Remove Watermark Wondershare PDFelement

Threat

Malware, Infrastructure, Social Engineering

Remove Watermark Wondershare PDFelement

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

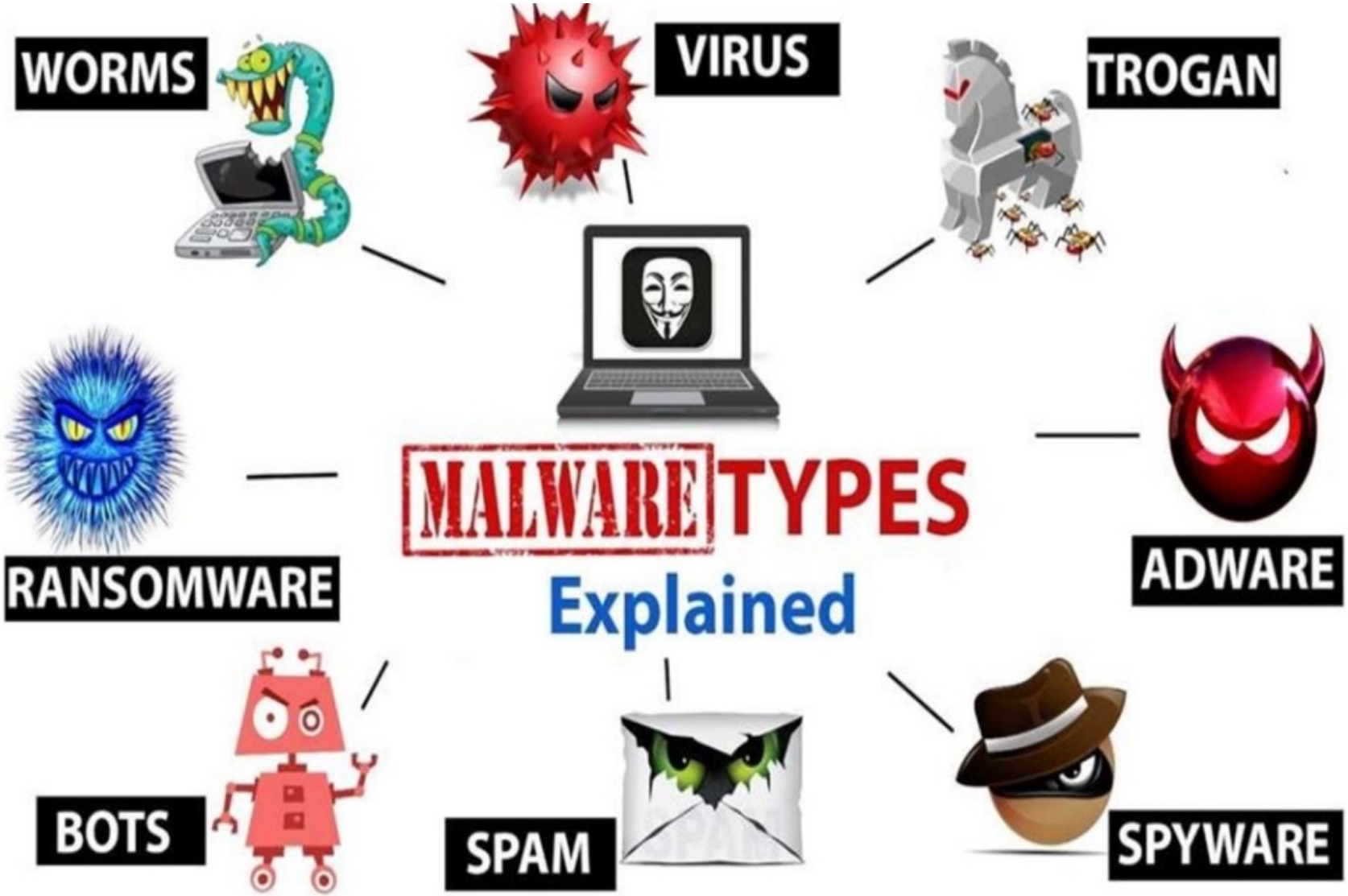
1. Trojan Horse
2. Backdoor
3. Rootkit
4. Ransomware
5. Adware
6. Virus
7. Worms
8. Spyware
9. Botnet
10. Crypter

Remove Watermark Wondershare PDFelement

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

Remove Watermark Wondershare PDFelement



Remove Watermark Wondershare PDFelement

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).

Remove Watermark Wondershare PDFelement

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.

Remove Watermark Wondershare PDFelement

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

Remove Watermark Wondershare PDFelement

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	

Remove Watermark Wondershare PDFelement

REKOMENDASI PENCEGAHAN

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

Remove Watermark
Wondershare PDFelement

Remove Watermark Wondershare PDFelement

Remove Watermark Wondershare PDFelement

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

Remove Watermark Wondershare PDFelement

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

Remove Watermark Wondershare PDFelement

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

Remove Watermark Wondershare PDFelement

Remove Watermark
Wondershare PDFelement

Remove Watermark Wondershare PDFelement

Wrapper

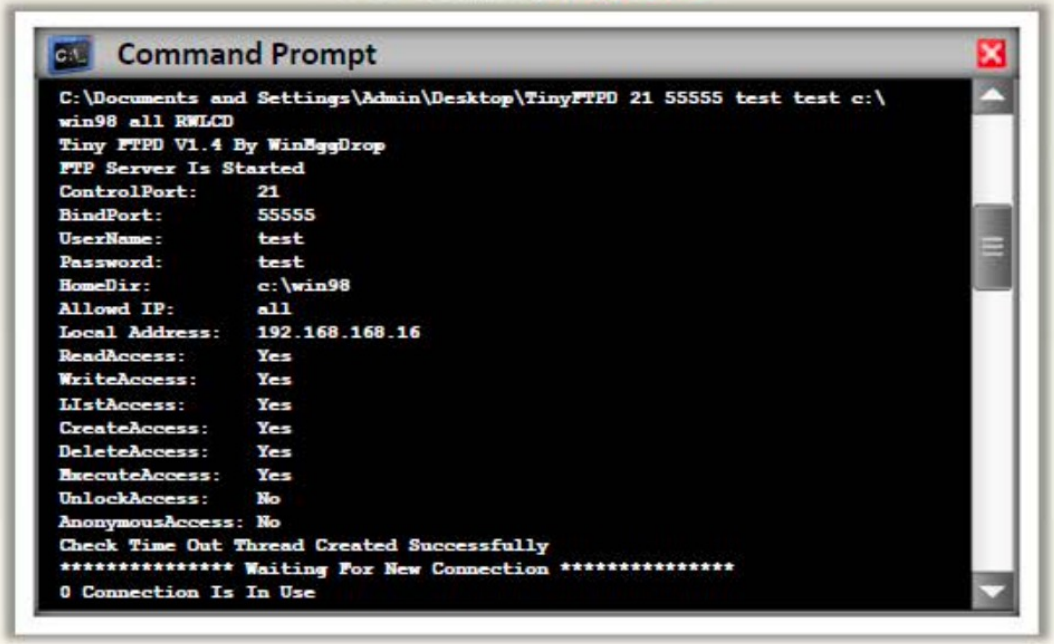
Remove Watermark Wondershare PDFelement

FTP Trojan

FTP Trojan: TinyFTPD

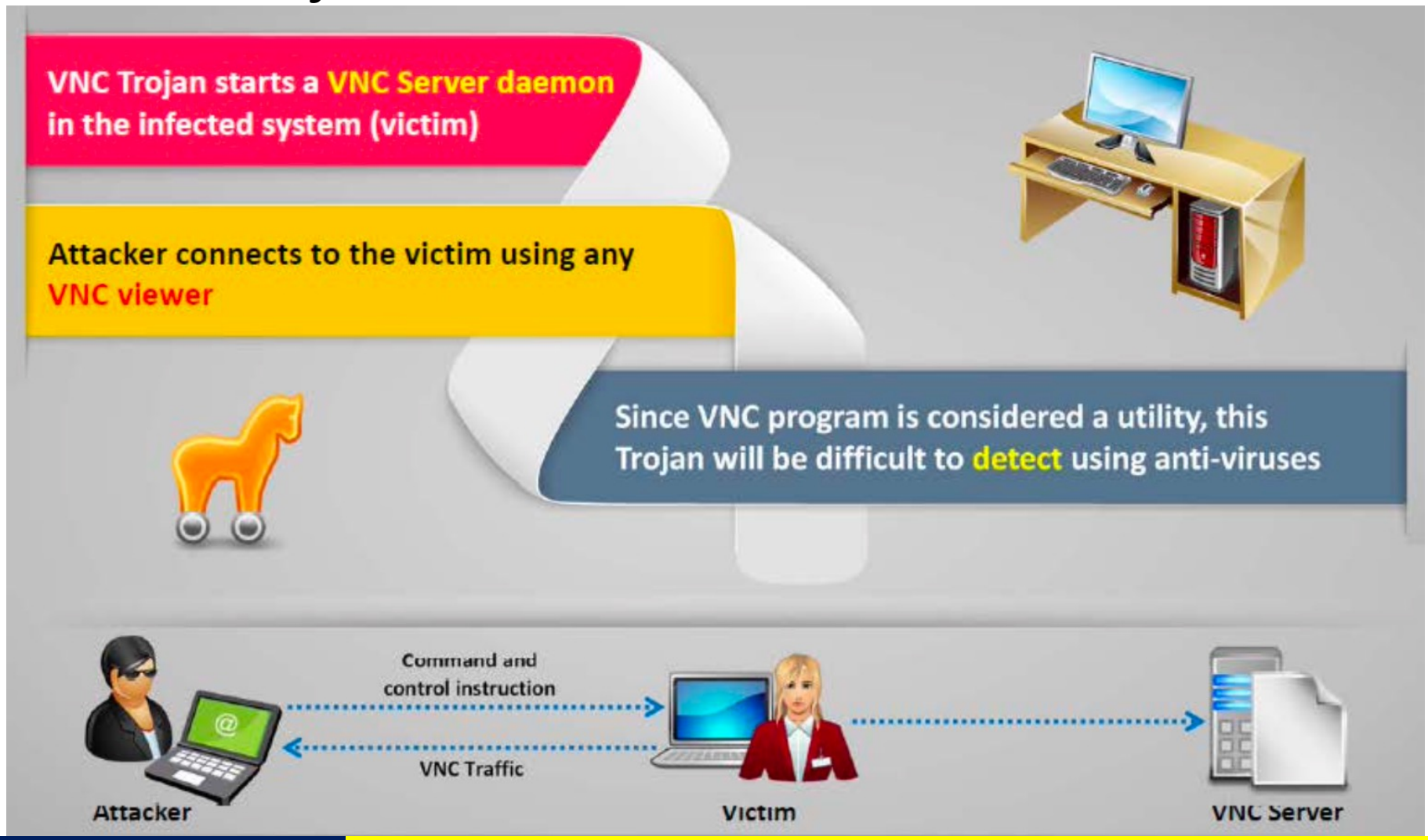
FTP Trojans install an FTP server on the victim's machine, which opens FTP ports

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



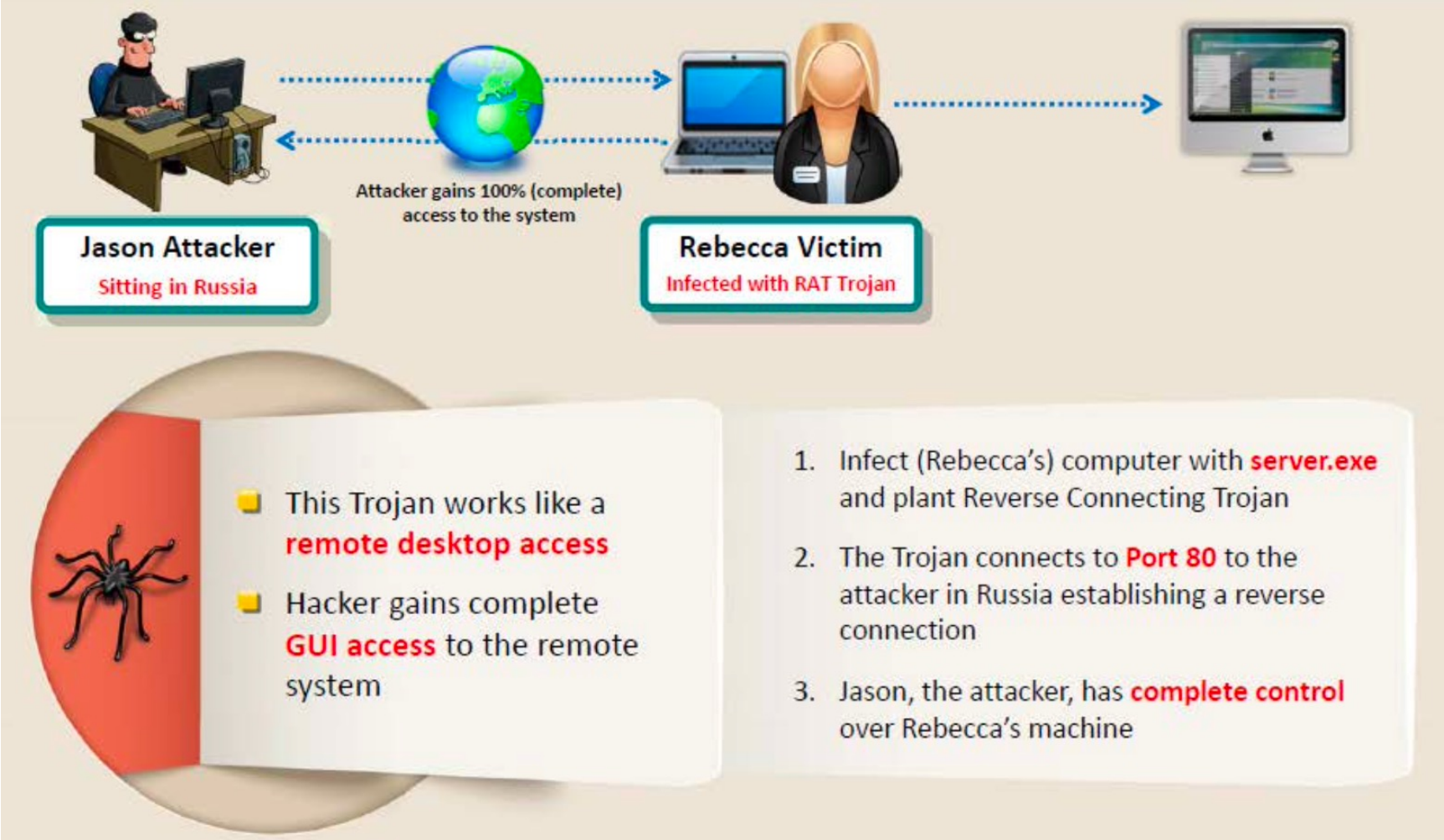
Remove Watermark Wondershare PDFelement

VNC Trojan

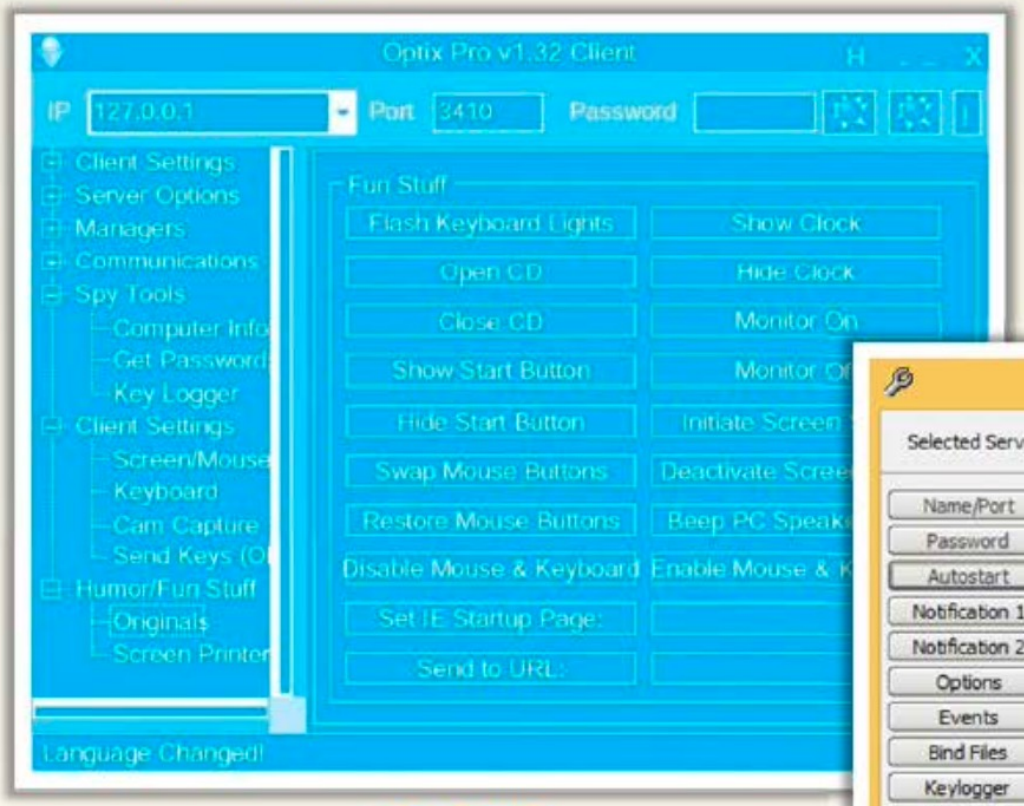


Remove Watermark Wondershare PDFelement

Remote Access Trojan (RAT)

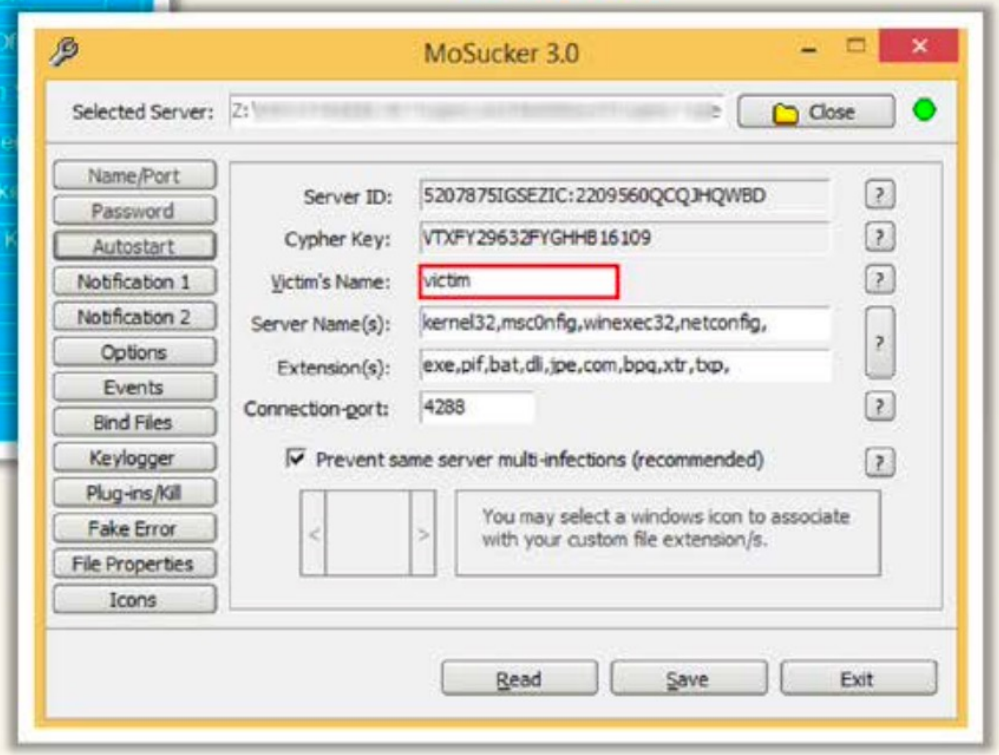


Remove Watermark Wondershare PDFelement



Optix Pro

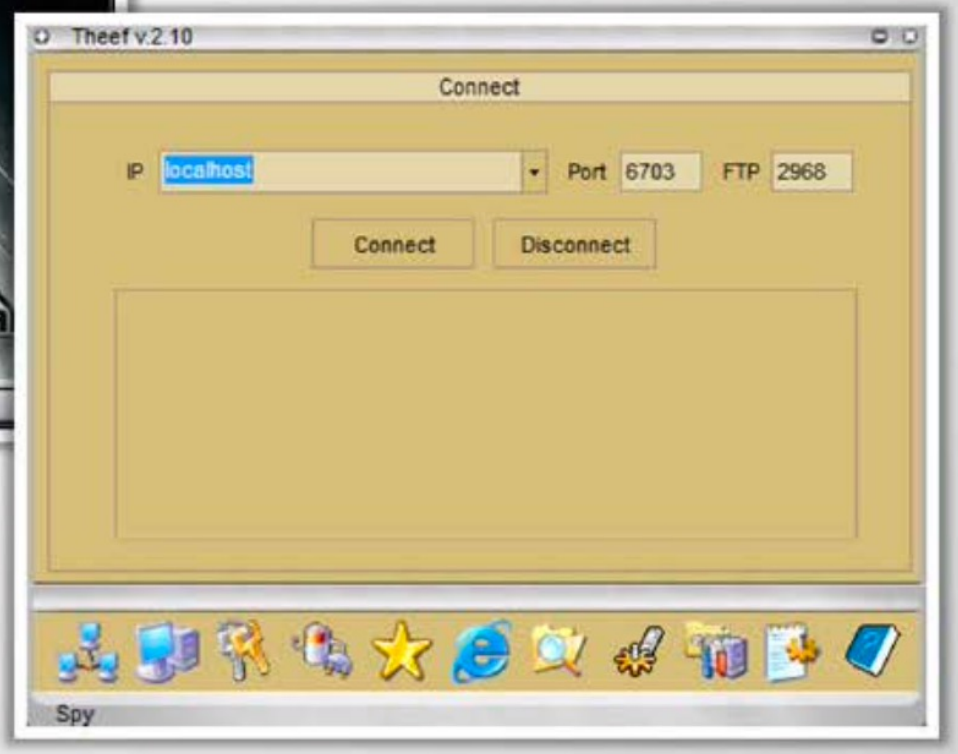
MoSucker



Remove Watermark Wondershare PDFelement

ProRat

Theef



Remove Watermark Wondershare PDFelement

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

Remove Watermark Wondershare PDFelement

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

Remove Watermark Wondershare PDFelement

Worms

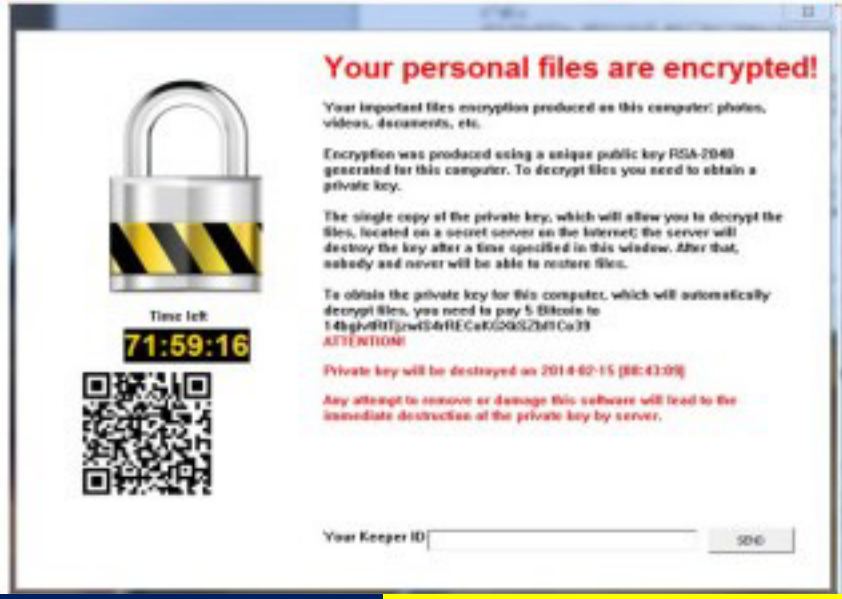
- *Standalone*
- Replikasi diri
- Seperti virus, sering bertukar istilah dengan virus
- Menyebar dengan cepat (*sleek*)
  - Tidak perlu host
  - Tidak perlu eksekusi user
  - Diprogram untuk menyebar melalui jaringan / email
- Memanfaatkan ***bug*** untuk membuat backdoor, botnets

Remove Watermark Wondershare PDFelement

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

Remove Watermark
Wondershare PDFelement



Remove Watermark Wondershare PDFelement

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

Remove Watermark Wondershare PDFelement

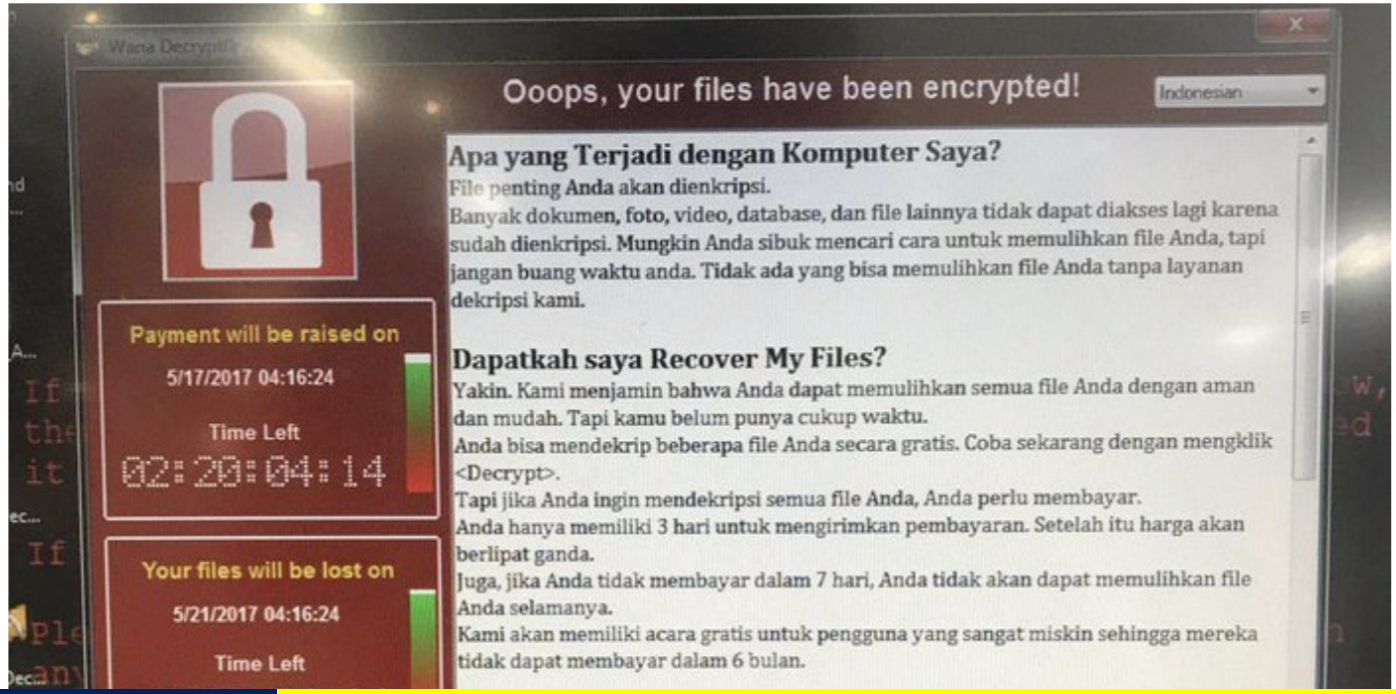
Serangan WannaCry di Indonesia Terbesar Kedua di Dunia

Muhammad Alif Goenawan - detikInet

Minggu, 06 Mei 2018 12:40 WIB

1 komentar

SHARE



Remove Watermark Wondershare PDFelement

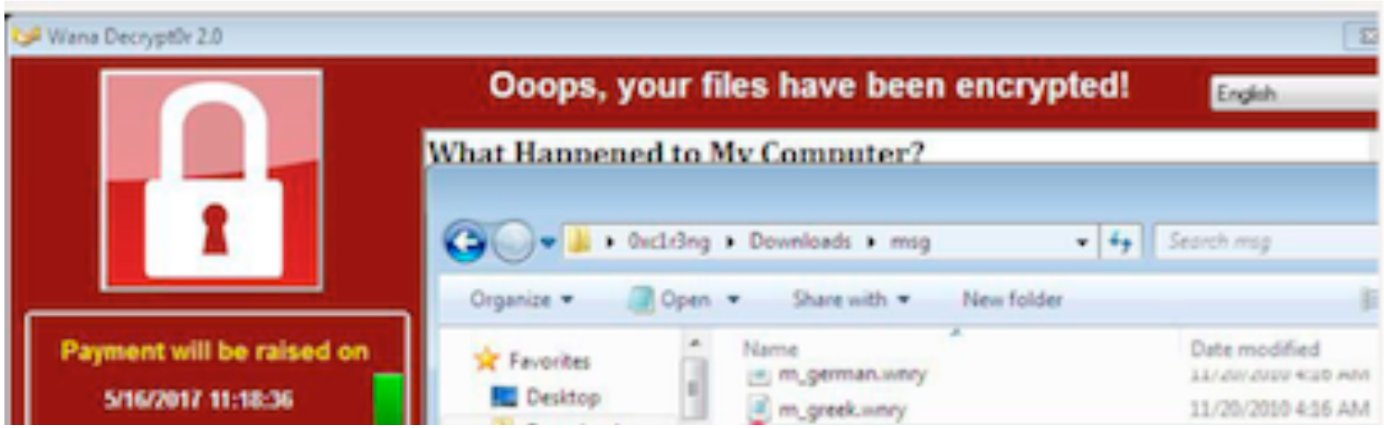
13
05-2017

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



Remove Watermark Wondershare PDFelement

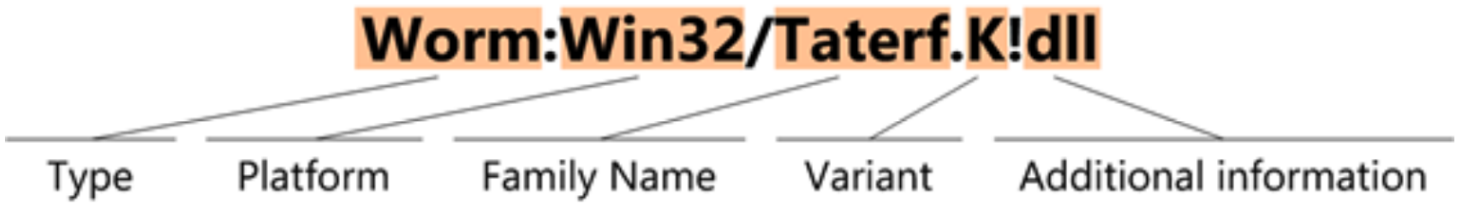
Non-standardized Naming Scheme

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

Remove Watermark Wondershare PDFelement

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

Remove Watermark Wondershare PDFelement

Backdoor
Spyware
adware
….

Remove Watermark Wondershare PDFelement

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 di kelas

Remove Watermark Wondershare PDFelement

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

Remove Watermark Wondershare PDFelement

Sample Malware

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