

Report sulle minacce

McAfee Labs

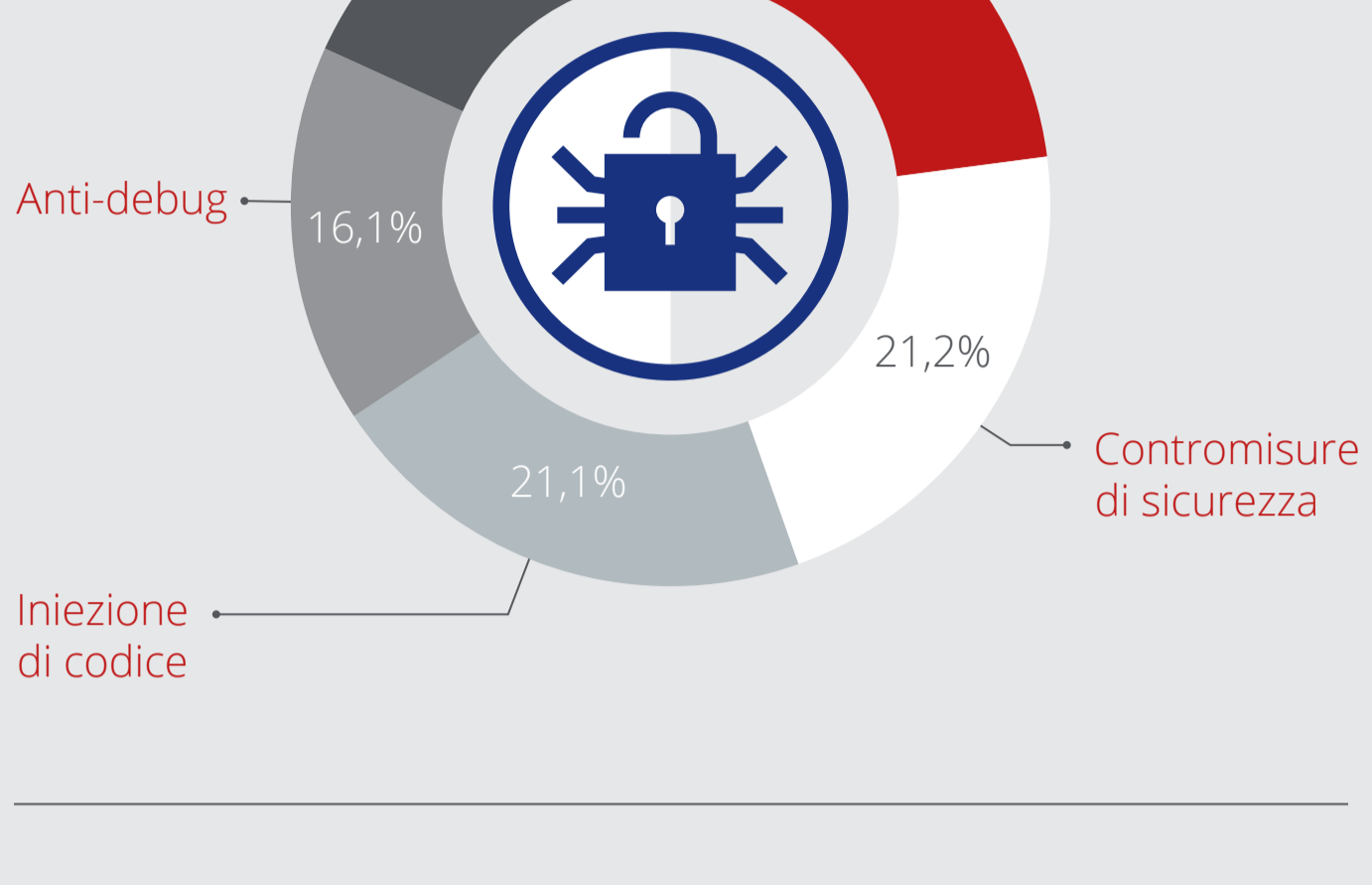
Tecniche e tendenze dell'evasione del malware

Le tecniche di evasione del malware sono ampiamente disponibili e stanno diventando più potenti.

La storia delle tecniche di evasione



Tecniche di evasione utilizzate dal malware



Evasione

Il codice delle tecniche di evasione può essere acquistato in serie, qualche volta a titolo gratuito.



Firmware

Un'infezione firmware è un metodo sempre più diffuso per evadere il rilevamento.



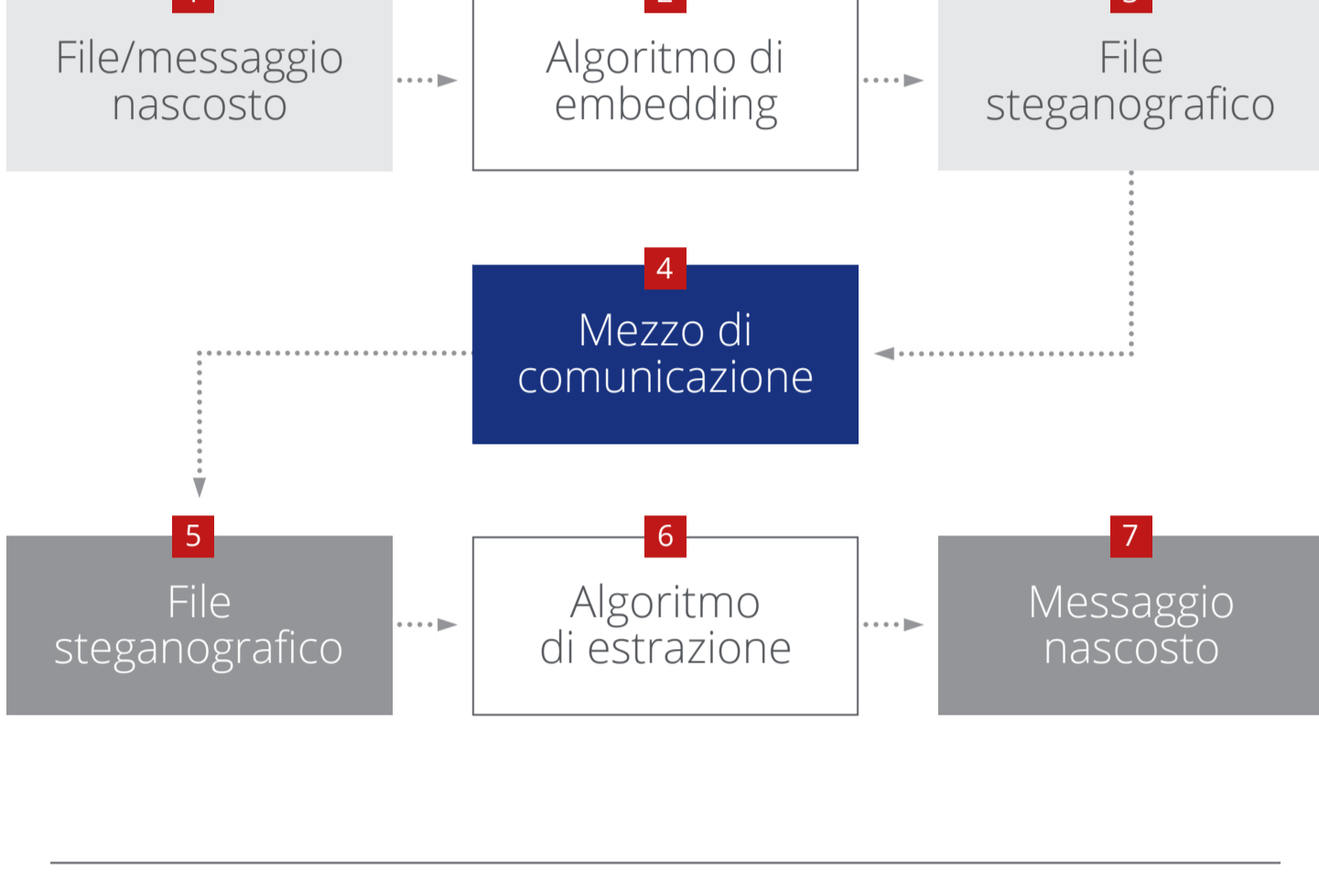
Apprendimento automatico

Gli aggressori stanno sviluppando tecniche per aggirare la sicurezza basata sull'apprendimento automatico.

Nascosto ma non troppo: la minaccia occulta della steganografia

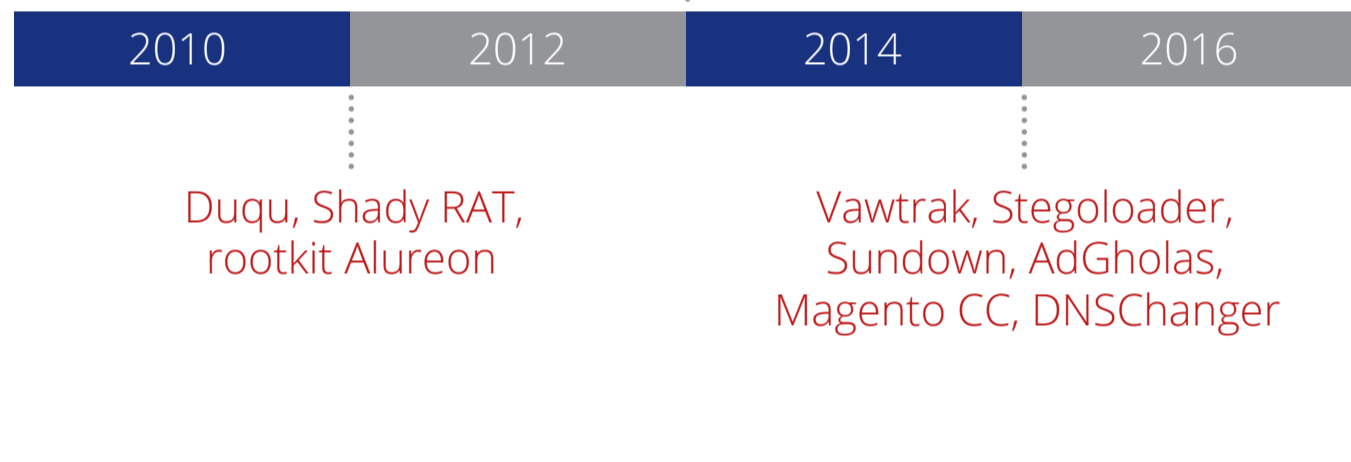
Steganografia: l'arte e la scienza di nascondere la comunicazione.

Il processo della steganografia digitale



La steganografia digitale nel malware

Zbot, Lurk, ZeusVM, MiniDuke, CosmicDuke



Messaggio segreto

La steganografia nasconde un messaggio segreto in uno apparentemente legittimo.



440 a.C.

La steganografia è stata utilizzata in varie forme almeno a partire dal 440 a.C.



2011

La steganografia digitale è stata utilizzata per la prima volta da Duqu nel 2011.



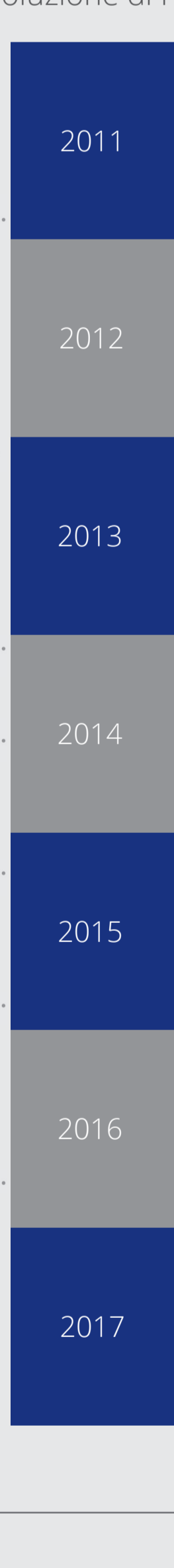
Rete

La steganografia di rete è l'ultimo genere di steganografia digitale usato dal malware.

Il pericolo crescente di Fareit, il password stealer che ruba le password

All'inizio di quasi tutti i maggiori attacchi compiuti dalle minacce avanzate persistenti vengono usati dei programmi per il furto delle password. Fareit è stato probabilmente utilizzato nel 2016 nella violazione del Comitato Democratico Nazionale.

L'evoluzione di Fareit



La prima variante di Fareit con funzionalità di furto di credenziali e attacco DDoS

BHEK diffonde Fareit con Zeus, FakeAV

Fareit scarica Medfos, Nymaim, diffondendosi attraverso una campagna spam

Fareit avvia l'estrazione da Bitcoin

Fuoriuscita del codice sorgente di Pony Loader 1.9

Pony Loader 2.0 è in grado di rubare i wallet Bitcoin

Il ransomware dello schermo di blocco utilizza Fareit per il furto di credenziali

Fuoriuscita del codice sorgente di Pony Loader 2.0

Fareit si diffonde attraverso il poisoning del DNS

Attacco DNC con Onion Duke

Modulo per il furto delle credenziali di Fareit individuato con Stegoloader

Fareit si diffonde utilizzando W97, PowerShell, JavaScript, MHT

Coinvolgimento di Fareit nell'operazione Grizzly Steppe

Disponibili molte varianti personalizzate di Pony Loader, fino a Pony Loader 2.2



5.599

Fareit fu scoperto nel 2011. Lo scorso anno si sono verificati 5.599 incidenti causati da Fareit presso i clienti.

Fareit ha numerose capacità:

- Ruba le password
- Scarica ed esegue malware arbitrario
- Sferra attacchi DDoS
- Ruba i wallet delle criptovalute
- Ruba le credenziali FTP

Statistiche sulle minacce

Nel primo trimestre, sono emerse 244 nuove minacce ogni minuto, ovvero più di 4 ogni secondo.

Incidenti

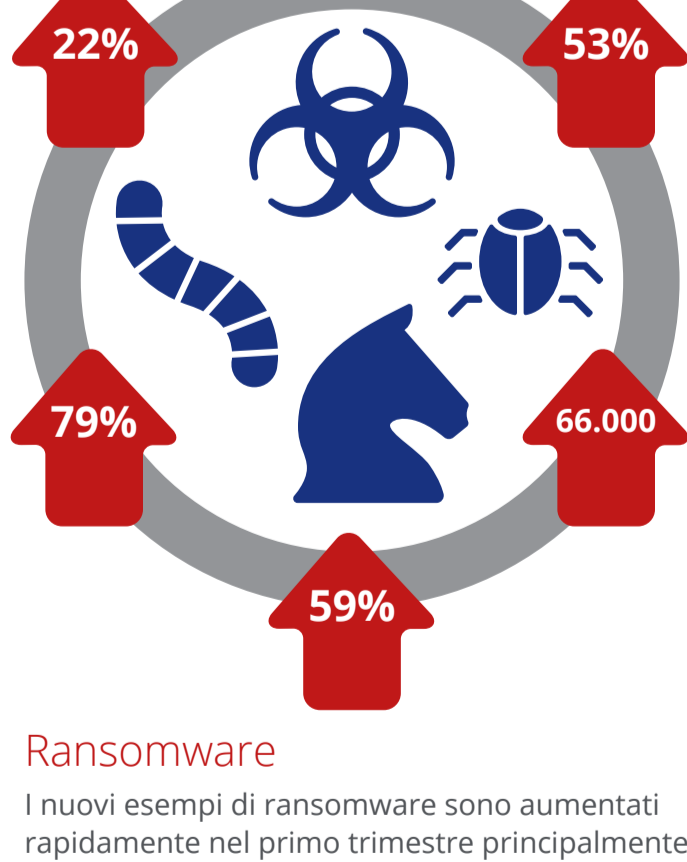
Nel primo trimestre abbiamo contato 301 incidenti di sicurezza divulgati pubblicamente, un aumento del 53% rispetto al quarto trimestre. I settori della sanità, dell'amministrazione pubblica e dell'istruzione hanno rappresentato più del 50% del totale. Il 78% di tutti gli incidenti di sicurezza divulgati pubblicamente nel primo trimestre si è verificato nelle Americhe.

Malware

Nel primo trimestre i nuovi esempi di malware sono risaliti a 32 milioni. **Il numero complessivo di esempi di malware è aumentato del 22% nei quattro trimestri scorsi per un totale di 670 milioni di esempi.**

Malware mobile

Le segnalazioni del malware mobile dall'Asia sono raddoppiate nel primo trimestre, contribuendo a un 57% di aumento nei tassi di infezione globali. **Il numero complessivo di malware mobile è aumentato del 79% nei quattro trimestri scorsi per un totale di 16,7 milioni di esempi.**



Malware per il sistema operativo Mac

Negli ultimi tre trimestri il nuovo malware per Mac OS è aumentato grazie a un piccolo dell'adware. Anche se ancora contenuto rispetto alle macro di Windows, **il numero complessivo di esempi di malware per il sistema operativo Mac è cresciuto del 53% nel primo trimestre.**

Malware delle macro

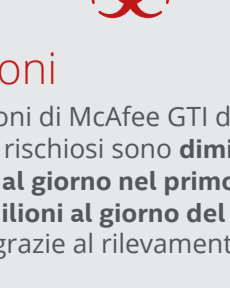
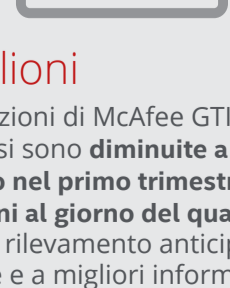
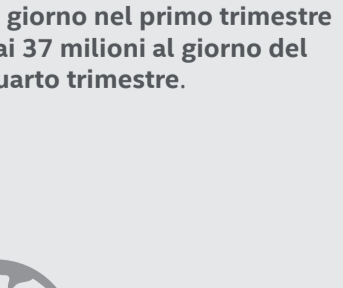
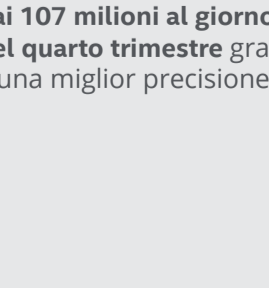
Il nuovo malware delle macro è diminuito alla media triennale. **Nel primo trimestre abbiamo osservato 66.000 nuovi esempi di malware delle macro.**

Ransomware

I nuovi esempi di ransomware sono aumentati rapidamente nel primo trimestre principalmente a causa degli attacchi del ransomware Congur sui dispositivi con sistema operativo Android. **Il numero complessivo di esempi di ransomware è aumentato del 59% nei quattro trimestri scorsi per un totale di 9,6 milioni di esempi.**

McAfee Global Threat Intelligence

Nel primo trimestre McAfee GTI ha ricevuto in media 55 miliardi di interrogazioni al giorno.



Report McAfee Labs sulle Minacce: giugno 2017

Visita www.mcafee.com/June2017ThreatsReport per il report completo.