



CHANNEL

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



Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or derg.
They can damage all your important data just for fun.

Now your files are crypted with the strongest military algorithm: RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Phishing, Ransomware etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails contacts are at the bottom of the sheet
and attach 2-3 encrypted files
less than 5 Mb each, non-archived and your files should not contain valuable information
databases, backups, large excel sheets, etc...
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC.
Nothing personal just business.

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future.
- we will recommend you special software that makes the most problems to hackers.

Attention! One more time!

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not hackers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
ell@marco@tutanota.com
or
Gander@cott@protonmail.com

BTC wallet:
1581wVrr7s1n7efvU1jg67ef8d8d8q8f

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

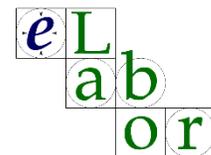
- Utilizzo di strumenti enterprise per controllo e monitoraggio (SOC, EDR, NOC, SIEM, IDS, IPS, ecc.)
- Backup Offline
- Assessment per la sicurezza per strutturare l'azienda
- Formazione del team IT e utenti finali
- Ogni strumento di lavoro e non porta con sé un rischio





BREAKFAST CHANNEL

Grazie



Segui @RIOS_opensource



<http://www.reteitalianaopensource.net>