og kan operere på vegne av myndigheter, og som med makt forsøker å få ulovlig tilgang til systemene til myndighetsorganer eller industri-virksomheter for å stjele, skade og/eller endre informasjon.

Statsstøttede aktører er ofte tilsvarende sofistikerte som statlige aktører.

Det er også kjente tilfeller der sofistikerte statsstøttede trusselaktører har blitt benyttet for å gi inntekter til staten, f.eks. Nord-Korea og Iran. Felles for disse landene er at de har reduserte inntekter på grunn av internasjonale sanksjoner, og dermed tyr til kriminell aktivitet for å øke sine inntekter.

Det er god grunn til å anta at denne gruppen gjennomfører cyberangrep også mot norske mål.

3.3 Organiserte kriminelle

Organiserte kriminelle er i stor grad profittdrevne og representerer en langsiktig, global og felles trussel. De går målrettet etter data for å selge, holde for løsepenger, eller på annen måte utnytte for (egen) økonomisk gevinst. Organiserte kriminelle kan jobbe individuelt eller i grupper for å oppnå sine mål.

Organiserte kriminelle er generelt sett vurdert til å være moderat sofistikert sammenlignet med stater og statsstøttede trusselaktører. Likevel har de planleggings- og støttefunksjoner i tillegg til spesialiserte tekniske kapasiteter som påvirker et stort antall ofre.

3.4 Hacktivister

Hacktivisme defineres som individer eller grupper som bruker "hacking" for å påvirke politiske eller sosiale endringer - dette er cyberkriminelle med en politisk intensjon. Det hacktivistiske landskapet er mangfoldig, og omfatter en rekke individer og grupper på ulike nivåer av ferdigheter og evner. Hacktivister er kjent for å bruke skadelig programvare, DDoS-angrep, "doxing", defacing av nettsider og sosiale medier for å avsløre inkriminerende informasjon om målet deres; alt fra "urettferdig" forretningspraksis til hemmelighold av myndighetene. Den mest kjente activist/hacktivist-gruppen er Anonymous.

En rekke uavhengige "hackergrupper" kan være sympatisører som på eget initiativ gjennomfører cyberangrep mot nasjonale mål. Disse trusselaktørene velger sine mål ut fra eget forgodtbefinnende, og hvem som helst kan derfor bli truffet.

3.5 Terrorgrupper

Cyberterrorister er en moderne mutasjon av et utbredt globalt problem som har plaget de fleste land i flere tiår. Terrorgrupper har ofte ideologiske, religiøse eller politiske motivasjoner. De kan også ha økonomisk motivasjon for å finansiere terrorvirksomhet. Deres cyberaktiviteter er vanligvis begrenset til støtende eller trakasserende aktiviteter, men kan også være forsøk på å forstyrre kritiske tjenester og forårsake skade. Terrorgrupper bruker først og fremst Internett til kommunikasjon og rekruttering.

3.6 Script Kiddies (thrill seekers)

"Script Kiddies" er et nedsettende begrep som brukes for å beskrive en ufaglært person som bruker eksisterende dataskript eller programmer til å angripe datamaskiner, nettverk eller nettsteder, og som mangler ekspertisen til å skrive sine egne.

Denne trusselaktøren er vanligvis ikke så sofistikert, og er ofte avhengig av allment tilgjengelige verktøy som krever lite tekniske ferdigheter å benytte. Handlingene har derav som regel ingen varig effekt, utover omdømme, på angrepsmålene.

3.7 Innsidere

En innsider defineres av NSM *"som en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap."*

Fremmede etterretningstjenester bruker store ressurser på å rekruttere både egne og norske borgere med tilgang til informasjon eller andre verdier som er viktige for deres nasjonale interesser. For å oppnå sine mål leter trusselaktører systematisk etter personer som kan utnyttes eller er villige til å gi dem tilgang til de verdiene de jakter på.

For en virksomhet vil en potensiell innsider være en betydelig risikofaktor. Medarbeidere eller andre som kjenner interne systemer og rutiner ved virksomheten, vil kunne omgå både digitale og fysiske sikkerhetsbarrierer eller sette slike tiltak ut av spill. Dersom virksomheten ivaretar viktige samfunnsfunksjoner, vil innsidevirksomhet kunne ha alvorlige konsekvenser for våre nasjonale sikkerhetsinteresser.

Motivasjonen til innsidere er ofte definert med begrepet "MICE" som er en forkortelse for “Money, Ideology, Compromise, og Ego”. Personer i virksomhetene kan rekrutteres på grunnlag av f.eks. ideologiske eller økonomiske motivasjoner. Press og frykt benyttes også som virkemiddel til rekruttering, f.eks. med trusler mot familie i hjemlandet.

4 Konsekvensene av tjenestenektangrep

Tjenestenektangrep har i seg selv vanligvis et begrenset skadepotensial og få varige konsekvenser. Det medfører støy og driftsforstyrrelser så lenge angrepet pågår, men det tar vanligvis ikke veldig lang tid før angrepet enten blir stoppet (f.eks. av nettverkstjenesteleverandør) eller at angriperen stopper av seg selv.

Store og målrettede angrep på kritisk infrastruktur og angrep som pågår over lang tid vil derimot kunne få langt større konsekvenser. Kritiske tjenester vil kunne berørt, og i enkelte tilfeller satt helt ut av drift i en periode. Dette er spesielt kritisk for tidskritiske tjenester som kan bli forstyrret.

I dekke av et tjenestenektangrep kan også trusselaktører gjennomføre andre type angrep, f.eks. skaffe seg uautorisert tilgang til systemer, legge inn ransomware etc.

5 Tiltak mot tjenestenektangrep

Vi anbefaler våre kunder å se til NSMs Grunnprinsipper for IKT-sikkerhet og i den grad det lar seg gjøre følge disse. Her oppsummerer i pkt. 2.2.7 relevante tiltak for beskyttelse mot tjenestenekt:

"*Etabler en robust og motstandsdyktig IKT-arkitektur som ivaretar tilgjengelighet til kritiske funksjoner og leveranser. a) Gjennomfør risikovurderinger for maskinvare-feil, menneskelige drifts-feil, data-angrep, internett-tilgjengelighet (bl.a. tjenestenekt-angrep), tjenesteleverandør-tilgjengelighet, elektrisitet-tilgjengelighet, naturskade og geopolitisk situasjon. b) Ut i fra resultatene fra risikovurdering og kritikalitet kan deler av IT-løsningen gjøres mer robust. Det kan være tiltak som duplisering av internett-forbindelse, duplisert datasenter på alternativ lokasjon, duplisering av domenekontrollere, delvis tjenesteutsetting, robust (midlertidig) strømforsyning, lager av kritiske reservedeler, mm.*"

5.1 Generelle tiltak og strategier

Vi vil også trekke frem følgende tiltak som kan bidra til å redusere effekten av forsøk på tjenestenektangrep og gi bedre responsevne hvis et tjenestenektangrep skulle lykkes.

- Inngå avtaler med din nettverkstjenesteleverandør og kartlegg hvilken hjelp de kan gi deg i tilfelle av et tjenestenektangrep. Skulle et angrep skje, jo raskere en leverandør kan implementere trafikkblokkeringer og reduksjonsstrategier på sitt nivå, desto raskere vil tjenestene dine bli tilgjengelige for legitime brukere.
- Vurder også å inngå avtaler med selskaper som tilbyr tjenester for beskyttelse mot tjenestenekt. Eks. Microsoft Azure DDoS Protection, Telenor DDoS-beskyttelse.
- Hvis du opplever et tjenestenektangrep, oppgi de angripende IP-adressene til din nettverkstjenesteleverandør slik at de kan implementere begrensninger på sitt nivå. Vær oppmerksom på at Reflection DDoS-angrep vanligvis kommer fra legitime offentlige servere. Det er viktig å undersøke hvem en IP-adresse tilhører når man undersøker nettverkslogger under et angrep. Bruk verktøy som f.eks. American Registry for Internet Numbers (ARIN) for å slå opp IP-adresser som er involvert i angrepet. Hvis ikke kan du risikere å blokkere trafikk fra legitime nettverk eller servere.

- Aktiver brannmurlogging av både akseptert og nektet trafikk for å finne ut hvor angrepet kan komme fra.
- Definer strenge "TCP keepalive" og "maximum connection" på alle perimeterenheter, for eksempel brannmurer og proxy-servere. Denne anbefalingen hjelper til med å forhindre at SYN Flood-angrep blir vellykket.
- Vurder port- og pakkestørrelsesfiltrering hos nettverkstjenesteleverandøren.
- Etabler og regelmessig valider "baseline" trafikkmønstre (volum og type) for Internett-eksponerte tjenester.
- Installer alle tilgjengelige sikkerhetsoppdateringer (patcher) fra leverandører etter å ha testet de.
- Foreta herding av (minimum) alle Internett-eksponerte enheter iht. CIS Benchmarks.
- Konfigurer brannmurer til minimum å blokkere innkommende trafikk fra IP-adresser som er reservert (0/8), loopback (127/8), private (RFC 1918 blocks 10/8, 172.16/12, og 192.168/16), ikke-tilordnede DHCP-klienter (169.254.0.0/16), multicast (224.0.0.0/4) og ellers oppført i RFC 5735. Denne konfigurasjonen bør også forespørres på nettverkstjenesteleverandør-nivå.
- Juster Internett-eksponerte serverprosesser for å tillate et minimum av prosesser eller tilkoblinger som er nødvendig for virksomhetsformål.
- Konfigurer brannmurer og IPS/IDS (inntrengningsforebyggende/-detekterende) enheter for å varsle om trafikkavvik.
- Konfigurer brannmurer til bare å akseptere trafikk som er beskrevet i virksomhetens sikkerhetspolicy og som kreves for virksomhetsformål.
- Vurder å sette opp Out-of-Band-tilgang, Internett og telefoni til et dedikert rom for hendelseshåndtering for å sikre kommunikasjon i tilfelle av et tjenestenektangrep som forstyrrer normal tilkobling.

6 Referanser

MITRE ATT&CK®
https://attack.mitre.org/

NSM - Tiltak for å unngå tjenestenektangrep
https://nsm.no/aktuelt/tiltak-for-a-unnga-tjenestenektangrep

NSM - Grunnprinsipper for IKT-sikkerhet
https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt

Vedlegg 1 – Vanlige tjenestenektangrep*

I tabellen nedenfor er en del av de vanligs forekommende teknikkene for tjenestenektangrep beskrevet.

Attack	Description
Direct Network Floods	Direct Network Floods are when one or more systems are used to send a high-volume of network packets towards the targeted service's network. Almost any network protocol may be used for flooding. Stateless protocols such as UDP or ICMP are commonly used but stateful protocols such as TCP can be used as well.
Reflection Attack	Adversaries may attempt to cause a denial of service (DoS) by reflecting a high-volume of network traffic to a target. This type of Network DoS takes advantage of a third-party server intermediary that hosts and will respond to a given spoofed source IP address. This third-party server is commonly termed a reflector. An adversary accomplishes a reflection attack by sending packets to reflectors with the spoofed address of the victim.
Reflection Amplification Attack	Reflection attacks often take advantage of protocols with larger responses than requests in order to amplify their traffic, commonly known as a Reflection Amplification attack. Adversaries may be able to generate an increase in volume of attack traffic that is several orders of magnitude greater than the requests sent to the amplifiers. The extent of this increase will depending upon many variables, such as the protocol in question, the technique used, and the amplifying servers that actually produce the amplification in attack volume. Two prominent protocols that have enabled Reflection Amplification Floods are DNS[2] and NTP[3], though the use of several others in the wild have been documented.[4] In particular, the memcache protocol showed itself to be a powerful protocol, with amplification sizes up to 51,200 times the requesting packet.
SYN Flood	With SYN floods, excessive amounts of SYN packets are sent, but the 3-way TCP handshake is never completed. Because each OS has a maximum number of concurrent TCP connections that it will allow, this can quickly exhaust the ability of the system to receive new requests for TCP connections, thus preventing access to any TCP service provided by the server.

Attack	Description
ACK Flood	ACK floods leverage the stateful nature of the TCP protocol. A flood of ACK packets are sent to the target. This forces the OS to search its state table for a related TCP connection that has already been established. Because the ACK packets are for connections that do not exist, the OS will have to search the entire state table to confirm that no match exists. When it is necessary to do this for a large flood of packets, the computational requirements can cause the server to become sluggish and/or unresponsive, due to the work it must do to eliminate the rogue ACK packets. This greatly reduces the resources available for providing the targeted service.
HTTP Flood	A simple HTTP flood is where an adversary sends a large number of HTTP requests to a web server to overwhelm it and/or an application that runs on top of it. This flood relies on raw volume to accomplish the objective, exhausting any of the various resources required by the victim software to provide the service.
SSL Renegotiation	A SSL renegotiation attack, takes advantage of a protocol feature in SSL/TLS. The SSL/TLS protocol suite includes mechanisms for the client and server to agree on an encryption algorithm to use for subsequent secure connections. If SSL renegotiation is enabled, a request can be made for renegotiation of the crypto algorithm. In a renegotiation attack, the adversary establishes a SSL/TLS connection and then proceeds to make a series of renegotiation requests. Because the cryptographic renegotiation has a meaningful cost in computation cycles, this can cause an impact to the availability of the service when done in volume.
Exploit software vulnerabilities	Adversaries may exploit software vulnerabilities that can cause an application or system to crash and deny availability to users. Some systems may automatically restart critical applications and services when crashes occur, but they can likely be re-exploited to cause a persistent denial of service (DoS) condition.
Exploit known or zero-day vulnerabilities	Adversaries may exploit known or zero-day vulnerabilities to crash applications and/or systems, which may also lead to dependent applications and/or systems to be in a DoS condition. Crashed or restarted applications or systems may also have other effects such as Data Destruction, Firmware Corruption, Service Stop etc. which may further cause a DoS condition and deny availability to critical information, applications and/or systems.

**Kilde: MITRE ATT&CK® Techniques*