SIGEMI
Cloud Managed Platforms

RANSOMWARE

Cosa sono, come agiscono e come si sono evoluti negli ultimi anni

INDICE DEI CONTENUTI

RansomWare: nel nome troviamo la loro vocazione e cioè il riscatto (ransom).

Questa famiglia di software malevoli (malware) sono pensanti per “rapire” i nostri dati, rendendoli inutilizzabili (cifrati), sino al pagamento di un riscatto a fronte della promessa di ridare l’accesso, tramite una chiave di decifratura.

Questo comportamento gli è avvalso il secondo nome di **Crypto-Locker.**

Negli ultimi anni, come tutti i criminali anche questi rapitori si sono evoluti per adattarsi alle strategie di difesa impiegate e raggiungere obbiettivi profittabilità e controllo.

Al costo di circa 1.100€ si può mettere nel carrello un cripto-locker con tanto di personalizzazioni (chiave personale per cifratura dei dati, messaggio di riscatto, ecc).

Email: commerciale@sigemi.it
Tel. 02.982.893.50 | www.sigemi.it

L’Evoluzione della specie

La mente e gli esecutori

In passato il gruppo che aveva preparato il crypto-locker era anche quello che si occupava di diffonderlo e ricevere il riscatto, richiedendo un livello tecnico medio/alto per preparare o variare questi software malevoli. Ora i ransomware sono in vendita nel dark-web, su siti di commercio elettronico, come un servizio a costo molto contenuto con tanto di offerte special-price!

In questo modo l’ideatore del piano di rapimento (lo sviluppatore) corre meno rischi, gli esecutori materiali del crimine sono cresciuti esponenzialmente e sono apparse centinaia di varianti dello stesso ransomware che sfruttano le stesse funzionalità ma che raggiungono i nostri dati grazie a email preparate da malintenzionati locali. Le email trappola che riceviamo sono sempre più ben fatte e contestualizzate, rendendole più ingannevoli e difficili da riconoscere da software antispam e antivirus. (Non ci sono più email con errori ortografici o di contenuto che consentivano con un minimo di attenzione, di riconoscerle come pericolose)

Colpo grosso e micro-ricatti

Come per la criminalità organizzata i ransomware si sono diversificati. Gli attacchi a pioggia via mail inviati al maggior numero di utenti sono stati affiancati da attacchi mirati e silenti verso specifici settori come Sanità (Ospedali, Assicurazioni, …) e enti amministrativi locali (comuni, dipartimenti ministeriali). La fluttuazione delle criptovalute come BitCoin e la volontà di aumentare il numero di riscatti pagati ha portato i criminali ad abbassare prezzi e inviare effettivamente le chiavi di accesso ai dati cifrati. Questa strategia è mirata a spostare la decisione se pagare o meno su un piano economico di costi/benifici come se fosse un qualsiasi intervento riparazione di un componente rotto.

Oltre il danno la beffa

In passato i ransomware si “limitavano” a rendere inaccessibili i dati su computer e server e richiedere un riscatto, negli ultimi anni questo comportamento si è evoluto inserendo come prima operazione malevola la copia dei dati, successivamente la cifratura dei dati utente ed infine il danneggiamento delle componenti dei sistemi.

L’Evoluzione della specie

I criminali ora hanno 3 paure sui cui far leva per ottenere il pagamento del riscatto

La paura di perdere i dati

La minaccia si è evoluta cercando di ridurre il tempo per decidere se pagare. (Se non paghi entro 96 ore non rivedrai mai più i dati. Se paghi entro 36 ore avrai un costo ridotto)

Disponibilità di servizi

L’indisponibilità di servizi critici per l’azienda (non solo i documenti sono bloccati ma anche i sistemi stessi (invio mail, siti web, applicazioni, …). I tempi (RTO Restore Time Object) e la capacità di ripristino di tutti servizi oltre ai dati costituiscono un altro costo significativo. Alcune realtà hanno accettato di pagare il riscatto non essendo in grado di ripristinare servizi e informazioni vitali per l’azienda e la comunità. (Sistemi di controlli di infrastrutture elettriche, Ospedali, …)

Perdita di confidenzialità

Oltre a non dare accesso ai nostri dati, se non viene pagato il riscatto nei tempi dettati, i dati saranno resi pubblici. I tal modo anche aziende pronte a reagire ripristinando dati e i servizi, corrono il rischio che informazioni aziendali e personali siano divulgate con tutti le problematiche legali e d’immagine. (foto, email, proprietà intellettuali, …)

Email: commerciale@sigemi.it
Tel. 02.982.893.50 | www.sigemi.it

I “magnifici” 7

WANNACRY

Apparso a Maggio 2017 con un attacco indiscriminato in tutto il mondo (150 nazioni) ha infettato in pochi giorni 200 mila computer. E’ stato fermato grazie ad un interruttore d’emergenza lasciato nel codice del ransomware (killswitch). WannaCry è stato il primo a sfruttare la debolezza dei sistemi windows non aggiornati, che consentiva il propagarsi su altri computer attraverso la rete informatica (SMB Protocol EternalBlue exploit – debolezza risolta da un aggiornamento disponibile dal 2008). La modalità diffusione e infezione iniziale avviene attraverso mail fraudolente.

PETYA

Identificato nel 2016 (da CheckPoint) si è evoluto nel 2017 in diverse varianti identificate come la famiglia dei NotPetya, sfruttando suggerimenti provenienti da WannaCry, anche questi ransomware sfruttano debolezza del protocollo di rete dei sistemi windows (SMB Protocol EternalBlue exploit). A giugno 2017 vi è stato un picco di infezioni in molte nazioni tra cui Francia, Germania, Italia e Regno Unito, Polonia, Stati Uniti, Ukraina e Russia. La modalità diffusione e infezione avviene attraverso mail fraudolente.

SAMSAM

Apparso a fine 2015 ha rapito con successo dati di enti governativi e sanitari (Colorado Department of Transportation, the City of Atlanta). Questo malware sfruttava debolezze di sistemi operativi non aggiornati (IIS – WebServer. FTP Scambio File, RDP Accesso Remoto).

RYUK

Identificato nel 2018-2019 negli Stati Uniti ha colpito piccole e medie aziende con bassi livelli sicurezza, ma anche giornali (Los Angeles Times) e enti di gestioni di pubblici servizi (North Carolina water utility). Questo Crypto-Locker è stato uno dei primi a disabilitare sistemi di protezione locale dei dati (Windows Restore Point), prima di cifrare i dati.

I “magnifici” 7

PURELOCKER

Identificato nel 2019, da IBM e Intezer, è una variante di ransomware pensato per attaccare le aziende, cercando di rivendere l’accesso e i dati ad altre aziende piuttosto che richiedere un riscatto. Questo ransomware, uno dei primi pensato per server Windows e Linux, si installa su computer già compromessi, cercando di diffondersi su altri computer, cerca server e dati e rimane in attesa istruzioni.

ZEPPELIN

Identificato a fine 2019, è l‘evoluzione “As a Service” di altri ransomware (Vega o VegasLocker), progettato per essere configurabile senza conoscenze di sviluppo; comportando la creazione di innumerevoli varianti con strategie di penetrazione diversificate (.exe, .dll, poweshell). Questo Crypto-Locker prende di mira aziende tecnologiche e sanitarie in particolare nei continenti europeo e nord americano. Si ipotizza che anche i fornitori di servizi di sicurezza siano stati colpiti e a sua volta abbiano costituito fonte di attacchi.

REVIL/SODINOKIBI

Identificato a meta 2019, è l’evoluzione di altri ransonware (GandCrab) progettato per attaccare specifiche componenti aziendali, contiene istruzione specifiche per non attaccare computer di alcune nazioni (Russia, Iran). Uno dei primi a minacciare espressamente la divulgazione dei dati al miglior offerente (“Non recupererai i tuoi dati se non paghi il riscatto”, ma inoltre, “Pubblicheremo tali dati riservati sul Web o li venderemo al miglior offerente”), questo ransomware adotta molteplici modalità d’intrusione, alcune specifiche per sfruttare le debolezze di sistemi esposti in internet come VPN e Oracle WebLogic. A settembre 2019 ha causato il fermo dei servizi di 22 piccole città nel Texas. A Dicembre 2019 (la notte di capodanno) in Gran Bretagna, ha bloccato il sistema di pagamento elettronico Travelex, rendendo inutilizzabili sportelli automatici e pagamenti in aeroporti e hotel che hanno dovuto ricorre a contanti o sistemi cartacei.

Come proteggere la tua azienda

Strategie di Prevenzione:

- ✓ Creare cultura informatica e di sicurezza. Ad esempio la gestione delle password (password deboli o utilizzate in più ambienti o comunicate ad altri costituiscono un rischio significativo) o la gestione delle email (Il 67% delle diffusioni di ransomware avviene tramite email spam / phishing)
- ✓ Adottare software di protezione (Antivirus, Firewall, impostazioni corrette della posta elettronica [SPF. DKIM, DMARC], …)
- ✓ Dare ai vostri utenti solo gli accessi che gli servono; ad esempio Microsoft riporta che se gli utenti non hanno accesso completo ai loro computer (Accesso amministrativo), l'impatto delle vulnerabilità si riduce sino al 99% (98% debolezza di Windows, 99,5% debolezze del web browser e del 95% per le debolezze di Office)
- ✓ Adottare politiche di sicurezza evolute in relazione al tipo di dato e rischio (complessità delle password, blocco di chiavette USB, …)
- ✓ Effettuare salvataggio dei dati affidabili e in luoghi remoti.
- ✓ Mantenere aggiornata costantemente e celermente la vostra infrastruttura informatica (sistemi operativi, applicazioni, firewall…). Moltissime infrastrutture contengono componenti non più supportati dal produttore e quindi non più aggiornabili per rimediare a debolezze utilizzabili dai criminali. (Windows Xp, Windows 7, Office 2010, Windows 2008, SQL Server 2008, Server linux mai aggiornati, Firewall con Servizi evoluti scaduti, …)

Email: commerciale@sigemi.it
Tel. 02.982.893.50 | www.sigemi.it

Come proteggere la tua azienda

SIGEMI
Cloud Managed Platforms

Quasi il 70% dei computer colpiti da WannaCry è avvenuta su computer Windows 7 per i quali era disponibile da otto anni l'aggiornamento che avrebbe bloccato il ransomware.

Strategie di Controllo:

- ✓ Monitorare lo stato e l'efficacia delle strategie precedenti
- ✓ Verificare periodicamente che le configurazioni in essere siano corrette (regole firewall, permessi di accesso, utenti abilitati, …)
- ✓ Monitorare accessi remoti (orari e provenienze non usuali)

Strategie di mitigazione e reazione:

- ✓ Adottare autenticazioni a 2 fattori. Se un fattore (username e password) è compromesso il secondo (cellulare e codice temporeo) blocca l'accesso malevolo
- ✓ Affidarsi a fornitori di servizi che possano garantire tempo di ripristino certi e testati (RTO Restore Time Object)

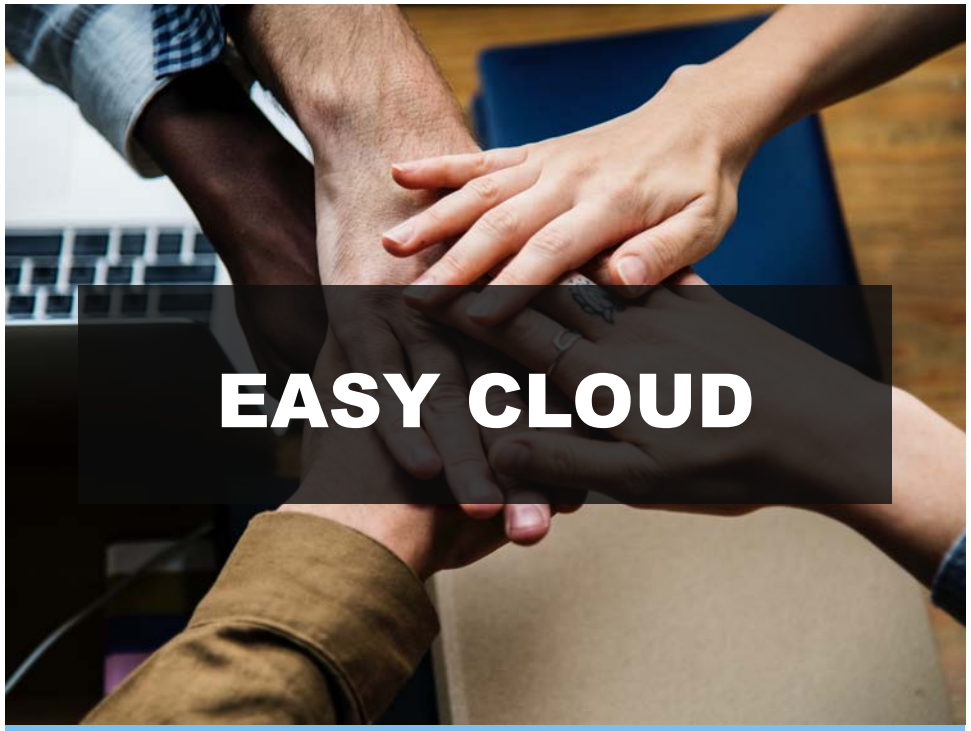
Email: commerciale@sigemi.it
Tel. 02.982.893.50 | www.sigemi.it

Le soluzioni Sigemi

- ✓ Le soluzioni Sigemi offrono Sistema Operativo e Sistema Antivirus monitorati continuamente e aggiornati periodicamente, a livello centralizzato.
- ✓ Tutti i dati hanno una o più copia in Cloud diversi; anche se i dati venissero criptati e risultassero illeggibili, è sufficiente reinstallare il Sistema Operativo e ripristinare i file alla versione antecedente l'infezione.
- ✓ Sigemi garantisce tempi di ripristino con SLA (Service Level Agreement) definiti.

Email: commerciale@sigemi.it
Tel. 02.982.893.50 | www.sigemi.it

Le soluzioni Sigemi



Permette di ospitare le applicazioni «critiche» per l'azienda, delegando completamente a Sigemi la gestione della piattaforma ospitante

Easy Workspace è un servizio di cloud desktop, Sigemi crea una virtual machine completamente dedicata e si fa carico della gestione dell'infrastruttura necessaria

Email: commerciale@sigemi.it
Tel. 02.982.893.50 | www.sigemi.it

Le soluzioni Sigemi

Sigemi ti solleva dalla gestione dei Backup dei dati, garantendo una copia di riserva di ogni tuo dato in Cloud

La protezione antivirus aziendale, completamente gestita da Sigemi

Email: commerciale@sigemi.it
Tel. 02.982.893.50 | www.sigemi.it

SIGEMI
Cloud Managed Platforms

Partner
Google Cloud

Sigemi Srl
Via Brembo, 23 Milano (MI) - Telefono: 02/98289350
Ufficio Commerciale
Via Pofi, 19 Roma (RM) – Telefono: 06/87165091
Email: commerciale@sigemi.it - www.sigemi.it