Giugno 2017

McAfee
Together is power.

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

1980
Virus Cascade
Il primo virus ad utilizzare la crittografia per codificare i contenuti.

1990
Virus della famiglia Chameleon
I primi virus polimorfi

1998
Malware metamorfico
Regswap utilizza il metamorfismo attraverso diversi registri per le stesse funzioni.

Anni '90
Programmi di compressione
I programmi di compressione in grado di crittografare o comprimere diventano popolari grazie alle dimensioni più contenute di RAM e dischi.

1999-2003
Rootkit
Nel 1999, fa la sua apparizione il primo rootkit Windows - NTRootkit - seguito da HackerDefender nel 2003.

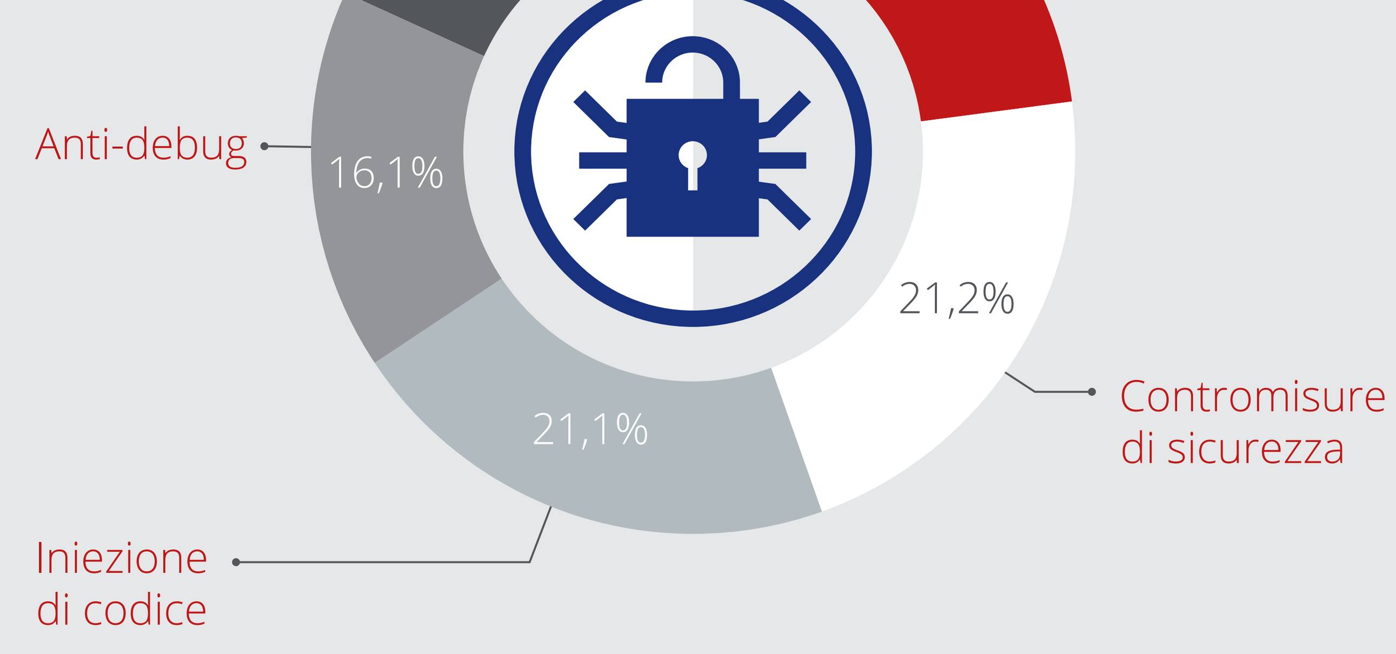
2008
Algoritmi di generazione dei domini
Il worm Conficker utilizza un DGA per evadere il rilevamento di rete.

2011
Marketplace
Silkroad è il primo mercato darknet a vendere prodotti e servizi per evadere il malware.

2015-2017
Dridex, Locky
Il primo offuscamento su larga scala, uso di PowerShell ed evasione della sandbox.

2015-2017
Malware del firmware
La fuga di notizie di Equation Group e Hacking Team rivela l'utilizzo di malware del firmware per evitare il rilevamento.

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

1. File/messaggio nascosto
2. Algoritmo di embedding
3. File steganografico
4. Mezzo di comunicazione
5. File steganografico
6. Algoritmo di estrazione
7. Messaggio nascosto

La steganografia digitale nel malware

2010 – 2012 – 2014 – 2016

Duqu, Shady RAT, rootkit Alureon

Zbot, Lurk, ZeusVM, MiniDuke, CosmicDuke

Vawtrak, Stegoloader, Sundown, AdGholas, Magento CC, DNSChanger

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

2011
- La prima variante di Fareit con funzionalità di furto di credenziali e attacco DDoS

2012
- BHEK diffonde Fareit con Zeus, FakeAV

2013
- Fareit scarica Medfos, Nymaim, diffondendosi attraverso una campagna spam
- Fareit avvia l'estrazione da Bitcoin

2014
- Fuoriuscita del codice sorgente di Pony Loader 1.9
- Il ransomware dello schermo di blocco utilizza Fareit per il furto di credenziali
- Pony Loader 2.0 è in grado di rubare i wallet Bitcoin

2015
- Fareit si diffonde attraverso il poisoning del DNS
- Fuoriuscita del codice sorgente di Pony Loader 2.0
- Attacco DNC con Onion Duke

2016
- Modulo per il furto delle credenziali di Fareit individuato con Stegoloader
- Fareit si diffonde utilizzando W97, PowerShell, JavaScript, MHT

2017
- Coinvolgimento di Fareit nell'operazione Grizzly Steppe
- Disponibili molte varianti personalizzate di Pony Loader, fino a Pony Loader 2.2

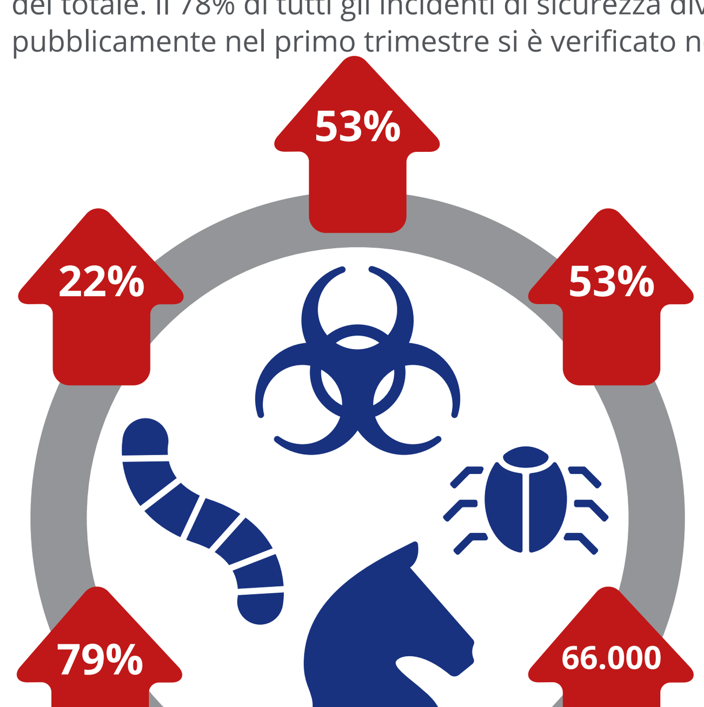
5.599
Fareit fu scoperto nel 2011. Lo scorso anno si sono verificati 5.599 incidenti causati da Fareit presso i clienti.

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

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 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.

95 milioni
Le protezioni di McAfee GTI dagli URL di rischio medio sono **diminuite a 95 milioni al giorno nel primo trimestre dai 107 milioni al giorno del quarto trimestre** grazie a una miglior precisione.

56 milioni
Le protezioni di McAfee GTI dai programmi potenzialmente indesiderati sono **aumentate a 56 milioni al giorno nel primo trimestre dai 37 milioni al giorno del quarto trimestre**.

McAfee GTI

34 milioni
Le protezioni di McAfee GTI dai file pericolosi sono **diminuite a 34 milioni al giorno nel primo trimestre dai 71 milioni al giorno del quarto trimestre** grazie al rilevamento anticipato del malware e a migliori informazioni locali.

59 milioni
Le protezioni di McAfee GTI dagli indirizzi IP rischiosi sono **diminuite a 59 milioni al giorno nel primo trimestre dagli 88 milioni al giorno del quarto trimestre** grazie al rilevamento anticipato.

Report McAfee Labs sulle Minacce: giugno 2017

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

McAfee
Together is power.

3181_0517_info-threat-report-malware-evasion