

ウイルス解析報告書

ウイルス名	FreeBSD.Scalper.Worm
プログラム名及び容量 (添付ファイル名)	.a (51,626バイト)
種別	ワーム
プログラム言語:	C言語
発症環境	FreeBSD x86 / Apache/1.3.20 (Unix) FreeBSD x86 / Apache/1.3.22-24 (Unix)
発見日時	2002年6月28日
発見場所(発信地)	イタリアと思われる。
危険性	中程度(5段階では2程度)
発症条件	即時
ウイルスの活動、影響	<p>このワームはFreeBSD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1.2.2以上 1.3.24までと、2.0以上 2.0.36までのバージョンにはchunk エンコード形式のデータを含む HTTP 要求の処理にバッファサイズ設定が適切でないというバグがあり、バッファオーバーフローを引き起こすセキュリティーホールが存在する。</p> <p>Scalperワームは巧妙に細工したHTTPリクエストを行うことにより自分自身のコードを実行させ、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受信する。このワームは/tmp/.uuuというファイル名で作成される。</p> <p>ワームは/tmp/.uuuをUUデコードし、/tmp/.aファイルを作成する。これを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2001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7月3日)
亜種、変種の有無	亜種が存在すると言われているが、正式には確認されていない。
	<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>元々作ってあったバックドアにApacheの脆弱性を利用して攻撃するツールのコードを合わせたものと思われる。</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。</p>

FreeBSD.Scalper.worm フローチャート

