Analisi dinamica basica

Sommario

Traccia esercizio

Utilizzare la sandbox https://cuckoo.cert.ee/ per analizzare:

C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe

Requisiti

Vedi report M6\W21\D5

Cos'è cuckoo.cert.ee

Cuckoo.cert.ee è un'implementazione pubblica di **Cuckoo Sandbox**, una piattaforma open-source per l'analisi automatica di malware. È gestita dal **CERT-EE**, il Computer Emergency Response Team dell'Estonia. Questo servizio offre la possibilità di caricare file sospetti per eseguirli in un ambiente isolato (sandbox) e monitorarne il comportamento, fornendo un'analisi dettagliata delle attività del malware.

Caratteristiche principali di cuckoo.cert.ee:

1. **Analisi automatizzata del malware:**
   - Permette di eseguire file sospetti in un ambiente simulato e controllato.
   - Monitora il comportamento del file, incluse le modifiche al sistema, il traffico di rete e le attività sui file.
2. **Rapporti dettagliati:**
   - Fornisce un'analisi completa, inclusi:
     - Modifiche al registro di sistema.
     - Connessioni di rete (es. tentativi di contattare server C2).
     - Attività sui file (lettura, scrittura, cancellazione).
     - Comportamenti sospetti come tentativi di iniezione di codice.
   - Include indicatori di compromissione (IoC) utili per la risposta agli incidenti.
3. **Ambiente sicuro:**
   - Tutte le analisi avvengono in una sandbox isolata, garantendo che il malware non possa diffondersi o causare danni al sistema reale.
4. **Usabilità:**
   - È gratuito e accessibile a chiunque voglia analizzare file sospetti, a condizione che siano rispettate le politiche del servizio.

Utilizzo di cuckoo.cert.ee:

- **Scopo:** È utilizzato principalmente da analisti di sicurezza, team di risposta agli incidenti (CSIRT, CERT), e ricercatori di malware per ottenere analisi veloci e accurate.
- **Procedura:**
  1. Caricare il file sospetto sulla piattaforma.
  2. Attendere il completamento dell'analisi automatica.
  3. Consultare il report generato per identificare eventuali comportamenti malevoli.

Considerazioni sulla privacy e sicurezza:

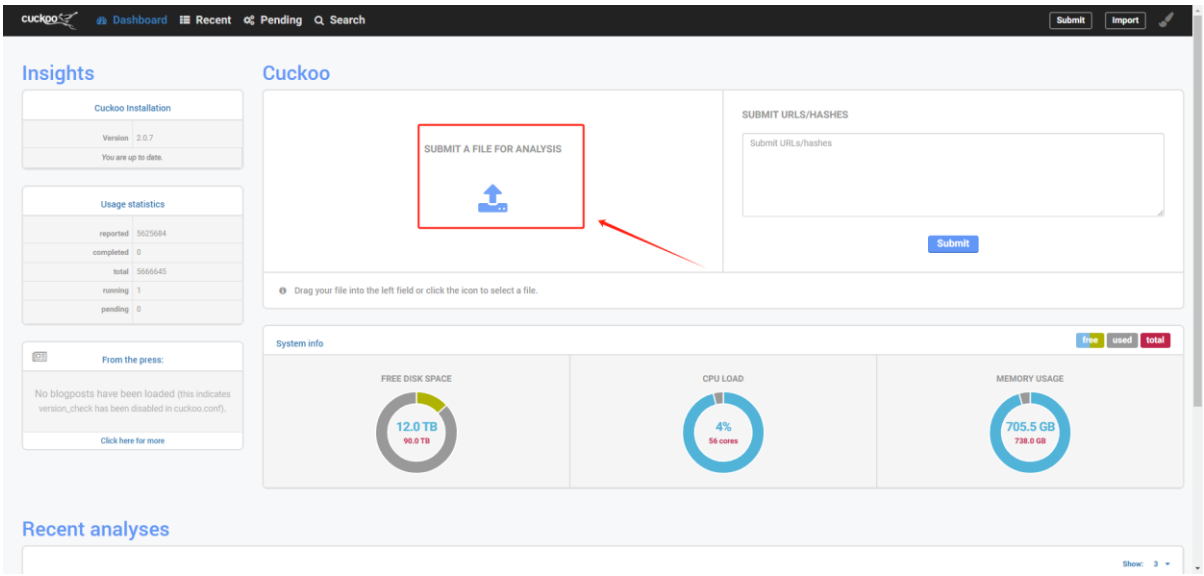
Prima di caricare file su piattaforme pubbliche come **cuckoo.cert.ee**, è importante considerare:

- **Confidenzialità:** Evitare di caricare file contenenti dati sensibili o proprietari, poiché potrebbero essere condivisi con altri utenti o utilizzati per scopi di ricerca.
- **Alternative locali:** Se necessario, è possibile scaricare ed eseguire **Cuckoo Sandbox** localmente per mantenere il controllo completo sull'analisi.

In sintesi, **cuckoo.cert.ee** è uno strumento affidabile e prezioso per l'analisi del malware, ma deve essere usato con attenzione per garantire la protezione delle informazioni sensibili.

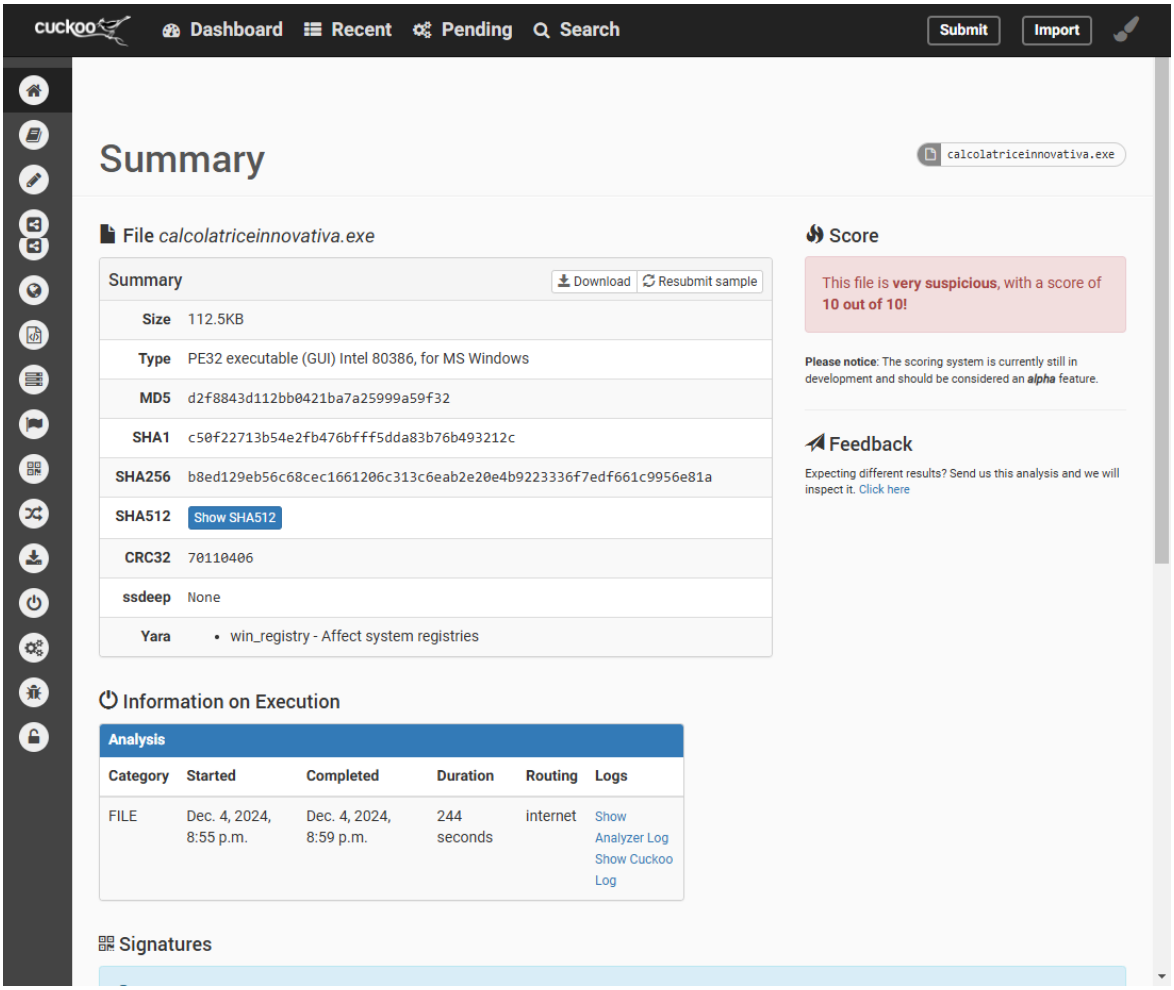
Svolgimento esercizio

Avviare il sito https://cuckoo.cert.ee/



Caricare il file “calcolatriceinnovativa.exe” e attendere l’analisi.

Risultato dell’analisi https://cuckoo.cert.ee/analysis/5633339/summary/



Analisi

Analisi del file calcolatriceinnovativa.exe

1. Comportamenti rilevati

- **NtAllocateVirtualMemory:** Il file alloca memoria con permessi di lettura, scrittura ed esecuzione (PAGE_EXECUTE_READWRITE). Questo è un comportamento tipico di malware che vogliono eseguire codice iniettato o decompressi in memoria.
- **Alta entropia:** L'analisi ha evidenziato sezioni con elevata entropia, indicando che il file potrebbe essere compresso o crittografato. Questo è spesso un segno dell'uso di **packer** per nascondere il codice malevolo.

2. Rilevazione da parte di antivirus

- **IRMA:** 16 motori antivirus hanno identificato il file come malevolo, classificandolo principalmente come:
  - Trojan (es. **Trojan.CryptZ.Marte.1.Gen**, **Win32/Rozena**).
  - Backdoor (es. **BKDR_SWRORT.SM**).
- **VirusTotal:** 52 motori antivirus su 52 hanno confermato la natura malevola del file, assegnandogli nomi simili (Trojan.Generic, Meterpreter, ecc.).

3. Classificazione del malware

Il file è stato associato a:

- **Trojan:** Malware progettato per infiltrarsi nel sistema, potenzialmente rubando dati o installando altri payload.
- **Backdoor:** Il comportamento suggerisce che il malware potrebbe stabilire un canale di comunicazione con un server remoto, spesso per controllo remoto o esfiltrazione di dati.
- **Meterpreter:** Questo è un payload utilizzato in exploit framework come Metasploit, il che potrebbe indicare che il file è stato generato come parte di un attacco mirato.

4. Screenshot e comportamento visivo

- Lo screenshot del sistema infetto mostra un'immagine del meme "Doge" come sfondo del desktop. Questo potrebbe essere un tentativo del malware di distrarre l'utente o un semplice segno distintivo del creatore.

Considerazioni finali

Il file calcolatriceinnovativa.exe è stato identificato come altamente malevolo. I principali indicatori sono:

1. **Allocazione di memoria eseguibile:** Comportamento anomalo e sospetto.
2. **Alta entropia:** Presenza di codice crittografato o compresso, spesso utilizzato per mascherare funzioni malevole.
3. **Rilevazione da antivirus:** Altissima percentuale di rilevamento.
4. **Classificazione:** Trojan/backdoor con potenziale collegamento a framework di exploit come Metasploit.

Raccomandazioni

- **Non eseguire il file:** Il file è pericoloso e potrebbe compromettere gravemente il sistema.
- **Isolamento del file:** Rimuoverlo immediatamente da qualsiasi sistema infetto.
- **Analisi aggiuntiva:** Per approfondimenti, eseguire un'analisi manuale o dinamica in un ambiente sicuro (sandbox offline).
- **Protezione:** Aggiornare gli antivirus e applicare patch di sistema per prevenire ulteriori infezioni.

Screenshoot report

Signatures

Yara rule detected for file (1 event)

description	Affect system registries	rule	win_registry

Allocates read-write-execute memory (usually to unpack itself) (1 event)

Time & API	Arguments	Status	Return	Repeated
NtAllocateVirtualMemory Dec. 4, 2024, 8:55 p.m.	process_identifier: 2740 region_size: 4096 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x003f0000 allocation_type: 4096 (MEM_COMMIT) process_handle: 0xffffffff	1	0	0

The binary likely contains encrypted or compressed data indicative of a packer (2 events)

section	{u'size_of_data': u'0x00012800', u'virtual_address': u'0x00001000', u'entropy': 6.863688338632866, u'name': u'.text', u'virtual_size': u'0x000126b0'}	entropy	6.86368833863	description	A section with a high entropy has been found
entropy	0.663677130045	description	Overall entropy of this PE file is high		

File has been identified by 16 AntiVirus engine on IRMA as malicious (16 events)

File has been identified by 52 AntiVirus engines on VirusTotal as malicious (50 out of 52 events)

File has been identified by 16 AntiVirus engine on IRMA as malicious (16 events)

G Data Antivirus (Windows)	Virus: Trojan.CryptZ.Marte.1.Gen (Engine A)
Avast Core Security (Linux)	Win32:SwPatch [Wrm]
C4S ClamAV (Linux)	C4S.MALWARE.SHA256.AUTOGEN.61050280.UNOFFICIAL
F-Secure Antivirus (Linux)	Trojan.TR/Patched.Gen2 [Aquarius]
Windows Defender (Windows)	Trojan:Win32/Meterpreter.A
Forticlient (Linux)	W32/Swrort.C!tr
Sophos Anti-Virus (Linux)	Mal/EncPk-ACE
eScan Antivirus (Linux)	Trojan.CryptZ.Marte.1.Gen(DB)
ESET Security (Windows)	a variant of Win32/Rozena.DT trojan
McAfee CLI scanner (Linux)	Swrort.d trojan
DrWeb Antivirus (Linux)	Trojan.Swrort.1
Trend Micro SProtect (Linux)	BKDR_SWRORT.SM
ClamAV (Linux)	Win.Trojan.MSShellcode-6360730-0
Bitdefender Antivirus (Linux)	Trojan.CryptZ.Marte.1.Gen
Kaspersky Standard (Windows)	HEUR:Trojan.Win32.Generic
Emsisoft Commandline Scanner (Windows)	Trojan.CryptZ.Marte.1.Gen (B)

File has been identified by 52 AntiVirus engines on VirusTotal as malicious (50 out of 52 events)

Bkav	W32.AIDetectMalware
Lionic	Trojan.Win32.Generic.INNG
Cynet	Malicious (score: 100)
CTX	exe.trojan.swrort
CAT-QuickHeal	Trojan.Swrort.A
Skyhigh	Swrort.d
ALYac	Trojan.CryptZ.Marte.1.Gen
Cylance	Unsafe
VIPRE	Trojan.CryptZ.Marte.1.Gen
Sangfor	Trojan.Win32.Swrort.Vrxr
CrowdStrike	win/malicious_confidence_100% (W)
Alibaba	Trojan:Win32/CobaltStrike.5c89
K7GW	Trojan (001172b51)
K7AntiVirus	Trojan (001172b51)
VirIT	Trojan.Win32.Rozena.AA
Symantec	ML.Attribute.HighConfidence
Elastic	malicious (high confidence)
ESET-NOD32	a variant of Win32/Rozena.DT

ESET-NOD32	a variant of Win32/Rozena.DT
APEX	Malicious
Paloalto	generic.ml
ClamAV	Win.Trojan.MSShellcode-6360730-0
Kaspersky	HEUR:Trojan.Win32.Generic
BitDefender	Trojan.CryptZ.Marte.1.Gen
NANO-Antivirus	Virus.Win32.Gen.ccmw
MicroWorld-eScan	Trojan.CryptZ.Marte.1.Gen
F-Secure	Trojan.TR/Patched.Gen2
Zillya	Trojan.Rozena.Win32.208559
TrendMicro	BKDR_SWRORT.SM
McAfeeD	ti!B8ED129EB56C
Trapmine	malicious.high.ml.score
Sophos	Mal/EncPk-ACE
SentinelOne	Static AI - Malicious PE
Avira	TR/Patched.Gen2
Antiy-AVL	Trojan/Win32.Rozena
Kingsoft	malware.kb.a.998
Gridinsoft	Trojan.Win32.Generic.oa!s3

Gridinsoft	Trojan.Win32.Generic.oa!s3
Xcitium	TrojWare.Win32.Rozena.A@4jwdqr
Arcabit	Trojan.CryptZ.Marte.1.Gen
Microsoft	Trojan:Win32/Meterpreter.A
AhnLab-V3	Trojan/Win.Generic.C5700267
McAfee	Swrort.d
DeepInstinct	MALICIOUS
VBA32	Trojan.Swrort
Malwarebytes	Trojan.MetaSploit
Ikarus	Trojan.Win32.Rozena
TrendMicro-HouseCall	BKDR_SWRORT.SM
Tencent	Trojan.Win32.Rozena.16001454
huorong	VirTool/Meterpreter.a
MaxSecure	Trojan.Malware.7164915.susgen
Fortinet	W32/Swrort.C!tr

Screenshots