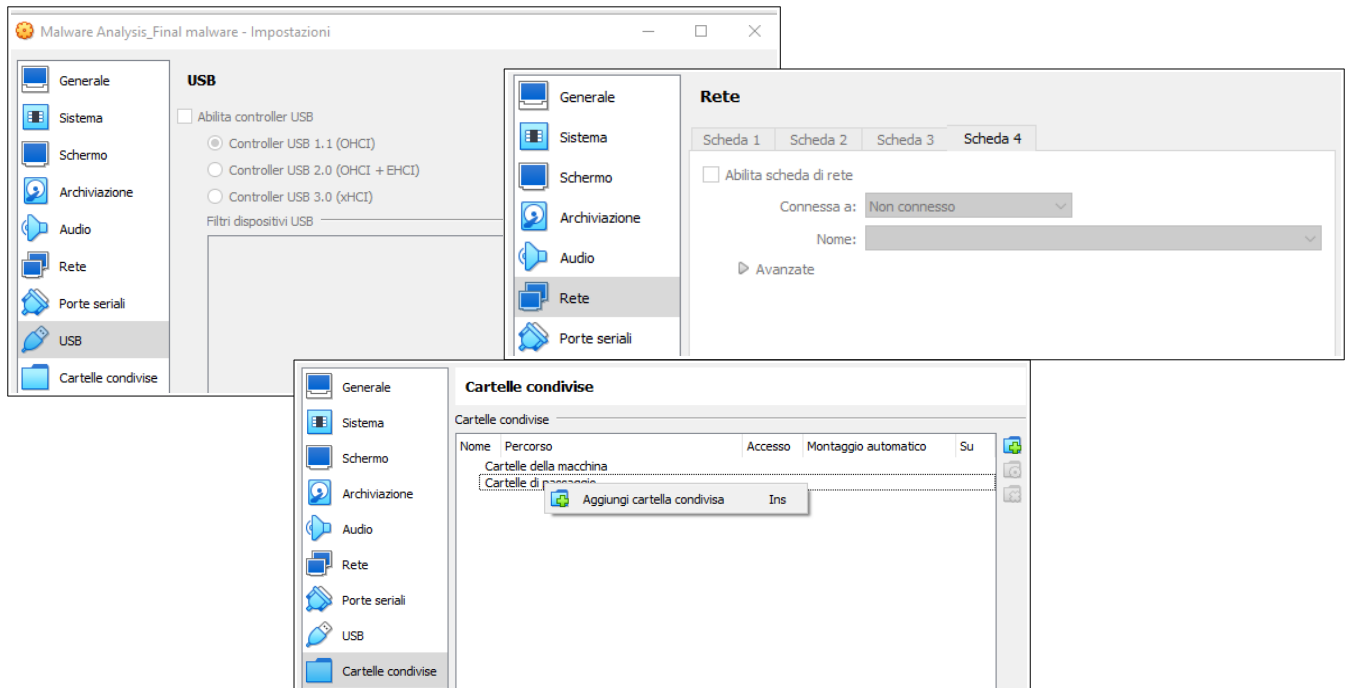


Analisi Dinamica Basica

Obiettivo: Effettuare un'analisi dinamica basica di un Malware su Windows XP 32 bit.

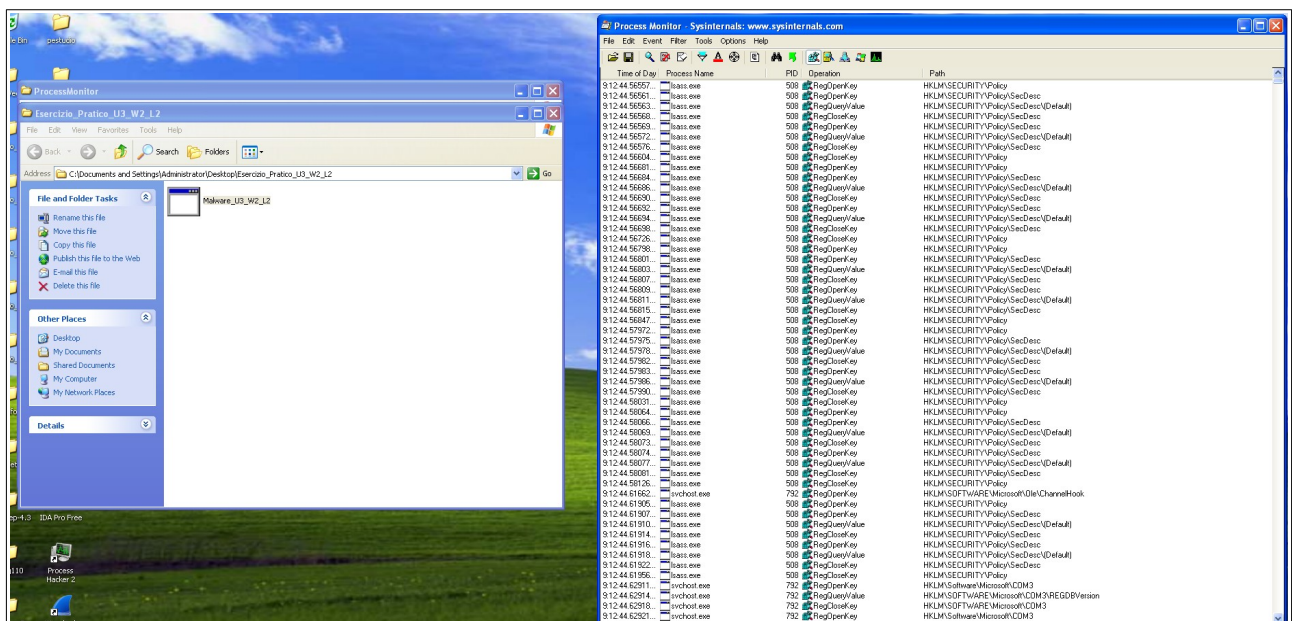
1) Macchina Offline

Prima di iniziare mi sono assicurato che la macchina virtuale fosse completamente *offline* e senza alcun collegamento con la macchina **Host Principale** controllando **Scheda di Rete Disattiva**, **Porte USB disattivate** e **Cartelle Condivise non collegate**.

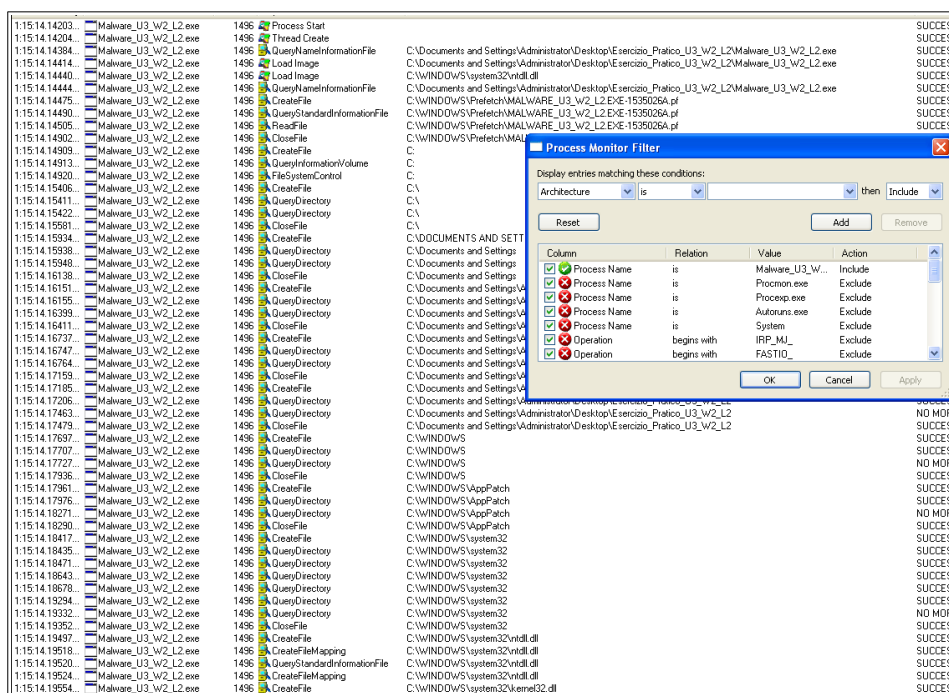


2) Avvio ProcMon e Malware

La traccia chiede di utilizzare il tool **Process Monitor** per analizzare il comportamento del **Malware**. Per cominciare ho avviato il tool per poi cliccare sul file .exe che la traccia chiede.



Essendo un tool che monitora continuamente i processi della macchina ho utilizzato un filtro per mostrare soltanto le modifiche riguardo il **Malware avviato (Malware_U3_W2_L2)**



Successivamente ho utilizzato i vari **switch** per poter controllare le singole tipologie di eventi.

3) Eventi di Registro

Il primo **switch** si riferisce alle attività relative alle **Chiavi di Registro** del Sistema Operativo.

1:15:14.14203...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Desired Access: Read
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Index: 0, Name: {34835ab-37b5-4631-9b89-ed5f9bd1328}
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Desired Access: Read
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_BINARY, Length: 16, Data: 5B 4F 30 4F 95 4A 89 6A 00 BC 31 15 40 15
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 4, Data: 32771
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Index: 1, Name: {7b8dc2e-3076-4d89-a57b-b81372dbb81}
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Desired Access: Read
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_BINARY, Length: 16, Data: 67 80 D4 8B 34 3F D3 BC E9 DC 64 67 04 F3 94
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 4, Data: 32771
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 8, Data: 0
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Index: 2, Name: {81d1e15-d654-4762-b164-7c29d6cae3f}
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Desired Access: Read
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_BINARY, Length: 16, Data: 32 78 D2 DC FE C8 82 DC BA B0 66 D0 84 7D 10
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 4, Data: 32771
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 8, Data: 0
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Index: 3, Name: {943e076-8953-42a5-6411-085cc18a68d}
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Desired Access: Read
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_BINARY, Length: 16, Data: 80 3A 2A D8 42 E8 D8 56 0E 25 0E 4D F8 15 2F 67
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 4, Data: 32771
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 8, Data: 0
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Index: 4, Name: {d371eaf-44ab-4f64-a02e-b91490411b6}
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Desired Access: Read
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_BINARY, Length: 16, Data: 38 6B 08 5F 64 EC F6 69 D3 68 95 64 22 C0 1E 00
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 4, Data: 32771
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 8, Data: 0
1:15:14.14204...	Malware_U3_W2_L2.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\OHashes	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0

Le attività svolte sui registri da questo Malware sono principalmente

- **Elencare** le Chiavi di Registro in una Directory (**RegEnumKey**);
- **Aprire** le Chiavi sopracitate, o tentare almeno di aprirle (**RegOpenKey**);
- **Interrogare** le Chiavi stesse per ottenerne i valori specifici (**RegQueryValue**).

Nell'analisi vengono analizzate le chiavi di registro delle categorie **HKEY_CURRENT_USER** e **HKEY_LOCAL_MACHINE** (HKCU e HKLM).

Permettere ad un Malware di leggere le **Chiavi di Registro** è molto pericoloso; potrebbe ottenere l'accesso ad informazioni sensibili o compromettere le impostazioni di sicurezza del Sistema.

4) File System

Il secondo *switch* mostra invece attività relative ai **File System** di **Windows**.

1:15:14.17897	Malware_U3_w2_L2.exe	1496	CreateFile	C:\Windows	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1:15:14.17707	Malware_U3_w2_L2.exe	1496	QueryDirectory	C:\Windows	SUCCESS	0; 1; ...; FileInformationClass: FileInformation, 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

Nella prima parte dell’analisi il Malware crea o importa le librerie di cui ha bisogno per funzionare e per interagire col Sistema Operativo (**kernel32**), con i Registri (**advapi32.dll**), con la gestione delle Operazioni di sicurezza (**secur32.dll**) e altre.

1:15:14.21304	Malware_U3_w2_L2.exe	1496	CreateFile	C:\Windows\System32\advapi32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.21325	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\advapi32.dll	SUCCESS	AllocationSize: 700,000; EndOfFile: 700,000; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.21327	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\advapi32.dll	SUCCESS	SyncType: SyncTypeOther
1:15:14.21331	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\advapi32.dll	SUCCESS	AllocationSize: 618,496; EndOfFile: 618,496; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.21361	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\advapi32.dll	SUCCESS	SyncType: SyncTypeOther
1:15:14.21506	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\advapi32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.21507	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\advapi32.dll	SUCCESS	AllocationSize: 985,728; EndOfFile: 985,728; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.21511	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\advapi32.dll	SUCCESS	SyncType: SyncTypeOther
1:15:14.21545	Malware_U3_w2_L2.exe	1496	CreateFile	C:\Windows\System32\secur32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.21570	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\secur32.dll	SUCCESS	AllocationSize: 57,344; EndOfFile: 56,320; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.21572	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\secur32.dll	SUCCESS	SyncType: SyncTypeOther
1:15:14.21576	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\secur32.dll	SUCCESS	SyncType: SyncTypeOther

Nella seconda parte dell’analisi invece il **Malware** crea e “killa” il processo **svchost.exe**, probabilmente per mascherare le modifiche che vuole effettuare al Sistema o sfruttare il processo legittimo per eseguire il proprio codice malevolo.

1:15:14.26336	Malware_U3_w2_L2.exe	1496	CreateFile	C:\Windows\System32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, SP: Filter: svchost.exe; 1: svchost.exe, FileInformationClass: FileInformation
1:15:14.26341	Malware_U3_w2_L2.exe	1496	QueryDirectory	C:\Windows\System32\svchost.exe	SUCCESS	
1:15:14.26343	Malware_U3_w2_L2.exe	1496	CreateFile	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26345	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, SyncType: SyncTypeOther
1:15:14.26347	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	AllocationSize: 16,384; EndOfFile: 16,384; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.26351	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26353	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.26355	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\svchost.exe	SUCCESS	AllocationSize: 16,384; EndOfFile: 16,384; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.26357	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
1:15:14.26359	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26361	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, SyncType: SyncTypeOther
1:15:14.26363	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26365	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.26367	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\svchost.exe	SUCCESS	AllocationSize: 16,384; EndOfFile: 16,384; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.26369	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
1:15:14.26371	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26373	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, SyncType: SyncTypeOther
1:15:14.26375	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26377	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.26379	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\svchost.exe	SUCCESS	AllocationSize: 16,384; EndOfFile: 16,384; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.26381	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
1:15:14.26383	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26385	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.26387	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\svchost.exe	SUCCESS	AllocationSize: 16,384; EndOfFile: 16,384; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.26389	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
1:15:14.26391	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26393	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.26395	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\svchost.exe	SUCCESS	AllocationSize: 16,384; EndOfFile: 16,384; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.26397	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
1:15:14.26399	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26401	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.26403	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\svchost.exe	SUCCESS	AllocationSize: 16,384; EndOfFile: 16,384; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.26405	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
1:15:14.26407	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26409	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.26411	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\svchost.exe	SUCCESS	AllocationSize: 16,384; EndOfFile: 16,384; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.26413	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
1:15:14.26415	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26417	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.26419	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\svchost.exe	SUCCESS	AllocationSize: 16,384; EndOfFile: 16,384; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.26421	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
1:15:14.26423	Malware_U3_w2_L2.exe	1496	QueryOpen	C:\Windows\System32\svchost.exe	SUCCESS	CreationTime: 4/14/2008 5:42:38 AM, LastAccessTime: 7/4/2023 1:15:14 PM, LastWriteTime: 4/14/2008 5:42:38 AM, ChangeTime: 9/20/2008 5:42:38 AM
1:15:14.26425	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, SyncType: SyncTypeOther
1:15:14.26427	Malware_U3_w2_L2.exe	1496	QueryStandardInformationFile	C:\Windows\System32\svchost.exe	SUCCESS	AllocationSize: 16,384; EndOfFile: 16,384; NumberOfLinks: 1; Deletable: Pending; File, Directory: False
1:15:14.26429	Malware_U3_w2_L2.exe	1496	CreateFileMapping	C:\Windows\System32\svchost.exe	SUCCESS	SyncType: SyncTypeOther

6) Processi e Thread

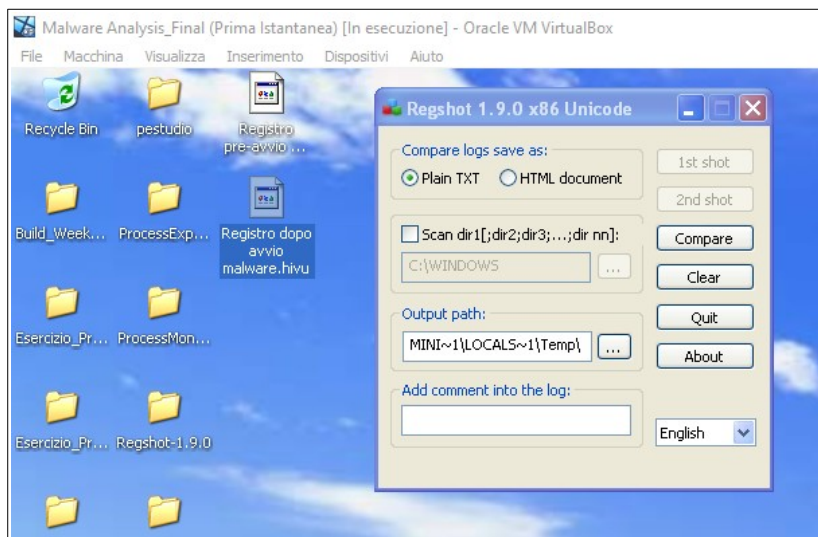
Il quarto *switch* mostra le attività relative ai **Processi e Thread** che il **Malware** avvia o meno.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:54:14.003	Malware_U3_W2_L2.exe	1496	Process Start		SUCCESS	Parent PID: 248. Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe"
11:54:14.004	Malware_U3_W2_L2.exe	1496	SUCCESS		SUCCESS	Thread ID: 168
11:54:14.014	Malware_U3_W2_L2.exe	1496	Thread Create	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000. Image Size: 0x0000
11:54:14.040	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\user32.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x40000
11:54:14.057	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\user32.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x40000
11:54:14.076	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\user32.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x20000
11:54:14.082	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\user32.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x40000
11:54:14.301	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\advapi32.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x80000
11:54:30.975	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\user32.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x40000
11:54:30.984	Malware_U3_W2_L2.exe	1496	Load Image	C:\WINDOWS\System32\advapi32.dll	SUCCESS	Image Base: 0x780000. Image Size: 0x1000
11:54:31.340	Malware_U3_W2_L2.exe	1496	Process Create		SUCCESS	Parent PID: 248. Command line: "C:\WINDOWS\System32\user32.exe"
11:54:31.356	Malware_U3_W2_L2.exe	1496	Thread Exit		SUCCESS	Thread ID: 168. Use Time: 0.000000. Real Time: 0.000000
11:55:33.025	Malware_U3_W2_L2.exe	1496	Process Exit		SUCCESS	Exit Status: 0. CPU: 0.019620 seconds, Kernel Time: 0.002500 seconds, Private Bytes: 274.432, Peak Private Bytes: 307.200, Working

Si possono notare i caricamenti delle varie librerie (alcune viste prima) e la creazione del processo **svchost.exe** sopracitato dal momento che viene avviato per poi “killarsi” automaticamente.

7) Modifiche del Registro

Grazie al tool **Regshot** si possono creare delle *Istantanee* pre e dopo l'avviamento di un **Malware** per poterle confrontare e osservare le modifiche che vengono eseguite sulle **Chiavi di Registro**.



Salvando il 1st (*pre-avvio Malware*) e 2nd shot (*post avvio Malware*) possiamo grazie al tool confrontarli in un file di testo che potremo successivamente salvare dove vogliamo.

[illegible]

Ci sono stati da come leggiamo *30 modifiche* alle **Chiavi di Registro** con relativi **Path**.

8) Conclusioni

Alla luce dei risultati della scansione con **Process Monitor** e con **Regshot** posso supporre che questo **Malware** crei una serie di Processi **svchost.exe** per poi “killarli”. Ogni processo creato probabilmente apporta ognuno delle modifiche al **Registro di Sistema** e poi si chiude per non farsi scoprire dal **Sistema**.