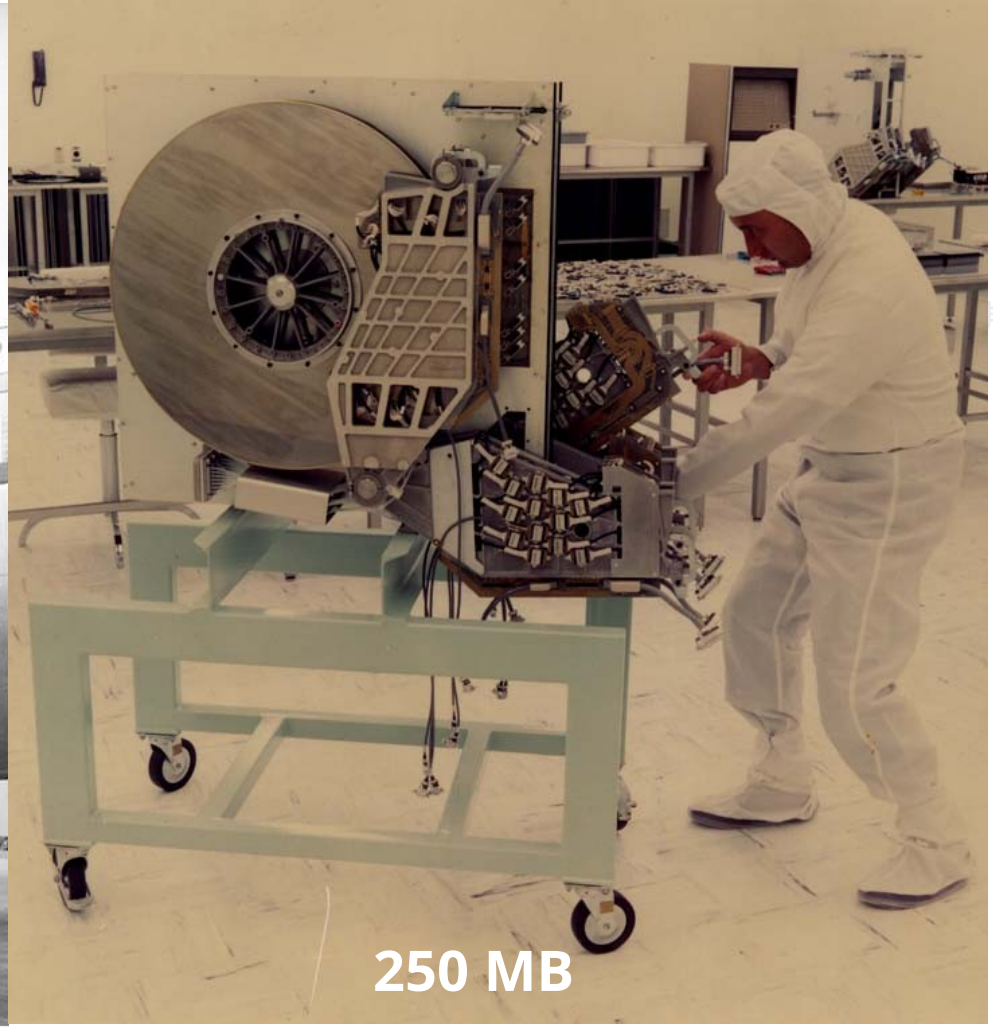
SİBER GÜVENLİK TRENDLERİ

Mehmet Fatih Zeyveli

Teknolojinin Hızlı Gelişimi

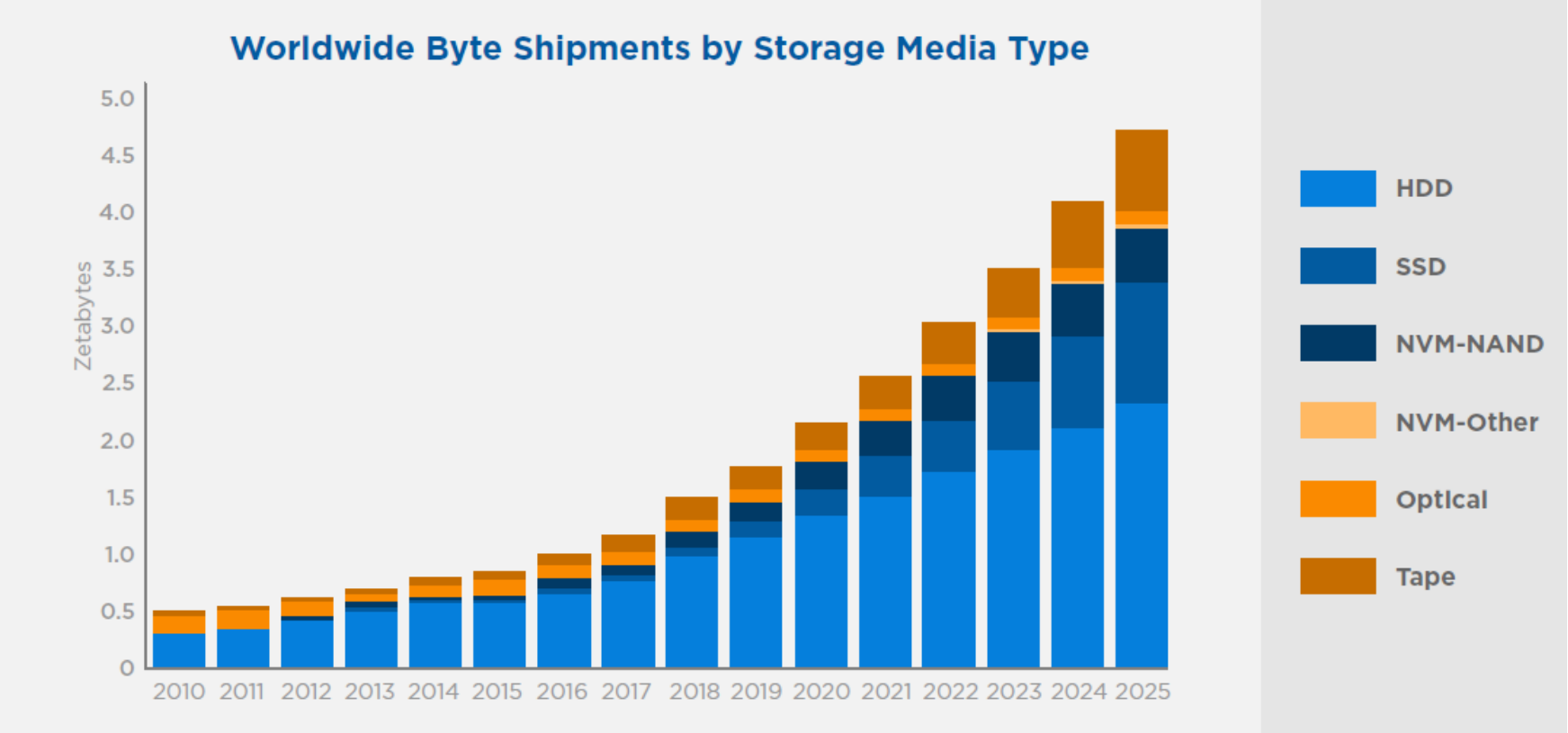


128 GB

100 TB

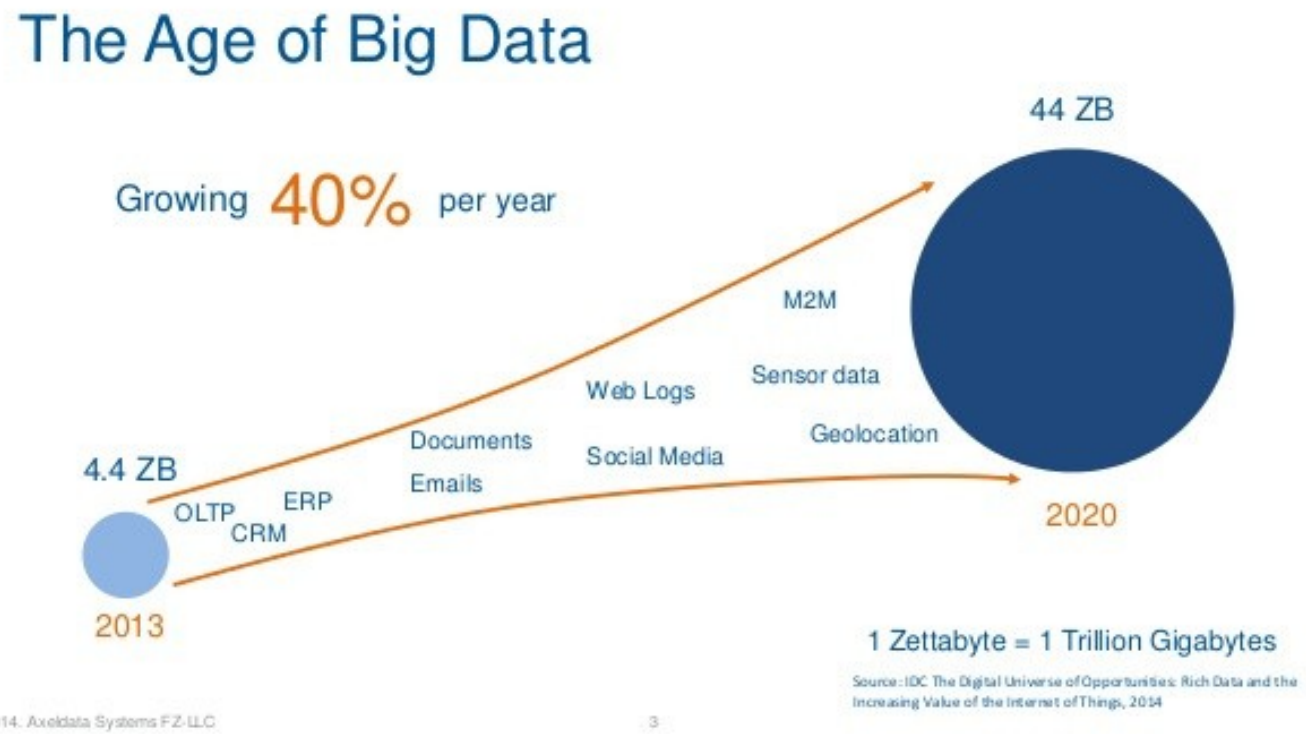
Depolama Kapasitesi Gelişimi

Depolama Kapasitesi



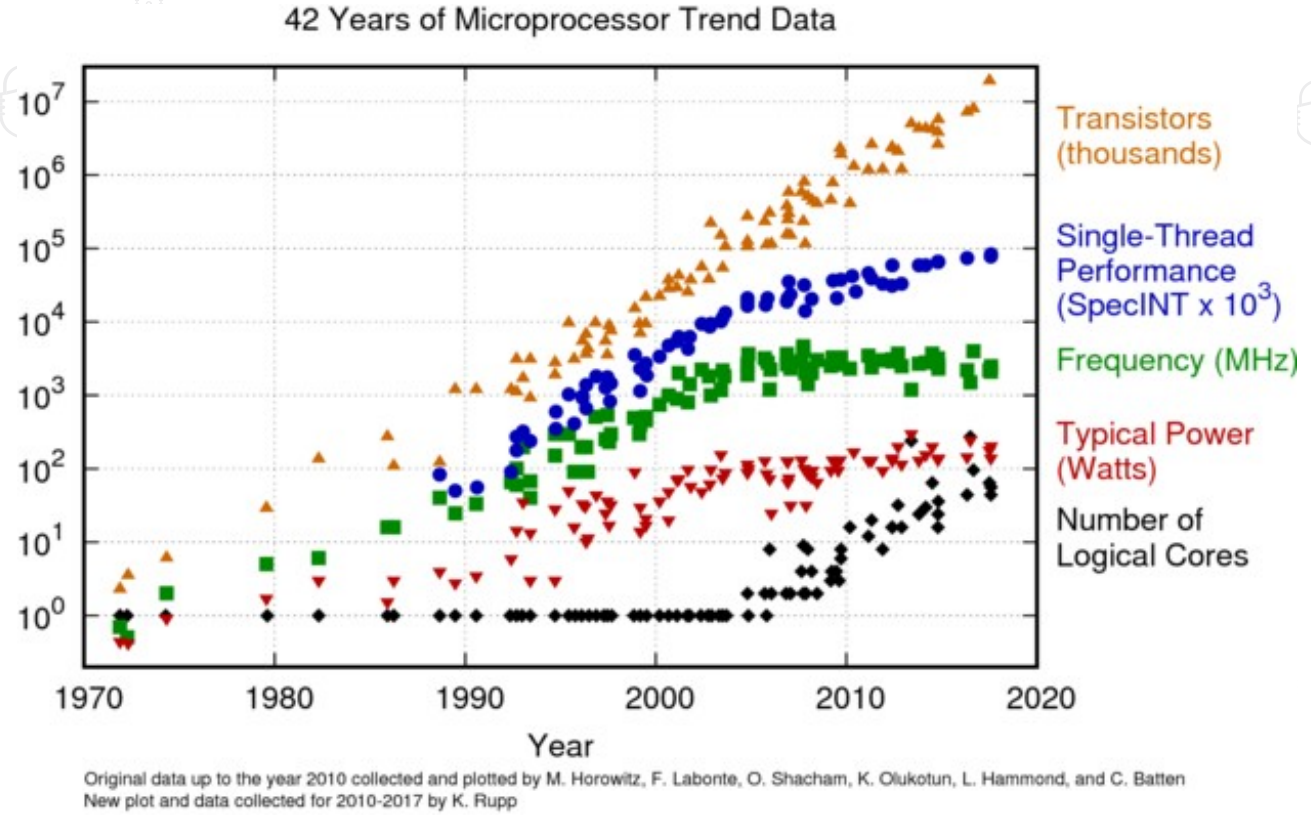
Her Yıl Satılan Depolama Miktarı

Depolama Kapasitesi



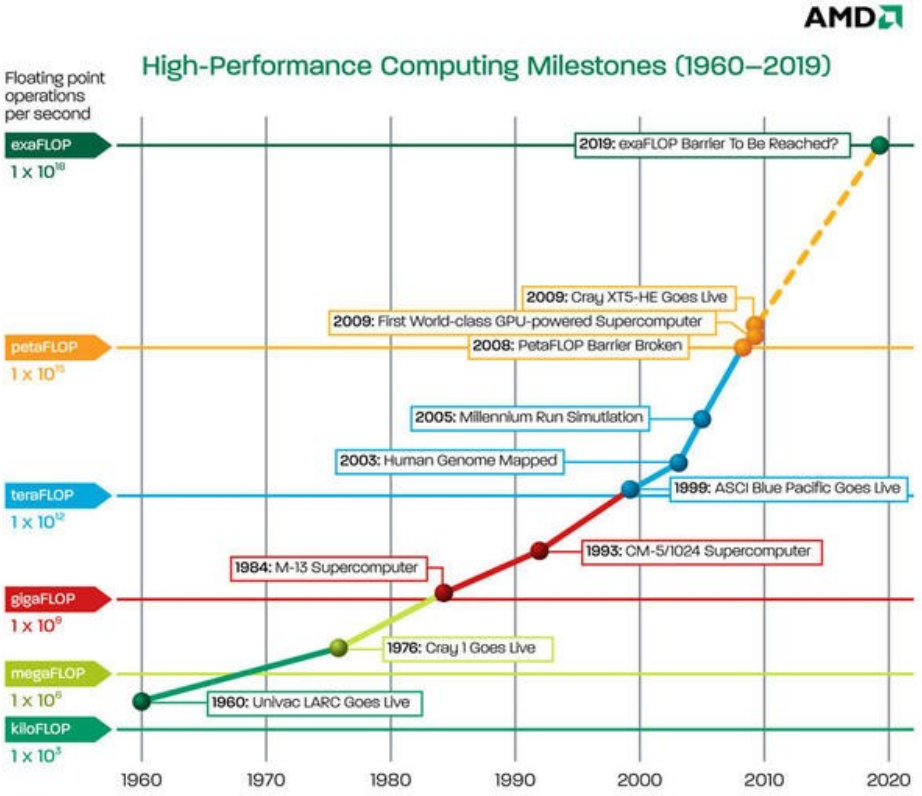
Toplam Depolama Miktarı

İşlemci Performansı



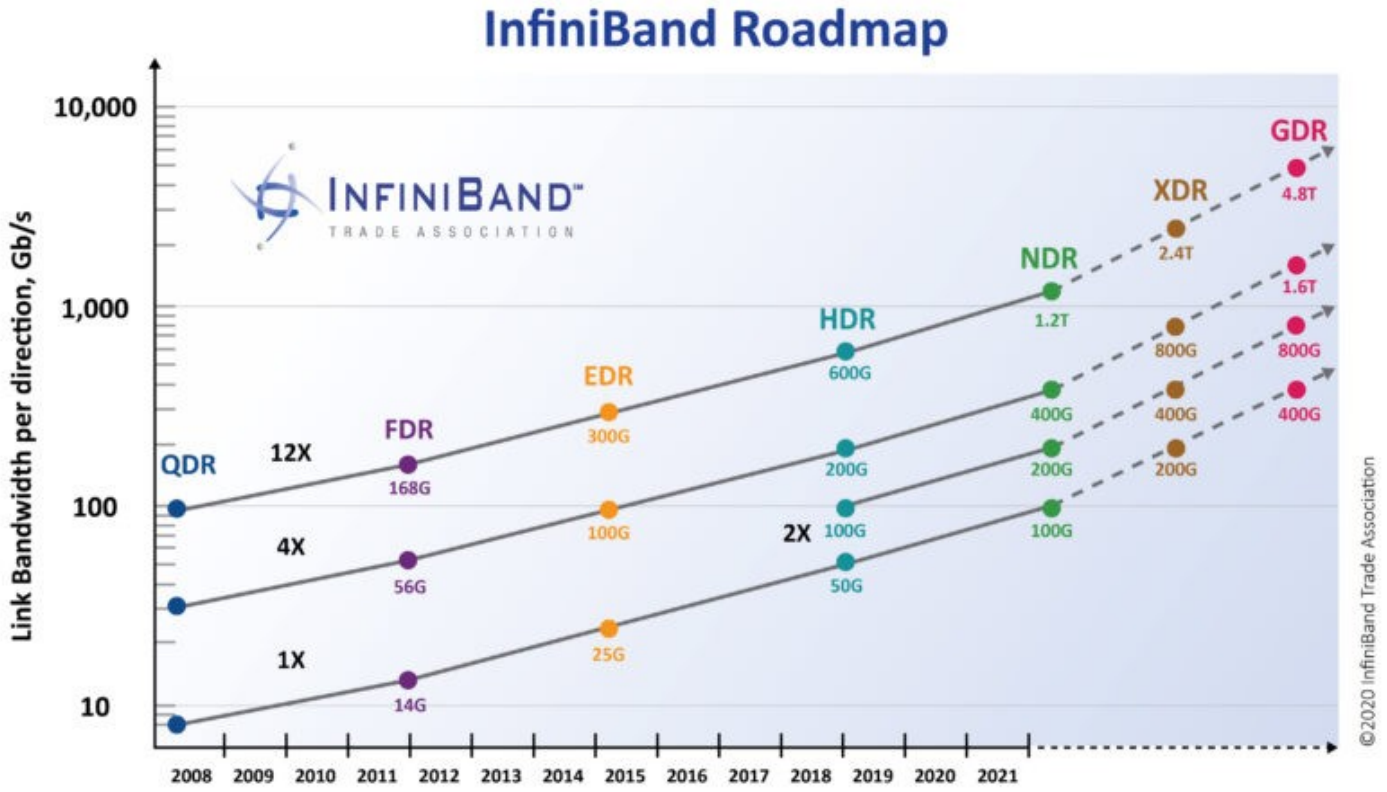
İşlemci Gelişimi

HPC Performansı



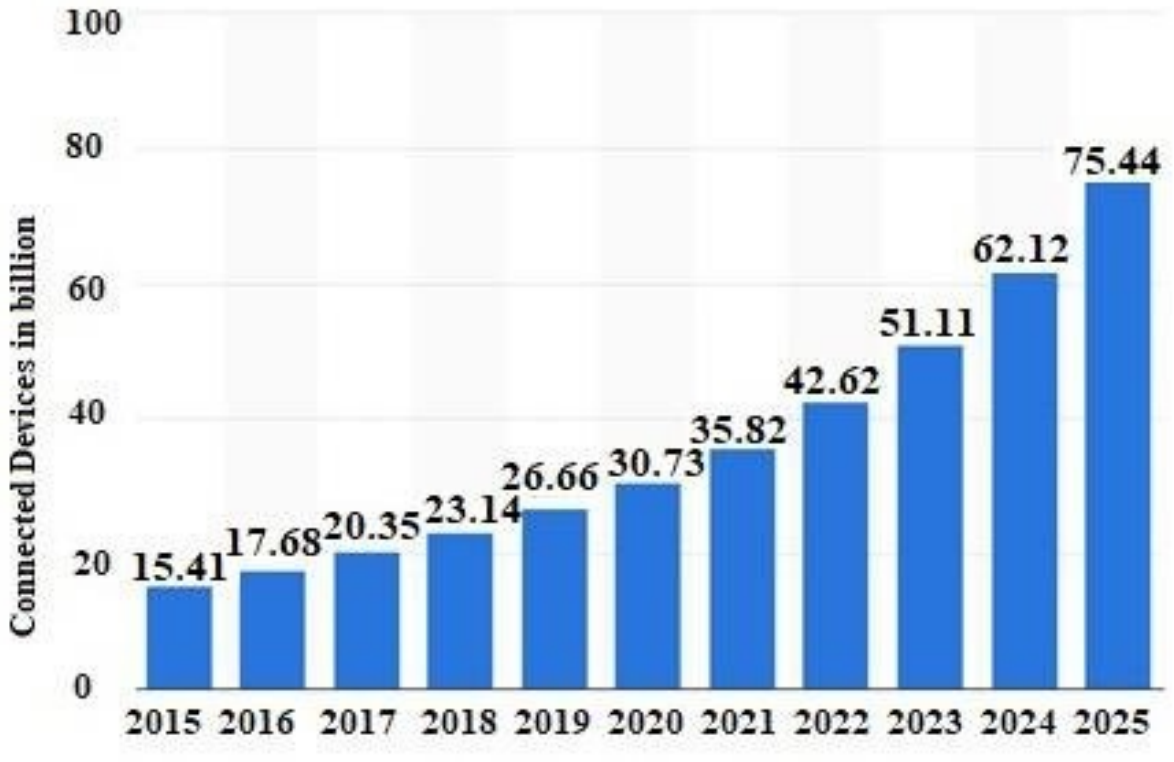
Süper Bilgisayar Gelişimi

Network Performansı



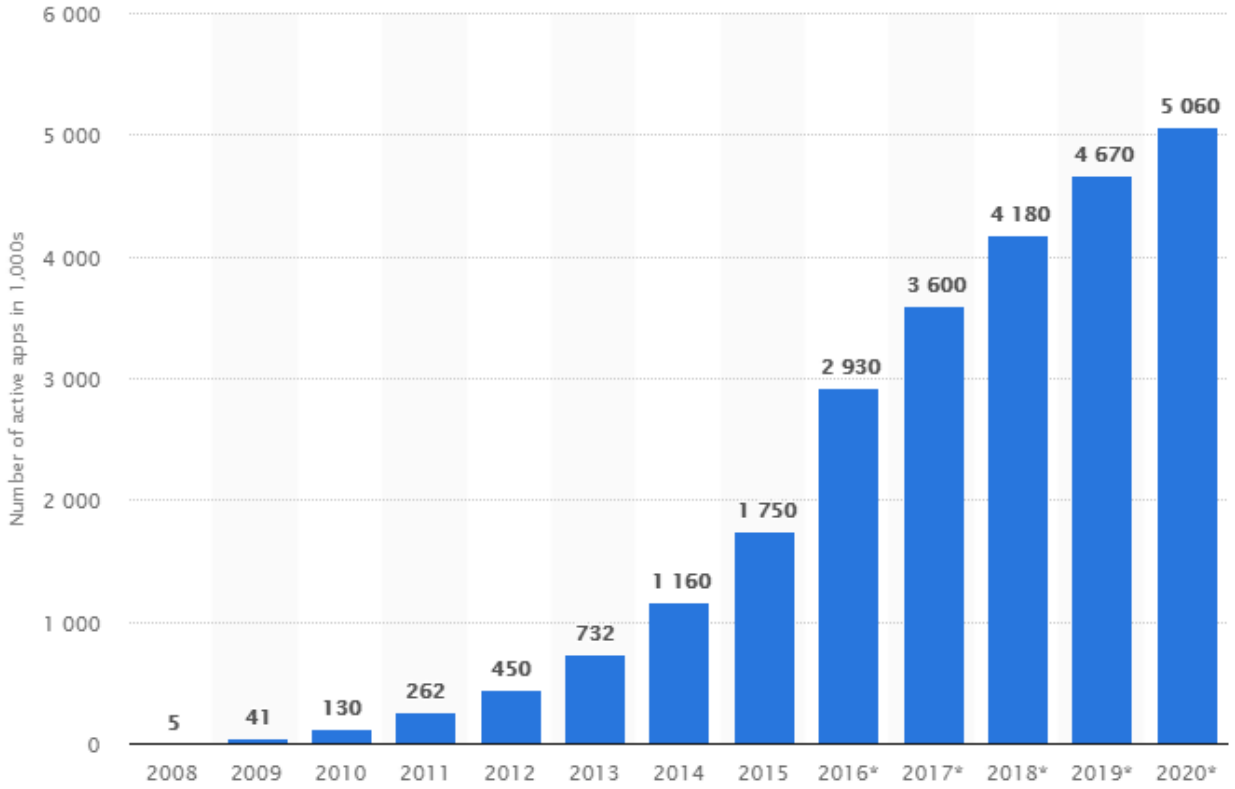
Ağ Hızları Gelişimi

Ağa Bağlı Cihazlar



Ağa Bağlı Cihaz Sayısı Gelişimi

Mobil Uygulama Sayısı



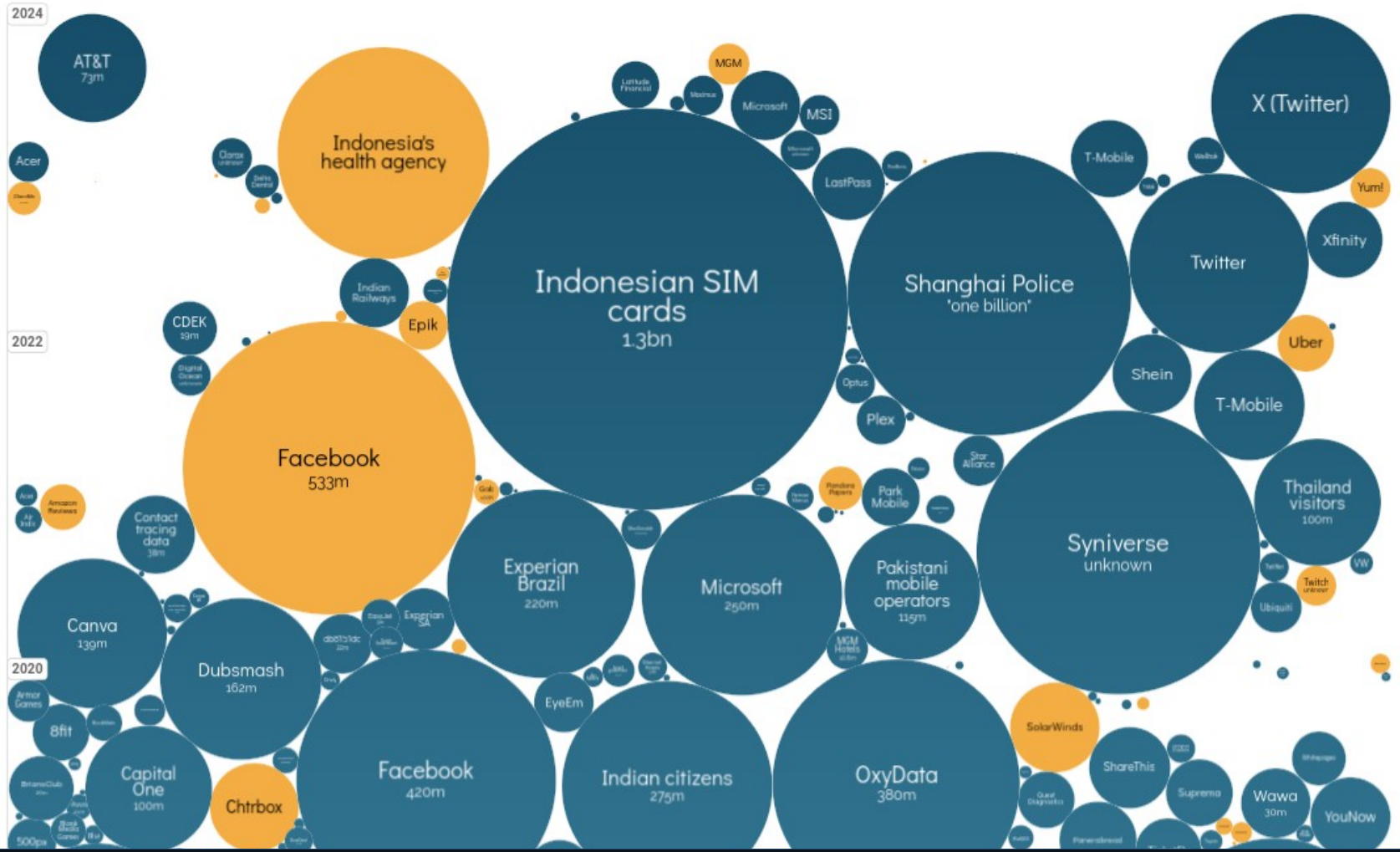
Aktif Mobil Uygulama Sayısı

SONUÇ: SALDIRI YÜZEYİ HIZLA BÜYÜYOR

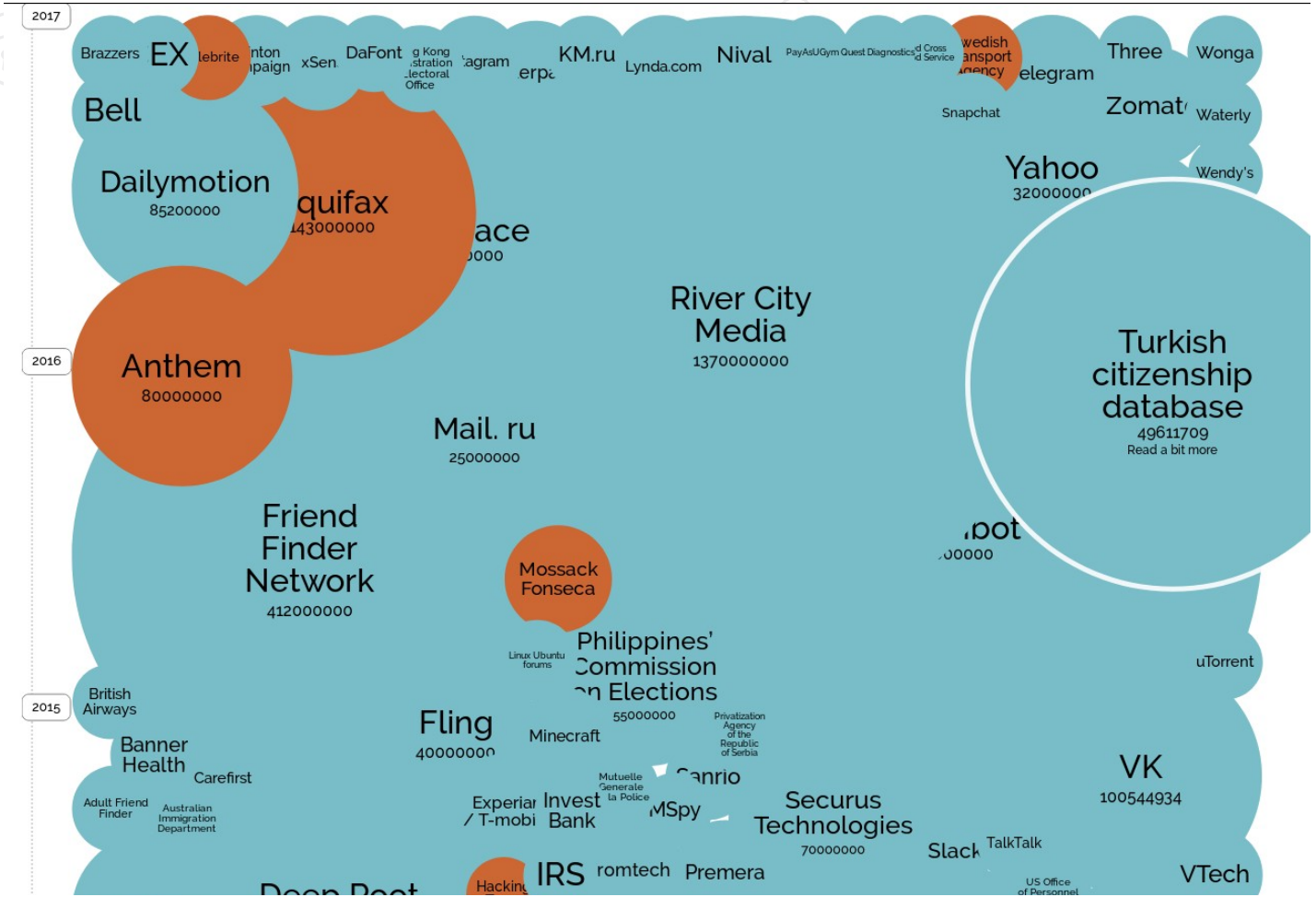
- Covid19 sonrası uzaktan çalışma ile milyonlarca çevrimiçi erişim
- 2025 yılında veri boyutu tahmini 200 zettabytes
- 2025 yılına kadar 30 milyardan fazla IoT bağlantısı
- Her saniye internette 127 yeni cihaz

HIZLI DEĞİŞİM

Siber Güvenlik Tehditleri



Veri Sızıntıları



Veri Sızıntıları (2016 Türkiye)

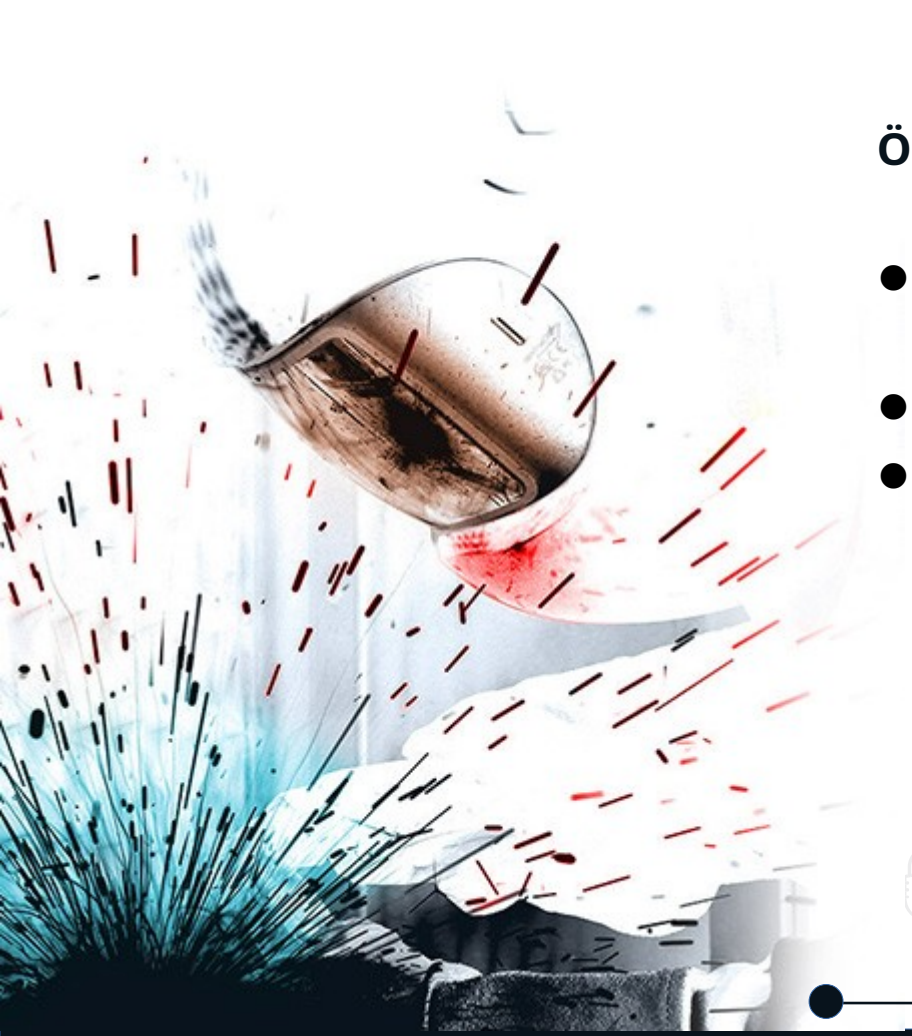
VERİ SIZINTILARI

- Veri Sızıntıları katlanarak artıyor
  - 2019 Sızan Veri: 4 milyar
  - 2020 Sızan Veri: 16 milyar
  - 2023 Sızan Veri: 84 milyar
- 2023’de Yaşanan En Büyük Veri İhlalleri
  - Microsoft
  - Twitter
  - Facebook
  - Zoom
  - Magellan Health

Devlet Destekli Kötücül Yazılımlar

- Stuxnet
- Flame
- Duqu
- Gauss
- The Mask
- Red October (Kızıl Ekim)
- Duqu 2.0
- Pegasus

Devlet Destekli Kötücül Yazılımlar



Örnek Farklı Siber Güvenlik Riskleri

- Ağ bağlantısı olmayan Araç Bilgisayarının uzaktan ele geçirilmesi
- Kalp Pillerinin durdurulması ve Uzaktan kontrolü
- Bebek monitörlerinin, Konuşan ve tepki veren çocuk oyuncaklarının ortam dinleme cihazı olarak veya çocuklarla konuşmak için kullanılması

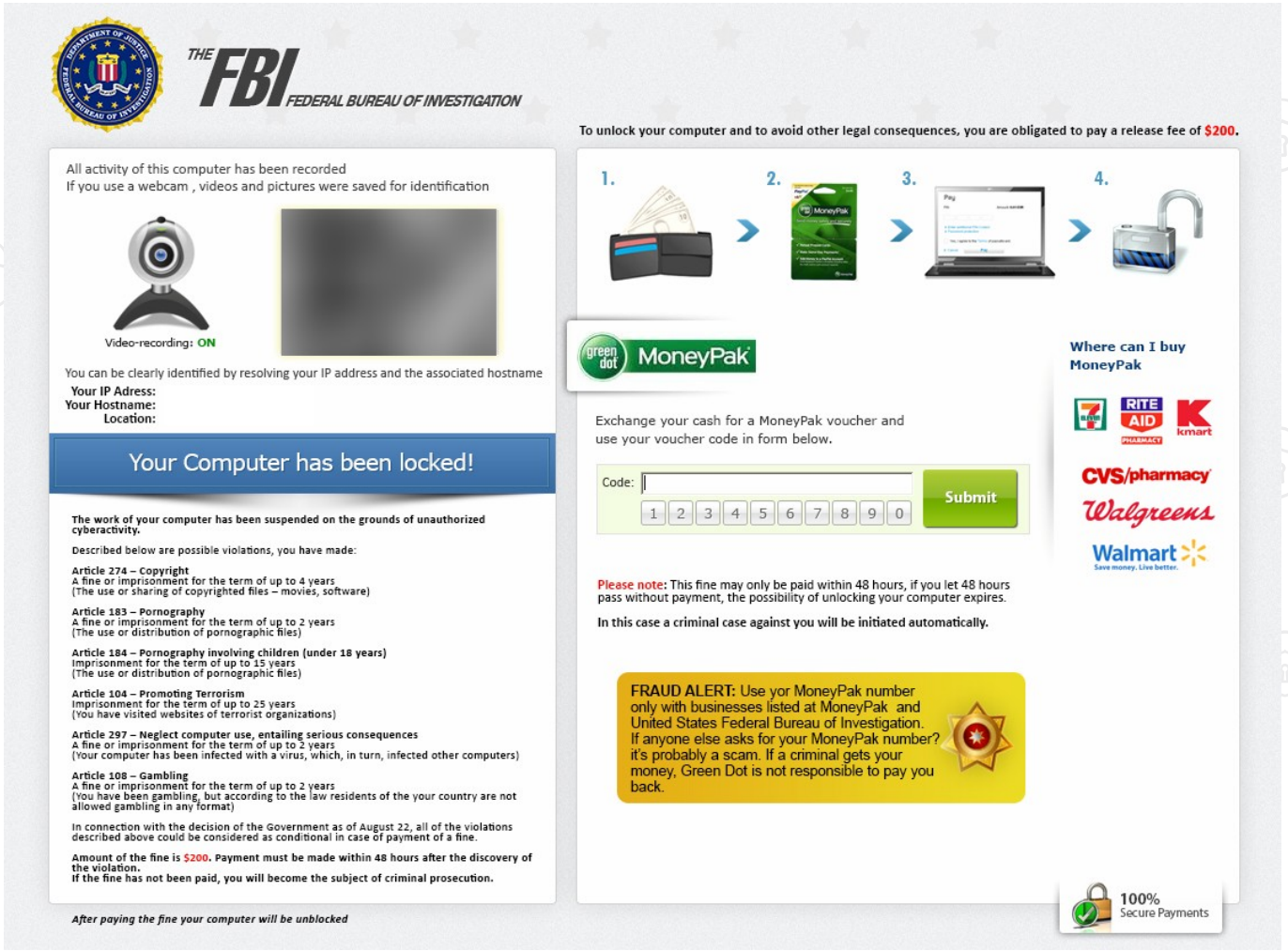

MOBILE

Nearly a half million pacemakers could get hacked

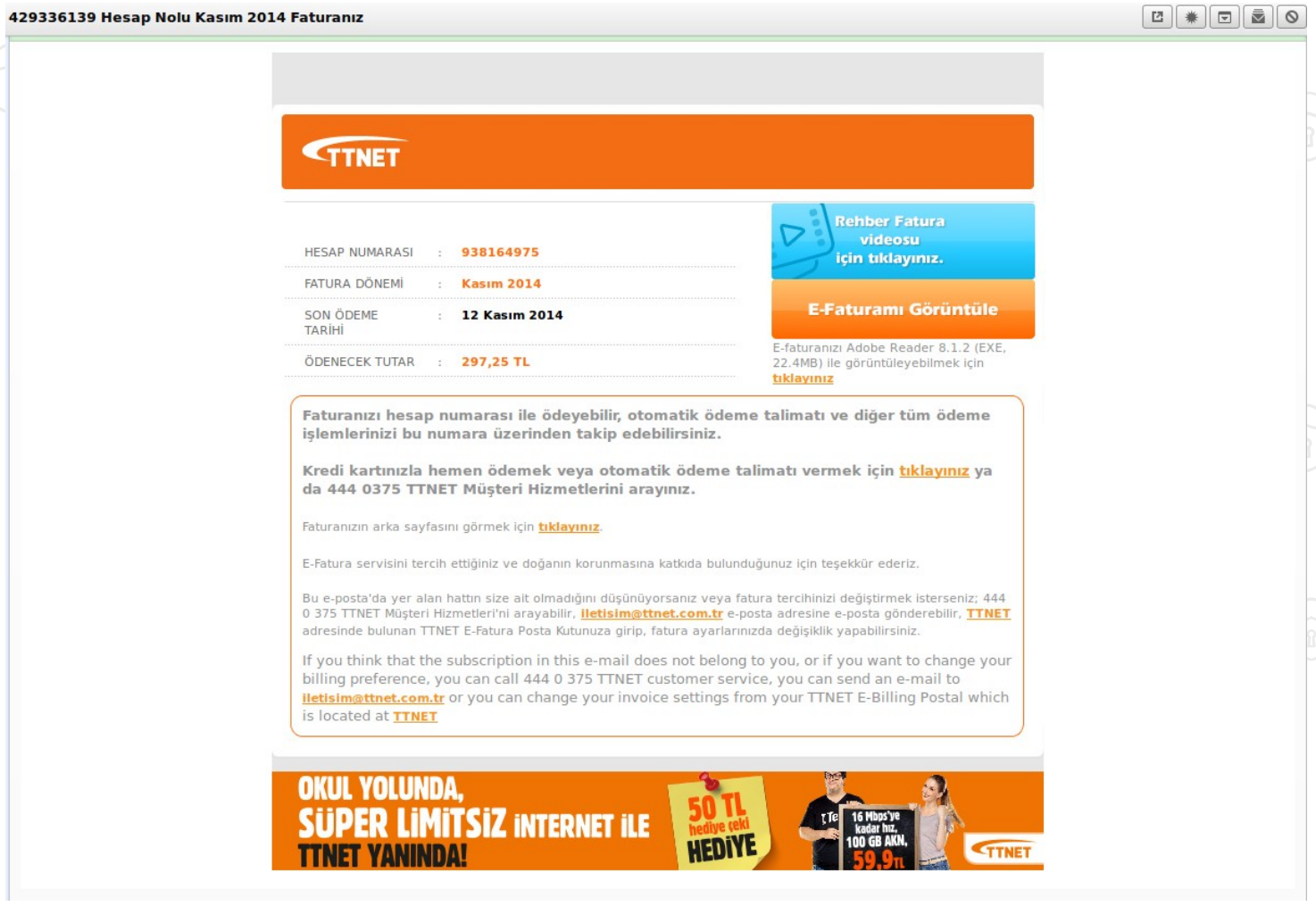
The FDA has authorized a voluntary recall of 465,000 pacemakers (y'know, the things that keep your heart beating) because they need a software update to protect from hacking.

iz

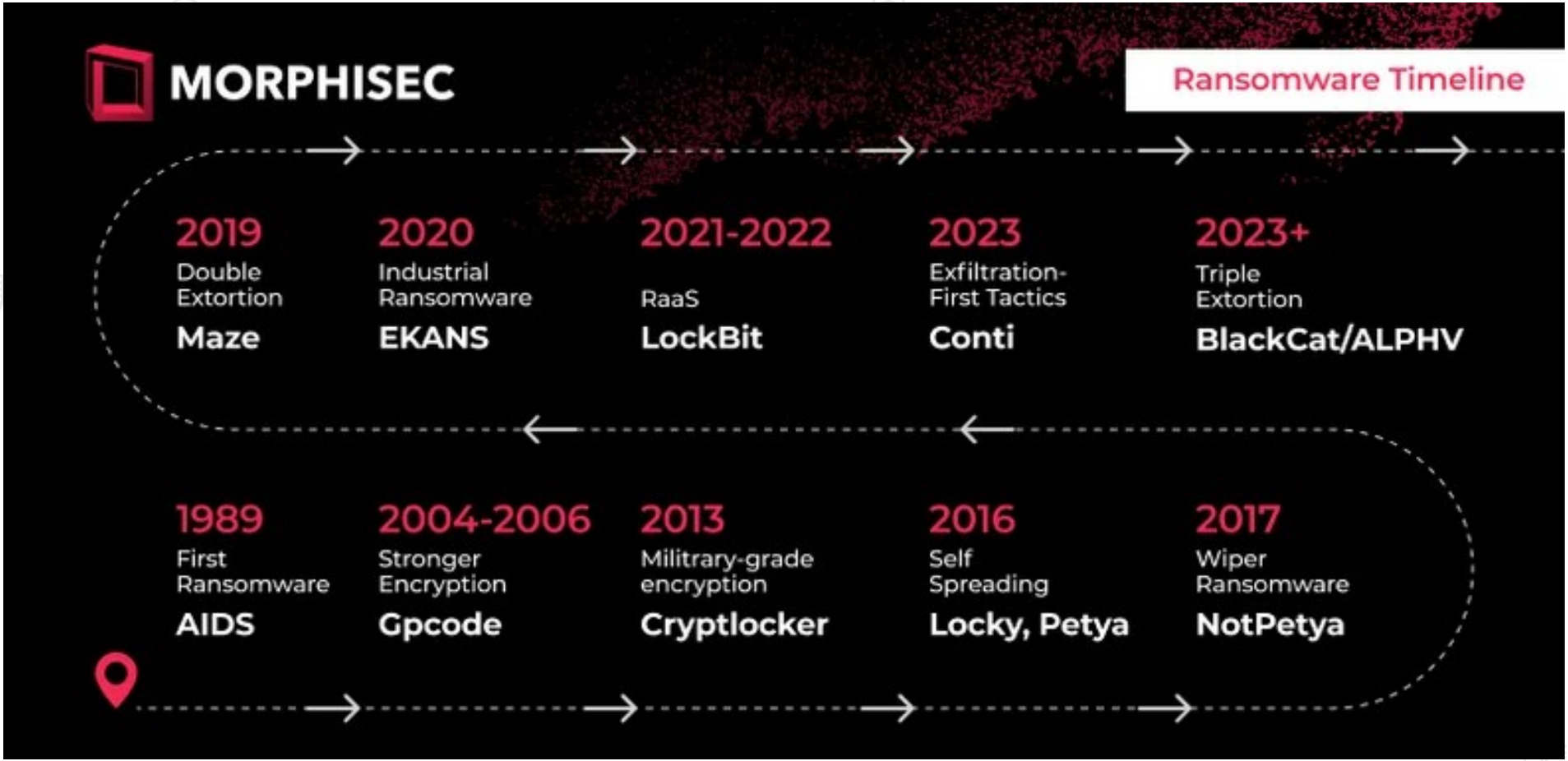
Enteresan Siber Güvenlik Riskleri


THE FBI
FEDERAL BUREAU OF INVESTIGATION
To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $200.
All activity of this computer has been recorded
If you use a webcam , videos and pictures were saved for identification
Video-recording: ON
You can be clearly identified by resolving your IP address and the associated hostname
Your IP Adress:
Your Hostname:
Location:
Your Computer has been locked!
The work of your computer has been suspended on the grounds of unauthorized cyberactivity.
Described below are possible violations, you have made:
Article 274 – Copyright
A fine or imprisonment for the term of up to 4 years
(The use or sharing of copyrighted files – movies, software)
Article 183 – Pornography
A fine or imprisonment for the term of up to 2 years
(The use or distribution of pornographic files)
Article 184 – Pornography involving children (under 18 years)
Imprisonment for the term of up to 15 years
(The use or distribution of pornographic files)
Article 104 – Promoting Terrorism
Imprisonment for the term of up to 25 years
(You have visited websites of terrorist organizations)
Article 297 – Neglect computer use, entailing serious consequences
A fine or imprisonment for the term of up to 2 years
(Your computer has been infected with a virus, which, in turn, infected other computers)
Article 108 – Gambling
A fine or imprisonment for the term of up to 2 years
(You have been gambling, but according to the law residents of the your country are not allowed gambling in any format)
In connection with the decision of the Government as of August 22, all of the violations described above could be considered as conditional in case of payment of a fine.
Amount of the fine is $200. Payment must be made within 48 hours after the discovery of the violation.
If the fine has not been paid, you will become the subject of criminal prosecution.
After paying the fine your computer will be unblocked
1.
2.
3.
4.
green dot MoneyPak
Exchange your cash for a MoneyPak voucher and use your voucher code in form below.
Code:
1 2 3 4 5 6 7 8 9 0
Submit
Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.
In this case a criminal case against you will be initiated automatically.
FRAUD ALERT: Use yor MoneyPak number only with businesses listed at MoneyPak and United States Federal Bureau of Investigation. If anyone else asks for your MoneyPak number? it's probably a scam. If a criminal gets your money, Green Dot is not responsible to pay you back.
Where can I buy MoneyPak
RITE AID
kmart
CVS/pharmacy
Walgreens
Walmart
Save money. Live better.
100% Secure Payments

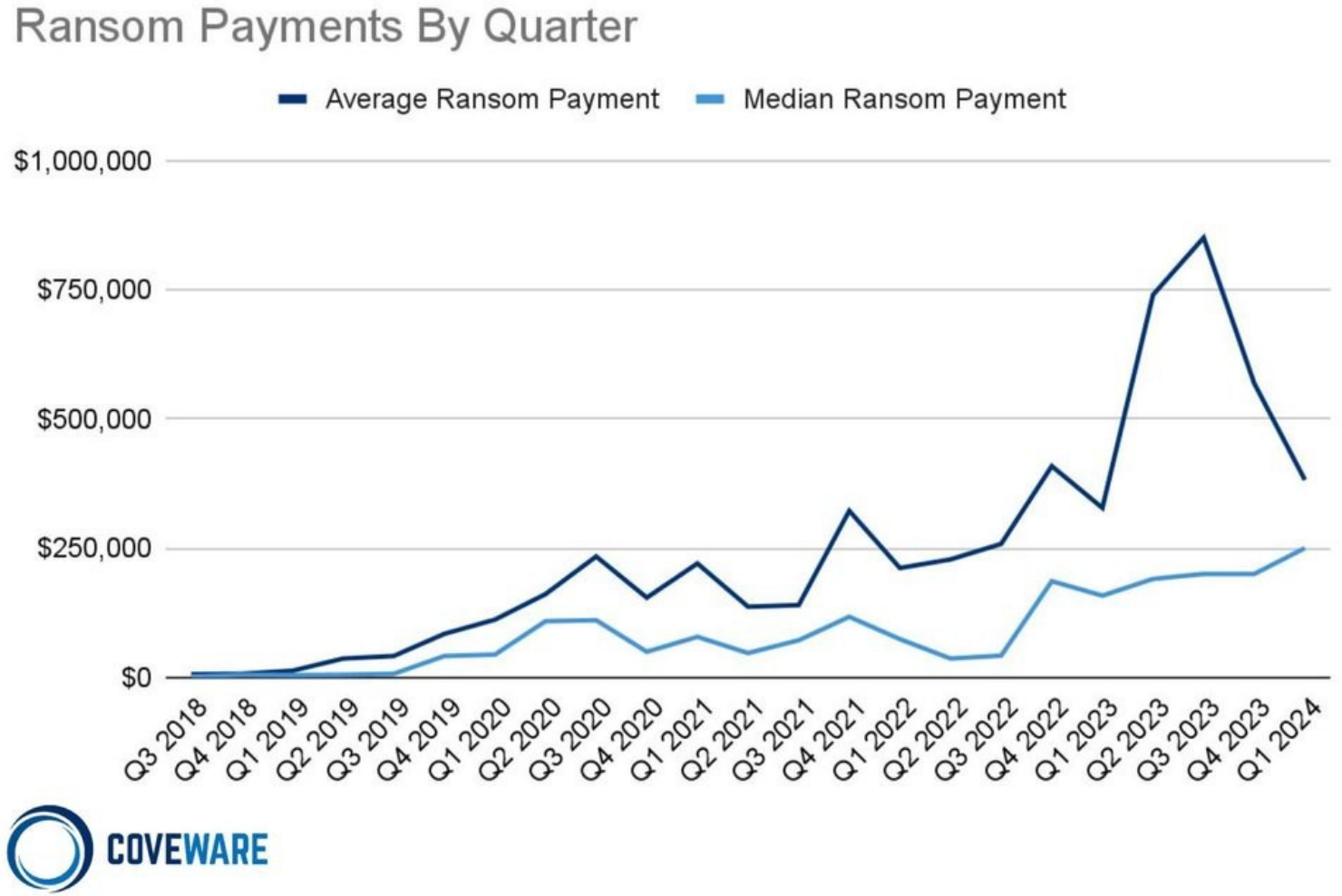
Ransomware


429336139 Hesap Nolu Kasım 2014 Faturanız
TTNET
HESAP NUMARASI : 938164975
FATURA DÖNEMİ : Kasım 2014
SON ÖDEME TARİHİ : 12 Kasım 2014
ÖDENECEK TUTAR : 297,25 TL
Rehber Fatura videosu için tıklayınız.
E-Faturamı Görüntüle
E-faturanızı Adobe Reader 8.1.2 (EXE, 22.4MB) ile görüntüleyebilmek için tıklayınız
Faturanızı hesap numarası ile ödeyebilir, otomatik ödeme talimatı ve diğer tüm ödeme işlemlerinizi bu numara üzerinden takip edebilirsiniz.
Kredi kartınızla hemen ödemek veya otomatik ödeme talimatı vermek için tıklayınız ya da 444 0375 TTNET Müşteri Hizmetlerini arayınız.
Faturanızın arka sayfasını görmek için tıklayınız.
E-Fatura servisini tercih ettiğiniz ve doğanın korunmasına katkıda bulunduğunuz için teşekkür ederiz.
Bu e-posta'da yer alan hattın size ait olmadığını düşünüyorsanız veya fatura tercihinizi değiştirmek isterseniz; 444 0 375 TTNET Müşteri Hizmetleri'ni arayabilir, iletisim@ttnet.com.tr e-posta adresine e-posta gönderebilir, TTNET adresinde bulunan TTNET E-Fatura Posta Kutunuza girip, fatura ayarlarınızda değişiklik yapabilirsiniz.
If you think that the subscription in this e-mail does not belong to you, or if you want to change your billing preference, you can call 444 0 375 TTNET customer service, you can send an e-mail to iletisim@ttnet.com.tr or you can change your invoice settings from your TTNET E-Billing Postal which is located at TTNET
OKUL YOLUNDA,
SÜPER LİMİTSİZ İNTERNET İLE
TTNET YANINDA!
50 TL hediye çeki HEDİYE
16 Mbps'ye kadar hız, 100 GB AKN, 59,9TL
TTNET

Ransomware


MORPHISEC
Ransomware Timeline
2019
Double Extortion
Maze
2020
Industrial Ransomware
EKANS
2021-2022
RaaS
LockBit
2023
Exfiltration-First Tactics
Conti
2023+
Triple Extortion
BlackCat/ALPHV
1989
First Ransomware
AIDS
2004-2006
Stronger Encryption
Gpcode
2013
Militrary-grade encryption
Cryptlocker
2016
Self Spreading
Locky, Petya
2017
Wiper Ransomware
NotPetya

Ransomware



COVEWARE

Ransomware

RANSOMWARE

- **Bazı Büyük Ramsomware saldırıları**
  - **LastPass**
  - **Reddit**
  - **WhatsApp**
  - **Trello**
  - **Bank of America**
  - **TR Bebek Malzemesi Firması**
  - **TR Elektrik Dağıtım Firması**
  - **TR Bakanlık**

Diğer Bazı Tehdit Türleri

- Zararlı yazılımlar
- Hedefli Saldırılar
- Botnet
- Güvenlik açığından yapılan saldırılar
- Sosyal Mühendislik / Kandırma (Social Engineering)
- Kimlik Hırsızlığı (Fraud)
- Spam
- Web sayfalarına saldırılar
- Kaynakların amacı dışında kullanımı (KriptoMadencilik)
- Suç Hizmeti (Crimeware as a service)
- YapayZeka SaldırılarıAI Based Attacks
- Sıfırıncı Gün Saldırıları (Zero Day)
- İçeriden Gelen Tehditler (Insider Threats)

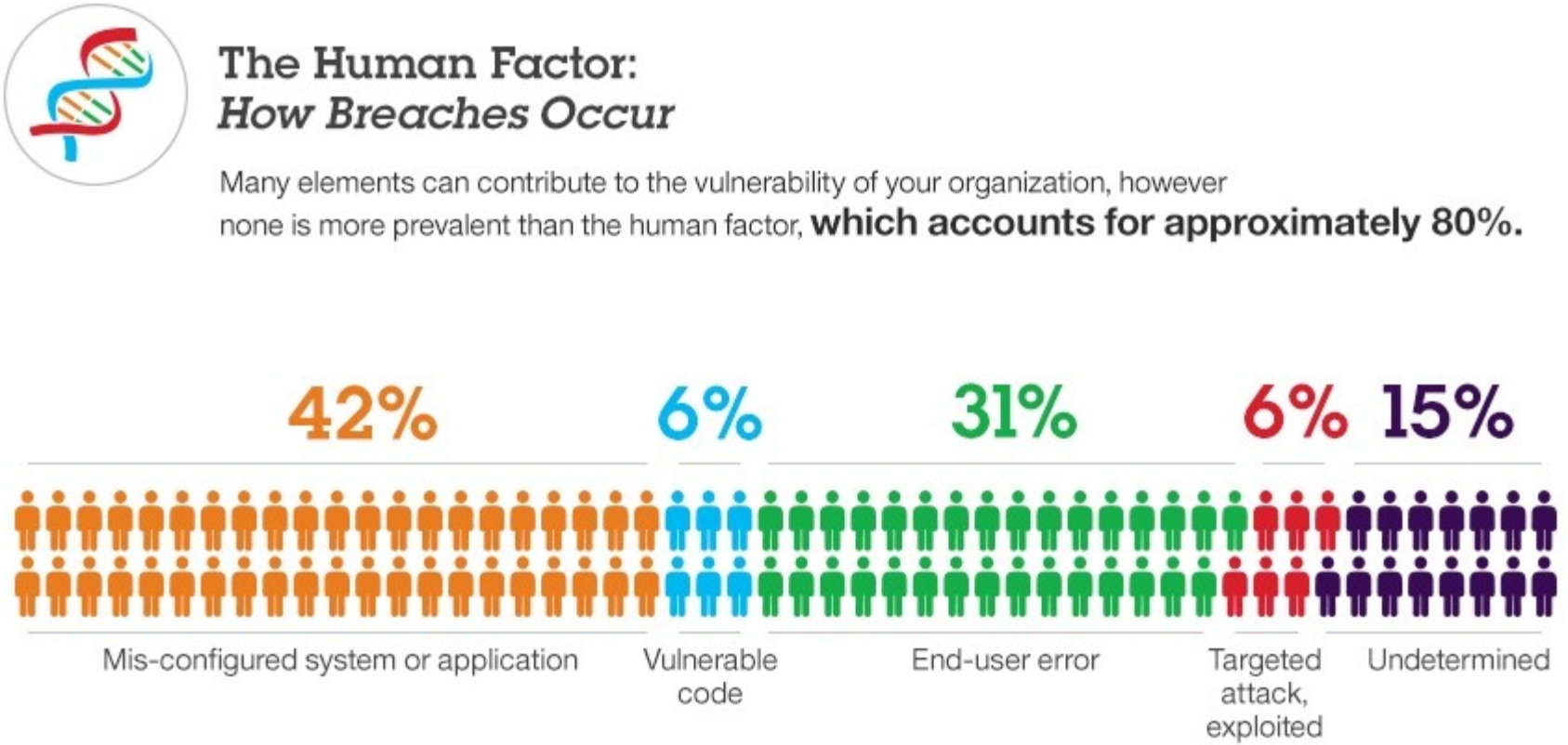
Diğer Tehditler

GELECEK

- Saldırı Yüzeyi hızla büyüyor
- Nesnelerin İnterneti (IoT) ve OT (ICS)'e yönelik saldırılar artıyor
- Uzak erişimin getirdiği riskler artıyor
- Bulut Kullanımı artışı ile bulut riskleri artıyor
- Sofistike saldırılar artıyor
- Logları incelemek zorlaşıyor

SİBER RİSKLERİN GELECEĞİ

YAŞANAN İHLALLERİN ÇOĞU İNSAN HATASINDAN KAYNAKLANIYOR



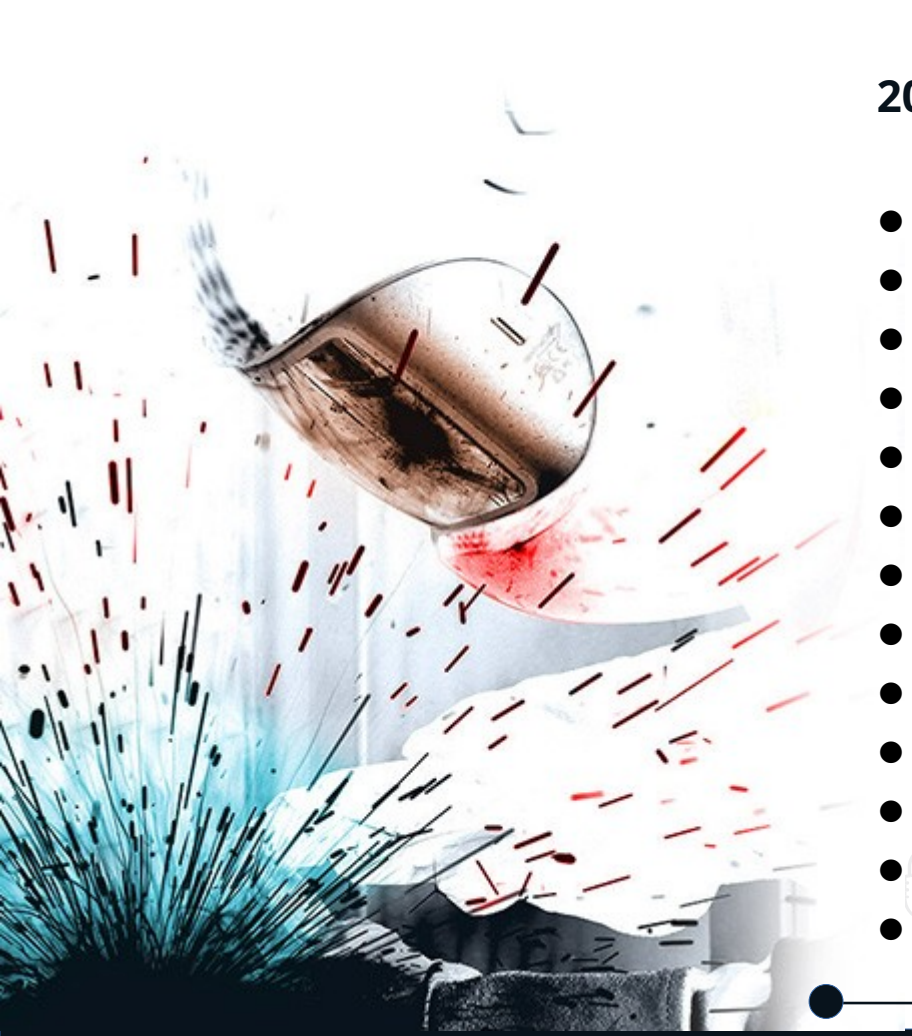
İNSAN HATASI

ÖNEMLİ NOTLAR

- Herkesin Mahremi vardır
- Siber Güvenlik Mümkündür
- Siber güvenlik yaşayan bir sistem olmalıdır

SİBER GÜVENLİK NOTLARI

Siber Güvenlik Teknolojileri

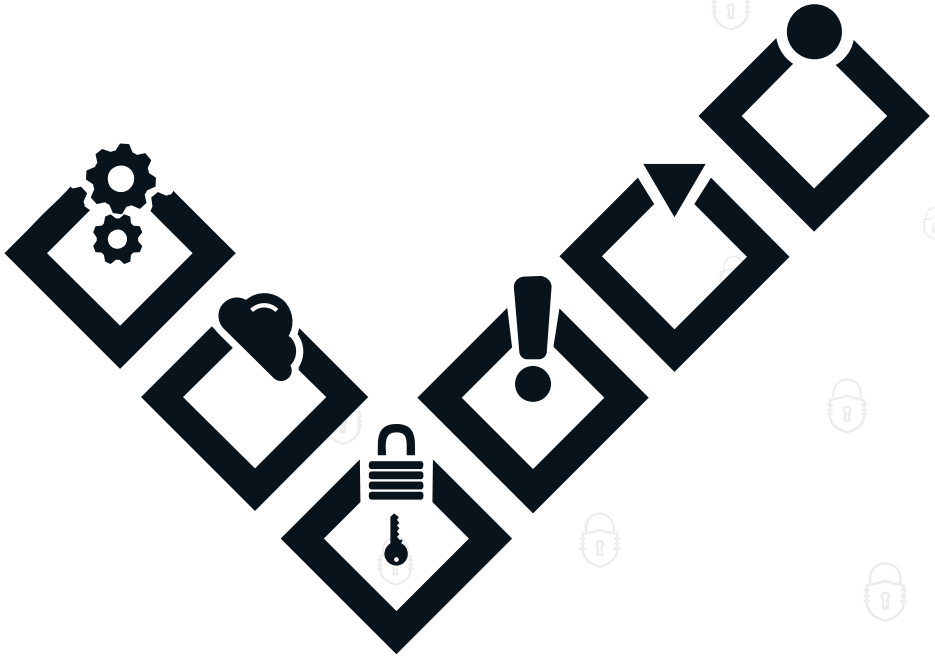


2024 Siber Güvenlik Teknolojileri/Trendleri

- Endpoint Detection and Response (EDR, XDR, NDR)
- Multi Factor Authentication (MFA, 2FA)
- Attack Surface Management (ASM)
- Web Application Firewall (WAF, ADC)
- Breach and Attack Simulation (BAS)
- Cyber Threat Intelligence (CTI)
- Zero Trust Network Access (ZTN, ZTNA)
- Secure Access Service Edge (SASE)
- Cybersecurity Mesh
- Artificial Intelligence
- Security Awareness
- Standarts and Frameworks
- Cyber Security Scoring

Standarts and Frameworks

- NIST CSF
- Mitre Att&Ck®
- ISO 27000 Family
- BİG Rehber
- Cobit 2019
- Center for Information Security (CIS)
- NIST SP 800-53
- NIST SP 800-171



TEŞEKKÜRLER