Report 2018
Rete Sicura

Mese della sicurezza Vodafone

allot
See. Control. Secure.

vodafone

Contenuti

1 Introduzione al report .....

2 Raccolta dati 2018 .....

3 Aumento nell'attività di VF SecureNet Italy: comparativa 1H 2017-2018 .....

3 Confronto tra l'Italia e gli altri paesi per i primi 6 mesi del 2018 .....

4 Maggiori minacce rilevate sui clienti di Rete Sicura .....

5 Maggiori minacce dai download .....

6.1 Not-a-virus:HEUR:RiskTool.Win32.Bit .....

6.2 Andr/Xgen-OB .....

6.3 HEUR:Hoax.Script.Generic .....

6.4 Trojan.JS.Miner.m .....

6.5 Not-a-virus:HEUR:AdWare.AndroidOS.E.....

7 Minacce sul dispositivi mobile nei primi 6 mesi del 2018.....

8 Analisi Coinhive .....

9 Nuovo Banking Trojan in Italia.....

10 Sommario.....

11 Per saperne di più.....

vodafone

1 Introduzione al report

Lo scopo di questo report è presentare alcuni dati aggregati relativi al servizio Rete Sicura di Vodafone Italia S.p.a per mostrare come vengano protetti dalle minacce informatiche durante l'ultimo anno.

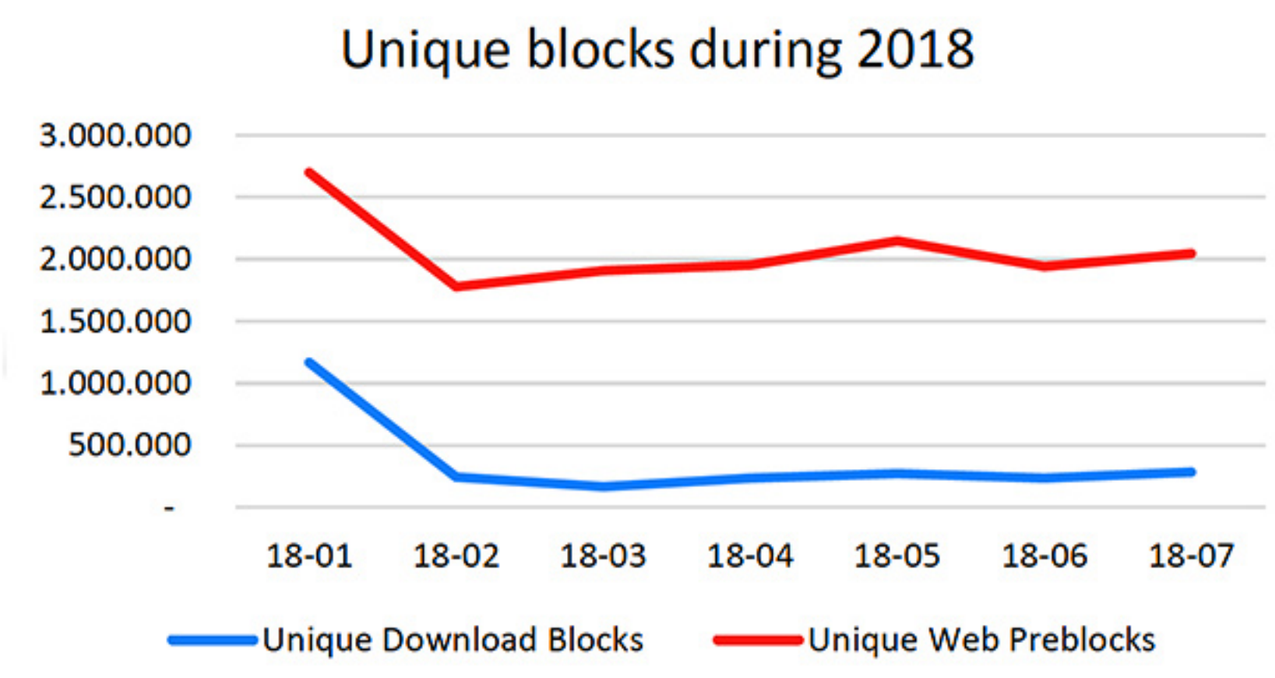
Per questo, in primo luogo, analizziamo una raccolta di dati del 2018. Poi ci concentreremo sull'agosto 2018 per quanto riguarda i blocchi web, così come i download di virus, e verranno spiegate alcune delle più importanti minacce verificatesi durante il mese. Inoltre, verranno evidenziate alcune recenti notizie di sicurezza informatica in Italia.

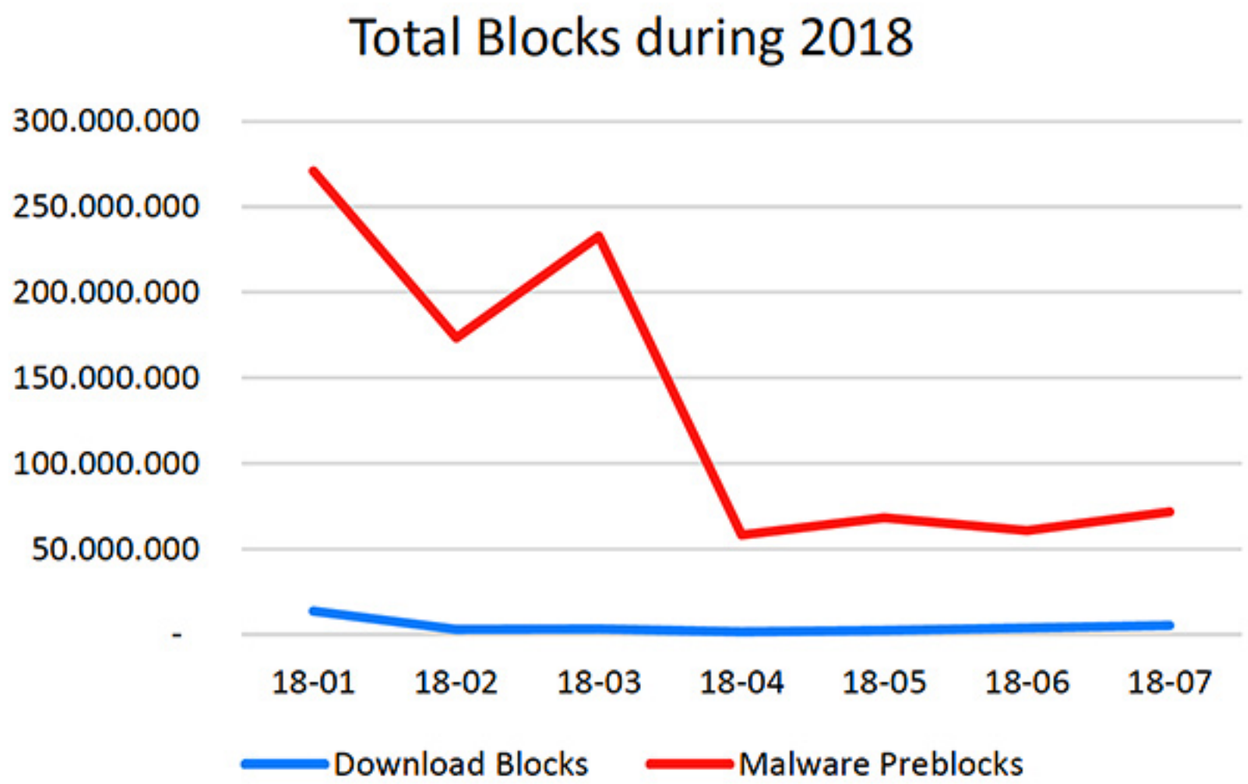
Infine, una sintesi sarà inclusa nelle principali conclusioni alla fine del documento.

2 Raccolta dati 2018

Di seguito è riportato il riepilogo dei dati del servizio Rete Sicura da Gennaio a Luglio 2018:

Year/Month	Unique Download Blocks	Unique Web Preblocks	Download Blocks	Malware Preblocks
18-01	1.167.836	1.532.677	13.699.543	257.213.199
18-02	242.514	1.535.625	3.181.639	170.176.409
18-03	164.800	1.744.401	3.441.863	229.448.685
18-04	235.645	1.719.370	1.665.876	56.553.749
18-05	272.154	1.875.360	2.557.356	65.686.607
18-06	235.788	1.705.647	3.962.315	56.729.935
18-07	282.678	1.764.361	5.232.294	66.417.168





Osservando questi dati, si può sottolineare quanto segue:

- Il numero totale di minacce bloccate in Italia tra gennaio e giugno 2018 sono state 935 milioni.

- Possiamo vedere che sono stati bloccati più siti con malware che virus da download. Questo perché possiamo trovare Malware ovunque (siti web, all'interno dei programmi...), mentre i virus nei download sono meno frequenti. Inoltre, un virus da download che infetta un cellulare, può successivamente generare multipli Malware pre-blocchi.

- Vediamo enormi picchi di malware bloccati a Gennaio e Marzo. Questi picchi sono dovuti al malware "CoinHive". Questo malware potrebbe infiltrarsi nel nostro sistema tramite la navigazione web o tramite applicazioni infette, e quando è all'interno, cerca di estrarre la cripto valuta usando le nostre risorse. Per ulteriori informazioni, consultare il capitolo 7 di questo rapporto, e l'allegato dettagliato sull'impatto di Coinhive sulle prestazioni mobile. Si può anche osservare che subito dopo l'enorme aumento di Coinhive, c'è stato un forte calo ad Aprile, in quanto questo il malware divenne così famoso, che gli hacker smisero di utilizzarlo poiché subito bloccato dalla maggior parte dei motori antivirus, tra cui Rete Sicura.

- Senza l'effetto Coinhive, il numero medio di blocchi per utente tra Aprile e Agosto è di 32.2

vodafone

3 Aumento nell'attività di VF SecureNet Italy: comparativa 1H 2017-2018

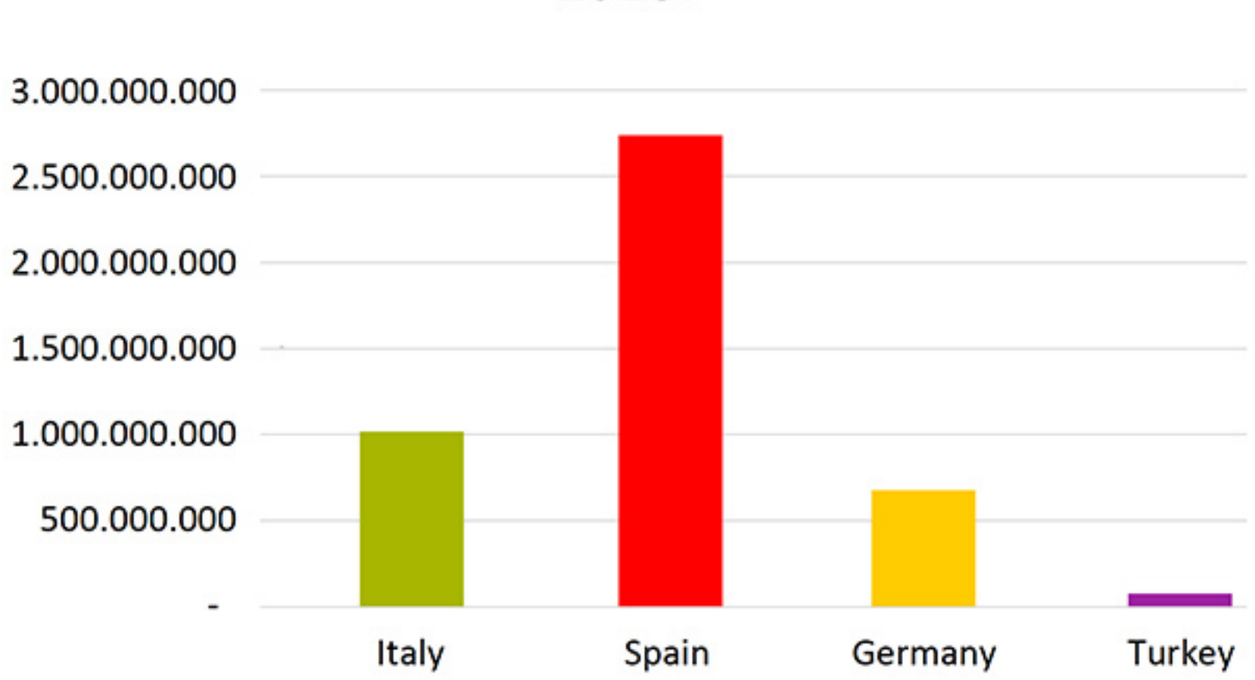
La seguente tabella comparativa mostra l'aumento della percentuale YoY dell'attività di VF SecureNet Italy nei primi sei mesi del 2018 rispetto ai dati dell'anno 2017:

	Customers >1 Virus	Customer > 1 Malware	Virus Blocked	Malware Blocked
18	2,318,737	10,113,080	28,508,592	835,808,584
17	499,995	7,316,819	10,073,340	372,526,692
DELTA YoY%	**+364%**	**+38%**	**+183%**	**+124%**

Come mostra, la crescita è significativa in tutti i parametri, in particolar modo la crescita dei clienti unici con almeno un virus (303% YoY)

4 Confronto tra l'Italia e gli altri paesi per i primi 6 mesi del 2018

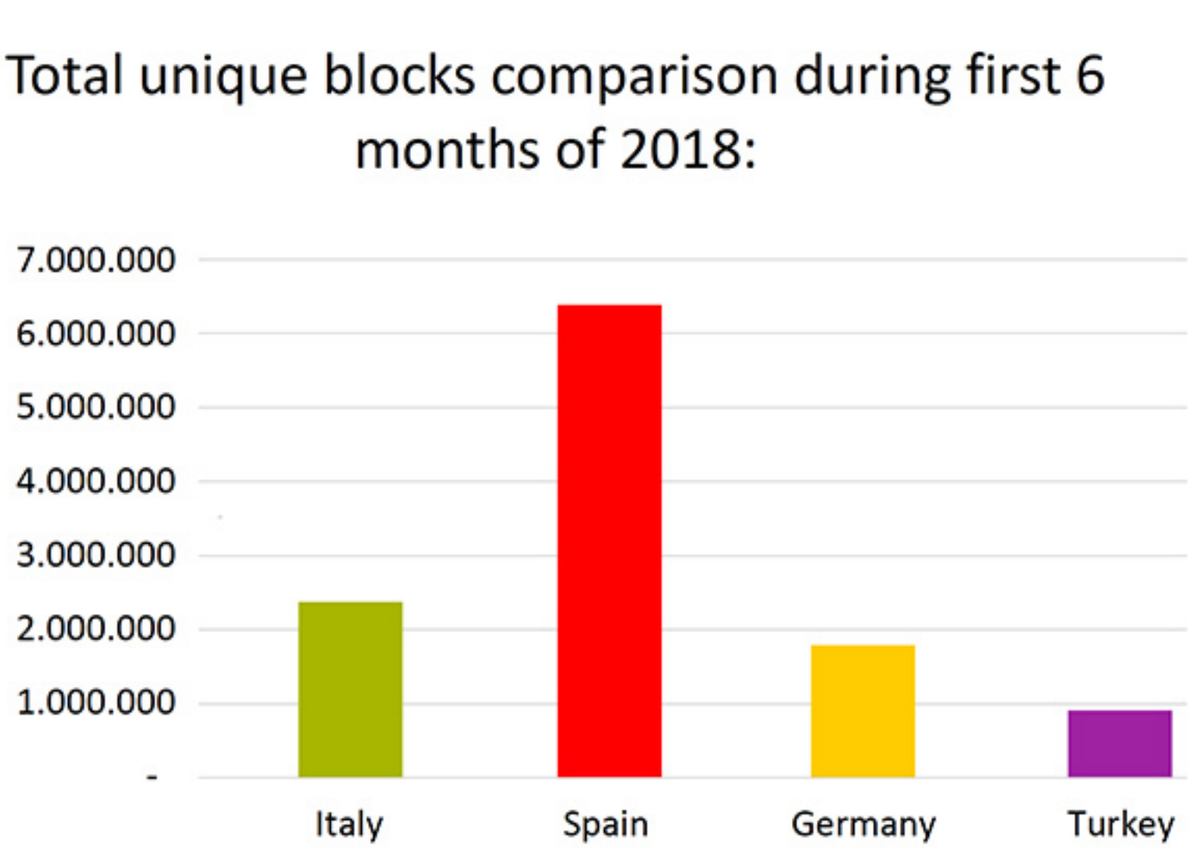
Il seguente è il confronto tra l'Italia e altri clienti Vodafone considerando i blocchi totali e i blocchi unici totali durante i primi sei mesi:



Countries	Total Blocks:
Italy	864.317.176
Spain	2.584.040.830
Germany	506.905.161
Turkey	9.561.653

Come possiamo vedere in questi grafici, la Spagna è al di sopra della media con un'enorme quantità di blocchi dovuti per lo più a CoinHive. L'Italia è il secondo paese subito seguito dalla Germania.

Il seguente è il confronto tra l'Italia e altri clienti Vodafone considerando i blocchi totali e i blocchi unici totali durante i primi sei mesi:

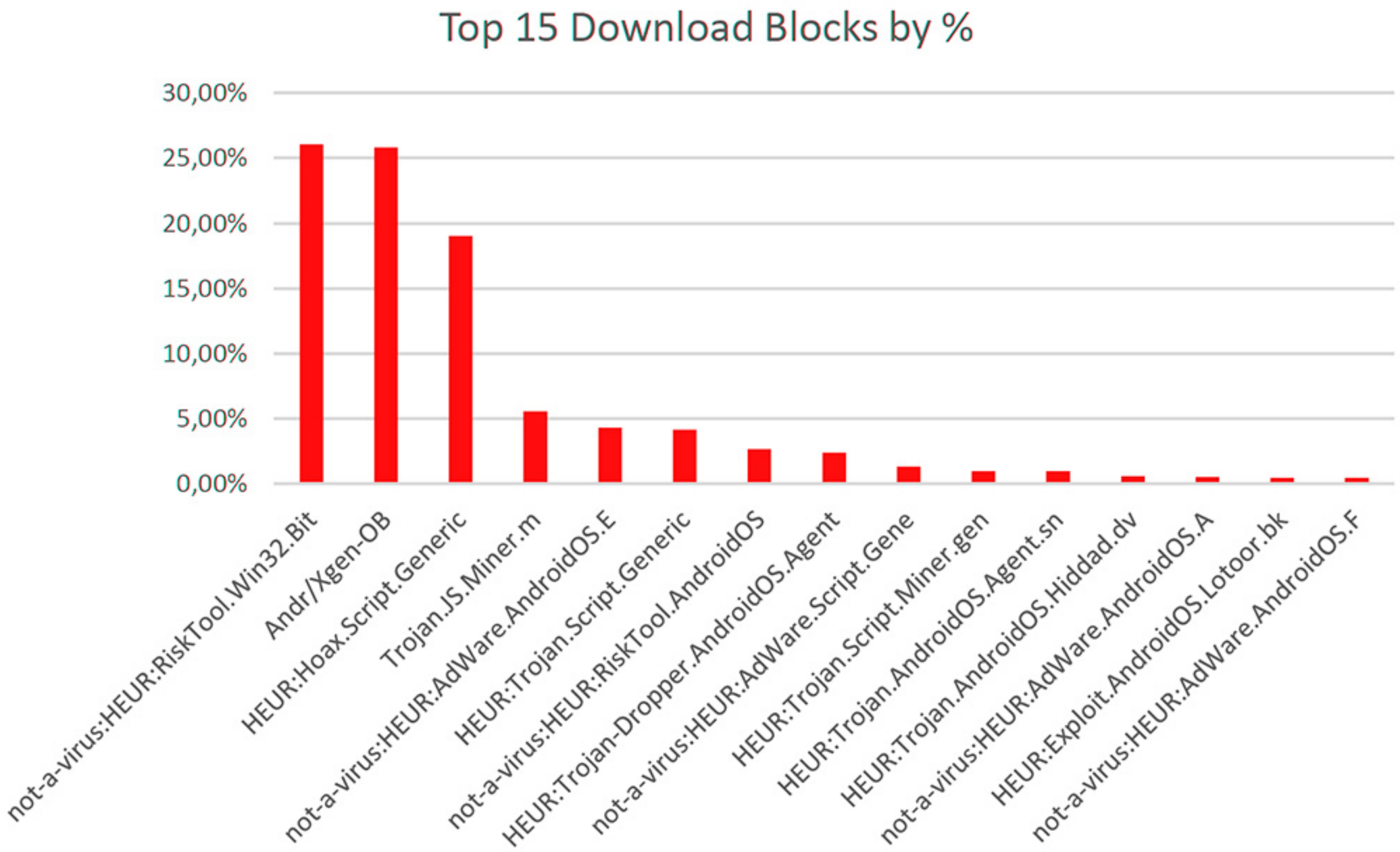


Countries	Total Unique Blocks:
Italy	1.818.742
Spain	6.271.919
Germany	1.685.356
Turkey	612.664

La Spagna è anche il leader dei blocchi Unici per utente, ma la differenza tra questi i paesi è minore. In questa categoria, l'Italia è ancora più vicina alla Germania.

5 Maggiori minacce rilevate sui clienti di Rete Sicura

Dall'analisi dei dati per Rete Sicura Italia, nel mese di Agosto 2018, le prime 15 minacce provenienti dai download bloccate, in percentuale, sono le seguenti:



TOP 5 Minacce bloccate

- HEUR:RiskTool.Win32.bit
- Andr/Xgen-OB
- HEUR:Hoax.Script.Generic
- Trojan.JS.Miner.m
- HEUR:AdWare.AndroidOS.E

Queste minacce sono spiegate in dettaglio nel seguente capitolo (Principali download bloccati per rilevanza)

6 Principali download bloccati per rilevanza

6.1 Not-a-virus:HEUR:RiskTool.Win32.Bit

Questa minaccia da download si trova al primo posto nella classifica con il 26,06% del totale. E' stato bloccato 1.204.021 volte durante il mese di Agosto.

Questo tipo di malware è un RiskTool. I programmi di questa categoria hanno svariate funzioni (come nascondere i file nel sistema, nascondere le finestre che eseguono le applicazioni, terminare processi attivi, ecc.) che possono essere usati con intenti malevoli. Di per non sono dannosi. Infati questi programmi sono utilizzati per iscriversi a servizi premium via SMS e per vincere denaro.

Se un utente ha installato tale programma sul suo computer, o se è stato installato dall'amministratore del sistema, non rappresenta alcuna minaccia.

6.2 Andr/Xgen-OB

Al secondo posto tra le prime 5 minacce da download, troviamo Andr / Xgen-OB. Questa minaccia è stata bloccata 1.194.060 volte, pari al 25,84% dei blocchi da download totali nel mese di Agosto.

Questo malware è un trojan pericoloso che colpisce i sistemi Android.

Andr/Xgen-OB

Category:	Viruses and Spyware
Type:	Trojan

Affected Operating Systems

Android

Un trojan è un tipo di malware che si traveste da software innoquo. I trojan possono essere impiegati dagli hacker che cercano di accedere ai sistemi degli utenti. Gli utenti sono generalmente ingannati da una qualche form di ingegneria sociale a caricare e eseguire i trojan sui loro sistemi. Una volta attivato, i trojan possono consentire ai cyber-criminali di spiarti, rubare i dati sensibili e ottenere l'accesso backdoor al sistema.

6.3 HEUR:Hoax.Script.Generic

Al terzo posto incontriamo HEUR: Hoax.Script.Generic. Questa minaccia è stata bloccata 879.176 volte, pari al 19,03% dei blocchi da download totali ad Agosto. Per la prima volta incontriamo la parola Hoax. Significa truffa, anche se, secondo fonti come Kaspersky, non e' al momento considerato un malware. Hoax.Script.Generic è un JavaScript archiviato nella cache del browser rilevata come dannosa. Anche se il JavaScript nella cache può essere dannoso, non è un virus. (Nota: il team di Allot continuerà a fare ricerche su questa minaccia per fornire ulteriori informazioni).

6.4 Trojan.JS.Miner.m

Questo virus è stato bloccato 257.437 volte, pari al 5,57% del totale. È un trojan quindi ha comportamenti molto diversi come spyware o solo infezione.

Trojan.JS.Miner.m è un malware pericoloso, come qualsiasi Trojan cercherà di intrufolarsi nel nostro terminale e svolgere tutti i tipi di attività. Ogni volta che il sistema viene avviato, questo Trojan sarà attivato e modificherà il registro e le opzioni di avvio, in modo che possa essere sempre attivo.

Una volta che questo Trojan è nel nostro dispositivo, può svolgere qualsiasi attività come spiare quello che stiamo facendo durante la navigazione in modo da raccogliere informazioni sensibili (come dati bancari e password), molestare l'utente con annunci pubblicitari, rallentare la nostra connessione, bloccare il nostro terminale e persino estrarre la cripto valuta senza che l'utente che se ne accorga.

6.5 Not-a-virus:HEUR:AdWare.AndroidOS.E

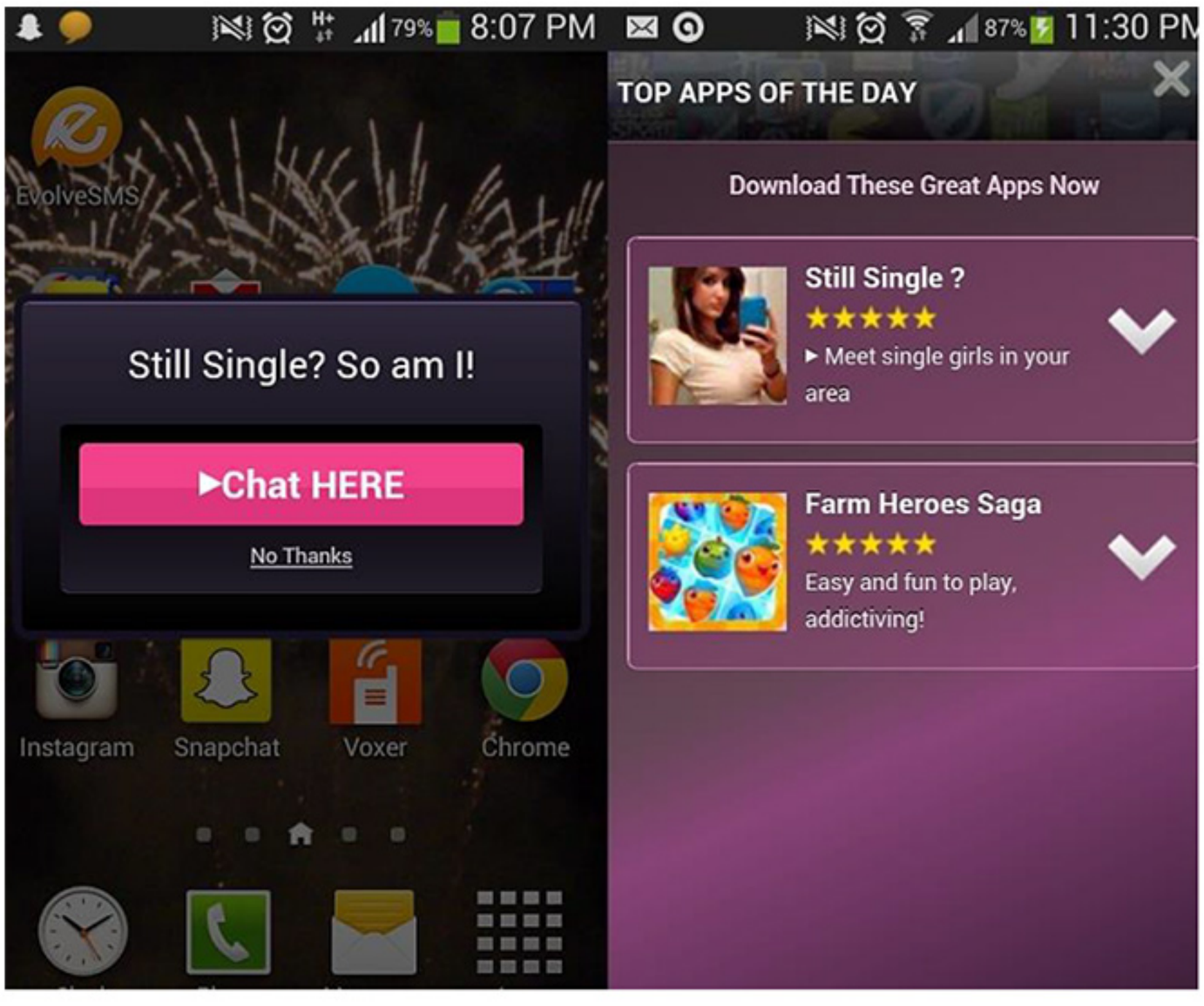
In quinta posizione troviamo EUR: AdWare.AndroidOS.E.

È stato bloccato 198.631 volte, raggiungendo il 4,30% dei blocchi da download totali.

Questo malware appartiene alla famiglia di Adware, lo scopo di questo tipo di malware è di bombardare l'utente con pubblicità e popup in modo da entrate tramite click o visualizzazione

(vedi esempio sotto). Questo è un semplice Adware come ce ne sono molti altri per Android

È un virus riconfigurabile, quindi una volta nel nostro sistema, gli hacker possono "riprogrammare" il virus in modo che possa svolgere qualsiasi attività che essi vogliano. Questo è il motivo per cui il comportamento di questo malware è diverso su ogni terminale. In questo caso, dato che è un Miner, si può dire per certo che inizia un processo di criptomining. (Nota: la squadra di Allot continuerà a fare ricerche su questa minaccia per fornire maggiori informazioni)



Il valore della cripto valuta fluttua in base alla domanda e all'offerta, sebbene non vi sia un valore fisso. Acquirenti e venditori concordano su un valore, che è equo e si basa sul valore del trading di cripto valuta altrove. Non vi sono intermediari come la banca coinvolti nella transazione, poiché si tratta di una transazione peer-to-peer, la commissione di transazione associata alle carte di credito viene eliminata. L'identità dell'acquirente e del venditore non viene rivelata. Tuttavia, ogni transazione è resa pubblica a tutte le persone nella rete blockchain. Si può acquisire una cripto valuta attraverso gli scambi trovati online o scambiati con le valute tradizionali.

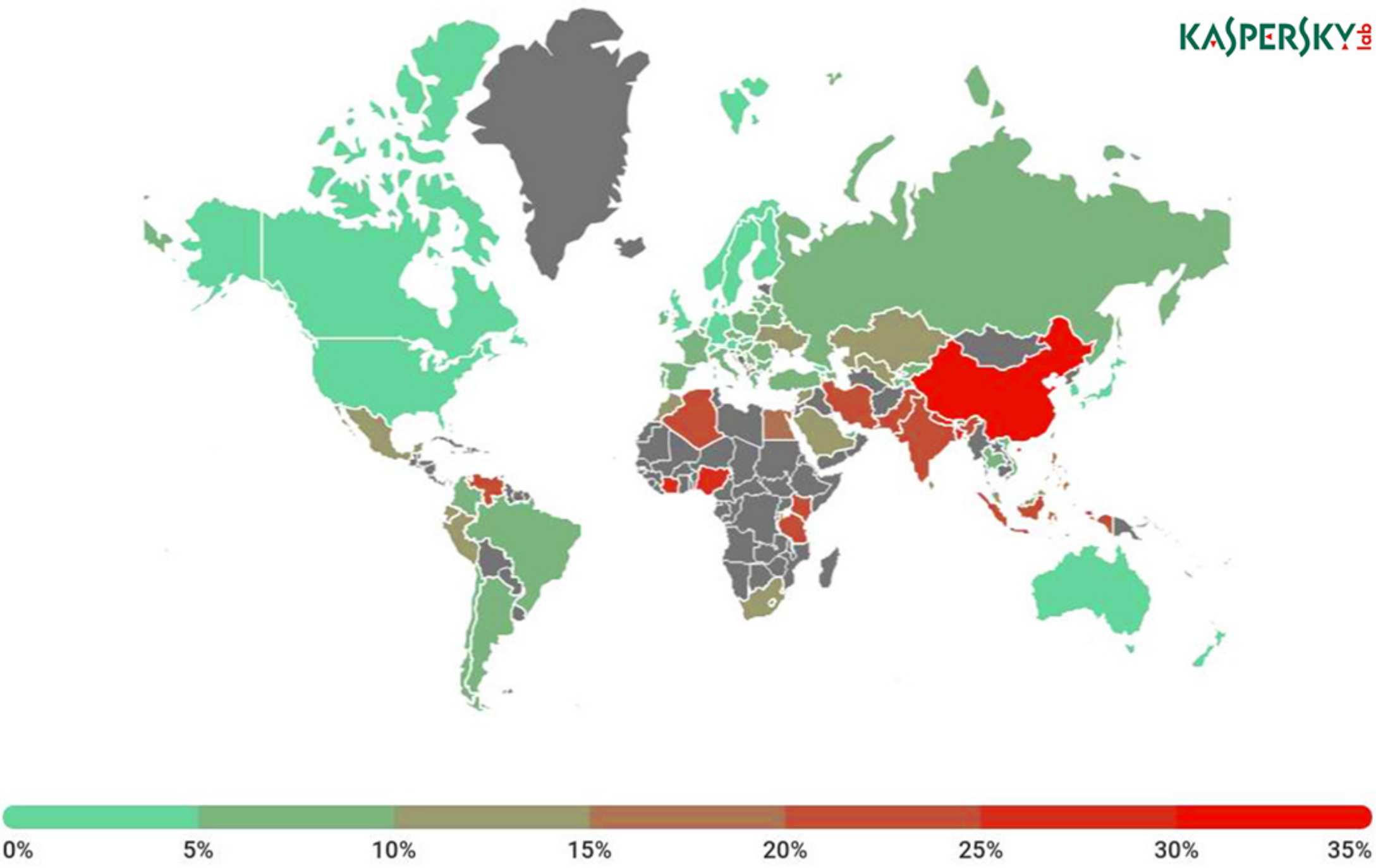
Estrazione

L’estrazione di criptovaluta include due funzioni, ovvero: aggiunta di transazioni alla blockchain (protezione e verifica) e rilascio di nuova valuta. I singoli blocchi aggiunti dagli estrattori devono contenere una proof-of-work o PoW.

L'attività di estrazione ha bisogno di un computer e di un programma speciale, che aiuta gli estrattori a competere con i loro pari nel risolvere complicati problemi matematici. Ciò richiederebbe enormi risorse informatiche. A intervalli regolari, gli estrattori tentano di risolvere un blocco con i dati della transazione utilizzando le funzioni crittografica di hash. Il valore Hash è un valore numerico di lunghezza fissa che identifica in modo univoco i dati. Gli estrattori usano il loro computer per individuare un valore di Hash inferiore al target e chiunque sarà il primo a craccarlo verrà considerato come colui che ha estratto il blocco ed è idoneo a ricevere un premio. Il premio per l’estrazione di un blocco è attualmente (al 24 settembre 2018) 6.2 bitcoin. In precedenza, solo gli appassionati di crittografia fungevano da estrattori. Tuttavia, poiché le cripto valute hanno guadagnato popolarità e valgono di più, l'attività di estrazione è ora considerata un'attività lucrativa. Di conseguenza, diverse persone e imprese hanno iniziato a investire in magazzini e hardware. Mentre le imprese si gettavano nella mischia, incapaci di competere, gli estrattori di bitcoin hanno iniziato a unirsi a dei gruppi aperti, combinando le risorse per competere in modo efficace. Un esempio può essere visto con la creazione del sito web chiamato www.coinhive.com. Questa piattaforma consente agli amministratori di pagine Web più avide di implementare una serie di script che estraggono queste cripto valute sui computer degli utenti in background, senza autorizzazione, con accesso solo alla pagina web.

7 Minacce sul dispositivi mobile nei primi 6 mesi del 2018

La seguente immagine mostra le minacce su dispositivi mobile per paese:

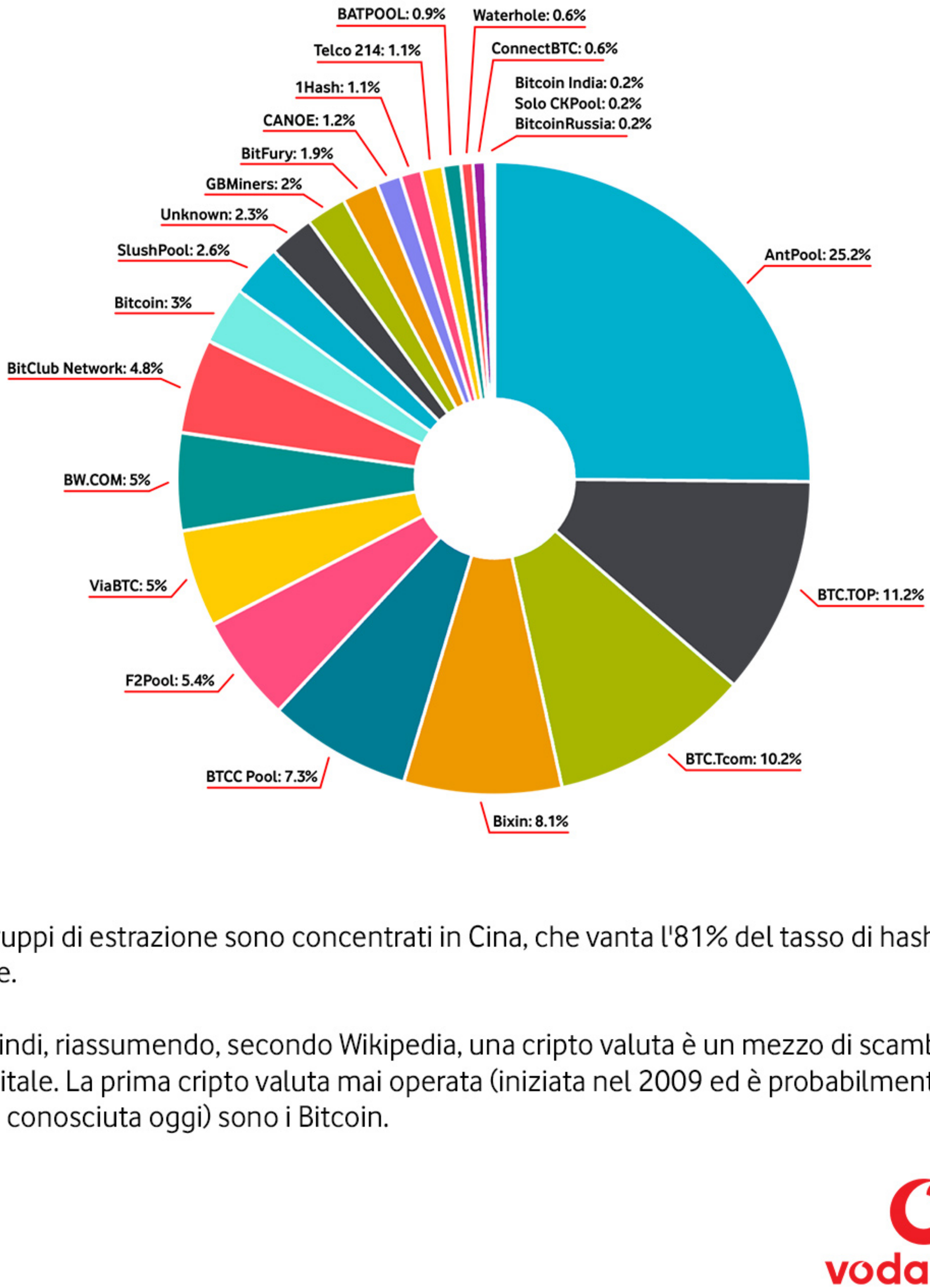


Qui sotto le top 10 per utenti attaccati da malware su dispositivi mobile:

	Country*	%**
1	China	34.43
2	Bangladesh	27.53
3	Nepal	27.37
4	Ivory Coast	27.16
5	Nigeria	25.36
6	Algeria	24.13
7	Tanzania	23.61
8	India	23.27
9	Indonesia	22.01
10	Kenya	21.45

Le due società che dominano l'industria di estrazione a livello consumer sono Canaan e Bitmain. Bitmain, con sede a Pechino, opera nel settore di estrazione e produce hardware per tale industria.

Gruppi di estrazione e la loro quota di estrazione



I gruppi di estrazione sono concentrati in Cina, che vanta l'81% del tasso di hash della rete.

Quindi, riassumendo, secondo Wikipedia, una cripto valuta è un mezzo di scambio digitale. La prima cripto valuta mai operata (iniziata nel 2009 ed è probabilmente la più conosciuta oggi) sono i Bitcoin.

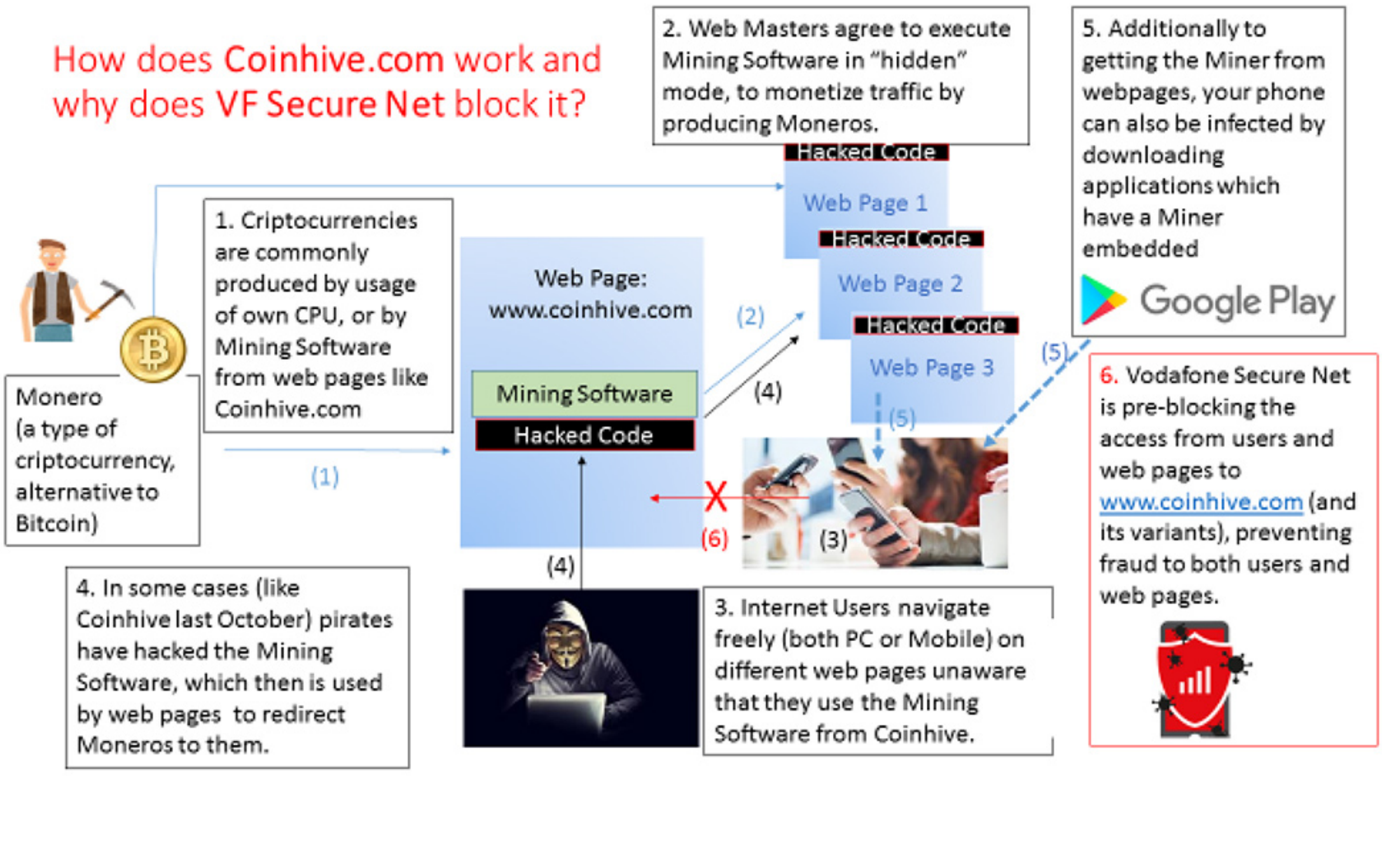
Il bitcoin è stata la prima, ma oggi non è l'unica cripto valuta: negli ultimi anni ne sono apparsi molte altre, con caratteristiche e protocolli diversi, come ad esempio Litecoin, Ripple e Dogecoin. Nel gruppo di Altcoin o cripto valute alternative, ultimamente si è parlato molto di Monero, poiché da non molto tempo questa cripto valuta era nota per essere la più privata e sicura di tutte. E' diventata presto famosa catturando l'attenzione dei mercati di Internet molto rapidamente, iniziando a essere usata come metodo di pagamento più anonimo e sicuro di Bitcoin.

Negli ultimi mesi, il valore delle cripto valute è aumentato in modo esponenziale, di conseguenza anche l'interesse per la loro attività di estrazione e commercializzazione. Questo ha attirato l'attenzione dei pirati di Internet che hanno messo gli occhi sulle cripto valute, per cercare di metterci le mani in vari modi illegali.

Il caso di Coinhive

Come menzionato in precedenza, gli estrattori "tradizionalmente" hanno sempre usato i propri computer e / o specifiche CPU per estrarre la cripto moneta. Ma più recentemente, c'è stata una diffusione dell'uso del software per integrarlo in diverse pagine web, come nel caso di www.coinhive.com. Questa piattaforma consente agli amministratori di pagine Web di implementarci una serie di script che vengono utilizzati per "estrarre" le cripto valute nei PC o telefoni cellulari degli utenti in una maniera differente, senza il loro permesso, ma semplicemente accedendo alla pagina web. È in questo modo che queste pagine web possono monetizzare il traffico dei loro utenti, senza aumentare la pubblicità o le entrate di un altro tipo (vedi screenshot qui sotto).

Questo tipo di pagine web, abbastanza recenti, stanno iniziando a essere riconosciute (dal momento che non richiedono il permesso dell'utente) come "dannose" da alcuni dei principali motori antivirus del mondo. A parte questo, nel caso di Coinhive.com, è stato scoperto di recente che è stato violato dai dagli hackers con l'obiettivo di farsi reindirizzare tutti i guadagni delle estrazione della cripto valuta (si veda lo schema seguente).



Riepilogo grafico di come funziona Coinhive.com e di come Rete Sicura protegge i propri clienti

Uno sguardo più approfondito su Monero e Coinhive.com

Ma oltre a tutto ciò, cos'è Monero e come funziona? È davvero utile solo nel Deep Internet? Per iniziare, bisogna dire che la sua nascita avvenne nell'Aprile 2014 come un Bytecoin Fork, la prima cripto valuta ad usare il protocollo CryptoNote invece che quello usato per Bitcoin.

Si tratta di un sistema crittografico descritto per la prima volta alla fine del 2012 da Nicolas van Saberhagen, in cui le transazioni sono anche registrate in una blockchain, ma senza rivelare né il mittente né il destinatario né l'importo effettivo: si può solo sapere che l'importo mostrato è sempre inferiore a quello vero.

In linea di principio, Monero (XMR) nasce con il nome di BitMonero, un'unione tra Bitcoin 'bit' e, letteralmente, 'valuta' in esperanto.

vodafone

Coinhive è diventato molto popolare nelle ultime settimane in quanto è uno strumento innovativo che ti consente di beneficiare Monero con il tuo browser.

Coinhive è uno strumento basato sulla libreria JavaScript dove i proprietari di siti Web possono caricarci. Quando gli utenti accedono al sito, la libreria di codici JavaScript di Coinhive esegue ed estrae le estrazione per Monero attraverso il proprietario del sito, ma utilizzando le risorse della CPU dell'utente. Coinhive è stato lanciato il 14 Settembre e i suoi autori lo annunciano come un'alternativa alla pubblicità classica. Monero utilizza una piccola parte della CPU dell'utente mentre l'utente naviga nel sito. I proprietari del sito possono guadagnare denaro e sostenere la loro attività e non disturbare i loro visitatori con annunci fastidiosi.

A Crypto Miner for your Website

Pirate Bay è uno dei siti di scambio di file più popolari e visitati al mondo utilizzato prevalentemente per condividere gratuitamente materiale protetto da copyright.

The Pirate Bay

The Pirate Bay, utilizzato per testare l'implementazione di questo strumento che utilizza la potenza di elaborazione dei propri visitatori per estrarre monete digitali. Questa pagina ha voluto generare dei ricavi sfruttando segretamente la potenza della CPU dei suoi milioni di visitatori per estrarre l'alternativa Bitcoin denominata Monero a loro insaputa.

L'Internet moderno dipende dalle entrate pubblicitarie per sopravvivere, il che a quanto pare rovina l'esperienza degli utenti. Ma The Pirate Bay sta cercando di scegliere un approccio diverso.

I visitatori di The Pirate Bay hanno recentemente scoperto che attraverso l'estrazione e la crittografia JavaScript-based di Coinhive (un servizio che aiuta i siti web a monetizzare attraverso la potenza della CPU) su siti torrent, loro utilizzano la potenza della CPU del computer del visitatore che genera le valute digitali.

Tuttavia, poco dopo che è venuto a galla il problema, The Pirate Bay ha rilasciato una dichiarazione sul proprio sito Web, affermando di aver testato l'estrattore per sole 24 ore per vedere se questo sistema potrebbe essere utilizzato come alternativa per generare entrate, sbarazzandosi completamente di annunci fastidiosi sui siti torrents.

The Pirate Bay ha anche chiarito che il software dell'estrattore dovrebbe consumare solo tra il 20 e il 30 percento della potenza della CPU e dovrebbe essere limitato a lavorare in una singola scheda. Gli utenti devono essere avvertiti su queste intrusioni dal rispettivo sito Web.

Sfortunatamente, nonostante l'uso intelligente dell'estrazione Monero, Coinhive si trova nella situazione di altri strumenti utili che sono stati usati dai ladri. Pochi giorni dopo il suo lancio, Coinhive si è diffuso in quasi tutti gli angoli della comunità di malware.

Per prima cosa, l'abbiamo visto incorporato in una popolare estensione Chrome denominata SafeBrowse, in cui è stato aggiunto il codice Coinhive per l'esecuzione in background su Chrome. Poi, Coinhive è stato incorporato in typosquatted dominos. Qualcuno ha registrato il dominio twitter.com.com e stava caricando la libreria di Coinhive JS sulla pagina. Gli utenti che digitavano l'URL di Twitter finivano erroneamente sulla pagina MOnero. Ciò accadeva solo per pochi secondi fino a quando l'utente non si sarebbe accorto della pagina sbagliata, ma era sufficiente per il proprietario del sito di generare profitti. Col tempo, il proprietario di tutte le URL digitate male avrebbe ottenuto un buon profitto.

Successivamente, i ricercatori della sicurezza hanno scoperto siti compromessi in cui gli intrusi hanno modificato il codice sorgente del sito e trasportato in segreto l'estrattore Coinhive. L'estrattore con una configurazione sfruttava Monero per l'account personale dell'hacker, ma utilizzando la potenza della CPU degli utenti che non si fidavano di accedere ai siti hackerati. I ricercatori hanno scoperto che i siti di WordPress e Magento sono stati modificati in questo modo.

Inoltre, gli esperti di sicurezza hanno trovato anche uno dei più grandi gruppi di malvertising che distribuiva lo script di Coinhive. Le pubblicità dannose reindirizzavano gli utenti alle truffe del supporto tecnico, dove oltre ai classici avvisi di virus falso, i criminali caricavano Coinhive nel navigatore per Monero mentre le vittime cercavano di scoprire se il sito fosse valido o meno.

8 Analisi Coinhive

Come è stato spiegato in precedenza, abbiamo assistito a un forte aumento dei blocchi in Italia tra Febbraio e Marzo 2018. Ciò è chiaramente dovuto a una minaccia diffusa nell'estrazione di cripto valuta in Europa che sicuramente ha avuto impatto in Italia in quei mesi: Coinhive.com.

Cos'è la cripto valuta?

La cripto valuta è una forma di moneta digitale progettata per essere sicura e anonima nella maggior parte dei casi casi. Viene usata una tecnica chiamata crittografia - un processo utilizzato per convertire le informazioni leggibili in un codice quasi non crackabile , per aiutarti a tracciare acquisti e trasferimenti. È utilizzata anche per proteggere comunicazioni, informazioni e denaro online.

Le cripto valute consente agli utenti di effettuare pagamenti sicuri, senza dover passare attraverso banche. Alcune delle più famose criptovalute includono Bitcoin, Bitcoin Cash, Ethereum,

DigitalNote, LiteCoin e PotCoin.

Come funzionano le cripto valute?

Una criptovaluta viene eseguita su una blockchain, che è un registro condiviso o un documento duplicato più volte attraverso una rete di computer. Il documento aggiornato è distribuito e messo a disposizione di tutti i possessori della criptovaluta.

Ogni singola transazione effettuata e la proprietà di ogni singola cripto valuta in

la circolazione è registrata nella blockchain. La blockchain è gestita da estrattori, che usano

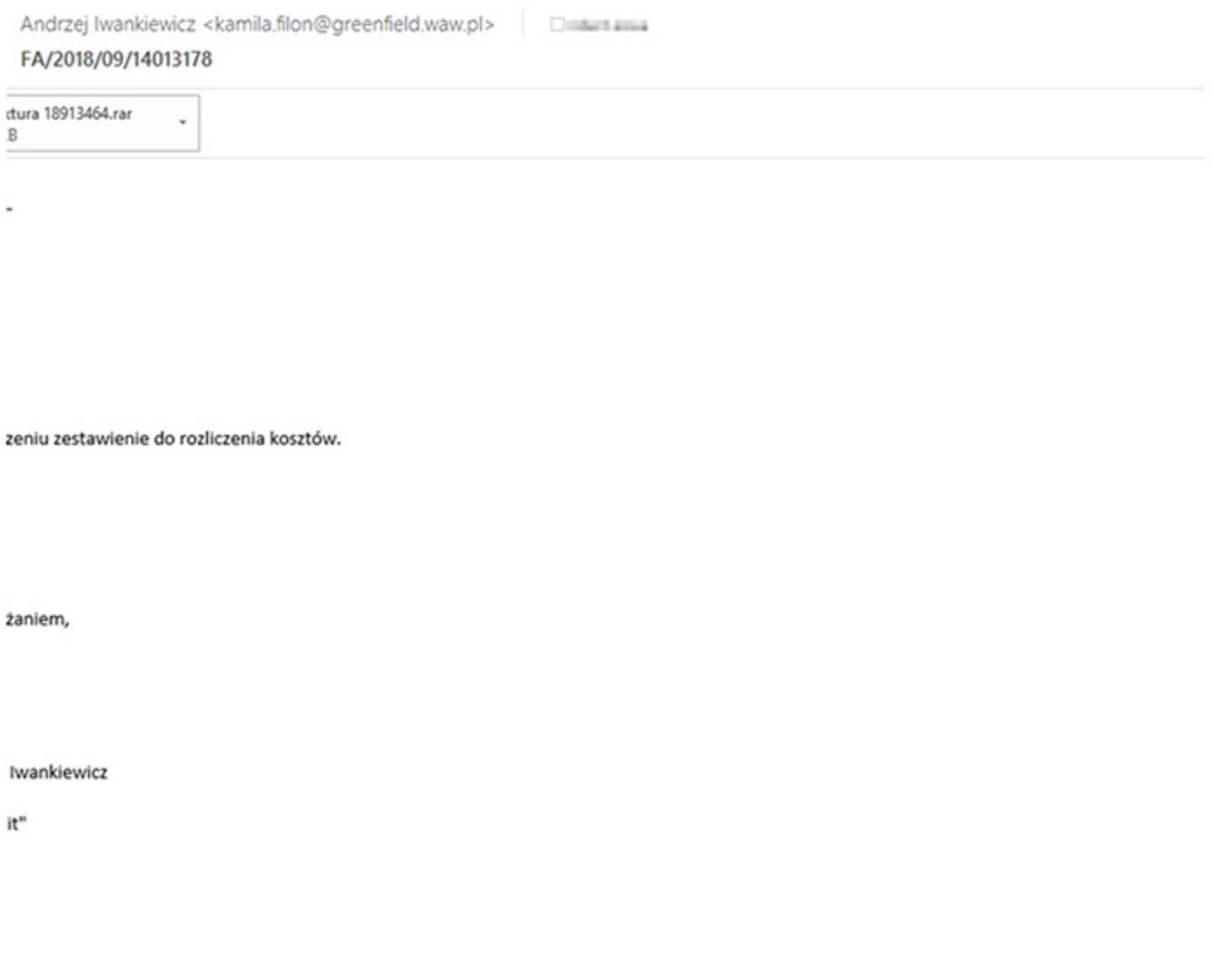
computer potenti che calcolano le transazioni. La loro funzione è di aggiornare ogni volta la transazione fatta e anche garantire l'autenticità delle informazioni, accertando in tal modo che ogni transazione è sicura e viene elaborata correttamente e in sicurezza.

9 Nuovo Banking Trojan in Italia

Il trojan bancario nascosto DanaBot scoperto da Proofpoint nel Maggio 2018 quando ha iniziato a colpire Australia e Polonia tramite URL malevoli si è ora trasferito in Europa, con nuove campagne di posta elettronica che hanno colpito l'Italia, l'Austria, la Germania e l'Ucraina.

Secondo un'analisi effettuata da ESET Research, il trojan bancario DanaBot scritto in Delphi ha una struttura modulare facilmente espandibile dagli attori delle minacce dietro di esso tramite plug-in.

Prima di trasferirsi in Europa, durante le campagne in Australia, DanaBot è arrivato con quattro plug-in. Il plug-in VNC che consente all'autore dell'attacco di connettersi alla macchina della vittima, mentre il plug-in di stealer è progettato per raccogliere automaticamente tutte le password immesse in una vasta gamma di applicazioni.



Andrzej Iwankiewicz <kamila.filon@greenfield.waw.pl>

FA/2018/09/14013178

ctura 18913464.rar
B

zeniu zestawienie do rozliczenia kosztów.

żaniem,

Iwankiewicz

it"

Campagna email Danabot, esempio dalla Polonia

Inoltre, la versione "australiana" di DanaBot è arrivata con un plug-in dello sniffer che avrebbe iniettato un codice dannoso all'interno dei siti visitati con l'obiettivo di rubare informazioni sensibili come credenziali e dati di pagamento e un plug-in TOR che lo ha aiutato a connettersi a Siti "a cipolla" (dal deep web).

10 Sommario

Alla luce delle informazioni di cui sopra, è possibile trarre le seguenti conclusioni del servizio Vodafone Rete Sicura per l'Italia nell'Agosto 2018.

- Il numero totale di minacce bloccate in Italia tra i primi 6 mesi, tra Gennaio e Giugno 2018 è stato di 935 milioni.

- La maggior parte delle minacce bloccate in questo periodo erano dovute a una diffusa minaccia di criptomining in Europa, originata da Coinhive.com.

- Senza l'effetto Coinhive, il numero medio di blocchi per utente da Aprile ad Agosto è 32.2.

- Tra le principali minacce di questo periodo, la principale minaccia bloccata nel download è stata "Not-a-Virus: HEUR: RiskTool.Win32.Bit, bloccato 1.204.021 volte durante il mese di Agosto.

- Il resto dei più importanti blocchi di visur provenienti dai download è:
    - Andr/Xgen-OB
    - HEUR:Hoax.Script.Generic
    - Trojan.JS.Miner.m
    - HEUR:AdWare.AndroidOS.E

- L'estrazione di cripto valute è stata molto popolare in Europa nel 2018 e ha avuto un grande impatto sulle minacce bloccate da Vodafone Rete Sicura. Ciò è dovuto al fatto che, negli ultimi mesi, il valore delle cripto valute è cresciuto in modo esponenziale, seguito dall'interesse per l'estrazione e il trading. Sfortunatamente, queste cripto valute hanno attirato l'attenzione degli hacker e hanno sollevato la richiesta di provare a utilizzare malware di cripto valuta, rubare database di cripto valute e persino piattaforme di attacco, come CoinHive, con lo scopo che tutti i profitti di estrazione vadano direttamente ai criminali informatici.

11 Per saperne di più

- https://www.enigmasoftware.com/heurtrojandownloaderscriptgeneric-removal/
- https://www.virustotal.com/es/
- http://www.malwarerid.com
- http://deletevirusmalware.com
- https://securelist.com/statistics/
- https://threats.kaspersky.com/
- Annex: Coinhive Effects in Mobile Performance, Allot, April 2018.

Si ringraziano della collaborazione il Team di Allot

(Product Marketing Manager Juan Latasa, Vito Cirillo), team di Rete e Marketing di Vodafone Italia S.p.a.

Tutti i dati riportati sono stati analizzati a livello aggregato in conformità con le norme europee in tema di GDPR.

www.allot.com
Americas: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA - Tel: +1 781-939-9300; Fax: +1 781-939-9393; Toll free: +1 877-255-6826
Europe: NCI–Les Centres d'Affaires Village d'Entreprises, 'Green Side' 400 Avenue Roumanille, BP309 06906 Sophia Antipolis,
Cedex France - Tel: +33 (0) 4-93-001160; Fax: +33 (0) 4-93-001165
Asia Pacific: 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104, Tel: +65 6749-0213; Fax: +65 6848-1015
Japan: 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 - Tel: +81 (3) 5297 7668; Fax: +81 (3) 5297 7669
Middle East & Africa: 22 Hanagar Street, Industrial Zone B, Hod Hasharon, 4501317 Israel - Tel: 972 (9) 761-9200; Fax: 972 (9) 744-3626

allot
See. Control. Secure.

vodafone