

Information Security on Digital World

18 May 2018

M. Bülent MUŞLU



bulentmuslu



BulentMuslu

Medium

Bulent Muslu



Agenda

1

About BKM

2

Cyber Security (Concepts, Threats, Risks, Preventions)

3

Cyber Crimes

4

How to Protect from CyberCrime

Section 1 : About BKM



Who is BKM ?

- The **Interbank Card Center (BKM)** was established in **1990** with the partnership of **13 public and private Turkish banks** for the purpose of providing solutions to the common problems and developing the rules and standards of credit and debit cards in Turkey, within the card payment system.
- The main activities of BKM are;
 - Carrying out the **authorization** operation between the banks,
 - Developing the procedures applicable to the banks in the credit card and debit card sector,
 - Forming the domestic rules and regulations,
 - Making efforts in relation to provision of standardization and taking the relevant decisions,
 - Establishing relations with the international organizations and commissions and representing the members
 - Executing the **ongoing bank operations from a single central operation site** in a more secure, fast and cost-effective manner
 - **BKM Express (e-Wallet),**
 - **Turkish Payment Systems – TROY**

Who is BKM ?

- In 1993,
- The Switch System was initiated with the aim of settling inter-bank domestic credit card and debit card authorization,
- Opening the ATM and POS system networks of the Turkish banks to the service of the customers, providing connection to the international communication networks such as Visa Base I and Europay EPS-NET from single point, and enabling clearing of the debit cards issued by the Turkish banks.
- Following activation of the advanced-technology-product second phase of BKM Switch System in 1999, the operational capacity was significantly increased compared to the former system and our members were provided with uninterrupted service with full productivity.

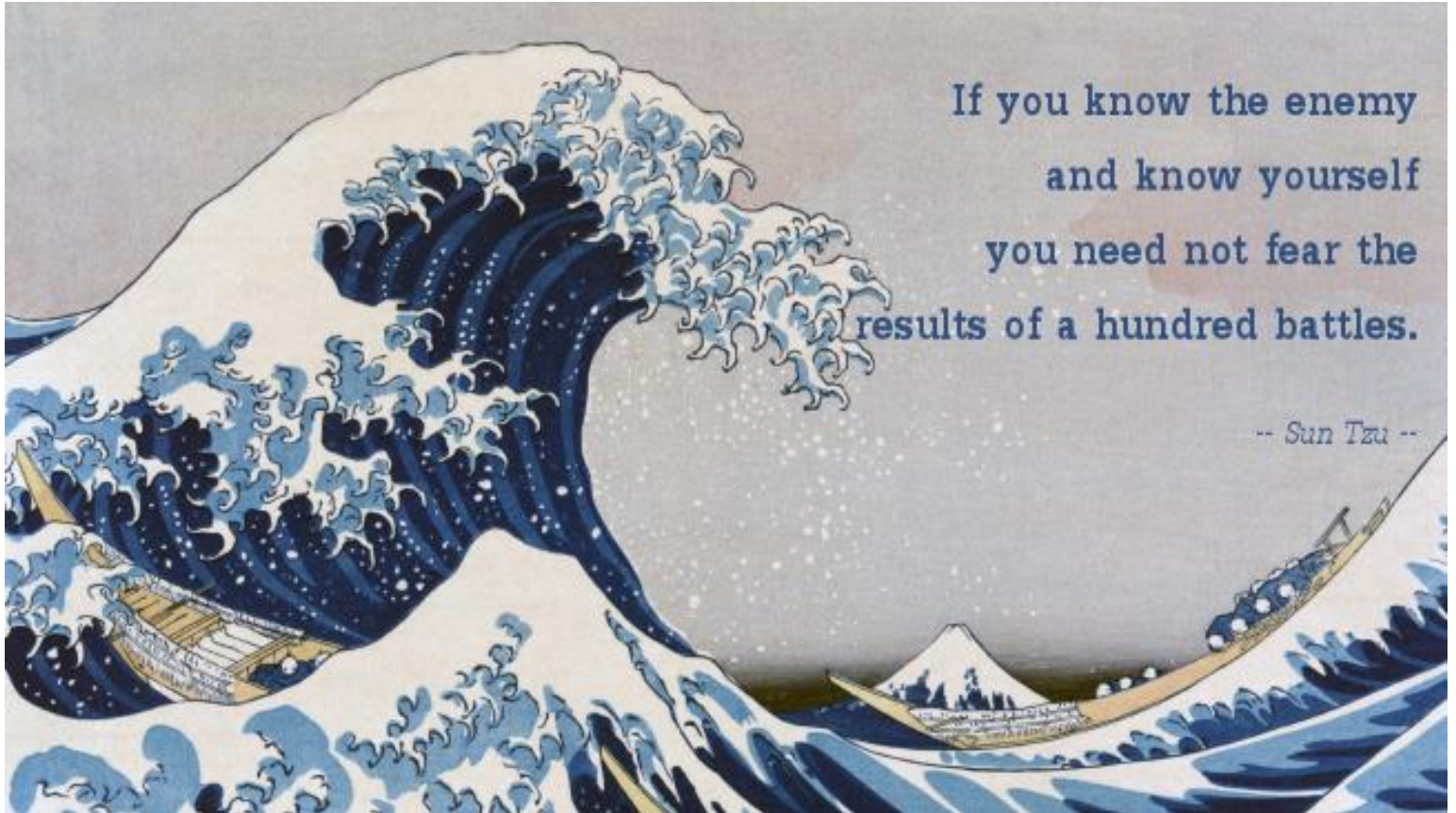
Section 2 :

Cyber Security

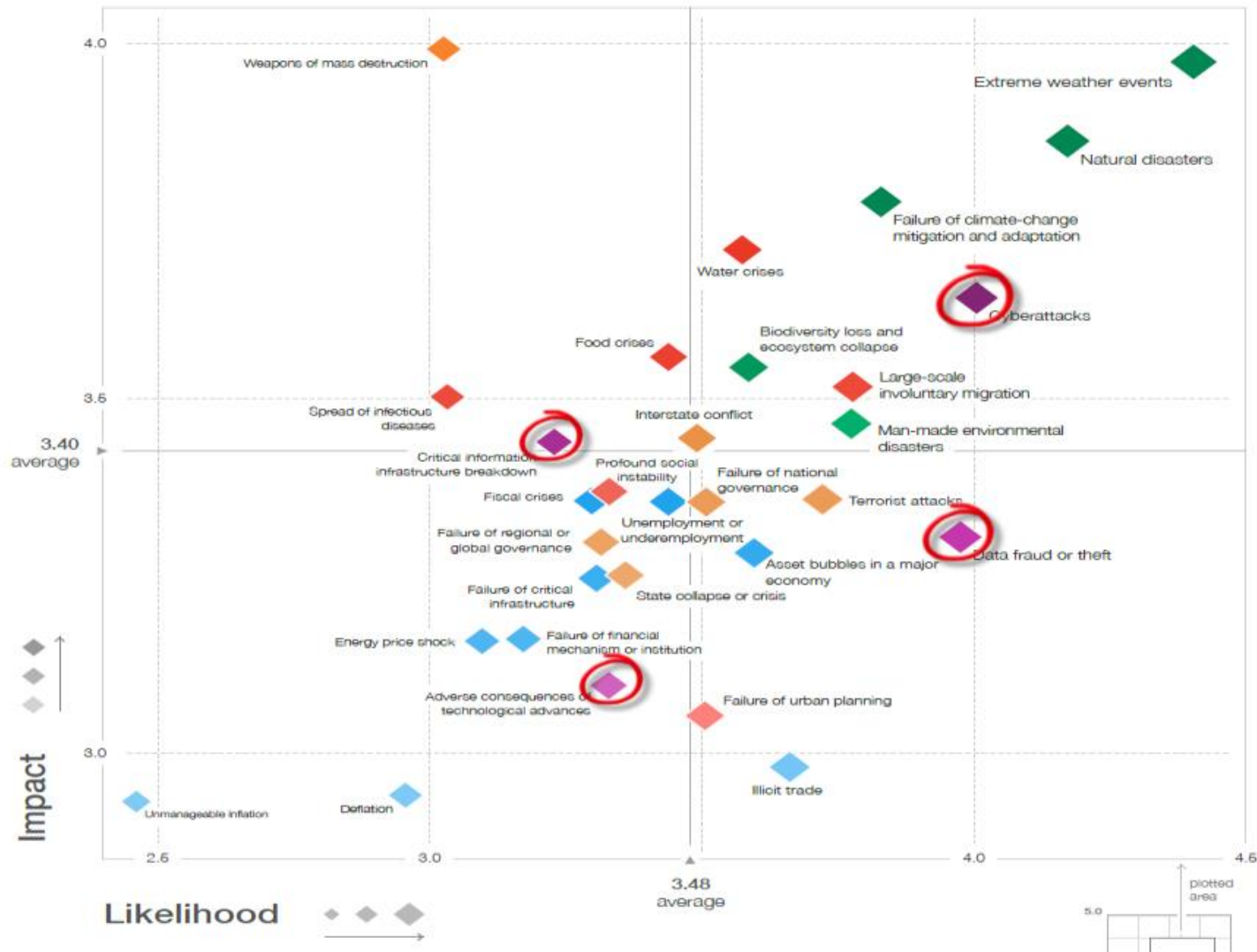
(Concepts, Threats,
Risks, Preventions)



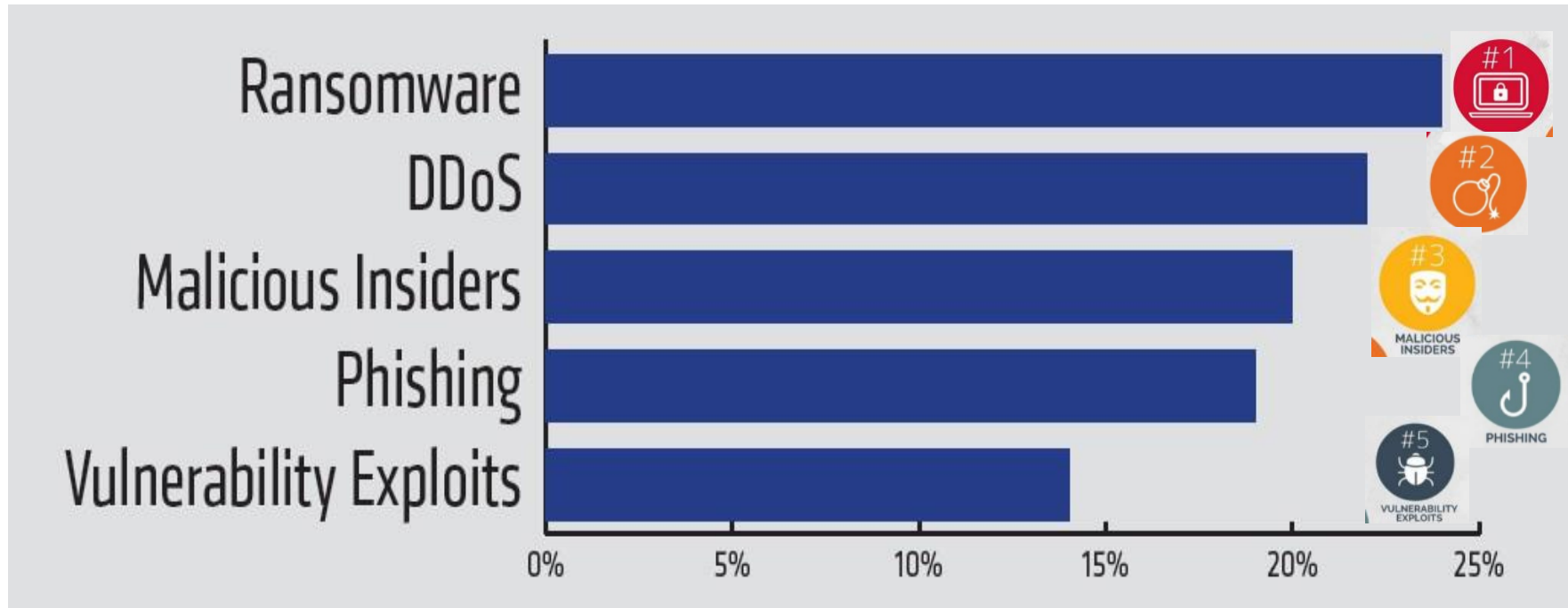
Know the enemy



The Global Risks Landscape 2018 - Technological Category

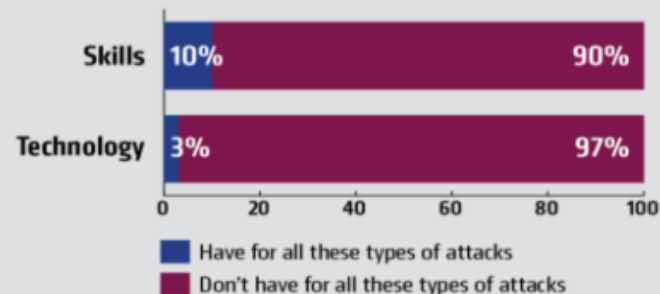


Cyber Security – Top 5 Cyber Threats - 2017

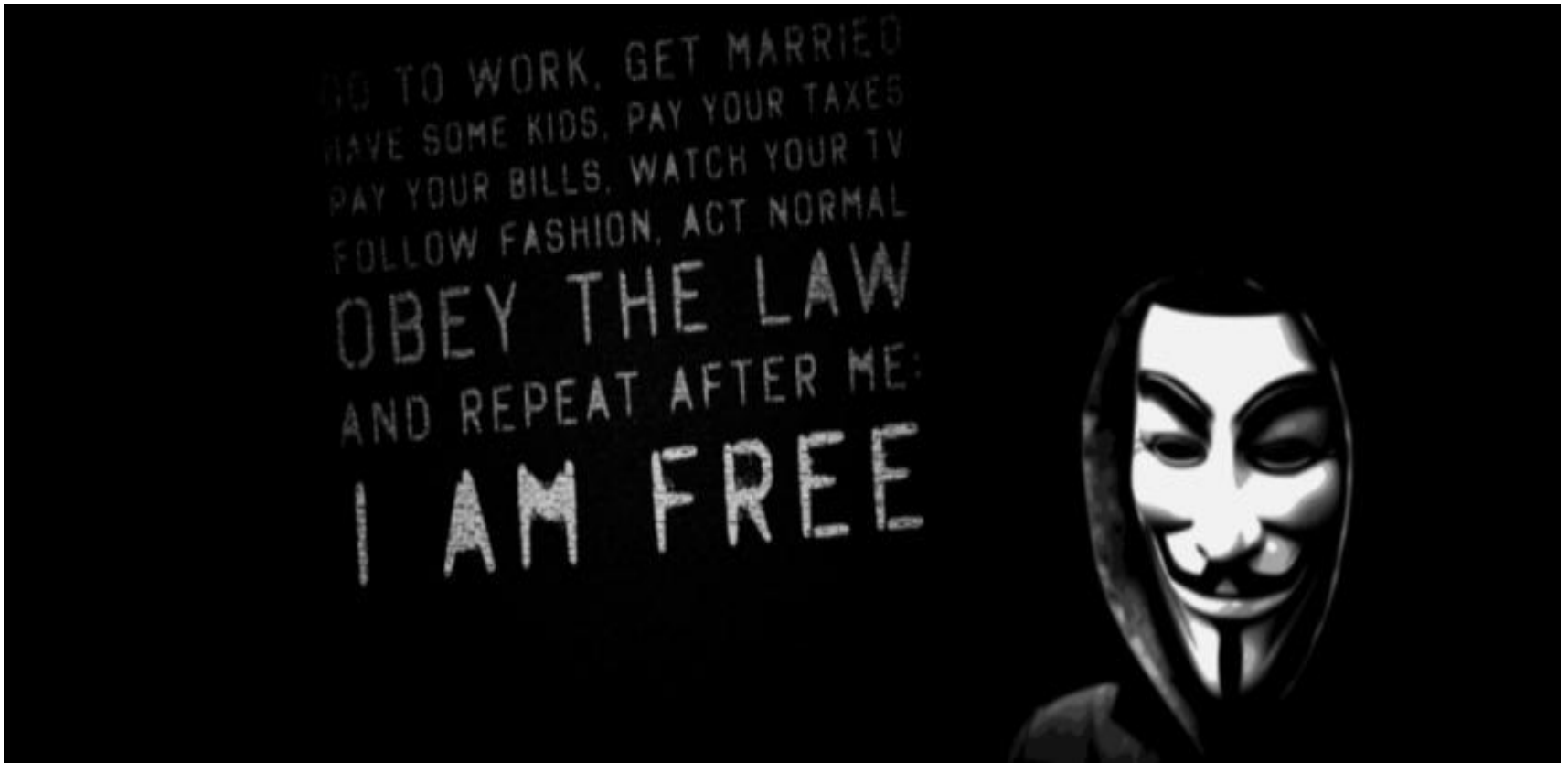


How prepared are organizations for those attacks?

90% lack the skills and 97% lack the technology to effectively address this full range attacks



Know the enemy



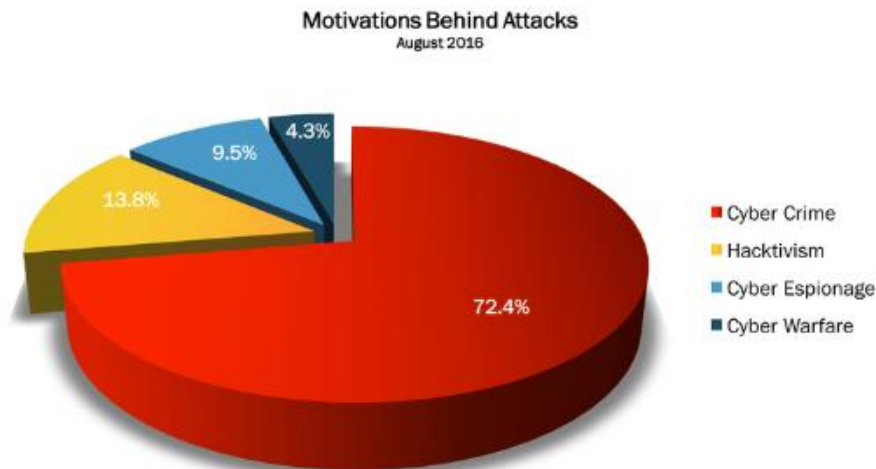
The Motivation Behind Targeted Cyber Attacks

Cyber Crime : When a cyber attack is used to steal money
(Siber saldırıların büyük bir çoğunluğu parasal kazanç amaçlı yapılıyor.)

Hactivism : When one uses cyber attacks to promote political agendas.

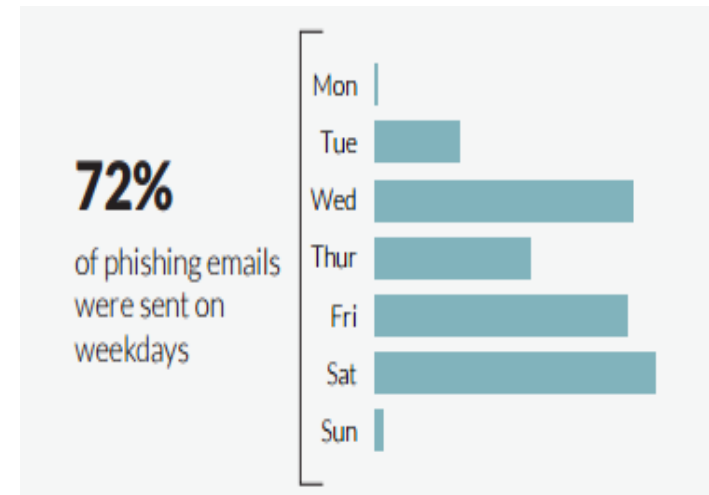
Cyber Espionage : When a cyber attack is used to steal specific information. (Kişilerin bilgilerine ulaşmak ve ülkeler arası mücadele amaçlı yapanlara da rastlanıyor.)

Cyber Warfare : When a cyber attack is used as a form of terrorism against a government. (Ulusal güvenlik ve ulusal çıkarlar)



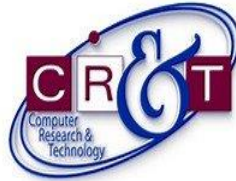
Social Engineering – Sosyal Mühendislik

- Phishing (Oltalama) : Bilindik sitelerin kopyalarını yaparak bu siteler üzerinden bilgi çalma.
- Bire-bir İkna : Telefon vs ile kullanıcıyla iletişime geçerek kişisel bilgilerin alınması
- Güven kazanarak bilgi edinmek : Bir başkası yerine geçerek, karşısındakinden bilgiler alma.



Ransomware (Fidye Yazılımları)

WANNACRY RANSOMWARE



WannaCry has been making headlines but ransomware is nothing new right? WannaCry is a much more aggressive variant. While you may be internet savvy, if a user on your network gets infected and your machine is not patched, you may get infected and encrypted as well.

CR&T recommend immediate patching of computers to protect against this particular variant and to test backup procedures as a more general protection against all types of encryption malware.



1 - A MALICIOUS EMAIL
An email either with a malicious attachment or linking to a malicious website is clicked by a user.



2 - INFECTION SPREADS

Most ransomware stops here and encrypts the user's computer. WannaCry instead uses a Windows Exploit to spread to other network computers. This exploit (CVE-2017-0144) affects from Windows XP through to Windows 10, including Windows Server editions. This means that one computer can encrypt the entire network, regardless of their permissions on other computers.



3 - ENCRYPTION BEGINS

The encryption routine can take as little as 28 seconds to encrypt a single computer.

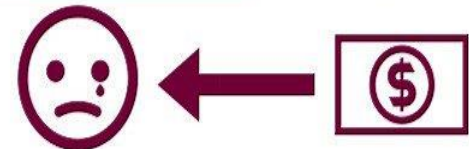


4 - RANSOM NOTE GIVEN



5 - PAY RANSOM OR RESTORE BACKUP

Along with security software and patch management, a strong backup practice is an essential part of ransomware prevention. In fact nowadays more backup restores are due to ransomware infections than traditional disaster recovery reasons.



SOURCES

<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

CREATED BY

David Graham - Computer Research & Technology (team@crt.net.au)

Ransomware – Computer

Hello Buddy! If you see this message all your important files are been crypted :)
What can you do? You can pay with bitcoin and wait 10 min for decryption!
It's very easy! Dont you know how to purchase bitcoin? www.localbitcoins.com it's your place!
If Antivirus block the crypter, you'll be unable to decrypt...
If is this your case, go to in any of this website:

<http://www.24honline3cdnrmny.onion.to>
<http://24honline3cdnrmny.onion.ru>
<http://24honline3cdnrmny.onion.link>

1) click on "Download for specific btc address"
2) insert the btc address, download
Thank you!

Your btc address is : 18QYWTBsq6MBmQ1AFwj8e18J7LXB2KUZkr

Hi Buddy!

Pay 0.40347888 to 18QYWTBsq6MBmQ1AFwj8e18J7LXB2KUZkr for decrypt your files

Ooops, your files have been encrypted!

English ▼



Payment will be raised on
5/16/2017 00:47:55

Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55

Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
GMT from Monday to Friday

You have 7

You must p

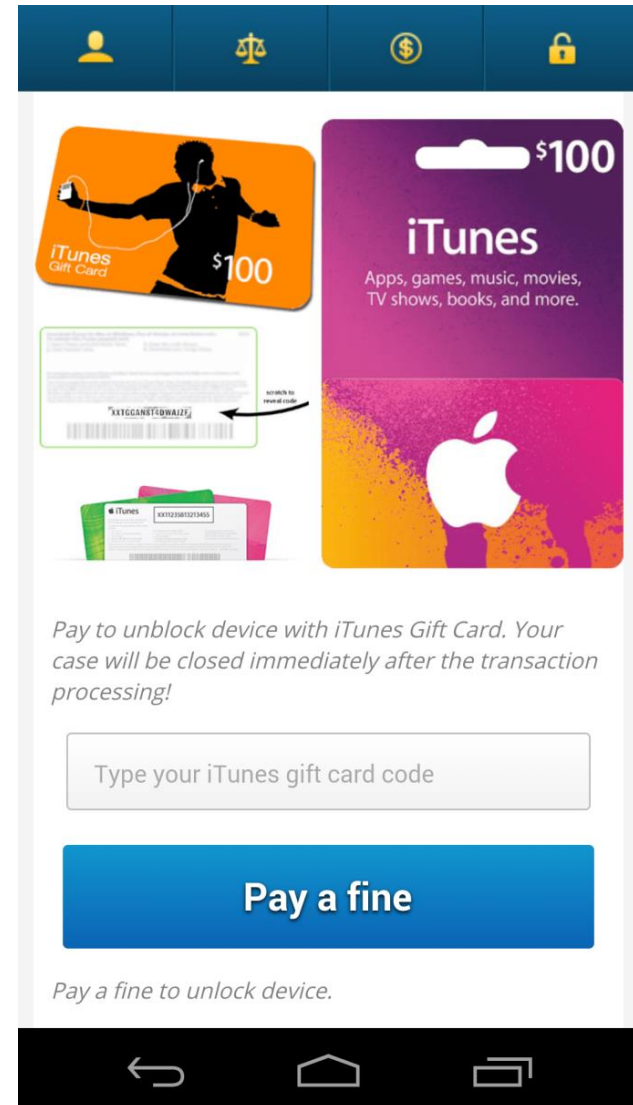
To pay the

located on

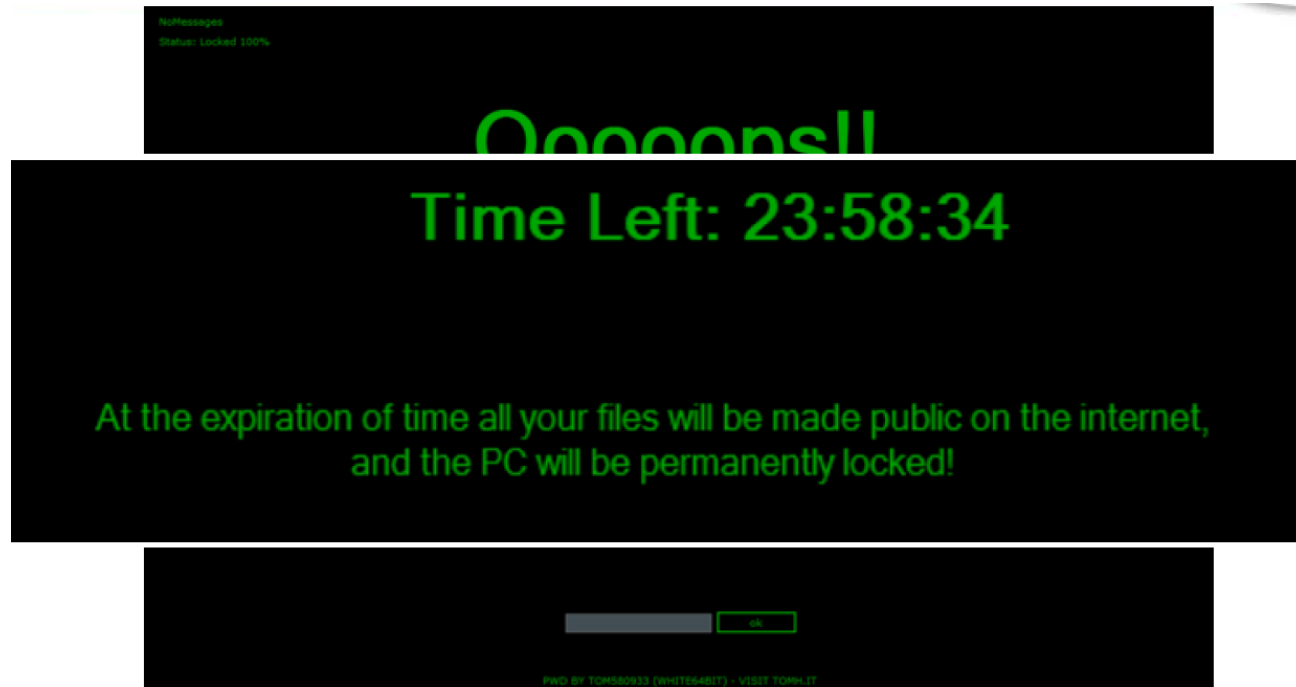
OK (if you l

OK)

Ransomware – Mobile



Ransomware – More examples



We will not respond immediatly. After we reply, you must send at least 10 nude pictures of you. After that we will have to verify that the nudes belong to you. Once you are verified, we will give you your unlock code and sell your nudes on the deep web



Ransomware – IoT Devices

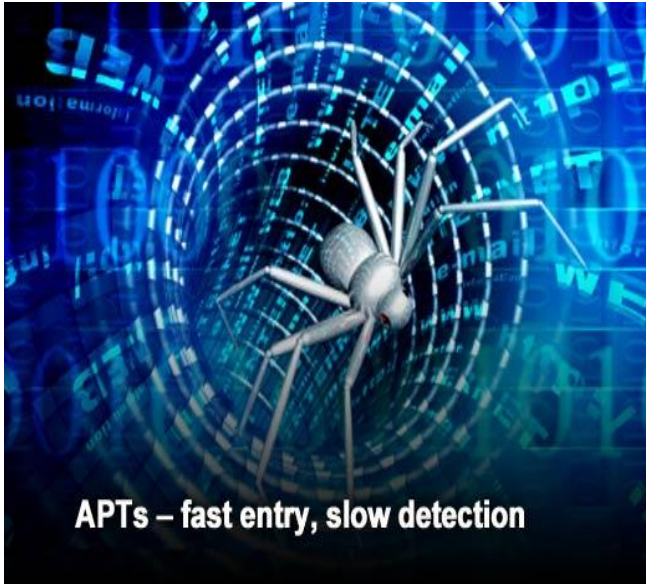


DDoS (Distributed Denial of Service Attack)



APT – Advanced Persistent Threat

- Türkçeye : Gelişmiş sürekli tehdit” veya “hedef odaklı saldırı” olarak çevrilen özel bir saldırı türüdür.
- Siber suçlular, Hacktivistler veya suç örgütlerinin motivasyon düzeyi : Birkaç deneme sonrası başka (kolay) hedefe yönelme
- APT saldırıları : Amaçlarına ulaşana kadar saldırmaya devam ederler.



APTs – fast entry, slow detection

Tehdit sınıflandırması


Basit tehdit: “wifi hackleme” ve “facebook patlatma” seviyesinde 1-2 kaynak okumuş “meraklı”, metodoloji bilmeyen, başlangıç seviyesi saldırganlardır.

Akıllı tehdit : Sürekli akıllı tehdit : İleri düzey teknik becerisi, hedef aldığı şirket veya kuruma sızmak için yürüttüğü sosyal mühendislik çalışmalarını yapan saldırganlardır.

İleri seviye tehdit : Sürekli İleri Seviye Tehdit : APT olarak adlandırdığımız tehdit türü (sürekli ileri seviye tehdit) en gelişmiş teknik beceri ve en yüksek seviyede motivasyon gerektiren saldırılardır.

2018 Cyber Security Predictions

1. **Ransomware** will be the most dangerous threat to businesses and organizations worldwide.
2. Cybercriminals focus on **cryptocurrencies**.
3. **APT groups** pressure will increase.
4. **Cloud security**, a top priority for enterprises
5. A joint **international effort** to fight the cybercrime
6. **IoT devices**, a privileged target of hackers
7. The rise of **Mobile threats**
8. **Cyberbullying** ... the emergency continues (Siber dünya kullanılarak birilerine ve özellikle çocuklara baskı kurma olayları daha fazla görülecek)
9. **Cyber-Insurance** proposal will explode
10. **GDPR**, many companies, will be not compliance with new EU regulation by the **deadline** (25.Mayıs.2018)

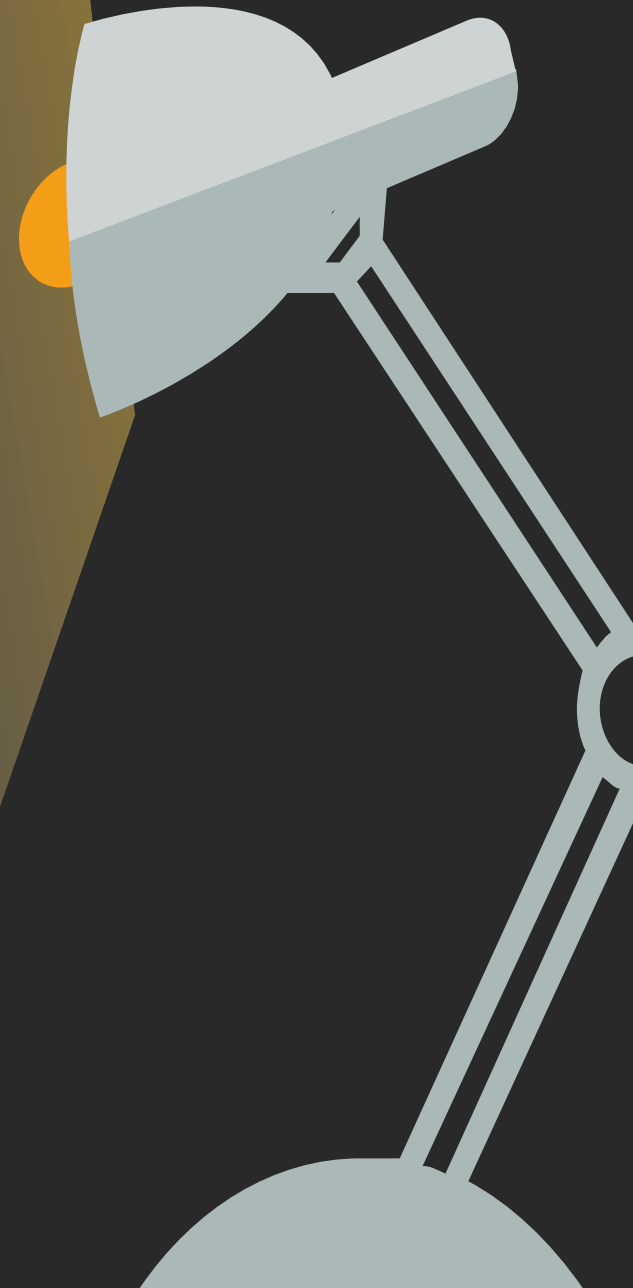


It takes 20 years to build a
reputation and five minutes to
ruin it. If you think about that
you'll do things differently.

Warren Buffett

Section 3:

Cyber Crimes



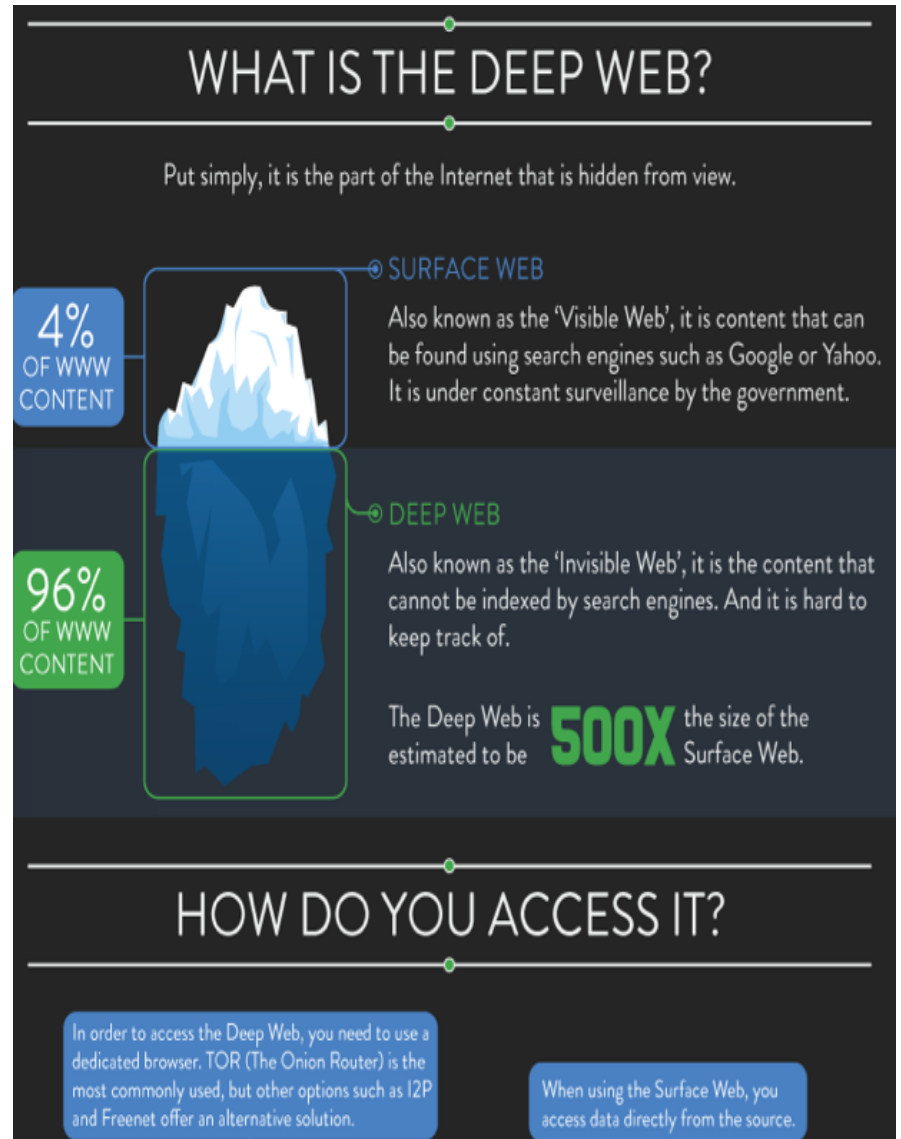
Web

Deep Web



Deep Web

- Arama motorlarının (**Google, Yandex, Bing, Yahoo**) internet arama sistemlerinin ulaşamayacağı internet siteleri ve içerikleri..
- Devlet kurumlarının, özel şirketlerin ve kişisel kullanıcıların, tüm kullanıcılara açık olmayan arama motorları tarafından **indexlenmeyen** verilerin ve sitelerin bütününe bulunduğu yer..
- Public erişim istenmeyen ya da illegal bilgilerin bulunduğu alandır.
- Kendi içinde katmanları vardır.



Dark Web – Dark Net

Deep Web içinde illegal içeriklerin bulunduğu alana **Dark Web** denir.

- *TOR Browser*
- *Illegal Information*
- *Drug Sales*

The screenshot shows the Silk Road anonymous market website. At the top, there's a navigation bar with a search bar, a login field, and a shopping cart icon. Below the navigation bar, there's a grid of product listings. Each listing includes a small image, a title, and a price. The products are categorized into Drugs, Apparel, Art, Books, Collectibles, Computer equipment, Custom Orders, Digital goods, Drug paraphernalia, Electronics, Erotica, Fireworks, Food, Forgeries, Hardware, Herbs & Supplements, Home & Garden, and Jewelry. The website has a dark theme with a green and black color scheme.

Silk Road
anonymous market

messages 1 | orders 0 | account \$0.00

Search Go

Hi logout

Shop by Category

- Drugs 4,093
 - Cannabis 999
 - Dissociatives 78
 - Ecstasy 314
 - Opioids 354
 - Other 153
 - Precursors 18
 - Prescription 903
 - Psychedelics 586
 - Stimulants 390
- Apparel 82
- Art 5
- Books 768
- Collectibles 15
- Computer equipment 42
- Custom Orders 27
- Digital goods 369
- Drug paraphernalia 153
- Electronics 35
- Erotica 296
- Fireworks 5
- Food 4
- Forgeries 55
- Hardware 1
- Herbs & Supplements 11
- Home & Garden 6
- Jewelry 57

5G Cocaine Pure Cristal Flakes \$41.94

[28.0G] High Quality Crystal Meth \$188.72

>>SPECIAL OFFER " BRAND SUBOXONE \$0.91

alprazolam [Xanax] 100 x 1mg \$11.31

News

- Closing the Armory
- A brand new look for Silk Road!
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes

Cocaine of high quality over 80% purity 25 gram \$190.12

"Ethyphenidate" -2,5g- of the best racemic HCl qit \$6.18

Colombian Cocaine Lady's and Gentleman 10G \$67.32

0.5g #3 Brown Heroin , good quality! \$7.52

SESAMPINO @ SILKROAD 25-02-2012

10 packs of shipped worldwide

MAGIC STONE

BIG PHISHAM "LEXIUM 600mg" (ALCALOID - MACDONIA)



Dark Web – Real World

Rent-A-Hacker

[Products](#) [FAQs](#) [Register](#) [Login](#)

Rent-A-Hacker

Experienced hacker offering his services!

(Illegal) Hacking and social engineering is my bussiness since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last +-20 years.

I have worked for other people before, now im also offering my services for everyone with enough cash here.

Prices:

Im not doing this to make a few bucks here and there, im not from some crappy eastern europe country and happy to scam people for 50 euro.

Im a professional computer expert who could earn 50-100 euro an hour with a legal job.

So stop reading if you dont have a serious problem worth spending some cash at.

Prices depend alot on the problem you want me to solve, but minimum amount for smaller jobs is 200 euro.

You can pay me anonymously using Bitcoin.

Technical skills:

- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successful, if i dont know it, ill learn it very fast
- Anonymity: noone will ever find out who i am.

Social Engineering skills:

- Very good written and spoken (phone calls) english and german.
- If i cant hack something technically ill make phone calls or write emails to the target to get the needed information, i have had people make things you wouldnt belive really often.
- Alot of experience with security practices inside big corporations.

What ill do:

Ill do anything for money, im not a pussy :) if you want me to destroy some bussiness or a persons life, ill do it!

Some examples:

Simply hacking something technically

Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.

Economic espionage

Getting private information from someone

Ruining your opponents, bussiness or private persons you dont like, i can ruin them financially and or get them arrested, whatever you like.

If you want someone to get known as a child porn user, no problem.

Product	Price	Quantity
Small Job like Email, Facebook etc hacking	200 EUR = 0.770 ₿	<input type="text" value="1"/> X Buy now
Medium-Large Job, ruining people, espionage, website hacking etc	500 EUR = 1.924 ₿	<input type="text" value="1"/> X Buy now

C – a – a – S - Crime as a Service

10- th version.

Packages:

â€¢ Minimum: DDoS Bot, no free updates, no modules = \$450

â€¢ Standart: DDoS Bot, 1 month free updates, password grabber module = \$499

â€¢ Bronze: DDoS Bot, 3 months free updates, password grabber module + free rebuilds = \$570

â€¢ Silver: DDoS Bot, 6 months free updates, password grabber module, + free rebuilds = \$650

â€¢ Gold: DDoS Bot, lifetime free updates, password grabber + "hosts" e

â€¢ Platinum: DDoS Bot, lifetime free updates, password grabber, unlimited free rebuilds, all

â€¢ Brilliant: DDoS Bot, lifetime free updates, unlimited free rebuilds, all

Other:

â€¢ ReBuild (URLs changing) â€" \$35.

â€¢ Sources - ~3500-5000\$, discuss individually

â€¢ New features - discuss individually.

â€¢ Web-Panel reinstalling (1st time is free) - \$50

Email Password Cracking made easy..!!

Request an E-mail Password :-

Fill in the below form to the best of your knowledge. email addresses are entered correctly. Once submitted for a confirmation mail. Add our email address(es) in your prevent our emails and the proofs landing in bulk folder the order by clicking on the confirmation link sent to your order.

Your Name

Your Email Address

Confirm your Email Address

Your Country

☐ Most Urgent ☐ Urgent ☐ Just do it whenever you can

Victim Name

Victim Email Address

Confirm Victim Email Address

Victim Country

Victim Language

CHEAP PROFESSIONAL DDOS SERVICE

Cheap Professional DDOS Service

Trusted

Strong/Fast Service

Takes down Large Website/Forum/Game Servers etc.

No time limit

PRICE

1 - 4 hours / 2\$ per hour

5 - 24 hours / 4\$ per hour

24 - 72 hours / 5\$ per hour

1 month / 1000\$ fix price

PAYMENT ACCEPTED

Paypal (Verified users only)

Liberty Reserve

Western Union

MoneyBookers

CONTACT

Yahoo Messenger :

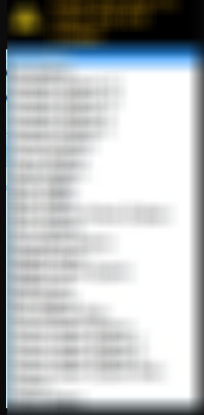
Msn :

Skype :

Deep Web – Forum Örnek

12 Farklı Büyük **Sigorta** Şirketinin Erişim Bilgileri

Konumuzda belirttiğimiz 12 firmanın satışını tekli satıştan toplu satışa geçirmiş bulunmaktayız.



İçerisinde 50 milyondan daha büyük bir data barındırmaktadır. Sistem 7/24 Günceldir. Dün doğan bebeği bile TC ile bulmanız mümkündür Aynı zamanda Tramer ve Mernis sistemide yanında verilmektedir. Sisteme girişler lisans anahtarı ve kişiye özel şifreler ile yapılmaktadır.

-Herkes ayrı şifre verilecektir.

Programa giriş yapıldıktan sonra şirketin ismine tıklayıp giriş butonuna basmanız yeterlidir. Her şirketin Müşteri Sorgusu mevcuttur. Aradığınız bir kişiyi en kolay nasıl bulabileceğiniz hakkında detaylı bilgi tarafımızca ICQ üzerinden verilecektir.

Teknik destek sağlanacaktır.

Tramer sistemi içinden Hasarlı araç sorgulama, plaka sorgulama tarzı istediğiniz her işlemi gerçekleştirebilirsiniz. Kafanıza koyduğunuz bir ismi bulmanız 3 dakikadan fazla sürmeyecektir.

Plaka yazarak TRde bulunan tüm araçları öğrenebilirsiniz ve detaylı kimlik bilgilerine rahatlıkla erişebilirsiniz.

Genel olarak bilgiler;

Ad, Soyad, Tc, Ana adı, Baba adı, Doğum Yeri, En güncel adresi, Telefon numarası, Kredi kartının ilk 8 ve son 4 hanesi, üzerine olan araç bilgileri vs.

Şeklinde listelenir. Dataların pek çoğu XML, PDF olarak çıkartılabilir. Şirketlerin tanesine günlük 500'e yakın yeni kişi eklenir ve bitmek üzere olan poliçeleri görebilirsiniz.

Bu sistemi kullanarak 3d gereksinimi olmadan istediğiniz kadar sigorta yapabilirsiniz.

C – a – a – S - Crime as a Service

- Although priced in U.S. dollars, payments are often made using cryptocurrencies, such as Bitcoin or Monero, at the daily exchange rate equivalent values.
- These prices are taken from publicly accessible underground forums and dark web TOR sites. Closed, private forums tend to have even lower prices.
- We cannot verify if the goods are genuinely sold for the asked price, some of them might be fake offers.


2018 Pricelist – Credit Cards

Single credit card	\$0.50-25
Single credit card with full details (Fullz)	\$1-40
Dump of magnetic strip track1/2 data (e.g. from skimming)	\$20-60
500 credit cards already used for fraud in the last week	\$1

Dumps	Estimate of Prices (without PIN, with PIN, PIN and good balance)									
	US		EU			CA, AU		Asia		
Visa Classic	\$15	\$80	\$40	\$150		\$25	\$150	\$50	\$150	
Master Card Standard	\$90		\$140			\$150		\$140		
Visa Gold/Premier	\$25	\$100	\$200	\$45	\$160	\$250	\$30	\$160	\$55	\$150
Visa Platinum	\$30	\$110		\$50	\$170		\$35	\$170	\$60	\$170
Business/Corporate	\$40	\$130		\$60	\$170		\$45	\$175	\$70	\$170
Purchasing/Signature	\$50	\$120		\$70			\$55		\$80	
Infinite				\$130	\$190		\$60	\$200		\$190
Master Card World	\$140									
AMEX	\$40			\$60			\$45		\$70	
AMEX Gold	\$70			\$90			\$75		\$100	
AMEX Platinum	\$50									

C – a – a – S - Crime as a Service

• 2018 Pricelist – Services

- 
- A man with a beard and a dark hoodie is pointing his right index finger directly at the camera. The background is a dark green field filled with glowing green digital code, resembling a computer screen or a data center. The word 'password' is visible in green text on the right side of the image.
- DDoS service, short duration <1 hour, medium protected targets \$5-20
 - DDoS service, duration >24 hours, medium and strong protected targets \$10-1000
 - Hacker for hire \$100+
 - Credit score repair \$50
 - Messing up peoples online presence \$500
 - Airplane ticket and hotel bookings 10% of value

C – a – a – S - Crime as a Service

Accounts (User Name and Password)

Video and sound streaming accounts	\$0.10-10
Various services, more than 120+ available (gaming, food, shopping, etc.)	\$0.5-10
Online banking accounts	0.5-10% of value
Online money accounts (depending on value and verification)	\$10-100
Retail shopping account	\$5-50
Cloud accounts	\$5-10
Hacked Gmail accounts	\$0.1-5
500,000 email accounts with passwords from data breaches	\$90
Hotel loyalty/reward program accounts with 100,000 points	\$10-20
Shopping loyalty accounts with cash points	\$2-7
VPN services	\$1-10
Online retailer gift cards	15-50% of face value
Restaurant gift cards	15-40% of face value

	Min Price	Max Price
Brazzers		\$1
Yahoo	\$0,7	\$1,2
Gmail	\$0,7	\$1,2
Dell	\$0,8	\$2
Uber	\$1	\$2
NetFlix	\$1	\$2
Walmart		\$2,5
Twitter	\$0,1	\$3

Section 4:

How to Protect from CyberCrime



Shore up weak points

Password :

- Use a different password for each site
- Use Longer Passwords
- Use 2 Step Verification



Asset Management :

- You cannot secure unknown.

Protect your data

Regulations:

- ISO 27001
- PCI/DSS
- COBIT
- Etc.



Tokenization Technology

Substituting a sensitive [data element](#) with a non-sensitive equivalent.



Encryption

Encryption prevents unauthorised access to your data by keeping communication secure between the parties involved.



Educate employees

You cannot patch human :

- Take users phishing!
- Is the sender also the receiver?
- Hack yourself... Ethically.
- Passwords, passwords, passwords...
- Think before you link!
- Create an accessible cyber security plan.





B K M
BANKALARARASI
KART MERKEZİ

Thank you
Teşekkürler
Təşəkkür edirəm



bulentmuslu

Linked in

BulentMuslu

Medium

Bulent Muslu