A sandboxing-on túli világ - hatékony malware analízis

Ács György
IT biztonsági konzulens
2016. április 25.

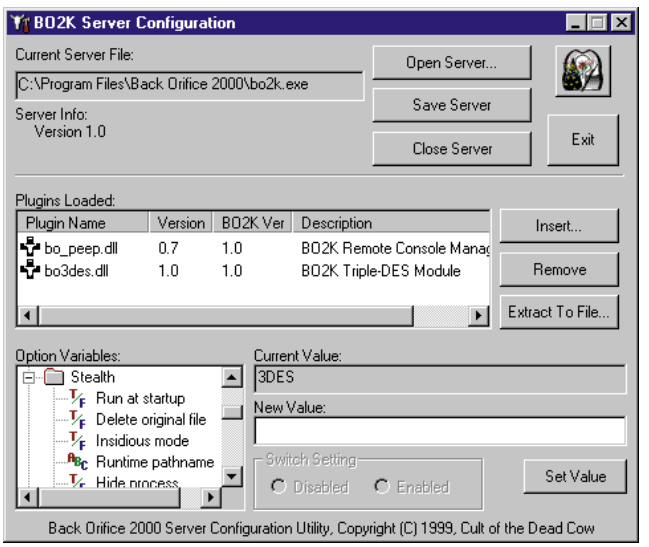
György Ács
Security Consultant
C|EH, SFCP, SFCE

gacs@cisco.com

Global Security Sales Organization

Tartalom

- Modern támadások
- Malware analízis technikák
- Mi a sandbox ?
- ThreatGrid sandbox
- Advanced Malware Protection
- A DNS csatorna
- Ajánlások



Cisco Éves Biztonsági Jelentés 2015:

Mi az a malware ?

Malware = **Mal**icous soft**ware**

Bármilyen kód, ami kárt okoz(hat)

Ismeretlen kód, ami érdekes lehet

Típusok

rootkitek, backdoor-ok
botnet-ek, scareware-ek
férgek, vírusok,

Common Vulnerability Scoring System (CVSS)

IntelliShield ID	Headline
33695	OpenSSL TLS/DTLS Heartbeat Information Disclosure Vulnerability
35880	GNU Bash Environment Variable Content Processing Arbitrary Code Execution Vulnerability
35879	GNU Bash Environment Variable Function Definitions Processing Arbitrary Code Execution Vulnerability
36121	Drupal Core SQL Injection Vulnerability
32716	Adobe Flash Player Remote Code Execution Vulnerability
33961	Microsoft Internet Explorer Deleted Memory Object Code Execution Vulnerability
28462	Oracle Java SE Security Bypass Arbitrary Code Execution Vulnerabilities
30128	Multiple Vendor Products Struts 2 Action Parameter Processing Command Injection Vulnerability

Hogyan védekezzünk ellenük, ha nem értjük a működésüket?

Van erre eszközünk?

Amikről mindenki hallott már …

... a támadó okosak és motiváltak

... a modern malware = egy iparág

zero day sérülékenység ára: $$$$$ -> $40,000 - $160,000

browser exploit pack ára : $$$$ -> BlackHole bérlése : $500-700/hónap, -> $450k

botnet ára : $$ botonként -> 10.000 zombi: $1000 (US)

bankkártya ára : $ kártyánként -> 9$ -35$

.....

... célzott támadások, Advanced Persistent Threats, Cyber Security...

... Spear Phishing, Water Holing, trójaiak, Buffer Overflow ....

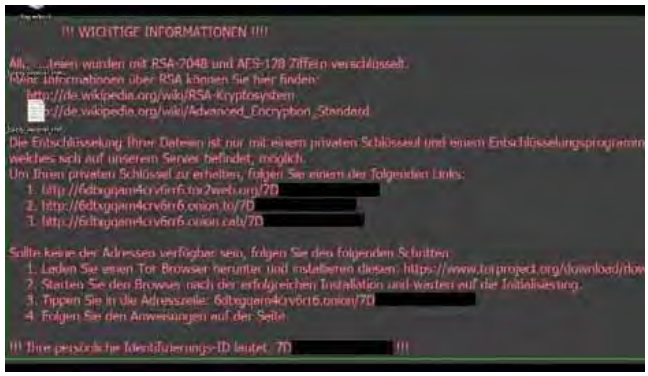
Zsaroló programokról ...

- Zsarolóvírusok (ransomware-ek) olyan kártékony programok, amelyek egy számítógépre jutva elérhetetlenné tesznek bizonyos fájlokat vagy akár az egész rendszert
- Az első :1989-ből
- 2 csoport:
  - Lockerek
  - Cryptoware-ek

Cryptowall

Zsaroló programokról ...

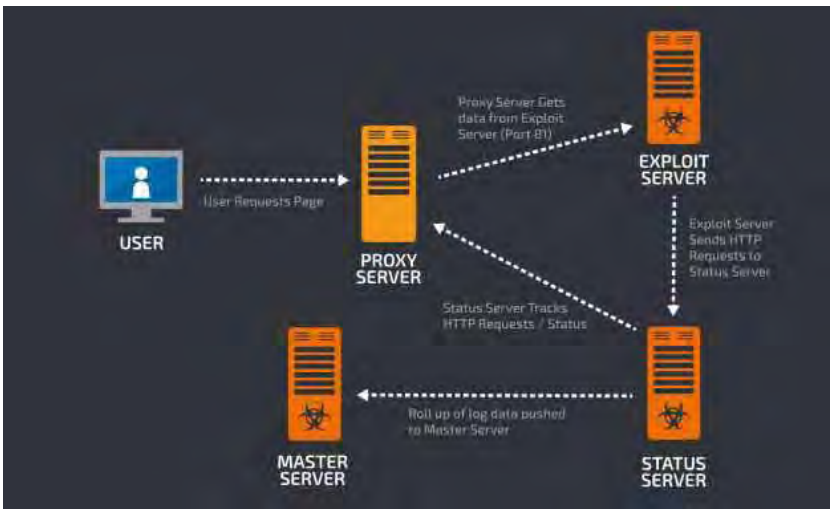
- Gyakran fejlődnek és mutálódnak
- Leggyakrabban emailcsatolmányban, fertőzött weboldalakon terjednek
- akár megbízható weboldalakról is (ha az azokat reklámokkal ellátó hirdetéskiszolgáló fertőződik meg)
- Itthon a Locky (valamilyen számlának tűnő Word + macro) és a CryptoWall 4 nevű zsarolóvírus fordul elő leggyakrabban



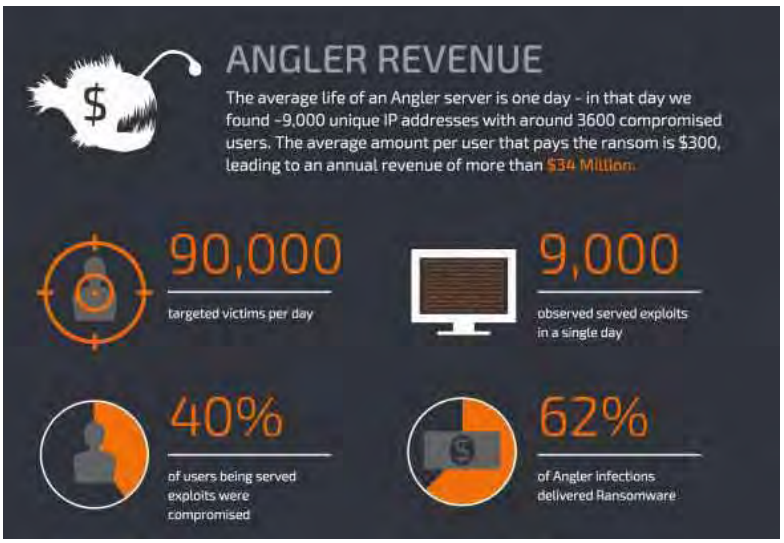
Egy érdekes cikk ...

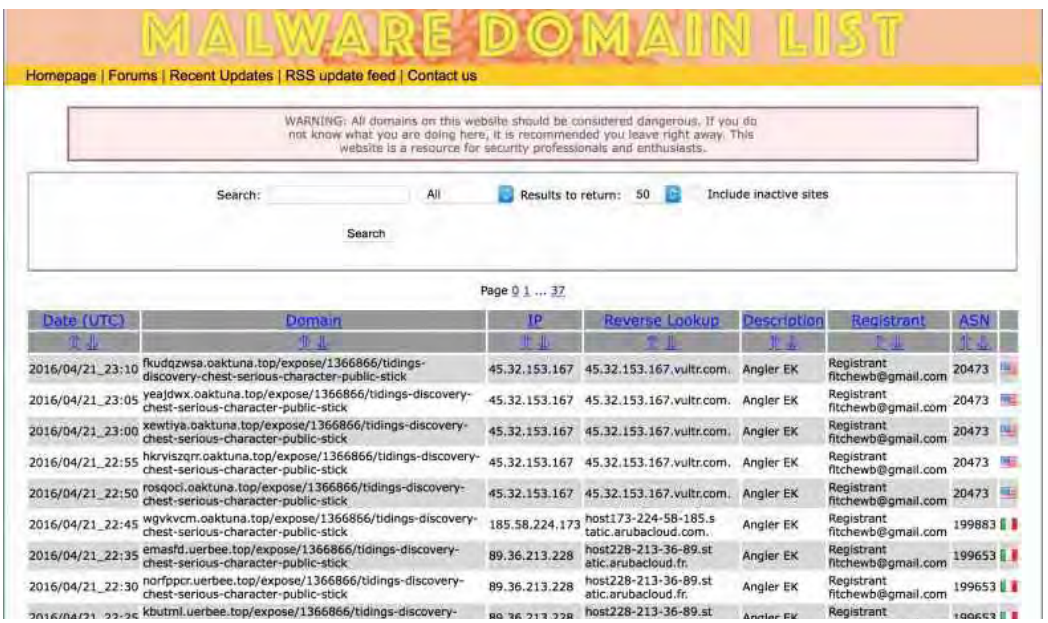
Cisco Talos és a zsaroló programok

Angler infrastruktúra



~40% of users being served exploits are compromised by Angler.
~62% of Angler infections delivered Ransomware and the average ransom is $300.

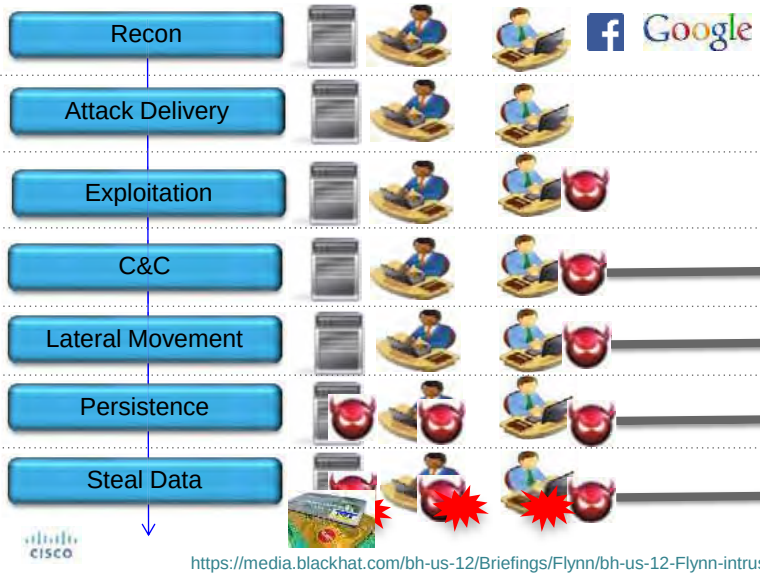




Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
2016/04/21_23:10	fkudqzwsa.oaktuna.top/expose/1366866/tidings-discovery-chest-serious-character-public-stick	45.32.153.167	45.32.153.167.vultr.com.	Angler EK	Registrant fitchewb@gmail.com	20473
2016/04/21_23:05	yeajdwx.oaktuna.top/expose/1366866/tidings-discovery-chest-serious-character-public-stick	45.32.153.167	45.32.153.167.vultr.com.	Angler EK	Registrant fitchewb@gmail.com	20473
2016/04/21_23:00	xewtiya.oaktuna.top/expose/1366866/tidings-discovery-chest-serious-character-public-stick	45.32.153.167	45.32.153.167.vultr.com.	Angler EK	Registrant fitchewb@gmail.com	20473
2016/04/21_22:55	hkrviszqrr.oaktuna.top/expose/1366866/tidings-discovery-chest-serious-character-public-stick	45.32.153.167	45.32.153.167.vultr.com.	Angler EK	Registrant fitchewb@gmail.com	20473
2016/04/21_22:50	rosqoci.oaktuna.top/expose/1366866/tidings-discovery-chest-serious-character-public-stick	45.32.153.167	45.32.153.167.vultr.com.	Angler EK	Registrant fitchewb@gmail.com	20473
2016/04/21_22:45	wgvkvcm.oaktuna.top/expose/1366866/tidings-discovery-chest-serious-character-public-stick	185.58.224.173	host173-224-58-185.static.arubacloud.com.	Angler EK	Registrant fitchewb@gmail.com	199883
2016/04/21_22:35	emasfd.uerbee.top/expose/1366866/tidings-discovery-chest-serious-character-public-stick	89.36.213.228	host228-213-36-89.static.arubacloud.fr.	Angler EK	Registrant fitchewb@gmail.com	199653
2016/04/21_22:30	norfppcr.uerbee.top/expose/1366866/tidings-discovery-chest-serious-character-public-stick	89.36.213.228	host228-213-36-89.static.arubacloud.fr.	Angler EK	Registrant fitchewb@gmail.com	199653
2016/04/21_22:25	kbutml.uerbee.top/expose/1366866/tidings-discovery-	89.36.213.228	host228-213-36-89.st	Angler EK	Registrant	199653

http://www.malwaredomainlist.com/mdl.php

The Kill Chain



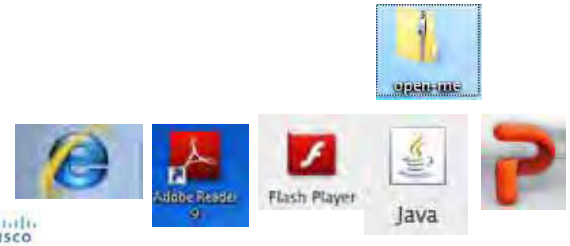
https://media.blackhat.com/bh-us-12/Briefings/Flynn/bh-us-12-Flynn-intrusion-along-the-kill-chain-WP.pdf

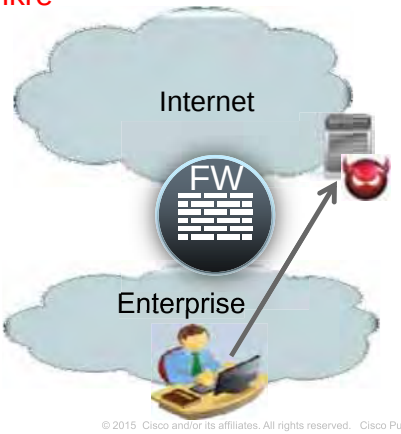
Az áldozat megtámadása

Valamilyen csatornán, email, social media, telefon elérjük hogy az áldozat megnyissa a csatolmányt vagy klikkeljen egy linkre

... Futtatható malware indítása
.exe, .msi, .vbs, .ps1, .dmg , ...

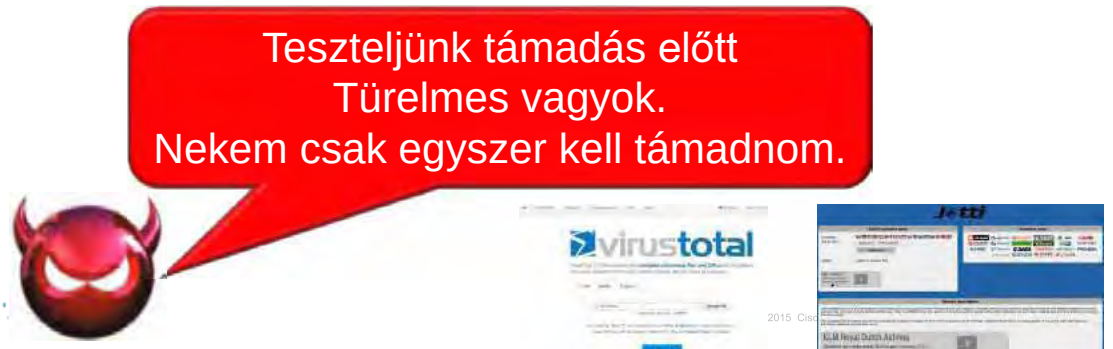
... Sérülékeny alkalmazás/plugin kihasználása





Támadás előtt: Az antivírus rendszeren átmenne?

- Online AV scanner: http://virustotal.com : megosztja a mintákat más AV vendorral
- Célzott támadások saját dedikált AV teszt rendszert használnak

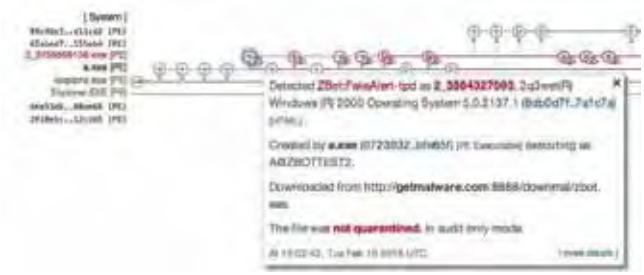


Más rendszerek nem osztják meg a mintákat

av-check,
virtest,
scan4you

Mit csinál egy malware ?

- Megnézi a „környezetet” (antivírus, anti-spyware, ...)
- Megpróbálja megőrizni magát (registry)
- Kártékony kódot tölt le
- File-t hoz létre
- Hook (saját kódot regisztrál) -> keylogger
- Malware vagy CnC (Command and Control) állomással kommunikál



Mi az a malware analízis?

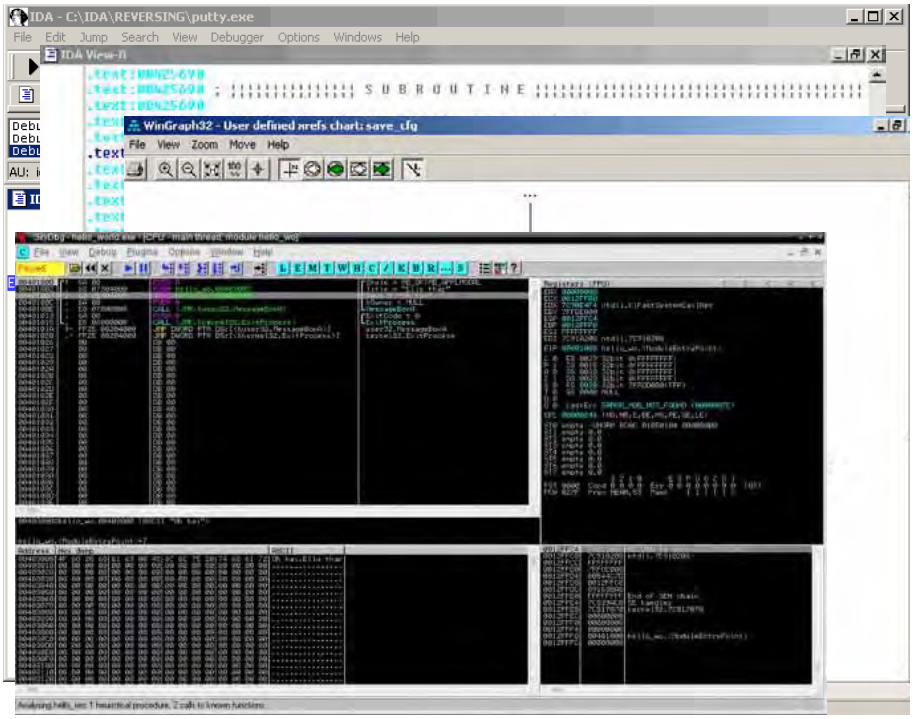
- A malware szétboncolása, viselkedés elemzése, részek elemzése
- Ami Nem:
  - forensics elemzés
  - Incident Response (IR)
- Macska- egér harc
- Ha jól csináljuk, vezeti az incident response munkálatokat
  - A malware analízis segítségével jóval magasabb biztonsági szint érhető el
  - Host alapú „nyomok” és hálózati szignatúrák

Malware analízis lehetőségei

- 1. Utána
  - forensics analízis a gépeden ... ?
  - Hoppá, a vállalati adatbázis kikerült !
- 2. Más gépén, előtte ?
  - Nagyon célzott támadás ?
  - Az egész gép tükrözése ?
  - Agent szükséges?

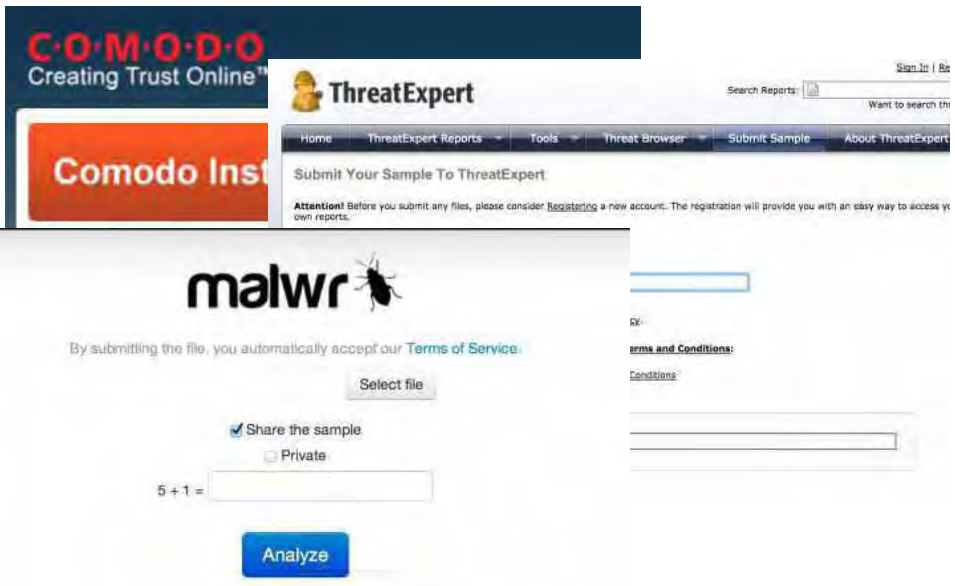
Malware analízis lehetőségei

- 1. Statikus
  - Disassembler, pl. : IDA, OllyDbg
  - Reverse engineering
  - Komponensek vizsgálata lépésről lépésre
  - Gépi kód-> assemply konverzió
  - Memory dumper: LordPE, OllyDump



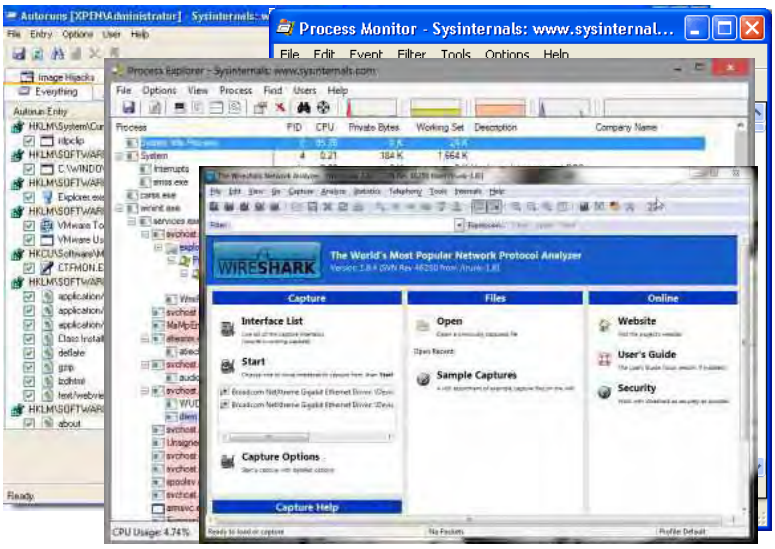
Malware analízis lehetőségei

- 2. Dinamikus analízis
  - Viselkedés naplózása
  - Virtuális gép
  - Sandboxing
  - Debugger (GDB, WindDGB)



Kód analízis manuálisan = sok munka nem automatizált eszközök

- Detect Autoruns:
  - Autoruns
- File system és registry monitoring:
  - Process Monitor és Capture BAT
- Process monitoring:
  - Process Explorer és Process Hacker
- Network monitoring:
  - Wireshark és SmartSniff
- Change detection:
  - Regshot



Sandbox

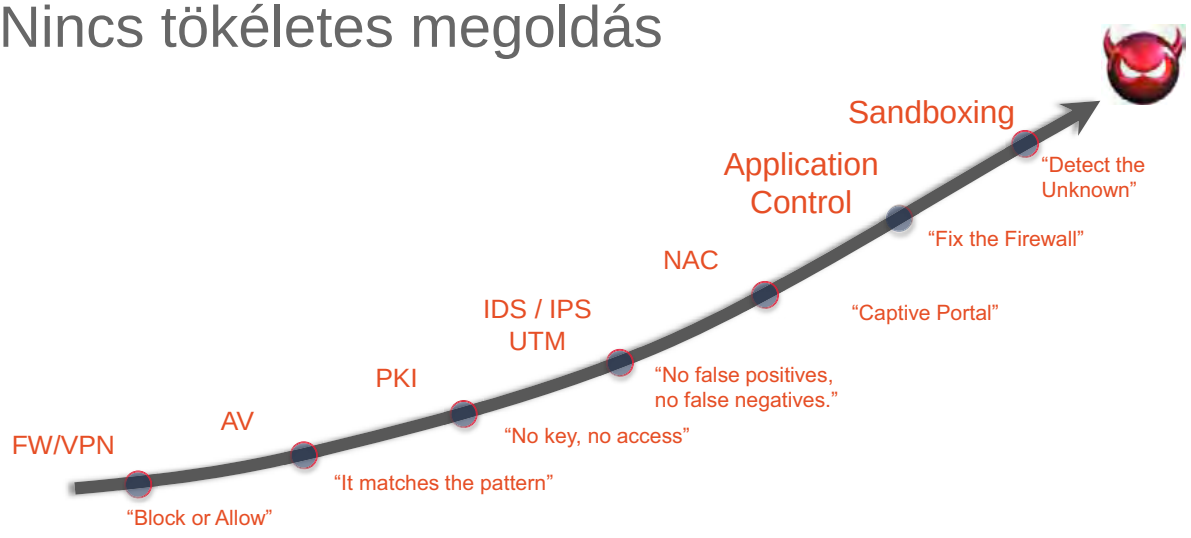
- Virtuális gépben a kód futása
- Appliance (felhőben vagy lokális)
- Kimenet : a viselkedés leírása, “bizonyítékok”
- Időbe telik az analízis
- Többnyire automata

Report :

- network activity
- persistence (registry writes, service creation)
- spreading
- anti-debugging
- reading password files
- keylogging

Report ArtifactsFile, video

Nincs tökéletes megoldás



Malware sandbox detektálás

- Miért érdekes ez?

- Ha a malware detektálja a sandbox környezetet, nem csinál “rosszat”
- Nem működik a dinamikus analízis a továbbiakban
- Csak a statikus analízis marad
- Jó sandbox: úgy csinál, mint egy “buta” felhasználó, …

3

Malware sandbox detektálás (piros-kék pirula)

- VM karekterisztikák ellenőrzése
  - registry keys, MAC address, processes, services
  - Kód végrehajtás különböző időzítéssel /eredménnyel
- Várj 10 reboot-ot, … 1000 egér kattintást …
- Malware csak alszik X órát
  - sandbox nem tudja végtelen ideig vizsgálni
  - Ellenintézkedés : órafelgyorsítás a sandbox-ban
  - Ellen-ellenintézkedés : ... <amit te gondolsz>

3

Sandbox detekció

“Turing test” vagy felhasználó input - tevékenység

- Mozog az egér? A billentyűzetet használják?
- Megkérjük a felhasználót, hogy klikkeljen …
- CAPTCHA

Kérlek,
kattints ide -> o

2

Sandboxing

- Antivírus a Malware ellen, csak fordítva…
- Sandboxing egy jó tool, de nem nyújt védelmet minden egyes támadással szemben, nem átverhetetlen
- **Fejlett támadások ellen többrétegű védelmi rendszer kell**

3

Cisco AMP Threat Grid – miben más?

Teljesítmény
- Gyors, automatizált analízis, állítható futásidő
- Láthatatlan a minta számára, sok viselkedés elemzés

Szolgáltatások
- Videó lejetszás, Glovebox : malware interakció
- Process Graph for visual representation of process lineage
- Threat Score & Behavioral Indicators

Kontext
- Keresés és korreláció minden adatrészletre (artifacts) a több milliárd mintabázison (globális kontext)
- Az elemző részletes leírást kap, jobban megérti a malware működését

Integráció
- API az első naptól, integráció a jelenlegi IT biztonsági megoldásokkal (minta feladás, riport), Cisco AMP
- Custom threat intelligence feed-ek támogatása

ThreatGrid platformok

Felhő: adatközpont US (EU jön)
- **Több millió analízis per nap**
- **6 - 8 millió** analízis hónaponta (és egyre nő …)
- ThreatGRID software és dedikált hardware
- **Más felhő szolgáltatóra nincs szükség**
- Több állomásos architektúra

On-premise Appliance: - helyi elemzés
- max **5,000 minta naponta** (ThreatGRID 5500 Series)
- Kiemelt biztonságú szervezetek számára
- Azonos funkciókészlet / GUI, mint a ThreatGRID SaaS
- Az appliance frissítést kap => a teljes kontext látja az elemző

Saját elemző rendszer - Proprietary Analysis

- Külső elemzés
- **Nincs jelen a VM-ben, mint más sandbox-ok, pl.: Cuckoo**
- **Dinamikus analízis** :
  – **External kernel monitor**, zero-instrumentation
  – **Dynamic disk** analysis showing modifications to the physical disk such as changes to the **Master Boot Record**
  – Full **user interaction** and emulation through **ThreatGRID's Glovebox**
  – Full **video capture**, playback of all screen activity
  – Detailed analysis of malware sample activities including **network traffic**
- **Statikus analízis** :
  – PDF, RTF, CDF, JavaScript, HTML and PE files

Threat Score

- 440+ viselkedés jelző : Behavioral indicators (and growing)
  - Malware családok, káros viselkedések
  - Részletes leírás, bizonyítékokkal
- Megbízhatóság alapú prioritás -> segít a SOC elemzésben és IR tudásbar

- If you knew you were going to be compromised, would you do security differently?"

- Marty Roesch
- Chief Architect – Cisco Security Group

AMP: Advanced Malware Protection

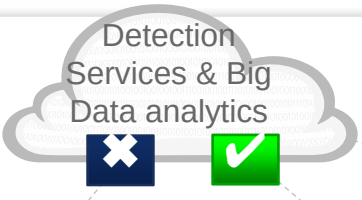
Network-based AMP

FireSIGHT Management Center

Sourcefire Sensor

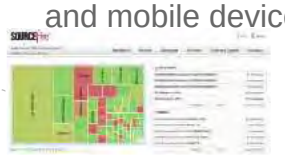
AMP Malware license

Detection Services & Big Data analytics



Nincs szükség agent-re

AMP for hosts desktop and mobile devices

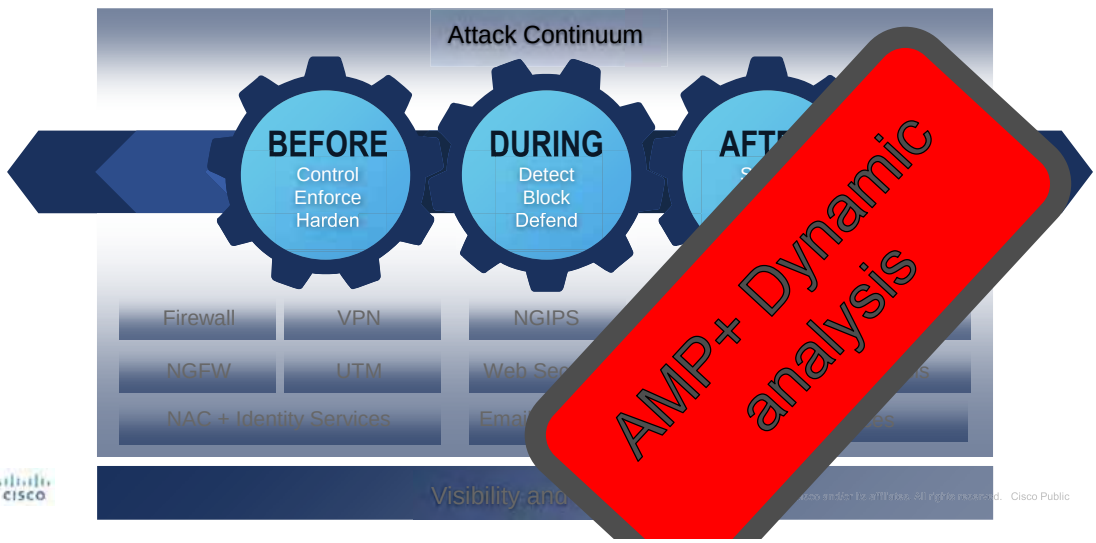


Private Cloud / SaaS Manager

Host-based AMP

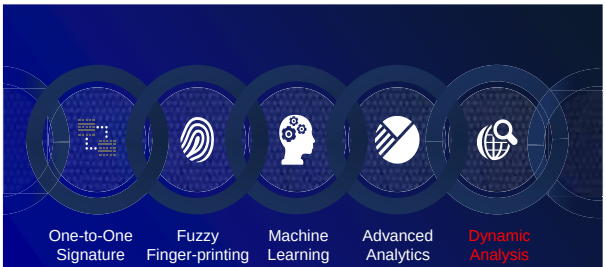
- Kis méretű agent
- File hozzáféréseket figyeli (move/copy/execute)
- Jellemzőket gyűjt (fingerprint & attributes)
- Lekérdezi a file státuszát (tiszta, malware, ismeretlen)

Cisco biztonsági model



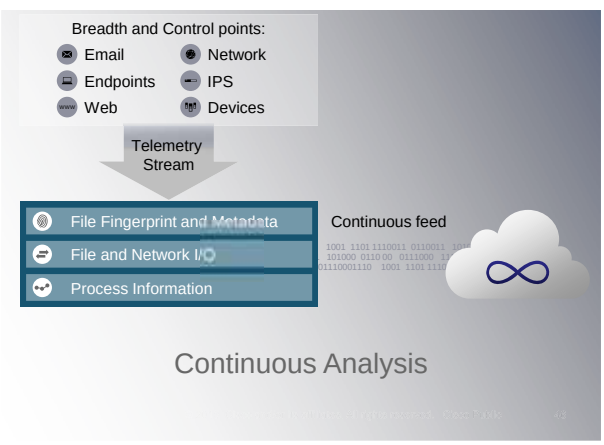
AMP : Point-in-Time + Retrospective Protection

Point-in-Time Protection



File Reputation & Sandboxing

Retrospective Security



Continuous Analysis

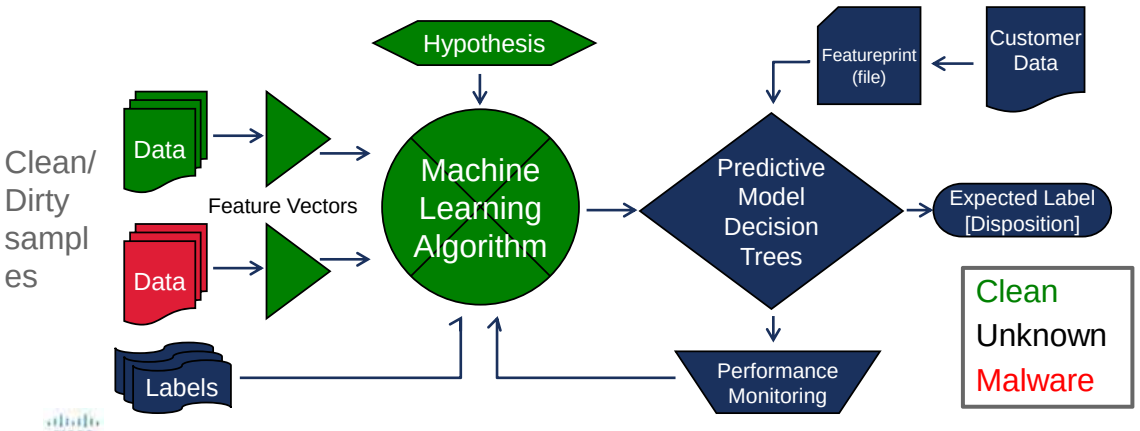
Protection Framework: Ethos Engine

- ETHOS = Fuzzy Fingerprinting statikus és passzív heurisztikát használva
  - A malware-ek polimorf variánsaira
  - Gyakran ugyanazok a struktúrális jellemzők
  - Az eredeti és variánsok elfogása -> pontosabb döntés
  - Döntési fát épít

4

Protection Framework: Spero Engine

- SPERO = Machine Learning using active heuristics



Protection Framework: IOCs

- IOC = Indicators of Compromise
  - Speciális jellemző, nyom (artifacts) ami a támadás után ottmaradt
  - XML alapú leíró nyelv, hogyan tudjuk azonosítani a malware-t
  - Host vagy/és hálózat alapú nyom, host alapon kezdeményezett letapodatás
  - OpenIOC 1.1 eredet

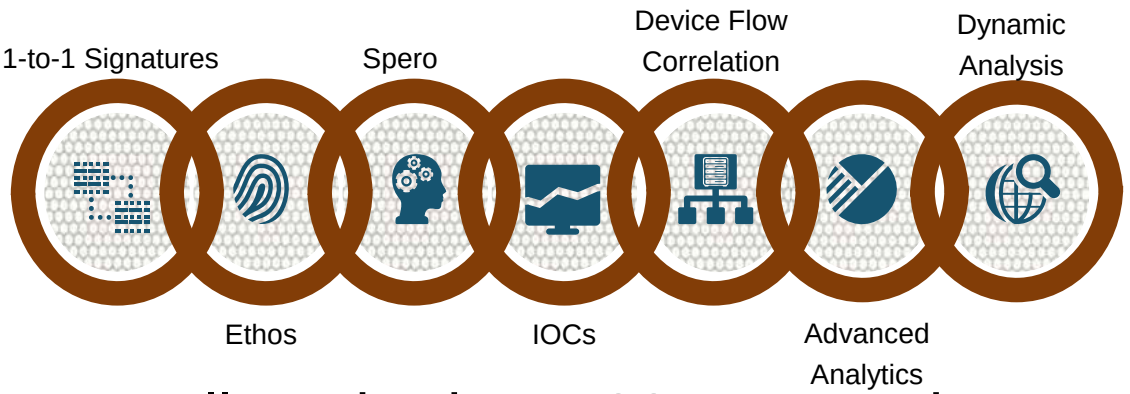
Wikipedia:

"in computer forensics is an artifact observed on a network or in operating system that with high confidence indicates a computer intrusion."

http://en.wikipedia.org/wiki/Indicator_of_compromise

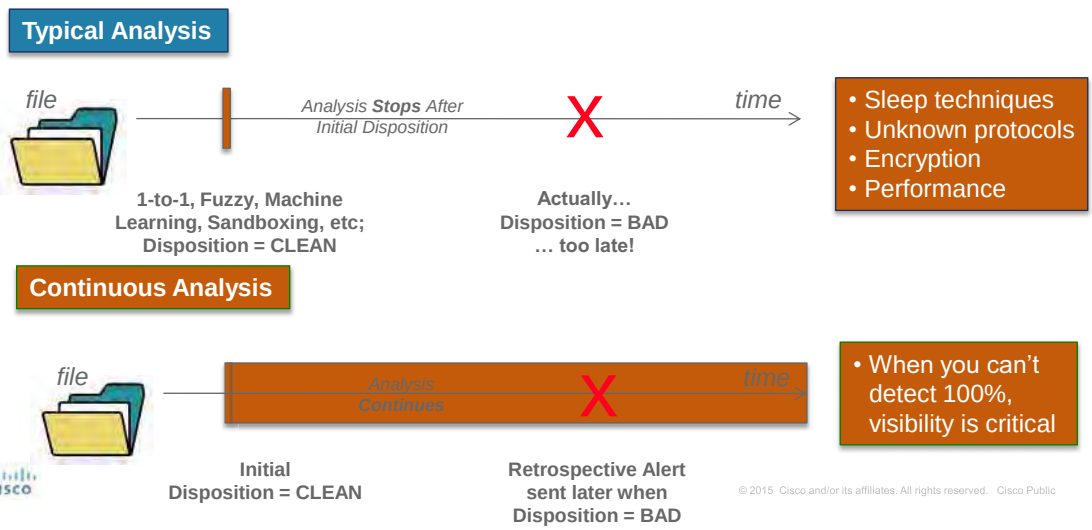
4

Plan A: The Protection Framework

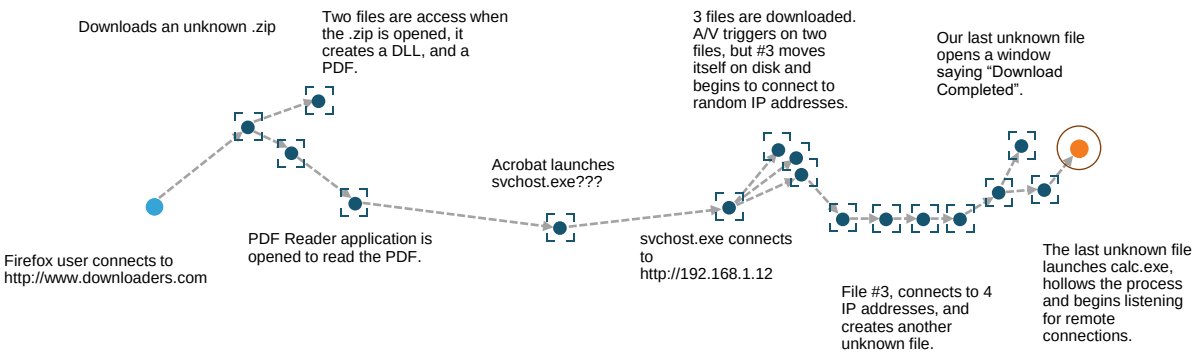


All Methods < 100% Detection

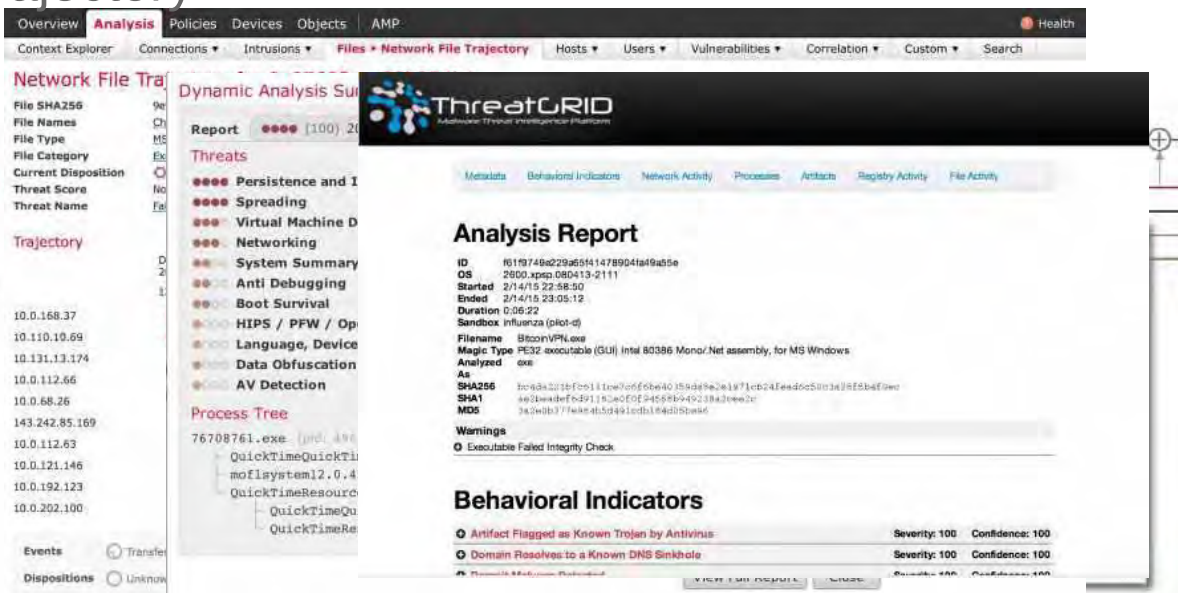
Plan B: Retrospection

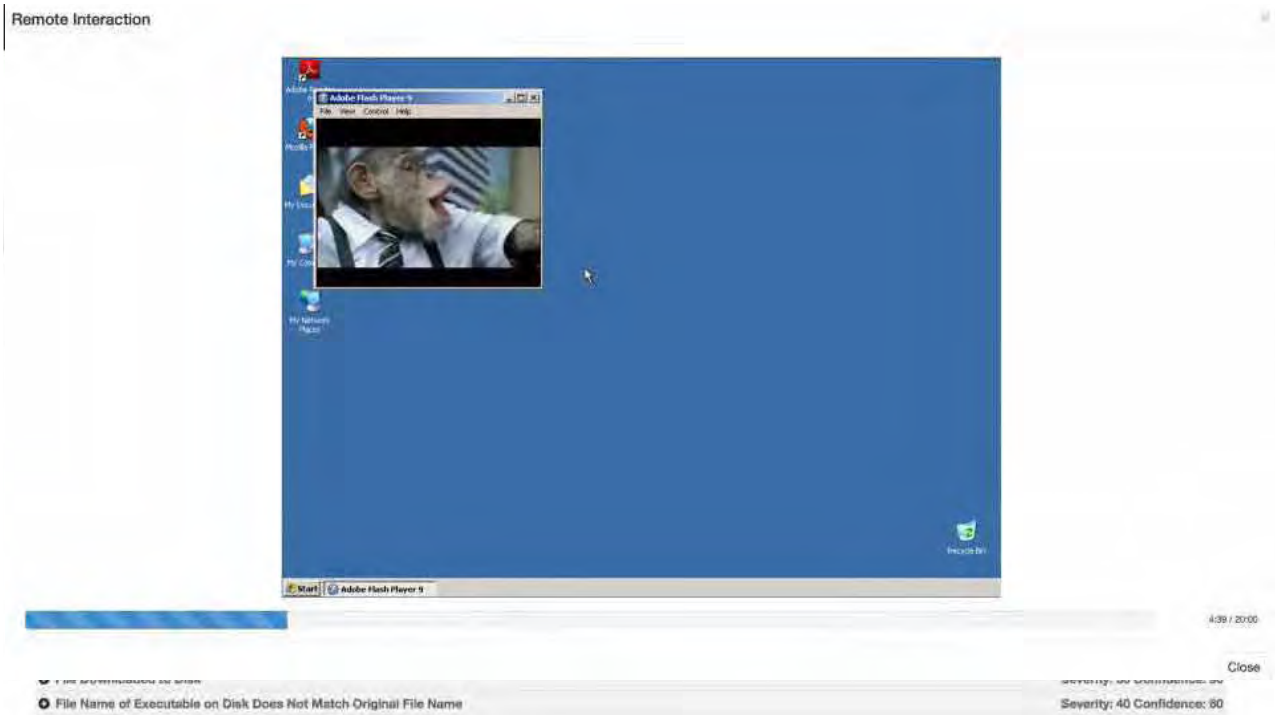


Retrospection Framework: Trajectory



Nyomkövetés alkalmazás és hálózati szinten: trajectory





Why OpenDNS?

DNS Services Built for World's Largest Security Platform

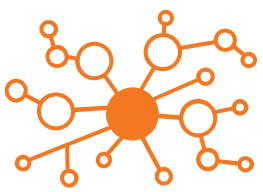
GLOBAL NETWORK

- 80B+ DNS requests/day
- 65M+ biz & home users
- 100% uptime
- Any port, protocol, app

\+

UNIQUE ANALYTICS

- security research team
- automated classification
- BGP peer relationships
- 3D visualization engine



= **80M+**

malicious requests blocked/day

A New Layer of Breach Protection

Threat Prevention
Not just threat detection

Protects On & Off Network
Not limited to devices forwarding traffic through on-prem appliances

Always Up to Date
No need for device to VPN back to an on-prem server for updates

Block by Domains, IPs & URLs for All Ports
Not just ports 80/443 or only IPs

Turn-Key & Custom API-Based Integrations
Does not require professional services to setup

Mit tudunk mi tenni ?
Közösségi együttműködés

- Snort : ingyenes, IDS/IPS rendszer
- ClamAV: ingyenes vírusírtó
- Immunet : ingyenes „advanced malware protection” rendszer
- OpenAppID : alkalmazás definiciók és azok megosztása
- OpenDNS : ingyenes, szabad DNS szolgáltatás

Összefoglalás

- Modern malware tökéletesen át tud menni a ma alkalmazott “point-in-time” detekciós eljárásokon
- Detekció fontos, de szükség van másra is.
- A sandboxing egy hatásos detekciós módszer, de nem mindenható
- Retrospektív elemzés megmutatja, mit nem kaptunk el
- AMP Everywhere – mindenhol : teljes rálátást és kontrolt ad

A VÁLASZIDŐ CSÖKKENTÉSE ..

... A BETÖRÉS OKOZTA KÖLTSÉGEK CSÖKKENTÉSE

TOMORROW starts here.