ANY RUN
INTERACTIVE MALWARE ANALYSIS

Informazioni generali

Nome file:	66bddfcb52736_vidar.exe
Analisi completa:	https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d
Verdetto:	Attività dannosa
Minacce:	**Caricatore** Un loader è un software dannoso che si infiltra nei dispositivi per distribuire payload dannosi. Questo malware è in grado di infettare i computer delle vittime, analizzare le informazioni di sistema e installare altri tipi di minacce, come trojan o stealer. I criminali solitamente distribuiscono i loader tramite e-mail e link di phishing, affidandosi all'ingegneria sociale per indurre gli utenti a scaricare ed eseguire i loro eseguibili. I loader impiegano tattiche avanzate di evasione e persistenza per evitare il rilevamento. **Luce** Lumma è un ladro di informazioni, sviluppato utilizzando il linguaggio di programmazione C. Viene offerto in vendita come malware-as-a-service, con diversi piani disponibili. Di solito prende di mira i wallet di criptovaluta, le credenziali di accesso e altre informazioni sensibili su un sistema compromesso. Il software dannoso riceve regolarmente aggiornamenti che ne migliorano ed espandono la funzionalità, rendendolo una seria minaccia di ladro. **Ladro** Gli stealer sono un gruppo di software dannosi che mirano a ottenere l'accesso non autorizzato alle informazioni degli utenti e a trasferirle all'aggressore. La categoria di malware stealer include vari tipi di programmi che si concentrano sul loro particolare tipo di dati, tra cui file, password e criptovaluta. Gli stealer sono in grado di spiare i loro obiettivi registrando le loro sequenze di tasti e scattando screenshot. Questo tipo di malware viene distribuito principalmente come parte di campagne di phishing. **Vidare** Vidar è un malware pericoloso che ruba informazioni e criptovaluta agli utenti infetti. Deve il suo nome all'antico dio scandinavo della Vendetta. Questo ladro terrorizza Internet dal 2018.
Data di analisi:	25 agosto 2024 alle 22:11:02
Sistema operativo:	Windows 10 Professional (build: 19045, 64 bit)
Etichette:	vedere · luce · ladro · caricatore
Indicatori:	
MIMO:	applicazione/x-dosexec
Informazioni sul file:	Eseguibile PE32 (GUI) Intel 80386 Mono/.Net assembly, per MS Windows
MD5:	FEDB687ED23F77925B35623027F799BB
SHA1:	7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81
Codice SHA256:	325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1
SSDEEP:	6144:yZIlGEaS7npmSNIfI330znhlBf4hJYBaZaH55B:rGEaSVmSmI30znhSYaZa5

Set di ambiente software e opzioni di analisi

Configurazione di avvio

Durata dell'attività:	60 secondi	**Opzione Evasione Pesante:**	spento	**Geolocalizzazione della rete:**	spento
Tempo aggiuntivo utilizzato:	nessuno	**Proxy MITM:**	spento	**Riservatezza:**	Presentazione pubblica
Opzione Fakenet:	spento	**Percorso tramite Tor:**	spento	**Autoconferma dell'UAC:**	SU
Rete:	SU				

Preimpostazione software

- Versione di Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64 bit) (23.001.20093)
- Versione 32.0.0.465 di Adobe Flash Player
- Versione PPAPI di Adobe Flash Player 32 (32.0.0.465)
- Pulizia di C (6.20)
- Versione 3.65.0 (3.65.0)
- Versione di Google Chrome (122.0.6261.70)
- Aiuto per gli aggiornamenti di Google (1.3.36.51)
- Aggiornamento Java 8 271 (64 bit) (8.0.2710.9)
- Aggiornamento automatico Java (2.8.271.9)
- Versione di Microsoft Edge (122.0.2365.59)
- Aggiornamento di Microsoft Edge (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office professionale 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - it-it (16.0.16026.20146)
- Strumenti di integrità di Microsoft Update (3.74.0.0)
- Microsoft Visual C++ 2013 ridistribuibile (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Runtime aggiuntivo - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 runtime minimo - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 ridistribuibile (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 ridistribuibile (x86) - 14.36.32532 (14.36.32532.0)

Correzioni rapide

- Pacchetto LanguagePack del cliente
- Pacchetto LanguagePack del cliente
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- Pacchetto FodMetadata
- Pacchetto di fondazione
- Pacchetto Hello Face
- Pacchetto Hello Face
- Pacchetto opzionale InternetExplorer
- Pacchetto opzionale InternetExplorer
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- Caratteristiche della lingua Pacchetto base en us
- Caratteristiche della lingua Scrittura a mano en us Pacchetto
- Pacchetto LanguageFeatures OCR en us
- Pacchetto LanguageFeatures Speech en us
- Caratteristiche del linguaggio Pacchetto TextToSpeech en us
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MediaPlayer
- Pacchetto MediaPlayer
- Pacchetto FOD desktop Microsoft OneCore ApplicationModel Sync

- Microsoft Visual C++ 2022 X64 Runtime aggiuntivo - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 runtime minimo - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Runtime aggiuntivo - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 runtime minimo - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Servizio di manutenzione Mozilla (123.0)
- Notepad++ (64 bit x64) (7.9.1)
- Componente di estensibilità Click-to-Run di Office 16 (16.0.15726.20202)
- Componente di licenza Click-to-Run di Office 16 (16.0.16026.20146)
- Componente di localizzazione Click-to-Run di Office 16 (16.0.15726.20202)
- Componente di localizzazione Click-to-Run di Office 16 (16.0.15928.20198)
- Versione 7.3.5.0 di PowerShell
- Skype versione 8.104 (8.104)
- Aggiornamento per Windows 10 per sistemi basati su x64 (KB4023057) (2.59.0.0)
- Aggiornamento per Windows 10 per sistemi basati su x64 (KB4023057) (2.63.0.0)
- Aggiornamento per Windows 10 per sistemi basati su x64 (KB4480730) (2.55.0.0)
- Aggiornamento per Windows 10 per sistemi basati su x64 (KB5001716) (8.93.0.0)
- Lettore multimediale VLC (3.0.11)
- WinRAR 5.91 (64 bit) (5.91.0)
- Controllo integrità PC Windows (3.6.2204.08001)
- Pacchetto FOD desktop Microsoft OneCore ApplicationModel Sync
- Pacchetto FOD del database Microsoft OneCore DirectX
- Pacchetto NetFx3 OnDemand
- Pacchetto FoD del blocco note
- Pacchetto FoD del blocco note
- Pacchetto FoD del blocco note
- Pacchetto FoD del blocco note
- Pacchetto FoD del blocco note
- Pacchetto client OpenSSH
- Pacchetto client OpenSSH
- Pacchetto FOD di PowerShell ISE
- Pacchetto FOD di PowerShell ISE
- Pacchetto FOD di PowerShell ISE
- Pacchetto FOD di PowerShell ISE
- Stampa PMCPPC Pacchetto FoD
- Stampa PMCPPC Pacchetto FoD
- Stampa PMCPPC Pacchetto FoD
- Stampa del pacchetto WFS FoD
- Stampa del pacchetto WFS FoD
- Stampa del pacchetto WFS FoD
- Stampa del pacchetto WFS FoD
- Edizione Professionale
- Edizione Professionale
- Pacchetto QuickAssist
- Pacchetto QuickAssist
- CorrezioneRollup
- CorrezioneRollup
- Stack di manutenzione
- Stack di manutenzione
- Stack di manutenzione 3989
- Pacchetto StepsRecorder
- Pacchetto StepsRecorder
- Pacchetto StepsRecorder
- Pacchetto StepsRecorder
- Pacchetto StepsRecorder
- Pacchetto TabletPCMath
- Pacchetto TabletPCMath
- Pacchetto Desktop UserExperience
- Pacchetto Desktop UserExperience
- Pacchetto WordPad FoD
- Pacchetto WordPad FoD
- Pacchetto WordPad FoD
- Pacchetto WordPad FoD
- Pacchetto WordPad FoD

Attività comportamentali

MALIZIOSO

È stato rilevato VIDAR (YARA)
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 6340)

Ruba le credenziali dai browser Web
- RegAsm.exe (PID: 6908)

Le azioni sembrano furto di dati personali
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 4704)

È stato rilevato LUMMA (YARA)
- RegAsm.exe (PID: 4704)

Comportamento della rete degli Stealer
- RegAsm.exe (PID: 4704)

LUMMA è stato rilevato (SURICATA)
- RegAsm.exe (PID: 4704)

SOSPETTOSO

Rilascia il file eseguibile subito dopo l'avvio
- 66bddfcb52736_vidar.exe (PID: 6780)
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 6340)

Legge le impostazioni di sicurezza di Internet Explorer
- RegAsm.exe (PID: 6908)

Controlla le impostazioni di attendibilità di Windows
- RegAsm.exe (PID: 6908)

Ricerche per software installato
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 4704)

Il contenuto eseguibile è stato eliminato o sovrascritto
- RegAsm.exe (PID: 6908)

Il processo elimina l'eseguibile legittimo di Windows
- RegAsm.exe (PID: 6908)

Il processo elimina le librerie C-runtime
- RegAsm.exe (PID: 6908)

Il processo elimina i file DLL di Mozilla
- RegAsm.exe (PID: 6908)

Legge la data di installazione di Windows
- RegAsm.exe (PID: 6908)

Utilizza TIMEOUT.EXE per ritardare l'esecuzione
- cmd.exe (PID: 6284)

INFORMAZIONI

Crea file nella directory del programma
- RegAsm.exe (PID: 6908)

Controlla le informazioni del server proxy
- RegAsm.exe (PID: 6908)

Controlla le lingue supportate
- RegAsm.exe (PID: 6908)
- 66bddfcb52736_vidar.exe (PID: 6780)
- HCAEHJJKFC.exe (PID: 1568)
- CAFHDBGHJK.exe (PID: 6248)
- RegAsm.exe (PID: 4704)
- RegAsm.exe (PID: 6340)

Legge il nome del computer
- RegAsm.exe (PID: 6908)
- 66bddfcb52736_vidar.exe (PID: 6780)
- HCAEHJJKFC.exe (PID: 1568)
- RegAsm.exe (PID: 4704)
- CAFHDBGHJK.exe (PID: 6248)

Legge il GUID della macchina dal registro
- RegAsm.exe (PID: 6908)

Legge il nome del prodotto
- RegAsm.exe (PID: 6908)

Crea file o cartelle nella directory utente
- RegAsm.exe (PID: 6908)

Avvia CMD.EXE per l'esecuzione dei comandi
- RegAsm.exe (PID: 6908)

Potenziale violazione della privacy aziendale
- RegAsm.exe (PID: 6908)

Legge i valori dell'ambiente
- RegAsm.exe (PID: 6908)

Legge le informazioni sulla CPU
- RegAsm.exe (PID: 6908)

Legge le impostazioni della politica software
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 4704)

Il processo controlla le impostazioni della posizione del computer
- RegAsm.exe (PID: 6908)

Crea file in una directory temporanea
- RegAsm.exe (PID: 6340)

Configurazione del malware

Vidare

(PID) Processo	(6908) RegAsm.exe
Corde (310)	INSERISCI_CHIAVE_QUI
	OttieniVariabileAmbienteA
	shlwapi.dll
	Connessione Internet
	FALSO
	%d/%d/%d %d:%d:%d
	Software\Microsoft\Sottosistema di messaggistica Windows\Profili\9375CFF0413111d3B88A00104B2A6676\
	DialogConfig.vdf
	OttieniIndirizzoProc
	CaricaLibreria
	lstrcatA
	EventoAperto
	CreaEventoA
	ChiudiManiglia
	Sonno
	OttieniIDlinguapredefinitoutente
	VirtualAllocExNuma
	VirtualeGratuito
	Ottieni informazioni di sistema
	VirtualAlloc
	HeapAlloc
	OttieniNomeComputerA
	lstrcpyA
	OttieniProcessHeap
	OttieniProcessoCorrente
	lstrlenA
	Processo di uscita
	StatoMemoriaGlobaleEx
	Ottieni ora di sistema
	Orario di sistema su ora file
	advapi32.dll
	gdi32.dll
	utente32.dll
	crypt32.dll
	ntdll.dll
	OttieniNomeUtenteA
	CreaDCA

	OttieniDeviceCaps
	CryptStringToBinaryA
	scansione
	NtQueryInformationProcess
	VMwareVMware
	9 GIORNI
	Giovanni Doe
	DISPLAY
	%hu/%hu/%hu
	OttieniAttributiFileA
	Blocco globale
	Senza Mucchi
	OttieniDimensioneFile
	Dimensione globale
	CreaStrumentoaiuto32Snapshot
	IsWow64Processo
	Processo32Avanti
	Ottieni ora locale
	Biblioteca gratuita
	OttieniInformazioni sul fuso orario
	OttieniStatoPotenzaSistema
	OttieniInformazioniVolumeA
	OttieniWindowsDirectoryA
	Processo32Primo
	OttieniInformazioniLocaliA
	Ottieninomelocalepredefinitoutente
	OttieniNomeFileModuloA
	EliminaFileA
	TrovaFileSuccessivoA
	LocaleGratuito
	TrovaChiudi
	ImpostaVariabileAmbienteA
	LocalAlloc
	OttieniDimensioneFileEx
	LeggiFile
	ImpostaFilePointer
	ScriviFile
	CreaFileA
	TrovaPrimoFileA
	Protezione Virtuale
	OttieniInformazioniLogicheProcessoreEx
	OttieniUltimoErrore
	lstrcpynA
	MultiByteToWideChar
	GlobaleGratuito
	WideCharToMultiByte
	GlobalAlloc
	Processo aperto
	TerminaProcesso

	OttieniCurrentProcessId
	gdiplus.dll
	ole32.dll
	bcrypt.dll
	wininet.dll
	shell32.dll
	psapi.dll
	rstrtmgr.dll
	CreaBitmapCompatibile
	SelezionaOggetto
	BiteBlt
	EliminaOggetto
	CreaCompatibleDC
	DimensioneGdipGetImageEncoders
	Codificatori di immagini GdipGet
	GdipCreaBitmapDaHBITMA
	GdiplusAvviamento
	Arresto Gdiplus
	GdipSaveImageToStream
	GdipDisposeImage
	GdipGratuito
	OttieniHGlobalFromStream
	CreaStreamOnHGlobal
	CoUninizializzare
	CoInizializza
	CoCreateIstanza
	BCryptGeneraChiaveSimmetrica
	Fornitore di algoritmi di chiusura BCrypt
	CrittografiaDecrittografia
	ProprietàBcryptSet
	Chiave di distruzione di BCrypt
	Fornitore di algoritmi aperti BCrypt
	OttieniRettangoloFinestra
	OttieniDesktopWindow
	OttieniDC
	wsprintfA
	EnumDisplayDevicesA
	OttieniElencoLayoutTastiera
	Da CharToOemW
	wsprintfW
	RegQueryValueExA
	RegEnumKeyExA
	RegOpenKeyExA
	RegCloseKey
	RegEnumValueA
	CrittografiaBinariaInStringaA
	CriptareNonProteggereDati
	SHOttieniPercorsoCartellaA
	ShellEseguiExA

InternetOpenUrlA
InternetChiudiGestione
InternetApertoA
HttpInviaRichiestaA
RichiestaApertaHttp
InternetLeggiFile
InternetCrackUrlA
StrCmpCA
StrStrA
StrCmpCW
PercorsoMatchSpecA
OttieniNomeFileModuloExA
RmStartSessione
RisorseRmRegister
ElencoRmGet
RmEndSessione
sqlite3_aperto
sqlite3_prepare_v2
passaggio_sqlite3
testo_colonna_sqlite3
sqlite3_finalizzare
sqlite3_chiudi
sqlite3_colonna_byte
sqlite3_colonna_blob
chiave_criptata
SENTIERO
C:\Programmi\nss3.dll
NSS_Init
NSS_Arresto
PK11_OttieniInternalKeySlot
PK11_Slot gratuito
PK11SDR_Decifra
C:\Programmi\
SELEZIONA origin_url, username_value, password_value DA logins
Morbido:
profilo:
Ospite:
Login:
Password:
Opera
OperaGX
Rete
Biscotti
.TXT
SELEZIONA HOST_KEY, is_httponly, percorso, is_secure, (expires_utc/1000000)-11644480800, nome, encrypted_value dai cookie
VERO
Riempimento automatico
SELEZIONA nome, valore DA riempimento automatico
Storia

	SELEZIONA URL DA URL LIMITE 1000
	CC
	SELEZIONA nome_sulla_carta, mese_di_scadenza, anno_di_scadenza, numero_di_carta_criptato DA carte_di_credito
	Nome:
	Mese:
	Anno:
	Carta:
	Biscotti
	Dati di accesso
	Dati Web
	Storia
	login.json
	moduloInviaURL
	Nome utenteCampo
	Nome utente criptato
	Password criptata
	guida
	SELEZIONA host, isHttpOnly, percorso, isSecure, scadenza, nome, valore DA moz_cookies
	SELEZIONA nomecampo, valore DA moz_formhistory
	SELEZIONA URL DA moz_places LIMITE 1000
	cookie.sqlite
	storiadellaforma.sqlite
	luoghi.sqlite
	Plugin
	Impostazioni estensione locale
	Impostazioni estensione sincronizzazione
	IndicizzatoDB
	Opera GX stabile
	ATTUALE
	estensione-chrome_
	_0.indexeddb.leveldb
	Stato locale
	profili.ini
	cromo
	opera
	volpe rossa
	Portafogli
	%08lX%04lX%lu
	SOFTWARE\Microsoft\Windows NT\Versione corrente
	Nome prodotto
	x32
	x64
	HARDWARE\DESCRIZIONE\Sistema\ProcessoreCentrale\0
	StringaNomeProcessore
	SOFTWARE\Microsoft\Windows\CurrentVersion\Disinstalla
	Nome da visualizzare
	Versione di visualizzazione
	freebl3.dll
	mozglue.dll

msvcp140.dll
nss3.dll
softokn3.dll
vcruntime140.dll
\Tempo\
.exe
correre
aprire
/c inizio
%DESKTOP%
%DATIAPPLICATIVI%
%DATIAPPLICATIVILOCALI%
%PROFILO UTENTE%
%DOCUMENTI%
%PROGRAMMI%
%PROGRAMMI_86%
%RECENTE%
*.lnk
File
\discordia\
\Archiviazione locale\leveldb\CORRENTE
\Archiviazione locale\leveldb
\Telegramma Desktop\
Italiano:
mappa*
Numero di parte: A7FDF864FBC10B77*
A92DAA6EA6F891F2*
Numero di parte: F8806DD0C461824F*
Telegramma
Tossico
*.tossina
*.ini
Password
Software\Microsoft\Windows NT\CurrentVersion\Sottosistema di messaggistica Windows\Profili\Outlook\9375
Software\Microsoft\Office\13.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
Software\Microsoft\Office\14.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
Software\Microsoft\Office .0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
Software\Microsoft\Office .0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
00000001
00000002
00000003
00000004
\Outlook\account.txt
Pidgin
\.viola\
account.xml
dQw4w9WgXcQ
gettone:
Software\Valvola\Steam

	Percorso a vapore
	\configurazione\
	Ssfn*
	configurazione vdf
	DialogConfigOverlay*.vdf
	cartellelibreria.vdf
	loginutenti.vdf
	\Vapore\
	sqlite3.dll
	browser
	Fatto
	Morbido
	\Discord\token.txt
	/c timeout /t 5 & del /f /q "
	" & del "C:\ProgramData*.dll"" & esci
	C:\Windows\system32\cmd.exe
	https
	Tipo di contenuto: multipart/form-data; boundary=----
	HTTP/1.1
	Contenuto-Disposizione: form-data; name="
	gentile
	costruire
	gettone
	nome_file
	file
	messaggio
	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
	schermata.jpg
Indirizzo URL	https://steamcommunity.com/profiles/76561199751190313
C2	Italiano: https://t.me/pech0nk

(PID) Processo	(6340) RegAsm.exe
Corde (239)	INSERISCI_CHIAVE_QUI
	lstrcpyA
	OttieniVariabileAmbienteA
	GdipSaveImageToStream
	Storia
	correre
	Ssfn*
	OttieniIndirizzoProc
	lstrcatA
	EventoAperto
	ChiudiManiglia
	Sonno
	OttieniIDlinguapredefinitoutente
	VirtualAllocExNuma
	VirtualeGratuito
	Ottieni informazioni di sistema
	HeapAlloc

	OttieniNomeComputerA
	OttieniProcessHeap
	OttieniProcessoCorrente
	lstrlenA
	Processo di uscita
	StatoMemoriaGlobaleEx
	Ottieni ora di sistema
	Orario di sistema su ora file
	gdi32.dll
	utente32.dll
	crypt32.dll
	ntdll.dll
	CreaDCA
	OttieniDeviceCaps
	RilascioDC
	CryptStringToBinaryA
	scansione
	NtQueryInformationProcess
	9 GIORNI
	Giovanni Doe
	DISPLAY
	%hu/%hu/%hu
	OttieniAttributiFileA
	Blocco globale
	Dimensione globale
	CreaStrumentoaiuto32Snapshot
	IsWow64Processo
	Processo32Avanti
	Ottieni ora locale
	OttieniInformazioni sul fuso orario
	OttieniStatoPotenzaSistema
	OttieniInformazioniVolumeA
	Processo32Primo
	OttieniInformazioniLocaliA
	Ottieninomelocalepredefinitoutente
	OttieniNomeFileModuloA
	TrovaFileSuccessivoA
	ImpostaVariabileAmbienteA
	LocalAlloc
	OttieniDimensioneFileEx
	ImpostaFilePointer
	TrovaPrimoFileA
	Protezione Virtuale
	OttieniInformazioniLogicheProcessoreEx
	OttieniUltimoErrore
	MultiByteToWideChar
	GlobaleGratuito
	WideCharToMultiByte
	TerminaProcesso

	OttieniCurrentProcessId
	rstrtmgr.dll
	CreaBitmapCompatibile
	SelezionaOggetto
	BiteBlt
	EliminaOggetto
	CreaCompatibleDC
	DimensioneGdipGetImageEncoders
	Codificatori di immagini GdipGet
	GdipCreaBitmapDaHBITMA
	GdiplusAvviamento
	Arresto Gdiplus
	GdipDisposeImage
	OttieniHGlobalFromStream
	CreaStreamOnHGlobal
	CoUninizializzare
	CoInizializza
	CoCreateIstanza
	BCryptGeneraChiaveSimmetrica
	Fornitore di algoritmi di chiusura BCrypt
	CrittografiaDecrittografia
	ProprietàBcryptSet
	Chiave di distruzione di BCrypt
	Fornitore di algoritmi aperti BCrypt
	OttieniRettangoloFinestra
	OttieniDesktopWindow
	OttieniDC
	EnumDisplayDevicesA
	OttieniElencoLayoutTastiera
	Da CharToOemW
	RegQueryValueExA
	RegEnumKeyExA
	RegOpenKeyExA
	RegEnumValueA
	CrittografiaBinariaInStringaA
	CriptareNonProteggereDati
	SHOttieniPercorsoCartellaA
	InternetOpenUrlA
	Connessione Internet
	InternetChiudiGestione
	InternetApertoA
	HttpInviaRichiestaA
	RichiestaApertaHttp
	InternetLeggiFile
	InternetCrackUrlA
	StrStrA
	PercorsoMatchSpecA
	OttieniNomeFileModuloExA
	RmStartSessione

	RisorseRmRegister
	RmEndSessione
	sqlite3_aperto
	sqlite3_prepare_v2
	passaggio_sqlite3
	testo_colonna_sqlite3
	sqlite3_finalizzare
	sqlite3_chiudi
	sqlite3_colonna_byte
	sqlite3_colonna_blob
	chiave_criptata
	SENTIERO
	C:\Programmi\nss3.dll
	NSS_Arresto
	PK11_OttieniInternalKeySlot
	PK11_Slot gratuito
	PK11_Autenticazione
	PK11SDR_Decifra
	C:\Programmi\
	SELEZIONA origin_url, username_value, password_value DA logins
	Morbido:
	Ospite:
	Login:
	Password:
	Opera
	OperaGX
	Rete
	Biscotti
	.TXT
	VERO
	FALSO
	SELEZIONA nome, valore DA riempimento automatico
	Storia
	SELEZIONA URL DA URL LIMITE 1000
	CC
	SELEZIONA nome_sulla_carta, mese_di_scadenza, anno_di_scadenza, numero_di_carta_criptato DA carte_di_credito
	Nome:
	Mese:
	Anno:
	Carta:
	Biscotti
	Dati di accesso
	moduloInviaURL
	Nome utenteCampo
	Nome utente criptato
	Password criptata
	guida
	SELEZIONA host, isHttpOnly, percorso, isSecure, scadenza, nome, valore DA moz_cookies
	SELEZIONA nomecampo, valore DA moz_formhistory

	SELEZIONA URL DA moz_places LIMITE 1000
	cookie.sqlite
	storiadellaforma.sqlite
	luoghi.sqlite
	Plugin
	Impostazioni estensione locale
	Impostazioni estensione sincronizzazione
	Opera Stabile
	Opera GX stabile
	ATTUALE
	estensione-chrome_
	_0.indexeddb.leveldb
	profili.ini
	cromo
	opera
	volpe rossa
	Portafogli
	%08lX%04lX%lu
	SOFTWARE\Microsoft\Windows NT\Versione corrente
	x64
	%d/%d/%d %d:%d:%d
	HARDWARE\DESCRIZIONE\Sistema\ProcessoreCentrale\0
	StringaNomeProcessore
	SOFTWARE\Microsoft\Windows\CurrentVersion\Disinstalla
	Versione di visualizzazione
	msvcp140.dll
	softokn3.dll
	vcruntime140.dll
	\Tempo\
	.exe
	aprire
	%DATIAPPLICATIVILOCALI%
	%PROFILO UTENTE%
	%PROGRAMMI%
	%PROGRAMMI_86%
	*.lnk
	File
	\Archiviazione locale\leveldb\CORRENTE
	\Archiviazione locale\leveldb
	\Telegramma Desktop\
	Italiano:
	mappa*
	Numero di parte: A7FDF864FBC10B77*
	A92DAA6EA6F891F2*
	Numero di parte: F8806DD0C461824F*
	Tossico
	*.tossina
	*.ini
	Software\Microsoft\Windows NT\CurrentVersion\Sottosistema di messaggistica Windows\Profili\Outlook\9375

	Software\Microsoft\Office\13.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\14.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office .0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Sottosistema di messaggistica Windows\Profili\9375CFF0413111d3B88A00104B2A6676\
	\Outlook\account.txt
	Pidgin
	account.xml
	gettone:
	Software\Valvola\Steam
	configurazione vdf
	DialogConfig.vdf
	DialogConfigOverlay*.vdf
	cartellelibreria.vdf
	loginutenti.vdf
	\Vapore\
	\Discord\token.txt
	/c timeout /t 5 & del /f /q "
	" & del "C:\ProgramData*.dll"" & esci
	C:\Windows\system32\cmd.exe
	Tipo di contenuto: multipart/form-data; boundary=----
	Contenuto-Disposizione: form-data; name="
	costruire
	gettone
	messaggio
	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
	schermata.jpg
Indirizzo URL	https://steamcommunity.com/profiles/76561199761128941
C2	Italiano: https://t.me/jamelwt

Luce

(PID) Processo	(4704) RegAsm.exe
La 2a (8)	condedqpwqm.shop
	stagedchheiqwo.negozio
	traineiwnqo.shop
	situatoblsoqp.shop
	caffegclasiqwp.shop
	evoliutwoqm.shop
	millyscroqwp.shop
	stamppreewntnq.shop

Informazioni statiche

Triciclo

.exe | Eseguibile CIL generico (.NET, Mono, ecc.) (82.9)
.dll | Libreria di collegamento dinamico Win32 (generica) (7.4)
.exe | Eseguibile Win32 (generico) (5.1)
.exe | Eseguibile generico Win/DOS (2.2)
.exe | DOS eseguibile generico (2.2)

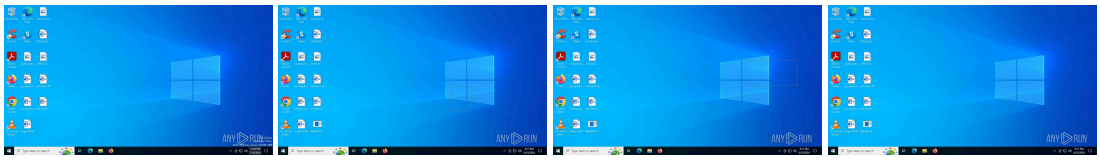
Dati EXIF

EXE

Tipo di macchina:	Intel 386 o successivo e compatibili
Data e ora:	2024:08:17 01:24:51+00:00
Caratteristiche del file immagine:	Eseguibile, 32 bit
Tipo PET:	PE32
Versione del linker:	11
Dimensione codice:	192000
InitializedDataSize:	2048

Dimensione dati non inizializzata:	-
Punto di ingresso:	0x30cfe
Versione del sistema operativo:	4
Versione Immagine:	-
Versione del sottosistema:	6
Sottosistema:	Interfaccia utente grafica di Windows
NumeroVersioneFile:	1.0.0.0
NumeroVersioneProdotto:	1.0.0.0
Maschera dei flag dei file:	0x003f
Flag dei file:	(nessuno)
Sistema operativo FileOS:	Win32
TipoFileOggetto:	Applicazione eseguibile
Sottotipo di file:	-
Codice lingua:	Neutro
Set di caratteri:	Unicode
Commenti:	Maledizione
Nome dell'azienda:	Trampolieri Outchide
Descrizione del file:	Sottovalutazione delle maschere
Versione file:	1.0.0.0
Nome interno:	MSG.exe
Diritto d'autore legale:	Diritto d'autore © 2024
Nome file originale:	MSG.exe
Nome prodotto:	Neutralizzato e dismesso
Versione del prodotto:	1.0.0.0
Versione Assemblea:	1.0.0.0

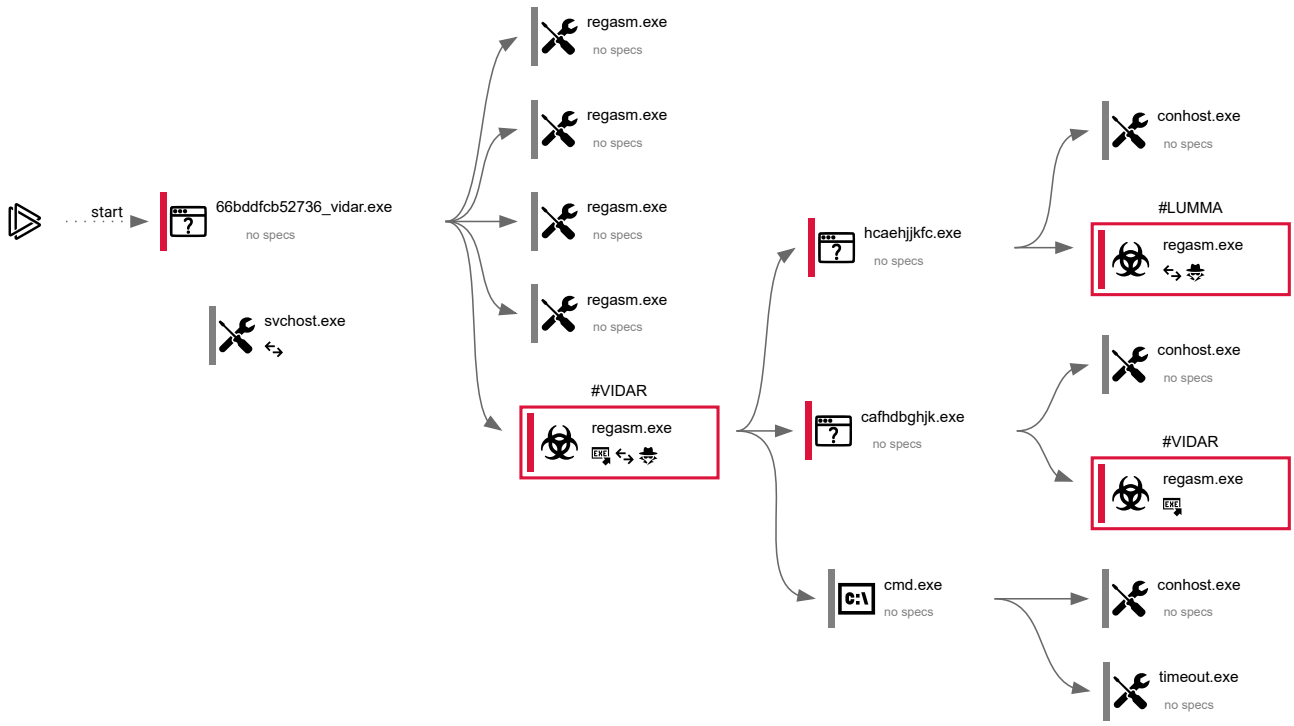
Video e screenshot



Processi

Processi totali	Processi monitorati	Processi dannosi	Processi sospetti
139	16	6	0

Grafico del comportamento



Descrizione delle specifiche

- Il programma non è stato avviato
- Probabilmente è stato utilizzato Tor
- Minaccia nota
- Si collega alla rete
- L'attività contiene diverse app in esecuzione
- Il file è stato rilevato dal software antivirus
- Il processo ha la configurazione del malware
- Accesso di basso livello all'HDD
- Comportamento simile allo spam
- RAM in eccesso
- Sovraccarico della CPU
- L'applicazione ha scaricato il file eseguibile
- L'oggetto ispezionato presenta una struttura PE sospetta
- Il processo è stato aggiunto all'avvio
- L'attività ha iniettato processi
- Sono stati rilevati attacchi alla rete
- Il processo avvia i servizi
- Azioni simili al furto di dati personali
- Comportamento simile allo sfruttamento della vulnerabilità
- Sono disponibili informazioni di debug
- Il file eseguibile è stato eliminato
- Elevazione del livello di integrità
- Il sistema è stato riavviato
- L'attività ha applicazioni terminate con un errore
- L'attività contiene un errore o è stata riavviata

Informazioni sul processo

PID	Comando	Sentiero	Indicatori	Processo padre
6780	"C:\Utenti\admin\Desktop\66bddfcb52736_vidar.exe"	C:\Utenti\admin\Desktop\66bddfcb52736_vidar.exe	–	esploratore.exe

Informazioni

Utente:	amministratore	**Azienda:**	Trampolieri Outchide
Livello di integrità:	MEDIO	**Descrizione:**	Sottovalutazione delle maschere
Codice di uscita:	0	**Versione:**	1.0.0.0

6864	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	—	66bddfcb52736_vidar.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Codice di uscita:	0	**Versione:**	4.8.9037.0 costruito da: NET481REL1

6872	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	—	66bddfcb52736_vidar.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Codice di uscita:	0	**Versione:**	4.8.9037.0 costruito da: NET481REL1

6884	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	—	66bddfcb52736_vidar.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Codice di uscita:	0	**Versione:**	4.8.9037.0 costruito da: NET481REL1

6896	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	—	66bddfcb52736_vidar.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Codice di uscita:	0	**Versione:**	4.8.9037.0 costruito da: NET481REL1

6908	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	—	66bddfcb52736_vidar.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Codice di uscita:	0	**Versione:**	4.8.9037.0 costruito da: NET481REL1

Configurazione del malware Vidare

Vidare

(PID) Processo	(6908) RegAsm.exe
Corde (310)	INSERISCI_CHIAVE_QUI
	OttieniVariabileAmbienteA
	shlwapi.dll
	Connessione Internet
	FALSO
	%d/%d/%d %d:%d:%d
	Software\Microsoft\Sottosistema di messaggistica Windows\Profili\9375CFF0413111d3B88A00104B2A6676\
	DialogConfig.vdf
	OttieniIndirizzoProc
	CaricaLibreria
	lstrcatA
	EventoAperto
	CreaEventoA
	ChiudiManiglia
	Sonno
	OttieniIDlinguapredefinitoutente
	VirtualAllocExNuma
	VirtualeGratuito
	Ottieni informazioni di sistema
	VirtualAlloc
	HeapAlloc

OttieniNomeComputerA
lstrcpyA
OttieniProcessHeap
OttieniProcessoCorrente
lstrlenA
Processo di uscita
StatoMemoriaGlobaleEx
Ottieni ora di sistema
Orario di sistema su ora file
advapi32.dll
gdi32.dll
utente32.dll
crypt32.dll
ntdll.dll
OttieniNomeUtenteA
CreaDCA
OttieniDeviceCaps
CryptStringToBinaryA
scansione
NtQueryInformationProcess
VMwareVMware
9 GIORNI
Giovanni Doe
DISPLAY
%hu/%hu/%hu
OttieniAttributiFileA
Blocco globale
Senza Mucchi
OttieniDimensioneFile
Dimensione globale
CreaStrumentoaiuto32Snapshot
IsWow64Processo
Processo32Avanti
Ottieni ora locale
Biblioteca gratuita
OttieniInformazioni sul fuso orario
OttieniStatoPotenzaSistema
OttieniInformazioniVolumeA
OttieniWindowsDirectoryA
Processo32Primo
OttieniInformazioniLocaliA
Ottieninomelocalepredefinitoutente
OttieniNomeFileModuloA
EliminaFileA
TrovaFileSuccessivoA
LocaleGratuito
TrovaChiudi
ImpostaVariabileAmbienteA
LocalAlloc

	OttieniDimensioneFileEx
	LeggiFile
	ImpostaFilePointer
	ScriviFile
	CreaFileA
	TrovaPrimoFileA
	Protezione Virtuale
	OttieniInformazioniLogicheProcessoreEx
	OttieniUltimoErrore
	lstrcpynA
	MultiByteToWideChar
	GlobaleGratuito
	WideCharToMultiByte
	GlobalAlloc
	Processo aperto
	TerminaProcesso
	OttieniCurrentProcessId
	gdiplus.dll
	ole32.dll
	bcrypt.dll
	wininet.dll
	shell32.dll
	psapi.dll
	rstrtmgr.dll
	CreaBitmapCompatibile
	SelezionaOggetto
	BiteBlt
	EliminaOggetto
	CreaCompatibleDC
	DimensioneGdipGetImageEncoders
	Codificatori di immagini GdipGet
	GdipCreaBitmapDaHBITMA
	GdiplusAvviamento
	Arresto Gdiplus
	GdipSaveImageToStream
	GdipDisposeImage
	GdipGratuito
	OttieniHGlobalFromStream
	CreaStreamOnHGlobal
	CoUninizializzare
	CoInizializza
	CoCreateIstanza
	BCryptGeneraChiaveSimmetrica
	Fornitore di algoritmi di chiusura BCrypt
	CrittografiaDecrittografia
	ProprietàBcryptSet
	Chiave di distruzione di BCrypt
	Fornitore di algoritmi aperti BCrypt
	OttieniRettangoloFinestra

OttieniDesktopWindow
OttieniDC
wsprintfA
EnumDisplayDevicesA
OttieniElencoLayoutTastiera
Da CharToOemW
wsprintfW
RegQueryValueExA
RegEnumKeyExA
RegOpenKeyExA
RegCloseKey
RegEnumValueA
CrittografiaBinariaInStringaA
CriptareNonProteggereDati
SHOttieniPercorsoCartellaA
ShellEseguiExA
InternetOpenUrlA
InternetChiudiGestione
InternetApertoA
HttpInviaRichiestaA
RichiestaApertaHttp
InternetLeggiFile
InternetCrackUrlA
StrCmpCA
StrStrA
StrCmpCW
PercorsoMatchSpecA
OttieniNomeFileModuloExA
RmStartSessione
RisorseRmRegister
ElencoRmGet
RmEndSessione
sqlite3_aperto
sqlite3_prepare_v2
passaggio_sqlite3
testo_colonna_sqlite3
sqlite3_finalizzare
sqlite3_chiudi
sqlite3_colonna_byte
sqlite3_colonna_blob
chiave_criptata
SENTIERO
C:\Programmi\nss3.dll
NSS_Init
NSS_Arresto
PK11_OttieniInternalKeySlot
PK11_Slot gratuito
PK11SDR_Decifra
C:\Programmi\

SELEZIONA origin_url, username_value, password_value DA logins
Morbido:
profilo:
Ospite:
Login:
Password:
Opera
OperaGX
Rete
Biscotti
.TXT
SELEZIONA HOST_KEY, is_httponly, percorso, is_secure, (expires_utc/1000000)-11644480800, nome, encrypted_value dai cookie
VERO
Riempimento automatico
SELEZIONA nome, valore DA riempimento automatico
Storia
SELEZIONA URL DA URL LIMITE 1000
CC
SELEZIONA nome_sulla_carta, mese_di_scadenza, anno_di_scadenza, numero_di_carta_criptato DA carte_di_credito
Nome:
Mese:
Anno:
Carta:
Biscotti
Dati di accesso
Dati Web
Storia
login.json
moduloInviaURL
Nome utenteCampo
Nome utente criptato
Password criptata
guida
SELEZIONA host, isHttpOnly, percorso, isSecure, scadenza, nome, valore DA moz_cookies
SELEZIONA nomecampo, valore DA moz_formhistory
SELEZIONA URL DA moz_places LIMITE 1000
cookie.sqlite
storiadellaforma.sqlite
luoghi.sqlite
Plugin
Impostazioni estensione locale
Impostazioni estensione sincronizzazione
IndicizzatoDB
Opera GX stabile
ATTUALE
estensione-chrome_
_0.indexeddb.leveldb
Stato locale
profili.ini

cromo
opera
volpe rossa
Portafogli
%08lX%04lX%lu
SOFTWARE\Microsoft\Windows NT\Versione corrente
Nome prodotto
x32
x64
HARDWARE\DESCRIZIONE\Sistema\ProcessoreCentrale\0
StringaNomeProcessore
SOFTWARE\Microsoft\Windows\CurrentVersion\Disinstalla
Nome da visualizzare
Versione di visualizzazione
freebl3.dll
mozglue.dll
msvcp140.dll
nss3.dll
softokn3.dll
vcruntime140.dll
\Tempo\
.exe
correre
aprire
/c inizio
%DESKTOP%
%DATIAPPLICATIVI%
%DATIAPPLICATIVILOCALI%
%PROFILO UTENTE%
%DOCUMENTI%
%PROGRAMMI%
%PROGRAMMI_86%
%RECENTE%
*.lnk
File
\discordia\
\Archiviazione locale\leveldb\CORRENTE
\Archiviazione locale\leveldb
\Telegramma Desktop\
Italiano:
mappa*
Numero di parte: A7FDF864FBC10B77*
A92DAA6EA6F891F2*
Numero di parte: F8806DD0C461824F*
Telegramma
Tossico
*.tossina
*.ini
Password

	Software\Microsoft\Windows NT\CurrentVersion\Sottosistema di messaggistica Windows\Profili\Outlook\9375
	Software\Microsoft\Office\13.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\14.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office .0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office .0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	00000001
	00000002
	00000003
	00000004
	\Outlook\account.txt
	Pidgin
	\.viola\
	account.xml
	dQw4w9WgXcQ
	gettone:
	Software\Valvola\Steam
	Percorso a vapore
	\configurazione\
	Ssfn*
	configurazione vdf
	DialogConfigOverlay*.vdf
	cartellelibreria.vdf
	loginutenti.vdf
	\Vapore\
	sqlite3.dll
	browser
	Fatto
	Morbido
	\Discord\token.txt
	/c timeout /t 5 & del /f /q "
	" & del "C:\ProgramData*.dll"" & esci
	C:\Windows\system32\cmd.exe
	https
	Tipo di contenuto: multipart/form-data; boundary=----
	HTTP/1.1
	Contenuto-Disposizione: form-data; name="
	gentile
	costruire
	gettone
	nome_file
	file
	messaggio
	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
	schermata.jpg

1568	"C:\ProgramData\HCAEHJJKFC.exe"	C:\ProgramData\HCAEHJJKFC.exe	—	RegAsm.exe	
	Indirizzo URL	https://steamcommunity.com/profiles/76561199751190313			
	C2	Italiano: https://t.me/pech0nk			

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di formattazione automatica del file system
Codice di uscita:	0	**Versione:**	Versione 10.0.19041.3636 (WinBuild.160101.0800)

2572	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	—	HCAEHJJKFC.exe	

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Host della finestra della console
Codice di uscita:	0	**Versione:**	Versione 10.0.19041.1 (WinBuild.160101.0800)

4704 "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe HCAEHJJKFC.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Versione:	4.8.9037.0 costruito da: NET481REL1		

Configurazione del malware Luce

Luce

(PID) Processo	(4704) RegAsm.exe
La 2a (8)	condedqpwqm.shop
	stagedchheiqwo.negozio
	traineiwnqo.shop
	situatoblsoqp.shop
	caffegclasiqwp.shop
	evoliutwoqm.shop
	millyscroqwp.shop
	stamppreewntnq.shop

6248 "C:\ProgramData\CAFHDBGHJK.exe" C:\ProgramData\CAFHDBGHJK.exe — RegAsm.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di formattazione automatica del file system
Codice di uscita:	0	**Versione:**	Versione 10.0.19041.3636 (WinBuild.160101.0800)

1292 \??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1 C:\Windows\System32\conhost.exe — CAFHDBGHJK.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Console Window Host
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

6340 "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe CAFHDBGHJK.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft .NET Assembly Registration Utility
Version:	4.8.9037.0 built by: NET481REL1		

Malware configuration Vidar

Vidar

(PID) Process	(6340) RegAsm.exe
Strings (239)	INSERT_KEY_HERE
	lstrcpyA
	GetEnvironmentVariableA
	GdipSaveImageToStream
	History
	runas
	ssfn*
	GetProcAddress
	lstrcatA
	OpenEventA
	CloseHandle
	Sleep

GetUserDefaultLangID
VirtualAllocExNuma
VirtualFree
GetSystemInfo
HeapAlloc
GetComputerNameA
GetProcessHeap
GetCurrentProcess
lstrlenA
ExitProcess
GlobalMemoryStatusEx
GetSystemTime
SystemTimeToFileTime
gdi32.dll
user32.dll
crypt32.dll
ntdll.dll
CreateDCA
GetDeviceCaps
ReleaseDC
CryptStringToBinaryA
sscanf
NtQueryInformationProcess
HAL9TH
JohnDoe
DISPLAY
%hu/%hu/%hu
GetFileAttributesA
GlobalLock
GlobalSize
CreateToolhelp32Snapshot
IsWow64Process
Process32Next
GetLocalTime
GetTimeZoneInformation
GetSystemPowerStatus
GetVolumeInformationA
Process32First
GetLocaleInfoA
GetUserDefaultLocaleName
GetModuleFileNameA
FindNextFileA
SetEnvironmentVariableA
LocalAlloc
GetFileSizeEx
SetFilePointer
FindFirstFileA
VirtualProtect
GetLogicalProcessorInformationEx

GetLastError
MultiByteToWideChar
GlobalFree
WideCharToMultiByte
TerminateProcess
GetCurrentProcessId
rstrtmgr.dll
CreateCompatibleBitmap
SelectObject
BitBlt
DeleteObject
CreateCompatibleDC
GdipGetImageEncodersSize
GdipGetImageEncoders
GdipCreateBitmapFromHBITMA
GdiplusStartup
GdiplusShutdown
GdipDisposeImage
GetHGlobalFromStream
CreateStreamOnHGlobal
CoUninitialize
CoInitialize
CoCreateInstance
BCryptGenerateSymmetricKey
BCryptCloseAlgorithmProvider
BCryptDecrypt
BCryptSetProperty
BCryptDestroyKey
BCryptOpenAlgorithmProvider
GetWindowRect
GetDesktopWindow
GetDC
EnumDisplayDevicesA
GetKeyboardLayoutList
CharToOemW
RegQueryValueExA
RegEnumKeyExA
RegOpenKeyExA
RegEnumValueA
CryptBinaryToStringA
CryptUnprotectData
SHGetFolderPathA
InternetOpenUrlA
InternetConnectA
InternetCloseHandle
InternetOpenA
HttpSendRequestA
HttpOpenRequestA
InternetReadFile

InternetCrackUrlA
StrStrA
PathMatchSpecA
GetModuleFileNameExA
RmStartSession
RmRegisterResources
RmEndSession
sqlite3_open
sqlite3_prepare_v2
sqlite3_step
sqlite3_column_text
sqlite3_finalize
sqlite3_close
sqlite3_column_bytes
sqlite3_column_blob
encrypted_key
PATH
C:\ProgramData\nss3.dll
NSS_Shutdown
PK11_GetInternalKeySlot
PK11_FreeSlot
PK11_Authenticate
PK11SDR_Decrypt
C:\ProgramData\
SELECT origin_url, username_value, password_value FROM logins
Soft:
Host:
Login:
Password:
Opera
OperaGX
Network
Cookies
.txt
TRUE
FALSE
SELECT name, value FROM autofill
History
SELECT url FROM urls LIMIT 1000
CC
SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards
Name:
Month:
Year:
Card:
Cookies
Login Data
formSubmitURL
usernameField

encryptedUsername
encryptedPassword
guid
SELECT host, isHttpOnly, path, isSecure, expiry, name, value FROM moz_cookies
SELECT fieldname, value FROM moz_formhistory
SELECT url FROM moz_places LIMIT 1000
cookies.sqlite
formhistory.sqlite
places.sqlite
Plugins
Local Extension Settings
Sync Extension Settings
Opera Stable
Opera GX Stable
CURRENT
chrome-extension_
_0.indexeddb.leveldb
profiles.ini
chrome
opera
firefox
Wallets
%08lX%04lX%lu
SOFTWARE\Microsoft\Windows NT\CurrentVersion
x64
%d/%d/%d %d:%d:%d
HARDWARE\DESCRIPTION\System\CentralProcessor\0
ProcessorNameString
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
DisplayVersion
msvcp140.dll
softokn3.dll
vcruntime140.dll
\Temp\
.exe
open
%LOCALAPPDATA%
%USERPROFILE%
%PROGRAMFILES%
%PROGRAMFILES_86%
*.lnk
Files
\Local Storage\leveldb\CURRENT
\Local Storage\leveldb
\Telegram Desktop\
D877F783D5D3EF8C*
map*
A7FDF864FBC10B77*
A92DAA6EA6F891F2*

	F8806DD0C461824F*
	Tox
	*.tox
	*.ini
	Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375
	Software\Microsoft\Office\13.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\14.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676\
	\Outlook\accounts.txt
	Pidgin
	accounts.xml
	token:
	Software\Valve\Steam
	config.vdf
	DialogConfig.vdf
	DialogConfigOverlay*.vdf
	libraryfolders.vdf
	loginusers.vdf
	\Steam\
	\Discord\tokens.txt
	/c timeout /t 5 & del /f /q "
	" & del "C:\ProgramData*.dll"" & exit
	C:\Windows\system32\cmd.exe
	Content-Type: multipart/form-data; boundary=----
	Content-Disposition: form-data; name="
	build
	token
	message
	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
	screenshot.jpg
URL	https://steamcommunity.com/profiles/76561199761128941
C2	https://t.me/jamelwt

6284 `"C:\Windows\system32\cmd.exe" /c timeout /t 10 & rd /s /q "C:\ProgramData\FHJDBKJKFIEC" & exit` — C:\Windows\SysWOW64\cmd.exe — — RegAsm.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	10.0.19041.3636 (WinBuild.160101.0800)

6240 `\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1` — C:\Windows\System32\conhost.exe — — cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Console Window Host
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

6372 `timeout /t 10` — C:\Windows\SysWOW64\timeout.exe — — cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	timeout - pauses command processing
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

2256 `C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache` — C:\Windows\System32\svchost.exe — ↔ services.exe

Information

User:	NETWORK SERVICE	**Company:**	Microsoft Corporation
Integrity Level:	SYSTEM	**Description:**	Host Process for Windows Services

Version: 10.0.19041.1 (WinBuild.160101.0800)

Attività del registro

Eventi totali	Leggi gli eventi	Scrivi eventi	Elimina eventi
7 999	7 987	12	0

Eventi di modifica

(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\5.0\Cache\Contenuto
Operazione:	scrivere	**Nome:**	Prefisso della cache
Valore:			
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\5.0\Cache\Cookie
Operazione:	scrivere	**Nome:**	Prefisso della cache
Valore:	Biscotto:		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\5.0\Cache\Cronologia
Operazione:	scrivere	**Nome:**	Prefisso della cache
Valore:	Visitato:		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\ZoneMap
Operazione:	scrivere	**Nome:**	Bypass proxy
Valore:	1		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\ZoneMap
Operazione:	scrivere	**Nome:**	NomeIntranet
Valore:	1		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\ZoneMap
Operazione:	scrivere	**Nome:**	Intranet UNCAs
Valore:	1		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\ZoneMap
Operazione:	scrivere	**Nome:**	Rilevamento automatico
Valore:	0		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Memorizzato nella cache
Operazione:	scrivere	**Nome:**	{40DD6E20-7C17-11CE-A804-00AA003CA9F6} {000214EF-0000-0000-C000-000000000046} 0xFFFF
Valore:	010000000000000006210E8F92AF7DA01		

Attività dei file

File eseguibili	File sospetti	File di testo	Tipi sconosciuti
10	24	72	0

File eliminati

PID	Processo	Nome file	Tipo
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\KKECFI **MD5:** — **Codice SHA256:** —	—
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\EBAKFI **MD5:** 06AD9E737639FDC745B3B65312857109 **Codice SHA256:** C8925892CA8E213746633033AE95ACFB8DD9531BC376B82066E686AC6F40A404	binario
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\EGIJEB **MD5:** F6C33AC5E1032A0873BE7BFC65169287 **Codice SHA256:** D97895CEDED32E33D57BDCACCDBE144E58AA87AF4D2F8855D630286CE30A8D83	binario
6908	RegAsm.exe	C:\Utenti\admin\AppData\Locale\Microsoft\Windows\INetCache\IE\RR3E01RZ\76561199751190313[1].htm **MD5:** C09F4FFB8C3C96304CA98F627660FFCA **Codice SHA256:** 85D30BA50E862CB5BE7BEEB6D384EE2E1515B4C4BD49B27D24675667A556B73A	codice html
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\CBAFID **MD5:** 31EF1E93260AED2FED884531149F5171 **Codice SHA256:** F2E9869285B794BF4B14BBB67CA6E680BC46BE8FD0DA55F4A7745F34E84815B7	binario
6908	RegAsm.exe	C:\Programmi\freebl3.dll **MD5:** 550686C0EE48C386DFCB40199BD076AC **Codice SHA256:** EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA	eseguibile

6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\JECBGC **MD5:** 19BA68C3ECBCA72C2B90AFADDE745DC6	**Codice SHA256:** 8B3758EE2D2C0A07EE7003F902F0667ABE5D9667941F8617EDA3CDF94C78E7B8	binario
6908	RegAsm.exe	C:\Programmi\FHJDBKJKFIEC\KJJECG **MD5:** 0B2213BCE3950F1E95FEEB8E8B3B9543	**Codice SHA256:** 71DB3D87713A320BA9FD3043392509B430630CFCF574EE84118406D6471CFC5A	binario
6908	RegAsm.exe	C:\Programmi\FHJDBKJKFIEC\GCBGCG **MD5:** 29A644B1F0D96166A05602FE27B3F4AD	**Codice SHA256:** BF96902FEB97E990A471492F78EE8386BCF430D66BDAEFDEAFBF912C8CF7CE46	binario
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\FIJJKE **MD5:** A45465CDCDC6CB30C8906F3DA4EC114C	**Codice SHA256:** 4412319EF944EBCCA9581CBACB1D4E1DC614C348D1DFC5D2FAAAAD863D300209	binario
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\CGHCGI **MD5:** 95FFD778940E6DF4846B0B12C8DD5821	**SHA256:** 21A2DEBD389DB456465DFEFFDB15F0AF3FBC46F007CBA67513A13EB10D14E94F	binary
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\AFBKKF **MD5:** 1E1F96F03DCB32CBEDE6A33AF67A44A7	**SHA256:** B6DCEC10039FBA99019A6DE818D433847EFAD62FAE59851E328EC42396DFD9CB	sqlite
6908	RegAsm.exe	C:\ProgramData\mozglue.dll **MD5:** C8FD9BE83BC728CC04BEFFAFC2907FE9	**SHA256:** BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A	executable
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\IECFIE **MD5:** FDDE63730E15DD2E18C540BA52B6A945	**SHA256:** 40740EAABD14FC0E08D3B5EE340C1E1B372E158F61EF58AEED1EE4B3A3F4492E	binary
6908	RegAsm.exe	C:\ProgramData\vcruntime140.dll **MD5:** A37EE36B536409056A86F50E67777DD7	**SHA256:** 8934AAEB65B6E6D253DFE72DEA5D65856BD871E989D5D3A2A35EDFE867BB4825	executable
6908	RegAsm.exe	C:\ProgramData\softokn3.dll **MD5:** 4E52D739C324DB8225BD9AB2695F262F	**SHA256:** 74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A	executable
6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp **MD5:** 656E4904ED4417C2838A753F8D9F415B	**SHA256:** FB97D98DB39FC97342AD278DAFEC14FC90AB3D337B45266F31B9ABAC6F3A5FC4	text
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\JECBGC-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911	**SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6908	RegAsm.exe	C:\ProgramData\nss3.dll **MD5:** 1CC453CDF74F31E4D913FF9C10ACDDE2	**SHA256:** AC5C92FE6C51CFA742E475215B83B3E11A4379820043263BF50D4068686C6FA5	executable
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\KKECFI-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911	**SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\CFHIIJ **MD5:** 7A97B8DBC4F98D175F958C00F463A52A	**SHA256:** 92074D2ED1AA1FD621287E35DB9EF1AE3DC04777EFAE5F09E7A3B4534C201548	text
6908	RegAsm.exe	C:\ProgramData\msvcp140.dll **MD5:** 5FF1FCA37C466D6723EC67BE93B51442	**SHA256:** 5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062	executable
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\JEGDGI **MD5:** 8D1E8332CF27F81427652A4E36BF120C	**SHA256:** 56B824B383D5C2AF6FA49B55F13119FEBD74A2B9BCE272168E44441294CBF807	image
6908	RegAsm.exe	C:\ProgramData\HCAEHJJKFC.exe **MD5:** E868144771E7CB04F68C6FE63A46D8C8	**SHA256:** 149D5C2949338ABB59F4FF360EA39229796C73F8E3A9C483442295A8E0F9FCC7	executable
6908	RegAsm.exe	C:\ProgramData\CAFHDBGHJK.exe **MD5:** 35641142FC8EE88F770F838649B0F7CB	**SHA256:** 285BDCF03E3924D309ADD80E795B18678899977F518DA55937DE5DC0A68614C9	executable
6908	RegAsm.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\E4DJRUXW\66cb2df1d4a01_vakerk[1].exe **MD5:** 35641142FC8EE88F770F838649B0F7CB	**SHA256:** 285BDCF03E3924D309ADD80E795B18678899977F518DA55937DE5DC0A68614C9	executable
6908	RegAsm.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\E4DJRUXW\66cb2df8bd684_lawrng[1].exe **MD5:** E868144771E7CB04F68C6FE63A46D8C8	**SHA256:** 149D5C2949338ABB59F4FF360EA39229796C73F8E3A9C483442295A8E0F9FCC7	executable

Attività di rete

Richieste HTTP(S)	Connessioni TCP/UDP	Richieste DNS	Minacce
5	53	16	0

Richieste HTTP

PID	Processo	Metodo	Codice HTTP	Proprietà intellettuale	Indirizzo URL	CN	Tipo	Misurare	Reputazione
6908	RegAsm.exe	OTTENERE	200	147.45.44.104:80	http://147.45.44.104/prog/66cb2df8bd684_lawrng.exe	sconosciuto	–	–	sconosciuto
5468	svchost.exe	OTTENERE	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	sconosciuto	–	–	sconosciuto
6344	SIHClient.exe	OTTENERE	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	sconosciuto	–	–	sconosciuto

6908	RegAsm.exe	OTTENERE	200	147.45.44.104:80	http://147.45.44.104/prog/66cb2df1d4a01_vakerk.exe	sconosciuto	–	–	sconosciuto
6344	SIHClient.exe	OTTENERE	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	sconosciuto	–	–	sconosciuto

Connessioni

PID	Processo	Proprietà intellettuale	Dominio	ASN	CN	Reputazione
3584	svchost.exe	40.127.240.158:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	sconosciuto
568	RUXIMICS.exe	40.127.240.158:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	sconosciuto
–	–	40.127.240.158:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	sconosciuto
–	–	192.168.100.255:138	–	–	–	inserito nella lista bianca
3888	svchost.exe	239.255.255.250:1900	–	–	–	inserito nella lista bianca
–	–	4.231.128.59:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	inserito nella lista bianca
6908	RegAsm.exe	23.212.216.106:443	comunitàdivapore.com	AKAMAI-AS	UA	sconosciuto
6908	RegAsm.exe	195.201.118.191:443	–	Hetzner Online GmbH	Di	sconosciuto
3260	svchost.exe	40.113.110.67:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCCO	NL	inserito nella lista bianca
5468	svchost.exe	40.126.32.136:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCCO	NL	sconosciuto
5468	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3584	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6908	RegAsm.exe	147.45.44.104:80	–	OOO FREEnet Group	RU	malicious
4704	RegAsm.exe	172.67.215.62:443	caffegclasiqwp.shop	CLOUDFLARENET	US	unknown
6344	SIHClient.exe	40.127.169.103:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
6344	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
6344	SIHClient.exe	13.95.31.18:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted

Richieste DNS

Dominio	Proprietà intellettuale	Reputazione
impostazioni-win.data.microsoft.com	40.127.240.158 4.231.128.59 20.73.194.208	inserito nella lista bianca
google.it/	142.250.186.46	inserito nella lista bianca
comunitàdivapore.com	23.212.216.106	inserito nella lista bianca
client.wns.windows.com	40.113.110.67	inserito nella lista bianca
login.live.com	40.126.32.136 40.126.32.133 20.190.160.22 40.126.32.74 20.190.160.20 20.190.160.14 40.126.32.68 40.126.32.76	inserito nella lista bianca
ocsp.digicert.com	192.229.221.95	inserito nella lista bianca
caffegclasiqwp.shop	172.67.215.62 104.21.16.180	maligno
arpdabl.zapto.org	0.0.0.0	sconosciuto
slscr.aggiornamento.microsoft.com	40.127.169.103	inserito nella lista bianca

www.microsoft.com	23.35.229.160	inserito nella lista bianca
fe3cr.delivery.mp.microsoft.com	13.95.31.18	whitelisted
nexusrules.officeapps.live.com	52.111.229.48	whitelisted

Minacce

PID	Processo	Classe	Messaggio
6908	RegAsm.exe	Traffico potenzialmente pericoloso	ET INFO Eseguibile Scarica da dotted-quad Host
6908	RegAsm.exe	Potenziale violazione della privacy aziendale	Scarica file EXE o DLL di Windows ET POLICY PE HTTP
6908	RegAsm.exe	Traffico potenzialmente pericoloso	ET HUNTING SOSPETTO Risposta MZ dell'ospite del Quad punteggiato
6908	RegAsm.exe	Attacco vario	ET DROP Spamhaus DROP Traffico elencato Gruppo in entrata 23
6908	RegAsm.exe	Traffico potenzialmente pericoloso	ET INFO Eseguibile Scarica da dotted-quad Host
4704	RegAsm.exe	È stato rilevato un trojan di rete	STEALER [ANY.RUN] Connessione TLS di Lumma Stealer
2256	svchost.exe	Traffico potenzialmente pericoloso	POLITICA ET Query DNS al dominio DynDNS *.zapto .org
6908	RegAsm.exe	Traffico potenzialmente pericoloso	ET HUNTING SOSPETTO Risposta MZ dell'ospite del Quad punteggiato

Stringhe di output di debug

Nessuna informazione di debug