Rapporto SonicWall 2019
sulle cyberminacce

Presentazione sintetica | Edizione europea

SonicWall.com

SONICWALL®
CAPTURE LABS

INTRODUZIONE: EDIZIONE EUROPEA

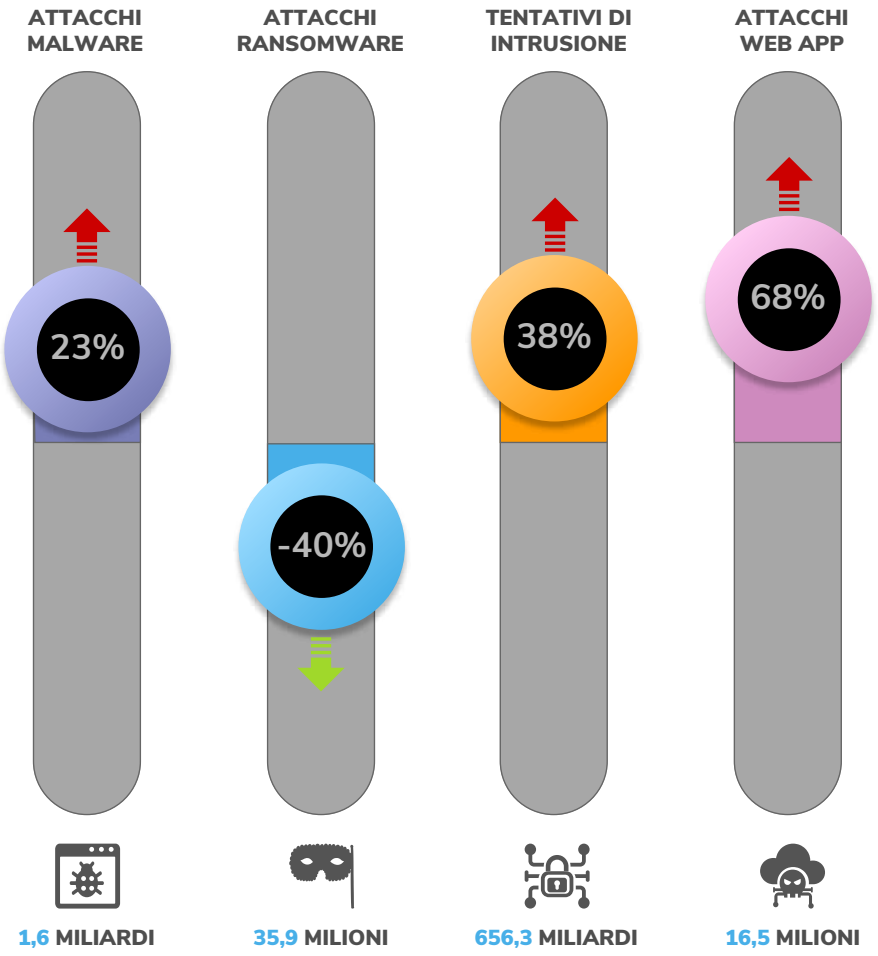
La corsa agli armamenti cibernetici non fa discriminazioni né differenze. Se una rete, un'identità, un dispositivo o dei dati sono preziosi - soprattutto le informazioni legate a proprietà intellettuale, prodotti finanziari, file sensibili, infrastrutture critiche o dati sull'elettorato -, i cibercriminali identificano, prendono di mira e attaccano senza pietà.

Per diffondere la conoscenza a livello globale e facilitare importanti scambi di opinioni SonicWall resta salda nell'impegno a ricercare, analizzare e condividere l'intelligence delle minacce attraverso il Rapporto SonicWall 2019 sulle cyberminacce. Questa presentazione sintetica, che va ad integrare la relazione approfondita, fornisce un punto di vista di alto livello sull'intelligence delle minacce dei ricercatori di SonicWall Capture Labs.

SONICWALL

PRINCIPALI RISULTATI PER IL 2018

TENDENZE DEI CIBERATTACCHI IN EUROPA NEL 2018



- Albania
- Andorra
- Austria
- Belgio
- Bielorussia
- Bosnia-Erzegovina
- Bulgaria
- Cipro
- Croazia
- Danimarca
- Estonia
- Finlandia
- Francia
- Germania
- Gibilterra
- Grecia
- Guernsey
- Irlanda
- Islanda
- Isola di Man
- Italia
- Jersey
- Lettonia
- Liechtenstein
- Lituania
- Lussemburgo
- Macedonia
- Malta
- Norvegia
- Paesi Bassi
- Polonia
- Portogallo
- Regno Unito
- Repubblica Ceca
- Romania
- Russia
- San Marino
- Serbia
- Slovacchia
- Slovenia
- Spagna
- Svezia
- Svizzera
- Ucraina
- Ungheria

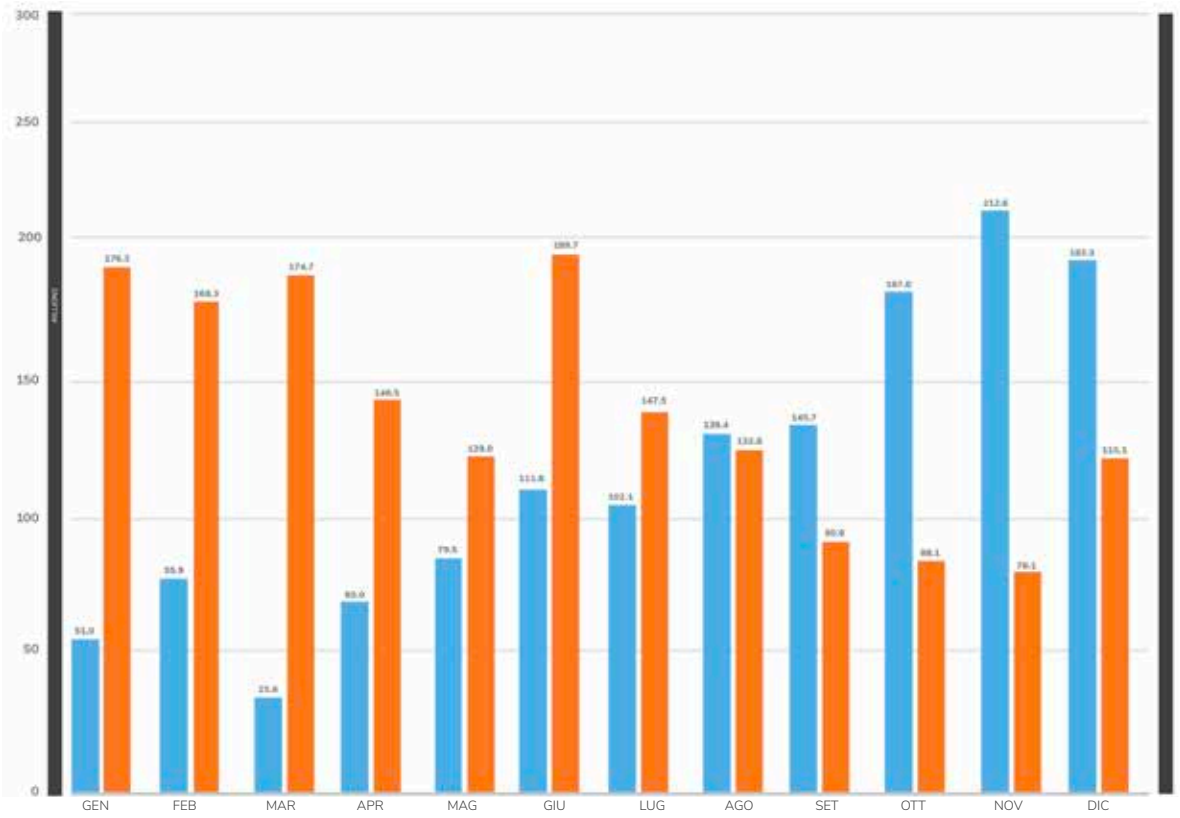
SONICWALL®

VOLUME DI MALWARE ANCORA IN CRESCITA

Nel 2016 si era registrato un calo del volume di malware, che aveva indotto qualcuno a ritenere che i cibercrimini nel complesso fossero in diminuzione. Da allora, **gli attacchi di malware sono aumentati del 33,4%.**

A livello globale SonicWall ha registrato 10,52 miliardi* di attacchi malware nel 2018, il maggior numero di sempre. In Europa SonicWall ha identificato **1.64 miliardi** di attacchi malware, con un aumento del 23% rispetto al 2017. Il dato più interessante è che, nonostante l'incremento nel 2018, a partire dal mese di Giugno il volume degli attacchi ha iniziato ad evidenziare una tendenza al ribasso.

VOLUME DI MALWARE - EUROPA 2018



* A livello di miglior prassi, SonicWall ottimizza di routine le sue metodologie di acquisizione, analisi e rendicontazione dei dati. Ciò si espleta anche attraverso miglioramenti al filtraggio dei dati, cambiamenti a livello delle fonti dei dati e consolidamento dei threat feeds. I dati pubblicati nelle relazioni precedenti possono essere stati adeguati per periodi, regioni e settori industriali diversi.

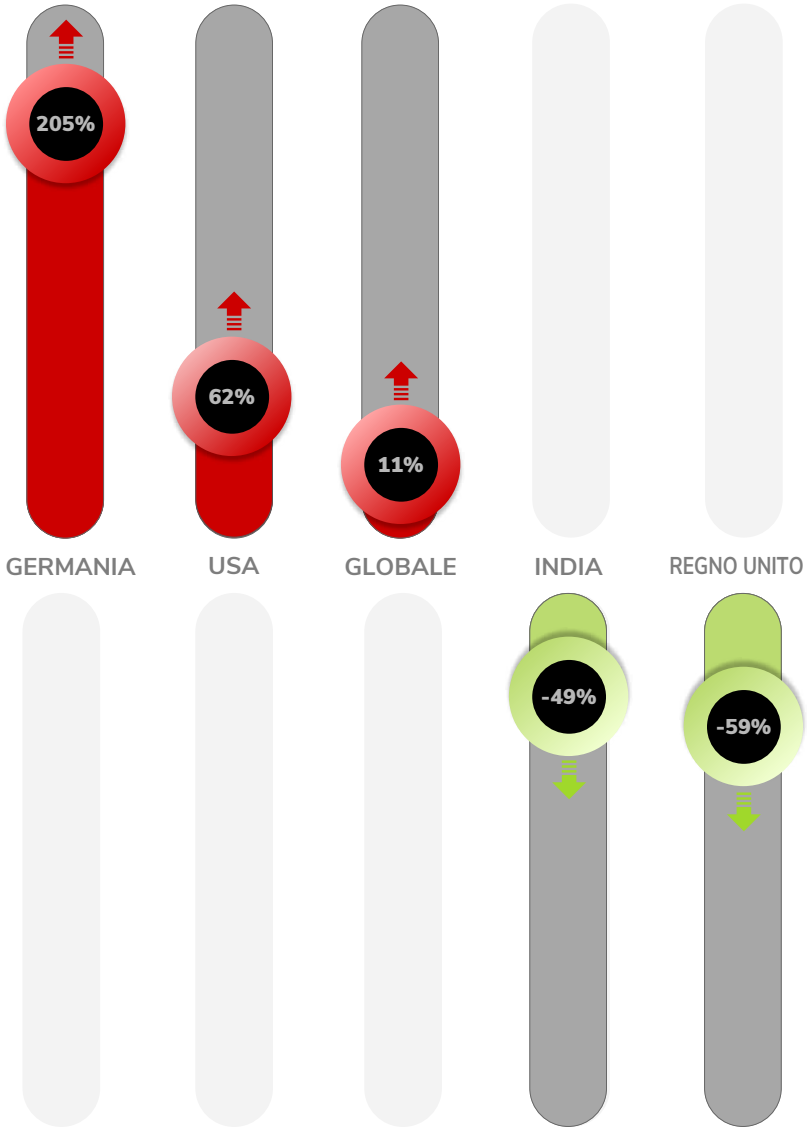
SONICWALL®

REGNO UNITO ED INDIA RESISTONO AL RANSOMWARE

Quando i ricercatori di SonicWall Capture Lab hanno finito di analizzare i dati sulle minacce del 2018, si è scoperto qualcosa di decisamente interessante. Il ransomware era cresciuto praticamente in tutte le regioni geografiche, tranne Regno Unito ed India.

Mentre i principali paesi in Nord America, Europa ed Asia avevano conosciuto un aumento degli attacchi ransomware, il **Regno Unito e l'India zitte zitte vantavano una riduzione rispettivamente del 59 e del 49%.**

A livello di paesi, **la Germania ha subìto il 27,6% di tutti gli attacchi europei di ransomware.** A seguire tra i paesi più bersagliati Italia (23%), Regno Unito (13,2%), Paesi Bassi (10,7%) e Francia (9,9%).



MINACCE PERICOLOSE PER LE MEMORIE, ATTACCHI A CANALE LATERALE IDENTIFICATI TEMPESTIVAMENTE

Real-Time Deep Memory Inspection (RTDMI™) mitiga anche i pericolosi attacchi a canale laterale utilizzando una tecnologia in attesa di brevetto. I canali laterali sono un veicolo fondamentale utilizzato per sfruttare la vulnerabilità dei processori ed esfiltrare i dati, come nel caso di Foreshadow, PortSmash, Meltdown, Spectre e Spoiler.

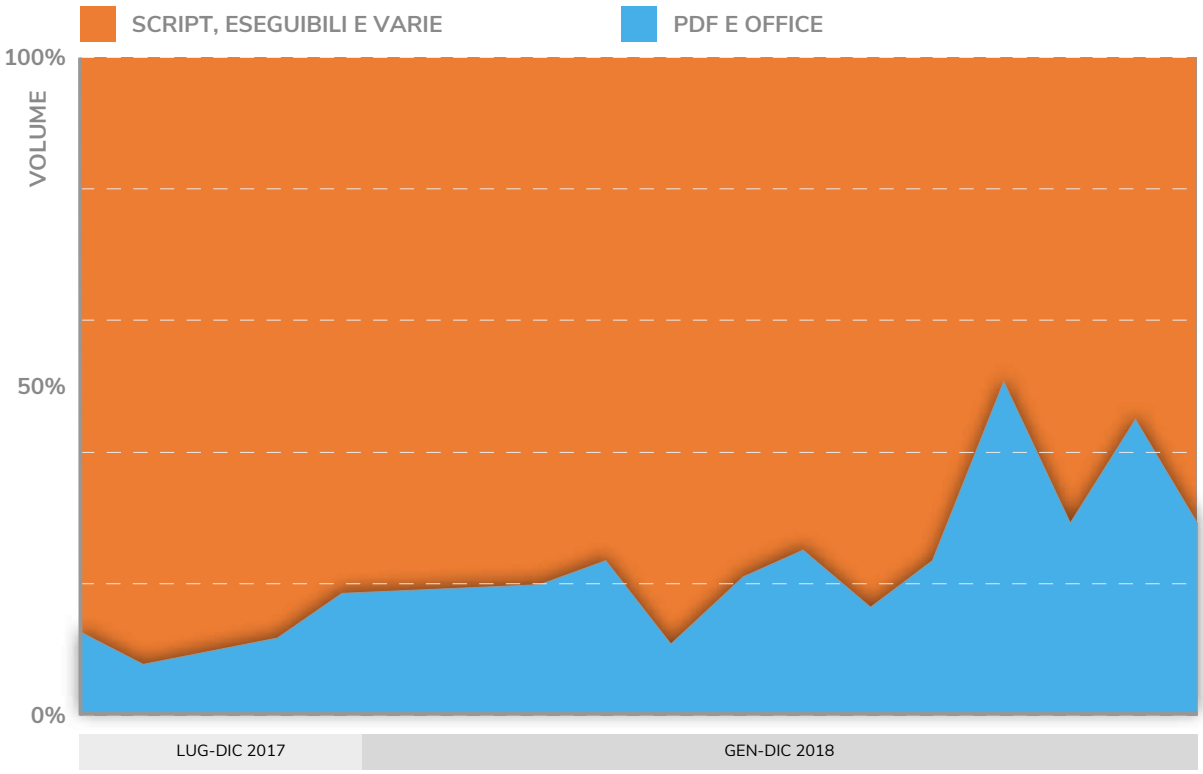
Purtroppo la ricerca attuale ammette che **'lo spettro durerà a lungo'** e riconosce che diverse vulnerabilità dei processori non possono essere sanate a livello di software né di hardware e che le stesse costituiscono un problema molto più grave per la sicurezza. In questo senso gli attacchi a canale laterale costituiranno un rischio costante nel panorama informatico, il che farà della tecnologia in grado di mitigare gli attacchi un requisito imprescindibile.

SONICWALL®

PDF E FILE OFFICE DANNOSI CHE SUPERANO I CONTROLLI DI SICUREZZA TRADIZIONALI

I cibercriminali manipolano file PDF e Office affidabili per aiutare i malware ad aggirare i firewall tradizionali e le sandbox single-engine.

AUMENTO DI PDF E FILE OFFICE DANNOSI



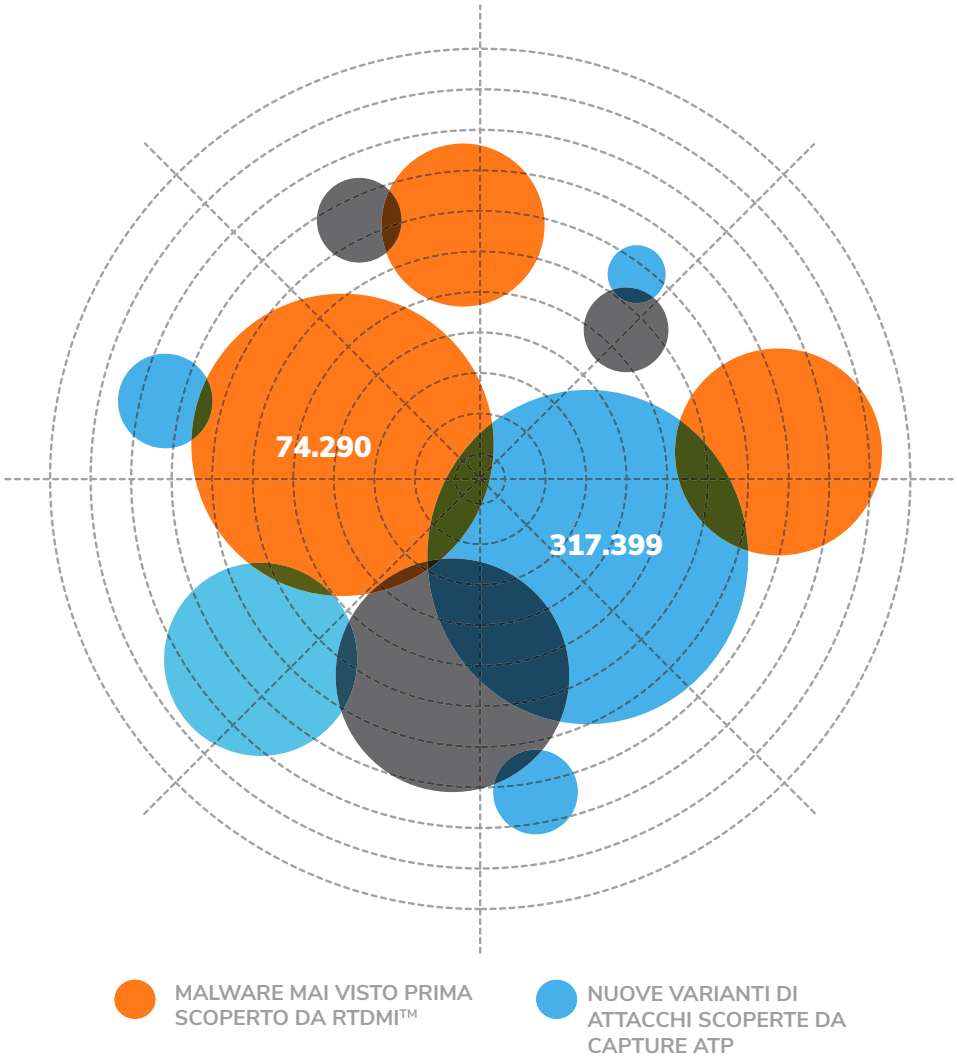
Nel 2018 il servizio sandbox single-engine Capture ATP di SonicWall ha scovato **malware nascosto in 47.073 file PDF e in 50.817 file Office**. Se a prima vista sembrerebbe trattarsi di un volume limitato, la maggior parte dei controlli di sicurezza non è in grado di identificare e mitigare il malware nascosto in questi file, il che fa aumentare decisamente il successo del payload.

L'APPRENDIMENTO AUTOMATICO STA FACENDO PROGRESSI PER BLOCCARE VARIANTI DI MALWARE SCONOSCIUTE

Nel 2018 SonicWall Capture Advanced Threat Protection (ATP) ha identificato 391.689 nuove varianti di attacchi, vale a dire, mediamente, più di **1072 nuovi attacchi scoperti e bloccati ogni giorno.**

Capture ATP utilizza una sandbox multi-engine in cloud in parallelo con la tecnologia di SonicWall in attesa di brevetto Real-Time Deep Memory Inspection™ (RTDMI). Entrambe le funzioni hanno beneficiato di un autoapprendimento e di un automiglioramento dinamici nel 2018.

Nello specifico, **RTDMI™ nel 2018 ha identificato 74.290 attacchi sconosciuti.** Si tratta di varianti di malware talmente nuove, uniche o complesse che nessuna azienda specializzata del settore è stata in grado di tracciare o crearne segnature quando SonicWall le ha scoperte.

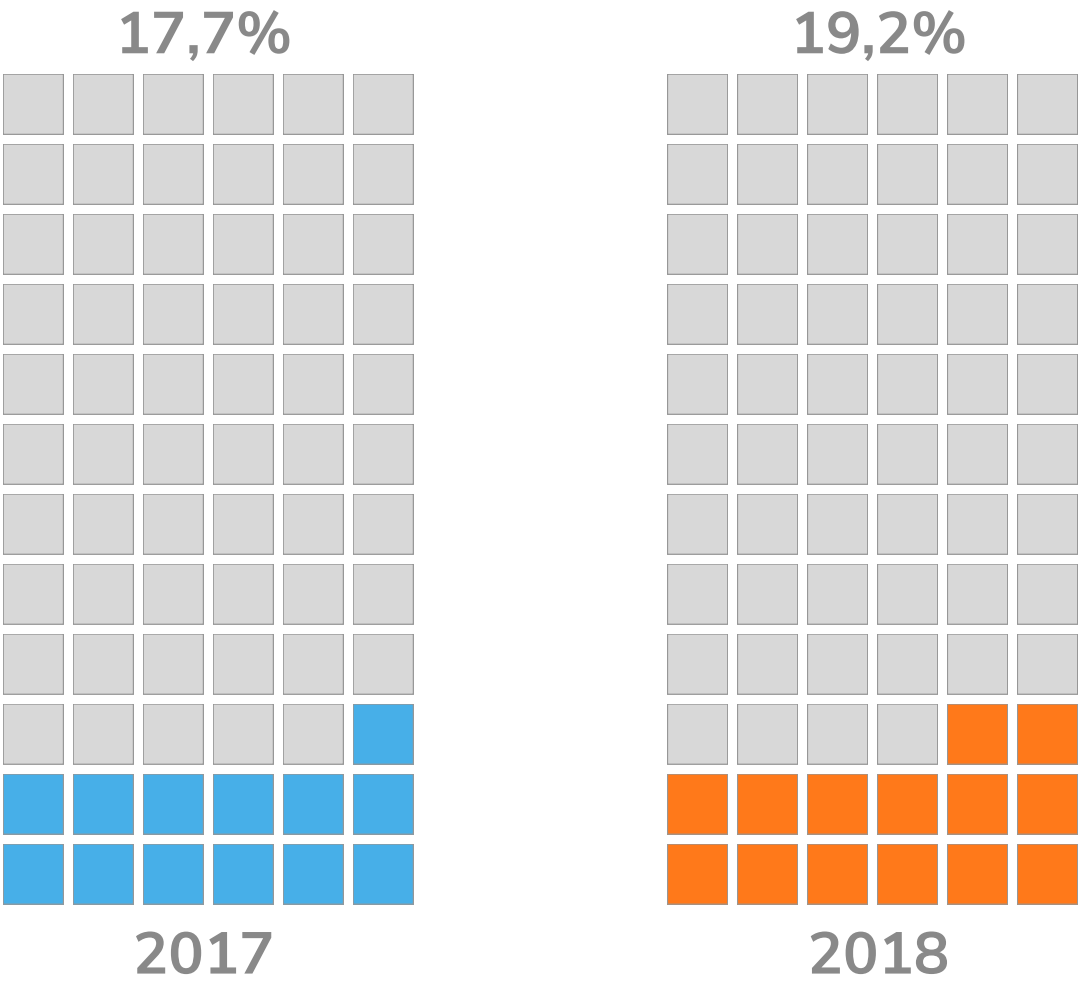


SONICWALL®

PORTE NON STANDARD SFRUTTABILI PER GLI ATTACCHI

Le porte 80 e 443 sono porte standard per il traffico web, per cui sono quelle sulle quali la maggior parte dei firewall concentra la protezione. In risposta, i cibercriminali prendono di mira le porte non standard per far sì che il loro payload possa diffondersi indisturbato nell'ambiente di destinazione.

ATTACCHI MALWARE 2018
A PORTE NON STANDARD



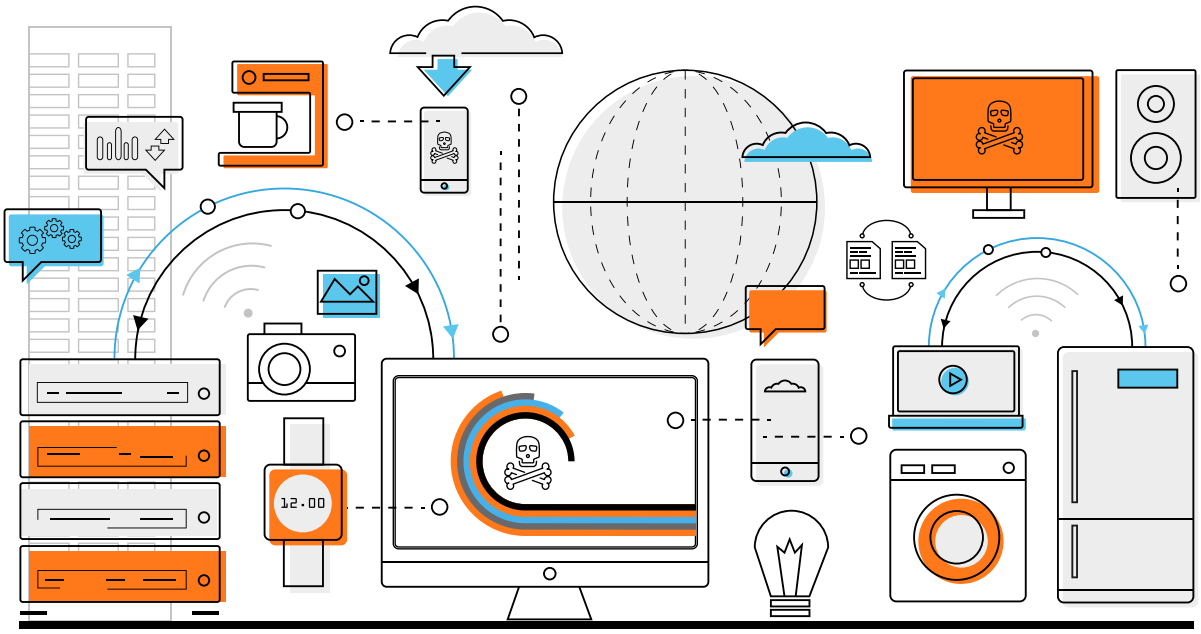
Sulla base di un campionamento di oltre 700 milioni di attacchi malware, SonicWall ha riscontrato che il **19,2% di tutti gli attacchi malware è passato attraverso porte non standard** nel 2018. Poiché le porte non standard da monitorare sono troppe, i firewall tradizionali basati su proxy non sono in grado di mitigare gli attacchi (sia per il traffico crittografato, sia per quello non crittografato).

SONICWALL®

CRESCITA DEGLI ATTACCHI IoT

I consumatori sono sempre più attratti dai dispositivi connessi. Ma questa tendenza ha comportato un aumento incredibile di dispositivi compatibili con l'Internet delle cose (IOT), che si sono riversati sul mercato privi dei regolari controlli di sicurezza. In molti casi i dispositivi IoT sono impostati su configurazioni di sicurezza di default, che li rendono facilmente compromettibili attraverso credenziali note o botnet potenti.

Con queste premesse, SonicWall ha registrato **32,7 milioni di attacchi IoT nel 2018,** con un incremento del 217,5% rispetto ai 10,3 milioni registrati nel 2017.



CRESCITA COSTANTE DEGLI ATTACCHI CRITTOGRAFATI

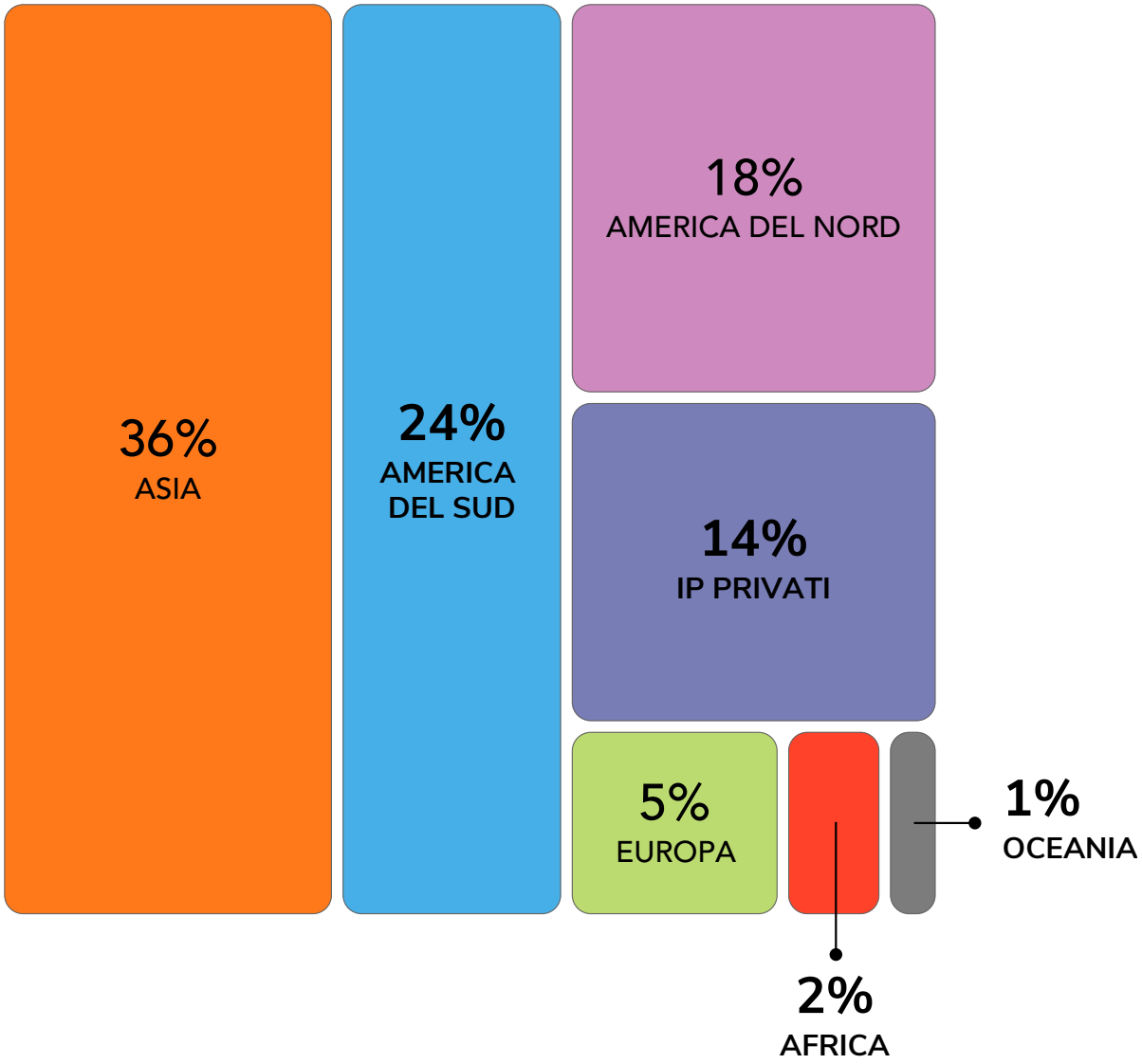
La crescita del traffico crittografato coincide con un maggior numero di attacchi nascosti con crittografia TLS/SSL. Più di **2,8 milioni sono stati gli attacchi crittografati** nel 2018, con un incremento del 27% rispetto al 2017.

ALTI E BASSI DEL CRIPTOJACKING

Ne 2018 il criptojacking è sparito con la stessa rapidità con cui era apparso. SonicWall ha registrato globalmente **57,5 milioni di attacchi di criptojacking** tra aprile e dicembre. Il picco del volume degli attacchi si è avuto a settembre, con 13,1 milioni di attacchi registrati, per poi calare costantemente.

Stando ai dati SonicWall, l'Europa da sola si è trovata a dover affrontare il 5% di tutti gli attacchi globali di criptojacking nel 2018. Nonostante il calo dei prezzi, le criptovalute restano un bene prezioso per i cibercriminali per via dell'anonimato.

CRIPTOJACKING PER REGIONE 2018



VOLUME GLOBALE DI PHISHING IN CALO, CON ATTACCHI PIÙ MIRATI

ATTACCHI DI PHISHING
A LIVELLO MONDIALE **26 MILIONI**

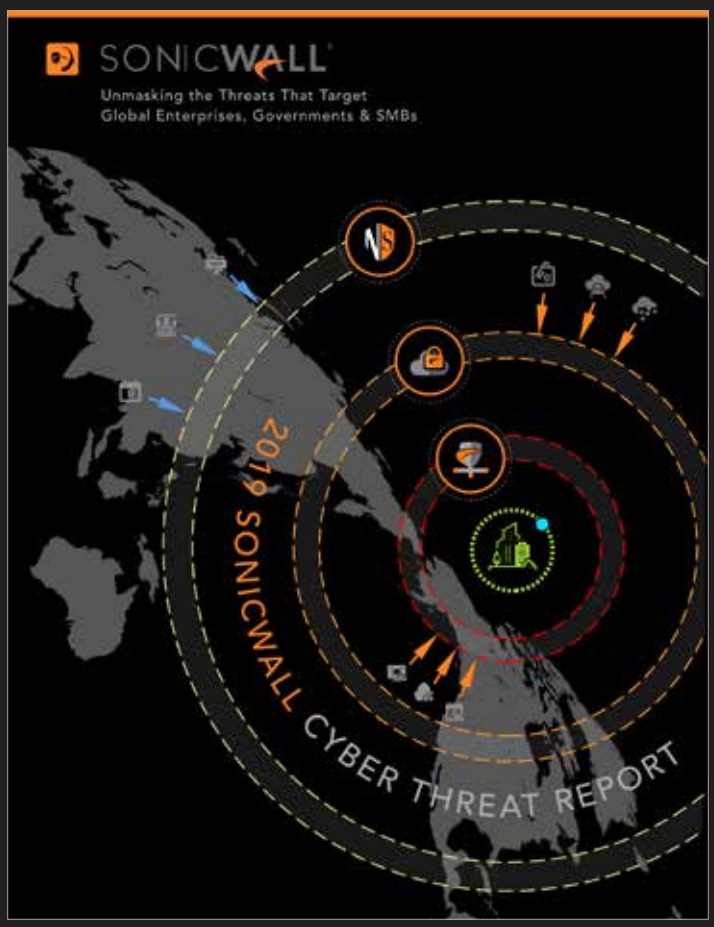
Dato che le imprese stanno diventando sempre più capaci di bloccare gli attacchi via email, mettendo i dipendenti in grado di individuare e cancellare i messaggi sospetti, i cibercriminali stanno cambiando tattica. Cala il numero complessivo, ma gli attacchi di phishing lanciati sono più mirati (ad esempio, compromissione della posta elettronica aziendale, sottrazione di account, whale phishing etc.).

Nel 2018 SonicWall ha registrato **26 milioni di attacchi di phishing a livello mondiale,** con un calo del 4,1% rispetto al 2017. Il cliente medio SonicWall si è trovato a dover affrontare 5488 attacchi di phishing nel 2018.

SONICWALL®

Intelligence e analisi esclusive delle cyberminacce. Solo da SonicWall Capture Labs.

ULTERIORI INFORMAZIONI



Visiti SonicWall.com/ThreatReport per scaricare il Rapporto SonicWall 2019 sulle cyberminacce. Apprenderà nuove prospettive sulle strategie degli attacchi cibercriminali e capirà come difendere efficacemente la Sua organizzazione o impresa dai ciberattacchi più sofisticati.

* A livello di miglior prassi, SonicWall ottimizza di routine le sue metodologie di acquisizione, analisi e rendicontazione dei dati. Ciò si espleta anche attraverso miglioramenti al filtraggio dei dati, cambiamenti a livello delle fonti dei dati e consolidamento dei threat feeds. I dati pubblicati nelle relazioni precedenti possono essere stati adeguati per periodi, regioni e settori industriali diversi.

SONICWALL