サイバー攻撃における攻撃元特定技術に関する調査

Survey on attack source identification techniques in cyber attacks

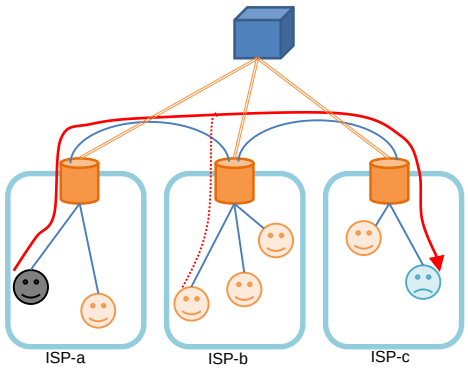
情報セキュリティ大学院大学　ネットワーク分科会
柴田理洋

Damage caused by cyber attacks are increasing worldwide, but cyber crime has a low clearance rate. Packet of attack for through the foreign, identify and arrest of the perpetrators has become increasingly difficult. This paper is survey several existing techniques for the purpose of attacking sensing is to be difficult. I will introduce them in outline:Large-scale demonstration experiments domestic provider business has a large number participation as research and development of IP traceback technology, Technique for information gathering by making viewing a dummy decoy files of the attacker, And its based research, Technique for hacking back as a trigger attacks. Introduces these four research papers, was compared with the study by considering the characteristics of each technology. In the future, I want to study effectively trace back to technology the perpetrator of cyber attack.

背景

近年，サイバー攻撃が非常に深刻化しており，その攻撃自体を防ぐ手法は多く研究されている．しかし根本的にサイバー犯罪を減らし，犯罪者を抑止するためには積極的に犯人を特定する必要がある．匿名化技術の進歩によって特定は極めて困難であるが，不可能ではない．いくつかの先行事例を紹介する．

先行事例1：IPトレースバック＋InterTrack



NECやNAISTを中心に開発が行なわれた研究．各インターネットサービスプロバイダー(ISP)の要所で，経由する全てのパケットのハッシュ値を取得する．攻撃を検知したとき，このハッシュ値と突合することで，攻撃パケットがどこから来たものか正確に判別できる．

例：プロバイダーaに存在する攻撃者が，発信元IPアドレスをプロバイダーbのユーザーのものに偽装し，攻撃を行った．被害者は攻撃パケットのハッシュ値を問い合わせ，各プロバイダーごとにハッシュ値の突合を行なう．

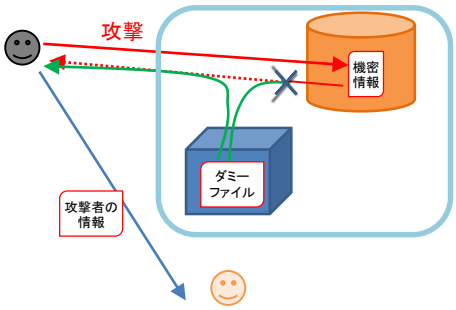
※図表では境界線上に一個置いてあるだけだが，本来はプロバイダー内部で階層構造となっている．

※若狭賢，山形昌也，大島龍之介，甲斐俊文，橋口輝，藤長昌，竹森敬祐，門林雄基，礒山寛章：インターネットにおけるトレースバック・システムのIPS実ネットワークにおける大規模実証実験の紹介，コンピュータセキュリティシンポジウム2009 (CSS2009)

先行事例2：Honeypot can bite

ロシアのAlexey氏は，攻撃者に設置した入力フォームを攻撃させ，ドライブ・バイ・ダウンロードでマルウェアを攻撃者の端末に感染させる実験に成功した．
筆者は「攻撃者は，攻撃を行うとき自分が攻撃されることを想定しない．この心理をうまく利用することで，攻撃者の特定が行なえる可能性がある．」と述べている．

先行事例3：関連論文情報漏洩を契機とした攻撃者探査システムの提案



機密情報へのアクセスを監視し，外部への移動が行なわれる際にダミーデータと入れ替える機構．ダミーデータは情報を収集し，ユーザーに送信する機能を有する．

※池上祐太，山内利宏：関連論文情報漏洩を契機とした攻撃者探査システムの提案，コンピュータセキュリティシンポジウム2013(CSS2013)

既存の問題点

先行事例2・3
・破壊的な行動や情報収集を行なうためには何らかのプログラムを攻撃者の端末に注入する必要がある．
・C&Cサーバーを用いた攻撃の場合，そこで特定が止まってしまう可能性が高い．
・攻撃者側にならかの脆弱性が存在しないと機能しない場合も多い．

先行事例1
・海外を経由するパケットに対応できない．
s・全世界が画一の対策を採れば不可能ではないが，政治的要因により実現性が薄い．