



최근 바이러스의 동향

- 해킹기술과 바이러스 기술의 융합화

출처: KISA

최근 바이러스의 동향

- 최근 등장한 바이러스의 특징
 - 유입경로의 다양화
 - OS 및 S/W의 보안 취약점을 이용한 자동실행이나 네트워크를 통한 유입
 - 네트워크 및 해킹 기술의 결합
 - 사용자 암호를 해킹해 트로이마이크로 등 설치/실행
 - 바이러스 기술과 결합한 DDoS 유형의 공격 시도 증가
 - 피해의 대량화
 - 예전처럼 PC와 데이터를 파괴하는 자발적인 피해에서 사회 경쟁적인 피해로 대량화 되는 추세임.
 - 빠른 확산속도
 - 실시간에 전세계로 확산, 시치기 거의 없음.

최근 바이러스의 동향

- 최근 등장한 바이러스의 특징
 - 보안 취약점 이용이 증가
 - 알려진 OS 및 각종 Application의 보안취약점이 다수존재
 - 보안의 취약점을 이용한 바이러스 제작 가능성도 증가
 - 빠도어 및 트로이마이크로 바이러스 증가
 - 정보의 유출, DDoS형의 공격 등의 피해 예상

최근 바이러스의 동향

- 주요 웜의 피해 사례
 - CodeRed Worm (2001.7)
 - 국내 피해 : 1일 7월 206개 기관에서 49378개 시스템
 - 대부분 기업형, 일반인 등 민간에서 집중적으로 발생
 - 교육기관 1476건, 방송기기관 163건, 연구소 35건
 - [FIRST(국제침해사고대응협의회) 발표]
 - Worm32.Nimda (2001.9)
 - 전 세계 100만대의 컴퓨터를 강타
 - 국내 피해 : 22000여건
 - 국내의 피해증률은 세계 4번째 [USA Today, 정통부]

주요 웜 바이러스 피해 사례

- 주요 웜의 피해 사례
 - Worm.SQL.Slammer (2003.1)
 - 전 세계적으로 1월 25일 슬래머 웜이 출현된 후 패치되지 않은 MS-SQL 서버의 90%가 10분 이내에 감염
 - [CAIDA(Cooperative Association for Internet Data Analysis)보고]
 - 국내 피해 : 세계 각국 시스템(약 7만 5천개)의 11.8%인 8800여대
 - 세계에서 2번째
 - Blaster (2003. 8)
 - 2003년 8월 12일 MS사의 RPC 보안 취약점을 이용하여 감염
 - 전 세계적으로 20만 7천대의 시스템을 감염시키는(누적=연합인포맥스).
 - 국내의 실제 감염건수는 최소 100만대 이상으로 예상

최근 보고된 바이러스 분석

- 최근 바이러스 분석을 통한 특징
 - 1999년 7월 10일에 발견된 바이러스는
 - Windows 95/98/ME, NT/2000/XP, Win2003, WinXP SP1, WinXP SP2, WinXP SP3, WinXP SP4, WinXP SP5, WinXP SP6, WinXP SP7, WinXP SP8, WinXP SP9, WinXP SP10, WinXP SP11, WinXP SP12, WinXP SP13, WinXP SP14, WinXP SP15, WinXP SP16, WinXP SP17, WinXP SP18, WinXP SP19, WinXP SP20, WinXP SP21, WinXP SP22, WinXP SP23, WinXP SP24, WinXP SP25, WinXP SP26, WinXP SP27, WinXP SP28, WinXP SP29, WinXP SP30, WinXP SP31, WinXP SP32, WinXP SP33, WinXP SP34, WinXP SP35, WinXP SP36, WinXP SP37, WinXP SP38, WinXP SP39, WinXP SP40, WinXP SP41, WinXP SP42, WinXP SP43, WinXP SP44, WinXP SP45, WinXP SP46, WinXP SP47, WinXP SP48, WinXP SP49, WinXP SP50, WinXP SP51, WinXP SP52, WinXP SP53, WinXP SP54, WinXP SP55, WinXP SP56, WinXP SP57, WinXP SP58, WinXP SP59, WinXP SP60, WinXP SP61, WinXP SP62, WinXP SP63, WinXP SP64, WinXP SP65, WinXP SP66, WinXP SP67, WinXP SP68, WinXP SP69, WinXP SP70, WinXP SP71, WinXP SP72, WinXP SP73, WinXP SP74, WinXP SP75, WinXP SP76, WinXP SP77, WinXP SP78, WinXP SP79, WinXP SP80, WinXP SP81, WinXP SP82, WinXP SP83, WinXP SP84, WinXP SP85, WinXP SP86, WinXP SP87, WinXP SP88, WinXP SP89, WinXP SP90, WinXP SP91, WinXP SP92, WinXP SP93, WinXP SP94, WinXP SP95, WinXP SP96, WinXP SP97, WinXP SP98, WinXP SP99, WinXP SP100, WinXP SP101, WinXP SP102, WinXP SP103, WinXP SP104, WinXP SP105, WinXP SP106, WinXP SP107, WinXP SP108, WinXP SP109, WinXP SP110, WinXP SP111, WinXP SP112, WinXP SP113, WinXP SP114, WinXP SP115, WinXP SP116, WinXP SP117, WinXP SP118, WinXP SP119, WinXP SP120, WinXP SP121, WinXP SP122, WinXP SP123, WinXP SP124, WinXP SP125, WinXP SP126, WinXP SP127, WinXP SP128, WinXP SP129, WinXP SP130, WinXP SP131, WinXP SP132, WinXP SP133, WinXP SP134, WinXP SP135, WinXP SP136, WinXP SP137, WinXP SP138, WinXP SP139, WinXP SP140, WinXP SP141, WinXP SP142, WinXP SP143, WinXP SP144, WinXP SP145, WinXP SP146, WinXP SP147, WinXP SP148, WinXP SP149, WinXP SP150, WinXP SP151, WinXP SP152, WinXP SP153, WinXP SP154, WinXP SP155, WinXP SP156, WinXP SP157, WinXP SP158, WinXP SP159, WinXP SP160, WinXP SP161, WinXP SP162, WinXP SP163, WinXP SP164, WinXP SP165, WinXP SP166, WinXP SP167, WinXP SP168, WinXP SP169, WinXP SP170, WinXP SP171, WinXP SP172, WinXP SP173, WinXP SP174, WinXP SP175, WinXP SP176, WinXP SP177, WinXP SP178, WinXP SP179, WinXP SP180, WinXP SP181, WinXP SP182, WinXP SP183, WinXP SP184, WinXP SP185, WinXP SP186, WinXP SP187, WinXP SP188, WinXP SP189, WinXP SP190, WinXP SP191, WinXP SP192, WinXP SP193, WinXP SP194, WinXP SP195, WinXP SP196, WinXP SP197, WinXP SP198, WinXP SP199, WinXP SP200, WinXP SP201, WinXP SP202, WinXP SP203, WinXP SP204, WinXP SP205, WinXP SP206, WinXP SP207, WinXP SP208, WinXP SP209, WinXP SP210, WinXP SP211, WinXP SP212, WinXP SP213, WinXP SP214, WinXP SP215, WinXP SP216, WinXP SP217, WinXP SP218, WinXP SP219, WinXP SP220, WinXP SP221, WinXP SP222, WinXP SP223, WinXP SP224, WinXP SP225, WinXP SP226, WinXP SP227, WinXP SP228, WinXP SP229, WinXP SP230, WinXP SP231, WinXP SP232, WinXP SP233, WinXP SP234, WinXP SP235, WinXP SP236, WinXP SP237, WinXP SP238, WinXP SP239, WinXP SP240, WinXP SP241, WinXP SP242, WinXP SP243, WinXP SP244, WinXP SP245, WinXP SP246, WinXP SP247, WinXP SP248, WinXP SP249, WinXP SP250, WinXP SP251, WinXP SP252, WinXP SP253, WinXP SP254, WinXP SP255, WinXP SP256, WinXP SP257, WinXP SP258, WinXP SP259, WinXP SP260, WinXP SP261, WinXP SP262, WinXP SP263, WinXP SP264, WinXP SP265, WinXP SP266, WinXP SP267, WinXP SP268, WinXP SP269, WinXP SP270, WinXP SP271, WinXP SP272, WinXP SP273, WinXP SP274, WinXP SP275, WinXP SP276, WinXP SP277, WinXP SP278, WinXP SP279, WinXP SP280, WinXP SP281, WinXP SP282, WinXP SP283, WinXP SP284, WinXP SP285, WinXP SP286, WinXP SP287, WinXP SP288, WinXP SP289, WinXP SP290, WinXP SP291, WinXP SP292, WinXP SP293, WinXP SP294, WinXP SP295, WinXP SP296, WinXP SP297, WinXP SP298, WinXP SP299, WinXP SP300, WinXP SP301, WinXP SP302, WinXP SP303, WinXP SP304, WinXP SP305, WinXP SP306, WinXP SP307, WinXP SP308, WinXP SP309, WinXP SP310, WinXP SP311, WinXP SP312, WinXP SP313, WinXP SP314, WinXP SP315, WinXP SP316, WinXP SP317, WinXP SP318, WinXP SP319, WinXP SP320, WinXP SP321, WinXP SP322, WinXP SP323, WinXP SP324, WinXP SP325, WinXP SP326, WinXP SP327, WinXP SP328, WinXP SP329, WinXP SP330, WinXP SP331, WinXP SP332, WinXP SP333, WinXP SP334, WinXP SP335, WinXP SP336, WinXP SP337, WinXP SP338, WinXP SP339, WinXP SP340, WinXP SP341, WinXP SP342, WinXP SP343, WinXP SP344, WinXP SP345, WinXP SP346, WinXP SP347, WinXP SP348, WinXP SP349, WinXP SP350, WinXP SP351, WinXP SP352, WinXP SP353, WinXP SP354, WinXP SP355, WinXP SP356, WinXP SP357, WinXP SP358, WinXP SP359, WinXP SP360, WinXP SP361, WinXP SP362, WinXP SP363, WinXP SP364, WinXP SP365, WinXP SP366, WinXP SP367, WinXP SP368, WinXP SP369, WinXP SP370, WinXP SP371, WinXP SP372, WinXP SP373, WinXP SP374, WinXP SP375, WinXP SP376, WinXP SP377, WinXP SP378, WinXP SP379, WinXP SP380, WinXP SP381, WinXP SP382, WinXP SP383, WinXP SP384, WinXP SP385, WinXP SP386, WinXP SP387, WinXP SP388, WinXP SP389, WinXP SP390, WinXP SP391, WinXP SP392, WinXP SP393, WinXP SP394, WinXP SP395, WinXP SP396, WinXP SP397, WinXP SP398, WinXP SP399, WinXP SP400, WinXP SP401, WinXP SP402, WinXP SP403, WinXP SP404, WinXP SP405, WinXP SP406, WinXP SP407, WinXP SP408, WinXP SP409, WinXP SP410, WinXP SP411, WinXP SP412, WinXP SP413, WinXP SP414, WinXP SP415, WinXP SP416, WinXP SP417, WinXP SP418, WinXP SP419, WinXP SP420, WinXP SP421, WinXP SP422, WinXP SP423, WinXP SP424, WinXP SP425, WinXP SP426, WinXP SP427, WinXP SP428, WinXP SP429, WinXP SP430, WinXP SP431, WinXP SP432, WinXP SP433, WinXP SP434, WinXP SP435, WinXP SP436, WinXP SP437, WinXP SP438, WinXP SP439, WinXP SP440, WinXP SP441, WinXP SP442, WinXP SP443, WinXP SP444, WinXP SP445, WinXP SP446, WinXP SP447, WinXP SP448, WinXP SP449, WinXP SP450, WinXP SP451, WinXP SP452, WinXP SP453, WinXP SP454, WinXP SP455, WinXP SP456, WinXP SP457, WinXP SP458, WinXP SP459, WinXP SP460, WinXP SP461, WinXP SP462, WinXP SP463, WinXP SP464, WinXP SP465, WinXP SP466, WinXP SP467, WinXP SP468, WinXP SP469, WinXP SP470, WinXP SP471, WinXP SP472, WinXP SP473, WinXP SP474, WinXP SP475, WinXP SP476, WinXP SP477, WinXP SP478, WinXP SP479, WinXP SP480, WinXP SP481, WinXP SP482, WinXP SP483, WinXP SP484, WinXP SP485, WinXP SP486, WinXP SP487, WinXP SP488, WinXP SP489, WinXP SP490, WinXP SP491, WinXP SP492, WinXP SP493, WinXP SP494, WinXP SP495, WinXP SP496, WinXP SP497, WinXP SP498, WinXP SP499, WinXP SP500, WinXP SP501, WinXP SP502, WinXP SP503, WinXP SP504, WinXP SP505, WinXP SP506, WinXP SP507, WinXP SP508, WinXP SP509, WinXP SP510, WinXP SP511, WinXP SP512, WinXP SP513, WinXP SP514, WinXP SP515, WinXP SP516, WinXP SP517, WinXP SP518, WinXP SP519, WinXP SP520, WinXP SP521, WinXP SP522, WinXP SP523, WinXP SP524, WinXP SP525, WinXP SP526, WinXP SP527, WinXP SP528, WinXP SP529, WinXP SP530, WinXP SP531, WinXP SP532, WinXP SP533, WinXP SP534, WinXP SP535, WinXP SP536, WinXP SP537, WinXP SP538, WinXP SP539, WinXP SP540, WinXP SP541, WinXP SP542, WinXP SP543, WinXP SP544, WinXP SP545, WinXP SP546, WinXP SP547, WinXP SP548, WinXP SP549, WinXP SP550, WinXP SP551, WinXP SP552, WinXP SP553, WinXP SP554, WinXP SP555, WinXP SP556, WinXP SP557, WinXP SP558, WinXP SP559, WinXP SP560, WinXP SP561, WinXP SP562, WinXP SP563, WinXP SP564, WinXP SP565, WinXP SP566, WinXP SP567, WinXP SP568, WinXP SP569, WinXP SP570, WinXP SP571, WinXP SP572, WinXP SP573, WinXP SP574, WinXP SP575, WinXP SP576, WinXP SP577, WinXP SP578, WinXP SP579, WinXP SP580, WinXP SP581, WinXP SP582, WinXP SP583, WinXP SP584, WinXP SP585, WinXP SP586, WinXP SP587, WinXP SP588, WinXP SP589, WinXP SP590, WinXP SP591, WinXP SP592, WinXP SP593, WinXP SP594, WinXP SP595, WinXP SP596, WinXP SP597, WinXP SP598, WinXP SP599, WinXP SP600, WinXP SP601, WinXP SP602, WinXP SP603, WinXP SP604, WinXP SP605, WinXP SP606, WinXP SP607, WinXP SP608, WinXP SP609, WinXP SP610, WinXP SP611, WinXP SP612, WinXP SP613, WinXP SP614, WinXP SP615, WinXP SP616, WinXP SP617, WinXP SP618, WinXP SP619, WinXP SP620, WinXP SP621, WinXP SP622, WinXP SP623, WinXP SP624, WinXP SP625, WinXP SP626, WinXP SP627, WinXP SP628, WinXP SP629, WinXP SP630, WinXP SP631, WinXP SP632, WinXP SP633, WinXP SP634, WinXP SP635, WinXP SP636, WinXP SP637, WinXP SP638, WinXP SP639, WinXP SP640, WinXP SP641, WinXP SP642, WinXP SP643, WinXP SP644, WinXP SP645, WinXP SP646, WinXP SP647, WinXP SP648, WinXP SP649, WinXP SP650, WinXP SP651, WinXP SP652, WinXP SP653, WinXP SP654, WinXP SP655, WinXP SP656, WinXP SP657, WinXP SP658, WinXP SP659, WinXP SP660, WinXP SP661, WinXP SP662, WinXP SP663, WinXP SP664, WinXP SP665, WinXP SP666, WinXP SP667, WinXP SP668, WinXP SP669, WinXP SP670, WinXP SP671, WinXP SP672, WinXP SP673, WinXP SP674, WinXP SP675, WinXP SP676, WinXP SP677, WinXP SP678, WinXP SP679, WinXP SP680, WinXP SP681, WinXP SP682, WinXP SP683, WinXP SP684, WinXP SP685, WinXP SP686, WinXP SP687, WinXP SP688, WinXP SP689, WinXP SP690, WinXP SP691, WinXP SP692, WinXP SP693, WinXP SP694, WinXP SP695, WinXP SP696, WinXP SP697, WinXP SP698, WinXP SP699, WinXP SP700, WinXP SP701, WinXP SP702, WinXP SP703, WinXP SP704, WinXP SP705, WinXP SP706, WinXP SP707, WinXP SP708, WinXP SP709, WinXP SP710, WinXP SP711, WinXP SP712, WinXP SP713, WinXP SP714, WinXP SP715, WinXP SP716, WinXP SP717, WinXP SP718, WinXP SP719, WinXP SP720, WinXP SP721, WinXP SP722, WinXP SP723, WinXP SP724, WinXP SP725, WinXP SP726, WinXP SP727, WinXP SP728, WinXP SP729, WinXP SP730, WinXP SP731, WinXP SP732, WinXP SP733, WinXP SP734, WinXP SP735, WinXP SP736, WinXP SP737, WinXP SP738, WinXP SP739, WinXP SP740, WinXP SP741, WinXP SP742, WinXP SP743, WinXP SP744, WinXP SP745, WinXP SP746, WinXP SP747, WinXP SP748, WinXP SP749, WinXP SP750, WinXP SP751, WinXP SP752, WinXP SP753, WinXP SP754, WinXP SP755, WinXP SP756, WinXP SP757, WinXP SP758, WinXP SP759, WinXP SP760, WinXP SP761, WinXP SP762, WinXP SP763, WinXP SP764, WinXP SP765, WinXP SP766, WinXP SP767, WinXP SP768, WinXP SP769, WinXP SP770, WinXP SP771, WinXP SP772, WinXP SP773, WinXP SP774, WinXP SP775, WinXP SP776, WinXP SP777, WinXP SP778, WinXP SP779, WinXP SP780, WinXP SP781, WinXP SP782, WinXP SP783, WinXP SP784, WinXP SP785, WinXP SP786, WinXP SP787, WinXP SP788, WinXP SP789, WinXP SP790, WinXP SP791, WinXP SP792, WinXP SP793, WinXP SP794, WinXP SP795, WinXP SP796, WinXP SP797, WinXP SP798, WinXP SP799, WinXP SP800, WinXP SP801, WinXP SP802, WinXP SP803, WinXP SP804, WinXP SP805, WinXP SP806, WinXP SP807, WinXP SP808, WinXP SP809, WinXP SP810, WinXP SP811, WinXP SP812, WinXP SP813, WinXP SP814, WinXP SP815, WinXP SP816, WinXP SP817, WinXP SP818, WinXP SP819, WinXP SP820, WinXP SP821, WinXP SP822, WinXP SP823, WinXP SP824, WinXP SP825, WinXP SP826, WinXP SP827, WinXP SP828, WinXP SP829, WinXP SP830, WinXP SP831, WinXP SP832, WinXP SP833, WinXP SP834, WinXP SP835, WinXP SP836, WinXP SP837, WinXP SP838, WinXP SP839, WinXP SP840, WinXP SP841, WinXP SP842, WinXP SP843, WinXP SP844, WinXP SP845, WinXP SP846, WinXP SP847, WinXP SP848, WinXP SP849, WinXP SP850, WinXP SP851, WinXP SP852, WinXP SP853, WinXP SP854, WinXP SP855, WinXP SP856, WinXP SP857, WinXP SP858, WinXP SP859, WinXP SP860, WinXP SP861, WinXP SP862, WinXP SP863, WinXP SP864, WinXP SP865, WinXP SP866, WinXP SP867, WinXP SP868, WinXP SP869, WinXP SP870, WinXP SP871, WinXP SP872, WinXP SP873, WinXP SP874, WinXP SP875, WinXP SP876, WinXP SP877, WinXP SP878, WinXP SP879, WinXP SP880, WinXP SP881, WinXP SP882, WinXP SP883, WinXP SP884, WinXP SP885, WinXP SP886, WinXP SP887, WinXP SP888, WinXP SP889, WinXP SP890, WinXP SP891, WinXP SP892, WinXP SP893, WinXP SP894, WinXP SP895, WinXP SP896, WinXP SP897, WinXP SP898, WinXP SP899, WinXP SP900, WinXP SP901, WinXP SP902, WinXP SP903, WinXP SP904, WinXP SP905, WinXP SP906, WinXP SP907, WinXP SP908, WinXP SP909, WinXP SP910, WinXP SP911, WinXP SP912, WinXP SP913, WinXP SP914, WinXP SP915, WinXP SP916, WinXP SP917, WinXP SP918, WinXP SP919, WinXP SP920, WinXP SP921, WinXP SP922, WinXP SP923, WinXP SP924, WinXP SP925, WinXP SP926, WinXP SP927, WinXP SP928, WinXP SP929, WinXP SP930, WinXP SP931, WinXP SP932, WinXP SP933, WinXP SP934, WinXP SP935, WinXP SP936, WinXP SP937, WinXP SP938, WinXP SP939, WinXP SP940, WinXP SP941, WinXP SP942, WinXP SP943, WinXP SP944, WinXP SP945, WinXP SP946, WinXP SP947, WinXP SP948, WinXP SP949, WinXP SP950, WinXP SP951, WinXP SP952, WinXP SP953, WinXP SP954, WinXP SP955, WinXP SP956, WinXP SP957, WinXP SP958, WinXP SP959, WinXP SP960, WinXP SP961, WinXP SP962, WinXP SP963, WinXP SP964, WinXP SP965, WinXP SP966, WinXP SP967, WinXP SP968, WinXP SP969, WinXP SP970, WinXP SP971, WinXP SP972, WinXP SP973, WinXP SP974, WinXP SP975, WinXP SP976, WinXP SP977, WinXP SP978, WinXP SP979, WinXP SP980, WinXP SP981, WinXP SP982, WinXP SP983, WinXP SP984, WinXP SP985, WinXP SP986, WinXP SP987, WinXP SP988, WinXP SP989, WinXP SP990, WinXP SP991, WinXP SP992, WinXP SP993, WinXP SP994, WinXP SP995, WinXP SP996, WinXP SP997, WinXP SP998, WinXP SP999, WinXP SP1000, WinXP SP1001, WinXP SP1002, WinXP SP1003, WinXP SP1004, WinXP SP1005, WinXP SP1006, WinXP SP1007, WinXP SP1008, WinXP SP1009, WinXP SP1010, WinXP SP1011, WinXP SP1012, WinXP SP1013, WinXP SP1014, WinXP SP1015, WinXP SP1016, WinXP SP1017, WinXP SP1018, WinXP SP1019, WinXP SP1020, WinXP SP1021, WinXP SP1022, WinXP SP1023, WinXP SP1024, WinXP SP1025, WinXP SP1026, WinXP SP1027, WinXP SP1028, WinXP SP1029, WinXP SP1030, WinXP SP1031, WinXP SP1032, WinXP SP1033, WinXP SP1034, WinXP SP1035, WinXP SP1036, WinXP SP1037, WinXP SP1038, WinXP SP1039, WinXP SP1040, WinXP SP1041, WinXP SP1042, WinXP SP1043, WinXP SP1044, WinXP SP1045, WinXP SP1046, WinXP SP1047, WinXP SP1048, WinXP SP1049, WinXP SP1050, WinXP SP1051, WinXP SP1052, WinXP SP1053, WinXP SP1054, WinXP SP1055, WinXP SP1056, WinXP SP1057, WinXP SP1058, WinXP SP1059, WinXP SP1060, WinXP SP1061, WinXP SP1062, WinXP SP1063, WinXP SP1064, WinXP SP1065, WinXP SP1066, WinXP SP1067, WinXP SP1068, WinXP SP1069, WinXP SP1070, WinXP SP1071, WinXP SP1072, WinXP SP1073, WinXP SP1074, WinXP SP1075, WinXP SP1076, WinXP SP1077, WinXP SP1078, WinXP SP1079, WinXP SP1080, WinXP SP1081, WinXP SP1082, WinXP SP1083, WinXP SP1084, WinXP SP1085, WinXP SP1086, WinXP SP1087, WinXP SP1088, WinXP SP1089, WinXP SP1090, WinXP SP1091, WinXP SP1092, WinXP SP1093, WinXP SP1094, WinXP SP1095, WinXP SP1096, WinXP SP1097, WinXP SP1098, WinXP SP1099, WinXP SP1100, WinXP SP1101, WinXP SP1102, WinXP SP1103, WinXP SP1104, WinXP SP1105, WinXP SP1106, WinXP SP1107, WinXP SP1108, WinXP SP1109, WinXP SP1110, WinXP SP1111, WinXP SP1112, WinXP SP1113, WinXP SP1114, WinXP SP1115, WinXP SP1116, WinXP SP1117, WinXP SP1118, WinXP SP1119, WinXP SP1120, WinXP SP1121, WinXP SP1122, WinXP SP1123, WinXP SP1124, WinXP SP1125, WinXP SP1126, WinXP SP1127, WinXP SP1128, WinXP SP1129, WinXP SP1130, WinXP SP1131, WinXP SP1132, WinXP SP1133, WinXP SP1134, WinXP SP1135, WinXP SP1136, WinXP SP1137, WinXP SP1138, WinXP SP1139, WinXP SP1140, WinXP SP1141, WinXP SP1142, WinXP SP1143, WinXP SP1144, WinXP SP1145, WinXP SP1146, WinXP SP1147, WinXP SP1148, WinXP SP1149, WinXP SP1150, WinXP SP1151, WinXP SP1152, WinXP SP1153, WinXP SP1154, WinXP SP1155, WinXP SP1156, WinXP SP1157, WinXP SP1158, WinXP SP1159, WinXP SP1160, WinXP SP1161, WinXP SP1162, WinXP SP1163, WinXP SP1164, WinXP SP1165, WinXP SP1166, WinXP SP1167, WinXP SP1168, WinXP SP1169, WinXP SP1170, WinXP SP1171, WinXP SP1172, WinXP SP1173, WinXP SP1174, WinXP SP1175, WinXP SP1176, WinXP SP1177, WinXP SP1178, WinXP SP1179, WinXP SP1180, WinXP SP1181, WinXP SP1182, WinXP SP1183, WinXP SP1184, WinXP SP1185, WinXP SP1186, WinXP SP1187, WinXP SP1188, WinXP SP1189, WinXP SP1190, WinXP SP1191, WinXP SP1192, WinXP SP1193, WinXP SP1194, WinXP SP1195, WinXP SP1196, WinXP SP1197, WinXP SP1198, WinXP SP1199, WinXP SP1200, WinXP SP1201, WinXP SP1202, WinXP SP1203, WinXP SP1204, WinXP SP1205, WinXP SP1206, WinXP SP1207, WinXP SP1208, WinXP SP1209, WinXP SP1210, WinXP SP1211, WinXP SP1212, WinXP SP1213, WinXP SP1214, WinXP SP1215, WinXP SP1216, WinXP SP1217, WinXP SP1218, WinXP SP1219, WinXP SP1220, WinXP SP1221, WinXP SP1222, WinXP SP1223, WinXP SP1224, WinXP SP1225, WinXP SP1226, WinXP SP1227, WinXP SP1228, WinXP SP1229, WinXP SP1230, WinXP SP1231, WinXP SP1232, WinXP SP1233, WinXP SP1234, WinXP SP1235, WinXP SP1236, WinXP SP1237, WinXP SP1238, WinXP SP1239, WinXP SP1240, WinXP SP1241, WinXP SP1242, WinXP SP1243, WinXP SP1244, WinXP SP1245, WinXP SP1246, WinXP SP1247, WinXP SP1248, WinXP SP1249, WinXP SP1250, WinXP SP1251, WinXP SP1252, WinXP SP1253, WinXP SP1254, WinXP SP1255, WinXP SP1256, WinXP SP1257, WinXP SP1258, WinXP SP1259, WinXP SP1260, WinXP SP1261, WinXP SP1262, WinXP SP1263, WinXP SP1264, WinXP SP1265, WinXP SP1266, WinXP SP1267, WinXP SP1268, WinXP SP1269, WinXP SP1270, WinXP SP1271, WinXP SP1272, WinXP SP1273, WinXP SP1274, WinXP SP1275, WinXP SP1276, WinXP SP1277, WinXP SP1278, WinXP SP1279, WinXP SP1280, WinXP SP1281, WinXP SP1282, WinXP SP1283, WinXP SP1284, WinXP SP1285, WinXP SP1286, WinXP SP1287, WinXP SP1288, WinXP SP1289, WinXP SP1290, WinXP SP1291, WinXP SP1292, WinXP SP1293, WinXP SP1294, WinXP SP1295, WinXP SP1296, WinXP SP1297, WinXP SP1298, WinXP SP1299, WinXP SP1300, WinXP SP1301, WinXP SP1

Anti-Virus Leader HAURI

바이러스 발견주제

◆ 앞으로의 발전 주제와 그에 따른 대응

- PDA 및 모바일 컴퓨터 바이러스
 - PDA 및 모바일 바이러스 현황
 - 현재 PDA 및 모바일에서 활동하는 바이러스의 예
- WAP에서의 바이러스
 - PC와 WAP의 차이점
 - > 초기 단계에서부터 보안이 고려
 - > DATA의 기밀성과 개인 정보 보호 필요성
 - > Content의 취약
 - WAP 1.2
 - > WAP 1.2 이상의 프로토콜에서는 바이러스를 만들 수 있는 새로운 모듈을 제공
 - > 핸드폰 주소록을 참조하는 모듈
 - > SMS 메시지를 보낼 수 있는 모듈
 - > 전화를 걸 수 있는 모듈

Anti-Virus Leader HAURI

바이러스 발견주제

◆ 앞으로의 발전 주제와 그에 따른 대응

- PDA 및 모바일 환경에서 위협 유형

배포형 바이러스 기본 확장 드롭스 기반 확장 배포형 바이러스/ 인간수 충동 확장	PDA 및 모바일 환경에서 종종 드롭스 형태로 활동하는 바이러스는 바이러스가 실행되면서 파일을 복제 예) 1. 배너지(Banner) : 웹상 플로그인 실행 후 파일 및 서버 플로그인 감염 2. Linux Crash : 네트워크 파일 시스템 플로그인 감염 3. WAP 1.2 이상의 프로토콜은 파일 시스템은 드롭스 형태로 활동하는 바이러스이다. 스마트폰 파일 시스템은 파일 시스템 자체에 파일이 부팅되는 바이러스이며, 터치스크린 환경은 사용자 입력에 기반한 바이러스이다. 예) 1. 토크나이트 : 스마트폰 파일 시스템에 파일이나 폴더를 추가하는 바이러스로 상당수 토크나이트 바이러스는 파일 시스템 자체에 파일이나 폴더를 추가하는 바이러스이다. 2. 토크나이트 바이러스는 파일 시스템에 파일이나 폴더를 추가하는 바이러스이다. 드롭스 형태로 활동하는 바이러스는 바이러스가 실행되는 경로로 바이러스를 전파하는 경로로 매우 다양한 바이러스는 드롭스 형태로 활동하는 바이러스이다. 드롭스 형태로 활동하는 바이러스를 전파하는 경로로 매우 다양한 바이러스는 드롭스 형태로 활동하는 바이러스이다.
--	--

Anti-Virus Leader HAURI

바이러스 대응체계의 선진국 동향 분석

◆ 미국의 사이버테러 대응 전략

- 사이버 대응의 기본 원칙
 - 민·관 협력
 - 규제 확장
 - 국민의 자유와 프라이버시 보호
 - 의회와의 조율
 - 주 및 지방 정부와 협력
- 조정기관의 지정
- 전략적 보안 원칙
 - 전자화를 위한 두분 보안
 - 과학기술 발전에 따른 보안 수단 개발

Anti-Virus Leader HAURI

바이러스 대응체계의 선진국 동향 분석

◆ 일본의 사이버테러 대응 체계

- 정보시스템과의 접속시 보안 대책
- 전화접속시의 대책
- 무선등용 네트워크에서의 대책
- 네트워크 계획, 설계 구축시 대책
- 컴퓨터 바이러스 대책
- 사회 공학 대응 대책

Anti-Virus Leader HAURI

바이러스 발견주제

◆ 앞으로의 발전 주제와 그에 따른 대응

- WAP 바이러스의 활동 시나리오
 - WAPI 2.0의 새로운 모듈 기능을 이용
 - > 악성 사이트의 링크를 전화번호부에 등록된 번호 모두에게 SMS 메시지 보냄
 > 사용자가 메시지를 확인하게 되면 자신의 전화번호부에 등록된 번호로 다시 악성 사이트의 링크를 보냄
 - 모바일폰 바이러스들이 바이러스 개발자의 수입의 수단으로 이용
 - > 전화번호 험의 변경, 핸드폰 세팅정보 변경 등...
 - WAP에서의 트로이 목마
 - > 개인정보 유출, 데이터 손실 피해, 현재 구현 가능...

Anti-Virus Leader HAURI

바이러스 발견주제

◆ 앞으로의 발전 주제와 그에 따른 대응

- PDA 및 모바일, 정보가전 등 다양한 환경에서의 방역이 필요
 - WAP의 구조
 - Anti Virus for WAP Gateway
 - WAP 서비스망의 구성
 - 모바일폰 백신의 필요

◆ 유비쿼터스 환경에서 바이러스 역시 진화

