IT FORENSICS & INCIDENT RESPONSE

Incident Response Notification

Indicators of Compromise (IoCs) SilverFish APT (Update 06/04/2021)

Datum: 06/04/2021

Versie: 1.1

Classificatie: Publiek

Copyright © 2021 NFIR BV

Handelsnamen

POB-vergunning

Het ministerie van Justitie en Veiligheid heeft NFIR een vergunning afgegeven, waardoor NFIR haar werkzaamheden mag uitvoeren. Deze vergunning betreft de POB-vergunning. De POB-vergunning dekt het verwerken van strafrechtelijke gegevens, waarmee NFIR in aanraking kan komen bij het uitvoeren van haar diensten.

Het POB-licentienummer van NFIR is: 1672.

Contactinformatie

Naam	NFIR B.V.
Adres	Verlengde Tolweg 2 2517 JV Den Haag Nederland
Telefoonnummer	+31 (0) 88 – 323 02 05
E-mail	info@nfir.nl

1 Inleiding

Het NFIR CERT heeft tijdens meerdere incident response trajecten zogenoemde Indicators of Compromise (IoCs) gedetecteerd –het delen van deze indicatoren is van grote waarde voor organisaties om vast te kunnen stellen of zij gecompromitteerd zijn en actie dienen te ondernemen om mogelijk (verdere) schade te voorkomen.

1.1 Doel

Het NFIR CERT deelt in dit geval deze specifieke dreigingsinformatie voor het expliciet gebruik binnen een eigen Security Operation Center (SOC) of Security Team met als doel om organisaties te beschermen.

2 Indicators of Compromise

2.1 Netwerkindicatoren

Door het NFIR CERT zijn op het moment van schrijven tenminste de volgende websites waargenomen waarop malafide scripts worden gehost:

Domeinnaam	IPv4-adres
ssnb[.]nl	213[.]34[.]71[.]8
onderzoekers[.]nl	37[.]230[.]99[.]55
laboratorium[.]nl	37[.]230[.]99[.]55

Update 06/04/2021

Per 6 april 2021 is de volgende domeinnaam toegevoegd aan de lijst:

Domeinnaam	IPv4-adres
zorgen[.]nl	37[.]230[.]99[.]55

Daarbij krijgen bezoekers een melding in het browser-venster waarbij door de website aangegeven wordt dat de Chrome, Firefox of Edge browser geüpdatet dient worden – dit betreft een social engineering-aanval waarbij de gebruiker ertoe bewogen wordt om op update te klikken.

Als de gebruiker op de update-notificatie geklikt heeft zal er vervolgens een zip-bestandsarchief gedownload worden.

De bestandsnaam van dit ZIP-bestand bevat een gegenereerd patroon, en is afhankelijk van de gebruikte browser:

- Edge.[..].zip
- Chrome.Update.[..].zip
- Firefox.Update.[..].zip

> Op de [..] staan 6 random hexadecimale karakters. Dus 6 karakters bestaande uit 0 tot en met 9 en a tot en met f.

2.2 Bestandsindicatoren

Het waargenomen zip-bestandsarchief bevat een malafide javascript code. Door het NFIR CERT is vastgesteld dat deze malafide code op het moment van schrijven verbinding maakt met tenminste de volgende domeinen:

- [..].news.nuwealthmedia[.]com
- [..].news.pocketstay[.]com
- [..].payment.refinedwebs[.]com

> Op de [..] staan 8 random hexadecimale karakters. Dus 6 karakters bestaande uit 0 tot en met 9 en a tot en met f.

Zodra er een verbinding met de Command and Control wordt gemaakt kan de aanvaller besluiten om aanvullende code uit te voeren of niet. Het NFIR CERT is op de hoogte dat er tenminste bij 1 partij aanvullende acties zijn uitgevoerd.

Aanvullende informatie over deze aanval kan gevonden worden bij de volgende externe bronnen:

- https://www.menlosecurity.com/blog/increase-in-attack-socgholish
- https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf

2.3 Wat moet uw organisatie doen bij mogelijk misbruik?

Indien uw organisatie het slachtoffer is geworden van een aanval, is het dringende advies om onderzoek uit te laten voeren naar de toedracht, in hoeverre aanvallers mogelijk andere systemen hebben gecompromitteerd en welke informatie mogelijk ongeautoriseerd geraadpleegd is.

2.3.1 Handelingsperspectief

1. Koppel indien mogelijk de getroffen systemen los van het netwerk, maar laat deze **aanstaan** (in verband met eventuele sporen zoals het vluchtige geheugen – RAM);
2. Laat de getroffen systemen forensisch onderzoeken; zorg voor adequate backups
3. Reset uw wachtwoorden en gebruikersgegevens
4. Doe aangifte bij de Politie
5. Overweeg een melding te doen bij de Autoriteit Persoonsgegevens

Over NFIR

NFIR is een specialist in cyberbeveiliging. Bij NFIR zijn cyber-engineers in dienst: Hackers die weten wat ze doen, testers die de werking van ICT-infrastructuren en software begrijpen, privédetectives die, indien nodig, onderzoeken kunnen uitvoeren en adviseurs/consultants die u het juiste advies kunnen geven of die u kunnen ondersteunen bij een incident.

Gespecialiseerd in

- Het verzamelen, identificeren en valideren van digitale informatie
- Onderzoek naar computers, servers, e-mailverkeer, gegevensdragers, websites en personen

Multidisciplinair onderzoek

- Sporen en gegevens verzamelen en reconstrueren
- Heldere rapportage bruikbaar voor juridische procedures en andere officiële instanties

Samenwerking met

- Tactisch rechercheurs, privacy juristen, gerechtsdeurwaarders, Politie, NCSC, IBD, het Openbaar Ministerie en internationale diensten.

NFIR als adviseur Forensisch Onderzoek

- Samen met de opdrachtgever wordt de scope van het onderzoek bepaald
- Praktisch toepasbare adviezen na afronding van het onderzoek

NFIR B.V.
Verlengde Tolweg 2
2517 JV Den Haag
Telefoon: 088 - 323 02 05
info@nfir.nl
https://www.nfir.nl