tech
FromTheNet

Achab spiega come difendersi dai pericolosi CryptoVirus

Nel corso del mese di dicembre, **Achab** ha tenuto un interessante webinar in materia di **security** e in particolare sulle modalità di attacco e di difesa contro i cosiddetti **CryptoVirus**.
A illustrare tecnologie, best practice e le modalità operative di questo tipo di malware sono intervenuti **Claudio Panerai, CTO Achab e Alessio Urban, Tech Support Manager Achab.**
L'obiettivo di questo momento formativo è stato quello di **ampliare il più possibile la conoscenza degli utenti in merito a questo tipo di fenomeni, purtroppo sempre più diffusi.** In questo senso, il 2016 vedrà una forte recrudescenza per quanto riguarda la proliferazione di ransomware, come sottolineano la maggior parte degli esperti di tecnologia. La **sicurezza del dato e della privacy è dunque cruciale** ma, spesso, **utenti e aziende non sono preparati contro questo tipo di minacce** e non sono in grado di difendersi in modo autonomo. Questo perché si tratta frequentemente di attacchi mascherati e perciò in grado di sfuggire ai comuni antivirus e ai controlli operati a livello di sistema operativo.

Nel mirino dei virus che cifrano i dati finiscono, indistintamente, **privati, PMI e multinazionali.** I risultati di un attacco di questo tipo possono essere estremamente gravi e possono mettere in ginocchio aziende e studi professionali, non attrezzati con adeguati strumenti di backup e disaster recovery.
Per supportare utenti privati e professionisti, gli esperti Achab hanno evidenziato quali processi devono essere messi in atto per arginare questo genere di attacchi, oltre alle best practice più efficaci.
In particolare si è parlato delle modalità con le quali questi malware sono in grado di "bucare" gli antivirus convenzionali e delle configurazioni di sistema da adottare per prevenire le infezioni. Non solo, sono state evidenziate le policy e i permessi da definire per arginare la diffusione di virus sconosciuti.

Durante il webinar si è scelto di percorrere brevemente la storia dei virus, dai primi anni '80 ad oggi, un interessante passaggio che aiuta a comprendere la filosofia che si cela in ogni tipo di attacco. **Si passa dunque dai primi virus in grado di avviarsi e replicarsi automaticamente, ai virus polimorfi degli anni '90 che, già più di vent'anni fa erano in grado di eseguire la cifratura del disco, in maniera analoga a quanto accade oggi con i CryptoVirus.** L'ampia diffusione delle email apre la via per numerose varianti, in grado di infettare immediatamente il sistema operativo, sfruttando bug e falle di programmazione degli ambienti lavorativi e domestici. Le evoluzioni più recenti sono state ulteriormente potenziate e mirato al furto di identità, ai dati sensibili degli utenti e ai conti bancari.

Malware come Cryptowall e CTB Locker sono in circolazione dal settembre 2013, sono classificati come Trojan Horse di tipo ransomware e sono in grado di criptare dischi locali, di rete e rimovibili in ambiente Windows. Il metodo di intrusione adottato per "entrare" nel PC degli utenti include la diffusione tramite email di spam o phishing con allegati specifici.
La diffusione avviene dunque tramite allegati email, oppure navigando su siti "sospetti" (porno/video streaming/dowload illegale) o su siti ufficiali ma "hackerati" e, perciò, compromessi.
Altri pericoli possono arrivare da alcuni plugin per i web browser, dai software free o non ufficiali e, in generale, usando sistemi non aggiornati.
Questo porta solitamente al **download di codice maligno ed exploit kits**. I file con estensioni più comuni (DOC, XLS, PDF, JPG, per esempio) vengono così **cifrati adottando la piattaforma RSA 2048 con chiave pubblica asimmetrica. Per sbloccare i file compromessi agli utenti viene richiesto il pagamento di un riscatto (da qui il nome ransomware), solitamente di qualche centinaio di Dollari, pagabile tramite Bitcoin e Moneypack.**
Adottando dunque un network che include un Command and Control Server virato, i cybercriminali sono in grado di far circolare il codice maligno, detenendo la chiave privata indispensabile per decifrare nuovamente i file.
Per l'anno 2015, Achab ha rilevato oltre 4.546 tipi di malware, 1.213 Server di controllo C&C, per un flusso di informazioni che include 56 Paesi.

Citando Symantec, Achab sottolinea come **i convenzionali antivirus basati su firme siano a tutti gli effetti inefficaci contro i CryptoVirus**. Ad oggi, servono sistemi **attivi e proattivi,** in grado di reagire autonomamente alle sollecitazioni provenienti dal web. Il ciclo "virus – firme – rilascio patch" è troppo lento e inadeguato, richiede molti campioni per l'aggiornamento e non è consente al software di protezione di rimanere al passo con attacchi exploit sempre più sofisticati e intelligenti.
Gli attacchi moderni sfuggono agli antivirus perché mettono in atto azioni diverse in base a location, sono in grado di mantenersi in stasi fino al verificarsi di un determinato evento e attivano componenti in modalità casuale.

Non solo, le mutazioni più recenti si "adattano" all'antivirus e sono capaci di avviare attività di hijack di processi regolari, in modo totalmente trasparente all'antivirus.
Su queste basi, nel tempo, sono stati disegnati **virus capaci di lavorare senza un'impronta sul disco fisso, totalmente in RAM, o di infettare direttamente il file system, agendo direttamente attraverso le chiamate di Windows.**
I "Fileless virus", in aggiunta, adottano un legittimo file di Windows, inserendo stringhe nel file di registro ed eseguendo una versione zombie di
dllhost.exe e un portable powershell. **Ciò rende l'attacco totalmente invisibile all'antivirus dato che l'esecuzione stessa non avviene a partire da un file ma da un processo avviato automaticamente attraverso il registry.**
Detto questo è possibile affermare che i moderni CryptoVirus sono tra i più complessi mai creati, data la natura variabile e polimorfica. Se, a questo, aggiungiamo il fatto che gli antivirus attuali non sono strutturati per questo tipo di minacce, il rischio di contagio e diffusione è davvero molto alto.

Come proteggersi al meglio?

Achab suggerisce pochi e semplici passaggi, che vanno a formare un insieme di regole da applicare sui sistemi di casa e di lavoro. Oltre a un **antivirus solido** è opportuno garantirsi il **costante aggiornamento e l'applicazione di patch per il sistema operativo e per tutti i programmi e le utility che utilizziamo. Anche il web browser deve essere aggiornato e, possibilmente, munito di ad-blocker, in grado di effettuare una prima scrematura dei contenuti.**

Per quanto riguarda le email, vettore preferenziale per questo genere di attacchi, **è opportuno imporre filtri capaci di bloccare la ricezione di messaggi sospetti (bloccare SCR, EXE, COM e VBS).** A livello di ambiente operativo è bene applicare policy per gli utenti, **in modo che accedano alle macchine come standard user, anziché come administrator. La limitazione delle permission consente infatti di limitare lo spazio d'azione delle possibili minacce.**

Il backup ricopre un ruolo fondamentale ed è perciò importante **irrobustire le policy di salvataggio di dati, in ottica di disaster recovery di macchine e ambienti.**
Per evitare che anche i percorsi di rete e i NAS aziendali vengano compromessi, Achab suggerisce di abilitare cartelle accessibili a un solo utente, effettuando successivamente il backup con privilegi di amministratore di rete. In questo modo eventuali virus non saranno in grado di cifrare il contenuto dei backup.
In generale, le policy di gestione sono fondamentali, è necessario bloccare l'esecuzione nella cartelle "temp", "appdata" e la creazione di entry nella "startup".
Achab suggerisce di bloccare l'accesso a Volume Shadow Copy Service (VSS) e di disabilitare Windows Script Host, per bloccare script VBS. Un aiuto può arrivare anche dal versatile Cryptoprevent, disponibile anche in **modalità portable e command line per RMM tools e studiato proprio per prevenire l'intrusione di codice che possa facilitare l'esecuzione dei CryptoVirus.**