Threat

Malware, Infrastructure, Social Engineering

Malware

- Malware is a malicious software that **damages or disables computer systems** and **gives limited or full control** of the systems to the malware creator for the purpose of theft or fraud

Examples of Malware

1. Trojan Horse
2. Backdoor
3. Rootkit
4. Ransomware
5. Adware
6. Virus
7. Worms
8. Spyware
9. Botnet
10. Crypter

Malicious Software / Malware

- Software yang dirancang untuk merusak atau mengambil akses komputer tanpa sepengetahuan pengguna
- Menjadi istilah umum untuk menyebut aplikasi jahat:
  - Virus, worms, trojan, ransomware, spyware, botnet, dll
- Beberapa mudah dideteksi, tetapi ada yang menyamar, hingga sulit terdeteksi

WORMS
VIRUS
TROGAN
RANSOMWARE
MALWARE TYPES
Explained
ADWARE
BOTS
SPAM
SPYWARE

Antivirus Tradisional Tak Sigap Perangi "Cyber Attack"

Kompas.com - 06/11/2016, 14:04 WIB

BAGIKAN:

Komentar

Dok.Wahab Yusoff, ASEAN Vice President and General Manager, Palo Alto Networks.

Editor:Reska K. Nistanto

KOMPAS.com - Produk-produk antivirus tradisional dirasa tidak cukup sigap dalam mengimbangi serangan siber yang semakin canggih. Untuk itu, perusahaan keamanan internet, Palo Alto merilis Traps, *advanced endpoint protection* ke pasar Indonesia, Kamis (3/11/2016).

Software Traps dipersenjatai dengan beragam fungsionalitas, salah satunya adalah kapabilitas *machine learning* untuk menangkal *unknown malware* secara *real-time*.

Traps dengan segala fungsionalitasnya mendukung perusahaan memangkas kebutuhan untuk pengadaan produk-produk antivirus biasa untuk perlindungan *endpoint,* seperti laptop, server, maupun *virtual desktop infrastructure* (VDI) yang terdapat di lingkungan IT mereka.

"Banyak perusahaan yang sudah memasang produk keamanan maupun *software agents* pada *sistem endpoint* mereka. Kendati demikian, di sisi lain, upaya pembobolan keamanan dan serangan siber justru tercatat meningkat, baik dari sisi jumlah, varietas, maupun tingkat kecanggihannya," kata Wahab Yusoff, ASEAN Vice President and General Manager, Palo Alto Networks.

"Produk-produk antivirus tradisional dirasa tidak cukup sigap untuk mengimbanginya dan selalu gagal dalam menangkal ragam serangan seperti ini yang dibidikkan langsung ke *endpoints*," imbuh Wahab dalam keterangan tertulisnya kepada *KompasTekno*, Minggu (6/11/2016).

Deskripsi Malware VPN Filter

VPNFilter malware adalah multi-stage malware yang memiliki kemampuan untuk mengumpulkan data/intelijen dan operasi serangan siber yang bersifat destruktif yang menginfeksi perangkat jaringan SOHO (*Small Office and Home Office*) dan NAS (*Network Attached Storage*). Perangkat jaringan tersebut rentan terhadap infeksi malware ini karena pada umumnya tidak dilengkapi dengan sistem keamanan tambahan (seperti anti-malware atau perangkat IPS (*Intrusion Prevention System*)). Sekitar 500.000 router di 54 negara terdampak oleh malware ini, termasuk Indonesia.

VPNFilter

BADAN SIBER DAN SANDI NEGARA

VPNFilter malware adalah multi-stage malware yang memiliki kemampuan untuk mengumpulkan data/intelijen dan operasi serangan siber yang bersifat destruktif yang menginfeksi perangkat jaringan SOHO (Small Office and Home Office) dan NAS (Network Attached Storage). Perangkat jaringan tersebut rentan terhadap infeksi malware ini karena pada umumnya tidak dilengkapi dengan sistem keamanan tambahan (seperti anti-malware atau perangkat IPS (Intrusion Prevention System)). Sekitar 500.000 router di 54 negara terdampak oleh malware ini, termasuk Indonesia.

Timeline VPNFilter

Cisco Talos Intelligence mengobservasi aktifitas infeksi malware VPNFilter	8 MEI
Cisco Talos Intelligence mendeteksi adanya korban VPNFilter yang berlokasi di Ukraina	17 MEI
Talos Intelligence rilis artikel "New VPNFilter malware targets at least 500K networking devices worldwide"	23 MEI
Symantec Threat Intelligence memuat laporan "VPNFilter: New Router Malware with Destructive"	23 MEI
FBI merilis Pengumuman mengenai "Foreign Cyber Actors Target Home And Office Routers And Networked Devices Worldwide"	25 MEI

referensi

[1] New VPNFilter malware targets at least 500K networking devices worldwide. https://blog.talosintelligence.com/2018/05/VPNFilter.html, Dimuat tanggal 25 Mei 2018

[2] VPNFilter: New Router Malware with Destructive Capabilities. https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware. Dimuat tanggal 25 Mei 2018

[3] Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide. https://www.ic3.gov/media/2018/180525.aspx, Dimuat tanggal 25 Mei 2018

DAMPAK MALWARE

BADAN SIBER DAN SANDI NEGARA

- Perangkat yang terinfeksi dapat digunakan sebagai media serangan atau "hop points" oleh pihak pembuat malware (aktor penyerang) untuk terkoneksi ke target korban, guna mengaburkan sumber asal serangan.
- Malware ini juga memiliki kemampuan untuk melakukan pengumpulan, pencurian informasi dan memonitor arus informasi jaringan yang dilewatkan melalui router yang terinfeksi.
- VPNFilter memiliki kemampuan "destruktif" yang dapat menyebabkan router skala "Small Office and Home Office" (SOHO) tidak dapat beroperasi.

DAFTAR PERANGKAT YANG TERDAMPAK

LINKSYS	MIKROTIK	NETGEAR
- E1200, - E2500 dan - WRVS4400N	Versi MIKROTIK ROUTEROS untuk CLOUD CORE ROUTERS (CCR) - 1016, - 1036, dan - 1072	- DGN2200, - R6400, - R7000, - R8000, - WNR1000, dan - WNR2000
QNAP	**TP-LINK**	
- TS251, - TS439 Pro, - QNAP NAS model yang menggunakan QTS 4.2.6 build 20170628, 4.3.3 build 20170703, dan versi sebelumnya	- R600VPN	

REKOMENDASI PENCEGAHAN

BADAN SIBER DAN SANDI NEGARA

1. BACKUP KONFIGURASI PERANGKAT

Melakukan backup seluruh konfigurasi pada perangkat sebelum melakukan proses reboot, factory reset maupun pemutakhiran firmware pada perangkat.

2. FACTORY RESET & REBOOT PERANGKAT

Melakukan factory reset dan reboot perangkat router yang digunakan untuk mengganggu proses kerja malware.

3. NON-AKTIFKAN FITUR REMOTE MANAGEMENT

Jika tidak diperlukan, non-aktifkan fitur konfigurasi melalui remote (remote management settings) pada perangkat.

4. GUNAKAN PASSWORD YANG KOMPLEKS

Gunakan password dengan kompleksitas yang baik (seperti panjang password lebih dari 8 karakter, kemudian karakter password terdiri dari kombinasi angka, huruf besar, huruf kecil, simbol dan karakter lainnya) untuk melakukan akses ke perangkat, serta non-aktifkan / hapus / ubah password untuk seluruh akun default

5. UPDATE FIRMWARE PERANGKAT

Lakukan pemutakhiran terhadap firmware perangkat yang terdampak ke versi terbaru jika tersedia

Recycle Bin
VeryFun
start
11:16 PM

WSJ

Malware Programmers develop and use it to:

- Attack browsers and track websites visited
- Affect system performance, making it very slow
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in the substantial data losses
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Get into a system using:

01	Instant Messenger applications
02	Portable hardware media / removable devices
03	Browser and email software bugs
04	Insecure patch management
05	Rogue / decoy applications
06	Untrusted sites and freeware web applications/ software
07	Downloading files from Internet
08	Email attachments
09	Network propagation
10	File sharing services (NetBIOS, FTP, SMB)
11	Installation by other malware
12	Bluetooth and wireless networks

Malware | Trojan

1. It is a program in which the **malicious or harmful code** is contained inside apparently harmless programming or data in such a way that it can **get control and cause damage**, such as ruining the file allocation table on your hard disk

2. Trojans get activated upon **users' certain predefined actions** and upon activation. It can grant attackers unrestricted access to all data stored on compromised information systems and can cause potentially immense damage

3. Indications of a Trojan attack include **abnormal system and network activities** such as disabling of antivirus, redirection to unknown pages, etc.

4. Trojans **create a covert communication channel** between the victim computer and the attacker for transferring sensitive data

private string FindContributorName(string Html)
{
string Pattern = "class=\"avatar \" alt=\"";
int SectionStart = Html.IndexOf(Pattern);
if (SectionStart != -1)
{
SectionStart += Pattern.Length;
int NameStart = SectionStart;
int NameEnd = Html.IndexOf("\"", SectionStart);
if (NameStart != -1 && NameEnd != -1 && NameEnd > NameStart)
{
string Name = Html.Substring(NameStart, NameEnd -
return Name;
}
else
{
logger.AddLine("Contributor Name wasn't
}
}
return "";
}

Wrapper

A wrapper binds a Trojan executable with an innocent looking .EXE application such as games or office applications
When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs the wrapping application in the foreground
The two programs are wrapped together into a single file
Attackers might send a birthday greeting that will install a Trojan as the user watches, for example, a birthday cake dancing across the screen
Chess.exe
File size: 90K
Trojan.exe
File size: 20K
Chess.exe
File size: 110K

FTP Trojan

Hacker

Send me
c:\creditcard.txt file

Here is the requested file

Victim

(FTP Server installed in the background)

FTP Server

```
Volume in drive C has no label.
Volume Serial Number is D45E-9FEE Directory of C:\
06/02/2014 1,024 .rnd
09/06/2014 0 abc.txt
08/24/2014 <DIR> AdventNet
05/21/2014 0 AUTOEXEC.BAT
05/21/2014 0 CONFIG.SYS
06/04/2014 <DIR> Data
08/11/2014 <DIR> Documents and
```

FTP Trojan: TinyFTPD

FTP Trojans install an FTP server on the victim's machine, which opens FTP ports

An attacker can then connect to the victim's machine using FTP port to download any files that exist on the victim's computer

Command Prompt

```
C:\Documents and Settings\Admin\Desktop\TinyFTPD 21 55555 test test c:\
win98 all RWLCD
Tiny FTPD V1.4 By WinBggDrop
FTP Server Is Started
ControlPort:      21
BindPort:         55555
UserName:         test
Password:         test
HomeDir:          c:\win98
Allowd IP:        all
Local Address:    192.168.168.16
ReadAccess:       Yes
WriteAccess:      Yes
LIstAccess:       Yes
CreateAccess:     Yes
DeleteAccess:     Yes
ExecuteAccess:    Yes
UnlockAccess:     No
AnonymousAccess:  No
Check Time Out Thread Created Successfully
*************** Waiting For New Connection ***************
0 Connection Is In Use
```

VNC Trojan

VNC Trojan starts a VNC Server daemon in the infected system (victim)
Attacker connects to the victim using any VNC viewer
Since VNC program is considered a utility, this Trojan will be difficult to detect using anti-viruses
Command and control instruction
VNC Traffic
Attacker
Victim
VNC Server

Remote Access Trojan (RAT)

- This Trojan works like a **remote desktop access**
- Hacker gains complete **GUI access** to the remote system

1. Infect (Rebecca's) computer with **server.exe** and plant Reverse Connecting Trojan
2. The Trojan connects to **Port 80** to the attacker in Russia establishing a reverse connection
3. Jason, the attacker, has **complete control** over Rebecca's machine

Optix Pro

MoSucker

ProRat

Theef

Malware | Virus

- A virus is a **self-replicating program** that produces its own copy by attaching itself to another program, computer boot sector or document
- Viruses are generally transmitted through **file downloads**, **infected disk/flash drives** and as **email attachments**

Characteristics of Viruses

- Infects other programs
- Transforms itself
- Encrypts itself
- Alters data
- Corrupts files and programs
- Self-replication

Purpose of Creating Viruses

- Inflict damage to competitors
- Financial benefits
- Vandalism
- Playing a prank
- Research projects
- Cyber terrorism
- Distribute political messages
- Damage network or computers
- Gain remote access of the victims computer

Virus

- Program yang menempel di program lain (usually trusted)
- Memiliki muatan (*payload*) yang berbahaya
- Replikasi perlu inang → OS-Oriented / Apps-Oriented
  - Menemukan koneksi jaringan; menyalin dirinya sendiri ke host lain di jaringan
    - Membutuhkan keterampilan pemrograman

  ATAU

  - Dikirimkan ke semua orang di daftar email host
    - Membutuhkan lebih sedikit keterampilan pemrograman

Worms

- *Standalone*
- Replikasi diri
- Seperti virus, sering bertukar istilah dengan virus
- Menyebar dengan cepat (*sleek*)
  - Tidak perlu host
  - Tidak perlu eksekusi user
  - Diprogram untuk menyebar melalui jaringan / email
- Memanfaatkan ***bug*** untuk membuat backdoor, botnets

Ransomware

- Mengambil alih sistem / file pribadi dan meminta tebusan
  - Pop-up banners
  - Sistem terkunci
  - Data dienkripsi
- Kasus pertama di 1980 → pembayaran via pos
- Saat ini masih marak
  - Penyebaran email, spam, pdf, word, pictures from internet
  - Pembayaran CC / Bitcoin

Cryptolocker 2.0
Your personal files are encrypted
Your files will be lost without payment on:
11/24/2013 3:16:34 PM
Info
Your important files were encrypted on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.
Encryption was produced using unique public key RSA-4096 generated for this computer. To decrypt files, you need to obtain private key.
The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files.
To retrieve the private key, you need to pay 0.5 bitcoins.
Click proceed to payment to obtain private key.
Any attempt to remove or damage this software will lead to immediate private key destruction by server.
See files
<< Back
Proceed to payment >>

CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, video, documents, etc. HERE is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key wich will allow you to decrypt the files is on a secret server on the internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR similar amount in another currency.
Click Next>> to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to immediate destruction of the private key by server.
Time left
4 d. 23 : 58 : 48
Next >>

Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain a private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files.
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 5 Bitcoin to
ATTENTION!
Private key will be destroyed on 2014-02-15 [00:43:09]
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Time left
71:59:16
Your Keeper ID
SEND

CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a performance list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; After the time specified in this window, the cost of data recovery will be increased 2 times.
In a month, the private key will be automatically deleted from the secret server. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 600 USD / 600 EUR / similar amount in another currency.
Click "Next" to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Price will be increased by 2 times
Time left
95:58:04

GOV-CSIRT INDONESIA

Beranda | Gov-CSIRT Indonesia | CSIRT Organisasi Sektor Pemerintah | Layanan | Event | Hubungi Kami

Home » Peringatan Keamanan Siber » Hati-hati! Serangan Ransomware Wannacry Belum Berakhir

Hati-hati! Serangan Ransomware Wannacry Belum Berakhir

Peringatan Keamanan Siber

Serangan WannaCry di Indonesia Terbesar Kedua di Dunia

Muhammad Alif Goenawan - detikInet

Minggu, 06 Mei 2018 12:40 WIB

1 komentar

SHARE

13
05-2017

284333

Himbauan Agar Segera Melakukan Tindakan Pencegahan Terhadap Ancaman Malware Khususnya Ransomware Jenis WannaCRY

SIARAN PERS NO. 55/HM/KOMINFO/05/2017

Kategori Siaran Pers

Non-standardized Naming Scheme

Antivirus	Result	Update
AhnLab-V3	Win32/Kido.worm.167698	20120502
AntiVir	Worm/Conficker.Z.43	20120502
Antiy-AVL	Worm/Win32.Kido.gen	20120503
Avast	Win32:Rootkit-gen [Rtk]	20120502
AVG	Worm/Downadup	20120502
BitDefender	Worm.Generic.41342	20120503
ByteHero	-	20120502
CAT-QuickHeal	Win32.Worm.Conficker.B.3	20120502
ClamAV	Trojan.Dropper-18535	20120503
Commtouch	W32/ConfickerIGeneric	20120503
Comodo	NetWorm.Win32.Kido.A	20120502
DrWeb	Win32.HLLW.Shadow.based	20120503

Vendor Naming Convention

- Computer Antivirus Research Organization (CARO) Malware Naming Scheme
  - Microsoft, F-Secure

Vendor	Name Convention	Example
Symantec	Prefix.Name.Suffix	Infostealer.Banker.C
Avira	Prefix:Name [Type]	Win32:Zbot-BS [Trj]
Kaspersky	[Prefix:]Behaviour.Platform.Name[.Variant]	Trojan.Win32.Genome.taql

Backdoor
Spyware
adware
….

Tugas & Demo

- Nonton video - Cisco Cyberops Associate - Lab 27.2.15: Investigating a Malware Exploit
- Klasifikasi jenis virus Anda di website yang ada dalam video
- Demo malware di kelas

Demo

- Isolated lab
  - **Physical machines**: Deep Freeze, FOG/Freeghost
  - **Virtual machines**: VirtualBox, VMWare, Xen, KVM
- OS Windows 7 VM (64bit-prefered)
  - https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
- FLARE VM – Distribusi windows untuk malware analysis
  - https://github.com/fireeye/flare-vm
- Cuckoo Sandbox
  - https://cuckoosandbox.org

Sample Malware

- http://contagiodump.blogspot.com/
- https://virusshare.com/
- https://www.malshare.com/
- http://www.malwaredomainlist.com/
- https://malware.lu/

Cloud Sandbox

- https://app.any.run
- https://sandbox.anlyz.io/dashboard
- https://www.joesandbox.com
- https://valkyrie.comodo.com
- https://www.intezer.com
- https://www.secondwrite.com
- https://www.hybrid-analysis.com

Threat

Malware, Infrastructure, Social Engineering

Physical Security

Tip # Make sure your server is physically secure

If an intruder can gain physical access to your server, then you're at risk for having the entire machine or one of its hard drives walk out the door.

Image Source: http://www.techpowerup.com/forums/threads/ssd-lost-some-space.153203/

Physical Security

- Physical security is the first layer of protection in any organization
- It involves protection of organizational assets from environmental and man made threats

Why Physical Security?

- To prevent any unauthorized access to the systems resources
- To prevent tampering/stealing of data from the computer systems
- To safeguard against espionage, sabotage, damage, or theft
- To protect personnel and prevent social engineering attacks

Physical Security Threats

- Environmental threats
  - Floods and earthquakes
  - Fire
  - Dust
- Man made threats
  - Terrorism
  - Wars
  - Explosion
  - Dumpster diving and theft
  - Vandalism

Cont….

- **Natural events** (e.g., floods, earthquakes, and tornados)
- **Other environmental conditions** (e.g., extreme temperatures, high humidity, heavy rains, and lightning)
- **Intentional acts of destruction** (e.g., theft, vandalism)
- **Unintentionally destructive acts** (e.g., spilled drinks, overloaded electrical outlets, and bad plumbing)

Create a Secure Environment -
Building and Room Construction:

Don't arouse unnecessary interest in your critical facilities: A secure room should have "low" visibility (e.g., there should not be signs in front of the building and scattered throughout the hallways announcing "expensive equipment and **sensitive information** this way").

Create a Secure Environment -
Building and Room Construction:

Maximize structural protection: A secure room should have full height walls and fireproof ceilings.

Create a Secure Environment -

Building and Room Construction:

Minimize external access (doors): A secure room should only have one or two doors--they should be solid, fireproof, lockable, and observable by assigned security staff. Doors to the secure room should never be propped open.

Create a Secure Environment - Building and Room Construction:

Be prepared for fire emergencies: In an ideal world, a secure room should be protected from fire by an automatic fire-fighting system. Note that water can damage electronic equipment, so carbon dioxide systems or halogen agents are recommended. If implemented, staff must be trained to use gas masks and other protective equipment. Manual fire fighting equipment (i.e., fire extinguishers) should also be readily available and staff should be properly trained in their use.

Fire and Safety Centre

Be particularly careful with non-essential materials in a secure computer room: Technically, this guideline should read "no eating, drinking, or smoking near **computers**," but it is quite probably impossible to convince staff to implement such a regulation. Other non-essential materials that can cause problems in a secure environment and, therefore, should be eliminated include curtains, reams of paper, and other flammables

Maintain a reasonable climate within the room: A good rule of thumb is that if people are comfortable, then equipment is usually comfortable--but even if people have gone home for the night, room temperature and humidity cannot be allowed to reach extremes (i.e., it should be kept between 50 and 80 degrees Fahrenheit and 20 and 80 percent humidity). Note that it's not freezing temperatures that damage **disks**, but the condensation that forms when they thaw out.

6 Layer data center security (google)

Layer 1: Signage and Fencing

Layer 2: Secure Perimeter

Layer 3: Building Access

Layer 4: Security Operations Center

Layer 5: Data Center Floor

Layer 6: Secure Hard Drive Destruction

Types of physical security control

Preventive Controls	Prevent security violations and enforce various access control mechanisms Examples include door lock, security guard, etc.
Detective Controls	Detect security violations and record any intrusion attempts Examples include motion detector, alarm systems and sensors, video surveillance, etc.
Deterrent Controls	Used to discourage attackers and send warning messages to the attackers to discourage an intrusion attempt Examples include various types of warning signs
Recovery Controls	Used to recover from security violation and restore information and systems to a persistent state Examples include disaster recovery, business continuity plans, backup systems, etc.
Compensating Controls	Used as an alternative control when the intended controls failed or cannot be used Examples include hot site, backup power system, etc.

Physical Security Control

Premises and company surroundings	Fences, gates, walls, guards, alarms, CCTV cameras, intruder systems, panic buttons, burglar alarms, windows and door bars, deadlocks, etc.
Reception area	Lock the important files and documents Lock equipment when not in use
Server and workstation area	Lock the systems when not in use, disable or avoid having removable media and DVD-ROM drives, CCTV cameras, workstation layout design
Other equipment such as fax, modem, and removable media	Lock fax machines when not in use, file the faxes obtained properly, disable auto answer mode for modems, do not place removal media at public places, and physically destroy the corrupted removal media
Access control	Separate work areas, implement biometric access controls (fingerprinting, retinal scanning, iris scanning, vein structure recognition, face recognition, voice recognition), entry cards, man traps, faculty sign-in procedures, identification badges, etc.
Computer equipment maintenance	Appoint a person to look after the computer equipment maintenance
Wiretapping	Inspect all the wires carrying data routinely, protect the wires using shielded cables, never leave any wire exposed
Environmental control	Humidity and air conditioning, HVAC, fire suppression, EMI shielding, and hot and cold aisles

Threat

Malware, Infrastructure, Social Engineering

CNN Money
HACKER?

ONLY
the biggest hacker convention of the year.
REAL FUTURE
GIRLS
FUSION

Social Engineering

"The art of convincing people to reveal confidential information"

Common target

- Receptionist and help desk personnel
- Technical support executive
- System administrator

Impact?

- Economic losses
- Damage to goodwill
- Loss of privacy
- Temporary or permanent closure

Behaviors vulnerable to attack

- Human nature of trust
- Ignorance about social engineering
- Fear of severe losses
- Greediness

Factors that Make Companies Vulnerable to Attacks

- Insufficient security training
- Unregulated access to the information
- Several organizational units
- Lack of security policies

Why is Social Engineering Effective?

- Security policies are as strong as their weakest link, and humans are the most susceptible factor
- It is difficult to detect social engineering attempts
- There is no method that can be applied to ensure complete security from social engineering attacks
- There is no specific software or hardware for defending against a social engineering attack

Phases of Social Engineering Attacks

Research on Target Company

- Dumpster diving, websites, employees, tour company, etc.

Select Victim

- Identify the frustrated employees of the target company

Develop Relationship

- Develop relationship with the selected employees

Exploit the Relationship

- Collect sensitive account and financial information, and current technologies

Types of Social Engineering Attacks

- Human-based: Impersonation, dumpster diving, eavesdropping, shoulder surfing
- Computer-based: Phishing, Pop up window attack, spam email
- Mobile-based: publishing Malicious apps, repackaging legitimate apps, fake security apps

Human Based - Impersonation

- It is the most common human-based social engineering technique where the attacker **pretends to be someone legitimate or an authorized person**
- Attackers may **impersonate** a legitimate or authorized person either personally or using a **communication medium** such as phone, email, etc.
- Impersonation helps attackers in **tricking a target** to reveal **sensitive information**

Impersonation Examples

Posing as a legitimate end user

- Give identity and ask for the sensitive information

"Hi! This is John from finance department. I have forgotten my password. Can I get it?"

Posing as an important user

- Posing as a VIP of a target company, valuable customer, etc.

"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system's password. Can you help me out?"

Posing as a technical support

- Call as technical support staff and request IDs and passwords

"Sir, this is Mathew, Technical support, X company. Last night we had a system crash here, and we are checking for the lost data. Can u give me your ID and password?"

- Vishing (voice or VoIP phishing) is an impersonation technique (electronic fraud) in which the attacker **tricks individuals** to reveal personal and financial information **using voice technology** such as the telephone system, VoIP, etc.

Vishing Examples

Over-Helpfulness of Help Desk

- Here, the attacker calls a company's help desk, pretends to be someone in a **position of authority** or relevance and tries to **extract sensitive information** from the help desk

"A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker a clear entrance into the corporate network"

Third-party Authorization

- Here, the attacker **obtains the name of the authorized employee** of the targeted organization who has access to the information he/she wants
- The attacker then places a **call to the target organization** where information is stored and claims that a particular employee has requested that such information be provided

"Hi I am John, I spoke with Mr. xyz last week before he went on vacation and he said that you would be able to provide me with this information in his absence. Can you help me out?"

Tech Support

- Here, the attacker **pretends to be technical support staff** of the targeted organization's software vendors or contractors
- He/she may **claims the user ID and password** for troubleshooting a problem in the organization

Attacker: *"Hi, this is Mike with tech support. We have had some persons from your office report/complain about slowdowns in logging in lately. Is this true?"*

Employee: *"Yes, it has been slow lately."*

Attacker: *"Well, we have moved you to a new server, so that your service can be much better. You can give me your password, so that I can check your service. Things should be better for you now."*

Cont….

Repairman

Computer technicians, electricians, and telephone repairpersons are generally unsuspected people. Attackers might impersonate a technician or repairperson and enter the organization. He/she performs normal activities associated with his/her duty while looking for hidden passwords, critical information on desks, trash bins, and so on, or even plant a snooping device in a hidden location.

Eavesdropping, shoulder surfing, dumpster diving

Eavesdropping

- Eavesdropping, unauthorized listening of conversations, or reading of messages
- Interception of audio, video, or written communication
- It can be done using communication channels such as telephone lines, email, instant messaging, etc.

Shoulder Surfing

- Shoulder surfing uses direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.
- Shoulder surfing can also be done from a longer distance with the aid of vision enhancing devices such as binoculars that are equipped with the capability of obtaining long distance information

Dumpster Diving

- Dumpster diving is looking for treasure in someone else's trash
- It involves collection of phone bills, contact information, financial information, operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

Human-based Social Engineering: Reverse Social Engineering, Piggybacking, and Tailgating

Reverse Social Engineering

- This is a situation in which an attacker presents himself as an **authority** and the target seeks his or her advice after or before offering the information that he needs

Piggybacking

- "I forgot my ID badge at home. Please help me."
- An authorized person allows (intentionally or unintentionally) an **unauthorized person** to pass through a secure door

Tailgating

- Here, an unauthorized person, wearing a **fake ID badge**, enters a secured area by closely following an authorized person through a door requiring key access

Piggybacking

Piggybacking usually implies entry into the building or security area with the consent of the authorized person. For example, attackers would request an authorized person to unlock a security door, saying that they have forgotten their ID badge. In the interest of common courtesy, the authorized person will allow the attacker to pass through the door.

Tailgating

Tailgating implies access to a building or secured area without the consent of the authorized person. It is the act of following an authorized person through a secure entrance, as a polite user would open and hold the door for those following him. An attacker, wearing a fake badge, attempts to enter the secured area by closely following an authorized person through a door requiring key access. He/she then tries to enter the restricted area by pretending to be an authorized person.

Computer-based Social Engineering: Phishing

- Phishing is a practice of **sending an illegitimate email** falsely claiming to be from a **legitimate site** in an attempts to **acquire a user's personal or account information**
- Phishing emails or pop-ups **redirect users to fake webpages** of mimicking trustworthy sites that ask them to submit their personal information

Clicking the link directs you to a fraudulent web page which looks similar to a genuine HMRC page

http://www.hmrc.gov.uk

Types of Phishing

Spear Phishing	A targeted phishing attack aimed at specific individuals within an organization Attackers use spear phishing to send a message with specialized, social engineering content directed at a specific person, or a small group of people
Whaling	An attacker targets high profile executives like CEO, CFO, politicians and celebrities who have complete access to confidential and highly valuable information Attacker tricks the victim into revealing critical corporate and personal information through email or website spoofing
Pharming	Attacker redirects the web traffic to a fraudulent website by installing malicious program on a personal computer or server Pharming attack is also known as "Phishing without a Lure" which is performed either by using DNS Cache Poisoning or Host File Modification
Spimming	This is a variant of spam that exploits Instant Messaging platforms to flood spam across the networks Attacker uses bots to harvest Instant Message IDs and spread spam

Example:

yahoo!mail | Temukan pesan, dokumen, foto, atau orang | Jimmy | Awal

Tulis

Email Masuk 919
Belum Dibaca
Berbintang
Draft
Terkirim
Arsip
Spam
Sampah
Lebih sedikit

Tampilan Sembunyikan
Foto
Dokumen
Langganan

Folder Sembunyikan
+ Folder Baru

Kembali

Re: [Order Confirmation] [invoice]: Statement of whether you bought this app [Clash Royale - Barrel of Gems] Id Number [HKNEVB90IOC] Saturday, November 21, 2020

Yahoo/Email M...

Apple ID <9b5s5d4dbox-3802881@bvsdbkfhj>
Min, 22 Nov 2020 jam 03.48
Kepada:
mail.receiporder@payment-store.com
Bcc: jim_moedja@yahoo.co.id

Dear customers,

We have received and will process your order through your account on your apps store in our store **[Clash Royale - Barrel of Gems]** With order number **[e-Receipt_INV HKNEVB90IOC]** Through a different address, please complete your account data to cancel the order. in our shop

regards,
apps Store

Clash-Roya....pdf
41.7KB

Balas, Balas ke Semua atau Teruskan

Clash-Royal-Barrel-of-Gem... Halaman 1 dari 1

Receipt

APPLE ID
PAYMENT: Credit Card
DATE November 20, 2020
ORDER ID HKNEVB90IOC
DOCUMENT NO. 280237246251

App Store — HARGA

Clash Royale - Barrel of Gems
Purchase In-App
iPhone X
Report a Problem
$ 27.99

TOTAL $ 27.99

If you didn't make this purchase or if you believe an unauthorized person is attempting to access Your account, Click Here to cancel your purchase.

Learn how to manage your password prefenrences for iTunes, iBooks and App Store purchases.

Apple ID Summary • Terms of Sale • Privacy Policy
Copyright © 2020 Apple Inc.
All rights reserved
1 Infinite Loop, Cupertino, CA 95014, United States

https://t.umblr.com/redirect?z=https%3A%2F%2Felpenalti.com%2F%3Fshignt_&t=OTFlMDE5YWM4M2ZkYjI2MTczNzU3NmE1OTA5NDRkMjllYThhYTA3Niw2NjA4NzU2NDE5YTlmZjlkMGY0ZGUyODdhNTkyMjViOGUwZWRiMzM1&ts=1605797703

Computer-based

Pop-up Windows	These are windows that suddenly pop up while surfing the Internet and ask for **users' information** to login or sign-in
Hoax Letters	Hoax letters are emails that issue **warnings** to the user on new viruses, Trojans, or worms that may harm the user's system
Chain Letters	Chain letters are emails that offer **free gifts** such as money and software on the condition that the user has to **forward the mail to the said number of persons**
Instant Chat Messenger	Gathering **personal information by chatting** with a selected online user to get information such as birth dates and maiden names
Spam Email	Irrelevant, unwanted, and unsolicited email to collect the **financial information**, **social security numbers**, and **network information**

- Phishing is a practice of **sending an illegitimate email** falsely claiming to be from a **legitimate site** in an attempts to **acquire a user's personal or account information**

Congratulations!
CONGRATULATIONS!
You're the 1 Million th
visitor this week!
Click "OK" button below to close window
and contact our Prize Department immediately
OK

TOC Research Group

A Global Research Consultancy

January Opinion Survey >>> Stanford University California

Dear Stanford University User,

You've been selected to participate in an anonymous survey about your experiences with Stanford University

Dear Stanford University User,

You've been selected to participate in an anonymous survey about your experiences with **Stanford University**.

In consideration for your time, at the end of this short survey you will be presented with several exclusive reward offers (worth at least $70).

Start

No

I'm Not Sure

WARNING!

YOUR COMPUTER MAY BE INFECTED:

System detected **(2)** Potentially Malicious Viruses.
The data on your computer is **NOT SAFE**!

Your Personal & Financial Information **IS NOT SAFE**
To Remove Viruses, Call Tech Support Now:

866-955-6104

(24/7 - Toll free- High Priority Virus Removal Call Line for Customers)

Clean Now!

Mobile-based

Publishing Malicious Apps

- Attackers create **malicious apps** with attractive features and **similar names** to that of popular apps, and publish them on major **app stores**
- Unaware, the **users download these apps** and get infected by malware that sends **credentials to attackers**

Repackaging Legitimate Apps

Mobile-based Social Engineering: Fake Security Applications

1. Attacker infects the victim's PC
2. Attacker uploads a malicious application to an app store
3. The victim logs onto his or her bank account. Malware in the system displays a pop-up message telling the victim to download an application onto his or her phone to receive security messages
4. Victim downloads the malicious application on his or her phone
5. At this point, the attacker can access second authentication factor sent to the victim from the bank via SMS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile-based Social Engineering: SMiShing (SMS Phishing)

- SMiShing (SMS Phishing) is the act of using **SMS text messaging system** of cellular phones or other mobile devices to **lure users into instant action** such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number
- SMiShing messages are generally crafted to provoke an instant action from the victim, requiring them **to divulge their personal information and account details**

SMiShing Example

1 Tracy received an **SMS** (text message), ostensibly from the security department at XIM Bank

2 It claimed to be **urgent** and that Tracy should call the phone number in the SMS immediately. Worried, she called to check on her account

3 She called thinking it was an XIM Bank customer service number, and it was a **recording** asking to provide her credit card or debit card number

4 Predictably, Tracy **revealed the sensitive information** due to the fraudulent texts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Insider Attack

- An insider is any **employee** (trusted person or persons) having **access to critical assets** of an organization
- An insider attack involves using privileged access to intentionally **violate rules** or **cause threat to the organization's information** or information systems in any form
- Insider attacks are generally performed by privileged user, **disgruntled employee**, **terminated employee**, accident-prone employee, **third party**, undertrained staff, etc.

Reasons for Insider Attacks

- **Financial gain**
- **Steal confidential data**
- **Taking revenge**
- **Become future competitor**
- **Perform competitors bidding**
- **Public announcement**

Type of Insider Threats

Malicious Insider	This is a disgruntled or terminated employees who steals data or destroys the company's networks intentionally by injecting malware into corporate network
Negligent Insider	These are insiders who are uneducated on potential security threats or simply bypasses general security procedures to meet workplace efficiency
Professional Insider	These are harmful insiders who use their technical knowledge to identify the weaknesses and vulnerabilities of the company's network and sell the confidential information to the competitors or black market bidders
Compromised Insider	This is an insider who has access to critical assets of an organization which is compromised by an outside threat actor

Why Insider Attack is Effective?

- It is easy to launch
- Prevention is difficult
- It can easily succeed
- It is easy for employees to cover their actions
- It is very difficult to differentiate harmful actions from employee's regular work
- It goes undetectable for years and remediation is very expensive

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Disgruntled Employee
Company's Secrets
Company Network
Sends the data to competitors using steganography
Competitors

Social Engineering Countermeasures

- **Good policies** and **procedures** are ineffective if they are not taught and reinforced by the employees
- After receiving training, employees should **sign a statement** acknowledging that they understand the policies
- The main objectives of social engineering defense strategies are to **create user awareness**, **robust internal network controls**, and secure policies, plans and processes

Password Policies

- Periodic password change
- Avoiding guessable passwords
- Account blocking after failed attempts
- Length and complexity of passwords
- Secrecy of passwords

Physical Security Policies

- Identification of employees by issuing ID cards, uniforms, etc.
- Escorting the visitors
- Access area restrictions
- Proper shredding of useless documents
- Employing security personnel

Defense Strategy

- Social engineering campaign
- Gap analysis
- Remediation strategies

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Insider Threats Countermeasures

1. Separation and rotation of duties
2. Least privileges
3. Controlled access
4. Logging and auditing
5. Employee monitoring
6. Legal policies
7. Archive critical data
8. Employee training on cyber security
9. Employee background verification
10. Periodic risk assessment
11. Privileged users monitoring
12. Credentials deactivation for terminated employees

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Quiz

Ganjil: Apa saja akibat dari malware “Holzer”

Genap: Apa saja akibat dari malware “memz”