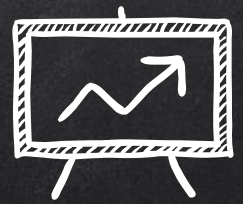


Retex - Analyse Forensic

Par Ricardo Matias - NBS System

Min2RiEN

NBS System

Qui suis je ?

Ricardo Matias

Consultant sécurité chez NBS System

Min2RIEN

NBS System

Et NBS System ?

Créateur de Cerberhost

Créateur de Naxsi

Créateur de SnuffleuPagus

Et NBS System ?

Une équipe d'experts

- Sécurité offensive
- Forensics
- Sécurité Opérationnelle
- DevSecOps
- R&D

Min2RIEN

NBS System

Forensic : Kesako ?

NBS System

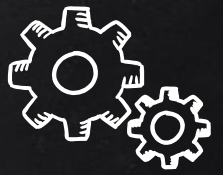
- ✗ Analyse post incident

- ✗ Les buts :
  - Confirmer ou infirmer l'intrusion
  - Détecter les causes de l'intrusion
  - Mesurer les impacts
  - Identifier les responsables et les objectifs
  - Proposer des remédiations

NBS System

Cas Classiques

NBS System



Min2RiEN

NBS System

Qu'en est-il de la menace interne ?

NBS System

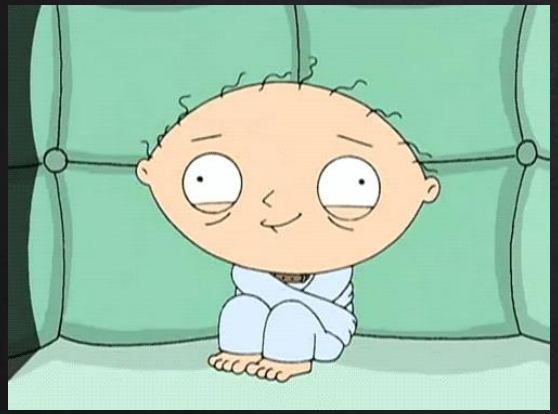
AVERTISSEMENT

TOUTE RESSEMBLANCE AVEC DES PERSONNES
OU DES SITUATIONS EXISTANTES OU AYANT
EXISTÉ NE SAURAIT ÊTRE QUE FORTUITE

Min2RIEN

NBS System

Contexte



Min2RiEN

NBS System

Symptomes

- ✗ Pertes de performance du parc
- ✗ Pertes de journaux d'évènements
- ✗ Augmentation de la consommation électrique en Datacenter

Min2RIEN

NBS System

Timeline définie par le client

Début - 2019: Premières perturbations

07/19 Forte dégradation des performances

03/08/19 Dégradation critique des performances

31/08/19 War Room client

18/09/19 Détection d'un malware après investigation interne

21/09/19 Prise de contact NBS

Min2RIEN

NBS System

Informations complémentaires

- ✗ Serveurs SQL premières cibles
- ✗ ~400 serveurs Windows infectés sur 700: pas de Linux à priori
- ✗ Suspicion sur une personne en interne
- ✗ Démarches juridiques entreprises

NBS System

Eléments Fournis

- ✗ Preuves transmises à la justice (captures d'écran, informations...)
- ✗ Logs d'outils de supervision
- ✗ 4 versions du malware
- ✗ Image disque (non analysée)

NBS System

Attendus

Min2RIEN

NBS System

Attendus

Min2RIEN

NBS System

Attendus

Min2RIEN

NBS System

Analyse du malware

Dernière version

Min2RIEN

NBS System

Développé en C# / .NET

✗ Update.exe ou wuxxxxxxx.exe : versions antérieures

```
rmatias@r-pc:~/Documents/Min2Rien/versions_malware$ file Update.exe
Update.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
```

✗ Dllhost.exe : dernière version

```
rmatias@r-pc:~/Documents/Min2Rien/last_version$ file dllhost.exe
dllhost.exe: PE32+ executable (console) x86-64 Mono/.Net assembly, for MS Windows
```

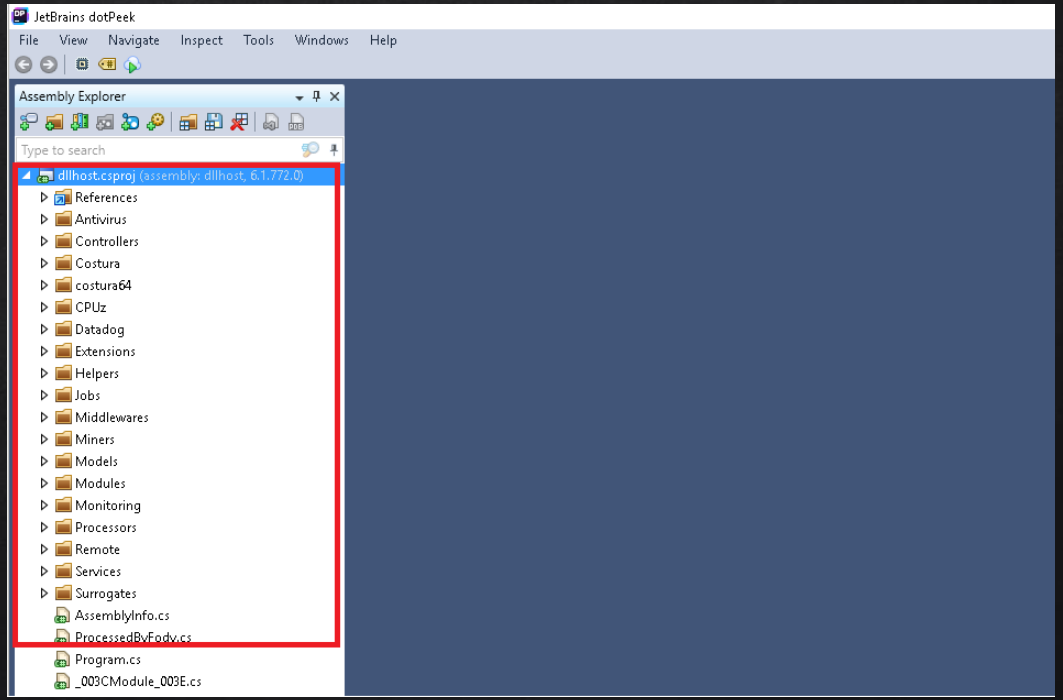
NBS System

STRINGS

```
<head><title>PANIC: {{.RecoveredPanic}}</title></head>
c:\go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/main_windows.go
C:/Users/[redacted]/DataDog/datadog-agent/vendor/golang.org/x/sys/windows/svc/debug/log.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/version.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/tagger_list.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/status.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/start.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/secret.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/run.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/remove_service_windows.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/reloadcheck.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/regimport_windows.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/open_browser_windows.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/listchecks.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/launchgui.go
```

Décompilation

✗ Possible avec JetBrains dotPeek



Min2RIEN

NBS System

Décompilation

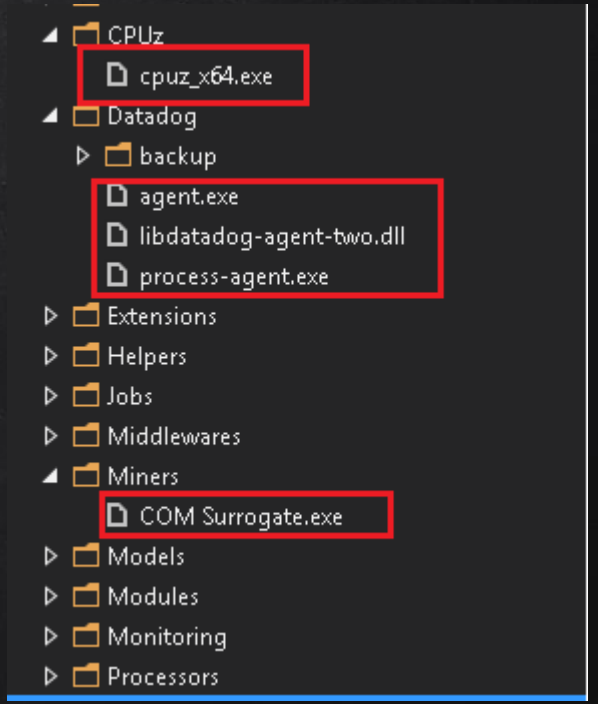
✗ Code non obfusqué

```
using dllhost.Models.Datadog;
using dllhost.Services.Datadog;
using Microsoft.AspNetCore.Mvc;
using Newtonsoft.Json;
using System.Threading;
using System.Threading.Tasks;

namespace dllhost.Controllers
{
  [Route("api/[controller]")]
  public class DatadogController : Controller
  {
    private readonly IDatadogAgentService _datadogAgentService;

    public DatadogController(IDatadogAgentService datadogAgentService)
    {
      this..ctor();
      this._datadogAgentService = datadogAgentService;
    }

    [HttpGet("cpu")]
    public async Task<IActionResult> GetCpu()
```

NBS System

Décompilation

- Trois exécutables embarqués :
  - CPUz : contrôle de l'architecture
  - Agent Datadog recompilé pour renvoyer des fausses valeurs
  - COM Surrogate : crypto-mineur

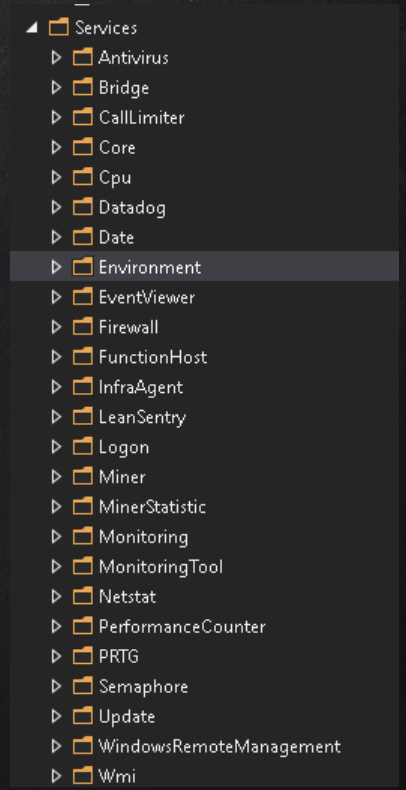


Min2RIEN

NBS System

Décompilation

- “Services” en place :
  - Analyse de l’environnement : pare-feu, anti-virus, système
  - Envoi de fausses valeurs aux services de monitoring
  - Lancement des activités malveillantes : minning, envoi d’informations vers l’externe
  - Détection de connexion distante
  - Mises à jour



Min2RIEN

NBS System

Service « environnement »

```
if (machineName.StartsWith("                                    .son.InvariantCultureIgnoreCase))
  flag1 = true;
else if (machineName.Contains("                                  .rison.InvariantCultureIgnoreCase))
  flag2 = true;
else if (machineName.Contains("                                  mparison.InvariantCultureIgnoreCase))
  flag3 = true;
else if (machineName.Contains("                                  .son.InvariantCultureIgnoreCase))
  flag4 = true;
else if (machineName.Contains("                                  .rison.InvariantCultureIgnoreCase))
  flag5 = true;
else if (machineName.Contains("                                  mparison.InvariantCultureIgnoreCase))
  flag6 = true;
else if (machineName.Contains("                                  .rison.InvariantCultureIgnoreCase))
  flag7 = true;
else if (machineName.Contains("                                  mparison.InvariantCultureIgnoreCase))
  flag8 = true;
else if (machineName.Contains("                                  mparison.InvariantCultureIgnoreCase))
  flag9 = true;
else if (machineName.Contains("                                  .rison.InvariantCultureIgnoreCase) || machineName
  flag10 = true;
else if (machineName.Contains("                                  gComparison.InvariantCultureIgnoreCase))
  flag11 = true;
else if (machineName.Contains("                                  .rison.InvariantCultureIgnoreCase))
  flag12 = true;
else if (machineName.Contains("                                  parison.InvariantCultureIgnoreCase))
  flag13 = true;
else if (machineName.Contains("                                  mparison.InvariantCultureIgnoreCase))
  flag14 = true;
else if (machineName.Contains("                                  mparison.InvariantCultureIgnoreCase))
  flag15 = true;
else if (machineName.Contains("                                  mparison.InvariantCultureIgnoreCase))
  flag16 = true;
else if (machineName.Contains("                                  .rison.InvariantCultureIgnoreCase))
  flag17 = true;
else if (machineName.Contains("                                  .rison.InvariantCultureIgnoreCase))
  flag18 = true;
else if (machineName.Contains("                                  .rison.InvariantCultureIgnoreCase))
  flag19 = true;
else if (machineName.Contains("                                  .ngComparison.InvariantCultureIgnoreCase))
  flag20 = true;
else if (machineName.Contains("                                  Comparison.InvariantCultureIgnoreCase))
  flag21 = true;
else if (machineName.Contains("                                  mparison.InvariantCultureIgnoreCase))
  flag22 = true;
```

Min2RIEN

NBS System

Fichier de constantes

```
public const string UpdatesEndpoint = "https://[redacted].core.windows.net/updates";
public const string ApplicationInsightsKey = "[redacted]06f";
public const int PrometheusProxyPort = 5999;
public const int PrometheusLocalPort = 5000;
public const int InfraAgentProxyPort = 6000;
public const string AzureFunctionEndpoint = "https://[redacted].azurewebsites.net";
public const string PRTGEndpoint = "https://1[redacted]";
public const string MinerEmbeddedResourcePath = "dllhost.Miners.COM Surrogate.exe";
public const string AntivirusEmbeddedResourcePath = "dllhost.Antivirus.Antivirus.txt";
public const string MonitoringToolsEmbeddedResourcePath = "dllhost.Monitoring.MonitoringTools.txt";
public const string RemoteToolsEmbeddedResourcePath = "dllhost.Remote.Remote.txt";
public const string DatadogAgentEmbeddedResourcePath = "dllhost.Datadog.agent.exe";
public const string DatadogBackupAgentEmbeddedResourcePath = "dllhost.Datadog.backup.agent.exe";
public const string DatadogProcessAgentEmbeddedResourcePath = "dllhost.Datadog.process-agent.exe";
public const string DatadogBackupProcessAgentEmbeddedResourcePath = "dllhost.Datadog.backup.process-agent.exe";
public const string LibDatadogAgentEmbeddedResourcePath = "dllhost.Datadog.libdatadog-agent-two.dll";
public const string LibDatadogBackupAgentEmbeddedResourcePath = "dllhost.Datadog.backup.libdatadog-agent-two.dll";
public const string DatadogAgentProxyMD5Hash = "3[redacted]2";
public const string DatadogProcessAgentProxyMD5Hash = "D[redacted]9";
public const string LibDatadogAgentProxyMD5Hash = "D[redacted]E";
public const string DatadogAgentName = "agent.exe";
public const string DatadogProcessAgentName = "process-agent.exe";
public const string LibDatadogAgentName = "libdatadog-agent-two.dll";
public const string MinerProxyEndpoint = "1[redacted]00";
public const int MinerApiPort = 65000;
public const string MinerAccessToken = "[redacted]";
```

Analyses

- ✗ Malware lancé comme un service de mise à jour légitime
- ✗ Le malware s'installe manuellement – aucune fonction de propagation détectée
- ✗ Pas d'envoi de données autre que des données statistiques de minage
- ✗ Excellente connaissance du SI interne

NBS System

Pour résumer

- ✗ Le malware peut :
  - Se mettre à jour automatiquement
  - Envoyer des statistiques de minage et des informations sur les serveurs
  - Détecter des connexions distantes et fausser des métriques
- ✗ Le malware ne peut pas :
  - Détruire le parc sans mise à jour
  - Envoyer des données à caractère personnel
  - Exécuter des commandes à distance
  - Se propager de manière automatique

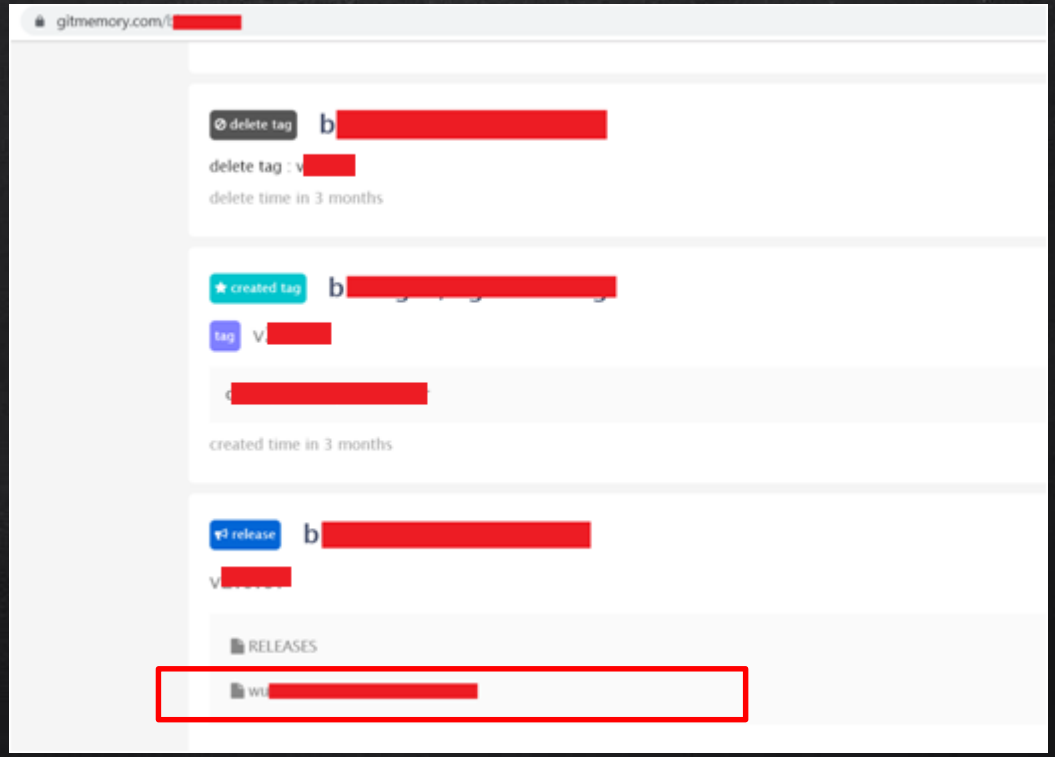
NBS System

Corrélations
Des Preuves

STRINGS

```
<head><title>PANIC: {{.RecoveredPanic}}</title></head>
c:\go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/main_windows.go
C:/Users/[redacted]/DataDog/datadog-agent/vendor/golang.org/x/sys/windows/svc/debug/log.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/version.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/tagger_list.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/status.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/start.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/secret.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/run.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/remove_service_windows.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/reloadcheck.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/regimport_windows.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/open_browser_windows.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/listchecks.go
C:/Users/[redacted]/DataDog/datadog-agent/cmd/agent/app/launchgui.go
```

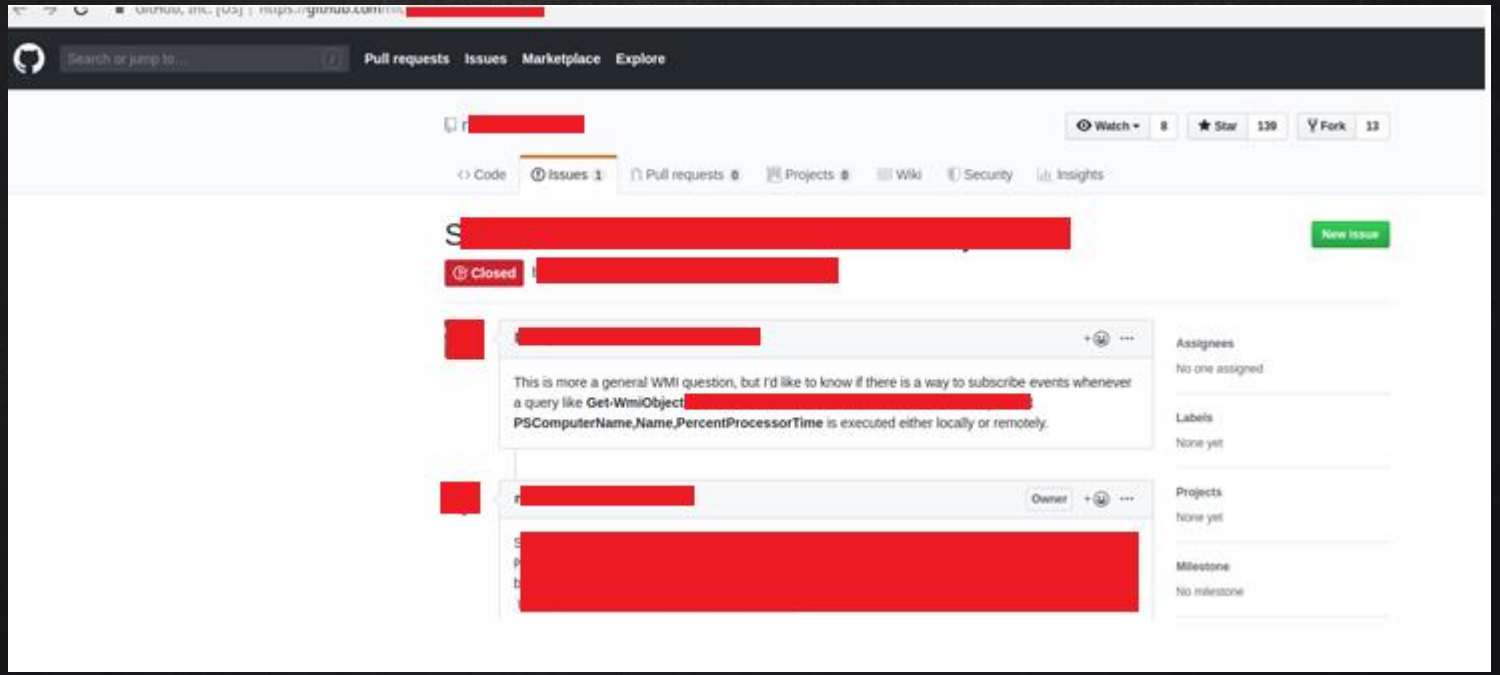
Google / GIT



Min2RIEN

NBS System

Google / GIT



Min2RIEN

NBS System

Autres

- ✗ Authentification avec un seul compte pour les administrateurs
- ✗ Corrélation entre : compte générique, identifiant VPN et installation du malware
- ✗ Expert Windows / .NET

NBS System

Conséquences

Pour l'entreprise et l'employé

Pour l'entreprise

- ✗ Pertes financières de plusieurs centaines de milliers d'euros
  - Renouvellement de matériels inopiné
  - Datacenters
  - Pertes potentielles de clients

- ✗ Temps humain
  - Astreintes
  - Recherche de bugs dans la solution

- ✗ Réglementaires : CNIL / RGPD

NBS System

Pour l'employé

- ✗ Perte de l'emploi
- ✗ Réputation
- ✗ Poursuite judiciaire :
  - Accès et maintien non autorisé à un STAD aggravé par une entrave au bon fonctionnement : 3 ans de prison / 45000 € d'amende

NBS System

Mais pourquoi ???

NBS System

Min2RIEN

NBS System

Min2RiEN

NBS System

4.

Remédiations & Recommandations

NBS System

Remédiations

- ✗ Modifications DNS – Fichier hosts : empêcher les mises à jour
- ✗ Bloquer l'adresse IP du pool de minage
- ✗ Désinfection : Simuler une mise à jour du malware pour y mettre une charge utile nulle via usurpation DNS

NBS System

Recommandations

- ✗ Accès nominatifs et restreints
- ✗ Mise en place de proxys
- ✗ Plateforme de supervision : SIEM

Min2RIEN

NBS System

Comment ca s'est finit ?

- ✗ Convocation par la direction
- ✗ Collaboration entre les deux parties

NBS System

Merci Pour votre attention!

Des questions ?

ricardo.matias@nbs-system.com

Min2RIEN

NBS System