Dicembre 2016

Report sulle minacce

McAfee Labs

I centri delle operazioni di sicurezza (SOC)

Lo stato corrente dei centri operazioni di sicurezza e i piani per il futuro.

Quasi nove su 10 aziende hanno un SOC.

91%
delle grandi aziende ha un SOC.

84%
delle aziende di medie dimensioni ha un SOC.

74%
sta progredendo verso l'obiettivo di ottimizzare e rendere proattive le operazioni di sicurezza, ma il 26% opera ancora in modo reattivo, con approcci ad hoc per le attività, la ricerca delle minacce e la risposta agli eventi.

64%
riceve un qualche tipo di assistenza nelle operazioni di sicurezza dai fornitori di servizi gestiti.

69%
utilizza una soluzione SIEM. Il 45% di chi non la possiede intende impiegare il SIEM entro i prossimi 12–18 mesi.

93%
La maggior parte delle aziende è inondata dagli allarmi e il 93% non riesce a eseguire il triage di tutte le minacce rilevanti.

65%
di quelle con un SOC svolgono operazioni formali di caccia alle minacce.

Le aree di crescita per il futuro. Migliorare la capacità di:

Risposta
agli attacchi confermati, tra cui coordinamento, remediation, eliminazione e prevenzione di nuove occorrenze.

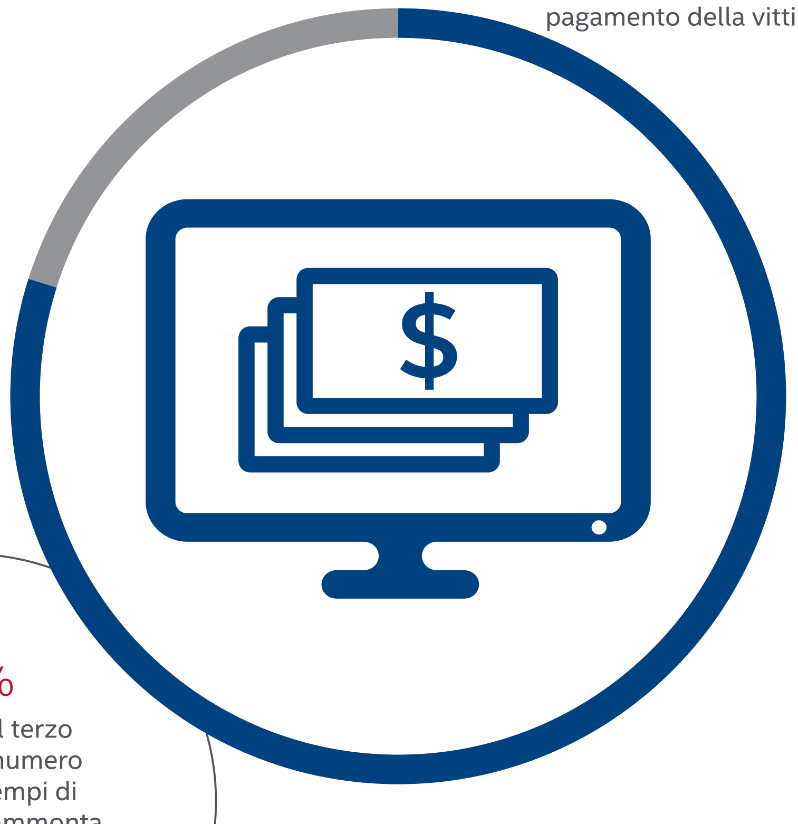
Rilevamento
dei segnali dei potenziali attacchi, fra cui il concentrarsi sui relativi eventi e allarmi, sul triage e sull'assegnazione delle priorità.

Indagine
sui potenziali attacchi, valutandone l'intera portata e l'impatto.

Un anno in ostaggio

Il 2016 ha visto un enorme incremento nel numero di attacchi ransomware nonché significativi progressi tecnici del ransomware. L'industria della sicurezza ha reagito.

Alcuni dei progressi tecnici più significativi del ransomware nel 2016 includono:



Crittografia del disco
Crittografia parziale e completa del disco.

Riscatto variabile
Le richieste variano in base alla capacità di pagamento della vittima.

Crittografia del sito web
Crittografia dei siti web utilizzata dalle applicazioni legittime.

Anti-sandboxing
Rilevamento e aggiramento delle sanbox di sicurezza utilizzate per testare il codice sospetto.

80%
Alla fine del terzo trimestre il numero di nuovi esempi di ransomware ammonta quest'anno a 3,9 milioni, con un aumento dell'80% dall'inizio dell'anno.

Il ransomware come servizio
Gli aggressori pagano i fornitori di servizi per l'utilizzo dell'infrastruttura e del ransomware.

Kit di exploit
Kit di exploit più sofisticati per la consegna del ransomware.

L'industria della sicurezza ha reagito.

Collaborazione

NO MORE RANSOM!

No More Ransom!
Fondata a luglio, quest'organizzazione fornisce consigli di prevenzione, assistenza nelle indagini e strumenti di decrittografia.

Le azioni delle forze dell'ordine

WildFire
Smantellamento del ransomware.

Shade
Smantellamento del ransomware.

Software legittimo infettato dai trojan

I trojan infettano il codice legittimo per poi nascondersi, al fine di passare inosservati il più a lungo possibile per massimizzare il rendimento.

I benefici dei trojan

Impressione di legittimità
I payload sono nascosti dietro marchi riconoscibili, contribuendo all'impressione di legittimità.

Offre copertura
Il software legittimo offre copertura durante le scansioni di icurezza e l'analisi forense.

Persistenza gratuita
Il software legittimo infettato dai trojan offre persistenza gratuita.

Modi per infettare il software legittimo con i trojan

Modifica
di codice interpretato, open source o decompilato.

Patch
di eseguibili al volo nel momento in cui vengono scaricati tramite attacchi man-in-the-middle.

Bundle
File puliti e infetti vengono riuniti utilizzando programmi binder o joiner.

Modifica degli eseguibili
utilizzando programmi patcher, mantenendo l'utilizzo dell'applicazione.

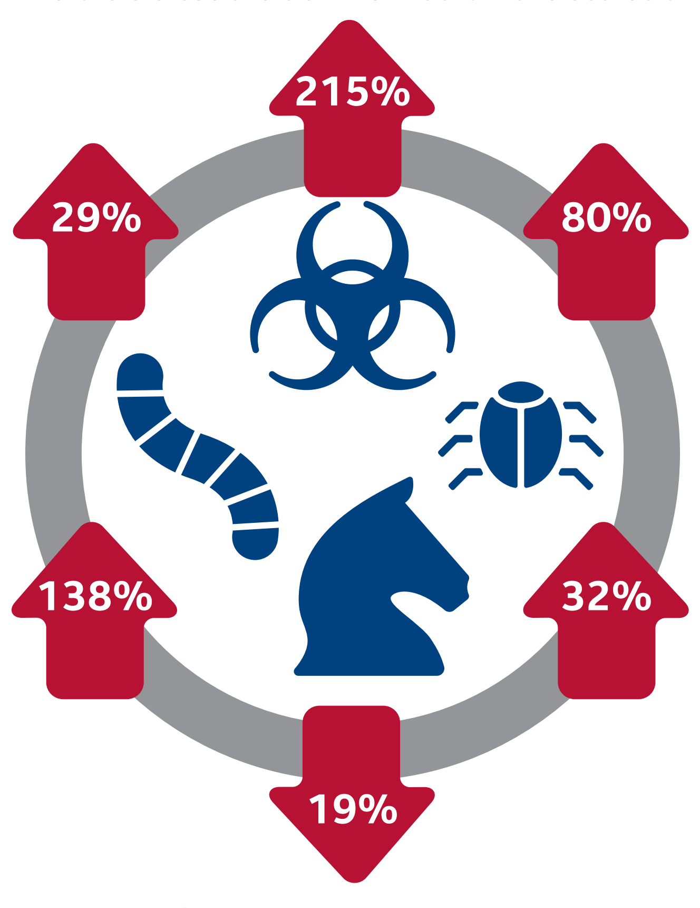
Corruzione
del codice sorgente principale, specialmente nelle librerie ridistribuite.

700.000
Nel corso del terzo trimestre, più di 700.000 codici binari infettati da trojan sono stati rilevati da tre famiglie di malware Android.

30.000
Nel corso del terzo trimestre, 30.000 codici binari Android sono stati infettati da trojan utilizzando due popolari kit di patching backdoor.

Statistiche sulle minacce

Emergono 245 nuove minacce ogni minuto, ovvero più di 4 ogni secondo.



Malware per il sistema operativo Mac
Anche se ancora contenuto rispetto alle minacce di Windows, il numero di nuovi esempi di malware per il sistema operativo Mac è cresciuto del 65% nel terzo trimestre. **Il malware per il sistema operativo Mac totale è cresciuto del 215% durante lo scorso anno.**

Malware
Il numero di nuovi esempi di malware nel terzo trimestre - 32 milioni - è sceso del 21% rispetto al secondo trimestre. **Tuttavia, lo scorso anno il conteggio complessivo è aumentato del 29% raggiungendo i 644 milioni di esempi**.

Ransomware
Il numero complessivo di esempi di ransomware nel 2016 è aumentato del 18% nel terzo trimestre e dell'80% ad oggi.

Malware mobile
Il numero di nuovi esempi di malware mobile - più di due milioni - nel terzo trimestre è il più alto mai registrato. **Il malware mobile totale è cresciuto del 138% durante lo scorso anno**.

Malware delle macro
Il nuovo malware delle macro continua a crescere a un ritmo elevato. **Il numero di malware delle macro totale è aumentato del 32% nell'ultimo trimestre**.

Botnet di spam
Le email di spam generate dalla botnet Kelihos sono diminuite del 97% nel terzo trimestre, ma la botnet Necurs è aumentata del 554%. **Complessivamente, le email spam provenienti da botnet sono diminuite del 19% nel terzo trimestre**.

McAfee Global Threat Intelligence

McAfee GTI ha ricevuto in media 44,1 miliardi di interrogazioni al giorno.

McAfee GTI

57 milioni
Le protezioni di McAfee GTI dagli URL pericolosi sono scese a 57 milioni al giorno nel terzo trimestre dai 100 milioni al giorno del secondo trimestre.

32 milioni
Le protezioni di McAfee GTI dai programmi potenzialmente indesiderati hanno mostrato un piccolo aumento nel terzo trimestre rispetto al secondo trimestre. Comunque c'è stata una drastica diminuzione nel terzo trimestre 2016 rispetto allo stesso periodo del 2015: **Nel terzo trimestre 2016 abbiamo rilevato 32 milioni al giorno rispetto ai 175 milioni al giorno nel terzo trimestre 2015**.

150 milioni
Le protezioni di McAfee GTI dai file pericolosi sono aumentate a 150 milioni al giorno nel terzo trimestre dai 104 milioni al giorno del secondo trimestre. Nello stesso periodo dello scorso anno abbiamo riscontrato un calo.

27 milioni
Le protezioni di McAfee GTI dagli indirizzi IP pericolosi hanno mostrato una lieve flessione a 27 milioni al giorno nel terzo trimestre dai 29 milioni al giorno del secondo trimestre. Si è trattato di una diminuzione molto più piccola di quella osservata dal secondo al terzo trimestre 2015.

Report McAfee Labs sulle minacce: dicembre 2016

Visita www.mcafee.com/December2016ThreatsReport per il report completo.

1941_1016_info_threats-report-dec-2016