情報通信研究機構
NICT 先端研究 ㊼

関数特定 マルウエア復号

マルウエアとは悪意あるソフトウエアを意味する造語である。パソコンがマルウエアに感染すると機密文書が流出するといった被害が出てしまうため、各種マルウエアへの対策が広く一般に周知されるべきだが、そもそもマルウエアの悪意ある挙動が不明なままでは対策の立てようもない。

対策を考案するためにはマルウエアをハッキング（解析）し、その挙動を明らかにしなければならない。解析にもいろいろな手段があるが、国立研究開発法人情報通信研究機構（NICT）と神戸大学情報通信研究室では「パソコンから機密文書を盗め」や「別のパソコンに感染せよ」といったマルウエアと指令者がやりとりする通信内容を取得するための解析技術を研究している。

ある種のマルウエアはパソコンに感染したが、解析を妨害する目的で通信を暗号化するせ、攻撃者からの指令を受信させると、解析環境内のメモリと呼ばれる広大な空間のどこかに通信内容が展開される。その場所を探し出すことが研究課題である。

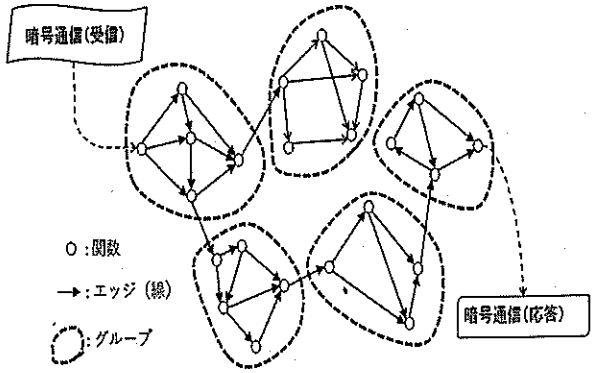
関数は多いときには数千の規模で内包されているが、事前に通信の復号関数がどれかはわからない。ところが二つの関数の間でデータがやりとりされるたびに関数同士を線で結んでいくと似た役割を担う関数群が密に結ばれ、グループを形成することを発見した。

この発見により復号に関連するグループに属する関数のみを確認するだけで復号関数を特定でき、大幅に解析の効率化を図れるようになった。復号関数の出力には指令が含まれることから、マルウエアの挙動の把握につながる。

（火曜日に掲載）

サイバーセキュリティ研究所・サイバーセキュリティ研究室主任研究員 **伊沢 亮一**

セキュリティー系ベンチャー企業を経て、12年、神戸大学大学院博士後期課程を修了。同年より現職。マルウエア解析に関する研究に従事する。博士（工学）。



マルウエアに内包される関数が線で結ばれている様子。似た役割を担う関数ではデータのやりとりが密に行われ、グループが形成される