La Coppa del Mondo FIFA 2022 sotto attacco informatico

Zscaler ThreatLabz rivela che un'impennata di attacchi informatici ha preso di mira i tifosi di calcio attraverso falsi siti di streaming, truffe per i biglietti aerei o per le partite, lotterie fasulle, videogiochi craccati che diffondono malware fino a falsi siti di e-commerce

Milano, 1°dicembre 2022 - **Zscaler ThreatLabz**, il team di ricerca responsabile dell'analisi del panorama globale delle minacce, rende noto che l'inizio della **Coppa del Mondo FIFA 2022 ha portato con sé un'impennata di attacchi informatici** che hanno preso di mira i tifosi di calcio attraverso **falsi siti di streaming e truffe**, sfruttando l'entusiasmo intorno a questo evento straordinario per infettare gli utenti con malware.

In particolare, Zscaler ThreatLabz ha osservato un aumento dei domini di nuova registrazione legati alla Coppa del Mondo FIFA, analogamente a quanto avvenuto nel corso delle Olimpiadi di Tokyo. Non tutti questi domini sono pericolosi, ma a tutela della sicurezza è importante classificare tutti i domini di nuova registrazione come sospetti e condurre analisi per eliminare quelli che lo sono davvero.

Risultati principali

- Con l'avvicinarsi della Coppa del Mondo FIFA, i ricercatori di Zscaler ThreatLabz hanno osservato un picco significativo di **nuovi siti di streaming con domini appena registrati**.
- I falsi siti di streaming utilizzano anche siti/portali legittimi per pubblicare **falsi link** di streaming.
- I criminali informatici hanno preso di mira gli utenti con **molteplici truffe correlate**, come biglietti per le partite della Coppa del Mondo, biglietti aerei, estrazioni di lotterie a tema, ecc.
- Diverse famiglie di **malware** stanno sfruttando la Coppa del Mondo FIFA per colpire gli appassionati di calcio.
- I criminali informatici stanno anche prendendo di mira gli utenti con le **versioni craccate dannose dei giochi legati a FIFA/calcio.**
- La maggior parte delle campagne di malware e truffe che sfruttano la Coppa del Mondo FIFA in corso **utilizzano domini registrati di recente**.

Truffe legate a siti di streaming fasulli

Zscaler ThreatLabz ha osservato un picco di falsi siti di streaming e altri siti truffaldini che affermano di offrire le partite della Coppa del Mondo FIFA in streaming gratuito ma che in realtà reindirizzano gli utenti verso siti fasulli e li invitano a inserire i dati della carta di credito. Nella maggior parte dei casi osservati dai ricercatori, oggi come in passato, i domini registrati di recente vengono utilizzati per ospitare siti contraffatti, ma in alcuni esempi siti legittimi e consolidati come quelli di Xiaomi, Reddit, OpenSea e LinkedIn ospitano link fasulli che reindirizzano ai siti dannosi.

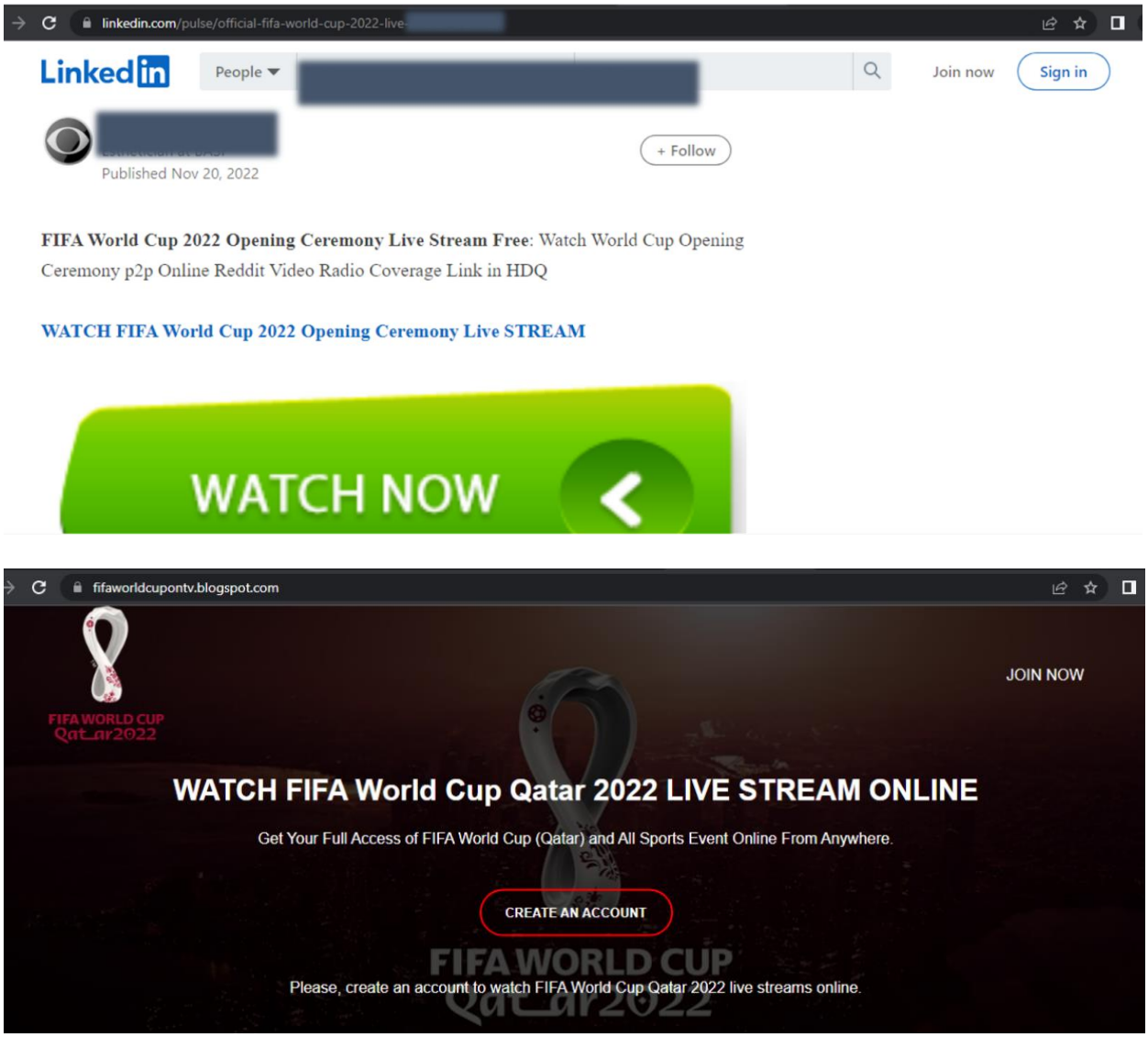

Figura 1: link di un falso sito di streaming pubblicato su un profilo Linkedin e il sito contraffatto su cui l'utente viene reindirizzato.

Truffe legate alla Coppa del Mondo FIFA

Con l'inizio della Coppa del Mondo FIFA, i ricercatori hanno osservato un rapido aumento delle minacce e dei **siti truffaldini** legati all'evento. Molti siti di recente registrazione, che offrono **biglietti per la Coppa del Mondo**, sono in realtà gestiti da criminali informatici che cercano di indurre gli utenti a pagare per biglietti falsi. Nell'esempio riportato di seguito, un sito sospetto che offre biglietti per le partite della Coppa del Mondo è stato registrato di recente, il 15 novembre.

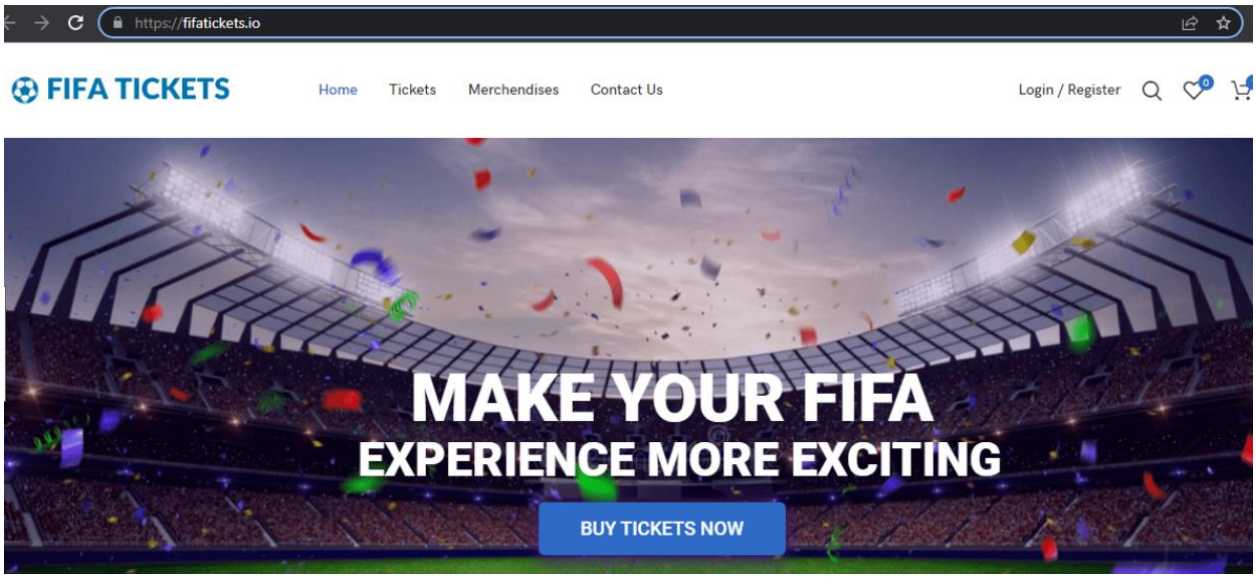

Figura 2: Falso sito di biglietti per le partite FIFA.

Queste truffe in corso non si limitano ai biglietti per le partite della Coppa del Mondo, ma si estendono a molti aspetti della "febbre" da Coppa del Mondo FIFA in corso. ThreatLabz ha anche osservato una truffa in cui agli utenti vengono offerti **premi in denaro e biglietti aerei da Qatar Airways**. Il dominio del sito truffa correlato, mostrato nello screenshot sottostante, è stato registrato l'11 novembre; questa tempistica suggerisce ai ricercatori che i criminali informatici dietro questo sito stanno prendendo di mira i tifosi della Coppa del Mondo.

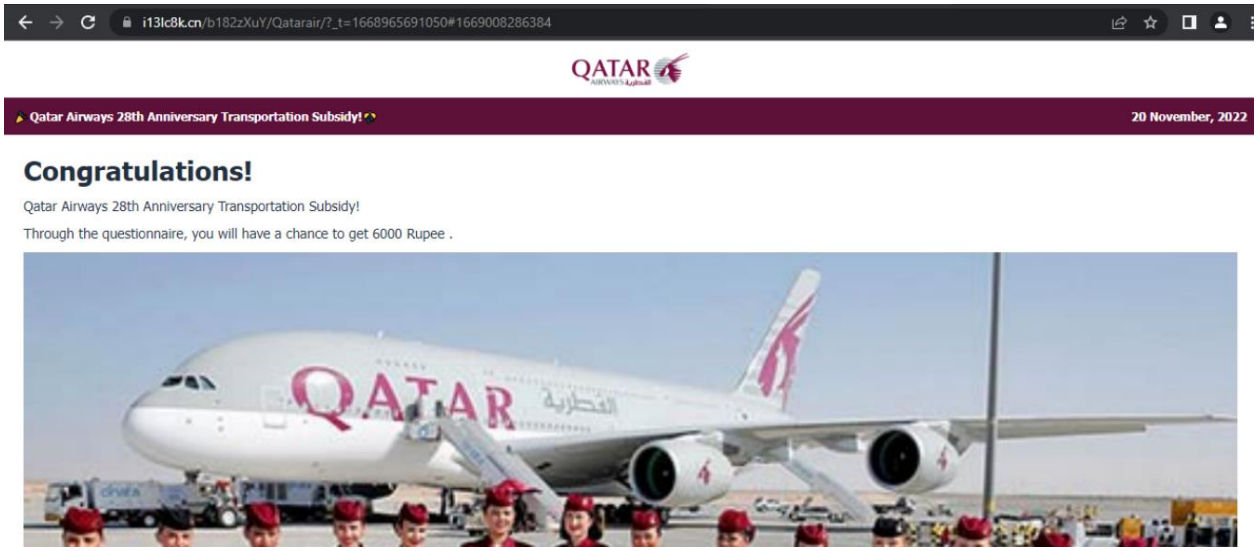

Figura 3: Sito web di truffa con falso messaggio di lotteria della compagnia aerea Qatar

I criminali informatici hanno preso di mira gli utenti anche inviando false email fingendosi un comitato della lotteria della Coppa del Mondo FIFA 2022 del Qatar. Di seguito è riportata una di queste email con allegato un PDF con i dettagli della lotteria.

QATAR 2022 WORLDCUP LOTTERY COMMITEE <[redacted]@gmail.com>

FIFA QATAR WORLD CUP 2022 WINNER

To [redacted]

Message | 2022 FIFA LOTTERY.pdf (1 MB)

Dear WINNER,

You have been selected as a winner in the 2022 FIFA Lottery Award.

Find attachment for more details for your reference.

QATAR 2022 WORLD CUP LOCAL ORGANIZING COMMITTEE.

Figura 4: e-mail di truffa che imita il comitato organizzatore della FIFA.

In questa truffa, un'e-mail con un allegato in formato PDF identifica la vittima target come il vincitore di una grande lotteria. Agli utenti viene chiesto di aprire l'allegato e di inviare i propri dati personali per ottenere il premio in denaro.

QATAR 2022 WORLDCUP LOCAL ORGANIZING COMMITEE

GLOBAL MEGA 2022 LOTTERY DRAW NOTICE

Dear Winner,

This is to inform you that the Global Mega Lottery Game Consulting and the Local Organizing Commitee (LOC) of the 2022 World Cup, here in Qatar, has held an Internet Raffle Draw, and your Email Address was among the (18,600) Email Addresses that was picked by the computer during the Final Raffle Draw (FRD).

We are therefore with great pleasure, to notify you that your Email Address has happened to come out top number (1) among the 5 winners out of the (18,600) Email Addresses, on the FINAL BALLOT DRAW, and this had made you the JACKPOT WINNER OF THE SUM OF US$2,950,000.00 (TWO MILLION NINE HUNDRED AND FIFTY THOUSAND UNITED DOLLARS.

Be aware that this Global Mega Raffle Draw was organised by the Global Mega Lottery Game Consulting (L G C) and the Local Organizing Commitee (L O C) of the 2022 World Cup, to create awareness for the world, as Qatar Host the 2022 World Cup.

BELOW ARE YOUR WINNING DETAILS:
EMAIL CODE NUMBER: 15/76/EF36
FINAL JACKPOT NUMBER: 0001
SN: 2022 / GML. LGC / LOC / QA
WINNING INSURANCE POLICY NUMBER: TTA23QA
INSURANCE COMPANY: CARDIF PINNACLE INSURANCE

AMOUNT WON: US$2,950,000.00.

Figura 5: file PDF allegato all'email truffa.

Siti di e-commerce compromessi

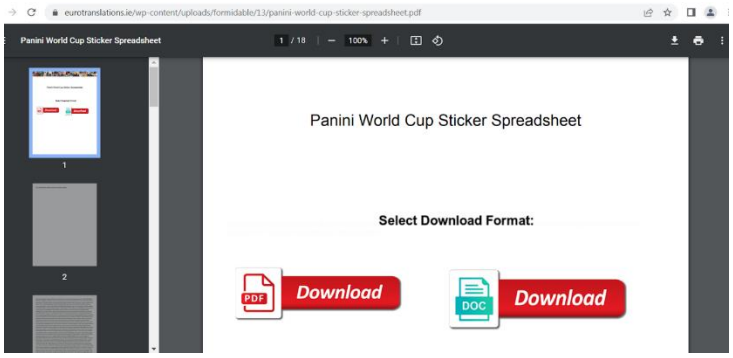

Figura 6: File PDF dannoso ospitato sul sito compromesso.

Zscaler ThreatLabz ha osservato alcuni casi in cui il malware SolarMarker sta prendendo di mira i tifosi di calcio che cercano di **acquistare figurine della Coppa del Mondo da siti di e-commerce in realtà compromessi**. Quando l'utente clicca per scaricare uno di questi falsi PDF, viene automaticamente reindirizzato a un sito controllato dagli hacker che fornisce il payload del servizio Microsoft Windows Installer (MSI) dannoso per eseguire il resto dell'attacco.

Falso gioco FIFA craccato che distribuisce un software dannoso che cerca di rubare informazioni tramite PDF

I criminali informatici stanno utilizzando file PDF dannosi ospitati su siti web compromessi per distribuire infostealer, **software dannosi che cercano di rubare informazioni,** attirando gli utenti a scaricare ciò che pensano sia una registrazione illegalmente craccata dei giochi FIFA.

Quando l'utente fa clic per scaricare il PDF, viene immediatamente reindirizzato a un dominio di nuova registrazione che serve un file di archivio contenente il malware dannoso.

Linee guida per la protezione da questi attacchi:

- Prenotare i biglietti aerei per la Coppa del Mondo FIFA solo da venditori autorizzati e siti verificati.
- Per lo streaming online delle partite della Coppa del Mondo utilizzare esclusivamente il sito web del partner di streaming della Coppa del Mondo FIFA.
- Fare attenzione alle email fraudolente relative a lotterie o a truffe legate a omaggi
- Evitare di scaricare software e giochi craccati da siti web non affidabili.
- Non lasciarsi ingannare da offerte "troppo belle per essere vere" provenienti da fonti sconosciute e siate estremamente cauti nel cliccare su link o documenti provenienti da queste fonti.
- Assicurarsi sempre di utilizzare connessioni HTTPS/sicure.
- Utilizzare l'autenticazione a due fattori ogni volta che è possibile, soprattutto per gli account sensibili come quelli bancari.

A proposito di Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti da attacchi informatici e dalla perdita di dati collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange, basato su SSE, è la più grande piattaforma di sicurezza cloud in line del mondo.

Per ulteriori informazioni:

Tania Acerbi

Monica Fecchio

Prima Pagina

Piazza Giuseppe Grandi 19 - 20129 Milano

e-mail: tania@primapagina.it

e-mail: monica@primapagina.it

Tel. +39 02 91339811