STAGEOPDRACHT

Bedrijf / opdrachtgever : the Security Factory

Adres: Samenwerkingsstraat 50
2845 Niel

Contactpersoon: Nico Cooman
+32 473 544632
nico.cooman@thesecurityfactory.be

Bedrijfspromotor: Ward Vermeulen
+32 471 620409
ward.vermeulen@thesecurityfactory.be

Aantal medewerkers: 20

Aantal IT medewerkers: 18

Aantal technische begeleiders: 5

Afstudeerrichting: Applicatie-ontwikkeling, Systemen en Netwerkbeheer

Opdracht

De doelstelling van de stageopdracht is om onderzoek te doen naar methodes om moderne anti-virus solutions te omzeilen.
De student heeft als doelstelling om een stuk malware (of een malware generator) te bouwen die we kunnen enten op Cobalt Strike en die in staat is om de meeste moderne anti-virus en host-based IPS solutions solutions te omzeilen, zodat we dit kunnen gebruiken in red team scenarios.
De deliverables van de opdracht zijn:

- Een onderzoeksdocument rond het omzeilen van moderne anti-virus en Host-based IPS solutions
- Idealiter ook een generator die malware genereert die we kunnen gebruiken in een bepaalde opdracht

Extra Info

the Security Factory is een consultancybedrijf dat gespecialiseerd is in het uitvoeren van penetration testing en red teaming op verschillende grote bedrijven doorheen ons land, de student komt terecht in een team gespecialiseerd in verschillende aspected van IT security

Omgeving

Web: CSS, Javascript, PHP, Angular, ..., Mobile: Android, iOS, Windows, ..., Systemen&Netwerken: Linux, Windows, ...

Randvoorwaarden

- we verwachten dat alles gerelateerd aan het onderzoek uitgevoerd door de student in het engels opgesteld wordt, ook verwachten we dat alle documentatie in het engels geschreven wordt
- aangezien ons kantoor zich niet bij de deur bevindt en het openbaar vervoer niet helemaal optimaal is in de buurt is het bezit van een auto aanbevolen, maar zolang de student zich kan verplaatsen naar onze locatie maakt het voor ons op zich niet veel verschil hoe hij of zij dat doet
- de student dient een interesse te tonen in IT security, en bereid te zijn om individueel onderzoek te verrichten naar relatief complexe topics zoals reverse engineering en windows internals, hier kan hij/zij uiteraard wel uitgebreid begeleid worden door het team binnen tSF
- de student dient voldoende programmeer ervaring te hebben om individueel problemen op te lossen en een eindproduct af te leveren, hier zal de begeleiding mogelijk iets minder extensief zijn dan bij security-related topics

Onderzoeksthema

Het onderzoek hangt kort samen met de stage, deze lopen zelfs in elkaar over.
We verwachten dat er onderzoek gedaan wordt naar hoe malware detectie gebeurt door moderne anti-virus en host-based IPS systemen, en een analyse over hoe deze detectie omzeild kan worden.
Het eindproduct van de stage (software die grotendeels undetectable malware genereert) is hier eerder een bijproduct van dat voort zal vloeien uit het onderzoek.

Inleidende Activiteiten: Sollicitatiegesprek, CV

Aantal studenten: 1 student

Aanwezig op het Handshake Event:

Stageopdracht voor:

Andere bemerkingen: Wij hebben vorig academiejaar met groot plezier samengewerkt met PXL en kijken er naar uit om dit opnieuw te doen.
De stagebegeleider van PXL uit was toen Maarten Sourbron.

Aangezien we beseffen dat de gemiddelde student misschien niet voldoet aan de voorwaarden voor deze stage (gezien de toch wel vrij "atypische" opdracht), dienen wij deze opdracht niet enkel in bij PXL en zou het in het slechtste geval dus kunnen dat we uiteindelijk toch kiezen om geen stagiair te nemen.
Maar uiteraard hopen we in de eerste plaats op een herhaling van de top ervaring van vorig academiejaar!

Handtekening Stagebedrijf
Nico Cooman

Naam en handtekening stagiair