

A sandboxing-on túli világ - hatékony malware analízis

Ács György

IT biztonsági konzulens

2016. április 25.



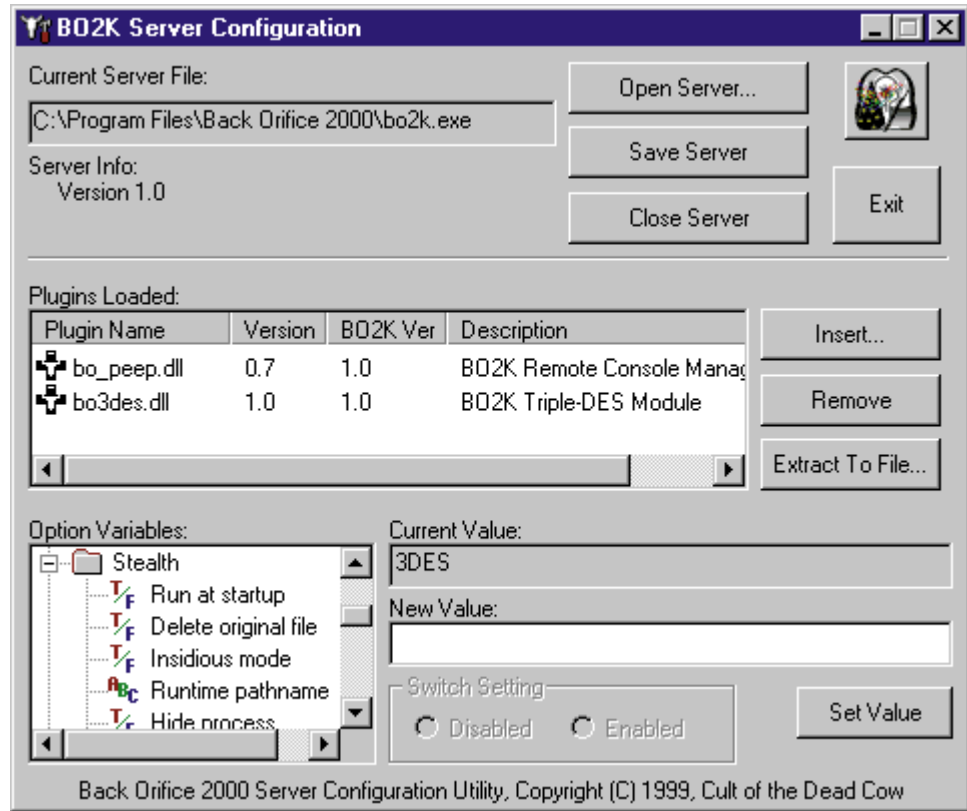
György Ács
Security Consultant
C|EH, SFCP, SFCE

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



Modern támadások

Mi az a malware ?

Malware = **Malicious software**

Bármilyen kód, ami kárt okoz(hat)

Ismeretlen kód, ami érdekes lehet

Típusok

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

Hogyan védekezzünk ellenük, ha nem értjük a működésüket?

Van erre eszközünk?

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
32718	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

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

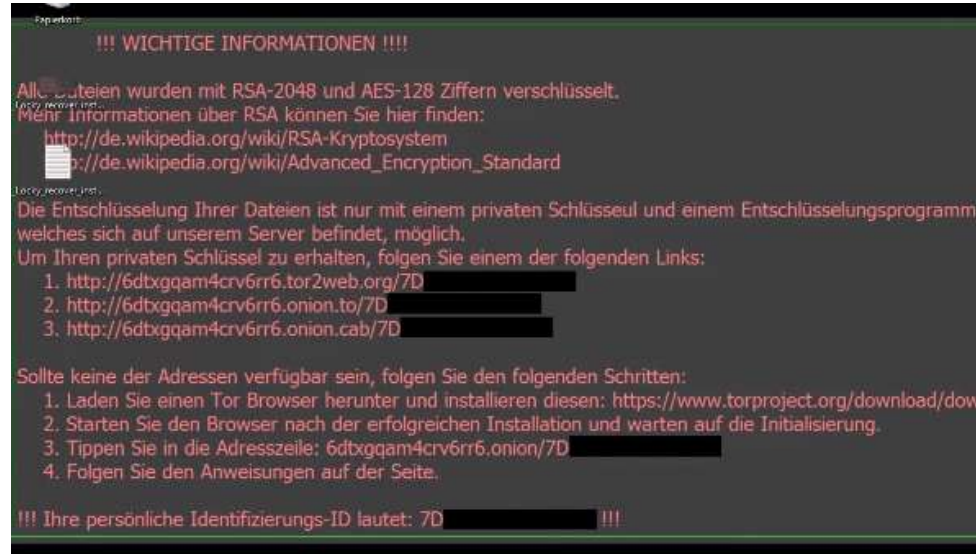
Cryptowall



The screenshot shows a ransomware window titled 'Cryptowall'. The background is red. On the left, there is a blue and white shield icon. Below it, the text reads: 'Your private key will be destroyed on: 4/13/2015' and 'Time left: 00:00'. On the right, a white box contains the following text: 'Your personal files are encrypted! Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete 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 only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window. Once this has been done, nobody will ever be able to restore files... In order to decrypt the files press button to open your personal page File decryption site and follow the instruction. in case of "File decryption button" malfunction use one of our gates: http://34r6hq26q2h4jkzj.42k2bu15.com https://34r6hq26q2h4jkzj.tor2web.blutmagic.de Use your Bitcoin address to enter the site: 1MQrnrWHRo52jt32eUzpNcarSJM Click to copy address to clipboard if both button and reserve gate not opening, please follow the steps: You must install this browser www.torproject.org/projects/torbrowser.html.en After installation, run the browser and enter address 34r6hq26q2h4jkzj.onion Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files. Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.' At the bottom, there are three buttons: 'Click for Free Decryption on site', 'Show files', and 'Enter Decrypt Key'.

Zsaroló programokról ...

- Gyakran fejlődnek és mutálódnak
- Leggyakrabban **emailcsatolmányban**, fertőzött **weboldalakon** terjednek
- akár megbízható weboldalokról 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 ...



PRÉMIUM BELÉPÉS 

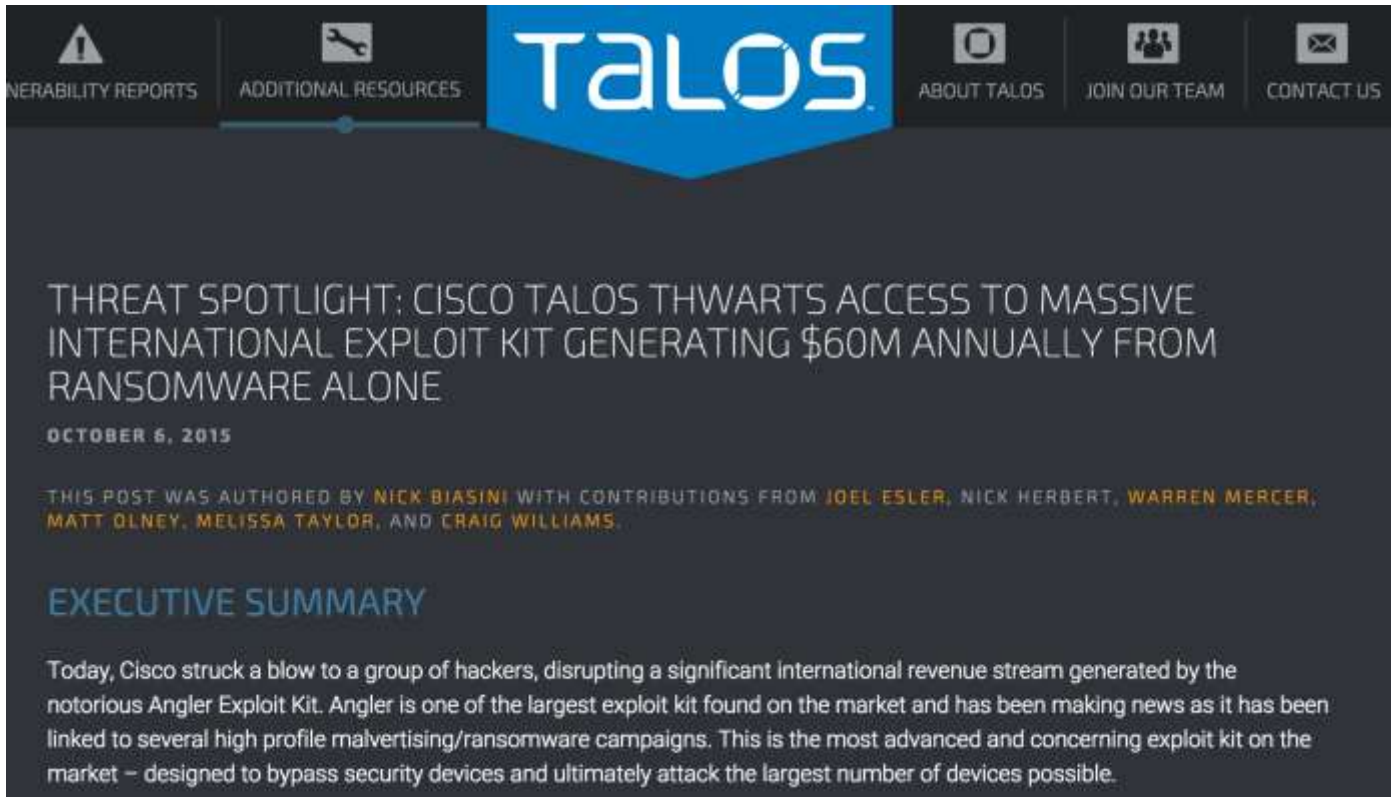
Vírusvédelem • Adatbiztonság • Sebezhetőségek • Családbiztonság • Mobilbiztonság •

Így kerestek milliókat az internetes csalók

Szerző: Kristóf Csaba | Utolsó módosítás: 2015.10.08. 07:32

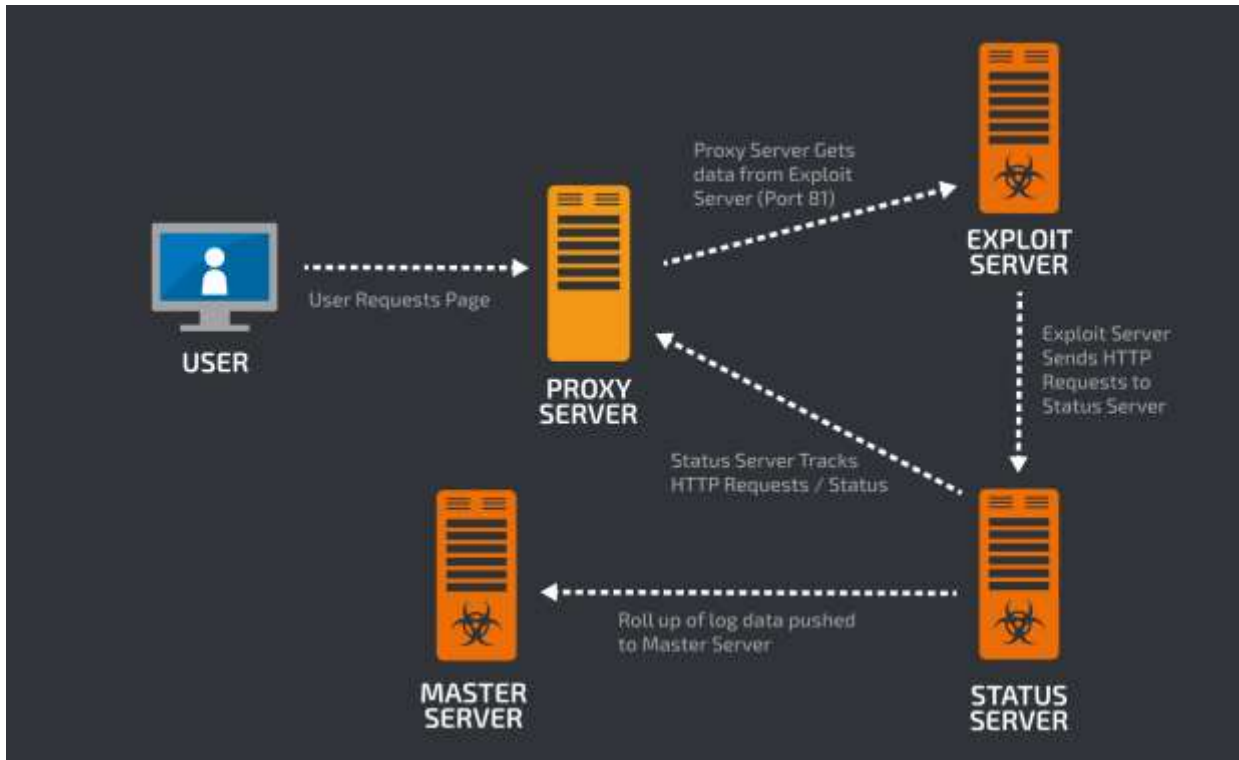
A Cisco jelentős csapást mért egy olyan kiberbűnözői csoportra, amely zsaroló vírusokkal dollár milliókat csalt ki az áldozatul eső felhasználóktól.

Cisco Talos és a zsaroló programok

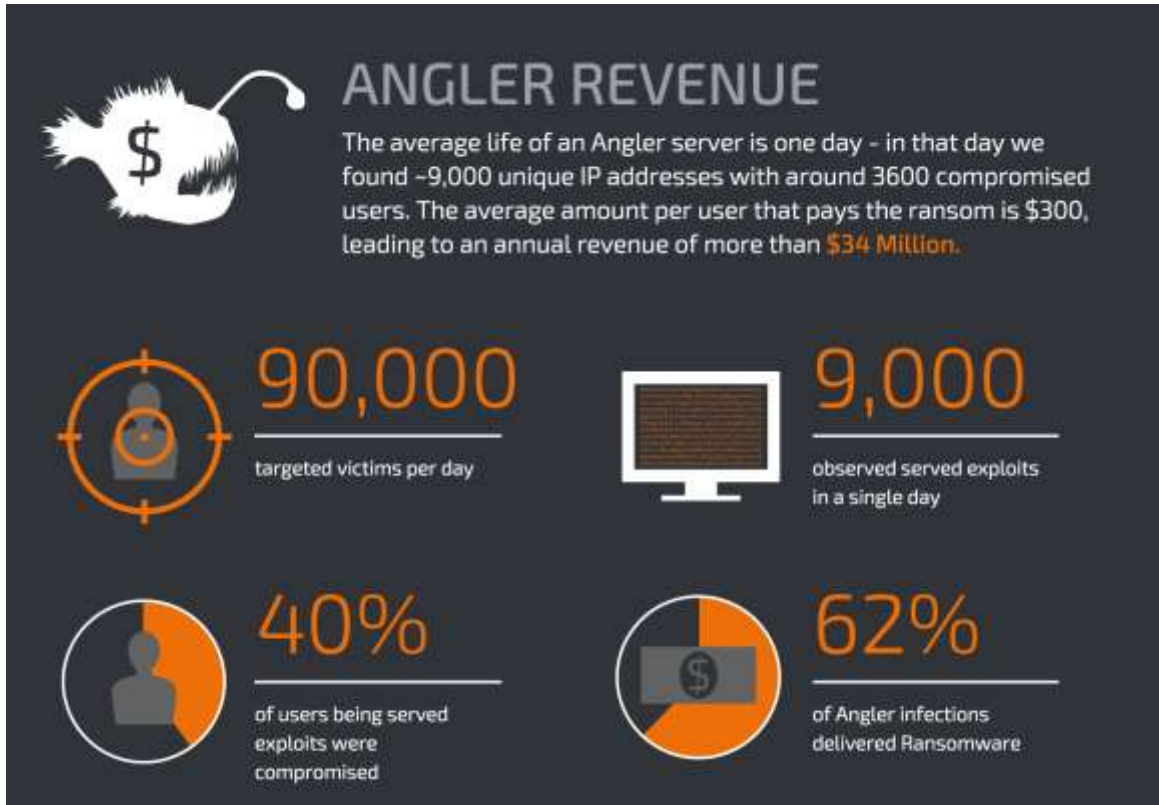


The image shows a screenshot of the Cisco Talos website. At the top, there is a navigation bar with the following items: a warning icon for 'VULNERABILITY REPORTS', a wrench icon for 'ADDITIONAL RESOURCES', the 'TALOS' logo in a blue banner, a camera icon for 'ABOUT TALOS', a group of people icon for 'JOIN OUR TEAM', and an envelope icon for 'CONTACT US'. Below the navigation bar, the main content area features a large headline: 'THREAT SPOTLIGHT: CISCO TALOS THWARTS ACCESS TO MASSIVE INTERNATIONAL EXPLOIT KIT GENERATING \$60M ANNUALLY FROM RANSOMWARE ALONE'. Underneath the headline is the date 'OCTOBER 6, 2015'. A line of text identifies the authors: 'THIS POST WAS AUTHORED BY NICK BIASINI WITH CONTRIBUTIONS FROM JOEL ESLER, NICK HERBERT, WARREN MERCER, MATT OLNEY, MELISSA TAYLOR, AND CRAIG WILLIAMS.' Below this is a section titled 'EXECUTIVE SUMMARY' in blue. The summary text reads: 'Today, Cisco struck a blow to a group of hackers, disrupting a significant international revenue stream generated by the notorious Angler Exploit Kit. Angler is one of the largest exploit kits found on the market and has been making news as it has been linked to several high profile malvertising/ransomware campaigns. This is the most advanced and concerning exploit kit on the market – designed to bypass security devices and ultimately attack the largest number of devices possible.'

Angler infrastruktúra



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












MALWARE DOMAIN LIST

[Homepage](#) | [Forums](#) | [Recent Updates](#) | [RSS update feed](#) | [Contact us](#)

WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

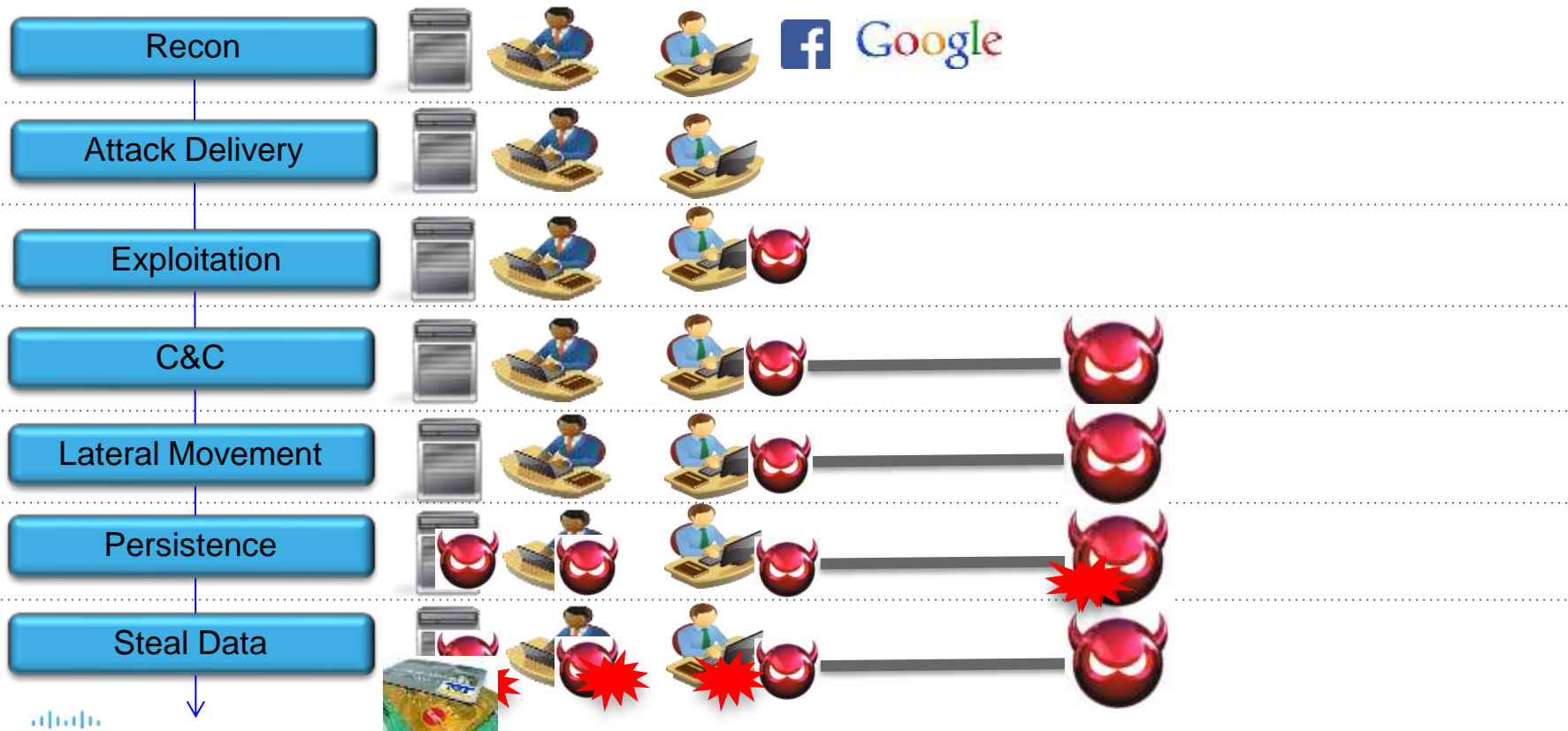
Search: All Results to return: 50 Include inactive sites

Page [0](#) [1](#) ... [37](#)

Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
v u	v u	v u	v u	v u	v u	v u
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.s tatic.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.st atic.arubacloud.fr.	Angler EK	Registrant fitchewb@gmail.com	199653 
2016/04/21_22:30	norfpqr.uerbee.top/expose/1366866/tidings-discovery-chest-serious-character-public-stick	89.36.213.228	host228-213-36-89.st atic.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



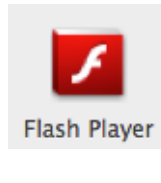
Az áldozat megtámadása

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

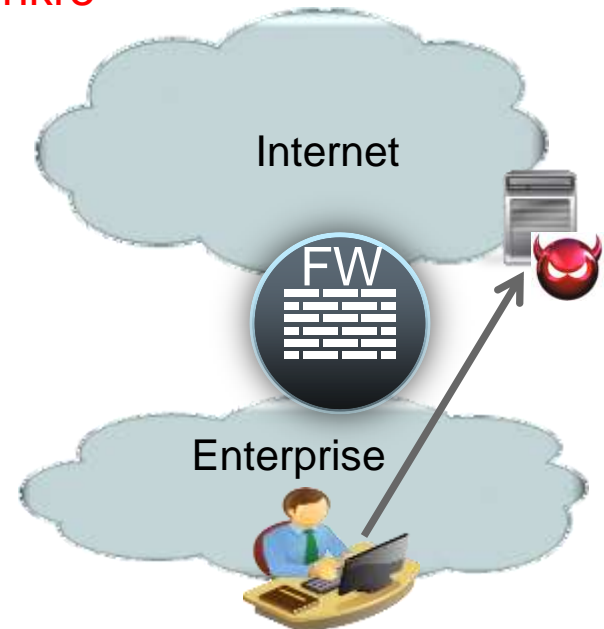
... Futtatható malware indítása

.exe, .msi, .vbs, **.ps1**, .dmg ,

... Sérülékeny alkalmazás/plugin kihasználása



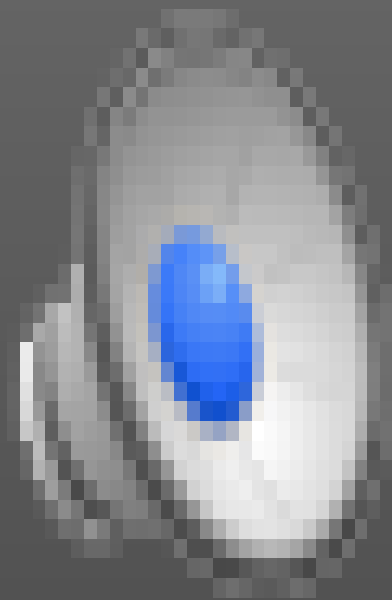
Java





Demonstráció

4 percben Flash alapú spearphising támadás



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

Teszteljük támadás előtt
Türelmes vagyok.
Nekem csak egyszer kell támadnom.



Más rendszerek nem osztják meg a mintákat

av-check,
virtest,
scan4you

The screenshot displays the AV-CHECK website interface. At the top, there is a navigation bar with links for 'Login', 'Check', 'My account', 'News', 'Features', and 'Our products'. Below this is a search bar and a 'Browse...' button. The main content area is divided into several sections:

- Account manager:** Includes a login form with fields for 'E-mail' and 'Password', and a 'Login' button.
- News:** A list of news items with dates and titles.
- Definitions:** A table listing various virus definitions with columns for name, version, and date.

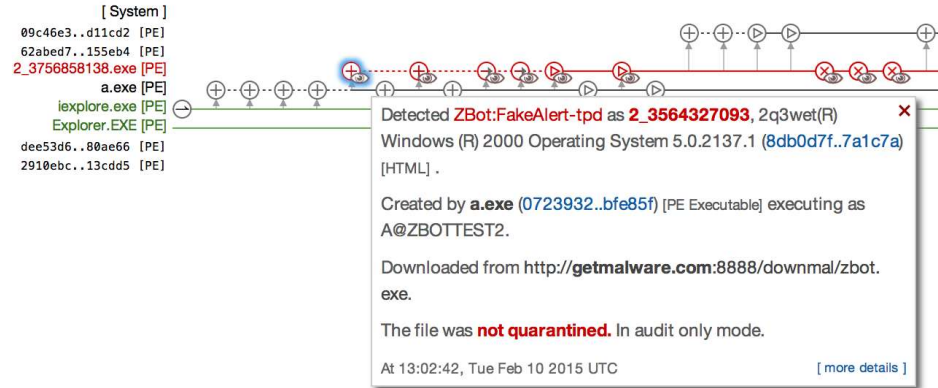
At the bottom of the page, there is a footer with the text: "All definitions are included with default settings and the default detection level of heuristic analysis, as it usually happens on real computers of real users."

This screenshot shows a different part of the AV-CHECK website, likely a user dashboard or control panel. It features a dark blue header with the AV-CHECK logo and the text "НАЧЕННЫЕ ЗАГРУЗКИ ВАШЕГО СЧЕТА". Below the header, there is a "Control Panel" section with a "Home" link. The main content area includes a "News" section with a date of "20.12.2009" and a "Бонусы за баги" (Bonuses for bugs) section. The bonus section contains a "Бонусы за баги" (Bonuses for bugs) heading, a "Получите бонус" (Get bonus) button, and a "Получите бонус" (Get bonus) button. There is also a "Support" section with a "Support" link.

Malware analízis technikák

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 gépen, 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-> assembly konverzió
 - Memory dumper: LordPE, OllyDump



The screenshot displays the IDA Pro interface. At the top, the menu bar includes File, Edit, Jump, Search, View, Debugger, Options, Windows, and Help. The main window is titled 'IDA View-B' and shows assembly code with several lines of '.text:00425690' instructions. A 'WinGraph32 - User defined xrefs chart: save_cfg' window is overlaid on top, showing a graph with various nodes and connections. Below this, the 'DisAsm' window shows assembly code for a function named 'hella_world.exe' with columns for address, disassembly, and comments. The 'HexView' window shows the corresponding hex dump of the assembly code. The 'Comments' window shows the comments for the assembly code. The 'Registers' window shows the state of the registers. The 'Stack' window shows the stack contents. The 'CPU' window shows the CPU registers and flags. The 'CPU' window also shows the CPU registers and flags. The 'CPU' window also shows the CPU registers and flags.

Malware analízis lehetőségei

• 2. Dinamikus analízis

- Viselkedés
naplózása
- Virtuális gép
- Sandboxing
- Debugger (GDB,
WindDBG)



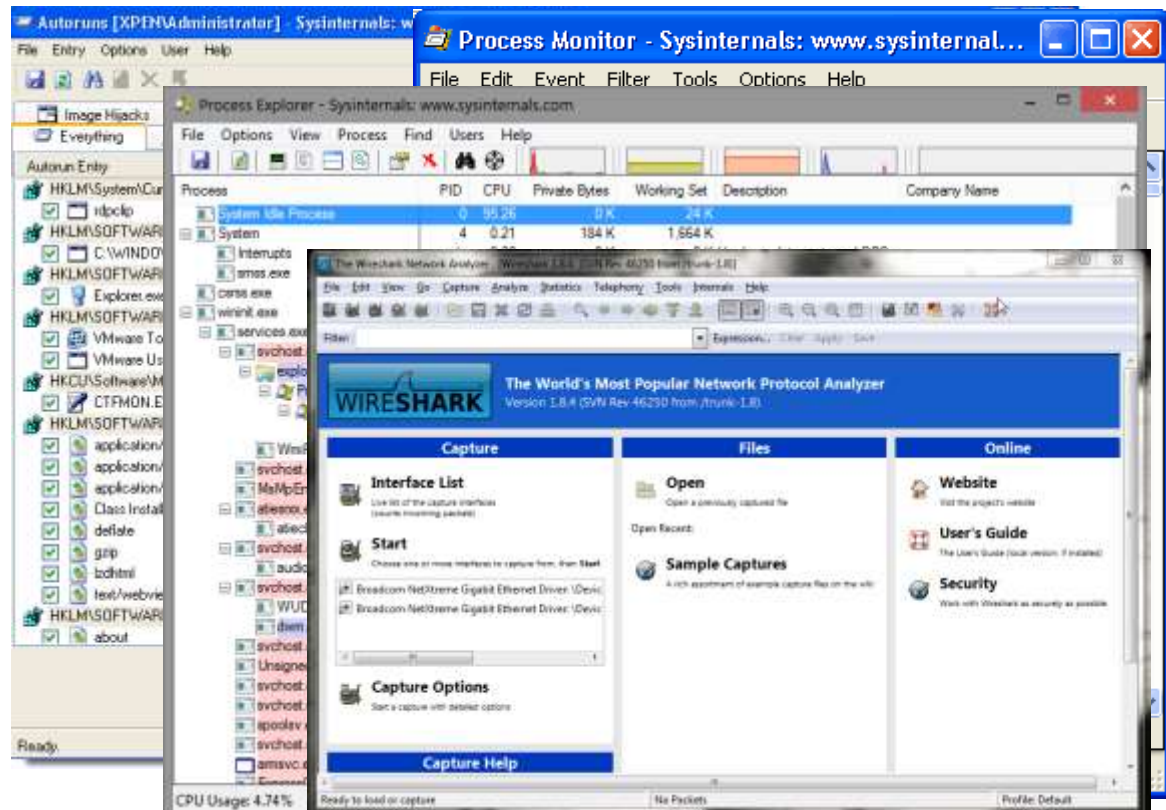
The image shows a screenshot of the Comodo ThreatExpert website. At the top left, the Comodo logo is displayed with the tagline "Creating Trust Online™". Below it, a red banner reads "Comodo Inst". The main navigation bar includes "Home", "ThreatExpert Reports", "Tools", "Threat Browser", "Submit Sample", and "About ThreatExpert". A search bar is located in the top right corner. The main content area is titled "Submit Your Sample To ThreatExpert" and includes an "Attention!" notice about account registration.



The image shows a screenshot of the "malwr" submission form. The logo "malwr" is accompanied by a black beetle icon. Below the logo, a message states: "By submitting the file, you automatically accept our [Terms of Service](#)." The form includes a "Select file" button, a checked checkbox for "Share the sample", and an unchecked checkbox for "Private". A CAPTCHA question "5 + 1 =" is followed by an input field. A blue "Analyze" button is at the bottom. On the right side, there are additional input fields and a "Conditions" link.

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



Mi az a sandboxing?

Sandbox

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



Report
ArtifactsFile,
video

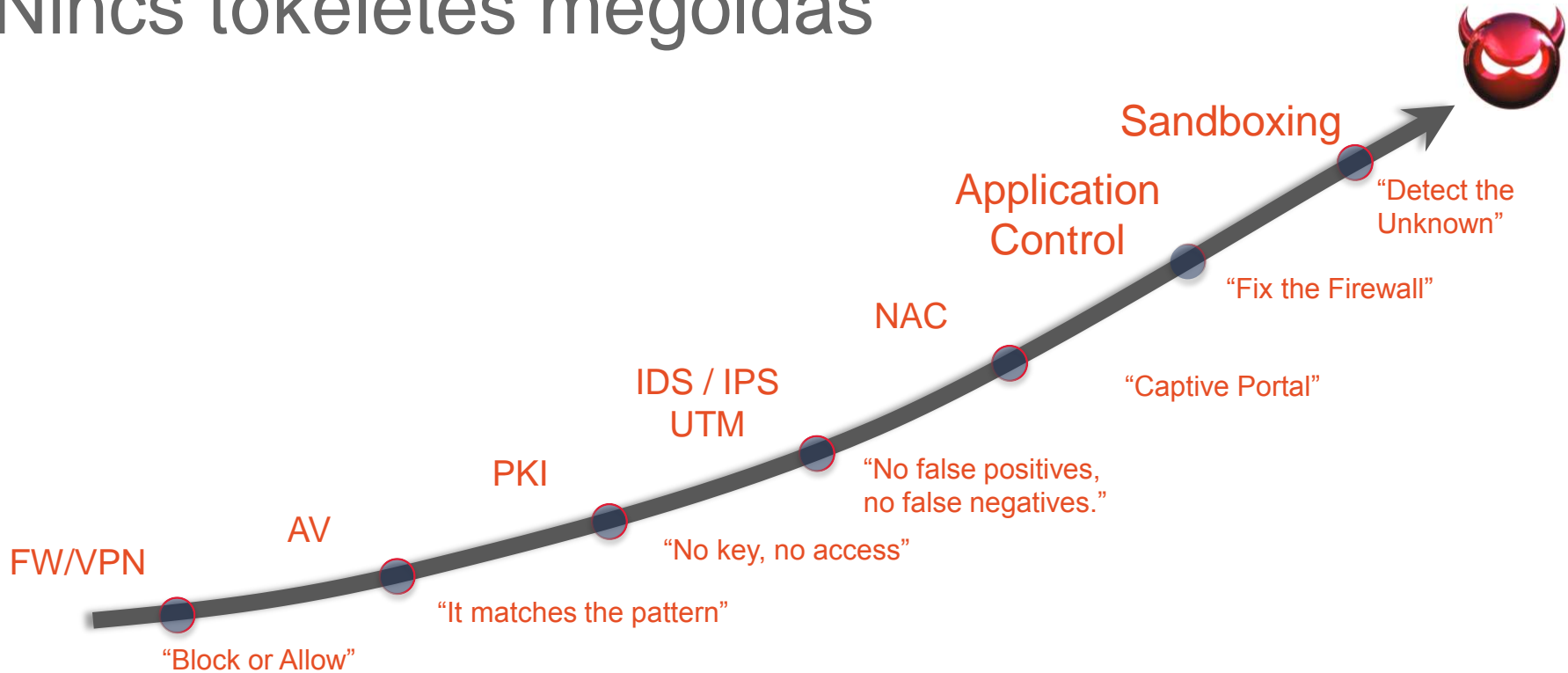


The screenshot shows the ThreatGRID Analysis Report interface. It includes a navigation bar at the top with options like 'Home', 'Behavior Indicators', 'Network Activity', 'Process', 'Artifacts', 'Host Activity', 'File Activity', 'Virus', and 'Download'. The main content area is divided into two sections: 'Analysis Report' and 'Behavioral Indicators'. The 'Analysis Report' section displays metadata such as ID, OS, Name, SHA256, Sandbox, Filesize, Filetype, and Analysis ID. The 'Behavioral Indicators' section shows a 'Threat Score: 81' and a list of indicators, including 'A Document File Established Network Communications'. A 'Categories' list includes 'network, document, malware' and a 'Tags' list includes 'trojan'.

Report :

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

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, ...



Malware sandbox detektálás (piros-kék pirula)

- VM karakterisztikák 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>



Sandbox detekció

“Turing test” vagy felhasználó input - tevékenység

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

Kérlek,
kattints ide ->

Sandboxing



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

ThreatGrid “a” sandbox

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

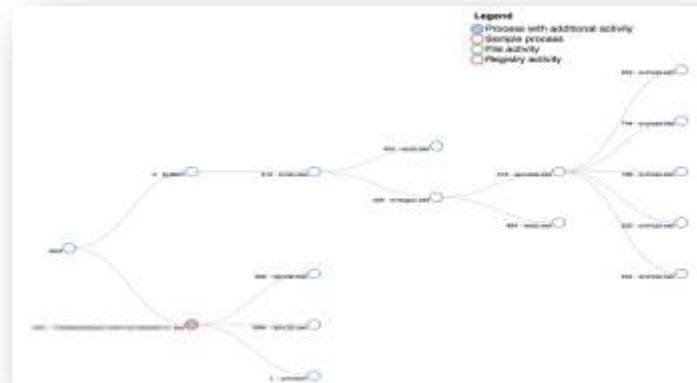
On-premise Appliance: - helyi elemzés

- 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



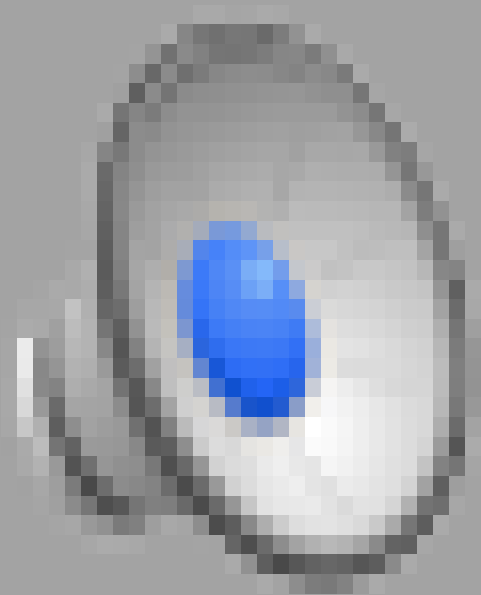
Threat Score

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

Behavioral Indicators						Threat Score: 100
⊕ Artifact Flagged as Known Trojan by Antivirus						Severity: 100 Confidence: 100
⊕ Process Modified an Executable File						Severity: 95 Confidence: 95
⊕ A Document File Established Network Communications						Severity: 90 Confidence: 90
⊕ PDF Contains Embedded JavaScript Stream						Severity: 80 Confidence: 80
⊖ Process Modified Shell Program Autorun Registry Key Value						Severity: 80 Confidence: 60
Autorun registry keys can be used to load applications when Windows is started. Malware often uses these key locations to maintain persistence on the host. The values to examine are located in subkeys Run or load. The key value will indicate where the program that will load on startup is located.				Categories persistence		
				Tags process, autorun, registry		
Process ID	Process Name	RegKey Name	RegKey Value Name	RegKey Data Type	RegKey Data	
1312 (spoolsv.exe)	spoolsv.exe	USERS-1-5-21-1202660629-583907252-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS	load	SZ	C:\DOCUME~1\JOEMAL~1\LOCALS~1\Temp\spoolsv.exe\0	
⊕ Artifact Flagged by Antivirus has Assigned CVE Number						Severity: 70 Confidence: 50
⊕ Process Modified File in a User Directory						Severity: 70 Confidence: 80

ThreatGrid Sandbox Demonstráció

A long-exposure photograph of a city street at night. The image shows light trails from cars and buildings, with a prominent blue light trail on the left. The text 'ThreatGrid Sandbox Demonstráció' is overlaid in white on the left side of the image.



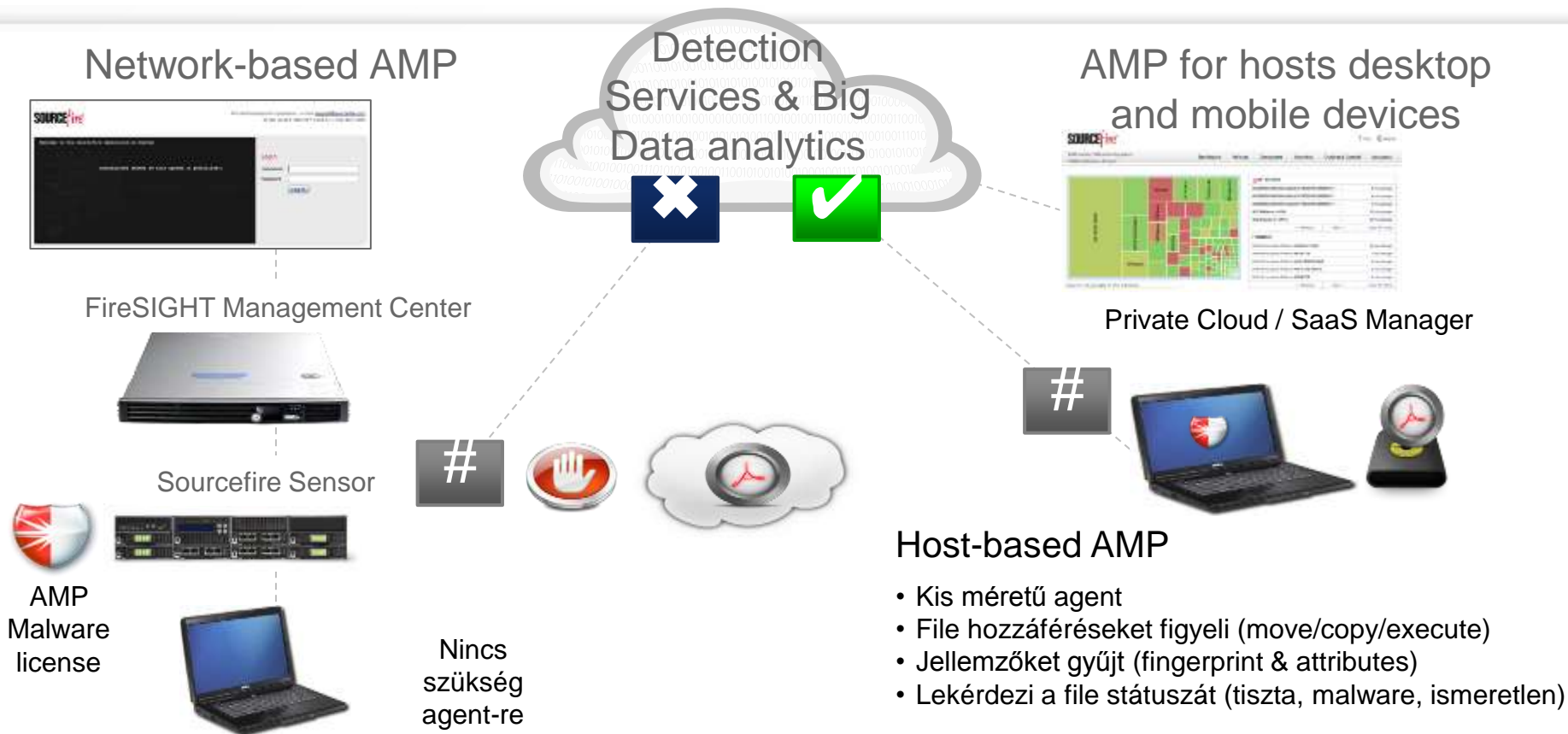
Advanced Malware Protection

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

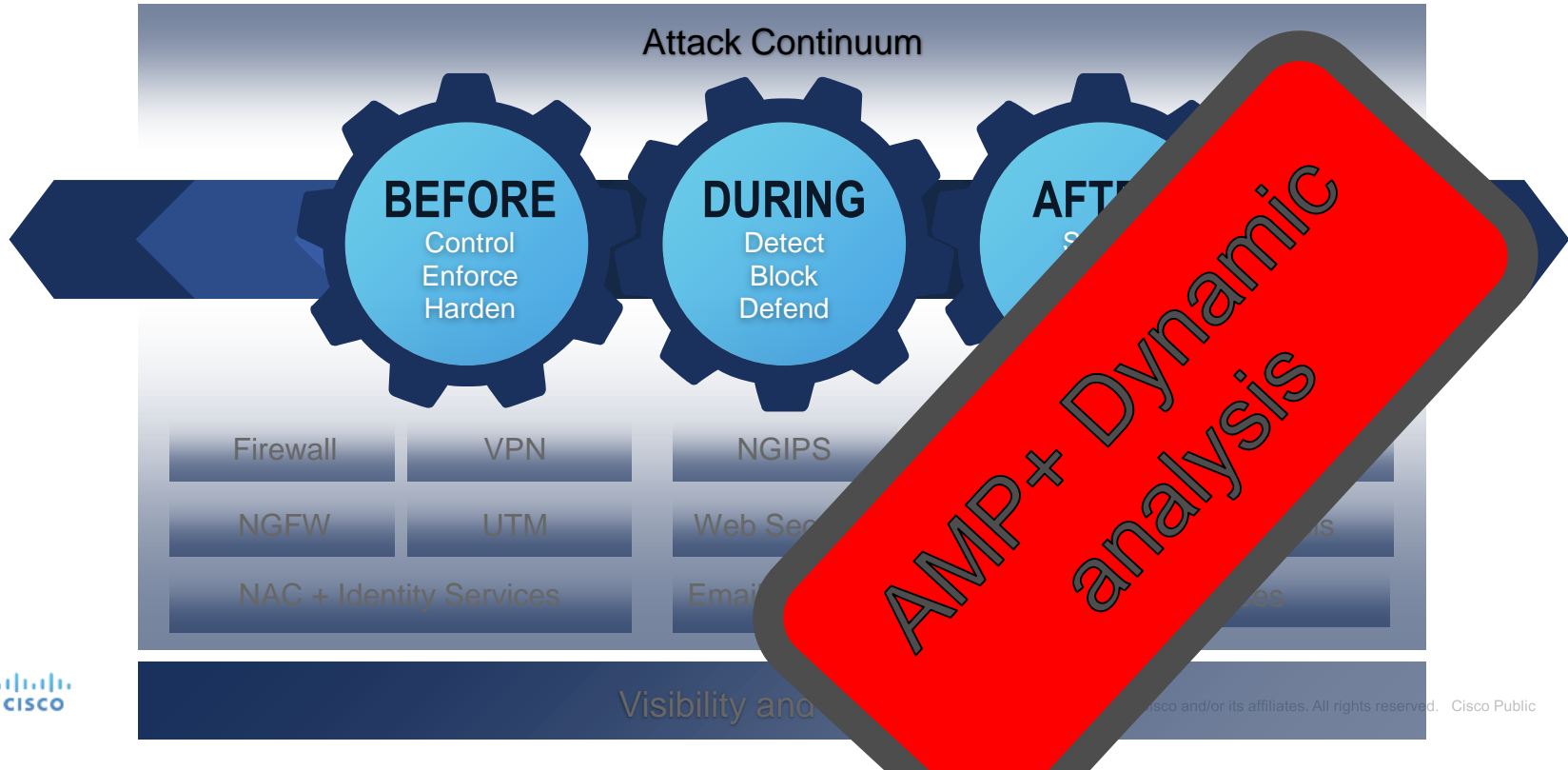
- Marty Roesch
- Chief Architect – Cisco Security Group

Új megközelítés szükséges

AMP: Advanced Malware Protection



Cisco biztonsági model



AMP : Point-in-Time + Retrospective Protection

Point-in-Time Protection

One-to-One
Signature

Fuzzy
Finger-printing

Machine
Learning

Advanced
Analytics

Dynamic
Analysis

File Reputation & Sandboxing

Retrospective Security

Breadth and Control points:

- Email
- Network
- Endpoints
- IPS
- Web
- Devices

Telemetry
Stream

File Fingerprint and Metadata

File and Network I/O

Process Information

Continuous feed

1001 1101 1110011 0110011 1011
101000 0110 00 0111000 11
01110001110 1001 1101 1110

Continuous Analysis

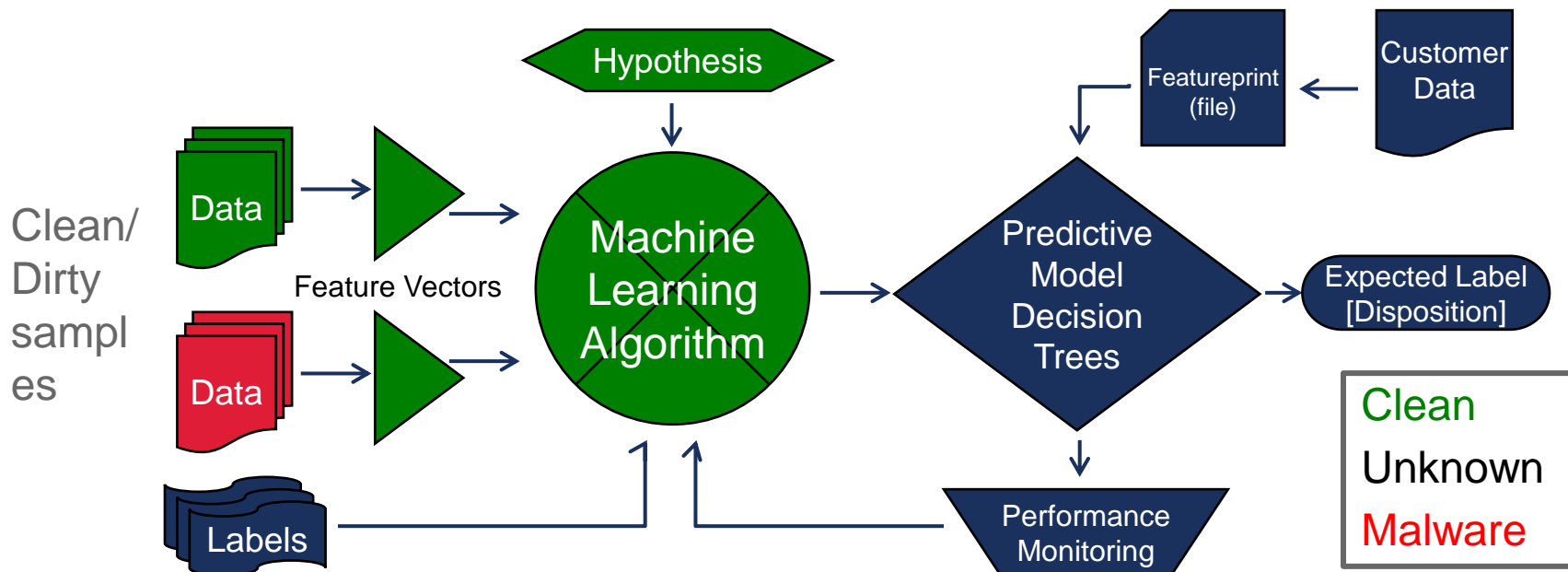
Protection Framework: Ethos Engine

- 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



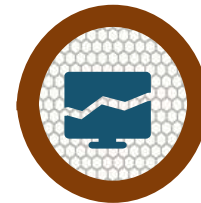
Protection Framework: Spero Engine

- 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 letapodtatás
- OpenIOC 1.1 eredet

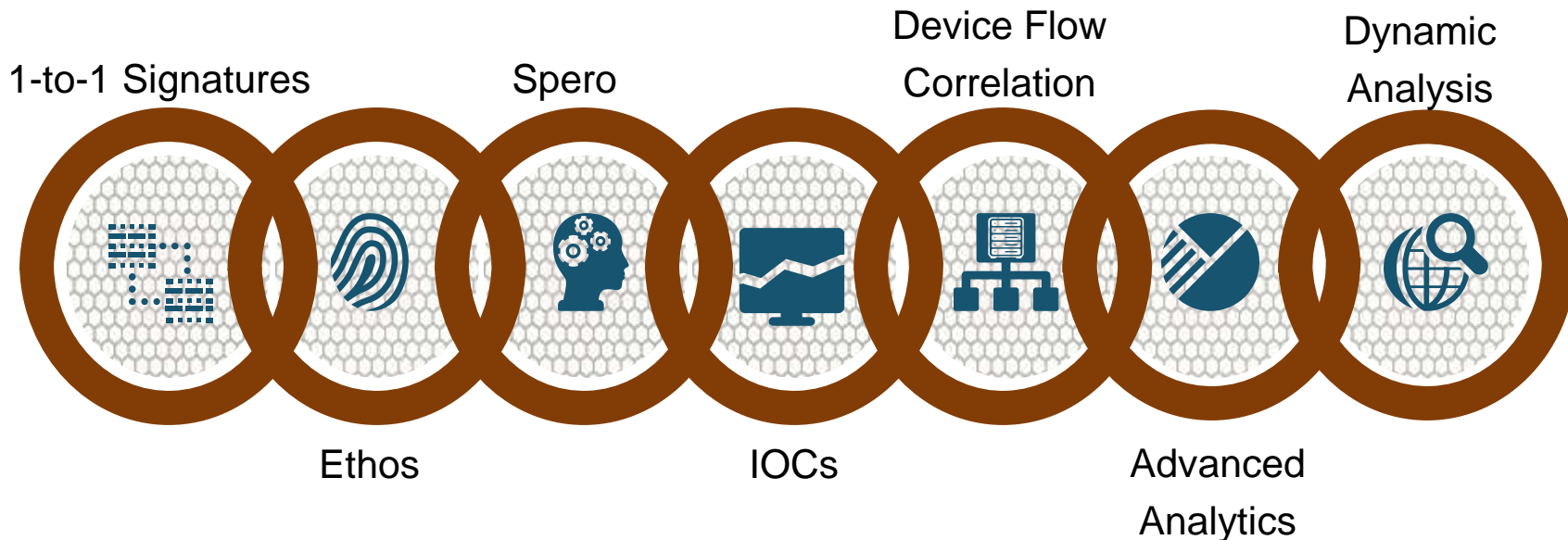


Wikipedia:

“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

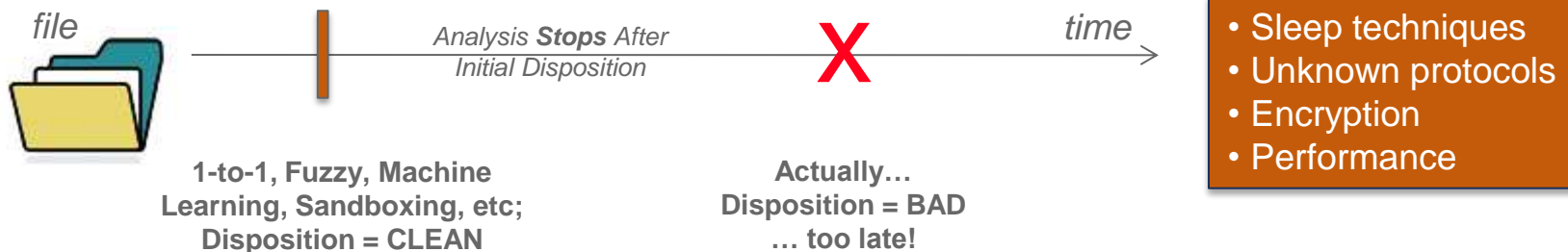
Plan A: The Protection Framework



All Methods < 100% Detection

Plan B: Retrospection

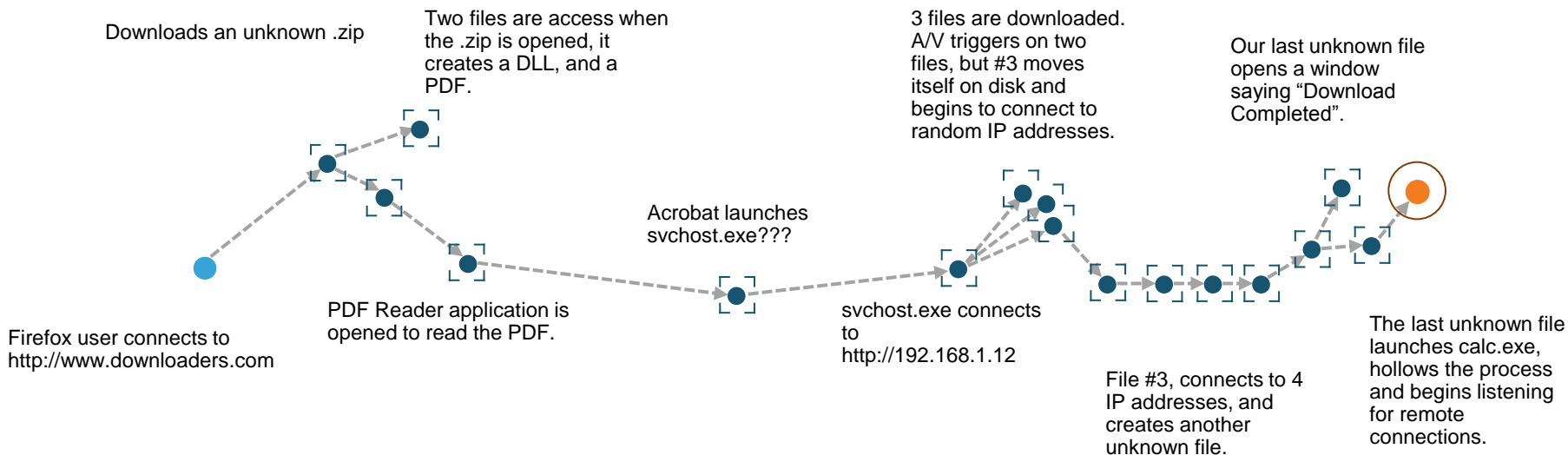
Typical Analysis



Continuous Analysis



Retrospection Framework: Trajectory



Nyomkövetés alkalmazás és hálózati szinten: trajectory

Overview **Analysis** Policies Devices Objects AMP Health

Context Explorer Connections Intrusions **Files > Network File Trajectory** Hosts Users Vulnerabilities Correlation Custom Search

Network File Trajectory

File SHA256
File Names
File Type
File Category
Current Disposition
Threat Score
Threat Name

Trajectory

10.0.168.37
10.110.10.69
10.131.13.174
10.0.112.66
10.0.68.26
143.242.85.169
10.0.112.63
10.0.121.146
10.0.192.123
10.0.202.100

Dynamic Analysis Summary

Report 100% (100) 20

Threats

- Persistence and I
- Spreading
- Virtual Machine D
- Networking
- System Summary
- Anti Debugging
- Boot Survival
- HIPS / PFW / Op
- Language, Device
- Data Obfuscation
- AV Detection

Process Tree

```
76708761.exe (pid: 496)
├── QuickTimeQuickTi
├── moFilesystem12.0.4
├── QuickTimeResourc
├── QuickTimeQu
└── QuickTimeRe
```

ThreatGRID

Malware Threat Intelligence Platform

Metadata Behavioral Indicators Network Activity Processes Artifacts Registry Activity File Activity

Analysis Report

ID 161f9749a229a65f41478904fa49a55e
OS 2600.xpsp.080413-2111
Started 2/14/15 22:58:50
Ended 2/14/15 23:05:12
Duration 0:06:22
Sandbox influenza (pilot-d)

Filename BitcoinVPN.exe
Magic Type PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Analyzed exe

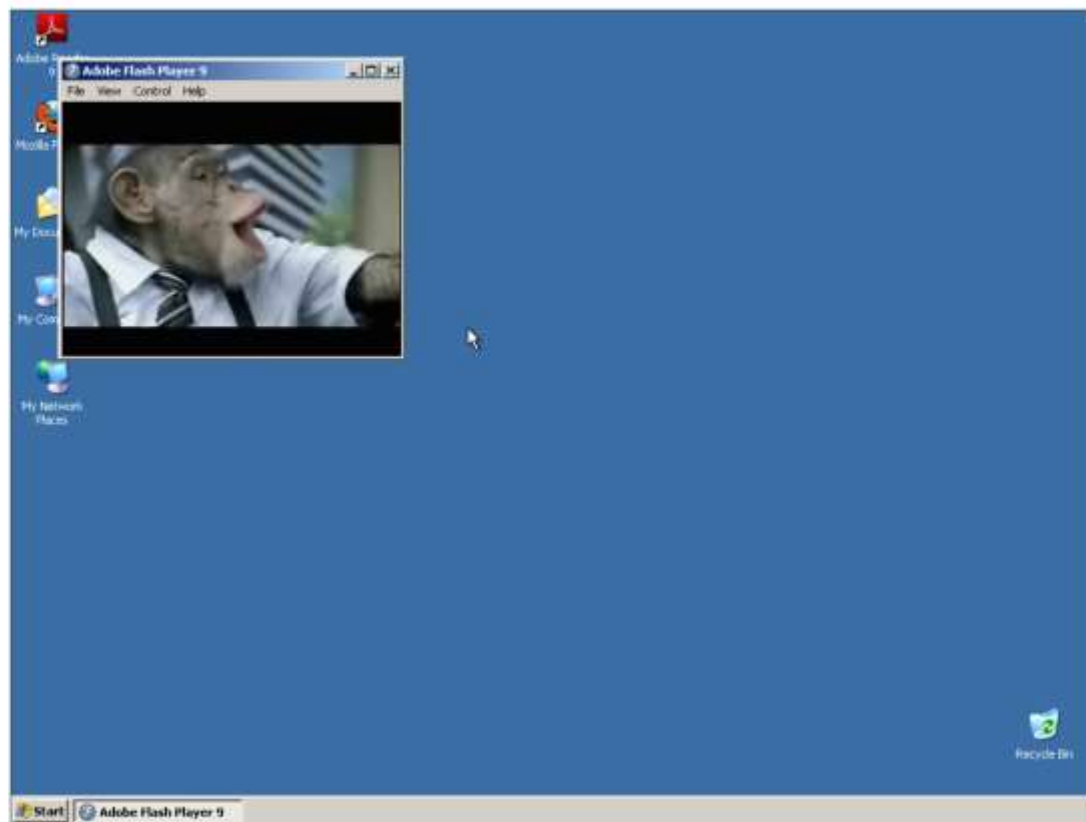
As
SHA256 bc4da231bfc6111ce7c6f6be40359da9e2e1971cb24Feed6c50c3a26f5b4f0ec
SHA1 ae2beadef6491162e0f0f9456eb949238a20ee2c
MD5 3a2e0b377e9e4b5d491c0db184d05be96

Warnings

- Executable Failed Integrity Check

Behavioral Indicators

- Artifact Flagged as Known Trojan by Antivirus Severity: 100 Confidence: 100
- Domain Resolves to a Known DNS Sinkhole Severity: 100 Confidence: 100
- Domain Malicious Detected Severity: 100 Confidence: 100



4:39 / 20:00

File downloaded to disk

File Name of Executable on Disk Does Not Match Original File Name

Severity: 60 Confidence: 60

Severity: 40 Confidence: 60

Close

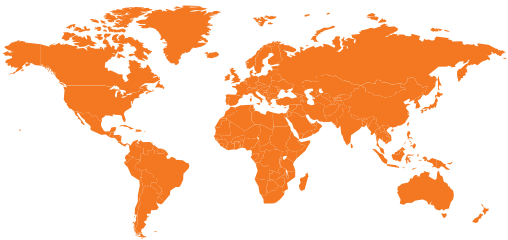
A DNS csatorna biztonsága : OpenDNS

Why OpenDNS?

DNS Services Built for World's Largest Security Platform

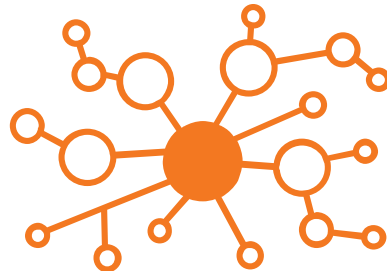
GLOBAL NETWORK

- 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



UMBRELLA Enforcement



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

Ajánlások

Mit tudunk mi tenni ? Közösségi együttműködés

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



 Immundet™



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 kontrollt ad

A VÁLASZIDŐ CSÖKKENTÉSE ..

A BETÖRÉS OKOZTA KÖLTSÉGEK CSÖKKENTÉSE

