UNIVERSITÀ
DI SIENA
1240

UniSIcuri in Rete - Ransomware!

Febbraio 2021

Cos'è un ransomware?

Il ransomware è una particolare categoria di malware ("codice malevolo") che colpisce i sistemi informatici **cifrandone il contenuto e chiedendo, successivamente, un riscatto all'utente** per ottenere la chiave (da qui "ransom", che significa "riscatto"). Un vero e proprio "sequestro" del PC, che spesso comprende anche directory condivise e altre risorse di Rete non adeguatamente protette.

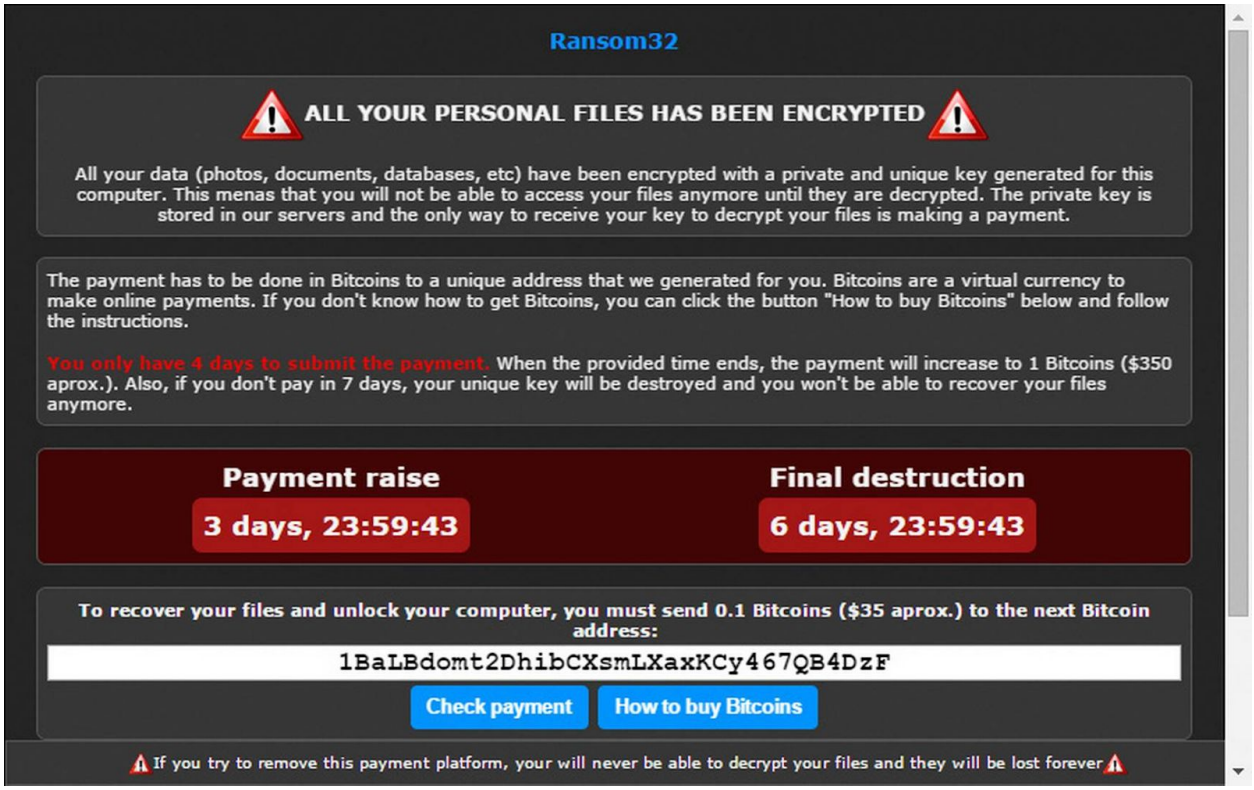
👉 le previsioni[1] indicano che nel 2021 gli attacchi ransomware costeranno complessivamente **oltre 6 trilioni di dollari**, con un attacco ogni 11 secondi circa.

L'attacco generalmente viene portato a compimento usando tre vettori: **la posta elettronica**, il **software illegale (***es. warez***)** e **vulnerabilità note sui servizi** esposti in Rete (RDP - *Remote Desktop Protocol* - è il più utilizzato, insieme alle vulnerabilità dei sistemi di VPN)[2].

Generalmente l'infezione avviene in due fasi: la prima è il **tentativo di diffondersi su altri sistemi**, così da aumentare le proprie possibilità di sopravvivenza, la seconda è **cifrare tutto (o parte) il contenuto del PC** e visualizzare all'utente le informazioni per procedere al pagamento del riscatto.

Il nostro Paese è l'ottavo più colpito al mondo, secondo in Europa: imparare come proteggersi dai ransomware è importante per la salvaguardia dei nostri dati e dell'operatività istituzionale.

[1] *2018-2020 Ransomware statistics and facts, CompariTech*
[2] *Ransomware: gli exploit più usati sono i bug delle VPN, ma gli attacchi RDP restano sul podio, YottaWeb*



Una minaccia molto costosa

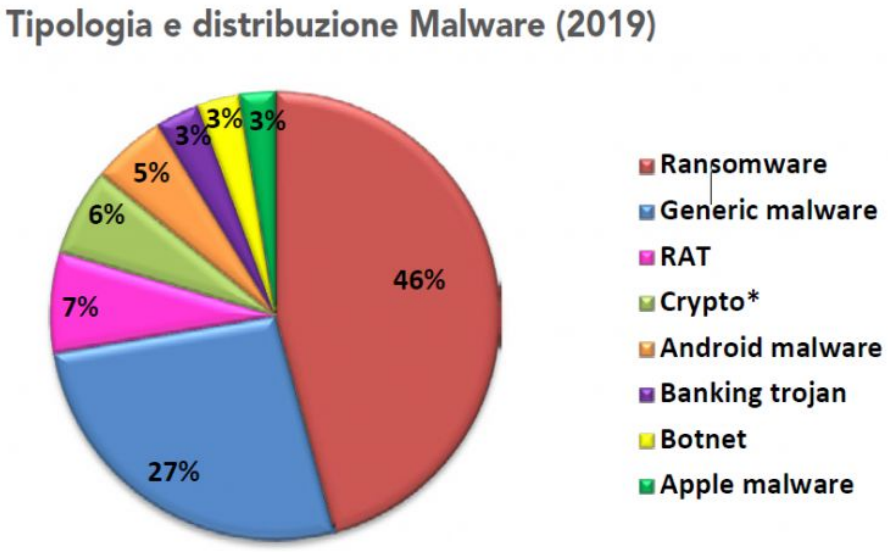
Come hanno imparato aziende del calibro di Luxottica, Geox ed ENEL[3], **essere colpiti da un attacco ransomware può essere molto costoso**, anche solo in termini di blocco dell'operatività aziendale.

In questi casi, **se non si ha una procedura di ripristino da backup in grado di recuperare in tempi rapidi i dati cifrati**, si rischia di dover pagare il riscatto (che spesso è molto oneroso) o, in certi casi, rischiare di perdere tutto: circolano alcuni ransomware particolarmente dannosi che utilizzano sistemi non reversibili di cifratura, distruggendo - *letteralmente!* - qualsiasi file sia presente sui sistemi compromessi.

[3] *Attacchi Ransomware, il caso Geox è solo la punta dell'iceberg, CyberSecurity Startup Italia*

Ultimamente si è consolidata una ulteriore strategia per indurre le vittime a pagare il riscatto (il vero obiettivo di questi cybercriminali è, ovviamente, "incassare" soldi): in caso di mancato pagamento, **tutti i documenti sottratti vengono pubblicati sul web.** Nel caso di una azienda, potrebbe trattarsi di documenti riservati, progetti e strategie aziendali, brevetti... *il danno, anche solo reputazionale, potrebbe essere davvero enorme!*

È proprio il forte ricavo economico ad aver fatto esplodere, *nel mondo del cybercrimine*, l'uso dei ransomware come strumento privilegiato di attacco alle piattaforme e sistemi informatici. Il rapporto ClusIt 2020 sulla sicurezza ICT[4] in Italia lo evidenzia molto bene:



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Talvolta si parla anche di "*doppia estorsione*", a indicare che l'attacco viene perpetrato su due fronti: quello economico e quello reputazionale[5]. Per questo, che si tratti del nostro lavoro in azienda o della nostra rete casalinga, **è importante adottare le**

[4] Rapporto Clusit 2020
[5] Double Extortion - Ransomware and Breach Tracker

buone pratiche per ridurre la possibilità di essere colpiti e dover subire le conseguenze dei *ransomware*.

Buone pratiche per difendersi

1. **Ogni giorno è un buon giorno per fare il backup dei dati importanti.** Assicuriamoci sempre che i documenti, le foto e tutto il materiale che riteniamo importante e fondamentale per la nostra attività e la nostra vita sia adeguatamente "*backuppato*" in un luogo sicuro. Consiglio di mantenere sempre allineate le cartelle dei documenti con un servizio cloud in tempo reale e procedere, almeno una volta a settimana, a salvare off-line tutto il materiale importante (ad esempio, su DVD o su un hard disk esterno). Nei contesti aziendali, spesso le soluzioni di backup centralizzato sono già implementate: assicuratevi di averne compreso il funzionamento e di utilizzarle correttamente, per non avere sgradite sorprese in caso di emergenza.

2. **Utilizzare la cifratura per i documenti che devono rimanere riservati.** La crittografia può essere una validissima alleata, forse la migliore (sempre se usata correttamente), per proteggere il materiale riservato. Nel caso di un attacco *ransomware* e conseguenze esfiltrazione dei documenti, sapere che sono cifrati con un algoritmo sicuro ne impedisce la divulgazione non autorizzata.

3. **Account con privilegi limitati per le attività quotidiane.** Una delle peggiori, e più diffuse, abitudini è quella di utilizzare quotidianamente il PC con un account amministratore: in caso di compromissione, il *ransomware* (ma vale per i malware in generale) troverà tutte le porte aperte e potrà causare danni ancora maggiori. Per le attività quotidiane è bene utilizzare un account utente

con i privilegi necessari e riservarsi l'accesso come "amministratore" solo nei casi in cui sia realmente necessario.

4. **Non installare software craccato o scaricato da fonti non attendibili**. Uno dei modi più facili per compromettere un PC è quello di rendere disponibile, sul Web, software "pirata" già infetto. Non solo, come già ricordato più volte, l'uso di software craccato è una pratica illegale: è uno dei veicoli privilegiati per

infettare i sistemi informatici degli incauti utenti. Credere di risparmiare, spesso, può costare molto più di quanto si creda.

5. **Utilizzare una soluzione antivirus professionale e aggiornata.** Anche se nessun prodotto può offrire una garanzia di protezione al 100%, l'utilizzo di una valida soluzione antivirus aggiornata può aiutare a difendersi da molte delle

minacce informatiche che circolano in Rete. Assicuratevi sempre che le firme dell'antivirus siano aggiornate con cadenza almeno quotidiana.

6. **Attenzione alle mail fraudolente.** Altro veicolo privilegiato sono le e-mail contenenti direttamente il malware o un "dropper" (software che scarica il malware da Internet per infettare il PC), talvolta nascosto nelle macro di Office. Non aprire allegati sospetti, soprattutto se provenienti da mittenti sconosciuti o da fonti non attendibili. È diffuso anche l'uso della cifratura per proteggere gli allegati malevoli come tecnica utilizzata per evadere le analisi degli antivirus:

non cadete nella trappola!

7. **Condividere con parsimonia.** Soprattutto nei contesti istituzionali e aziendali, l'uso di directory condivise può semplificare notevolmente l'attività lavorativa. Tuttavia questa pratica semplifica, in un certo senso, la diffusione del ransomware che può sfruttare queste "condivisioni" per diffondersi attraverso

la Rete istituzionale e comprometterne i sistemi. A meno che non sia strettamente necessario, certe volte è meglio lavorare su piattaforme *as-a-service* (es. *Google Docs* per lavorare su documenti condivisi) che sulle tradizionali "condivisioni" dei files.

In caso di attacco...

Nella sventurata ipotesi che il vostro PC si blocchi e mostri una schermata tipo quelle mostrate sopra, con la richiesta di un riscatto, evitate di cedere alla tentazione di spegnere tutto: quando compare la schermata, ormai è troppo tardi. Procedete quindi a scollegare dalla Rete il nodo infetto (operazione fondamentale per evitare la propagazione del malware ad altri sistemi) e contattate l'assistenza informatica per ottenere supporto.

Se avete seguito i consigli sull'importanza del backup e come proteggere i documenti importanti, il tutto potrebbe risolversi positivamente in poche ore. Altrimenti, come recitava un simpatico *refrain* di una nota agenzia di viaggi *...ahi ahi ahi ahi!!!!*

Riferimenti normativi

La normativa europea sulla protezione dei dati personali ("GDPR") impone **la definizione di contromisure atte a minimizzare la possibilità del furto di dati** ("*data breach*") e le eventuali conseguenze.

La rete Internet è diventata strumento indispensabile per l'espletamento di gran parte delle attività lavorative dell'Ateneo. Attraverso la Rete, l'Ateneo permette agli studenti, ai docenti, ai ricercatori, ai tecnici, agli amministrativi, ai collaboratori e a tutto il restante personale, l'accesso ai dati e ai servizi necessari allo svolgimento delle attività didattiche e amministrative. **La sicurezza dei dati e delle infrastrutture assume, pertanto, un ruolo essenziale per le libertà e i diritti degli interessati e per il mantenimento della *business continuity*.**

Qualsiasi dispositivo connesso in Rete diventa attore del processo di business e deve rispettare alcuni requisiti minimi per la salvaguardia dell'infrastruttura ICT e dei suoi servizi.

- ➔ **Garante per la protezione dei dati personali** - Regolamento europeo in materia di protezione dei dati personali - www.garanteprivacy.it/regolamentoue
- ➔ **Agenzia per l'Italia digitale** - Misure minime di sicurezza ICT per le PA - www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Contatti e siti web utili

- ➔ Gestione delle **credenziali unisiPass** e **aggiornamento password**: my.unisi.it
- ➔ **Avvisi di sicurezza** dell'Università di Siena: www.uet.unisi.it/category/sicurezza/
- ➔ Servizio di **assistenza tecnico-informatica** dell'Università degli Studi di Siena: helpdesk@unisi.it
- ➔ Segnalazione **violazioni al trattamento dei dati personali**: abuse@unisi.it