



SÖDERTÖRNS TINGSRÄTT
Avdelning 3

DOM
2022-06-23
meddelad i
Huddinge

Mål nr: B 7397-22

PARTER (Antal motparter: 1)

Motpart

Inferno Solutions, -
Pskovskaya Str 32A, 4H
190121 St Petersburg
Ryssland

Sökande

Kammaråklagare Johanna Kolga
Åklagarmyndigheten
Riksenheten mot internationell och organiserad brottslighet
Box 57
101 21 Stockholm

DOMSLUT

Förverkande och beslag

I beslag tagen egendom förklaras förverkad. Beslaget ska bestå (Beslagsliggare 2021-5000-BG58395 p 1).

Om domstolens behandling av personuppgifter, se www.domstol.se/personuppgifter. Kontakta oss för information på annat sätt.

Besöksadress
Björnkullavägen 5 A

Öppettider
måndag - fredag
08:30-16:00

Postadress
141 84 Huddinge

E-post
sodertorns.tingsratt.avdelning3@dom.se

Telefon
08-561 660 30

Webbplats
www.sodertornstingsratt.domstol.se

Avdelning 3

YRKANDEN M.M.

Åklagaren har begärt att en i beslag tagen hårddisk ska förklaras förverkad med stöd av 36 kap 2 § brottsbalken under åberopande av att hårddisken har använts som hjälpmedel vid brott. Åklagaren har till stöd för sin talan anfört det som följer av *bilaga 1*.

Inferno Solutions har bestritt yrkandet och anfört att de vill få tillbaka hårddisken efter att den blivit raderad på information samt gjort gällande att det finns metoder som kan säkerställa att all information raderas.

Åklagaren har genmält att det för närvarande saknas säkra raderingsmetoder och att det därför inte kan säkerställas att raderad information inte kan återskapas. Åklagaren har härvid särskilt framhållit det finns barnpornografiskt material på en av de virtuella servrarna som finns på hårddisken.

Målet har avgjorts utan huvudförhandling.

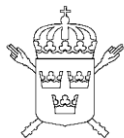
DOMSKÄL

Ett förverkande får, såvitt nu är av intresse, beslutas beträffande egendom som har använts som hjälpmedel vid brott enligt bl.a. brottsbalken om det behövs för att förebygga brott eller om det annars finns särskilda skäl, se 36 kap. 2 § brottsbalken. Utifrån den information som åklagaren har lämnat finner tingsrätten att förutsättningarna för ett förverkande av nu aktuell egendom är uppfyllda.

HUR MAN ÖVERKLAGAR, se *bilaga 2* (TR-02)

Överklagande, ställt till Svea hovrätt, ska ha inkommit till tingsrätten senast den 14 juli 2022.

Erik Högdahl



Södertörns tingsrätt

SÖDERTÖRNS TINGSRÄTT
Avdelning 3

INKOM: 2022-05-09
MÅLNR: B 7397-22
AKTBIL: 1

Särskild talan**I beslag tagen egendom tillhörande:**

Inferno Solution
Pskovskaya Str 32A, 4H
190121
Saint Petersburg
RUSSIAN FEDERATION

Särskilt yrkande

Det yrkas att i beslag tagen egendom, en hårddisk, förverkas. Det yrkas att beslaget ska bestå (2021-5000-BG58395 p 1).

Bakgrund*1.1 Anonymt tips*

I slutet av april 2021 inkom ett anonymt tips till Polismyndigheten som uppgav att en rysk kriminell hackergruppering, TA505/FIN11, använde sig av en C2-server (Command and control) placerad i Sverige för att begå dataintrång.

Polisen kunde bekräfta uppgifterna som fanns i tipset och konstatera att servern stod hos hostingbolaget Glesys Internet Services AB [Glesys] i Stockholm. Glesys sköter serverdriften åt sina kunder.

1.2 Förundersökning inleds

En förundersökning gällande grovt dataintrång inleddes och den 10 maj 2021 genomfördes en husrannsakan där aktuell server togs i beslag. I förhör med företrädare för Glesys framkom att servern ägs av Webhostingboaget Inferno solutions. Inferno solutions är ett ryskt hostingbolag. Inferno solution hyr in sig hos Glesys, där Glesys tillhandahåller lokal med plats, ström, kylning och internetuppkoppling. Inferno Solutions hyr sedan ut plats på själva serverarna till sina slutkunder. Innehållet på serverarna och vilka slutkunder som finns har inte Glesys insyn i.

Det är i dagsläget inte möjligt för svensk polis att komma vidare med att få fram uppgifter på vem eller vilka som ligger bakom grupperingen TA505/FI1 och som ska anses vara gärningsmän till aktuell brottslighet. Utredning om detta pågår i ett flertal länder runt om i Europa.

1.3 Grupperingen (TA505/FIN11)

TA505/FIN11 är en väletablerad rysk hackergruppering som begår grova dataintrång/hackerattacker mot privatpersoner, företag och myndigheter över

hela världen. De ses främst en finansiellt motiverad hotaktör, men som bedöms även genomföra statligt sponsrade uppdrag.

Etablerade IT-säkerhetsföretag världen över bedömer TA505 som ett stort och mycket allvarligt cybersäkerhetshot. Deras aktivitet kan spåras tillbaka till åtminstone 2014 och de anses vara mycket skickliga och mångsidiga. De använder både skadlig kod som utvecklas av andra, men har även förmåga att utveckla egen för att genomföra hackerattacker.

TA505, mer än någon annan känd hotaktör, är kända för att sina massiva e-postkampanjer i syfte att sprida skadlig kod. De attackerar brett över alla branscher över hela världen där de bland annat skapar access till system och nätverk, stjälar information, tar kontroll över och fjärrstyr målsägandes datorer och planterar ransomware för att begära lösensummor i miljonbelopp.

De har varit aktiva under covid 19 pandemin där de fokuserat ransomware-attacker mot sjukvårdsinrättningar. TA505 bedöms i närtid även ligga bakom attacker mot kritisk infrastruktur, oljebolag, säkerhetsfirmor, banker, advokatkontor, universitet med mera. De bedöms vara inblandade i attacker mot flera företag på Fortune 500-listan som består av de 500 största bolagen i USA.

1.4 Analys av server i beslag

Den initiala analysen av servern i beslag visade att den fysiska servern användes för att hosta (vara värd åt) 134 st virtuella servrar. En virtuell server är en metod att dela upp en fysisk serverdator i flera delar. Genom programvara som körs på den fysiska servern skapar man en virtuell maskin på vilket man kan köra ett operativsystem och önskad programvara. Dessa virtuella servrar är skilda från varandra och kan ha olika kunder. Polisens analys har också visat att Inferno solutions, förutom deras slutkunder, haft tillgång till innehållet på dessa servrar.

Bearbetning och analys av de virtuella servrarna visar på ett mycket stort antal målsägande gällande grova dataintrång där man fått sin personliga, mycket känsliga data stulen, samt skadlig kod installerat som möjliggör för en hotaktör att kontrollera målsägandes dator. På en specifik virtuell server, namngiven 37.252.9.122, konstaterades mer än 25 000 målsägande som blivit drabbade i över 70 länder. Denna virtuella server, tillsammans med två andra, bedöms kontrolleras av TA505.

På en annan virtuell server fanns material som bedöms vara stulet från ett stort företag i ett land i Afrika som arbetar med känslig infrastruktur. Företaget i fråga är landets största privata aktör inom jordbruk, energi, infrastruktur och livsmedelsindustri.

Minst tretton av de virtuella serverna innehåller mjukvara och script som polisen bedömer används av hotaktörer för att begå dataintrång och serverna själva utgör en del av en större IT-infrastruktur som nyttjas av kriminella grupperingar. Ytterligare fem virtuella servrar används sannolikt för utskick av så kallade phishing-mail som är första steget i ett dataintrång i många hackerattacker.

På en av de virtuella serverna har dokumenterat sexuell övergrepp på barn påträffats. Servern innehåller även en tjänst där användare kan registrera sig för att köpa och sälja filer med kryptovaluta. Bland annat saluförs flertalet filer med lösenord som uppges låsa upp filarkiv som ska innehålla barnpornografiskt material. De utpekade filarkiven har ej påträffats på den aktuella servern, utan det är lösenord till försäljning och länkar till filarkiven.

Bland övriga virtuella servrar finns fem som bedöms användas för att sälja olagliga substanser eller ha olika funktionalitet kopplat till cyberbrottslighet. Annan brottslighet som förekommer på andra virtuella servrar kan kopplas till bedrägerier och försäljning av sexuella tjänster.

Förverkandefrågan

Servern som tagits i beslag har använts som hjälpmedel för att begå brott. Den ska förverkas för att det behövs för att förebygga brott (36:2 Brb). Servern ägas av Inferno Solutions som i sin tur hyr ut utrymme på servern till gärningsmännen (36:5 a och b Brb). Ingen kommer att åtalas i Sverige för aktuell brottslighet (1 § i lag (1986:1009) om förfarandet i vissa fall vid förverkande m.m.) varför särskild talan nu väcks (2 § lag (1986:1009) om förfarandet i vissa fall vid förverkande m.m.).

Inferno Solutions har angett att värdet på servern uppgår till 11 975 Euro motsvarande ca 124 000 kr, (se 3 § lag (1986:1009) om förfarandet i vissa fall vid förverkande m.m.).

Förverkandeyrkandet avser hela servern som är i beslag. Utifrån vad som anges ovan är det inte oskäligt att förverka den.

Ett återlämnade av aktuell servern skulle kunna innebära att allt material på servern åter gjordes tillgängligt för gärningsmännen som kan fortsätta sin brottsliga verksamhet.

Bevisning

Anmälan (och PM), fup s. 3-11

PM – beslutsunderlag för förverkande, fup s. 12-35

Beslagsprotokoll, fup s. 161

Faktura från Inferno Solutions, fup s. 125
Förhör med företrädare för Glesys, fup s. 157
Kommunikation med Inferno Solutions, fup s. 108 ff.
Lista på servrar, fup s.36-37

Handläggning

Egendomen är i beslag och eftersom den är av betydande belopp ska frågan om förverkande prövas av rätten enligt 3 § lag (1986:1009) om förfarande i vissa fall vid förverkande m.m.

Målet kan med stöd av 2 § samma lag avgöras utan huvudförhandling.
Förhandling behövs inte med hänsyn till utredningen och jag begär inte att en sådan ska hållas (2 § 1 st).

Det begärs att tingsrätten vid utfärdande av stämning ska förelägga Inferno Solutions att yttra sig vid äventyr av att egendomen annars kan förklaras förverkad (2 § 2 st).

Forum

Beslaget är taget från Glesys på adress Västberga Allé 60, 126 30 Hägersten.

Johanna Kolga



Hur man överklagar

Dom i brottmål, tingsrätt

TR-01

Vill du att domen ska ändras i någon del kan du överklaga. Här får du veta hur det går till.

Överklaga skriftligt inom 3 veckor

Ditt överklagande ska ha kommit in till domstolen inom 3 veckor från domens datum. Sista datum för överklagande finns på sista sidan i domen.

Överklaga efter att motparten överklagat

Om ena parten har överklagat i rätt tid, har den andra parten också rätt att överklaga även om tiden har gått ut. Det kallas att anslutningsöverklaga.

En part kan anslutningsöverklaga inom en extra vecka från det att överklagandetiden har gått ut. Ett anslutningsöverklagande måste alltså komma in inom 4 veckor från domens datum.

Ett anslutningsöverklagande upphör att gälla om det första överklagandet dras tillbaka eller av något annat skäl inte går vidare.

Så här gör du

1. Skriv tingsrättens namn och målnummer.
2. Förklara varför du tycker att domen ska ändras. Tala om vilken ändring du vill ha och varför du tycker att hovrätten ska ta upp ditt överklagande (läs mer om prövningstillstånd längre ner).
3. Tala om vilka bevis du vill hänvisa till. Förklara vad du vill visa med varje bevis.

Skicka med skriftliga bevis som inte redan finns i målet.

Vill du ha nya förhör med någon som redan förhörts eller en ny syn (till exempel besök på en plats), ska du berätta det och förklara varför.

Tala också om ifall du vill att målsäganden ska komma personligen vid en huvudförhandling.

4. Lämna namn och personnummer eller organisationsnummer.
Lämna aktuella och fullständiga uppgifter om var domstolen kan nå dig: postadresser, e-postadresser och telefonnummer.
Om du har ett ombud, lämna också ombudets kontaktuppgifter.
5. Skriv under överklagandet själv eller låt ditt ombud göra det.
6. Skicka eller lämna in överklagandet till tingsrätten. Du hittar adressen i domen.

Vad händer sedan?

Tingsrätten kontrollerar att överklagandet kommit in i rätt tid. Har det kommit in för sent avvisar domstolen överklagandet. Det innebär att domen gäller.

Om överklagandet kommit in i tid, skickar tingsrätten överklagandet och alla handlingar i målet vidare till hovrätten.

Har du tidigare fått brev genom förenklad delgivning, kan även hovrätten skicka brev på detta sätt.

Prövningstillstånd i hovrätten

När överklagandet kommer in till hovrätten tar domstolen först ställning till om målet ska tas upp till prövning.

Om du *inte* får prövningstillstånd gäller den överklagade domen. Därför är det viktigt att i överklagandet ta med allt du vill föra fram.

När krävs det prövningstillstånd?

Brottmålsdelen

I brottmålsdelen behövs prövningstillstånd i två olika fall:

- Den åtalade har dömts enbart till böter.
- Den åtalade har frikänts från ett brott som inte har mer än 6 månaders fängelse i straffskalan.

Skadeståndsdelen

Det krävs prövningstillstånd för att hovrätten ska pröva en begäran om skadestånd. Undantag kan gälla när en dom överklagas i brottmålsdelen, och det är kopplat en begäran om skadestånd till brottet. Då krävs inte prövningstillstånd för skadeståndsdelen om

- det inte krävs prövningstillstånd i brottmålsdelen eller om
- hovrätten meddelar prövningstillstånd i brottmålsdelen.

Beslut i övriga frågor

I de mål där det krävs prövningstillstånd i brottmålsdelen (se ovan), krävs det också prövningstillstånd för sådana beslut som bara får överklagas i samband med att domen överklagas. Beslut som kan överklagas särskilt kräver inte prövningstillstånd.

När får man prövningstillstånd?

Hovrätten ger prövningstillstånd i fyra olika fall.

- Domstolen bedömer att det finns anledning att tvivla på att tingsrätten dömt rätt.
- Domstolen anser att det inte går att bedöma om tingsrätten har dömt rätt utan att ta upp målet.
- Domstolen behöver ta upp målet för att ge andra domstolar vägledning i rättstillämpningen.
- Domstolen bedömer att det finns synnerliga skäl att ta upp målet av någon annan anledning.

Vill du veta mer?

Ta kontakt med tingsrätten om du har frågor. Adress och telefonnummer finns på första sidan i domen.

Mer information finns på www.domstol.se.