Attack Scenarios and Methods

Here, we outline the seven most likely cyber exploits and attack vectors organisations will encounter this year.[4]

1. Ransomware Attack
2. Distributed Denial of Service (DDoS) Attack
3. Data Compromise – Internal or Customer/Supplier, IP or personal information
4. Internet of Things (IoT) Device Attack/Breach
5. USB Stick Infection
6. Mobile Device Compromise
7. Cryptojacking Attack

Email is excluded as a standalone vector simply because its role in attacks is already well understood, with *phishing* being the usual method of unauthorised access to systems.

---

[4] They are listed in no particular order. We have chosen to exclude website defacement and the generation of fake news/commentary/reviews from our scenarios for reasons of space and also because the economic impact is harder to measure and less critical in its effect.

Fraudulent emails ('business email compromise') though prevalent, are not likely to trigger the media reaction that other exploits have given rise to, so are also excluded from our analysis.

Ransomware attack

What it might look like: Workers are locked out of machines or files, extortion messages appear on screens, the exploit spreads horizontally across all connected machines on the network. Data may be irretrievably lost and business disrupted.

The *WannaCry* and *NotPetya* global ransomware attacks of 2017 highlighted a set of practical and ethical dilemmas that businesses and organisations must face when deciding whether to concede to ransomware demands.

Ransomware involves criminal hackers hijacking your computer and denying access to operations and/or data unless a ransom is paid. It can cripple an entire business within minutes.

Ransomware attacks are most likely email initiated. Users are 'socially engineered' to open malicious

attachments or click on links to websites. Attacks may also be due to undetected malware on your network.

It is one of the most prevalent cyberthreats today. Its rapid growth has come about because of two main factors. Firstly, ransomware technology has become democratised. Today, anyone can play.

The proliferation of low cost, easy to use malware kits makes the cost and skills involved in implementation very low. If you don't want to do it yourself, you can hire pay-per-use ransomware services to execute the exploit and collect the ransom on your behalf.

Secondly, payments via Bitcoin or less traceable cryptocurrencies like Monero, afford the perpetrator a negligible risk of detection, since traditional law enforcement methods of following the money are less effective in the shadowy cryptoworld these cybercriminals inhabit. For these reasons, ransomware exploits are the near-perfect crime. It's little wonder business is

booming. Relative to the costs and risks, the yields are immense.

By 2016, according to the FBI, over $1 billion was paid to ransomers, who use the psychology of small numbers to their advantage. The demands are typically in the $300-$600 range, increasing the propensity of victims to pay compared to the costs of holding out.

Options:

1. Pay the ransom: you'll have about a 1 in 3 chance of recovering the data,[5] you will be ignoring advice of government and law enforcement, reinforcing the business case for further attacks, and identifying your organisation as ransom-compliant.

2. Defy ransomers: you risk data loss and business continuity.

Despite some recent indications that the incidence of ransomware may be falling (in favour of other

[5] Even if returned, it may be infected with more malware.

To read more, please purchase the book at

https://www.cyberbreachplaybook.com/store/p1/buythebook