

Dinamik Analiz

Dinamik analiz zararlıyı çalıştırarak gerçekleştirilen analiz sürecidir. Genellikle izole ve güvenli sistemler haline getirilmiş sandboxlarda gerçekleştirilir.

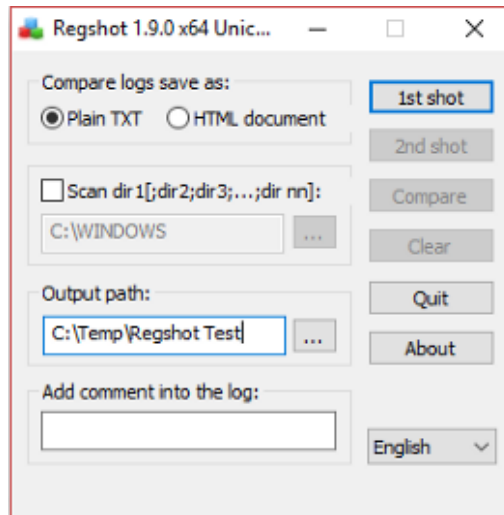
Davranışsal analiz, aktif debuglama, ağ analizi, API çağrısı incelenmesi, Memory Dump Analizi dinamik analiz metodlarındandır.

Dinamik analiz, basic (temel) ve advanced (gelişmiş) olarak ikiye ayrılabilir.

Temel dinamik analiz, araçları kullanarak bulgu keşfetmek ve zararlının davranışını anlamak olarak tanımlanırken gelişmiş dinamik analiz zararlıyı debuglamak, patchlemek üzerine kurulmuştur.

Regshot

Regshot Windows Registrysinin “önce ve sonra” snapshotlarını alıp bunları karşılaştırmaya yarayan bir araç. Snapshotlar arasındaki farklılıklara göre zararlının davranışları (ek droplanmış dosyalar ve birkaç diğer IoC) tespit edilebilir.



Procmon

Process Monitor, Windows sistemlerinde registry, filesystem, dll, thread, process ve ağ davranışlarının eş zamanlı incelenebildiği bir araçtır. Fikir olarak RegMon ve FileMon adlı iki aracın birleştirilmesi ile başlamıştır. Anlık sistem durumunun captureu alınabilir. Çıktılar filtrelenebilir. (PID, kullanıcı adı, zaman, tarih...)

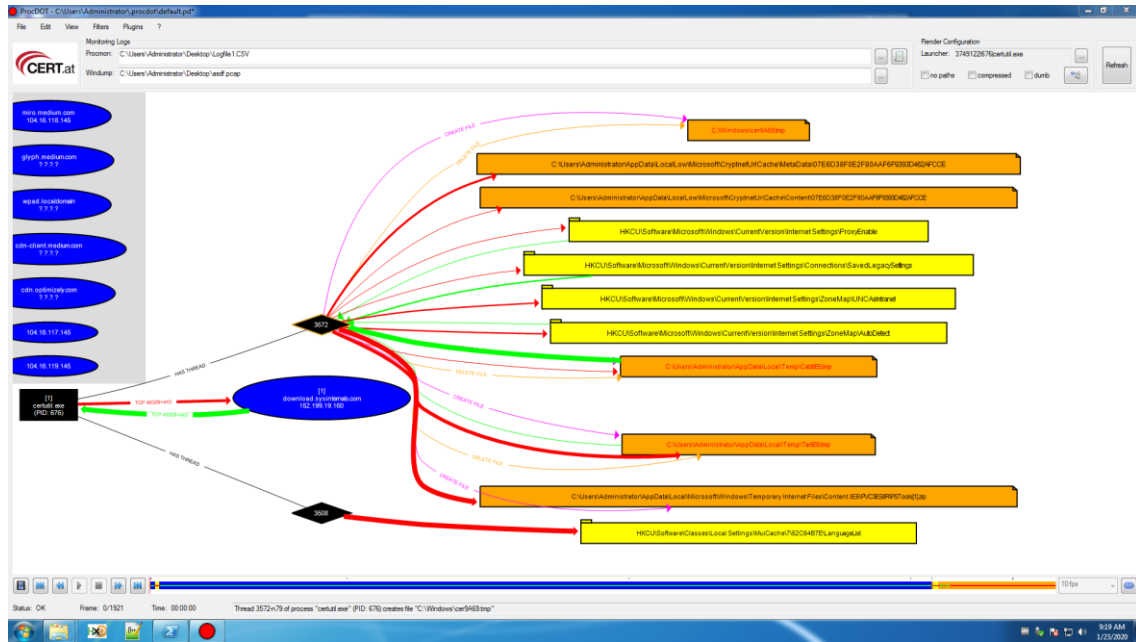
Process Tree özelliğini kullanarak processler arası parent-sibling ilişkileri incelenebilir.

Time o...	Process Name	PID	Operation	Path	Result	Detail
10:01:51...	lsass.exe	832	CreateFile	C:\Windows\System32\Microsoft\Protect...	SUCCESS	Desired Access: G...
10:01:51...	lsass.exe	832	CloseFile	C:\Windows\System32\Microsoft\Protect...	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_DW...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ Le...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\Software\Microsoft\Cryptography...	SUCCESS	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	KeySelfInformation...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ Le...
10:01:51...	sw2_service.exe	3732	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	Type: REG_SZ Le...
10:01:51...	sw2_service.exe	3732	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\Software\Microsoft\Cryptography...	NAME NOT FOUND	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\Software\Microsoft\Cryptography...	NAME NOT FOUND	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptogra...	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegCloseKey	HKLM\SOFTWARE\SecureW2\License	SUCCESS	
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Serv...	REPARSE	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\System\CurrentControlSet\Serv...	SUCCESS	Desired Access: R...
10:01:51...	sw2_service.exe	3732	RegOpenKey	HKLM\System\CurrentControlSet\Serv...	NAME NOT FOUND	Length: 144
10:01:51...	sw2_service.exe	3732	RegCloseKey	HKLM\System\CurrentControlSet\Serv...	SUCCESS	

Showing 460,776 of 956,665 events (48%) Backed by virtual memory

ProcDot

ProcDOT daha çok yan araç olarak düşünülebilir. Procmon çıktısını tree haline getirebilmektedir. Ayrıca başka bir araçtan çıkarılmış ağ hareketlerinin de girdi olarak verilmesi durumunda onu da treenin içine eklemektedir.



Process Explorer

Process Explorer, görev yöneticisinin çok daha işlevli ve sofistike hali olarak düşünülebilir. Çalışan processleri renklendirerek farklı bilgiler vermektedir.

Pembe: Process servisi hostlamaktadır.

Mavi: Process, Process Explorer ile aynı güvenlik şartlarına (aynı kullanıcı) sahiptir.

Turkuaz: Process, Windows Uygulamalarındandır.

Yeşil: Yeni processler anlık olarak yeşil gözükür.

Kırmızı: Biten processler anlık olarak kırmızı gözükür.

Gri: Durdurulmuş processler gri gözükür.

Koyu Mavi: Paketlenmiş processler koyu mavi gözükür.

Beyaz: Yukarıdaki şartlardan hiçbirine uymamaktadır.

Kendi içerisinde VirusTotal'e çıkabilmektedir.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Autostart Location	Verified Signer	Process Timeline	Integrity	VirusTotal
System Idle Process	0.72	0 K	4 K	0						System	
System	0.87	0 K	0 K	n/a	Hardware Interrupts and DPCs					System	
smss.exe		376 K	504 K	364	Windows Session Manager	Microsoft Corporation		(Verified) Microsoft		System	
csrss.exe	< 0.01	716 K	55,848 K	2672	Client Server Runtime Process	Microsoft Corporation		(Verified) Microsoft		System	
csrss.exe		1,948 K	2,020 K	528	Windows Start-Up Application	Microsoft Corporation		(Verified) Microsoft		System	
services.exe	< 0.01	4,356 K	5,748 K	788	Services and Controller app	Microsoft Corporation		(Verified) Microsoft		System	
svchost.exe	< 0.01	17,372 K	20,016 K	892	Host Process for Windows S...	Microsoft Corporation	HKLM\System\Cu...	(Verified) Microsoft		System	
WmPrvSE.exe		3,548 K	7,208 K	5932	WMI Provider Host	Microsoft Corporation		(Verified) Microsoft		System	
RuntimeBroker.exe		17,944 K	46,132 K	4020	Runtime Broker	Microsoft Corporation		(Verified) Microsoft		Medium	
ShellExperienceHost.exe	0.29	47,824 K	89,584 K	4356	Windows Shell Experience H...	Microsoft Corporation		(Verified) Microsoft		AppContainer	
SearchUI.exe	Susp...	66,488 K	1,15,868 K	10196	Search and Content applicat...	Microsoft Corporation		(Verified) Microsoft		AppContainer	
SearchHost.exe	Susp...	32,496 K	10,364 K	7200	Microsoft Search Preview	Microsoft Corporation		(Verified) Microsoft		AppContainer	
SettingsSyncHost.exe		14,804 K	5,176 K	5164	Host Process for Setting S...	Microsoft Corporation		(Verified) Microsoft		Medium	
CallSvc.exe		3,000 K	5,820 K	3740	Calling protocol connection...	Microsoft Corporation		(Verified) Microsoft		Medium	
dhcpcd.exe		3,420 K	10,472 K	12084	COM Surrogate	Microsoft Corporation	HKLM\System\Cu...	(Verified) Microsoft		Medium	
ApplicationFrameHost.exe		4,716 K	19,752 K	5284	Application Frame Host	Microsoft Corporation		(Verified) Microsoft		Medium	
SystemSettingsBroker.exe		4,852 K	20,084 K	7940	System Settings Broker	Microsoft Corporation		(Verified) Microsoft		Medium	
emrtacore.exe		8,316 K	13,828 K	9424	SmartScreen	Microsoft Corporation		(Verified) Microsoft		Medium	
BackgroundTaskHost.exe	Susp...	17,252 K	42,856 K	4288	Background Task Host	Microsoft Corporation		(Verified) Microsoft		AppContainer	
svchost.exe		8,652 K	10,356 K	964	Host Process for Windows S...	Microsoft Corporation	HKLM\System\Cu...	(Verified) Microsoft		System	
svchost.exe	< 0.01	1,10,636 K	95,948 K	524	Host Process for Windows S...	Microsoft Corporation	HKLM\System\Cu...	(Verified) Microsoft		System	
WUDFHost.exe		1,756 K	1,824 K	1116	Windows Driver Foundation...	Microsoft Corporation		(Verified) Microsoft		System	
dasHost.exe		972 K	356 K	2244	Device Association Framework...	Microsoft Corporation		(Verified) Microsoft		System	
svchost.exe		18,796 K	20,540 K	852	Host Process for Windows S...	Microsoft Corporation	HKLM\System\Cu...	(Verified) Microsoft		System	
svchost.exe	< 0.01	13,832 K	17,616 K	396	Host Process for Windows S...	Microsoft Corporation	HKLM\System\Cu...	(Verified) Microsoft		System	
svchost.exe		19,216 K	26,648 K	1104	Host Process for Windows S...	Microsoft Corporation	HKLM\System\Cu...	(Verified) Microsoft		System	
svchost.exe		68,396 K	75,216 K	1292	Host Process for Windows S...	Microsoft Corporation	HKLM\System\Cu...	(Verified) Microsoft		System	
phost.exe		6,212 K	23,852 K	200	Shell Infrastructure Host	Microsoft Corporation		(Verified) Microsoft		Medium	
taskhost.exe		7,368 K	21,000 K	12112	Host Process for Windows T...	Microsoft Corporation		(Verified) Microsoft		Medium	
msiexec.exe		6,580 K	3,936 K	4732	Office Telemetry Agent	Microsoft Corporation	Task Scheduler\...	(Verified) Microsoft		Medium	
SIHClient.exe	< 0.01	1,744 K	4,692 K	8680	SIH Client	Microsoft Corporation	Task Scheduler\...	(Verified) Microsoft		System	
conhost.exe	0.01	1,356 K	2,740 K	652	Console Window Host	Microsoft Corporation		(Verified) Microsoft		System	
gscUserService.exe		2,680 K	4,624 K	1392	gscUserService Module	Intel Corporation	HKLM\System\Cu...	(Verified) Intel(R) p...		System	
svchost.exe		2,948 K	6,540 K	1576	Host Process for Windows S...	Microsoft Corporation	HKLM\System\Cu...	(Verified) Microsoft		System	
audiodg.exe	6.76	85,000 K	72,148 K	840	Windows Audio Device Grap...	Microsoft Corporation		(Verified) Microsoft		System	
RAVBg64.exe		1,956 K	2,964 K	1680	Realtek Audio Service	Realtek Semiconductor	HKLM\System\Cu...	Verifying...		System	
RAVBg64.exe		5,940 K	14,288 K	11144	HD Audio Background Proc...	Realtek Semiconductor		Verifying...		System	
RAVBg64.exe		5,624 K	13,724 K	424	HD Audio Background Proc...	Realtek Semiconductor		Verifying...		System	
svchost.exe	< 0.01	28,888 K	32,272 K	1808	Host Process for Windows S...	Microsoft Corporation	HKLM\System\Cu...	(Verified) Microsoft		System	

CPU Usage: 14.01% Commit Charge: 38.32% Processes: 104 Physical Usage: 41.74%

Process Hacker

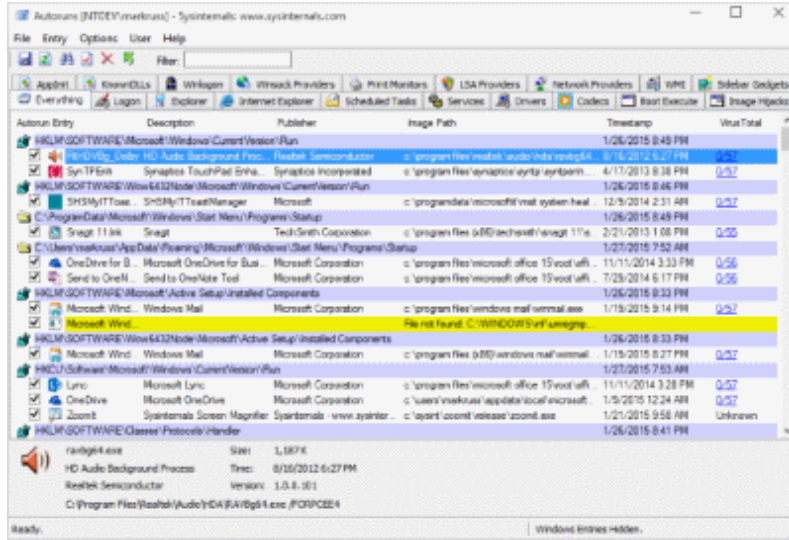
Process Hacker, Process Explorer'ın özelliklerinin yanında gizli processleri gösterebilmei servis oluşturma, DLL inject etme gibi birçok özelliğe sahiptir. Sistemde çalışan processleri bir arada görmemizi sağlar.

Name	PID	Pvt. Memory	CPU	I/O Total	Username	Description
System Idle Process	0	0 B	93.08		SYSTEM	System Idle Process
csrss.exe	384	1.93 MB			SYSTEM	Client Server Runtime Process
winit.exe	456	1.44 MB			SYSTEM	Windows Start-Up Application
csrss.exe	484	3.23 MB		744 B/s	SYSTEM	Client Server Runtime Process
conhost.exe	2776	1.13 MB			Nakodari	Console Window Host
conhost.exe	3424	1.13 MB			Nakodari	Console Window Host
winlogon.exe	620	2.68 MB			SYSTEM	Windows Logon Application
explorer.exe	1520	69.75 MB	3.85		Nakodari	Windows Explorer
mssecss.exe	1620	3.98 MB			Nakodari	Microsoft Security Essentials U...
firefox.exe	2652	210.69 MB			Nakodari	Firefox
msnmsgr.exe	3624	35.54 MB		16 B/s	Nakodari	Windows Live Messenger
WindowsLiveWriter.exe	3520	46.51 MB			Nakodari	Windows Live Writer
SnippingTool.exe	296	9.44 MB			Nakodari	Snipping Tool
grokify.exe	2052	9.21 MB			Nakodari	Gmail Notifier
iTunesHelper.exe	4032	5.66 MB			Nakodari	iTunesHelper Module
iTunes.exe	4040	85.43 MB		361 B/s	Nakodari	iTunes
AppleMobileDeviceHelper.exe	1044	19.64 MB			Nakodari	AppleMobileDeviceHelper
distroted.exe	1120	10.4 MB			Nakodari	distroted.exe
ProcessHacker.exe	3776	51.07 MB	0.77		Nakodari	Process Hacker

50 processes CPU: 6.15% Phys. Memory: 50.10%

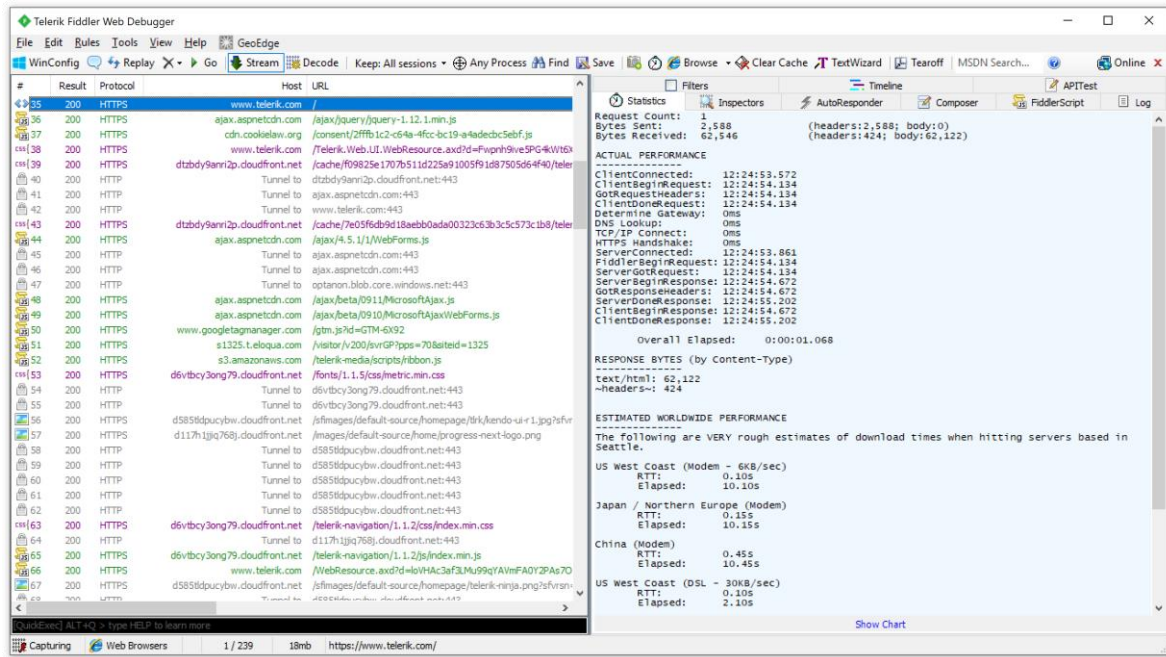
Autoruns

Sistem açıldığında çalıştırılan tüm programları gösteren bir araç.



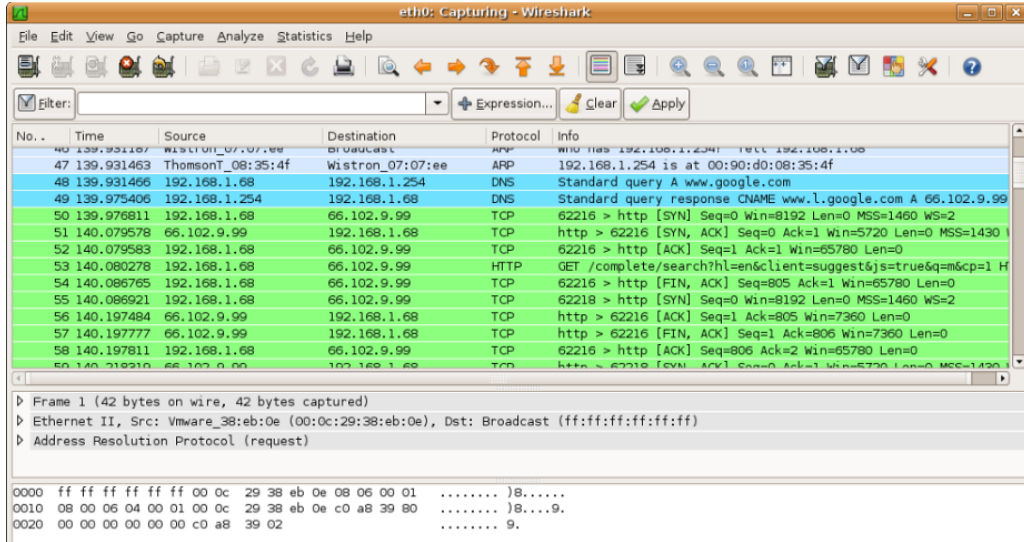
Fiddler

(Telerik) Fiddler platform/tarayıcıdan bağımsız ücretsiz bir web debugging proxy'sidir. Genellikle ağ trafiğini gözlemlemek için kullanılsa da kendi içerisinde HTTPS trafiğini çözümlmek, request atmak gibi birçok feature ve özelleştirme bulundurmaktadır.



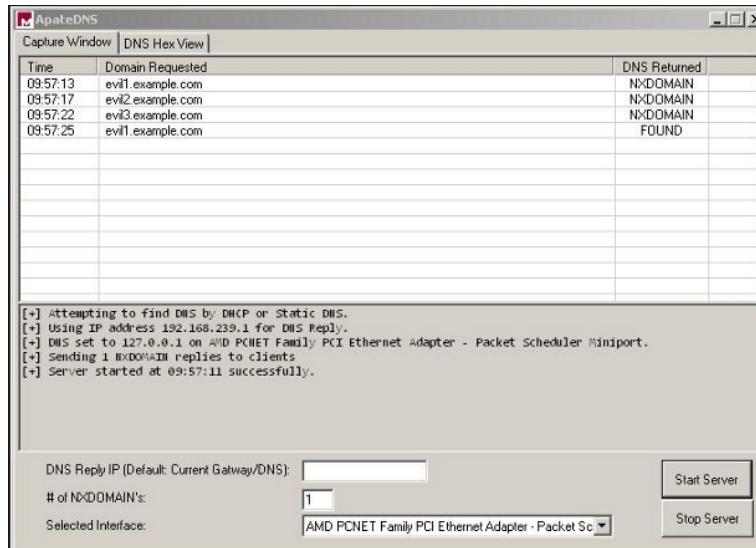
Wireshark

Paket snifflerme aracı. Ağ trafiğinin arasına girer. Bulunan TCP session'ının içeriklerini incelemek için session'a sağ tıklayıp Follow TCP stream demeniz yeterlidir.



1.3.1.9 ApatDNS

DNS isteklerini gösteren bir araç. Kullanıcının özel olarak belirttiği bir IP adresinin 53. portunda UDP dinleyerek DNS yanıtlarını çekebilmektedir.



1.3.1.10 Netcat

Netcat, TCP/IP işiçre çıkışı olarak adlandırılır. Inbound ya da outbound bağlantılar için port tarama, tünelleme, Proxy oluşturma, port yönlendirme gibi birçok işlevi bulunmaktadır. Dinleme modundayken server (sunucu), bağlantı modundayken client (alıcı) olarak davranır.

```
root@kali:~/Documents/PWK/lab/10.11.1.13# nc -lvp 31337
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::31337
Ncat: Listening on 0.0.0.0:31337
Ncat: Connection from 10.11.1.13.
Ncat: Connection from 10.11.1.13:3196.

root@kali:~/Documents/PWK/lab/10.11.1.13# netcat -lvp 31337
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::31337
Ncat: Listening on 0.0.0.0:31337
Ncat: Connection from 10.11.1.13.
Ncat: Connection from 10.11.1.13:3198.
```

INetSim

Ücretsiz Linux tabanlı internet servis simülasyon aracıdır.

```
nymia@inetsim:~$ sudo inetsim
INetSim 1.2.6 (2016-08-29) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 41747) ===
Session ID: 41747
Listening on: 192.168.1.153
Real Date/Time: 2017-06-09 22:54:52
Fake Date/Time: 2017-06-09 22:54:52 (Delta: 0 seconds)
Forking services...
* irc_6667_tcp - started (PID 41759)
* chargen_19_udp - started (PID 41775)
* time_37_udp - started (PID 41765)
* syslog_514_udp - started (PID 41763)
* echo_7_tcp - started (PID 41768)
* discard_9_tcp - started (PID 41770)
* discard_9_udp - started (PID 41771)
```

Fakenet

Ücretsiz internet servisi simülasyon aracıdır.

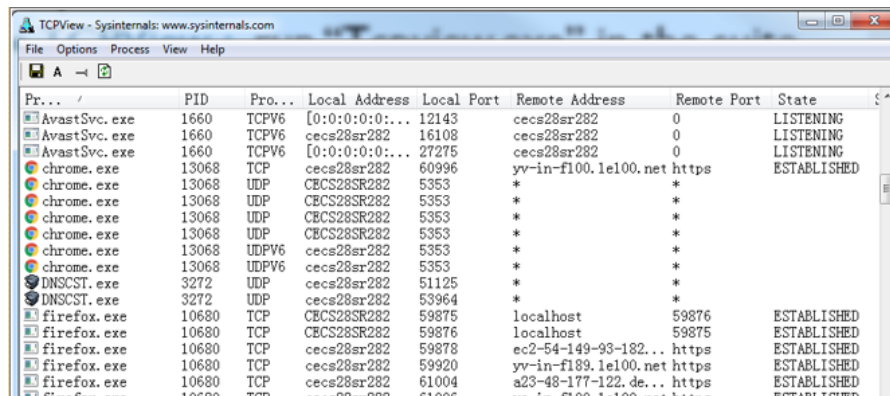
```
FAKENET-NG
Version 1.3

Developed by
Peter Kacherginsky and Michael Bailey
FLARE (FireEye Labs Advanced Reverse Engineering)

04/08/18 03:48:35 PM [ FakeNet] Loaded configuration file: configs\default.ini
04/08/18 03:48:35 PM [ Diverter] Using default listener ProxyTCPListener on port 38926
04/08/18 03:48:35 PM [ Diverter] Using default listener ProxyUDPListener on port 38926
04/08/18 03:48:35 PM [ Diverter] External IP: 192.168.1.3 Loopback IP: 127.0.0.1
04/08/18 03:48:35 PM [ Diverter] Failed calling GetNetworkParams
04/08/18 03:48:35 PM [ Diverter] WARNING: No DNS servers configured!
04/08/18 03:48:36 PM [ Diverter] Setting DNS 192.168.1.3 on interface Ethernet
04/08/18 03:48:36 PM [ Diverter] Setting DNS 192.168.130.1 on interface VMware Network Adapter VMnet1
04/08/18 03:48:37 PM [ Diverter] Setting DNS 192.168.190.1 on interface VMware Network Adapter VMnet8
04/08/18 03:48:37 PM [ Diverter] Capturing traffic to packets_20180408_154837.pcap
04/08/18 03:48:37 PM [ ProxyTCPListener] Starting...
04/08/18 03:48:37 PM [ ProxyTCPListener] TCP Server(0.0.0.0:38926) thread: Thread-1
04/08/18 03:48:37 PM [ ProxyUDPListener] Starting...
04/08/18 03:48:37 PM [ ProxyUDPListener] UDP Server(0.0.0.0:38926) thread: Thread-2
04/08/18 03:48:37 PM [ RawTCPListener] Starting...
```

TCP View

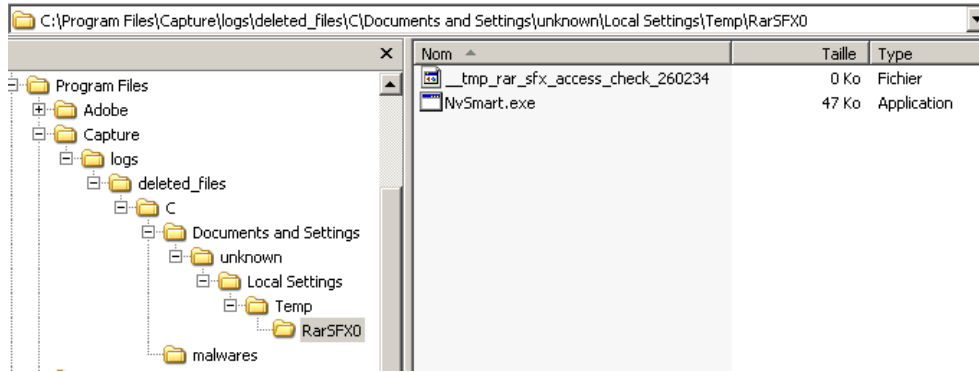
Sistem üzerindeki yerel ve uzaktan TCP ve UDP uç noktalarını listelemeye yarayan araçtır.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
AvastSvc.exe	1660	TCPV6	[0:0:0:0:0:0:0:0]	12143	cecs28sr282	0	LISTENING
AvastSvc.exe	1660	TCPV6	cecs28sr282	16108	cecs28sr282	0	LISTENING
AvastSvc.exe	1660	TCPV6	[0:0:0:0:0:0:0:0]	27275	cecs28sr282	0	LISTENING
chrome.exe	13068	TCP	cecs28sr282	60996	yv-in-f100.1e100.net	https	ESTABLISHED
chrome.exe	13068	UDP	CECS28SR282	5353	*	*	
chrome.exe	13068	UDP	CECS28SR282	5353	*	*	
chrome.exe	13068	UDP	CECS28SR282	5353	*	*	
chrome.exe	13068	UDP	CECS28SR282	5353	*	*	
chrome.exe	13068	UDPV6	cecs28sr282	5353	*	*	
chrome.exe	13068	UDPV6	cecs28sr282	5353	*	*	
DNSCST.exe	3272	UDP	cecs28sr282	51125	*	*	
DNSCST.exe	3272	UDP	cecs28sr282	53964	*	*	
firefox.exe	10680	TCP	CECS28SR282	59875	localhost	59876	ESTABLISHED
firefox.exe	10680	TCP	CECS28SR282	59876	localhost	59875	ESTABLISHED
firefox.exe	10680	TCP	cecs28sr282	59878	ec2-54-149-93-182...	https	ESTABLISHED
firefox.exe	10680	TCP	cecs28sr282	59920	yv-in-f189.1e100.net	https	ESTABLISHED
firefox.exe	10680	TCP	cecs28sr282	61004	a23-48-177-122.de...	https	ESTABLISHED
firefox.exe	10680	TCP	cecs28sr282	61006	ESTABLISHED

CaptureBAT

Kernel seviyesindeki değişiklikleri incelemek için kullanılır. İşlemi bittiğinde bir pcap dosyası oluşturur.



Debuggerlar

Debuggerlar program çalışırken, durumunu inceleyebilmenize olanak sağlayan araçlardır. Breakpointler aracılığıyla programı istediğiniz yere kadar çalıştırmayı sağlayabilirler. Anlık register değerleri, hexdump, ascii değerleri gibi bilgiler gösterebilirler. Debuggerlar uygulamayı patchlememize olanak sağlarlar.

Zararlı analizi için kullanılan debuggerlar genellikle assembly seviyesinde çalışırlar.

Olydbg, x64dbg, x32dbg gibi araçlar debuggerdır. Bazı disassemblerlar da kendi içlerinde debug gerçekleştirebilirler. (IDA gibi)

