DEN ÖKÄNDA HÄSTEN FRÅN TROJA

Det verkar som de flesta västerlänningar har insett att de inte har någon rik släkting i Afrika och att kedjebrev inte längre är att lita på, så nätfiskarna har börjat byta taktik, från att vilja ”investera pengar i ditt land” och att påstå att ”du har ett utstående paket hos Post Nord” och gått över till rena kommandotaktiken.

Nu tycks det vara chefsbrev eller sk ”VD-bedrägerier” som gäller. Nätfiskarna utforskar företaget eller myndigheten och tar reda på organisationens sammansättning och skickar e-brev som låtsas komma från en högre chef, till ekonomiavdelningen och begär utbetalningar. Det har visat sig fungera.

Denna artikel behandlar problemen med skräppost ur flera perspektiv:

- Hur Sunets e-postfilter tar sig an saken
- Statistik om mängden skräppost i världen
- KTHs lösning på skräppost och cybersäkerhet
- Ett lyckat fall där bedragaren kunde gripas
- Föreslagna åtgärder

Chainmail = kedjebrev. Bild: Worldantiques, CC BY-SA 3.0

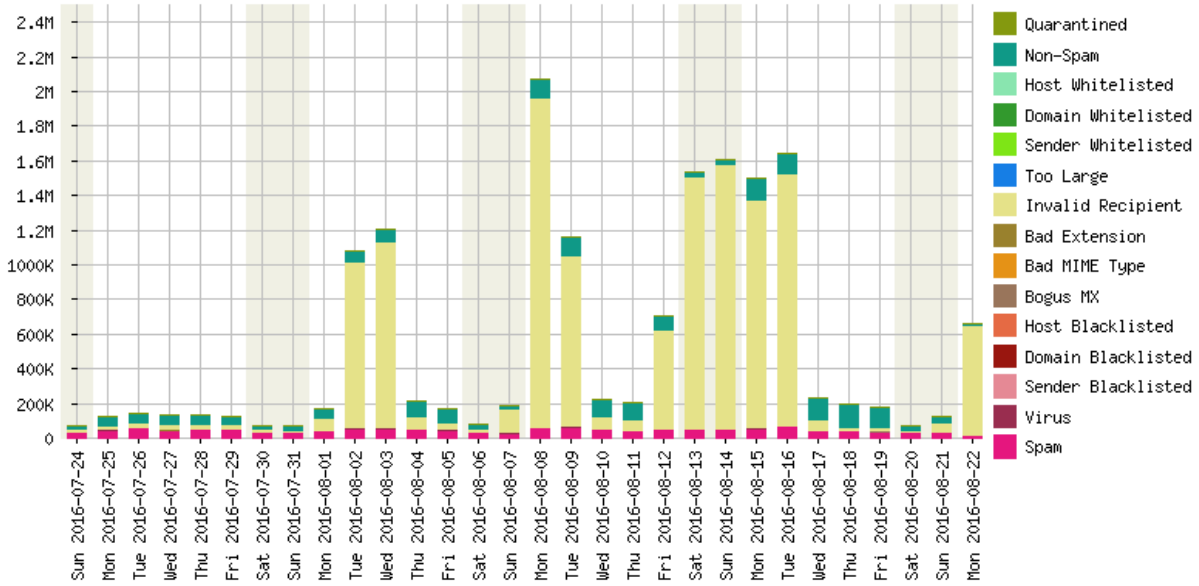
De två allra största IT-företagen i världen som båda sysslar med nyheter och borde ha koll på saken, nämligen Google och Facebook, drabbades när en litauisk man låtsades representera en asiatisk underleverantör och skickade phishing-brev och begärde utbetalningar på sammanlagt 100 miljoner dollar. Han kunde hålla på i två och ett halvt år, utan att någon misstänkte något. Det är social engineering när den är som bäst. Helt vanliga e-brev utan någon som helst brottslig bilaga.

Ransomware-attackerna fortsätter över hela världen och kostar medborgare enorma summor. Ett sjukhus kan få betala tio miljoner dollar för att få tillbaka sina journaler efter att de krypterats av en elak rutin i en e-postbilaga.

SUNETS E-POSTFILTER SLÅR REKORD

De lärosäten som så önskar kan få sin inkommande och utgående e-posttrafik filtrerad mot kända svartlistor på virus, phishing och spam innan de når den egna e-postservern, i form av en sunettjänst. Sanningen är att den allra mesta e-posten, för det mesta mer än 90% är skräp. I mitten av juni 2017 slog filtertjänsten ett nytt rekord på 15 miljoner filtrerade e-brev på en dag och som vanligt slängdes 93% av dem, något under 14 miljoner. Världen producerar alltså cirka 160 skräpbrev i sekunden, avsedda för just SUNETs tjänst.

Filtreringen sker i två steg. Först kontrolleras om brevet är adresserat till en existerande användare på lärosätet. Om inte, kan det raderas direkt om den anslutne så önskar. De resterande breven undersöks för att se om de innehåller ett känt virus eller verkar vara spam i allmänhet. Det märks då i ämnesraden och brevet kan sättas i karantän. Skulle brevets avsändare finnas med på en vitlista kan det släppas igenom ändå.

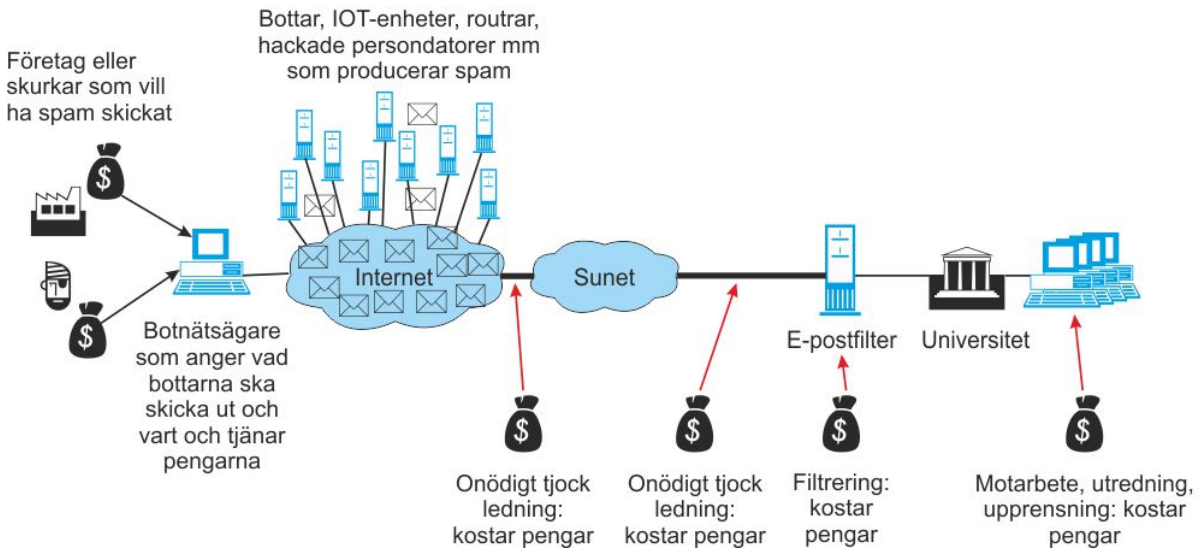


Bilden ovan visar e-poststatistik för en typisk vecka hos Stockholms Universitet. Man kan se att under vissa dagar är 95% av inkomna mail skräp, med huvudsakligen ogiltiga mottagaradresser. Andra dagar kan andelen ha sjunkit till ”bara” 50%. Ändå slinker skadliga brev igenom och orsakar ekonomiska förluster för lärosätena.

FLÖDET

Nittiofem procent! Och vem betalar för det? Du och jag. Sunets e-postfiltertjänst kostar lärosätet 120.000 – 180.000 kronor per år beroende på volymer. Eftersom universitetet är statligt, betalas spamfiltreringen med skattepengar.

Flödet är ganska intressant och en helt fantastisk uppvisning i meningslöshet.



Miljarder spambrev driver omkring på Internet varje dag, och alla ledningar och routrar måste dimensioneras för att kunna ta hand om dem, vilket egentligen är pengar kastade i sjön. Institutioner måste köpa e-postfilter, vilket är skattepengar kastade i sjön. Det skräp som ändå slinker igenom kräver återställningsarbete hos användarna och kan eventuellt förstöra forskningsarbete och liknande, vilket också är skattepengar kastade i sjön. Skulle man känna sig nödgad att betala utpressaren en lösensumma för att få tillbaka sina krypterade filer, är det också pengar kastade i sjön. Mängder av sjukhus och myndigheter drabbas av detta varje dag.

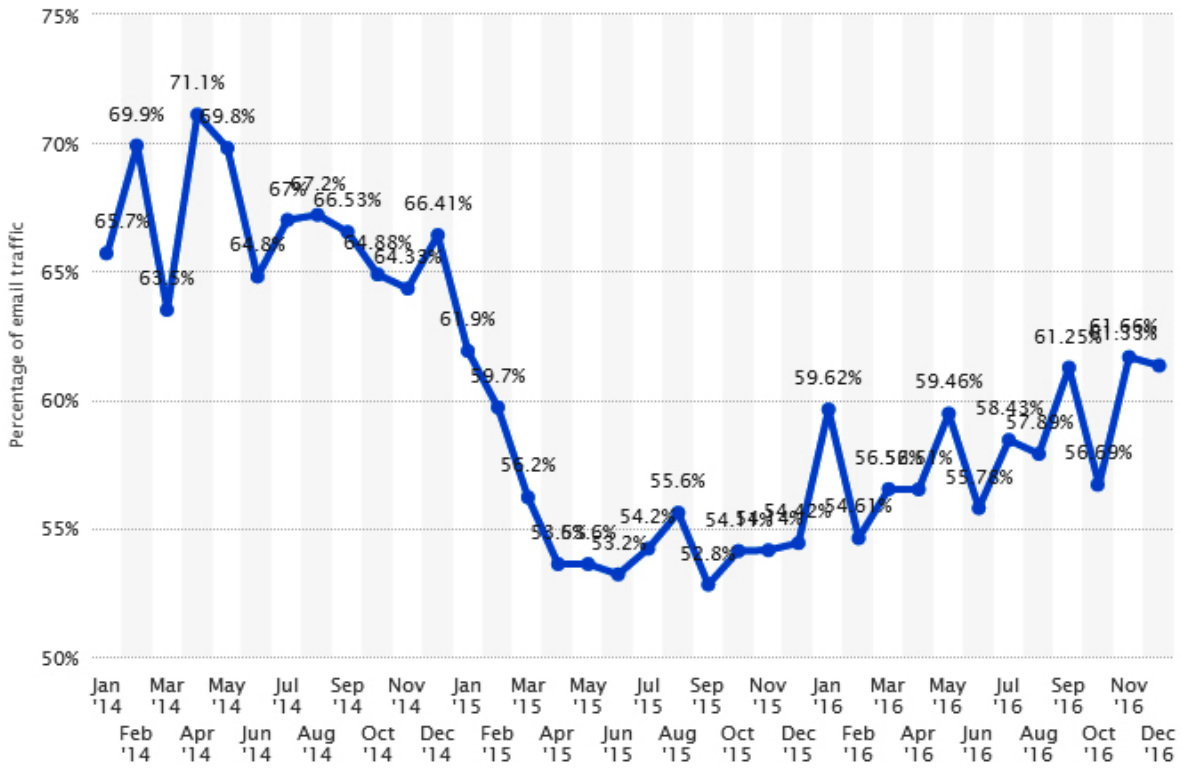
Allt detta ger vid handen att hanteringen är lönsam för botnätsägaren, som blir uppmuntrad och kommer att fortsätta sin verksamhet. Inga polisinsatser i världen tycks kunna motarbeta trenden. Utom en, som vi ska se längre fram i artikeln!

SPAMSTATISTIK

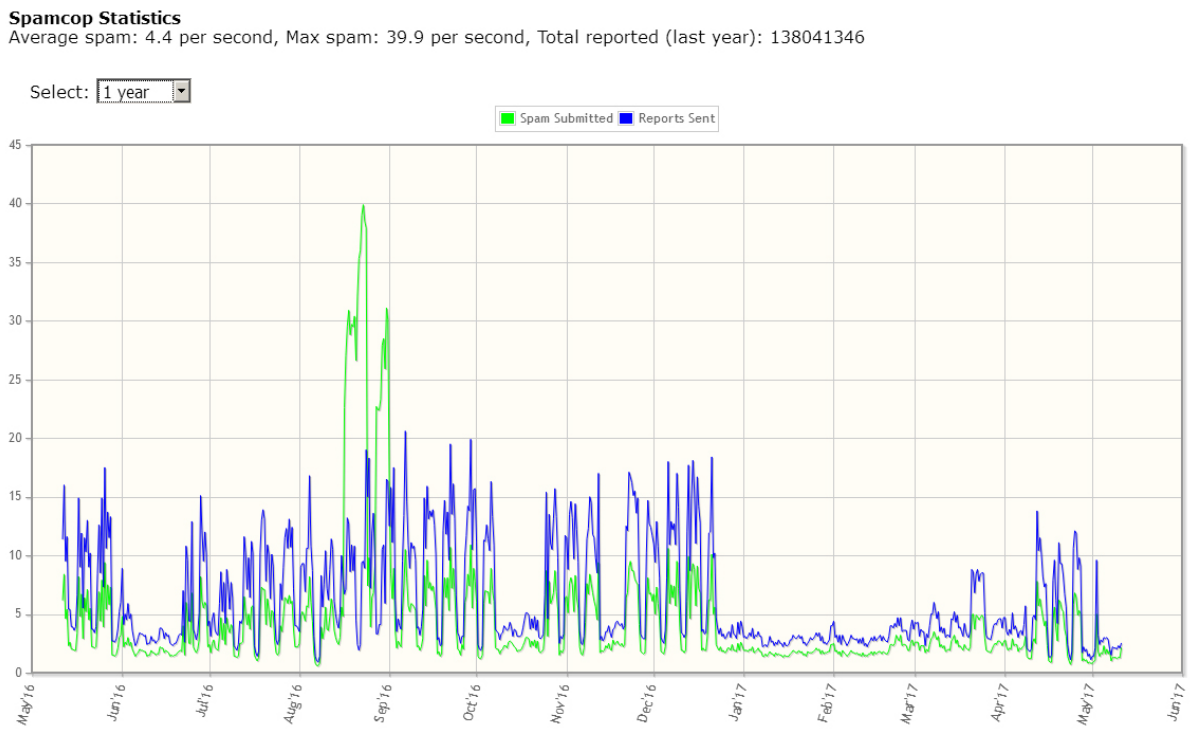
Spammet är som vår tids digerdöd. Det kilar sig in överallt och förgiftar allas inkorgar. De falska profeterna trumpetar sina budskap över oss och människor faller i drösar.

– Bring out your dead!

Heltäckande ansiktsmasker med välluktande kryddor hjälpte inte på 1300-talet och hjälper inte nu. Bara hård kunskap.

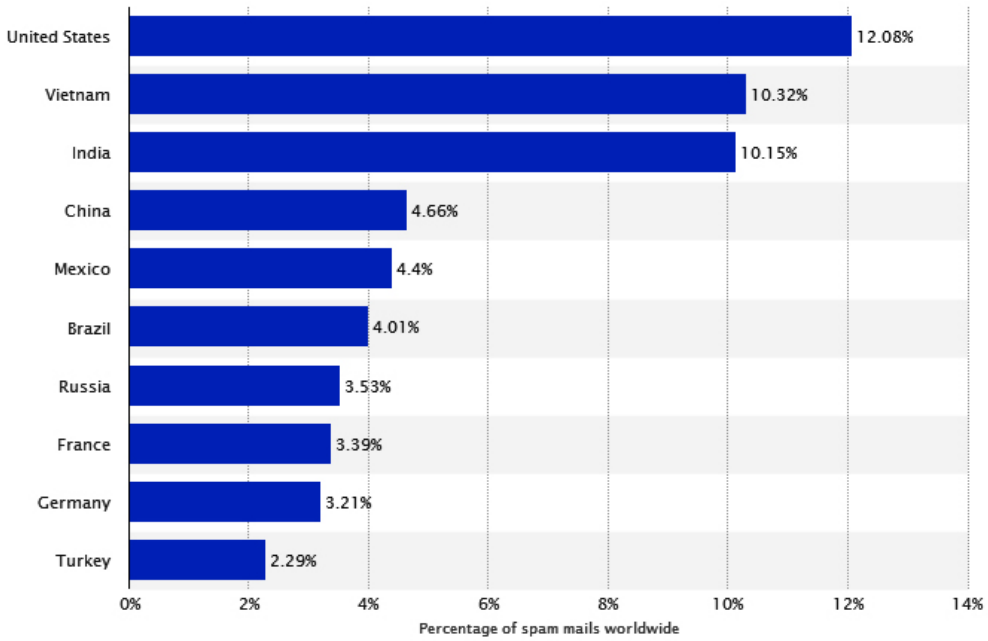


Statista (https://www.statista.com/statistics/420391/spam-email-traffic-share/) visar andelen spam av all världens e-posttrafik, från 2014 och framåt. Spammarna fick sig uppenbarligen en knäck i december 2014, men är på god väg att återta sin framskjutna position.



Spamcop (https://www.spamcop.net/spamstats.shtml) visar följande mängd spambrev från maj 2016 till maj 2017, räknat i miljarder. De menar att det skickas 4,4 spambrev per sekund i normalfallet och 40 brev per sekund i topparna. Det är aningen lite, sett till hur många som SUNETs tjänst får ta hand om.

Statista rapporterar en global volym av 28 miljarder spambrev per dag! Men uppgifterna varierar mellan olika statistiker beroende på när och hur mätningen gjordes.



Spamlaws (http://www.spamlaws.com/spam-stats.html) menar att 14,5 miljarder e-brev per dag är spam och att spammet utgör 45 procent av alla brev. Andra forskningsföretag menar att spammet utgör en större del, uppåt 73 procent. SUNETs tjänst kan påvisa en ännu större förekomst. Den största källan till spammet är USA, medan Korea kommer på andra plats. Den vanligaste typen av spam är annonser, vilka utgör cirka 36 procent av alla spambrev. På andra plats med 31 procent, hamnar pornografiskt material. På tredje plats med 26,5 procent kommer brev med oönskade ekonomiska transaktioner.

Och nu kommer det trista: Enligt Radicati Research Group Inc. (http://www.radicati.com/) kostar spammet företagen omkring 20,5 miljarder dollar årligen i minskad produktivitet och tekniska kostnader. Ett annat företag, Nucleus Research, menar att medelförlusten per anställd per år på grund av spam uppgår till 1934 dollar.

KTH KÖR MED EGEN LÖSNING

Långt ifrån alla lärosäten använder sig av SUNETs e-postfilter. Umeå Universitet köper filtrering av Cisco, medan KTH kör en egen lösning i sin egen datorhall.

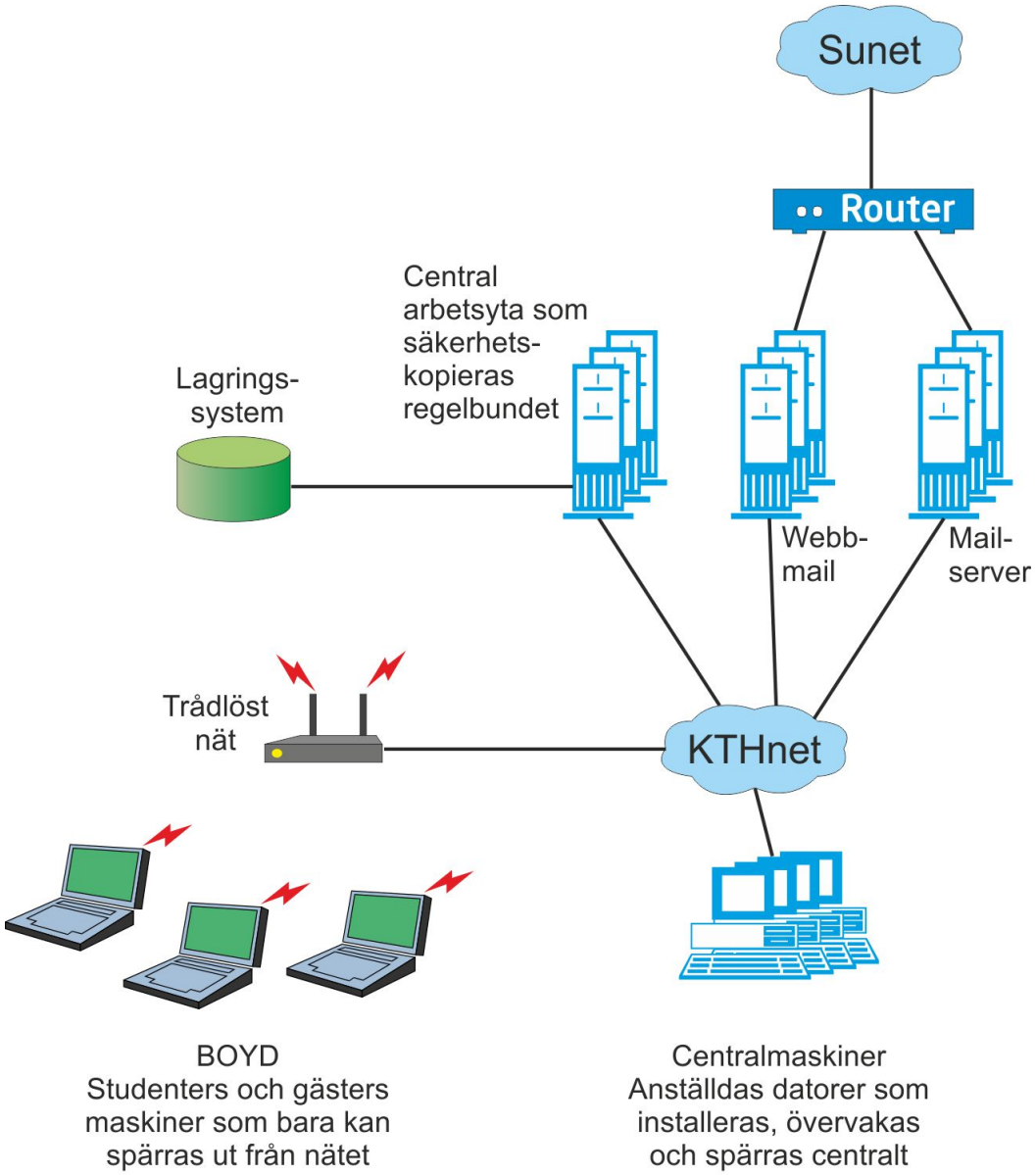
Det kommer typiskt in cirka 2,5 miljoner e-brev till KTH varje dag och ungefär 90% av dem slängs. Återstår 266.000 brev som måste kontrolleras vidare. För att få reda på vad man gör med denna enorma mängd skräp har vi talat med KTHs IT-säkerhetschef Patrik Lidehäll.

Patrik börjar med att förklara att det är ett tudelat system. Först försöker man spärra bort så mycket spam som möjligt, men det hjälper inte till hundra procent så en stor del av arbetet går ut på att hålla efter användarna i efterhand. Anställda ska inte spara sitt arbete lokalt på sin egen dator utan det ska läggas på en server där var och en har en egen arbetsyta. Dessa arbetsytor säkerhetskopieras automatiskt. Det hjälper ändå inte till hundra procent, eftersom smittor kan komma in på andra vägar. Smittade datorer kommer givetvis att tömmas av IT-avdelningen och installeras om. Kan man dekryptera en maskin som blivit krypterad av malware försöker man det, annars blir det formatering.

Datorer som övervakas på detta sätt kallas för centralmaskiner. KTHs IT-avdelning säljer dem, installerar, uppdaterar, övervakar och kan ta tillbaka dem och titta på checksummorna på filerna om de skulle drabbas av en URL, eller utför andra aktiviteter som systemet tycker verkar suspekt.

KTHs system samlar på sig listor med suspekta URL:er och spärrar dem i brandväggen och skulle en användare råka klicka på en sådan, hänvisas denne istället till en intern webbsida där problemet förklaras. Men en URL blir inte suspekt förrän den faktiskt uppträtt en gång och orsakat någon form av suspekt aktivitet som OPS-gruppen kunnat spåra. Därefter hamnar den i listan och alla påföljande klick kommer att resultera i en omdirigering till den ofarliga sidan. Viruskontrollen tar hand om kända ransomware, men det måste gå några dagar tills profilen blivit känd. Huvudsaken är att när IT-avdelningen är alert på ett skadligt brev eller skadlig länk, blir det stopp för alla som försöker klicka på länken i framtiden.

Det finns emellertid metoder som gör det svårt att spärra URL:er. Det förekommer till exempel webbhotell där man kan lägga upp gratissidor, vilket gärna används av skummisar. Dessa webbhotell äger ett helt spann IP-adresser, varför det är svårt att spärra dem alla.



Så här ser miljön i korthet ut på KTH. Centralmaskinerna ska om allt går som det ska, spara allt sitt arbetsdata på en central arbetsyta som säkerhetskopieras, och kan återtas i fall av smitta. IT-avdelningen vet precis var alla maskiner finns och kan gå och hämta dem om det skulle behövas. Men så finns de trådlösa maskinerna, ofta tillhörande studenter och gäster, som inte omfattas av detta system. Dessa får endast varningar vid suspekta URL:er.

Vissa anställda har sin e-post hos en extern leverantör och vill att post som kommer in till KTH skickas vidare till den externa leverantören. Den posten studsar i stort sett bara i KTHs system och skickas vidare. När den anställde sedan hämtas sin webbmail från den externa leverantören kan skräp komma in den vägen.

Nu ökar kraven för att få ha ett konto med avsändare ”kth.se”. Man har infört olika typer av autentisering som gjort ett sådant konto mera attraktivt för bedragare att ha som avsändarkonto. Dessutom strävar olika institutioner mot att ha samma konto för olika funktioner, som ekonomisystem, fakturakontering, VPN-anslutning, e-post och eduroam för att förenkla för användaren, vilket gör kontot än mer attraktivt.

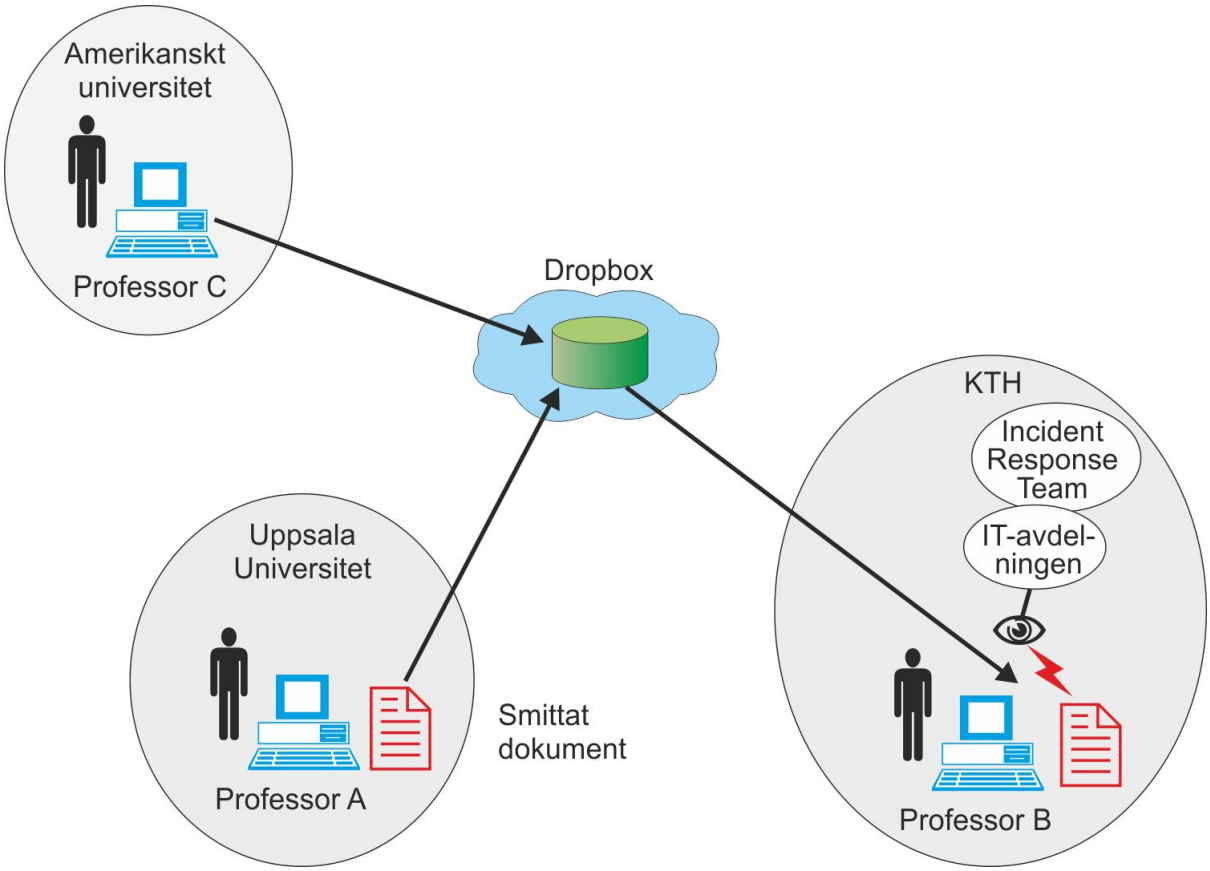
Kom inte hit med dina massutskick. Vi kniper dem. Just precis här!

För att stävja bedrägerier med kapade konton har IT-avdelningen lagt in olika tröskelvärden som ska hindra massutskick. Man upptäcker om någon till exempel försöker skicka 1000 mail, köar utskicket och tar kontakt med avsändaren. Det finns en särskild arbetsgång för skolans olika informationsavdelningar, nämligen att massbrev bara får skickas till en särskild adress vid en särskild tid, då postmaster medger sådana utskick.

Resebokning via webben är ett annat, potentiellt säkerhetshål. Förr bokade man tjänsteresor manuellt via en resebyrå, men det är bortrationaliserat. Om ett åtråvärt KTH-konto kan tas över skulle en bedragare kunna boka resor till vem som helst. Den resande får då beteckningen ”Swedish Government, Other” och det kan vara både bra och dåligt. ”Swedish Government” inger ju förtroende, men upptäcks brottet och Säpo lämnar över listan till exempelvis FBI kan de stå och vänta på skummisarna när de försöker kommer in i USA.

SYNKRONISERA, MEN MED FÖRNUFT

IT-avdelningen har avslöjat än flera sätt för infekterade filer att ta sig in i ett ”rent” system, in på den centrala arbetsytan.



I Uppsala fanns Professor A som lagrade smittade filer på Dropbox. På KTH fanns Professor B som synkade dessa filer mot sin dator. Larmet gick. IT-avdelningen tog kontakt med Patrik som fick ta kontakt med B, som i sin tur inte riktigt visste hur många filer han hade och var de fanns och hur han burit sig åt för att få tag i dem.

Det går ju att tala Professor A till rätta, men hur ska man göra med den okände Professor C på ett berömt amerikanskt universitet som kanske var ursprunget till dokumentet?

Tyvärr är det så att nästan oavsett vad IT-avdelningen hittar på för att stänga ute smitta, så kan man slinka förbi genom att hämta filer på andra sätt. Patrik rekommenderar användning av SUNETs Box före Dropbox, eftersom Box garanterat är krypterat.

MOTARBETE

Patrik berättar om hur KTHs IT-avdelning motarbetar skummisarna. Ett exempel är de tidigare nämnda gratishotellen, vilka emellertid känner ett visst ansvar och ganska snabbt plockar bort skadliga webbsidor om man ringer dem och anmäler. Det kan röra sig om reaktionstider på nedåt fem minuter.

– Man tror allmänt att det skulle vara sämre i Ryssland, men det är inte alls min uppfattning. Jag har skickat hela listor med skadliga URL:er till ryska myndigheter och de tar tag i det på en gång, för i Ryssland blir detta tydligen ett polisiärt ärende. Och de skickar också listor till oss när de har hittat skadliga adresser. De är klart hjälpsamma. Även Chrome och Firefox med flera webbläsare har interna listor som hjälper till att spärra onda sajter.

Ett skadligt e-brev kan ha hamnat hos många. Därför gör postmaster automatiskt en genomsökning av allas brevlådor när något sådant upptäcks, och flyttar det skadliga till särskilda brevlådor.

Bilden visar de hårda grabbarna i incidentenheten, OPS-gruppen som försöker hålla KTH rent från smittor och ransomware. Den grönsvarta skylten nere i högerhörnet med avdelningens logotyp på, har en varnande text ”Ja, vi såg vad du gjorde”. Under denna hittar man en lista med åtgärder om ransomware upptäcks, som anger vilka kontaktpersoner som ska involveras, vilka diskytor som ska genomsökas och när ett incidentteam ska inkallas.

WANNACRY GICK BET PÅ KTH

IT-avdelningen har ägnat sig åt massiva kampanjer för att höja medvetandet om malware och blev därför inte drabbat av Wannacry. Dessutom uppdaterade man alla centralt övervakade maskiner med Microsofts rättningar till olika windowsversioner. Det lustiga inträffade att en maskin som inte var uppdaterad hade stått oanvänd i två månader och slogs på just under wannacry-attacken. Den var osmittad, men ouppdaterad och orsakade därför larm. Lärdomen av detta får bli att aldrig någonsin sluta uppdatera maskiner.

Wannacry annonserade sin närvaro för att skummisarna skulle kunna få betalt, men hur många andra, liknande malware finns det ute som inte annonserar sin närvaro utan ligger i bakgrunden och gör något otrevligt?

ETT LYCKAT FALL

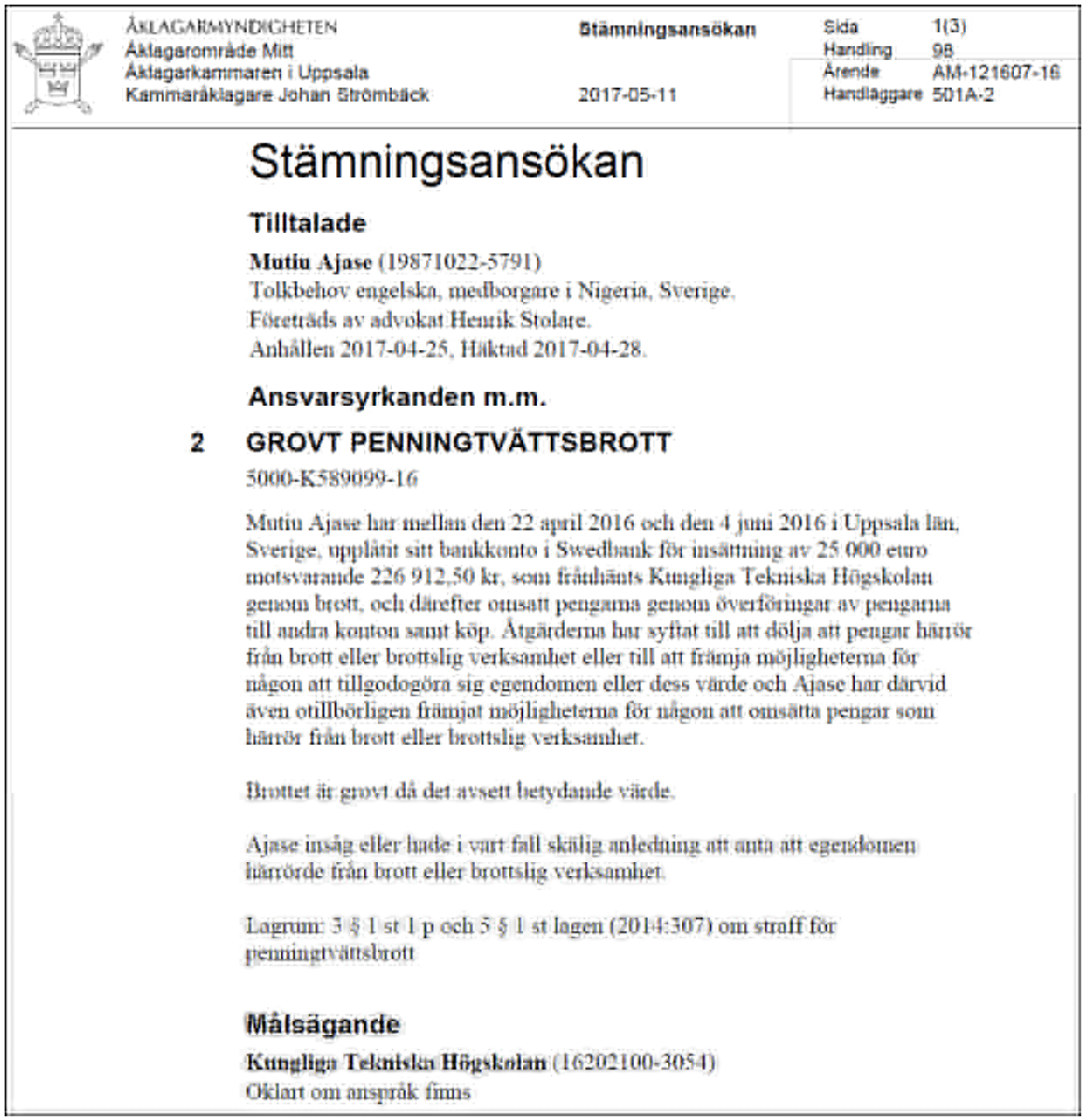
Under juni 2016 utsattes KTH för ett ”VD-bedrägeri” och en ekonomiperson lurades att betala ut en halv miljon till en falsk mottagare. Bedragaren kunde senare gripas.

Här är början av artikeln i KTHs interntidning Campi från mitten av juni 2016, där Patrik redogör för fallet, som inträffade i december 2015. Några e-postkonton på KTH hade kapats, posten genomsökts och riktiga fakturor suddats bort och ersattes med andra.

Läs hela artikeln på **https://campi.kth.se/nyheter/bedragare-lurade-kth-pa-halv-miljon-1.657619** och ta varning av Patriks rekommendationer på slutet.

– Lite lagom paranoia är bra.

Bedrägeriet upptäcktes i och med att en anställd fick en inbjudan att dela en mapp på Dropbox. Denne blev misstänksam, kanske främst för att IT-avdelningen predikat fördelarna med sunettjänsten Box. Resultatet blev en anmälan till åklagarmyndigheten i Uppsala.



ÅKLAGARMYNDIGHETEN
Åklagarområde Mitt
Åklagarkammaren i Uppsala
Kammaråklagare Johan Strömbäck

Stämningsansökan

2017-05-11

Sida 1(3)
Handling 98
Ärende AM-121607-16
Handläggare 501A-2

Stämningsansökan

Tilltalade

Mutiu Ajase (19871022-5791)
Tolkbehov engelska, medborgare i Nigeria, Sverige.
Företräds av advokat Henrik Stolare.
Anhållen 2017-04-25, Häktad 2017-04-28.

Ansvarsyrkanden m.m.

2 GROVT PENNINGTVÄTTSBROTT

5000-K589099-16

Mutiu Ajase har mellan den 22 april 2016 och den 4 juni 2016 i Uppsala län, Sverige, upplåtit sitt bankkonto i Swedbank för insättning av 25 000 euro motsvarande 226 912,50 kr, som frånhänts Kungliga Tekniska Högskolan genom brott, och därefter omsatt pengarna genom överföringar av pengarna till andra konton samt köp. Åtgärderna har syftat till att dölja att pengar härrör från brott eller brottslig verksamhet eller till att främja möjligheterna för någon att tillgodogöra sig egendomen eller dess värde och Ajase har därvid även otillbörligen främjat möjligheterna för någon att omsätta pengar som härrör från brott eller brottslig verksamhet.

Brottet är grovt då det avsett betydande värde.

Ajase insåg eller hade i vart fall skälig anledning att anta att egendomen härrörde från brott eller brottslig verksamhet.

Lagrum: 3 § 1 st 1 p och 5 § 1 st lagen (2014:307) om straff för penningtvättsbrott

Målsägande

Kungliga Tekniska Högskolan (16202100-3054)
Oklart om anspråk finns

Gärningsmannen var instämd för flera brott på samma gång, men jag har klippt bort det oväsentliga. Det allra väsentligaste är att han blev gripen och lagförd.

Gripandet är bra för moralen och en uppmuntran i striden mot spam och bedrägerier, för det visar att kampen inte är hopplös utan att det går att vinna.

MYNDIGHETEN FÖR SAMHÄLLSSKYDD

MSB har äntligen börjat rulla ut ett elektroniskt ärendehanteringssystem för att underlätta incidentrapportering vid cyberincidenter.

– Men, menar Patrik, det är svårt för dem som inte är vana. Vi på KTH är vana vid att rapportera och har en tradition av öppenhet, medan många andra skäms för att rapportera. Sedan finns det sådana som Skatteverket som är väldigt ordentliga med att rapportera. Men vi kommer inte att rapportera varenda virusattack för då skulle vi sänka hela systemet. Vi har kapacitet att göra det.

Från och med 1 april, 2016 ska alla statliga myndigheter rapportera IT-incidenter som inträffar i myndighetens informationssystem eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Det är mycket bra att staten äntligen har lärt sig. Läs mer här: **https://www.msb.se/sv/Forebyggande/Informationssakerhet/It-incidentrapportering/**

VAD SPELAR ROLL?

Det allra viktigaste är att ledningen är med på åtgärderna. På KTH har man fördelen av att rektorer med flera är datortekniker och förstår, men på andra ställen är man kanske inte så lyckligt lottad. Därför föreslår Patrik följande åtgärder.

- Skärpta rutiner. Cybersäkerhet är viktigt.
- Uppdatera alla maskiner kontinuerligt
- Spärra misskötta datorer
- Säkerhetskopiera alla arbetsytor kontinuerligt
- Konfigurera datorer och nät för att hindra angrepp
- Övervaka arbetsytor och maskiner för att hitta misstänka signaturer
- Sudda inga brev, utan spara allt om det skulle behövas till en utredning
- Håll efter skrivrättigheterna. Ingen ska kunna ändra i filer denne inte har rätt till. Trots att denne råkar vara chef. Det blir den som slinker undan, som inför skadeprogrammen.
- Ställ allmänt högre krav på verksamheten, så att människor blir medvetna om problemen.
- Informera de anställda om farorna på ett pedagogiskt sätt. Utbildning är allt!
- Följ upp och ser till att alla har förstått.
- I vissa fall kan det bli nödvändigt med ”kvartssamtal” där den enskilde får verkligheten förklarad för sig, med samtalstonen anpassad efter antalet återfall.

Det spelar egentligen ingen roll hur det genomförs, bara organisationen tar faran med social engineering, spam och ransomware på allvar och agerar därefter.

HUR SKA MAN FÅ SLUT PÅ DET?

När en resurs är gratis tenderar skrupellösa människor att missbruka den. Fortsätter den att vara gratis ökar missbruket lavinartat och vi hamnar där vi är idag.

Om man antog att man kunde införa porto på e-brev, skulle det minska spammandet? Inga fantastiska priser, bara 10 öre per brev. För en vanlig användare som skickar 5-10 e-brev per dag är kostanden försumbar, men för en storspammare som skickar hundra tusen eller en miljon brev kan kostanden bli förödande.

Givetvis ska brevet märkas med ett krypterat ”frimärke” så att en mottagare direkt kan kassera ofrankerade brev. Var och en ska samtidigt ha rätten att ta emot ofrankerade brev.

Portokostnaden kan påverka den enskilde på flera sätt. Är din dator, TV, övervakningskamera eller rumstermostat en spamrobot blir räkningen betydande. Då lär sig den enskilde eller en myndighet att hålla sina datorer rena. Du ser för din egen skull till att rensa bort alla trojaner illa kvickt. Det ställe där det svider mest är plånboken.

Kom ihåg – det är ingenting personligt. De vill bara ha dina pengar.

LÄS MER

Sunets e-potsfilter: **https://www.sunet.se/tjanster/mailfilter/**

Fakturabedrägeriet på KTH: **https://campi.kth.se/nyheter/bedragare-lurade-kth-pa-halv-miljon-1.657619**

Attackvektorn, det är du: **http://www.sweclockers.com/artikel/21218-attackvektorn-det-ar-du**

Mitt eget detaljförslag till spamstopp – porto: **http://www.idg.se/2.1085/1.401486/men-gor-nagot-at-spammet-da**

Största lurendrejeriet någonsin: **http://fortune.com/2017/04/27/facebook-google-rimasauskas/**

Även berömda universitet åker dit: **http://www.bbc.com/news/education-40288548**

Sydkoreanska webbhotellet Nayana betalade en miljon dollar: **http://www.bbc.com/news/technology-40340820**

Engelska sjukhus föll ihop av Wannacry: **http://www.bbc.com/news/health-39904851**

Skriven av

JÖRGEN STÄDJE

Jag heter Jörgen Städje och har skrivit om teknik och vetenskap sedan 1984. Friskt kopplat, hälften brunnet!