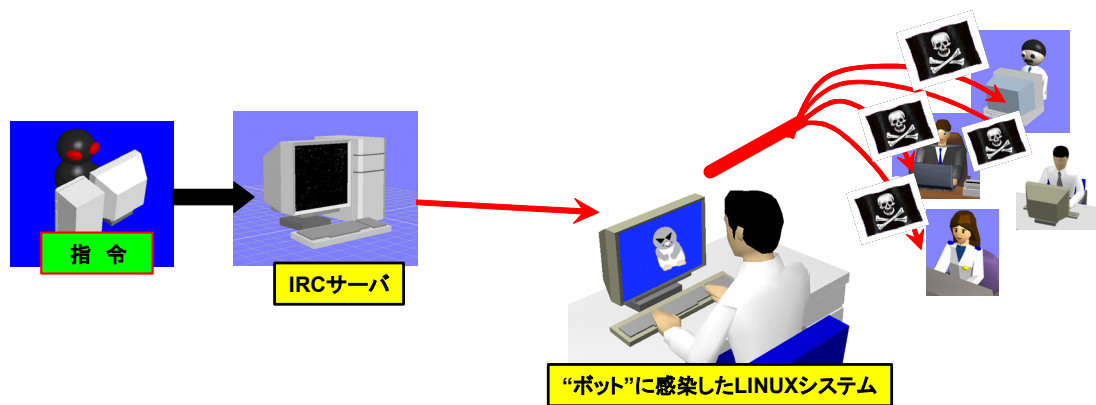


Linux システムを標的としたボットについて

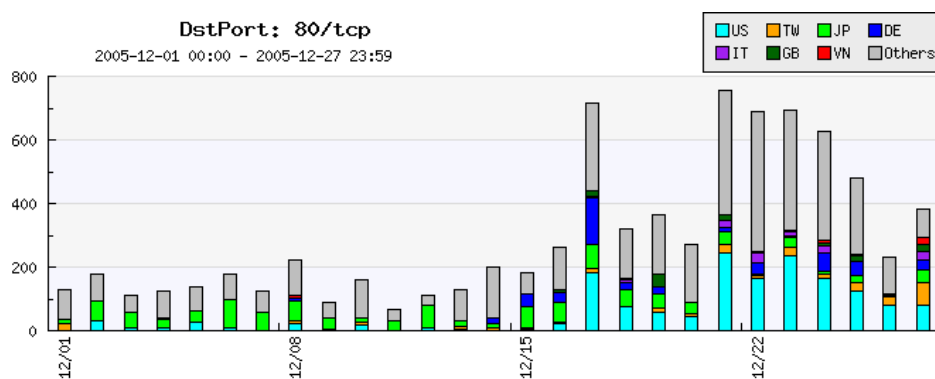
“ボット”は、従来、Windows システム上で動作するものが多かったのですが、Linux システム上で動作するものもあり、DDoS 攻撃を行うとの情報があります。

このボットについて動作を検証しました。

感染経路については現在のところ不明ですが、PHP の脆弱性を悪用して感染するとの情報があり、12月17日頃からTCP80番ポートに対するアクセス状況に変化が見られます。



なお、TCP80番ポートに対するアクセス状況は次のとおりです。



今後も、同様のボットの感染活動が発生する可能性があることから、Windows システムのみならず、Linux システムについても、脆弱性の修正プログラムの適用やセキュリティに関する各種設定の見直し等、使用されているコンピュータのセキュリティの再確認をお勧めします。