

VAN ITT MINDEN, MINT KARÁCSONYKOR

Pénzt vagy életet!

A múlt hónapban a hamis antivírus programokkal foglalkoztunk. Ezek fő jellemzője, hogy nem létező fertőzéseket imitálva pénzt próbálnak meg kizsarolni tőlünk. A nagy előd, a magyar Furkó Antivírus lehet, hogy talán mintául szolgálhatott az utódoknak. Sorozatunk mostani, tizenhatodik epizódjában mindenesetre bemutatjuk ezt a korát megelőző programot, valamint néhány más váltságdíjszedő kártevőt.

Ki a múltat háborgatja, folyjon ki a fél szeme. De ki a múltat elfelejti, annak mind a kettő – mondja *Alexander Solzsenyicin*. Mi sem tehetjük meg, hogy korábbi malőrökről elfeledkezzünk, és igazság szerint nem is érdemes ezt tenni, hiszen nagyon tanulságos esetekről van szó.

Ransomware – ezt a kategóriát magyarul zsaroló, váltságdíjat követelő kártevőnek nevezhetjük. Megszületését egy 1989-es esethez kötik, ahol egy cég AIDS-szel kapcsolatos információs floppylemezt küldött szét mintegy huszonhatezer egészségügyi intézmény címére. A címjegyzék tanúsága szerint három példányt Magyarországra is elküldtek: a Hematológiai Intézetbe, a János Kórházba és a KFKI-be, de ezeknek – állítólag postázás közben – lába kelt, ami jelen esetben utólag szerencsés fordulatnak is értékelhető. A lemez egy aljas programozási trükkel operált, és közben figyelte a rendszerindítások számát. Egy saját algoritmus alapján folyamatosan titkosította a merevlemez az állományokat és a könyvtárakat. Szerencsés esetben, ha valaki idejekorán észlelte, korai fázisban tiszta rendszerlemezről bootolva még el tudta menteni a saját adatait. A kilencvenedik újraindítás után aztán

a trójai az alábbi üzenetet jelenítette meg a képernyőn, angolul: „A szoftverbérleti szerződés erre a számítógépre lejárt. Amennyiben még szeretné használni ezt a számítógépet, meg kell újítania a bérleti szerződést. További információért kapcsolja be a nyomtatót és nyomja meg az Enter billentyűt”. A kinyomtatott üzenetben aztán szerepelt egy panamai postafiók címe és hogy 189, illetve 378 amerikai dollárt kell küldeni a készítőnek váltságdíjként, amit fizethetünk csekken vagy átutalással is. Ez egy szintizsra zsarolási manőver volt, és vegyük észre azt is, hogy remek érzékkel kihasználta, hogy sokan érdeklődtek az akkor még új, ismeretlen és félelmetes AIDS iránt. A történet utóéletéhez tartozik, hogy később sikerült elfogni a készítőt, egy bizonyos *Joseph L. Poppot*, aki Panamában a PC Cyborg Corporation nevű céget jegyezte és majd’ egy évig készítette elő ezt az akcióját.

Hány fél egy egész?

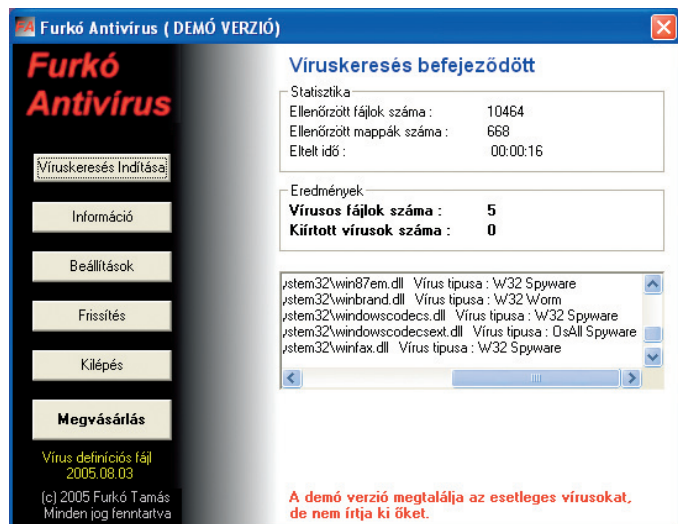
Korábban, a 12. epizódban már megemlékeztünk a körülbelül 1995-ben feltűnt One Half nevű DOS-os vírusról, amely a merevlemezről történő bootolásként 2-2 cylinder teljes tartalmát titkosította, a merevlemez végéről indulva. Ha csak simán mente-

Dear Customer:

It is time to pay for your software lease from PC Cyborg corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed invoice, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive: a renewal software package with easy to follow, complete instructions; an automatic, self-installing diskette that anyone can apply in minutes.

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashiers check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Az AIDS tájékoztatólemezen terjesztett trójai szerzője állítólag egy évig készítette elő az akcióját. Azt nem tudni, hogy mire gondolt, amikor megadta cége nevét és a panamai postafiókát. Mindenesetre ezzel nem tette túl magasra a lécezt az utána nyomozó szövetségi és titkos ügynököknek



Furkó Tamás műve valódi szellemi elődnek tekinthető a mai hamis antivírusok szempontjából. Íme a szokásos öt .dll állomány, ami állítólag mindenkinél „fertőzött”. Mi most mosolygunk ezen, de igazából egyáltalán nem mulatságos a kevésbé hozzáértők ilyen átverése

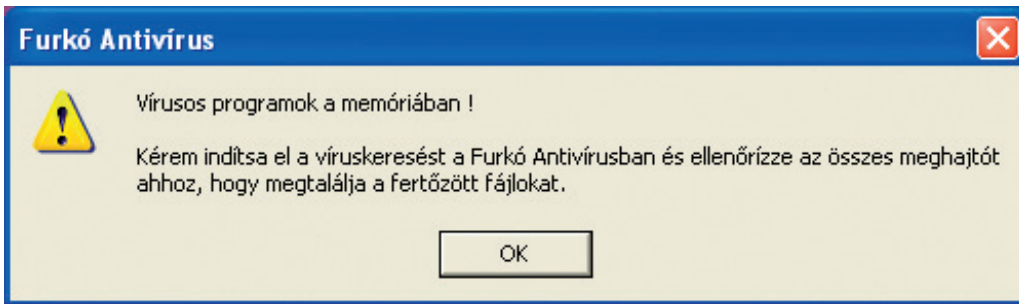


Bár a PC Cyborg Corporation már megszűnt, az emléke megmaradt a Wikipédián: en.wikipedia.org/wiki/PC_Cyborg_Trojan

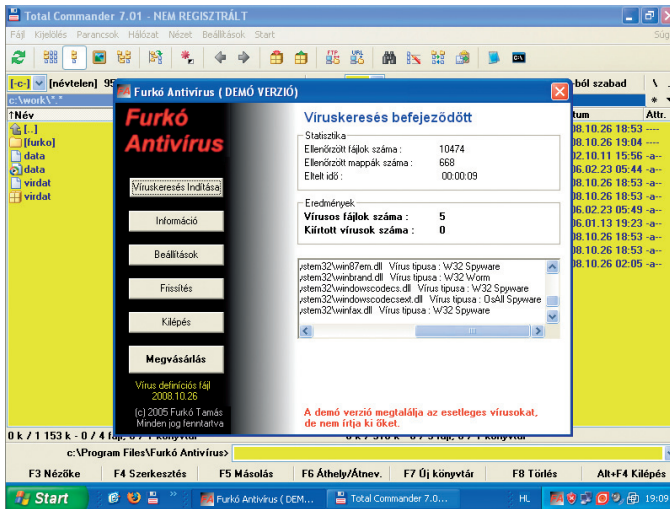
sítettük a gépet, az elkódolt részhez soha többé nem férünk hozzá, hiszen a szükséges kulcsfontosságú információt a Master Boot Recordba (MBR) beköltöztött vírusban tárolták. Egy meggondolatlan „fdisk /mbr” parancs után – az egyedi kód hiányában már lehetetlen volt az adatok visszaalakítása. Szerencsére később *Leitold Ferenc* vírusvédelmi szakértő készített hozzá egy egyedi dekódoló segédprogramot OneHalf Killer né-

ven, amely a tényleges fizikai mentés előtt képes volt visszaalakítani az eredeti adatokat. Itt valójában ugyan nem kértek váltságdíjat, de a károkozást igyekeztek minél tovább rejtve tartani, hogy ezzel is fokozhassák a felhasználót érő kárt.

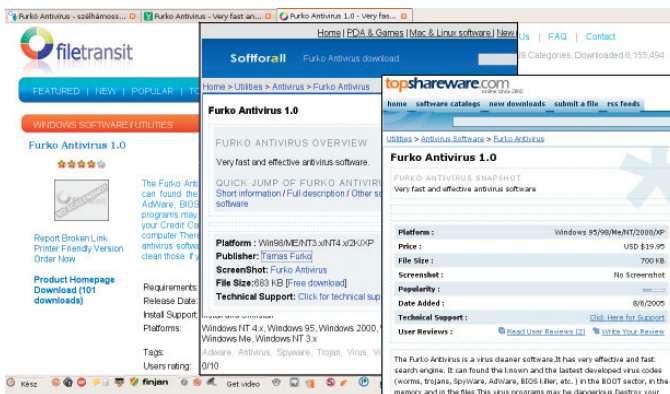
Csak kiegészítésként érdemes megemlíteni, hogy a OneHalf vírus kora ellenére nem feltétlenül csak a múltat jelképezi. Képes arra, hogy egy mai windowsos rendszeren is ténykedjen,



Még az újonnan telepített gépeken is megkaptuk a figyelmeztetést. Valószínűleg ez indíthatta be a felhasználók fantáziáját, hogy itt valami nagyon gyanús machináció zajlik a háttérben



Ez a kép azért vicces, mert a frissítés idejéhez beírta az aznapi dátumot



Lustaság és hanyagság – akár ez is lehetne ennek kisplasztikai biennálén induló műnek a címe. A letöltési oldalak jól láthatóan nagy ívben tesznek arra, mit kínálnak fel letöltésre

hiszen a MBR-ből indul. Ezt igazolja, hogy azóta is felbukkan néha néhány számítógépen. Terjedni persze nehezen tud, mert a Windows elindulását követően már törölődik a memóriából, viszont ahányszor újraindítjuk a gépet, annyiszor végzi el a következő 2 cylinder kódolását.

Hát ennyit a távoli múlttól, most nézzünk néhány további frissebb érdekességet a zsarolás műfajából.

Magyar gépre magyar „antivírust”

2005 táján megjelent az interneten egy Furkó Antivírus nevű csomag, amely nemcsak a www.furkoantivirus.com weblapon, hanem számos letöltőoldal kínálatában is szerepelt.

Ha valaki vette a fáradságot és letöltötte, érdekes dolgokat tapasztalhatott. Először is a többi vírusirtó próbálva változathoz képest nem egy időkorlátozással szembesülünk a demóban, ami amúgy teljes értékűen működik, hanem szokatlan módon az ingyenes próbaváltozat csak kijelzte a veszélyeket, de irtani csak és kizárólag a fizetős változattal tudtunk a készítő ígérete szerint.

Csiszér Béla (a NOD32 programot Magyarországon forgalmazó Sicontact Kft. vezetője) nevéhez köthetik a nagy leleplezés, rájött ugyanis, hogy a program könyvtárában található data.dat fájl valójában egy EA Sports játékból származó MP3 audiofájl, ahol a bemondó egy autóverseny

kezdetét jelenti be – ezt érdemes is átnevezés után meghallgatni, ahol világosan hallani benne, hogy a Nascar autóverseny nevét is emlegetik. Nem érdemi vírusadatbázis állomány az eredeti virdat.dat sem, ez pedig egy jelszóval védett közönséges RAR tömörített állomány. A vírusirtó adatbázisának „frissítésekor” egy ingyenes magyar tárhelyszolgáltató szerveréről letöltődő új virdat.dat sem tartalmaz a kártevők azonosításához használható információkat, ugyanis ez az állomány a Moorhuhn 2 című csirkevadász sikerjáték mudGE.dll fájlja volt, átnevezve. Mi a mostani ki-

sérletnél már ezt nem is tudtuk letölteni, a „frissítés” után csak egy 0 bájt hosszú virdat.dat állományt kaptunk, viszont a program felhasználói menüjében a frissítés ideje az aktuális dátumra frissült. Szóval szemfényvesztés az egész.

A király meztelen

Főleg a fertőzésre, a kénytelen ablakokra és a fizetős változat megvásárlására tett erőfeszítésekre koncentráltuk eddig figyelmünket, azonban van még egy fontos szempont, amit mindenképpen érdemes megemlíteni. Amivel még nagy bajt okozhat egy ilyen hamis antivírus program, az a hamis biztonságerzet, amit a gyanútlan felhasználókban kelthet: aki telepíti, csak hiheti, hogy így már védve van a vírusoktól, kémprogramoktól – holott erről, ahogyan láttuk is, szó sincsen.

A Furkó Antivírus szinte minden tekintetben nagy elődnek tekinthető a manapság ipari méretekben zajló hamis antivírus üzletbiznisz szempontjából: nem végez érdemi vírusírtást, mert saját maga a kártevő; újonnan telepített tiszta rendszeren is talál

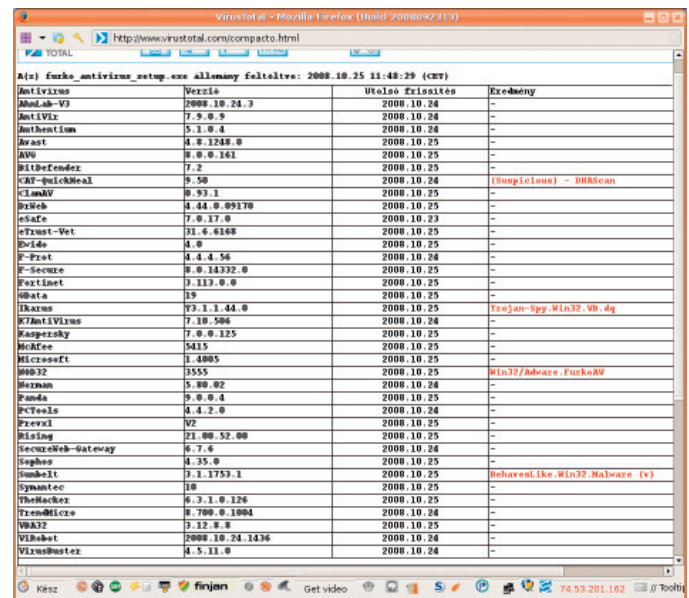
meta name "description"

content="A Furkó Antivírus egy 5 csillagos értékeléssel nagyon gyors és hatékony antivírus szoftver"

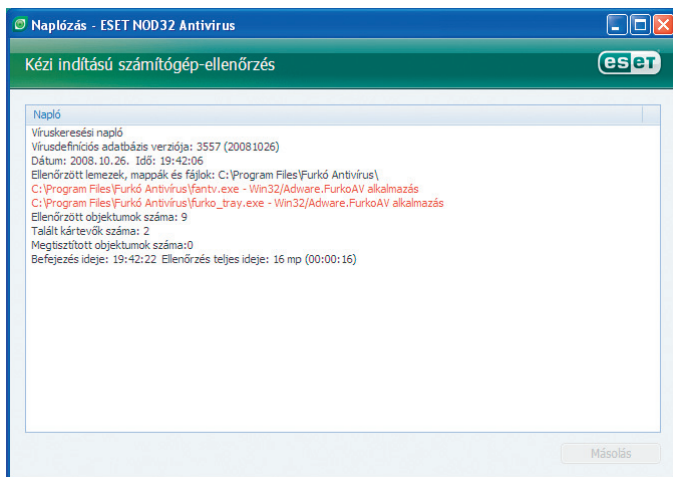
meta name "keywords"

content="antivirus.com antivirus, vírusirtó, antivirus, anti-vírus,anti-vírus,vírus irtó, vírus irtó, szex, sex, tini, szex, baszas, pina, fuck, víruskereső, vírus kereső, víruskereső, vírus, kereső, szex,sex,mp3,zene,film,dvd,cd,letöltés,download, software, ferrari, lamborghini, porsche, mercedes, bmw, schumacher, forma 1, sport, foci, football, internet, hardware, vásárlás"

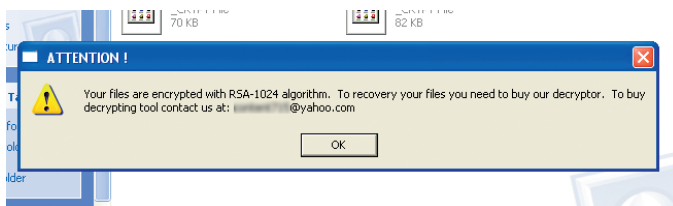
Bár a weboldal már nem működik – a leleplező HWSW-s, illetve origós cikk után azonnal megszűnt –, a lementett változat sok mindenről árulkodik a figyelmes szemlélőnek. Az biztos, hogy az ilyen kulcsszavak nem sok bizalmat ébresztenek abban, aki egy komoly biztonsági program weblapján véletlenül belekukkant az oldal HTML-kódjába



Négy, csak négy legény van talpon a vidéken a VirusTotalon végzett ellenőrzés szerint. Azaz a hazai ál-antivírus termést külföldön csak kevesen ismerik fel kártevőként



A kísérletezéshez ki kellett kapcsolni a NOD32 antivírust, mert azonnal beírtott már a Furkó telepítőcsomagjára is



Amit senki sem szeretne látni a saját monitorán: „Az ön állományait RSA-1024 algoritmussal elkódoltuk. Ezek visszaalakításához szüksége lesz a mi dekódoló programunk megvásárlására. A dekódoló eszköz megvásárlásához kérjük, írjon a következő e-mail címre!”

„fertőzést”; az adatbázis-frissítés egyáltalán nem oldja meg a gondjainkat vagy nem is csinál semmit; és végül, de nem utolsósorban pénzt akar – ez a program fő célja.

Ami még nevesítéses vagy inkább sírnyaló, hogy a Furkó Antivírus még a mai napig (2008. novemberben készült ez az írás) szerepel számos letöltéssel foglalkozó honlap kínálatában. Egy magára valamit is adó letöltőoldalon egy termékéről hogy mondhat olyat vagy másolhat át bambán, hogy „Uses cutting edge technology to detect virus and remove them immediately”? Ki sem próbálták, annyi szent, csak ment az iparszerű tartalom- és linkgyártás, kopi meg a paszta, amelyet egy megfelelően idomított pávián is megtehetne megfelelő mennyiségű banánnal dresszírozva. Sajnos, ahogy az élet más területén is, sok mindenben a felhígulást és a spórolást látjuk: könyvek jelennek meg

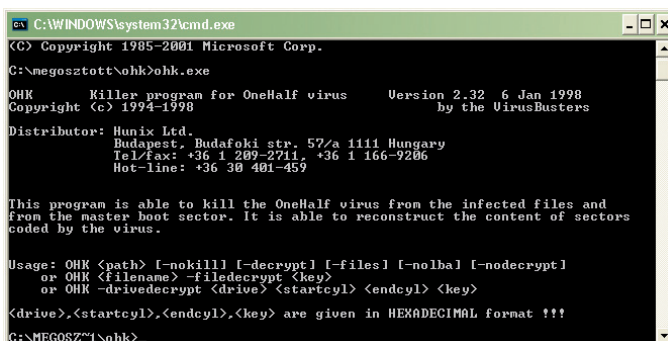
futószalagon szakmai lektor és nyelvi ellenőrzés nélkül, de ez már messzire vezetne, kanyarodjunk vissza a ransomware témájához.

Zsarolók és váltságdíjak

Mintha ez a gondolatmenet éledt volna ismét újjá a GPCode kártevő 2008-ban megjelent új változata esetében is, amelyre a Kaspersky kutatói hívták fel a figyelmet. A család első tagja még 2005 decemberében látott napvilágot. A GPCode kártevő új változata különösen erős, 1024 bites RSA-titkosítással kódolja el a felhasználó adatait (például a .doc, .jpg, .pdf kiterjesztésű fájlokat), majd letörli az eredeti, kódolatlan példányokat. Ha végzett, akkor üzenetet küld a felhasználónak, hogy az állományai túsul lettek ejtve, és némi készpénz fejében felajánlja a titkosítást feloldó kulcsot. A titkosítás ezekben az esetekben

Kaspersky Lab - Kaspersky Lab Technical Support - Kaspersky Lab's Fan Club				
Welcome Guest (Log In Register)				
Kaspersky Lab Forum > Stop GPCode > GPCode subforum				
1 Pages 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000				
Topic Title	Replies	Topic Starter	Views	Last Action
[IMPORTANT] @Data recovery	2	Medvedevskiy	4814	26.08.2008 21:28 Last post by: Medvedevskiy
[IMPORTANT] @Recovery of deleted files	2	Medvedevskiy	4186	26.08.2008 18:59 Last post by: Medvedevskiy
[IMPORTANT] @Recently asked questions	1	Medvedevskiy	5836	20.08.2008 18:18 Last post by: Medvedevskiy
[IMPORTANT] @Data recovery of deleted files	1	Medvedevskiy	3614	20.08.2008 17:48 Last post by: Medvedevskiy
[IMPORTANT] @Recovery of deleted files	1	Medvedevskiy	6323	20.08.2008 15:41 Last post by: Medvedevskiy
[IMPORTANT] @Data recovery of deleted files	0	Medvedevskiy	14874	08.08.2008 20:59 Last post by: Medvedevskiy
[IMPORTANT] @Data recovery of deleted files	0	Medvedevskiy	8433	08.08.2008 18:48 Last post by: Medvedevskiy

A GPCode zsaroló vírus visszafertőzésére nemcsak felhívást tett közzé a Kaspersky cég, de a kapcsolódó fórumon a szakemberek a világ minden tájáról meg is osztották a tapasztalataikat



OneHalf Killer: ez a remek segédprogram sokaknak mentette meg a merevlemezben csapdába esett létfontosságú adatait



Vírusirtót készítené, de nem boldogul? Sebaj, vegyen egy DLL-t egy lövöldözős játékból, egy MP3 állományt egy másik, autóversenyes játékból, és máris kész az új vírusismereti adatbázis. Akármilyen hihetetlen, de volt, aki tényleg így csinálta

a brute force (azaz nyers erő, vagyis próbálgatásos) módszerrel akár több millió évig is eltarthatna, de szerencsére az antivírus cégek összefogásával sikerült hibát találni a kártevőben és ennek segítségével visszaállítani a kódolt fájlokat. Az új, GPCode.AK jelű változat már 143-féle állománytípusot tesz olvashatatlanná, amihez a Windows beépített Microsoft Enhanced Cryptographic Provider modulját használja. A Kaspersky cég nyáron felhívást tett közzé, amelyben titkosítási szakembereket toborzott a visszafertítéshez. Ennek meg is lett az eredménye, első körben sikerült kideríteni, hogy a már elkódolt állományok eredeti állományainak törlése egyszerű delete funkcióval történik, ezért minden „Undelete” segédprogram segíthet ezekben az esetekben, ha még nem történt felülírás. Ez kétségkívül hiba volt a támadók részéről, amit a következő kártevőverzióban már biztosan javítani fognak. Később aztán érdemi megoldás is született az állományok mentésére, bár a visszakódolás hatékonysága itt csak körülbelül 80–90 százalékosra sikerült.

Annyit mindenesetre láthatunk, hogy bár szinte minden esetben vi-

szonylag kis összegeket kértek az elkövetők, a zsarolásból befolyó pénz átvétele elég körülményes és rendszerint kinyomozható, ezért e rizikótényező mellett valószínűleg nem találták meg a számításukat. Erre utal az is, hogy néhány esetben – a nulradik napi sebezhetőségek demonstrációs exploit kódjaihoz hasonlóan – igyekeztek közvetlenül az antivírus cégeknél kopogtatva pénzzé tenni a titkosítótípusjukat. Egy biztos, nekünk felhasználóknak ezek az esetek remek példák arra, hogy ne hanyagoljuk el munkáink rendszeres mentését külső adathordozóra.

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemen@pcworld.hu).

Csizmazia István,

vírusvédelmi tanácsadó

Sicontact Kft., a NOD32 antivírus magyarországi képviselője
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

www.eset.hu/virus

www.antivirus.hu