LE NUOVE FRONTIERE DEL CYBER-RICATTO

Alvise Scarpa, Nicola Bressan

CYBERSECURITY, KEYWORDS

Concetto molto ampio

Blocco completo delle aziende

Prevenzione

Formazione

Security Operation Center

Assessment per la sicurezza

Cyber Intelligence

Bonifica/Decontaminazione

Backup Offline

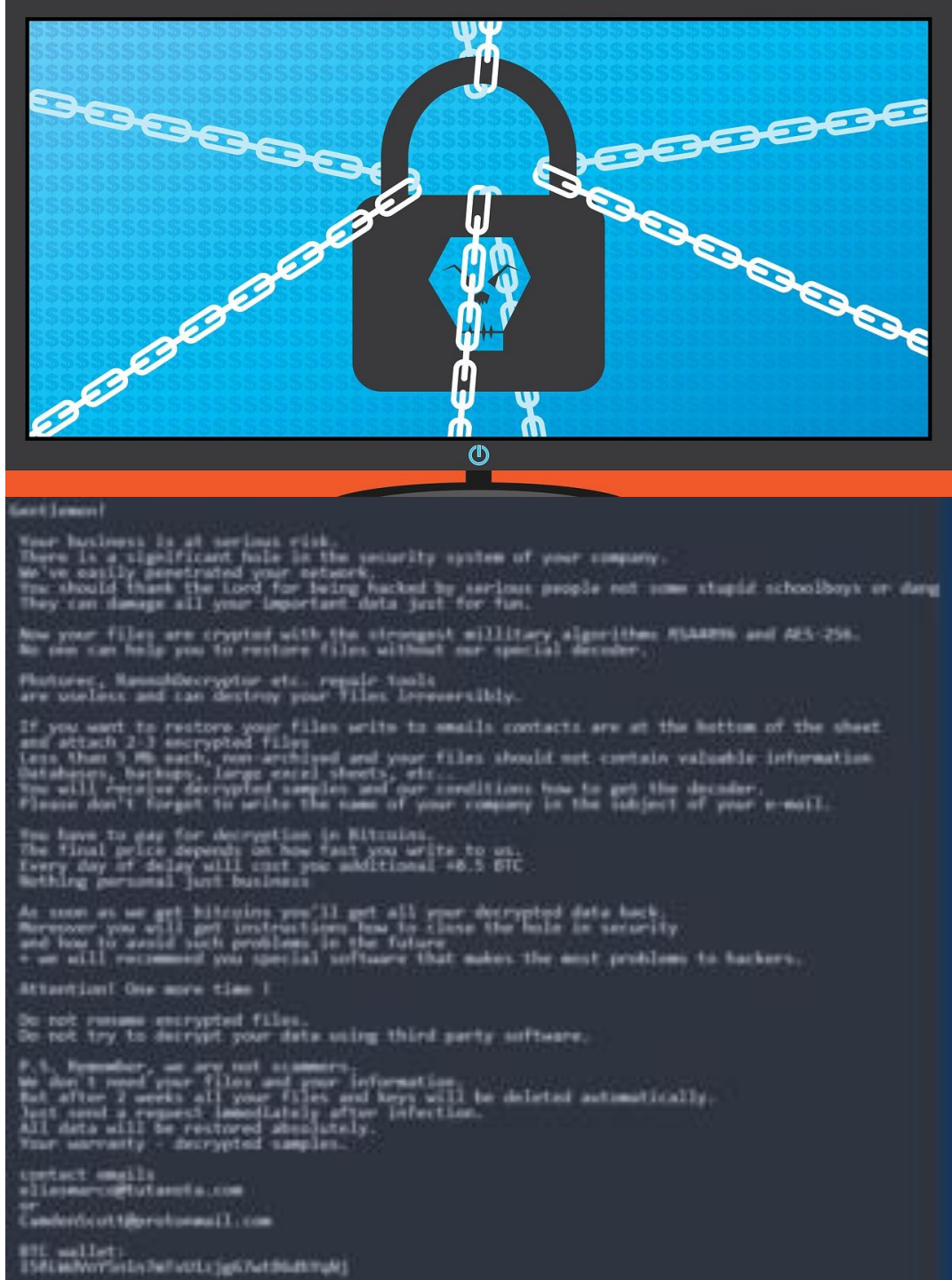
LA CONTRAZIONE DEL VIRUS

Incident management

Incident Response Team!

Cyber Ricatti: attacchi mirati

Trend in crescita nel 2019-20



LE CAUSE, I PUNTI DI INGRESSO DEL VIRUS

Attacchi creati da organizzazioni che hanno un chiaro obiettivo

- Sistemi esposti nel perimetro: porte e servizi vulnerabili
- Email con allegato malevolo
- Azioni pericolose da parte degli utenti (es. chiavette usb)

LE 3 FASI COMUNI DELL'ATTACCO

- **Fase 1**

  Apertura allegato e avvio processo (trojan Emotet o simili)

- **Fase 2**

  Scaricamento di un secondo componente: Trickbot (malware modulare costantemente aggiornato) – recupero credenziali dalle directory e dai Browser e apre backdoors

  Attacco molto breve ultimamente, mappatura dei servizi critici (backup, console veeam, console vmware, ecc)

- **Fase 3**

  Download di un componente Ransomware (es. Riuk) che si occupa della cifratura dei dati

Blocco dei processi aziendali e ricatto

COSA FARE IN CASO DI ATTACCO

- Non spegnere i sistemi ma scollegarli
- Affidarsi ad un partner qualificato che abbia una metodologia chiara
- Totale fiducia nell’operato del partner (concordare un piano d’azione e attenersi ad esso)
- Togliere la connettività da e verso internet fino a stabilità
- Bonifica
- Creazione di una nuova rete non infetta

PREVENZIONE

- Utilizzo di strumenti enterprise per controllo e monitoraggio (SOC, EDR, NOC, SIEM, IDS, IPS, ecc.)

- Backup Offline

- Assessment per la sicurezza per strutturare l’azienda

- Formazione del team IT e utenti finali

- Ogni strumento di lavoro e non porta con sé un rischio

BREAKFAST CHANNEL

Grazie

Segui @RIOS_opensource

http://www.reteitalianaopensource.net