HC 7, 20-03-2018, speuren op het Dark Web (Geen verplichte tentamenstof!)

Bijna iedereen bezoekt wel eens het Deepweb. Deepweb sites zijn niet vindbaar voor zoekmachines, omdat ze bijvoorbeeld achter een login pagina zitten. Toegang tot Deepweb is beperkt tot bevoegden, de content is dynamisch of je moet een zoekformulier invullen.

Met het Darknet wordt meestal Tor hidden services bedoeld. Tor (The Onion Router) is een computernetwerk dat web traffic omleidt, waardoor je anoniem kunt internetten. Hidden services of Onion sites zijn websites die alleen te bezoeken zijn via het Tor netwerk. Andere darknets zijn bijvoorbeeld I2P, Zeronet en Freenet. Je kan zowel gewone websites als hidden services bezoeken via de Tor, via de andere darknets kan dat niet. Er bestaat een 'bright side' en 'dark side'. Onder de 'bright side' valt de anonieme communicatie. Het is een veilige omgeving en je kan de internetcensuur omzeilen. De 'dark side' bestaat onder andere uit de handel in drugs en vuurwapens, ransomware-as-a-service en kinderpornografie.

Hansa Market wordt overgenomen door de Politie. Ze hebben een kopie van de website online gezet en het beheer overgenomen. De infiltratieactie is uniek, toen rees de vraag hoe ver de politie mocht gaan op dit moment. Op dat moment is de FBI bezig met het neerhalen van de grootste market, AlphaBay. Alle kopers en verkopers gingen naar Hansa Market. De politie nam veel bitcoins in beslag en er kwamen heel veel adressen van kopers en verkopers vrij. Reddit is de belangrijkste bron voor informatie over het darknet. Er zijn een aantal gevolgen door de takedowns, allereerst was er veel speculatie en paniek. Veel kopers en verkopers gingen op zoek naar de next best market. Veel Markets namen een pauze door de toenemende drukte, kopers en verkopers moesten bedenken hoe ze elkaar terug gingen vinden. De beveiliging van Markets werden opgeschroefd en er kwam een kans voor kleine Markets. Daarnaast volgden er veel arrestaties. Maar hoe lopen kopers en verkopers nou tegen de lamp? Meestal doordat er een pakketje onderschept wordt, de verkoper hield een gedetailleerde administratie bij of er werd een menselijke fout gemaakt. Af en toe door een bitcoin/blockchainanalyse of infiltratie.

Web-IQ is een klein bedrijf dat bestaat sinds 2011 en heeft 14 vaste medewerkers. Ze werken met verschillende bedrijven samen zoals de gemeente, de politie etc. Hun doel is het in kaart brengen van criminele acties op het internet. Ze gebruiken web crawlers die ze opdrachten meegeven in het Dark Web. Zo sporen ze allerlei websites en informatie op. Uitdagingen in de nabije toekomst zijn: DIY policing, livestreaming, internet of things en het waterbed-effect. Oplossingen zijn eventueel auto-classificatie, darknet of things, DIY policing, publiek-private samenwerking en arachnid.