DNS 設定を書き換えるマルウェアにご注意ください

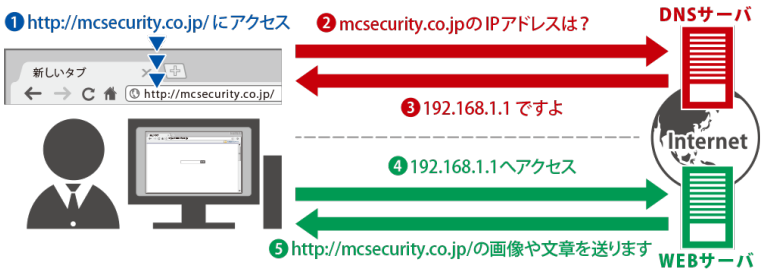
DNS 設定を書き換えるマルウェア

2012 年頃より、「DNS Changer（ディーエヌエス チェンジャー）」と呼ばれる、パソコンの DNS 設定を書き換え、不正なサイトにアクセスさせようとするマルウェアが流行しています。

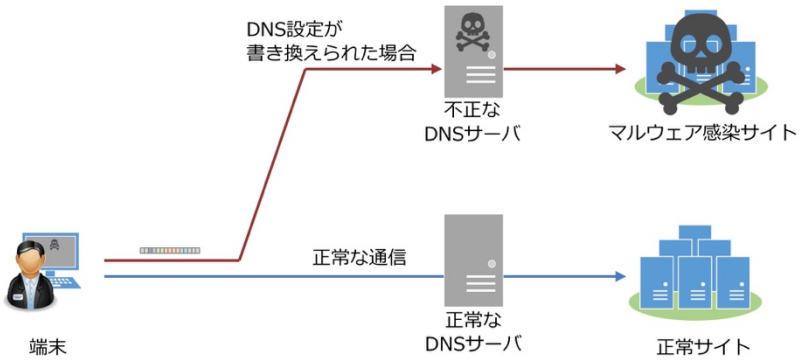
2019 年現在でも、同様の動作をするマルウェアが存在しており、
「GhostDNS（ゴースト ディーエヌエス）」と名前を変えて存在しています。

DNS 設定が書き換わると？

DNS は、Web サイトの閲覧など、インターネットに不可欠な仕組みです。
例えば、http://mcsecurity.co.jp/ にアクセスしようとした際、ドメイン名の mcsecurity.co.jp を IP アドレスに変換してくれるのが DNS サーバです。



この DNS 設定が不正なものに書き換えられてしまうと、一般のサイトにアクセスしようとした際に、不正な DNS サーバによって、悪意のある IP アドレスに接続させられ、マルウェア感染をしてしまう恐れがあります。



NetStable での検知

NetStable では、DNS Changer や GhostDNS の脅威を検知するシグネチャをリリースしています。

- 2000861 – 2000864 Malicious DNS Server connection
  DNS 設定を書き換え、不正サイトに誘導する DNS サーバへの接続を検出するシグネチャです。

- 2001057 – 2001058 DNSpionage Office document download
  DNSpionage のマルウェアを実行する際に発生する通信を検出するシグネチャです。

- 2001163 – 2001184 GhostDNS C2 IP Connect
- 2001185 – 2001208 GhostDNS C2 Domain Connect
- 2001209 – 2001210 GhostDNS C2 URL Connect
  DNS 設定を書き換えるマルウェア GhostDNS が感染後にアクセスする C2 サーバへのアクセスを検出するシグネチャです。

まとめ

- DNS はインターネットを利用する際に不可欠な仕組み
- DNS 設定を書き換えるマルウェアが存在している
- 不正な DNS サーバによって、マルウェア感染をしてしまう恐れがある