



BİLGİ GÜVENLİĞİ İHLAL OLAYI ŞÜPHESİNİN ANALİZ EDİLMESİ

- İstanbul Şehir Üniversitesi -

Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı Bilgisayar Adli Analizi Dersi

NOT: Öğitmenlerimizden Huzeyfe Önal'ın İstanbul Şehir Üniversitesi 2016 bahar döneminde Yüksek Lisans Programı Adli Bilişim Dersi öğrencileri tarafından hazırlanmıştır.

Hazırlayan: Fatih TALI – Murat KATIRCIOĞLU

Tarih: 09.05.2016

[BİR BİLGİ GÜVENLİĞİ İHLAL OLAYI ŞÜPHESİNİN ANALİZ EDİLMESİ]

Windows'un günlük ayrıntısında da cmk.exe isimli bir dosyanın çalıştığı görülmüş ve uygulamanın çalıştığı yer ve isim itibari ile şüpheli bir exe olabileceği değerlendirilmiştir.

TimeGenerated	Machinename	EventType	EventID	Source	Kadı	param6
2.03.2016 21:36	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 21:43	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 21:51	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 21:55	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 22:00	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 22:01	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	C:\Users\ [REDACTED] \cmk.exe
2.03.2016 22:10	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 22:19	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 22:26	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 22:31	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 22:27	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 22:34	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 22:35	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	C:\Users\ [REDACTED] \cmk.exe
2.03.2016 22:35	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe
2.03.2016 22:36	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe

Yapılan incelemede uygulamanın birçok bilgisayarda çalıştığı tespit edilmiştir.

Google'da yapılan cmk.exe araması sonucunda yazılımın **"Bypass Windows 7 Login**

Password with Kon Boot" uygulaması olduğu görülmüştür.

Bu tespit sonrasında uygulama zararlı olarak nitelendirilmiş ve her iyi uygulamanın aktiviteleri incelenmeye başlamıştır.

Kon Boot Aktivite örneği:

Open a command prompt and execute the following commands to obtain administrator rights.

copy C:\Windows\System32\cmd.exe cmk.exe cmk.exe

whoami

```
Administrator: C:\Windows\system32\cmd.exe - cmk

C:\Users\Guest>whoami
vndie\guest

C:\Users\Guest>copy c:\Windows\system32\cmd.exe cmk.exe
1 file(s) copied.

C:\Users\Guest>cmk
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Guest>whoami
nt authority\system

C:\Users\Guest>
```

Ekranda görüleceği gibi Kon Boot uygulaması sınırlı kullanıcı durumundan admin haklarına kendini yükseltmektedir.

[BİR BİLGİ GÜVENLİĞİ İHLAL OLAYI ŞÜPHESİNİN ANALİZ EDİLMESİ]

Yaşanan aktivite ile ilgili günlük kayıtları da Kon Boot uygulaması ile örtüşmektedir.

2.03.2016 21:36	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	C:\Windows\SysWOW64\cmd.exe	1
2.03.2016 21:36	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	D:\Profiles\ [REDACTED] \cmk.exe	2
2.03.2016 21:36	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	C:\Windows\SysWOW64\whoami.exe	3
2.03.2016 21:36	[REDACTED]	audit success	4688	Microsoft-Windows-Security-Auditing	[REDACTED]	C:\Windows\SysWOW64\rundll32.exe	4

Diğer taraftan bu şekilde bir aktiviteye sebep olabilecek iç uygulamaların araştırılmasının başlanmıştır.

cmk.exe isimli dosyanın çalıştırma ihtimali olan kaynaklara durum bildirildi. Özellikle böyle bir aktiviteye log toplama yazılımının ajanının yapabileceği düşünülerek firma ile iletişime geçildi. Firma bu tip bir aktiviteye sebep olacak bir uygulamalarının olmadığını belirtti.

Aktivitenin GPO ile gelen ya da GP aktivitelerinden birinin olup olmadığını öğrenmek için AD' admin'inden bilgi istendi. AD admini bu aktivitelerin kesinlikle kendisine ait olmadığını ve şüpheli olduğunu söyledi.

Şüpheli exe hakkında yeterli bilgi elde edilememesinden dolayı anti virüs tarafında uygulamanın çalışmasına engel olundu.

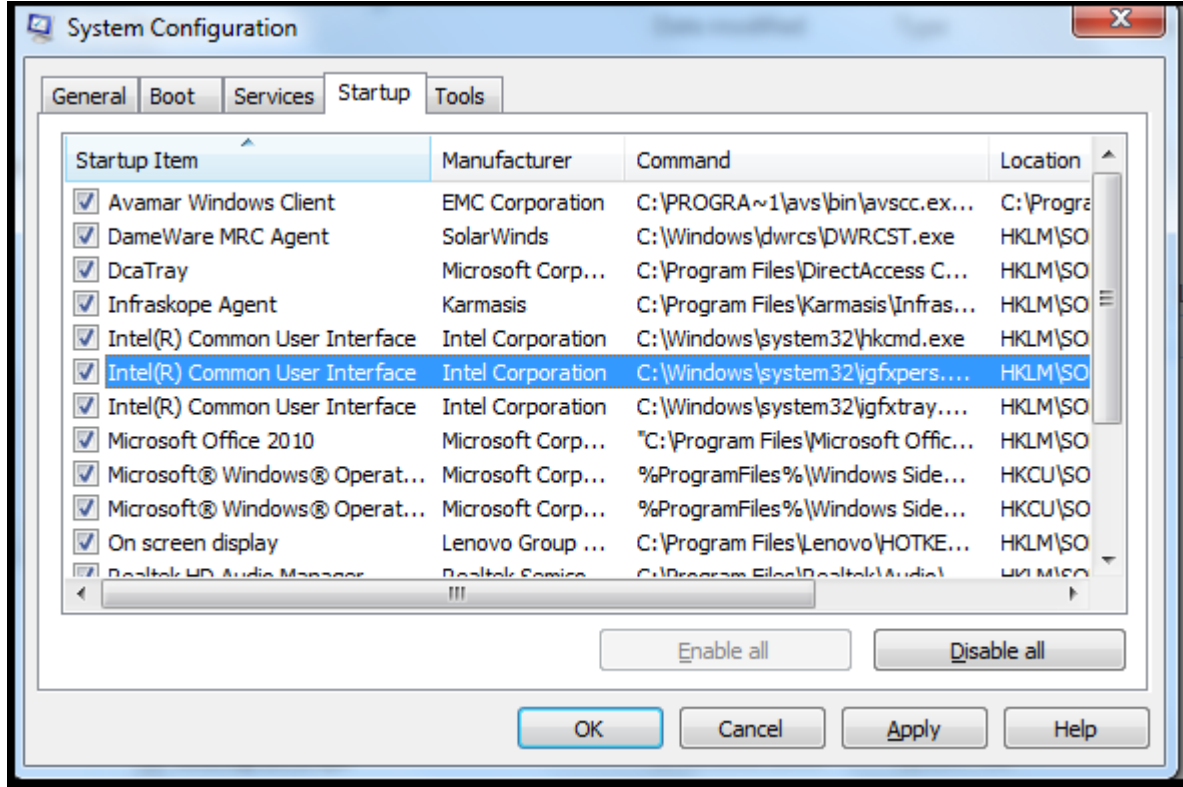
Analiz Çalışmaları:

Yukarıda yapılanlara paralel olarak alttaki analiz çalışmaları gerçekleştirilmiştir. Bilgisayar üzerinde yapılan analiz çalışmaları Microsoft Sysinternals ile yapılmıştır.

<https://technet.microsoft.com/en-us/sysinternals>

Uygulamanın çalıştığı bilinen bir bilgisayar temin edilmiş ve Msconfig uygulaması ile açılış yerleşen bir uygulama olup olmadığı kontrol edilmiştir. İlk bakışta tanımsız bir uygulama görülememiştir.

[BİR BİLGİ GÜVENLİĞİ İHLAL OLAYI ŞÜPHESİNİN ANALİZ EDİLMESİ]



Günlük kayıtları kontrol edildiğinde 4688 eventi ile karşılaşıldı.

Dosyanın analiz edilebilmesi için bilgisayar üzerinde cmk.exe aratıldı fakat hiç bir yerde bu dosyaya rastlanmadı.

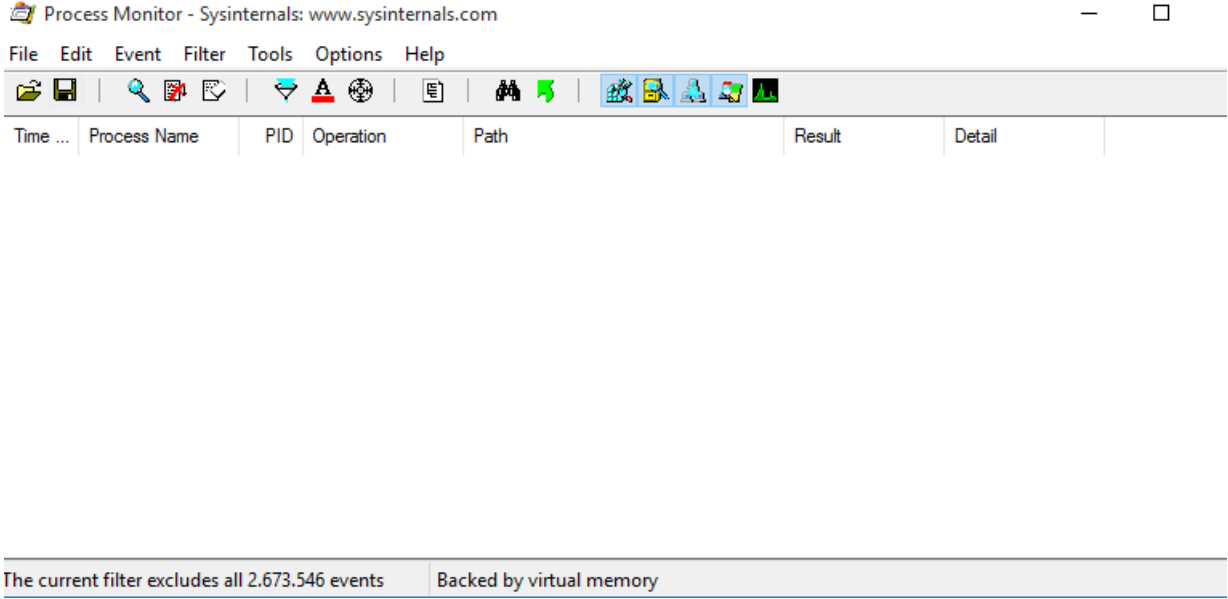
Bilgisayar restart edilerek aktivitenin gerçekleşip gerçekleşmediği teyit edildi.

cmd.exe
cmk.exe

whoami dosyaları sırasıyla çalışmakta ve loglara yansımaktaydı.

Sysinternals Process Monitor uygulaması açılarak filter kısmında aşağıda da görüleceği gibi filtre uygulanarak aktivite takibi yapıldı. Bilgisayarın açık kaldığı süre zarfında cmk.exe ile ilgili hiç bir aktivite tespit edilemedi.

[BİR BİLGİ GÜVENLİĞİ İHLAL OLAYI ŞÜPHESİNİN ANALİZ EDİLMESİ]



Bunun üzerine Process Monitor aracının bilgisayar açılışında nasıl çalıştırılacağı araştırıldı. Bunun için programın içerisinde Options -> Enable Boot Logging özelliği olduğu öğrenildi. Bu işlem yapıldıktan sonra bilgisayar yeniden başlatıldı.

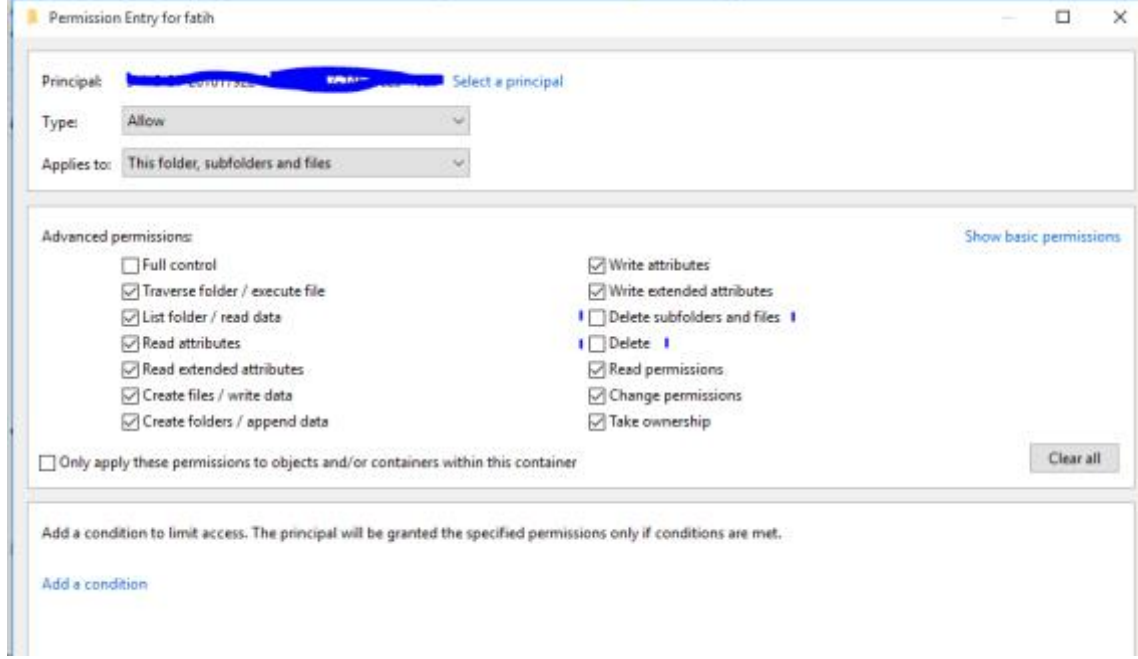
Bilgisayarın yeniden başlaması sırasında uygulama aktiviteleri gözlenmedi. Eventloglara da yansıyan bir şey olmadı. Bu işlem 5 kez tekrarlandıktan sonra uygulamanın analize karşı kendini korumaya almış olabileceği düşünülerek normal bir şekilde bilgisayar açıldı ve aktiviteler tekrar görülmeye başlandı.

Dosyanın bu bilgisayarda olduğu kesinleştikten sonra CMK.exe dosyasına nasıl ulaşabileceği araştırıldı.

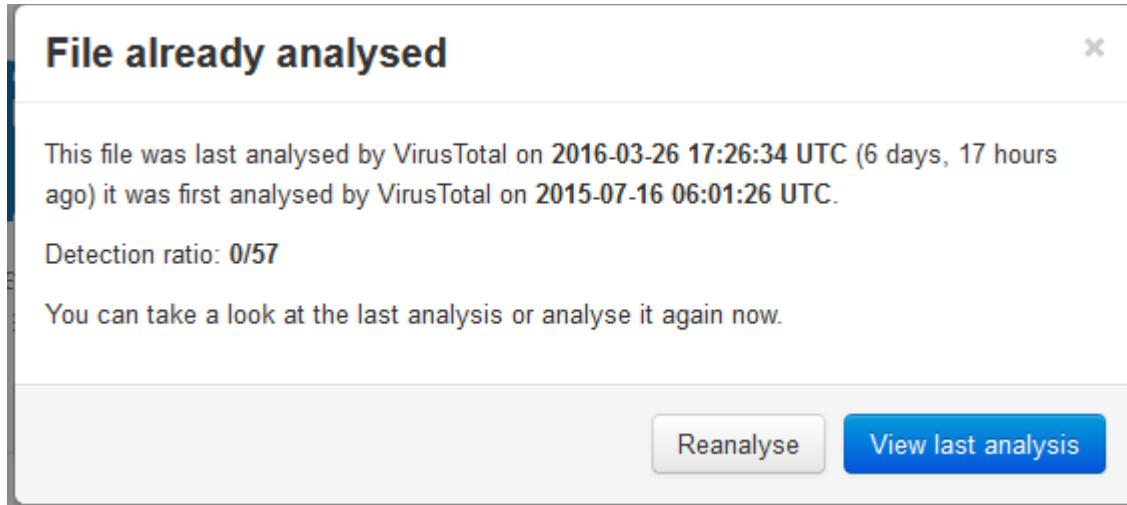
Cmk.exe kendisine ulaşılmasını üzerine %profile% klasörünün file permission'larda dosya ve klasör silme yetkisi kaldırıldı. Bu yöntemle dosya oluşturulabilecek fakat dosya silinemeyecek şekilde getirildi.

Bilgisayarın yeniden başlatılması ile cmk.exe terar %userprofile% altından oluşturuldu ve çalıştı. File Permissionlara takılan uygulama kendisini silemedi.

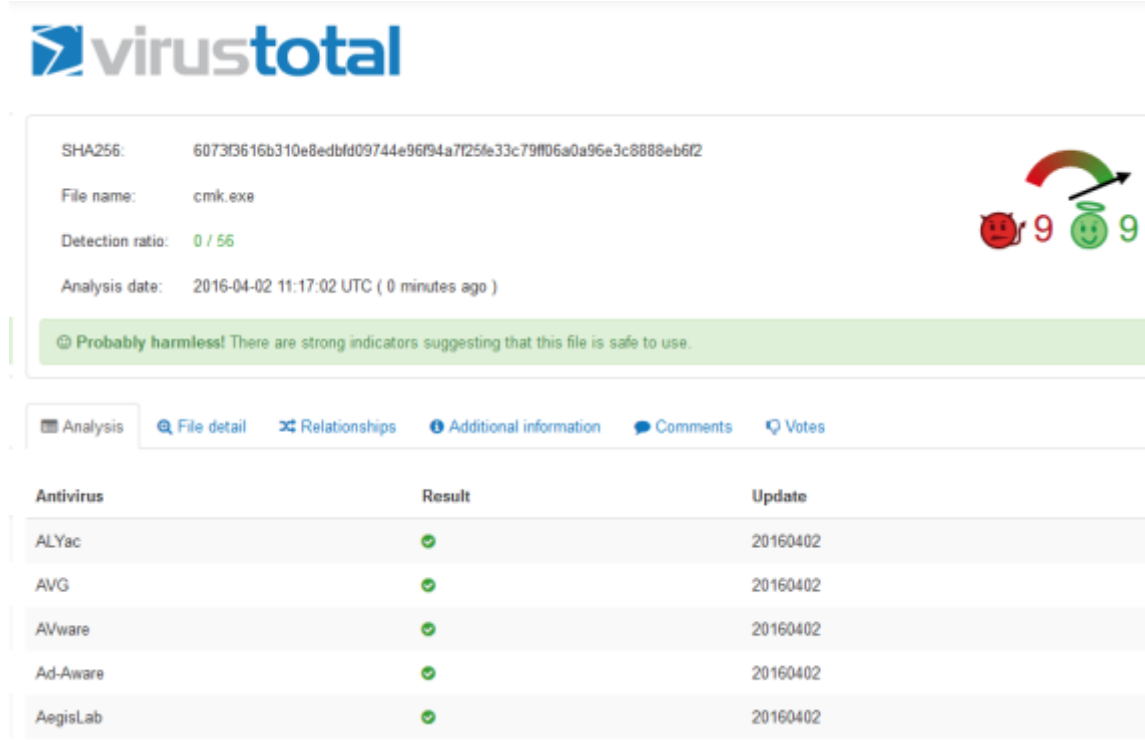
[BİR BİLGİ GÜVENLİĞİ İHLAL OLAYI ŞÜPHESİNİN ANALİZ EDİLMESİ]



Bu işlem sonrasında cmk.exe dosyasının kendisine ulaşılmış oldu. Dosya virustotal.com adresine yüklendiğinde virüs olmadığı ve daha önceden analiz edildiği görüldü.



[BİR BİLGİ GÜVENLİĞİ İHLAL OLAYI ŞÜPHESİNİN ANALİZ EDİLMESİ]



The screenshot shows the VirusTotal analysis interface for a file named 'cmk.exe'. The SHA256 hash is 6073f3616b310e8edbfd09744e96f94a7f25fe33c79ff06a0a96e3c888eb6f2. The detection ratio is 0 / 56, indicating no detections. The analysis date is 2016-04-02 11:17:02 UTC (0 minutes ago). A green banner at the bottom states: 'Probably harmless! There are strong indicators suggesting that this file is safe to use.' Below the banner, there are tabs for Analysis, File detail, Relationships, Additional information, Comments, and Votes. The Analysis tab is active, showing a table of antivirus results.

Antivirus	Result	Update
ALYac	✓	20160402
AVG	✓	20160402
AVware	✓	20160402
Ad-Aware	✓	20160402
AegisLab	✓	20160402

Bu işlem sonrasında bu uygulamanın nasıl ve ne ile çalıştırıldığı araştırıldı. Başlangıca yerleşmiş bir Visual Basic scripti araştırılsa da bir sonuç elde edilemedi. Yeterli bilgiye ulaşılamamasından dolayı dosyanın antivirüs tarafında cmk.exe'ye erişim ve çalıştırma talepleri yasaklandı.

Bu işlem sonrasında antivirüs uygulaması bilgisayarlarda alarm üretmeye başladı. WMI*.exe dosyasının cmk.exe'yi oluşturduğu uyarısı gelmeye başladı.

Uygulama elle çalıştırılarak bulguların tekrarlayıp tekrarlamadığı teyit edildi.

Bu çalışmalar sırasında uygulamanın dışarıya doğru call back trağine rastlanmadı.

Process monitorde ilgili exe'lere filtre uygulanarak aşağıdaki sonuçlar elde edildi.

[BİR BİLGİ GÜVENLİĞİ İHLAL OLAYI ŞÜPHESİNİN ANALİZ EDİLMESİ]

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
13:58:...	svchost.exe	1036	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
13:58:...	svchost.exe	1036	CreateFile	C:\Windows\System32\Tasks\Microsof...	SUCCESS	Desired Access: R...
13:58:...	svchost.exe	1036	QuerySecurityFile	C:\Windows\System32\Tasks\Microsof...	BUFFER OVERFL...	Information: Owner...
13:58:...	svchost.exe	1036	CloseFile	C:\Windows\System32\Tasks\Microsof...	SUCCESS	
13:58:...	svchost.exe	1036	CreateFile	C:\Windows\System32\Tasks\Microsof...	SUCCESS	Desired Access: R...
13:58:...	svchost.exe	1036	QuerySecurityFile	C:\Windows\System32\Tasks\Microsof...	SUCCESS	Information: Owner...
13:58:...	svchost.exe	1036	CloseFile	C:\Windows\System32\Tasks\Microsof...	SUCCESS	
13:58:...	svchost.exe	1036	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
13:58:...	svchost.exe	1036	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM	SUCCESS	
13:58:...	svchost.exe	1036	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_SZ, Le...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
13:58:...	svchost.exe	1036	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: M...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
13:58:...	svchost.exe	1036	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_BINA...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_BINA...
13:58:...	svchost.exe	1036	RegOpenKey	HKLM	SUCCESS	Desired Access: R...
13:58:...	svchost.exe	1036	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Information: Owner...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM	SUCCESS	Desired Access: R...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Control: FSCTL_Q...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Control: FSCTL_R...
13:58:...	svchost.exe	1036	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Creation Time: 21.0...
13:58:...	svchost.exe	1036	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: M...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
13:58:...	svchost.exe	1036	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
13:58:...	svchost.exe	1036	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM	SUCCESS	
13:58:...	svchost.exe	1036	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_BINA...
13:58:...	svchost.exe	1036	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_BINA...

Showing 604.874 of 804.660 events (75%) Backed by virtual memory

Process Monitor Filter

Display entries matching these conditions:

Process Name is cmk.exe then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/>	Process N...	is	cmk.exe
<input checked="" type="checkbox"/>	Process N...	is	Procmon.exe
<input checked="" type="checkbox"/>	Process N...	is	Procexp.exe
<input checked="" type="checkbox"/>	Process N...	is	Autounst.exe
<input checked="" type="checkbox"/>	Process N...	is	System
<input checked="" type="checkbox"/>	Operation	begin with	IRP_MJ

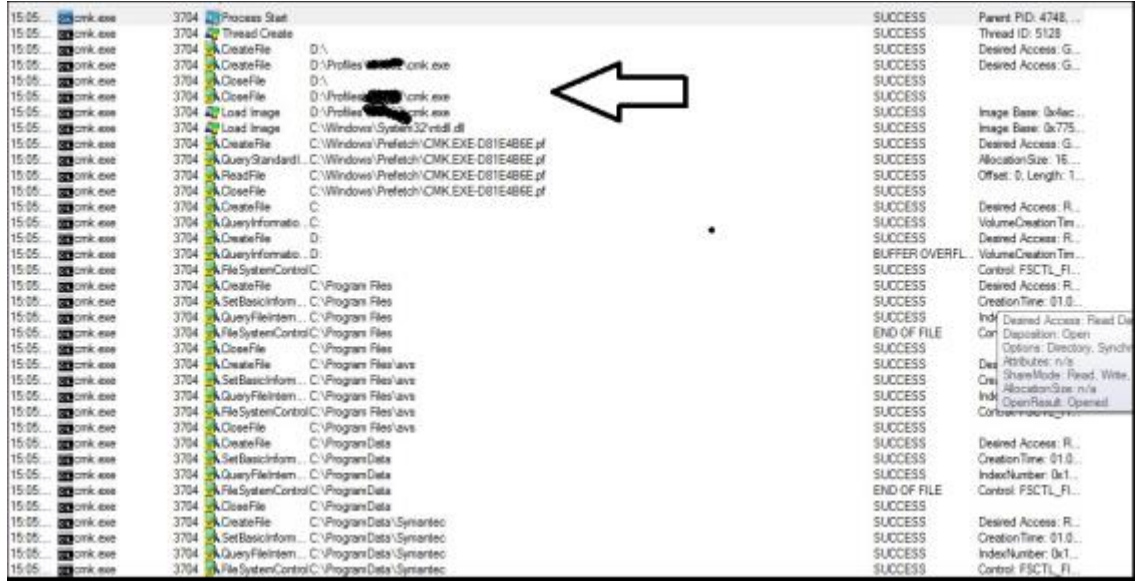
OK Cancel Apply

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
15:05:...	cmk.exe	3704	CreateFile	C:\Windows\System32\whoami.exe	SUCCESS	Desired Access: R...
15:05:...	cmk.exe	3704	CreateFileMap	C:\Windows\System32\whoami.exe	FILE LOCKED WI...	SyncType: SyncTy...
15:05:...	cmk.exe	3704	CreateFileMap	C:\Windows\System32\whoami.exe	SUCCESS	SyncType: SyncTy...
15:05:...	cmk.exe	3704	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\whoami.exe	NAME NOT FOUND	Desired Access: Q...
15:05:...	cmk.exe	3704	QuerySecurityFile	C:\Windows\System32\whoami.exe	SUCCESS	Information: Label
15:05:...	cmk.exe	3704	QueryNameInfo	C:\Windows\System32\whoami.exe	SUCCESS	Name: \Windows\...
15:05:...	cmk.exe	3704	CreateFile	C:\Windows\System32\whoami.exe	SUCCESS	Desired Access: R...
15:05:...	cmk.exe	3704	QueryStandardI	C:\Windows\System32\whoami.exe	SUCCESS	AllocationSize: 45...
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\System32\whoami.exe	SUCCESS	
15:05:...	cmk.exe	3704	CreateFile	C:\Windows\System32\whoami.exe	SUCCESS	Desired Access: R...
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\System32\whoami.exe	SUCCESS	
15:05:...	cmk.exe	3704	CreateFile	C:\Windows\System32\whoami.exe	SUCCESS	Desired Access: R...
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\System32\whoami.exe	SUCCESS	
15:05:...	cmk.exe	3704	CreateFile	C:\Windows\System32\whoami.exe	SUCCESS	Desired Access: G...
15:05:...	cmk.exe	3704	QueryBasicInfo	C:\Windows\System32\whoami.exe	SUCCESS	CreationTime: 14.0...
15:05:...	cmk.exe	3704	QueryFileIntern	C:\Windows\System32\whoami.exe	SUCCESS	IndexNumber: 0x1...
15:05:...	cmk.exe	3704	QueryStandardI	C:\Windows\System32\whoami.exe	SUCCESS	AllocationSize: 45...
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\System32\whoami.exe	SUCCESS	
15:05:...	cmk.exe	3704	CreateFile	C:\Windows\System32\whoami.exe	SUCCESS	Desired Access: G...
15:05:...	cmk.exe	3704	CreateFile	C:\Windows\winsxs\x86_microsoft-windows-whoami_31bf3856ad364e35_6.1.7600.16385_none_oe52d479e3...	SUCCESS	Desired Access: G...
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\winsxs\x86_microsoft-windows-whoami_31bf3856ad364e35_6.1.7600.16385_none_oe52d479e3...	SUCCESS	
15:05:...	cmk.exe	3704	QuerySecurityFile	C:\Windows\winsxs\x86_microsoft-windows-whoami_31bf3856ad364e35_6.1.7600.16385_none_oe52d479e3...	SUCCESS	Information: Owner...
15:05:...	cmk.exe	3704	QueryStandardI	C:\Windows\winsxs\x86_microsoft-windows-whoami_31bf3856ad364e35_6.1.7600.16385_none_oe52d479e3...	SUCCESS	AllocationSize: 45...
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\winsxs\x86_microsoft-windows-whoami_31bf3856ad364e35_6.1.7600.16385_none_oe52d479e3...	SUCCESS	
15:05:...	cmk.exe	3704	QueryStandardI	C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.6608.6300.105\Data\IRON\Iron.db	SUCCESS	AllocationSize: 5.7...
15:05:...	cmk.exe	3704	ReadFile	C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.6608.6300.105\Data\IRON\Iron.db	SUCCESS	Offset: 24, Length...
15:05:...	cmk.exe	3704	QueryStandardI	C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.6608.6300.105\Data\IRON\Iron.db	SUCCESS	AllocationSize: 5.7...
15:05:...	cmk.exe	3704	QueryStandardI	C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.6608.6300.105\Data\IRON\Iron.db	SUCCESS	AllocationSize: 5.7...
15:05:...	cmk.exe	3704	ReadFile	C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.6608.6300.105\Data\IRON\Iron.db	SUCCESS	Offset: 24, Length...
15:05:...	cmk.exe	3704	QueryStandardI	C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.6608.6300.105\Data\IRON\Iron.db	SUCCESS	AllocationSize: 5.7...
15:05:...	cmk.exe	3704	QueryStandardI	C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.6608.6300.105\Data\IRON\Iron.db	SUCCESS	AllocationSize: 5.7...
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\System32\whoami.exe	SUCCESS	Desired Access: G...
15:05:...	cmk.exe	3704	QueryStandardI	C:\Windows\System32\whoami.exe	SUCCESS	AllocationSize: 45...
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\System32\whoami.exe	SUCCESS	
15:05:...	cmk.exe	3704	CreateFile	C:\Windows\System32\whoami.exe	SUCCESS	Desired Access: R...
15:05:...	cmk.exe	3704	QueryStandardI	C:\Windows\System32\whoami.exe	SUCCESS	AllocationSize: 45...
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\System32\whoami.exe	SUCCESS	
15:05:...	cmk.exe	3704	Process Create	C:\Windows\system32\whoami.exe	SUCCESS	PID: 5664, Comma...
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\system32\whoami.exe	SUCCESS	
15:05:...	cmk.exe	3704	CloseFile	C:\Windows\system32\whoami.exe	SUCCESS	

[BİR BİLGİ GÜVENLİĞİ İHLAL OLAYI ŞÜPHESİNİN ANALİZ EDİLMESİ]



Time	Process	Operation	Path	Result	Details
15:05:37	cmk.exe	Process Start		SUCCESS	Parent PID: 4748...
15:05:37	cmk.exe	Thread Create		SUCCESS	Thread ID: 5128
15:05:37	cmk.exe	CreateFile	D:\	SUCCESS	Desired Access: G...
15:05:37	cmk.exe	CreateFile	D:\Profiles\cmk.exe	SUCCESS	Desired Access: G...
15:05:37	cmk.exe	CloseFile	D:\	SUCCESS	
15:05:37	cmk.exe	CloseFile	D:\Profiles\cmk.exe	SUCCESS	
15:05:37	cmk.exe	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x0...
15:05:37	cmk.exe	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x775...
15:05:37	cmk.exe	CreateFile	C:\Windows\Prefetch\CMK.EXE-D81E4B6E.pf	SUCCESS	Desired Access: G...
15:05:37	cmk.exe	QueryStandardI...	C:\Windows\Prefetch\CMK.EXE-D81E4B6E.pf	SUCCESS	AllocationSize: 16...
15:05:37	cmk.exe	ReadFile	C:\Windows\Prefetch\CMK.EXE-D81E4B6E.pf	SUCCESS	Offset: 0, Length: 1...
15:05:37	cmk.exe	CloseFile	C:\Windows\Prefetch\CMK.EXE-D81E4B6E.pf	SUCCESS	
15:05:37	cmk.exe	CreateFile	C:	SUCCESS	Desired Access: R...
15:05:37	cmk.exe	QueryInformatio...	C:	SUCCESS	VolumeCreationTim...
15:05:37	cmk.exe	CreateFile	D:	SUCCESS	Desired Access: R...
15:05:37	cmk.exe	QueryInformatio...	D:	SUCCESS	VolumeCreationTim...
15:05:37	cmk.exe	File System Contro...	C:\Program Files	FAILURE	Control: FSCTL_FI...
15:05:37	cmk.exe	CreateFile	C:\Program Files	SUCCESS	Desired Access: R...
15:05:37	cmk.exe	SetBasicInform...	C:\Program Files	SUCCESS	CreationTime: 01.0...
15:05:37	cmk.exe	QueryFileInfor...	C:\Program Files	SUCCESS	IndexNumber: 0x1...
15:05:37	cmk.exe	File System Contro...	C:\Program Files	FAILURE	Control: FSCTL_FI...
15:05:37	cmk.exe	CloseFile	C:\Program Files	SUCCESS	
15:05:37	cmk.exe	CreateFile	C:\Program Files\av...	SUCCESS	Desired Access: R...
15:05:37	cmk.exe	SetBasicInform...	C:\Program Files\av...	SUCCESS	CreationTime: 01.0...
15:05:37	cmk.exe	QueryFileInfor...	C:\Program Files\av...	SUCCESS	IndexNumber: 0x1...
15:05:37	cmk.exe	File System Contro...	C:\Program Files\av...	FAILURE	Control: FSCTL_FI...
15:05:37	cmk.exe	CloseFile	C:\Program Files\av...	SUCCESS	
15:05:37	cmk.exe	CreateFile	C:\Program Data	SUCCESS	Desired Access: R...
15:05:37	cmk.exe	SetBasicInform...	C:\Program Data	SUCCESS	CreationTime: 01.0...
15:05:37	cmk.exe	QueryFileInfor...	C:\Program Data	SUCCESS	IndexNumber: 0x1...
15:05:37	cmk.exe	File System Contro...	C:\Program Data	FAILURE	Control: FSCTL_FI...
15:05:37	cmk.exe	CloseFile	C:\Program Data	SUCCESS	
15:05:37	cmk.exe	CreateFile	C:\Program Data\Symantec	SUCCESS	Desired Access: R...
15:05:37	cmk.exe	SetBasicInform...	C:\Program Data\Symantec	SUCCESS	CreationTime: 01.0...
15:05:37	cmk.exe	QueryFileInfor...	C:\Program Data\Symantec	SUCCESS	IndexNumber: 0x1...
15:05:37	cmk.exe	File System Contro...	C:\Program Data\Symantec	FAILURE	Control: FSCTL_FI...

Uygulamanın aktiviteleri yukarıda görülmektedir.

WMI*.exe uygulamasımerkezi log toplama yazılımı içerisinde olan bir özelliğten kaynaklandığı değerlendirilmiştir. Yazılımı geliştiren firmaya konu bildirilmiştir.

Yaşanan bu olaylar 12 saatlik çalışma ile sonuca bağlanmıştır.

Şüpheli aktivitelerle karşılaşıldığında tüm güvenlik ekibi bilgilendirilmeli ve herkesin tecrübelerinden faydalanmalıdır.

Bu tip olaylar yaşanmadan önce gerekli önlemler alınmalı ve ihtiyaç duyulacak bilgi birikimi tatbikatlarla ve testlerle artırılmalıdır.

Bilgisayarlarda çalışan exe dosyalar ve uygulamalar önceden belirlenmeli bunlardaki değişiklikler takip edilmelidir.

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA’da sürdüren BGA Bilgi Güvenliği’nin ilgi alanlarını “Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri” oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000’den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlike-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.’nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar “Siber Güvenlik Kampları”, “Siber Güvenlik Staj Okulu”, “Siber Güvenlik Ar-Ge Destek Bursu”, “Ethical Hacking yarışmaları” ve “Siber Güvenlik Kütüphanesi” gibi birçok gönüllü faaliyetin destekleyici olmuştur.