Kaspersky APT Intelligence Reporting

kaspersky BRING ON THE FUTURE

Kaspersky APT Intelligence Reporting

Grazie agli APT Intelligence Reporting i clienti Kaspersky potranno usufruire dell'accesso costante ed esclusivo alle analisi e ai rilevamenti, inclusi i dati tecnici completi (in un'ampia gamma di formati) su ogni attacco APT rilevato, nonché sulle minacce che non verranno mai rese pubbliche. I report contengono una sintesi di informazioni immediate e rilevanti che illustrano l'APT oltre a offrire una descrizione tecnica dettagliata dell'APT con le relative regole YARA e IOC, offrendo ai ricercatori di sicurezza, agli analisti malware, ai security engineer, agli analisti di sicurezza di rete e ai ricercatori APT, dati applicabili che consentono una risposta accurata e veloce alle minacce.

I nostri esperti avvisano immediatamente di eventuali modifiche rilevate nelle tattiche dei gruppi di criminali informatici e sarà inoltre garantito l'accesso al database completo dei report APT, un altro potente strumento di analisi e ricerca in ambito di difese di sicurezza.

Vantaggi

MITRE ATT&CK

Tutte le TTP descritte nei report risultano mappate in MITRE ATT&CK: ciò consente la conduzione di attività di rilevamento e risposta ancor più efficaci, grazie allo sviluppo dei relativi use case in termini di monitoraggio della sicurezza, con assegnazione delle indispensabili priorità. La specifica metodologia consente inoltre di effettuare accurate analisi delle eventuali lacune di sicurezza e di testare le attuali difese informatiche in relazione a determinate TTP

Informazioni sugli APT non pubblici

Per diversi motivi, non tutte le minacce di alto profilo vengono rese note pubblicamente, ma vengono condivise con i nostri clienti

Accesso privilegiato

Ricezione di descrizioni tecniche sulle minacce più recenti durante le indagini in corso, prima del rilascio al pubblico

Analisi retrospettiva

Durante il periodo di validità dell'abbonamento, è disponibile l'accesso all'archivio dei report privati

Accesso ai dati tecnici

È incluso un ampio elenco di IoC, disponibile in formati standard quali OpenIOC o STIX, e l'accesso alle regole YARA

Profili degli autori delle minacce

Sono inclusi il presunto paese di origine e l'attività principale, le famiglie di malware utilizzate, i settori e le aree geografiche colpite e le descrizioni di tutte le TTP utilizzate, con mappatura nel framework MITRE ATT&CK

Monitoraggio continuo delle campagne APT

Accesso all'intelligence applicabile durante le indagini con informazioni sulla distribuzione APT, IOC, infrastrutture di controllo e comando e così via

Restful API

Automatizzazione e integrazione immediate con i flussi di lavoro di sicurezza esistenti

www.kaspersky.it