SELF REPLICATED PAYLOAD

WANNA CRYPTO

WANNA DECRYPTO

SERVER MESSAGE BLOCK

RANSOMWARE

WANNA CRY

WINDOWS SMB PROTOCOL PORT 445

FILE SHARE

→ wannacry.exe → encrypts all files

① ② → self replicated payload through SMB

HISTORY → Discovered by NSA → Hacked by shadow Broker → Sold in dup web → Exploited thro phishing

HOW ???

Symmetric ⊕ Asymmetric

HYBRID ENCRYPTION

HISTORY → Symmetric Key Encrypt (FAST) ONE KEY (OR) Asymmetric Key Encrypt (SLOW) MORE CONTROL (SEP KEYS)

Generates SYMMETRIC KEY → SCLIENT

Generate CLIENT ASYMMETRIC KEYS → Cp, Cpriv

(Diff Keys)

DIFF SCLIENT

E(FILE1)

E(FILE2)

E(FILE3)

⋮

USES WINDOWS ENCRYPTION ENGINE

SCLIENT (FILE)

Cp (SCLIENT)

DELETE

COMMAND & CONTROL (Tor)

INTERESTING FINDS

- Hardcoded IP whitelist for (some lab setup) to disable if machine is rebooted ip.
- Dont pay money, some WHH fix the issue or hack server for private key

DELIVERY ??? PHISHING EMAILS ⊕ SELF REPLICATE

MITIGATE ???

- Firewall to block SMB
- Patch windows

PAYLOAD ???

- BITCOIN ADDRESS
- TOR COMMAND + CONTROL ADD.
- BINARY