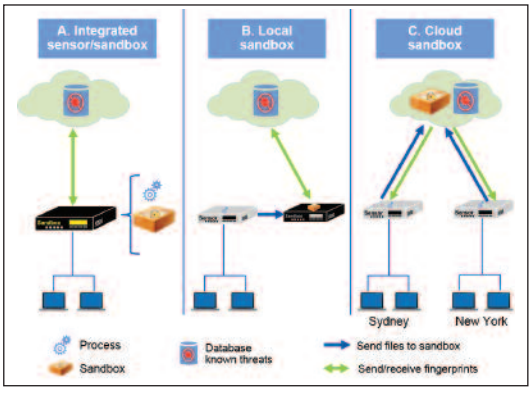
Sandblast: il sandboxing 2.0 secondo Check Point

La nuova frontiera della simulazione di postazioni per prevenirne il detection da parte dei malware

È un dato di fatto: qualsiasi vendor di network security include ormai nella sua offerta un sistema per trovare malware che sfruttano vulnerabilità non ancora conosciute (zero-day vulnerabiliy) per attaccare postazioni di lavoro. Il sistema di protezione si basa principalmente sul principio di sandbox, macchine virtuali che simulano i pc degli utenti per rilevare eventuali comportamenti anomali una volta aperto il file o eseguito il programma.

Presenti sul cloud oppure on-premise presso i datacenter, e con tecnologie di detecting molto differenti tra loro, che rendono quindi più o meno efficace il risultato, le sandbox rappresentano comunque un metodo più che valido per la detection di questo tipo di malware.

Ora però iniziano a non essere più così efficaci, soprattutto perché, come accade sempre nel mondo della security, sono state sviluppate tecniche sempre più sofisticate per evadere questo tipo di detection, come per esempio controllare se esiste il movimento di un mouse, oppure inserire degli sleep time che attivano il malware vero e proprio solo dopo minuti (talvolta ore) dopo l'apertura del file. Queste sono solo alcune delle più semplici tecniche, che comunque rendono la maggior parte delle sandbox inefficaci, e quindi necessitano di un metodo più avanzato di detection.



In quest'ottica, Check Point ha introdotto un'evoluzione del loro sistema di sandboxing, denominata "SandBlast", che non si limita più al semplice controllo del comportamento di un file a livello di emulazione, bensì analizza le operazioni svolte dal file direttamente a livello CPU, analizzando il flusso di istruzioni sul processore e accorgendosi quindi se vengono eseguite operazioni di evasion.

Questa nuova visione del sandboxing, unita all'ormai collaudata tecnologia di Threat Extraction, rende ancora più efficace la detection di malware sulle piattaforme Check Point, qualsiasi sia la loro complessità ma soprattutto la loro capacità di evadere dai controlli tradizionali.

Per questa ragione, Il nuovo bundle "Next Generation Threat Extraction" (NGTX) si unisce ai già esistenti "Next Generation Firewall" (NGFW) e "Next Generation Threat Prevention" (NGTP) per consentire lo sfruttamento di tutte le potenzialità messe a disposizione dalla tecnologia Check Point, mandando definitivamente in pensione il firewall "Classico".

Ulteriori informazioni:
https://www.checkpoint.com/resources/expose-the-unknown/. ■

Marco Coppolino

THINK YOU ARE SECURE? THINK AGAIN.

If asked whether you are secure, what would be your answer? Today having a security infrastructure is not good enough; having the BEST SECURITY is critical. A security that prevents zero-day threats, protects your data and mitigates attacks. A security that provides the best threat catch rate, in the fastest time. A security that secures your data anywhere it goes.

That BEST SECURITY is Check Point's.

Check Point®
SOFTWARE TECHNOLOGIES, INC.
WE SECURE THE FUTURE

CONSYS.IT
dal 1994 Innovativi per Tradizione