

Attività di Analisi del Malware

Di seguito è riportata una relazione completa basata sui dati raccolti dalle schermate fornite.

1. Panoramica del Malware

- **Nome del file:** calc.exe (alias calcolatriceinnovativa.exe)
- **Dimensione:** 112.50 KB (Malware Bazaar conferma 115.200 bytes)
- **Hash SHA256:**
b8ed129eb56c68cec1661206c313c6eab2e20e4b92233367fedf661c9956e81a
- **Classificazione Generale:** Trojan (etichettato con "trojan.swrort/cryptz")
- **Comportamento principale:** Likely backdoor e/o dropper.
- **Rilevazioni dai Vendor (VirusTotal):** 59/71 soluzioni antivirus hanno identificato il file come dannoso.

2. Analisi Statica

2.1. Risultati da VirusTotal

- **Minacce associate:**
 - Trojan generici (es: Trojan.CryptZ.Marte.1.Gen, Win32/MShellcode, Backdoor:Win/meterpreter.A)
 - Cobalt Strike, una piattaforma comunemente utilizzata per penetration testing, ma sfruttata anche da attori malevoli.
 - Firma predominante: ShikataGaNai (un crypter/metamorphic encoder per nascondere il codice malevolo).

59

/ 71

Community Score

-12

59/71 security vendors flagged this file as malicious

Reanalyze

Similar

More

b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a

CALC.EXE

Size

112.50 KB

Last Analysis Date

40 minutes ago

EXE

peexe

idle

checks-user-input

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.swrort/cryptz

Threat categories

trojan

Family labels

swrort

cryptz

marte

Security vendors' analysis

Do you want to automate checks?


Alibaba	Trojan.Win32/CobaltStrike.5c89	AliCloud	Backdoor:Win/meterpreter.A
ALYac	Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	Trojan/Win32.Rozena
Arcabit	Trojan.CryptZ.Marte.1.Gen	Avast	Win32:SwPatch [Wrm]
AVG	Win32:SwPatch [Wrm]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Marte.1.Gen	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Trojan.MSShellcode-6360730-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.cryptz	Cylance	Unsafe


- Firma ShikataGaNaI: conferma che il codice è stato offuscato usando un encoder avanzato, noto per mutare il suo payload per evitare rilevamenti.
- Altri indicatori (IOC):
 - Hash multipli confermano unicità.
 - Nessuna descrizione completa del payload è fornita, il che suggerisce necessità di analisi dinamica per approfondire.

MalwareBazaar Database









You are currently viewing the MalwareBazaar entry for **SHA256 b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

Database Entry


ShikataGaNai


Vendor detections: **13**

Intelligence 13	IOCs	YARA 1	File information	Comments	Actions ▾
------------------------	------	---------------	------------------	----------	-----------

SHA256 hash:	 b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a
SHA3-384 hash:	 b211f60b618a49136d23af49bbfa5cb15d2cebd47b5714e58ec81f0a503eb3c8e5bbb1aefd756d1538f4d922a5944415
SHA1 hash:	 c50f22713b54e2fb476bfff5dda83b76b493212c
MD5 hash:	 d2f8843d112bb0421ba7a25999a59f32
humanhash:	 oranges-freddie-wisconsin-undress
File name:	calcolatriceinnovativa.exe
Download:	 download sample
Signature ⓘ	 ShikataGaNai  Alert ▾
File size:	115'200 bytes
First seen:	2024-11-26 14:00:49 UTC

2.3. Analisi con CFF Explorer

L’analisi statica della struttura binaria mostra:

- **Dipendenze Importate:** Librerie critiche del sistema operativo Windows:
 - **KERNEL32.dll:** include funzioni come GetModuleHandleA, LoadLibraryA, e gestione della memoria (GlobalAlloc, GlobalFree).
 - **SHELL32.dll** e altre librerie usate per interazioni con il sistema operativo.
- **Funzioni sospette identificate:**
 - **Sleep:** potrebbe simulare inattività per evitare sandbox.
 - **LoadLibraryA e GetProcAddress:** spesso utilizzate per caricare funzioni a runtime, un comportamento caratteristico del codice offuscato o dinamico.
 - **WriteProfileStringW:** potrebbe modificare configurazioni o registri di sistema.

File Settings ?

calcolatriceinnovativa.exe

File: calcolatriceinnovativa.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- Debug Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000125D4	N/A	00011FBC	00011FC0	00011FC4	00011FC8	00011FCC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
SHELL32.dll	1	00012CA8	FFFFFFFF	FFFFFFFF	00012E42	0000109C
msvcrt.dll	26	00012DC8	FFFFFFFF	FFFFFFFF	00012F60	000011BC
ADVAPI32.dll	3	00012C0C	FFFFFFFF	FFFFFFFF	00012FFC	00001000
KERNEL32.dll	30	00012C2C	FFFFFFFF	FFFFFFFF	000131D4	00001020
GDI32.dll	3	00012C1C	FFFFFFFF	FFFFFFFF	0001320C	00001010
USER32.dll	69	00012CB0	FFFFFFFF	FFFFFFFF	000136A4	000010A4

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
000131AE	77E79F93	0167	GetModuleHandleA
0001319E	77E805D8	022E	LoadLibraryA
0001318C	77E7A5FD	0189	GetProcAddress
0001317C	77E9A9AD	01D8	GlobalCompact
0001316E	77E736A3	01D7	GlobalAlloc
00013160	77E73803	01DE	GlobalFree
00013150	77E6E341	01E5	GlobalReAlloc
00013144	77E78D60	0393	lstrcmpW
0001313C	77E61BE6	0329	Sleep
00013126	77E72A2B	0383	WriteProfileStringW
000131C2	77E6177A	019C	GetStartupInfoA
0001310A	77E6C879	01E6	GlobalSize

3. Analisi Dinamica (suggerita)

Per completare l'analisi, il file dovrà essere eseguito in un **sandbox sicuro**, come Cuckoo Sandbox o Any.Run, per osservare il comportamento runtime:

3.1. Aspettative

- **Persistenza:** Creazione di chiavi di registro o modifiche di configurazioni.
- **Comunicazioni di rete:** Tentativi di contattare un server C2 (Command and Control).
- **Azioni ostili:** Potenziale rilascio di payload aggiuntivi (es: ransomware, keylogger).

3.2. Cosa monitorare

- **File Dropped:** Se il malware scrive altri file su disco.
- **Connessioni di rete:** IP/DNS sospetti, protocolli usati.
- **Processi anomali:** Creazione di processi figli o iniezioni in altri processi.

4. Raccomandazioni

1. **Isolamento:** Non eseguire il file al di fuori di un ambiente virtualizzato (VM o sandbox).
2. **Segnalazione:** Hash e IOC dovrebbero essere condivisi con il team di sicurezza informatica per avvisare altri sistemi.
3. **Protezione futura:**
 - Rafforzare le soluzioni AV con regole YARA che rilevano signature come ShikataGaNai.
 - Monitorare log per tracciare modifiche di registro o rete.

cuckoo.ee/analysis/pending/

Task ID	Sample ID	Date	Filename / URL	Category	Status
5587571	5434714	Nov. 26, 2024, 5:05 p.m.	calcolatriceinnovativa.exe	file	pending
5587570	5434713	Nov. 26, 2024, 5:04 p.m.	calcolatriceinnovativa.exe	file	pending
5587564	5434707	Nov. 26, 2024, 4:56 p.m.	createabetterbuttersmoothsmoothkingstog tmesweetness.tif	file	pending
5587563	5434706	Nov. 26, 2024, 4:55 p.m.	setup.exe	file	pending
5587560	5434704	Nov. 26, 2024, 4:45 p.m.	he_ilo-x64.48.zip	file	pending
5587559	5434703	Nov. 26, 2024, 4:45 p.m.	he_ilo-x64.48.exe @ he_ilo-x64.48.zip	archive	pending
5587558	5434702	Nov. 26, 2024, 4:41 p.m.	he_ilo-x64.48.zip	file	pending
5587540	5434689	Nov. 26, 2024, 2:57 p.m.	bestofthingswithentiretimegivenebsthignstod owithgreat.tif	file	pending
5587539	5434688	Nov. 26, 2024, 2:57 p.m.	igri_gonki_s_rulyom_L_pedalyami.json	file	pending
5587537	5434686	Nov. 26, 2024, 2:55 p.m.	videos_for_you.zip	file	pending
5587536	5434685	Nov. 26, 2024, 2:51 p.m.	REK-OHA_2014-2020_eBook.pdf	file	pending
5587535	5434684	Nov. 26, 2024, 2:51 p.m.	1.guia.pdf	file	pending
5587533	5434682	Nov. 26, 2024, 2:51 p.m.	ubicacionmpio.jpg	file	pending
5587532	5434681	Nov. 26, 2024, 2:50 p.m.	Contratto_ES_MOD_CONAF_NAM_4_0.pdf	file	pending

Conclusione:

Basandosi sull'analisi statica, il file calc.exe è altamente sospetto e rappresenta una potenziale minaccia. L'offuscamento tramite ShikataGaNai, le funzioni importate e le classificazioni antivirus suggeriscono che il malware abbia capacità di evasione e funzioni avanzate come la comunicazione con un server remoto o l'iniezione di codice.

Un'analisi dinamica sarà essenziale per confermare il comportamento e i target precisi.