HOW RANSOMWARE USES POWERSHELL

STARTING WITH PHISHING

STARTING WITH COMPROMISED WEBSITES

Email

1 Socially engineered phishing email with attached document is retrieved

macros

2 Document is open and runs macros directly in memory

macros

3 Macros start a command line

7 User is presented with payment instructions required to decrypt data

d12 0a2 t12 01a

6 New script encrypts data

5 Power Shell downloads additional script and encryption key

Power Shell   C:_

4 Command line runs PowerShell script straight into memory

www._

1 User browses compromised or malicious website

app

2 Vulnerable application is exploited

Exploited application

3 Exploited application starts a command line