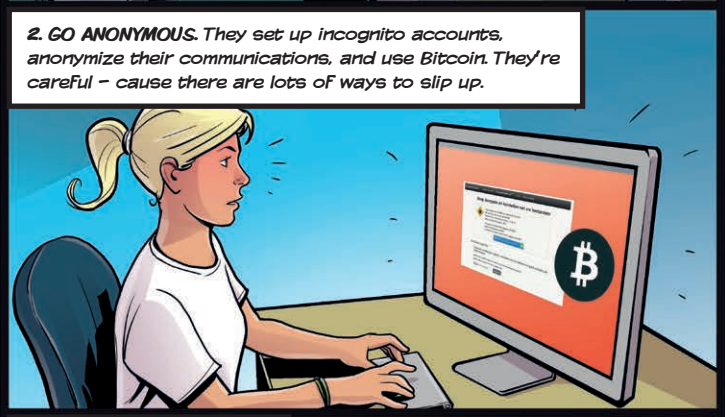
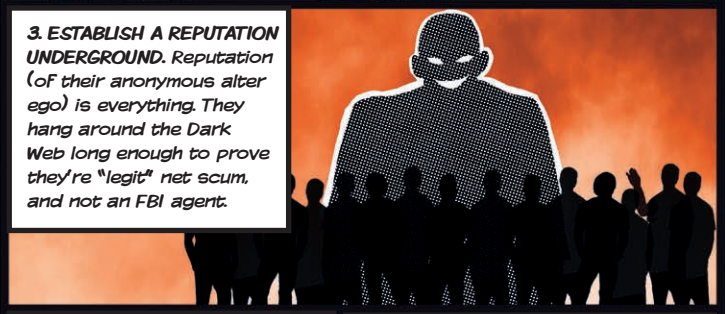
5 HABITS OF SUCCESSFUL RANSOMWARE CYBERCRIMINALS

Crypto-ransomware has risen to levels some describe as epidemic. One reason? It's a fairly easy "biz" to be in. The crimeware market is highly commoditized, with many suppliers and distributors. It's Malware As-A-Service, and these crooks don't even necessarily need to know how to code. Here are their secrets to success.

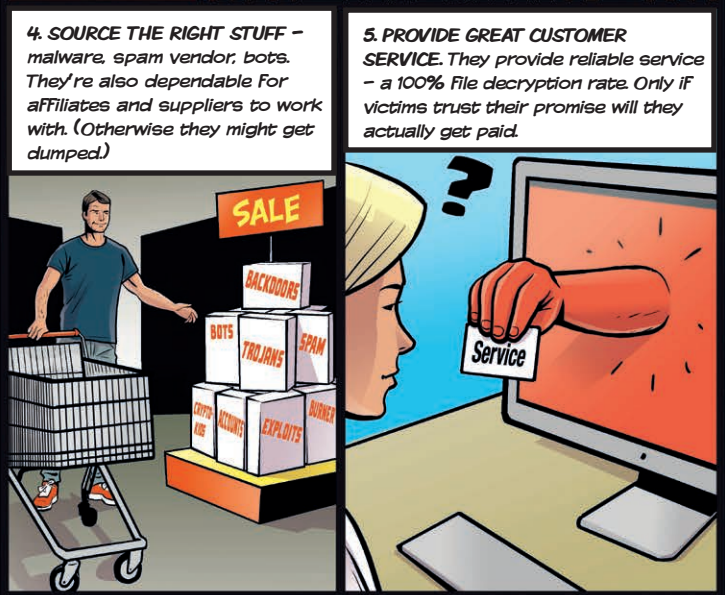
1. ABANDON ALL ETHICAL AND MORAL PRINCIPLES. They make money by causing other peoples' misfortune. So First, they gotta get over their ethics.



2. GO ANONYMOUS. They set up incognito accounts, anonymize their communications, and use Bitcoin. They're careful – cause there are lots of ways to slip up.



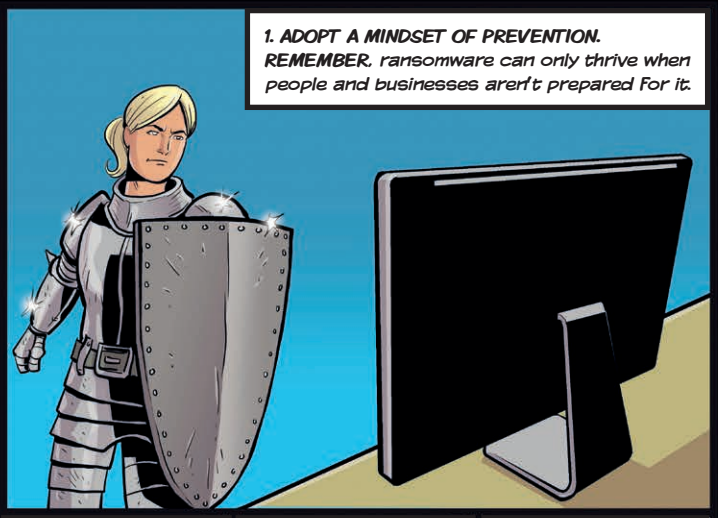
3. ESTABLISH A REPUTATION UNDERGROUND. Reputation (of their anonymous alter ego) is everything. They hang around the Dark Web long enough to prove they're "legit" net scum, and not an FBI agent.



4. SOURCE THE RIGHT STUFF – malware, spam vendor, bots. They're also dependable for affiliates and suppliers to work with. (Otherwise they might get dumped.)

5. PROVIDE GREAT CUSTOMER SERVICE. They provide reliable service – a 100% file decryption rate. Only if victims trust their promise will they actually get paid.

5 WAYS YOU CAN FIGHT BACK

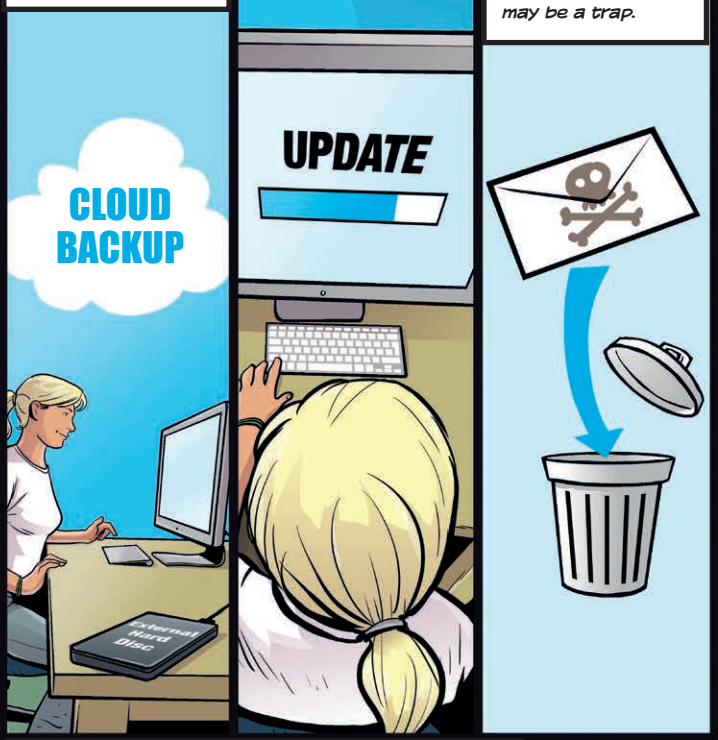


1. ADOPT A MINDSET OF PREVENTION. REMEMBER, ransomware can only thrive when people and businesses aren't prepared for it.

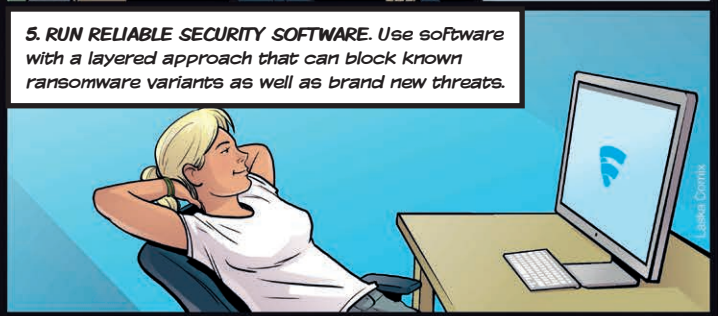
2. FIGHT FORWARD – WITH BACKUPS. The fight against ransomware begins before you're ever hit, with reliable backups of your files.

3. KEEP YOUR SOFTWARE UP TO DATE. Ransomware often exploits flaws in old software to edge in and take over your files.

4. BEWARE OF EMAIL. Be suspicious of attachments and links. The post office doesn't send .zip files! A document asking you to "enable content" may be a trap.



5. RUN RELIABLE SECURITY SOFTWARE. Use software with a layered approach that can block known ransomware variants as well as brand new threats.



F-Secure