



Analisi di un binario estratto da un Incident Response

Antonio “s4tan” Parata



14^a EDIZIONE



whoami.exe

- Senior Security Researcher at CrowdStrike
- Owasp Italy Board since 2006
- Phrack Author
http://www.phrack.org/papers/dotnet_instrumentation.html
- Passionate F# developer
- Main developer at <https://taipansec.com/index>
- Social:
 - <https://github.com/sponsors/enkomio> 
 - <https://twitter.com/s4tan>
 - <http://antoniorparata.blogspot.com/>
 - <https://www.linkedin.com/in/antoniorparata/>





Introduzione

- Un Incident Response e' spesso la conseguenza di un security incident
- Parte di questa attivita' e' l'identificazione e analisi di eventuali binari che possono aiutare a capire meglio cosa sia successo e quali danni sono stati fatti
- In questa demo verranno analizzati due binari, le cui varianti, sono state identificate anche durante casi di incident response
(<https://github.com/enkomio/Conferences/tree/master/HackInBoSafeEditionMay2020>):
 - c5fedb78ca5799fed3010812941f0da7222803a444efea0594bec67c6eca1254
 - aaa9268b4a80f75eeb58b61cbd745523b1823d5adf54c615ad9ddf6b8fa0e806

Correva l'anno 2013...

- Veniva eletto Papa Bergoglio
- Esce Topolino n. 3000
- La Lazio vince contro la Roma la 66esima coppa D'italia (vincendo 1-0)
- Edward Snowden svela dettagli sull'esistenza di diversi programmi di sorveglianza di massa del governo statunitense e britannico
- **Evgeniy Bogachev (aka Slavic) decide di creare un nuovo Ransomware che cifra i dati utente e decide di chiamarlo Cryptolocker. Dopo Zeus, Slavic da' il via ad una nuova tipologia di malware.**



Evoluzione

- Gli attaccanti hanno migliorato la loro strategia per ottenere soldi, dandosi al Big Game Hunting (BGH)
 - Compromettere aziende grosse, installare il ransomware, chiedere un grosso riscatto (non è raro vedere richieste maggiori di 300 bitcoin). Qualità piuttosto che quantità
- Non solo cifrano i dati, ma minacciano gli utenti di rilasciare i loro dati online



Evoluzione

- Fine 2019 viene emesso un mandato di arresto eclatante per Aqua.
 - Fino ad allora Slavic aveva la ricompensa maggiore (3 milioni di euro), per Aqua la somma e' arrivata a 4 milioni.
- Aqua e' connesso a malware come il malware bancario Dridex e ransomware come BitPaymer. BitPaymer e' usato con strategia Big Game Hunting*
- Ne sara' valsa la pena puntare sul Big Game Hunting?

Evoluzione

- Aqua lifestyle



Lab time!

