CYBER OPS ASSOCIATED (BLUE TEAM)

RED TEAM

- Offensive Security
- Hackliyormuş gibi yapıp açıkları bulan
- Ethical Hacking (Etik Hacker)
- Penetration Test (Sızma testleri)
- Social Engineering (Sosyal Mühendislik)

BLUE TEAM

+ Defensive Security
+ Ağın dedektifidir. Ağda bir olay yaşanıyor mu? Yaşandı mı? Ne yapıldı?
+ Infastructure Protection
+ Damage Control
+ Incident Respond
+ Operational Security
+ Threat Hunters
+ Dijital Forensics

CISCO CERTIFIED
CyberOPS
Associated

→ CyberOPS Giriş Sertifikası
Giriş → A
Medium → P
Expert → E

- GÜVENLİK UCUZ DEĞİLDİR
  —Gökhan Akın

archlinux

Security Onion

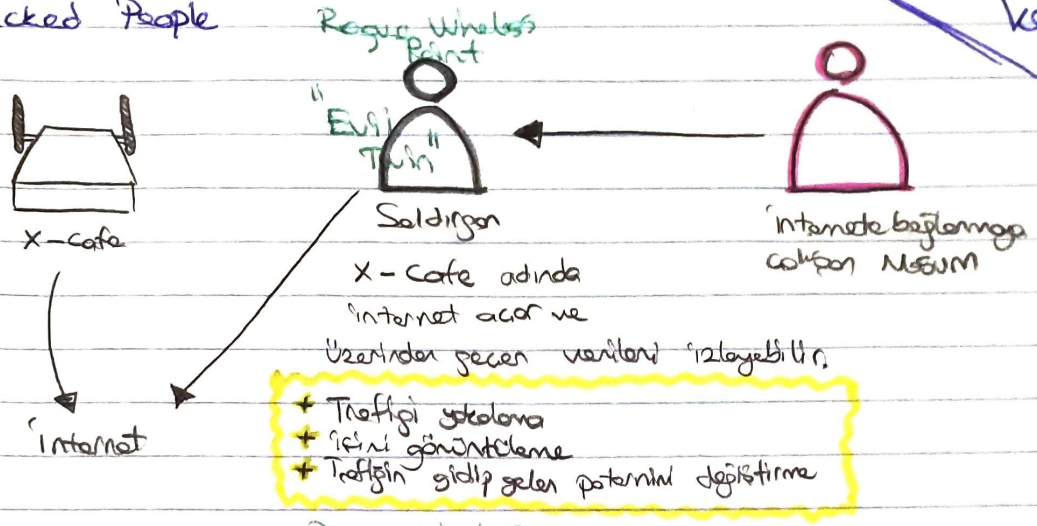
- Client Makinesini sanallaştırmak için kullanılacaktır

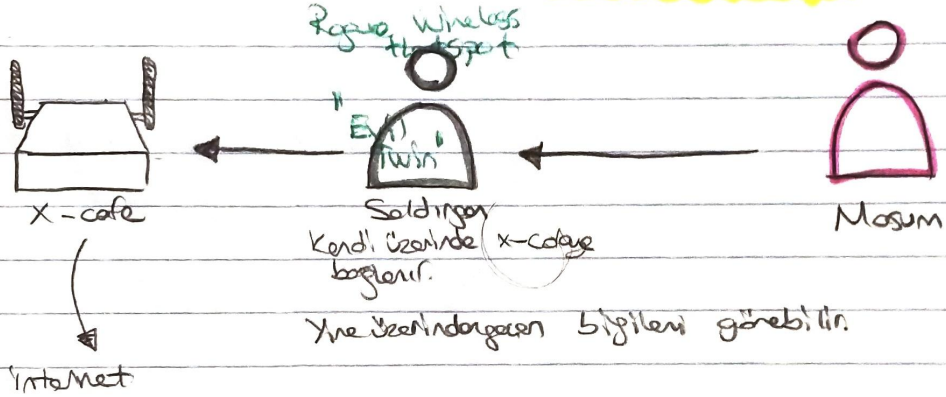
- Mavi takım üyelerinin kullandığı hazır uygulamaları incelemek için kullanılacak

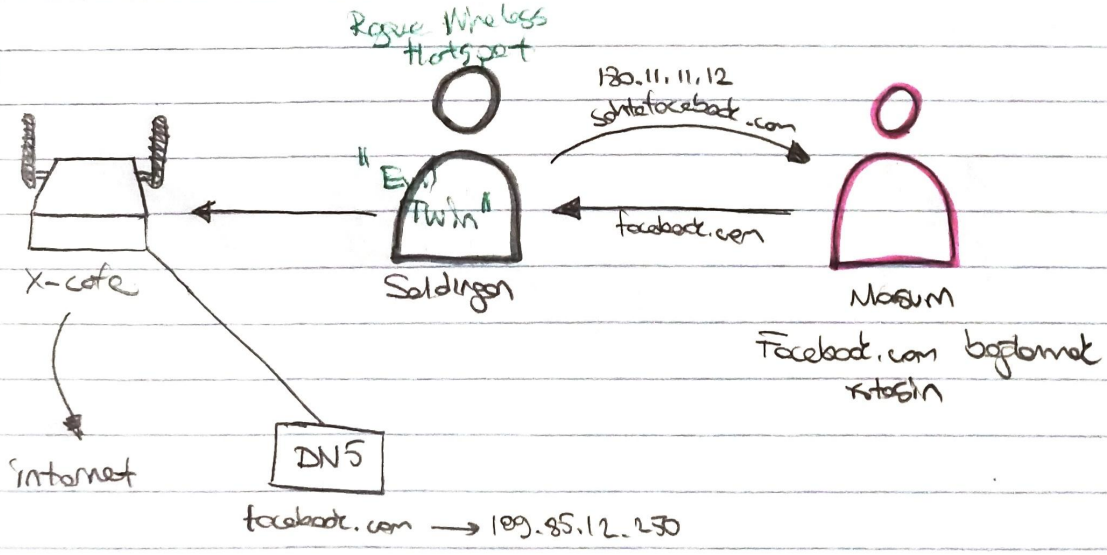
KONU 1 - DANGER - TEHLİKE

http_ https kontrol edin

Hijacked People





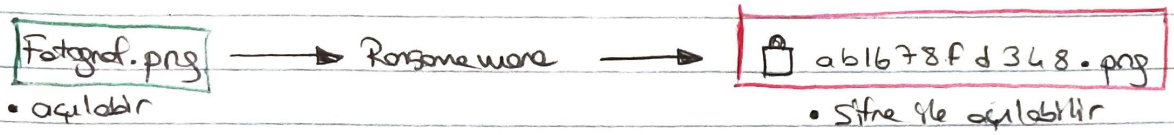


Normalde haberleşmeler https üzerinden gerçekleşiyor ve https haberleşmeler şifrelenmiştir. Dolayısıyla saldırgan verilerini şifreli şekilde görebilir. Ama sizi bağlanmaya çalıştığınız onlayıp size sahte bir internet sitesine yönlendirebilir. Sahte DNS sunucu olur.

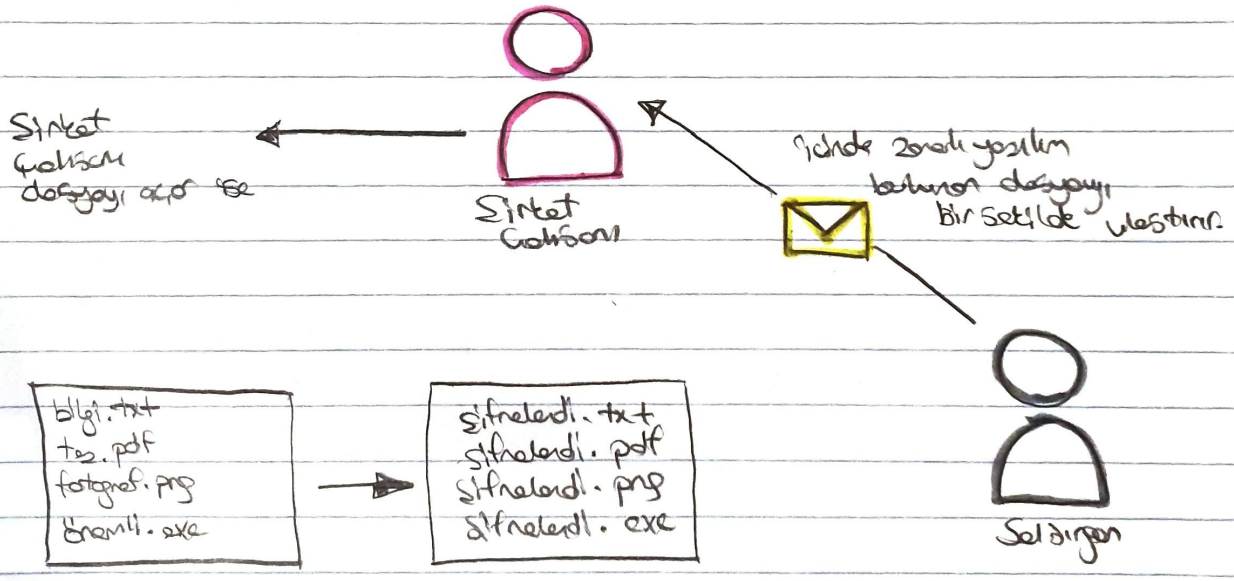
Ransomware Comparison

Ransomware
-Zararlı Yazılımlar-

Ransomware bir çeşit wormdur. Bir yazılımın içine kendini gömer, içinde saklanır. Daha sonra kendini çalıştırır ve bilgisayarındaki tüm verileri şifreler. Şifreleri kırmak yılları alabilir. Fakat yazılımı bulaştıran kişiler "bir hafta içinde silinecektir" gibi mesajlar bırakır ve fidye isterler. Bu fidyeler genelde bitcoin şeklinde olur.



Bir firmayı hedefleyip, sadece ona odaklanarak yapılan saldırılara APT adı verilir.
IoT cihazları güncellenmediği taktirde tehlikelidir.



Not: Eğer şu kadar zaman içerisinde şu kadar parayı şu hesaba göndermezseniz şifrelerini silicegim

TEHTİD AKTÖRLERİ / THREAT ACTORS

- STUXNET (Yazı)
- ZERODAY (Yazı)
- BUFFEROVERFLOW (Yazı)

Amateurs / Loner / Script kiddie

- Little or no skill
- Kurumla hiç önlem olmadıysa zarar verebilirler.
- Hazır araçları ve uygulamaları kullanarak saldırırlar.

Hacktivists

- Genel olarak protesto amaçlı saldırı yapan saldırganlardır.

Financial Gain

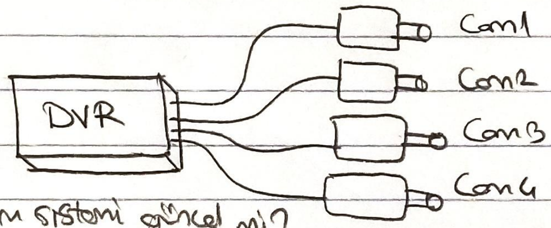
- Finansal çıkar sağlamak için saldırı düzenlerler.
- Yanından geçmeden uğraşırlar ve ya parayı kazanırlar ya da yakalanırlar.

Trade Secrets and Global Politics

- Ülkeler başka ülkeleri hackleyebilir (Siber savaş)

IoT cihazları / IoT Devices

- Nesnelerin interneti cihazları genelde güncellenmez ve üzerinde açıklar, sızılabilecek olanlar vardır ve kolayca sızılabilir.



İşletim sistemi güncel mi?

TEHTİDİN ETKİLERİ / THREAT ~~VECTOR~~ IMPACT

Kişisel Verilen Çalınması:

- PII (Personally Identifiable Information)
  - Kişi hakkındaki önemli ve tanımlayıcı bilgiler sızdırılabilir. — Telefon Numarası, Name, SSN, Birthdate, Credit Card Number
- PHI (Protected Health Information)
  - Kişinin sağlık bilgileri sızdırılabilir. — Medical Information
- PSI (Personal Security Information)
  - Kişilerin güvenlik bilgileri sızdırılabilir — Username, password, other related security information
- EMRs (Electronic Medical Records)

- Kişiler verilerin çalınması
- Rekabet Avantajı Kaybı (Şirketlerin gizli bilgileri çalınabilir)
- Politika ve Ulusal Güvenlik (Ulusal bilgiler çalınabilir)