# Correlation Rule Overview

* **DT - CMD or Powershell execution after MS Office or PDF Reader execution**
* **DT - DNS - Communication with Malicious Host - Event or Flow**
* **DT - Excessive Firewall SMTP Connection**
* **DT - Spam Attack Detection from MailGateway Logs**
* **DT-log4j-01**
* **DT0005 - Installing Unauthorized Application on a Server**
* **DT0006 - Attempting to install unauthorized application on a server**
* **DT0008 - Install new service on the system**
* **DT0010-Making changes to the Domain GPO**
* **DT0011 - Making changes to the Local GPO**
* **DT0012 - Attempts to Access Backup Files**
* **DT0013-Opening host file**
* **DT0014-Editing host file**
* **DT0015-Route changes on servers**
* **DT0018 - High CPU RAM usage**
* **DT0021 - Creating deleting or modifying fileshare**
* **DT0022 - Changes on Virtualization System - Delete VM**
* **DT0022 - Changes on Virtualization System - OS shutdown**
* **DT0022 - Changes on Virtualization System - Password Change**
* **DT0022 - Changes on Virtualization System - Power off**
* **DT0023 - Attempt to Failed Access the Vcenter**
* **DT0023 - Attempt to access the virtualization management panel from unauthorized sources - Success**
* **DT0023 - Attempt to access the virtualization management panel from unauthorized sources - failed**
* **DT0025 - Too many error messages on the server system**
* **DT0026 - Unexpected server shutdown restart crash**
* **DT0027 - Microsoft windows Application crash**
* **DT0034 - Update Patch System Failure**
* **DT0038 - AD- user account creation or activation EP**
* **DT0039 - AD- disabled user account**
* **DT0040 - AD- Delete user account**
* **DT0041 - AD- created user group account**
* **DT0042 - AD Delete User Group Account**
* **DT0043 - AD- Add User to the Authorized Account Group**
* **DT0044 - AD- Remove User from the Authorized Account Group**
* **DT0052-Logon with RDP Privilage Account**
* **DT0053-Failed Logon to Privileged Account**
* **DT0055-Logging in or Attempting to Log in out of Business Hours**
* **DT0057 - 1000 Stopped Sending Events**
* **DT0058 - Servers Logging Problem**
* **DT0062 - Deletion of security and system logs from servers**
* **DT0066-Excessive Number of Outbound SMTP Connections**
* **DT0067-Excessive Number of Outbound Web connections**
* **DT0068-Excessive Number of Inbound SMTP Connections**
* **DT0075-Excessive Number of Outbound FTP Connections**
* **DT0076-Excessive Number of Inbound FTP Connections - 1**
* **DT0076-Excessive Number of Inbound FTP Connections - 2**
* **DT0085-Detecting a Malware**
* **DT0119 - SQL Injection Activity**
* **DT0132 - Port Scan Activity**
* **DT0132 - Port Scan Activity - Distinct Destination IP**
* **DT0133 - IP Scan Activity**
* **DT0135 - ICMP Scan**
* **DT0136 - FTP Scan**
* **DT0137 - HTTP HTTPS Tarama**
* **DT0138 - NetBIOS Scan**
* **DT0139 - RDP Scan**
* **DT0140 - RPC Scan**
* **DT0141 - SMB Scan**
* **DT0142 - SNMP Scan**
* **DT0143 - SMTP Scan**
* **DT0144 - SSH Scan**
* **DT0145 - TELNET Scan**
* **DT0154 - Suspicious IPS Evasion Event**
* **DT0170 - Lots of Login Fails**
* **DT0171 - Locked Users**
* **DT0173 - Password Brute Force Attacks**
* **DT0182 - Failed login attempts on SSL VPN or VPN Services**
* **DT0184-WannaCry Detection**
* **DT0198-Credential Dumping Detection**
* **DT0199-PsExec Detection**
* **DT0201 - Login After Brute Force**
* **DT0202- Directory Traversal Detection**
* **DT0203- Detecting rogue SMTP servers within the organization**
* **DT0204- Detecting rogue DNS servers within the organization**
* **DT0207- CMD or Powershell execution after MS Office or PDF Reader execution**
* **DT0210 - More than 20 users are disabled within a hour**
* **DT0211 - More than 20 users are deleted within an hour**
* **DT0212 - Creating and deleting user within 24 hours**
* **DT0214 - Same user logging in more than one source for an hour**
* **DT0219 - Changing critical register values**
* **DT0221 - Creating schedule tasks on servers**
* **DT0224 - File is Infected - Fortigate AV**
* **DT0224 - Query Result**
* **DT0225 - More than 20 users are created within a hour**
* **DT0226 - Anti-virus engine detection malware**
* **DT0227 - Access to Malicious IP**
* **DT0228 - Sending Malicious IP**
* **DT0302-Web vulnerability scanning with the Vulnerability Scan tool**
* **DT0303-IPS Attack Detection**
* **DT0304-Access from Malicious IPs**
* **DT0305 - A new external device was recognized by the system**
* **DT0306 - DNS Access with Malicious IP**
* **DT0307 - Exploit Prevention Detection**
* **DT0308 - T1003 LSASS Attack**
* **DT0309 - Telegram Activities**
* **DT0310 - AnyDesk Activities**
* **DT0311 - Sql Injection Attack - BSMSEC**
* **DT0312-Powershell XML requests**
* **DT0313-Mimikatz**

# DT - CMD or Powershell execution after MS Office or PDF Reader execution

## Description

DT - CMD or Powershell execution after MS Office or PDF Reader execution

## General Information

* **Rule ID:** 47-6000032
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** @4

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046880’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259870’ CONTAINS ‘Process\_Name|12622590293378144023[cmd.exe,powershell.exe]’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259878’ CONTAINS ‘Target\_Process\_Name|10814778825021535730[excel.exe,EXCEL.EXE,WINWORD.EXE]’

# DT - DNS - Communication with Malicious Host - Event or Flow

## Description

This rule detects the occurrence of communication over the DNS port with a malicious host.

Communication over the DNS UDP port has been detected with an external system that has been identified as a malicious host. This behavior is often associated with hosts that have been infected.

Possible Action: Users may wish to create an alarm to alert an incident response team when the correlation rule matches certain conditions. Block any communications to or from the blacklisted IP address. The local host involved should be investigated for possible infection or compromise. Note: Ideal solutions may vary based on your network conditions and security policy.

Detection Logic: This detection alerts when an event or flow is received which has the Destination Port 53 (DNS) and the External IP address is in the “Botnet - Bot,” “Botnet - Control Channel,” “Malware URLs,” or “Passive DNS - Malware Domain” watchlists.

Group By Field: Events are grouped by Internal IP.

Parameter Defaults: Time\_Window: 5 minutes Number\_of\_Events: 1 event

## General Information

* **Rule ID:** 47-8000003
* **Normalization ID:** 671088640
* **Severity:** 75
* **Group By:** INTERNAL\_IP

## Correlation Details



### Parameters

* **Time\_Window**
  + **Description:** All events must occur within this amount of time.
  + **Default Value:** 300
* **Number\_of\_Events**
  + **Description:** All events must occur within this amount of time.
  + **Default Value:** 1

### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** !Time\_Window!
  + **Time Units:** SECOND
  + **Threshold:** !Number\_of\_Events!
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘53’
  + **Filter Component**
    - **Condition:** ‘PROTOCOL’ EQUALS ‘17’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ IN ‘watch=USOM - Blocklist IP’

# DT - Excessive Firewall SMTP Connection

## Description

DT - Excessive Firewall SMTP Connection

korelasyon 1 dakika içerisinde 500 farkli destination ip ile SMTP portu kullanilarak iletiSim gerçekleSmesi durumunda tetiklenecektir.

## General Information

* **Rule ID:** 47-6000102
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 10
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_CLASS’ EQUALS ‘Firewall’
  + **Filter Component**
    - **Condition:** ‘CONTEXT’ EQUALS ‘1’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘25’

# DT - Spam Attack Detection from MailGateway Logs

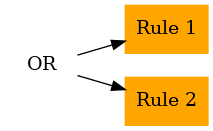
## Description

Spam Attack Detection from MailGateway Logs 1 Dakika içerisinde toplamda 100 adet adresten spam saldirisi gelmesi sonucu tetiklenecektir.

## General Information

* **Rule ID:** 47-6000103
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘390-2756655507’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ EQUALS ‘10.100.10.28’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ IN ‘25,587’

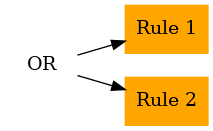
# DT-log4j-01

## Description

## General Information

* **Rule ID:** 47-6000088
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356,308,141,393,503’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259841’ CONTAINS ‘URL|10814778825021535730[jndi:dns,jndi:ldap:,jndi:ldaps,jndi:rmi:]’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356,308,141,393,503’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259849’ CONTAINS ‘User\_Agent|10814778825021535730[jndi:dns,jndi:ldap:,jndi:ldaps,jndi:rmi:]’

# DT0005 - Installing Unauthorized Application on a Server

## Description

DT0005 - Installing Unauthorized Application on a Server

## General Information

* **Rule ID:** 47-6000090
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-264117070’
  + **Filter Component**
    - **Condition:** ‘ACTION’ EQUALS ‘8’

# DT0006 - Attempting to install unauthorized application on a server

## Description

## General Information

* **Rule ID:** 47-6000091
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-264117070’
  + **Filter Component**
    - **Condition:** ‘ACTION’ DOES\_NOT\_EQUAL ‘8’

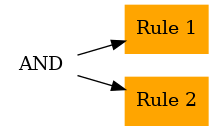
# DT0008 - Install new service on the system

## Description

## General Information

* **Rule ID:** 47-6000092
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-216070450’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘CUST\_65609’ CONTAINS ‘Service\_Name|12622590293378144023[McAfee,Support,Veeam]’

# DT0010-Making changes to the Domain GPO

## Description

## General Information

* **Rule ID:** 47-6000043
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047390’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’

# DT0011 - Making changes to the Local GPO

## Description

DT0011 - Making changes to the Local GPO

## General Information

* **Rule ID:** 47-6000098
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-265015020’
  + **Filter Component**
    - **Condition:** ‘ACTION’ EQUALS ‘13’
  + **Filter Component**
    - **Condition:** ‘CUST\_7’ EQUALS ‘UserIDSrc|6751494449278544611[nt authority]’

# DT0012 - Attempts to Access Backup Files

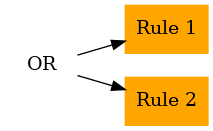
## Description

DT0012 - Attempts to Access Backup Files

## General Information

* **Rule ID:** 47-6000097
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263051400’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259883’ EQUALS ‘Access\_Privileges|12622590293378144023[4416 - ReadData (or ListDirectory)]’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259852’ REGEX ‘Destination\_Filename|10814778825021535730[.\*?.(bak|ova|bkf|img)$]’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259883’ EQUALS ‘Access\_Privileges|12622590293378144023[4416 - ReadData (or ListDirectory)]’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259852’ EQUALS ‘Destination\_Filename|10814778825021535730[.\*?.(bak|ova|bkf|img)$]’

# DT0013-Opening host file

## Description

## General Information

* **Rule ID:** 47-6000029
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046560’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259852’ CONTAINS ‘Destination\_Filename|10814778825021535730[]’

# DT0014-Editing host file

## Description

## General Information

* **Rule ID:** 47-6000030
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046630’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259852’ CONTAINS ‘Destination\_Filename|10814778825021535730[]’

# DT0015-Route changes on servers

## Description

## General Information

* **Rule ID:** 47-6000044
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046880’
  + **Filter Component**
    - **Condition:** ‘CUST\_1’ EQUALS ‘AppID|6751494449278544611[route.exe]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259870’ EQUALS ‘Process\_Name|12622590293378144023[C:.exe]’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘10.100.10.137’

# DT0018 - High CPU RAM usage

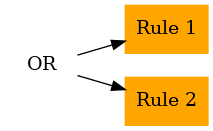
## Description

DT0018 - High CPU RAM usage

## General Information

* **Rule ID:** 47-6000096
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-159185960’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-159171310’

# DT0021 - Creating deleting or modifying fileshare

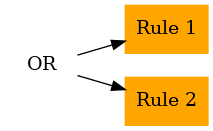
## Description

Bu kural ile SMB windows dosya paylaSimi ile paylaSilan dosyalarinda ortaya çikan modify, delete ve create iSlemlerinin ve bu faaliyetlerin nerede kin tarafindan yapildiginin için tespit edilmesi amaçlanir.

## General Information

* **Rule ID:** 47-6000104
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259883’ EQUALS ‘Access\_Privileges|12622590293378144023[4417 - WriteData (or ListDirectory)]’
  + **Filter Component**
    - **Condition:** ‘ACTION’ EQUALS ‘18’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263051450’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259883’ CONTAINS ‘Access\_Privileges|12622590293378144023[Delete]’

# DT0022 - Changes on Virtualization System - Delete VM

## Description

DT0022 - Changes on Virtualization System - Delete VM

Bu kural ile sanallaStirma sistemlerinde yapilan konfigurasyon degiSikliklerinin tespit ve takibi amaçlanmaktadir.

## General Information

* **Rule ID:** 47-6000064
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘492-2167013803’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144117388726501376/40’

# DT0022 - Changes on Virtualization System - OS shutdown

## Description

## General Information

* **Rule ID:** 47-6000061
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘492-3225215044’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144117388726501376/40’

# DT0022 - Changes on Virtualization System - Password Change

## Description

## General Information

* **Rule ID:** 47-6000062
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘492-3324258384’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144117388726501376/40’

# DT0022 - Changes on Virtualization System - Power off

## Description

## General Information

* **Rule ID:** 47-6000063
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘492-2623311354’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144117388726501376/40’

# DT0023 - Attempt to Failed Access the Vcenter

## Description

Bu kural ile SanallaStirma sisteminin yönetim için kullanilan arayuze baglanmayi deneyen kullanicinin tespit edilmesi amaçlanmiStir.

## General Information

* **Rule ID:** 47-6000089
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘553,621,492,164’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘492-2643908047’

# DT0023 - Attempt to access the virtualization management panel from unauthorized sources - Success

## Description

## General Information

* **Rule ID:** 47-6000066
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘492-2145349321’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144117388726501376/40’

# DT0023 - Attempt to access the virtualization management panel from unauthorized sources - failed

## Description

## General Information

* **Rule ID:** 47-6000065
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘492-2643908047’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144117388726501376/40’

# DT0025 - Too many error messages on the server system

## Description

## General Information

* **Rule ID:** 47-6000095
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 500
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘ACTION’ EQUALS ‘7’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_CLASS’ NOT\_IN ‘Antivirus,Firewall’

# DT0026 - Unexpected server shutdown restart crash

## Description

## General Information

* **Rule ID:** 47-6000031
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-243010760’

# DT0027 - Microsoft windows Application crash

## Description

DT0027 - Microsoft windows Application crash Korelasyonu 10 farkli service name stopeed oldugunda tetiklenmektedir.

## General Information

* **Rule ID:** 47-6000094
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-216070360’
  + **Filter Component**
    - **Condition:** ‘CUST\_2’ EQUALS ‘CommandID|6751494449278544611[stopped]’

# DT0034 - Update Patch System Failure

## Description

DT0034 - Update Patch System Failure

## General Information

* **Rule ID:** 47-6000093
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-216070360’
  + **Filter Component**
    - **Condition:** ‘CUST\_65609’ EQUALS ‘Service\_Name|12622590293378144023[Windows Update]’
  + **Filter Component**
    - **Condition:** ‘CUST\_2’ EQUALS ‘CommandID|6751494449278544611[stopped]’

# DT0038 - AD- user account creation or activation EP

## Description

## General Information

* **Rule ID:** 47-6000001
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047200’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’
  + **Filter Component**
    - **Condition:** ‘CUST\_3’ EQUALS ‘DomainID|6751494449278544611[$watch=Domain-Account]’

# DT0039 - AD- disabled user account

## Description

## General Information

* **Rule ID:** 47-6000002
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047250’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’
  + **Filter Component**
    - **Condition:** ‘CUST\_3’ EQUALS ‘DomainID|6751494449278544611[$watch=Domain-Account]’

# DT0040 - AD- Delete user account

## Description

## General Information

* **Rule ID:** 47-6000003
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047260’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’
  + **Filter Component**
    - **Condition:** ‘CUST\_3’ EQUALS ‘DomainID|6751494449278544611[$watch=Domain-Account]’

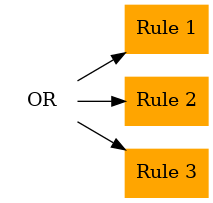
# DT0041 - AD- created user group account

## Description

## General Information

* **Rule ID:** 47-6000004
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047270’
  + **Filter Component**
    - **Condition:** ‘CUST\_3’ EQUALS ‘DomainID|6751494449278544611[$watch=Domain-Account]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047310’
  + **Filter Component**
    - **Condition:** ‘CUST\_3’ EQUALS ‘DomainID|6751494449278544611[$watch=Domain-Account]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’

#### Rule 3

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047540’
  + **Filter Component**
    - **Condition:** ‘CUST\_3’ EQUALS ‘DomainID|6751494449278544611[$watch=Domain-Account]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’

# DT0042 - AD Delete User Group Account

## Description

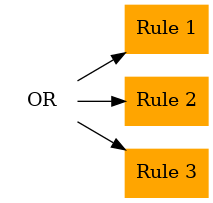
Bu kural ile Microsoft AD den silinen kullanici gruplarinin tespit ve takip edilmesi amaçlanir. Saldirganlar agda yapmiS olduklari aktiviteleri gizlemek amaciyla genellikle kendi oluSturduklari veya etkinleStirdikleri kullanicilar ve kullanici gruplari ile iSleri bittiginde bu kullanicilari silerek izlerini kaybettirmeye çaliSirlar. Benzer Sekilde sistemin eriSebilirligini (availability) hedef alan saldirilarda kullanici gruplari silinerek sistemlerin çaliSmasi engellebilir. Tespit sonrasinda olayin BT ve Guvenlik ekiplerinin bilgisi dahilinde mi yoksa bir saldiri veya zararli yazilim tarafindan mi gerçekleStirildiginin belirlenmesi gerekir. Benzer Sekilde bu vb. kurallar ile gunluk/haftalik raporlarin ve gösterge panellerinin oluSturulmasi saglanabilir. Olay bir zararli yazilim veya saldiri aktivitesi veya Suphesi ise Olay Mudahale faaliyetlerinin ivedi bir Sekilde baSlatilmasi saglanmalidir.

Domain Controller Server’larin Windows Security loglarindakiEvent ID:4730 ‘A security-enabled global group was deleted’,Event ID:4734 ‘A security-enabled local group was deleted’, Event ID: 4758 ‘A security-enabled universal group was deleted’ eventleri için filtre yazilir.

## General Information

* **Rule ID:** 47-6000005
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047300’
  + **Filter Component**
    - **Condition:** ‘CUST\_3’ EQUALS ‘DomainID|6751494449278544611[$watch=Domain-Account]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047340’
  + **Filter Component**
    - **Condition:** ‘CUST\_3’ EQUALS ‘DomainID|6751494449278544611[$watch=Domain-Account]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’

#### Rule 3

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047580’
  + **Filter Component**
    - **Condition:** ‘CUST\_3’ EQUALS ‘DomainID|6751494449278544611[$watch=Domain-Account]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’

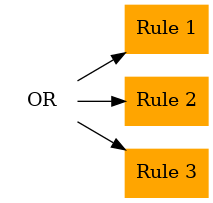
# DT0043 - AD- Add User to the Authorized Account Group

## Description

## General Information

* **Rule ID:** 47-6000006
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047280’
  + **Filter Component**
    - **Condition:** ‘CUST\_5’ EQUALS ‘ObjectID|6751494449278544611[$watch=Yetkili-Kullanici\_Grubu]’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047320’
  + **Filter Component**
    - **Condition:** ‘CUST\_5’ EQUALS ‘ObjectID|6751494449278544611[$watch=Yetkili-Kullanici\_Grubu]’

#### Rule 3

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047560’
  + **Filter Component**
    - **Condition:** ‘CUST\_5’ EQUALS ‘ObjectID|6751494449278544611[$watch=Yetkili-Kullanici\_Grubu]’

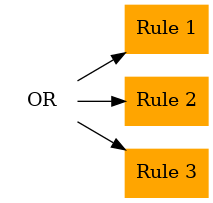
# DT0044 - AD- Remove User from the Authorized Account Group

## Description

## General Information

* **Rule ID:** 47-6000007
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047290’
  + **Filter Component**
    - **Condition:** ‘CUST\_5’ EQUALS ‘ObjectID|6751494449278544611[$watch=Yetkili-Kullanici\_Grubu]’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047330’
  + **Filter Component**
    - **Condition:** ‘CUST\_5’ EQUALS ‘ObjectID|6751494449278544611[$watch=Yetkili-Kullanici\_Grubu]’

#### Rule 3

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047570’
  + **Filter Component**
    - **Condition:** ‘CUST\_5’ EQUALS ‘ObjectID|6751494449278544611[$watch=Yetkili-Kullanici\_Grubu]’

# DT0052-Logon with RDP Privilage Account

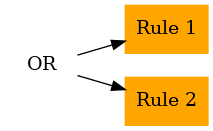
## Description

Bu kural Administrator gibi yetkili kullanicilarla sistemlere login olunmasi olayinin tespiti için yazilmaktadir. Yetkili kullanicilarla login olunmasi beklenen bir durum degildir Bu olayin yetkili personel tarafindan kullanilmasi durumu da yine tespit edilip alarm uretilmesini gerektirir, personelin yetkili olmasi bu kullaniciyla yapilacak hatalarin sonuçlari açisindan ayricalik tanimaz Saldirganlarin hedefledikleri sistemlerde yetki kisitlamasi olmaksizin iSlem yapmasina olanak sagladigi için tespit ve mudahale gerekir

## General Information

* **Rule ID:** 47-6000008
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046240’
  + **Filter Component**
    - **Condition:** ‘CUST\_7’ EQUALS ‘UserIDSrc|6751494449278544611[$watch=Admin Hesaplari]’
  + **Filter Component**
    - **Condition:** ‘CUST\_65580’ EQUALS ‘Logon\_Type|12622590293378144023[$watch=Logon Type]’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘$watch=DT0052 - Exclude’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046240’
  + **Filter Component**
    - **Condition:** ‘CUST\_7’ EQUALS ‘UserIDSrc|6751494449278544611[$watch=AD - Yetkili User\_Import1]’
  + **Filter Component**
    - **Condition:** ‘CUST\_65580’ EQUALS ‘Logon\_Type|12622590293378144023[$watch=Logon Type]’

# DT0053-Failed Logon to Privileged Account

## Description

## General Information

* **Rule ID:** 47-6000009
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 3
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046250’
  + **Filter Component**
    - **Condition:** ‘CUST\_7’ EQUALS ‘UserIDSrc|6751494449278544611[$watch=Privilage Account]’
  + **Filter Component**
    - **Condition:** ‘CUST\_65580’ EQUALS ‘Logon\_Type|12622590293378144023[$watch=Logon Type]’

# DT0055-Logging in or Attempting to Log in out of Business Hours

## Description

## General Information

* **Rule ID:** 47-6000010
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046240’
  + **Filter Component**
    - **Condition:** ‘LAST\_TIME\_DOW’ IN ‘6,2,5,3,4’
  + **Filter Component**
    - **Condition:** ‘LAST\_TIME\_MOD’ DOES\_NOT\_EQUAL ‘300:900’
  + **Filter Component**
    - **Condition:** ‘CUST\_65580’ EQUALS ‘Logon\_Type|12622590293378144023[$watch=Logon Type]’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘$var=MESAI\_DISI\_BAGLANABILEN\_IP’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259870’ CONTAINS ‘Process\_Name|12622590293378144023[C:.exe,C:.exe]’
  + **Filter Component**
    - **Condition:** ‘CUST\_7’ NOT\_IN ‘UserIDSrc|6751494449278544611[DWM-1,DWM-2,DWM-3,DWM-4,DWM-5]’

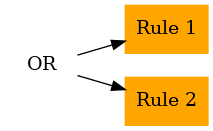
# DT0057 - 1000 Stopped Sending Events

## Description

## General Information

* **Rule ID:** 47-6000099
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1000
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘ACTION’ EQUALS ‘20’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1000
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘CUST\_2’ EQUALS ‘CommandID|6751494449278544611[stopped]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’

# DT0058 - Servers Logging Problem

## Description

## General Information

* **Rule ID:** 47-6000100
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-290011000’

# DT0062 - Deletion of security and system logs from servers

## Description

## General Information

* **Rule ID:** 47-6000074
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-290011020’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘484,43’

# DT0066-Excessive Number of Outbound SMTP Connections

## Description

## General Information

* **Rule ID:** 47-6000053
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ NOT\_IN ‘176.88.209.46,31.154.46.146,$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ IN ‘25,465,587’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.200,10.100.10.28,10.100.10.155’
  + **Filter Component**
    - **Condition:** ‘CUST\_5’ DOES\_NOT\_EQUAL ‘ObjectID|6751494449278544611[Gmail]’

# DT0067-Excessive Number of Outbound Web connections

## Description

## General Information

* **Rule ID:** 47-6000058
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 500
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘10.100.10.155’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ DOES\_NOT\_EQUAL ‘$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘CUST\_65575’ DOES\_NOT\_EQUAL ‘External\_Hostname|12622590293378144023[$watch=Advertise\_Domain]’

# DT0068-Excessive Number of Inbound SMTP Connections

## Description

## General Information

* **Rule ID:** 47-6000054
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 30
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ EQUALS ‘$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.155,172.26.43.157’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ IN ‘25,465,587’

# DT0075-Excessive Number of Outbound FTP Connections

## Description

## General Information

* **Rule ID:** 47-6000057
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ NOT\_IN ‘172.26.46.12,94.138.196.170,$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘10.100.10.155’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘21’

# DT0076-Excessive Number of Inbound FTP Connections - 1

## Description

Home Net 10.200.20.0/24 dahil olan ve threshold 1 dkde 20den fazla olan olaylar için yazildi.

## General Information

* **Rule ID:** 47-6000055
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 20
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ EQUALS ‘$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘10.100.10.155’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ NOT\_IN ‘10.100.250.0/24,94.138.196.170’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ EQUALS ‘10.100.20.0/24’
  + **Filter Component**
    - **Condition:** ‘CUST\_5’ EQUALS ‘ObjectID|6751494449278544611[FTP]’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘355-28704’
  + **Filter Component**
    - **Condition:** ‘ACTION’ IN ‘5,1,8’

# DT0076-Excessive Number of Inbound FTP Connections - 2

## Description

## General Information

* **Rule ID:** 47-6000056
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ EQUALS ‘$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘21’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘10.100.10.155’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘10.100.20.0/24’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ NOT\_IN ‘10.100.250.0/24,192.168.13.127’

# DT0085-Detecting a Malware

## Description

## General Information

* **Rule ID:** 47-6000059
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘576-1027’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144118486610739200/24’

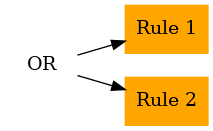
# DT0119 - SQL Injection Activity

## Description

## General Information

* **Rule ID:** 47-6000042
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘141-3804292213’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘CUST\_4259841’ CONTAINS ‘URL|10814778825021535730[$watch=SQL\_Injection\_Payloads\_List]’

# DT0132 - Port Scan Activity

## Description

## General Information

* **Rule ID:** 47-6000012
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** DEST\_IP,SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.40,10.100.10.155’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ IN ‘var=Kurumun\_Dis\_IPleri’

# DT0132 - Port Scan Activity - Distinct Destination IP

## Description

## General Information

* **Rule ID:** 47-6000013
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.40,10.100.10.155,10.100.10.151,10.100.10.150’

# DT0133 - IP Scan Activity

## Description

## General Information

* **Rule ID:** 47-6000014
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 150
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.155,10.100.10.40,10.100.20.12,10.100.20.6,10.100.10.150,10.100.10.151’
  + **Filter Component**
    - **Condition:** ‘CUST\_65575’ DOES\_NOT\_EQUAL ‘External\_Hostname|12622590293378144023[$watch=Advertise\_Domain]’
  + **Filter Component**
    - **Condition:** ‘CUST\_65540’ DOES\_NOT\_EQUAL ‘Category|12622590293378144023[Advertising]’

# DT0135 - ICMP Scan

## Description

## General Information

* **Rule ID:** 47-6000015
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 200
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘PROTOCOL’ EQUALS ‘1’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.40,10.100.10.155,10.100.10.150,10.100.10.151’

# DT0136 - FTP Scan

## Description

## General Information

* **Rule ID:** 47-6000016
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 100
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘20:21’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.40,10.100.10.155’

# DT0137 - HTTP HTTPS Tarama

## Description

Bu kural ile HTTP/HTTPS Scan faaliyetlerinin tespit edilmesi amaçlanir. Saldirgani recon fazinda tespit etmek ivedi tedbir alabilmek için önemlidir. Scan aktivitesi kurumun vuln. assesment urunu tarafindan ya da pentest aktivitesi sonucu da ortaya çikmiS olabilir. Tespit sonrasinda olayin BT ve Guvenlik ekiplerinin bilgisi dahilinde mi yoksa bir saldiri veya zararli yazilim tarafindan mi gerçekleStirildiginin belirlenmesi gerekir. Olay bir zararli yazilim veya saldiri aktivitesi veya Suphesi ise Olay Mudahale faaliyetlerinin ivedi bir Sekilde baSlatilmasi saglanmalidir.

## General Information

* **Rule ID:** 47-6000017
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ IN ‘1080,443,80,8008,8080’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.40,10.100.10.155,192.168.140.100’
  + **Filter Component**
    - **Condition:** ‘CUST\_65540’ DOES\_NOT\_EQUAL ‘Category|12622590293378144023[Advertising]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_CLASS’ EQUALS ‘Firewall’

# DT0138 - NetBIOS Scan

## Description

DT0138 - NetBIOS Scan Bir Source IP uzerinden Herhangi bir Destination IP’ye dogru ve Destination port=139 veya Protocol=NETBIOS olan 10 dakika içerisinde 100 event gerçekleSirsealarm uretilir. Source IP, Destianation IP ve time kullanilir.

## General Information

* **Rule ID:** 47-6000105
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_CLASS’ EQUALS ‘Firewall’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ EQUALS ‘$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ EQUALS ‘$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘137:139’

# DT0139 - RDP Scan

## Description

## General Information

* **Rule ID:** 47-6000018
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 10
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘PROTOCOL’ EQUALS ‘27’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.40,10.100.10.155’

# DT0140 - RPC Scan

## Description

## General Information

* **Rule ID:** 47-6000020
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 100
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘135’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.40,10.100.10.155,10.100.10.151,10.100.10.150’

# DT0141 - SMB Scan

## Description

## General Information

* **Rule ID:** 47-6000033
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘445’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.155,10.100.20.6,10.100.10.150,10.100.10.151’

# DT0142 - SNMP Scan

## Description

## General Information

* **Rule ID:** 47-6000034
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘161:162’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.155,10.100.20.6,10.100.10.150,10.100.10.151,10.100.10.137’

# DT0143 - SMTP Scan

## Description

## General Information

* **Rule ID:** 47-6000035
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ IN ‘25,465,587’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.150,10.100.10.151,10.100.10.155,10.100.20.6’

# DT0144 - SSH Scan

## Description

## General Information

* **Rule ID:** 47-6000036
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘22’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.150,10.100.10.151,10.100.10.155,10.100.20.6’

# DT0145 - TELNET Scan

## Description

## General Information

* **Rule ID:** 47-6000037
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ IN ‘23,992’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ NOT\_IN ‘10.100.10.150,10.100.10.151,10.100.10.155,10.100.20.6’

# DT0154 - Suspicious IPS Evasion Event

## Description

DT0154 - Suspicious IPS Evasion Event

## General Information

* **Rule ID:** 47-6000101
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘CUST\_1’ EQUALS ‘AppID|6751494449278544611[ips]’

# DT0170 - Lots of Login Fails

## Description

## General Information

* **Rule ID:** 47-6000038
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** SRC\_IP

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046250’
  + **Filter Component**
    - **Condition:** ‘CUST\_65580’ EQUALS ‘Logon\_Type|12622590293378144023[$watch=Logon Type]’

# DT0171 - Locked Users

## Description

## General Information

* **Rule ID:** 47-6000039
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047400’

# DT0173 - Password Brute Force Attacks

## Description

## General Information

* **Rule ID:** 47-6000027
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** @4,@7

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 300
  + **Time Units:** SECOND
  + **Threshold:** 5
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046250’
  + **Filter Component**
    - **Condition:** ‘CUST\_65580’ EQUALS ‘Logon\_Type|12622590293378144023[$watch=Logon Type]’

# DT0182 - Failed login attempts on SSL VPN or VPN Services

## Description

## General Information

* **Rule ID:** 47-6000060
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** @7

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 300
  + **Time Units:** SECOND
  + **Threshold:** 3
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘355-39426’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’

# DT0184-WannaCry Detection

## Description

## General Information

* **Rule ID:** 47-6000068
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘CUST\_65624’ EQUALS ‘Hash|12622590293378144023[$watch=WannaCry-SHA1]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144118486610739200/24’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘583-35112’

# DT0198-Credential Dumping Detection

## Description

## General Information

* **Rule ID:** 47-6000041
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046880’
  + **Filter Component**
    - **Condition:** ‘CUST\_12’ EQUALS ‘File\_Operation|6751494449278544611[$watch=Credential Dumping Detection]’

# DT0199-PsExec Detection

## Description

## General Information

* **Rule ID:** 47-6000022
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046880’
  + **Filter Component**
    - **Condition:** ‘CUST\_1’ IN ‘AppID|6751494449278544611[psexec.exe,PsExec.exe,PsExec64.exe]’

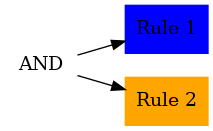
# DT0201 - Login After Brute Force

## Description

## General Information

* **Rule ID:** 47-6000028
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** @4,@7

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** REFERENCE
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046240’

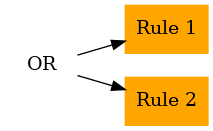
# DT0202- Directory Traversal Detection

## Description

## General Information

* **Rule ID:** 47-6000040
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘308’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259841’ CONTAINS ‘URL|10814778825021535730[../]’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘308’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259841’ CONTAINS ‘URL|10814778825021535730[..]’

# DT0203- Detecting rogue SMTP servers within the organization

## Description

## General Information

* **Rule ID:** 47-6000048
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ EQUALS ‘$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ NOT\_IN ‘$var=SMTP\_SERVERS,10.100.10.155’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ IN ‘25,587’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ EQUALS ‘$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘$var=SMTP\_SERVERS’

# DT0204- Detecting rogue DNS servers within the organization

## Description

## General Information

* **Rule ID:** 47-6000049
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ EQUALS ‘$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ DOES\_NOT\_EQUAL ‘$var=DNS\_SERVERS’
  + **Filter Component**
    - **Condition:** ‘DEST\_PORT’ EQUALS ‘53’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ EQUALS ‘$var=HOME\_NET’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘$var=DNS\_SERVERS’
  + **Filter Component**
    - **Condition:** ‘ACTION’ DOES\_NOT\_EQUAL ‘2’

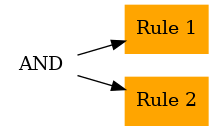
# DT0207- CMD or Powershell execution after MS Office or PDF Reader execution

## Description

## General Information

* **Rule ID:** 47-6000021
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** @4,@7

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
  + **Sequence:** true
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046880’
  + **Filter Component**
    - **Condition:** ‘CUST\_1’ IN ‘AppID|6751494449278544611[acrord32.exe,excel.exe,winword.exe]’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
  + **Sequence:** true
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046880’
  + **Filter Component**
    - **Condition:** ‘CUST\_1’ IN ‘AppID|6751494449278544611[cmd.exe,msiexec.exe,powershell.exe]’

# DT0210 - More than 20 users are disabled within a hour

## Description

## General Information

* **Rule ID:** 47-6000025
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** @7

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 3600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047250’

# DT0211 - More than 20 users are deleted within an hour

## Description

## General Information

* **Rule ID:** 47-6000023
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** @7

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 3600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047260’

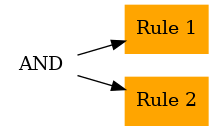
# DT0212 - Creating and deleting user within 24 hours

## Description

## General Information

* **Rule ID:** 47-6000026
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** @6

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 82800
  + **Time Units:** SECOND
  + **Threshold:** 1
  + **Sequence:** true
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047200’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 82800
  + **Time Units:** SECOND
  + **Threshold:** 1
  + **Sequence:** true
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047260’

# DT0214 - Same user logging in more than one source for an hour

## Description

## General Information

* **Rule ID:** 47-6000047
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** @7

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 3600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘43’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046240’
  + **Filter Component**
    - **Condition:** ‘CUST\_65580’ EQUALS ‘Logon\_Type|12622590293378144023[$watch=Logon Type]’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259870’ CONTAINS ‘Process\_Name|12622590293378144023[C:.exe,C:.exe]’

# DT0219 - Changing critical register values

## Description

## General Information

* **Rule ID:** 47-6000045
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046570’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259870’ EQUALS ‘Process\_Name|12622590293378144023[regedit.exe]’

# DT0221 - Creating schedule tasks on servers

## Description

## General Information

* **Rule ID:** 47-6000046
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263046980’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117387115888640/40,144117387132665856/40’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259870’ NOT\_IN ‘Process\_Name|12622590293378144023[,DAT Built in test]’

# DT0224 - File is Infected - Fortigate AV

## Description

## General Information

* **Rule ID:** 47-6000019
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ DOES\_NOT\_EQUAL ‘172.26.46.12’
  + **Filter Component**
    - **Condition:** ‘NORM\_ID’ EQUALS ‘675282944/12’
  + **Filter Component**
    - **Condition:** ‘CUST\_1’ IN ‘AppID|6751494449278544611[virus,Virus]’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’

# DT0224 - Query Result

## Description

## General Information

* **Rule ID:** 47-6000078
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** REFERENCE
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1

# DT0225 - More than 20 users are created within a hour

## Description

## General Information

* **Rule ID:** 47-6000024
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** @7

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 3600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263047200’

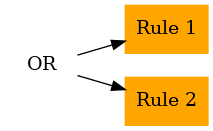
# DT0226 - Anti-virus engine detection malware

## Description

## General Information

* **Rule ID:** 47-6000050
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘390-3743786807’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144117388743278592/40’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘$watch=Trusted Source IPs’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘390-3844973455’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144117388743278592/40’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘$watch=Trusted Source IPs’

# DT0227 - Access to Malicious IP

## Description

## General Information

* **Rule ID:** 47-6000051
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_CLASS’ EQUALS ‘Firewall’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ EQUALS ‘$watch=Fortigate IPS AV Blacklist Source IPs’
  + **Filter Component**
    - **Condition:** ‘ACTION’ IN ‘5,30,21,1,8,12’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ DOES\_NOT\_EQUAL ‘$var=HOME\_NET’

# DT0228 - Sending Malicious IP

## Description

## General Information

* **Rule ID:** 47-6000052
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘527,171,355,540,454,356’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ EQUALS ‘$watch=Malicious IP’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ DOES\_NOT\_EQUAL ‘195.142.246.245’

# DT0302-Web vulnerability scanning with the Vulnerability Scan tool

## Description

## General Information

* **Rule ID:** 47-6000067
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ EQUALS ‘308’
  + **Filter Component**
    - **Condition:** ‘CUST\_4259849’ IN ‘User\_Agent|10814778825021535730[watch=User\_Agent List 2]’

# DT0303-IPS Attack Detection

## Description

DT0303- IPS Attack Detection

Korelasyonda amaçlanan durum FW trafigi içerisinde IPS Katmanina takilan zararli istekleri tespit etmektir.

## General Information

* **Rule ID:** 47-6000069
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_CLASS’ EQUALS ‘Firewall’
  + **Filter Component**
    - **Condition:** ‘CUST\_1’ EQUALS ‘AppID|6751494449278544611[ips]’
  + **Filter Component**
    - **Condition:** ‘ACTION’ DOES\_NOT\_EQUAL ‘3’

# DT0304-Access from Malicious IPs

## Description

DT0304-Access from Malicious IPs

## General Information

* **Rule ID:** 47-6000070
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_CLASS’ EQUALS ‘Firewall’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ EQUALS ‘$watch=Malicious IP’
  + **Filter Component**
    - **Condition:** ‘ACTION’ IN ‘30,1,8’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ EQUALS ‘$var=HOME\_NET’

# DT0305 - A new external device was recognized by the system

## Description

## General Information

* **Rule ID:** 47-6000072
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘43-263064160’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_TYPE’ IN ‘484,43’

# DT0306 - DNS Access with Malicious IP

## Description

## General Information

* **Rule ID:** 47-6000073
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117388139298816/40,144117388156076032/40’
  + **Filter Component**
    - **Condition:** ‘SRC\_IP’ EQUALS ‘$watch=Malicious IP’
  + **Filter Component**
    - **Condition:** ‘DEST\_IP’ EQUALS ‘$watch=Malicious IP’

# DT0307 - Exploit Prevention Detection

## Description

## General Information

* **Rule ID:** 47-6000075
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144118486610739200/24’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘576-18055’
  + **Filter Component**
    - **Condition:** ‘CUST\_65537’ EQUALS ‘Signature\_Name|12622590293378144023[OLEAuto32.dll Remote Code Execution Vulnerability]’

# DT0308 - T1003 LSASS Attack

## Description

## General Information

* **Rule ID:** 47-6000076
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144118486610739200/24’
  + **Filter Component**
    - **Condition:** ‘CUST\_65537’ EQUALS ‘Signature\_Name|12622590293378144023[$watch=T1003 LSASS Attack]’

# DT0309 - Telegram Activities

## Description

## General Information

* **Rule ID:** 47-6000080
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘CUST\_4259870’ CONTAINS ‘Process\_Name|12622590293378144023[telegram.exe,Telegram.exe]’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘49190-3634883731’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144117388592283648/40’

# DT0310 - AnyDesk Activities

## Description

## General Information

* **Rule ID:** 47-6000081
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘CUST\_4259870’ CONTAINS ‘Process\_Name|12622590293378144023[AnyDesk.exe]’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘49190-3634883731’
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ EQUALS ‘144117388592283648/40’

# DT0311 - Sql Injection Attack - BSMSEC

## Description

## General Information

* **Rule ID:** 47-6000082
* **Normalization ID:** 556843008
* **Severity:** 100
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 60
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘CUST\_4259841’ CONTAINS ‘URL|10814778825021535730[$watch=SQL\_Injection\_Payloads\_List]’

# DT0312-Powershell XML requests

## Description

## General Information

* **Rule ID:** 47-6000085
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117388592283648/40,144117388793610240/40’
  + **Filter Component**
    - **Condition:** ‘CUST\_12648459’ CONTAINS ‘ParentImage|10814778825021535730[powershell.exe]’
  + **Filter Component**
    - **Condition:** ‘CUST\_12648449’ CONTAINS ‘CommandLine|12622590293378144023[Xml.XmlDocument]’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘49190-2736244783’

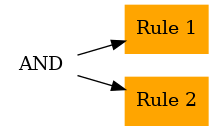
# DT0313-Mimikatz

## Description

## General Information

* **Rule ID:** 47-6000086
* **Normalization ID:** 4026531840
* **Severity:** 50
* **Group By:** NONE

## Correlation Details



### Rules

#### Rule 1

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117388592283648/40,144117388793610240/40’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘49190-2736244783’
  + **Filter Component**
    - **Condition:** ‘CUST\_12648453’ CONTAINS ‘Image|12622590293378144023[powershell.exe]’
  + **Filter Component**
    - **Condition:** ‘CUST\_12648449’ CONTAINS ‘CommandLine|12622590293378144023[DownloadString]’

#### Rule 2

* **Activate:** EVENT
* **Match Type:** FILTER
  + **Count:** 1
* **Action:** Trigger
  + **Timeout:** 600
  + **Time Units:** SECOND
  + **Threshold:** 1
* **Match Filter**
  + **Filter Component**
    - **Condition:** ‘DEVICE\_ID’ IN ‘144117388592283648/40,144117388793610240/40’
  + **Filter Component**
    - **Condition:** ‘CUST\_12648461’ EQUALS ‘GrantedAccess|12622590293378144023[0x1010]’
  + **Filter Component**
    - **Condition:** ‘CUST\_12648460’ CONTAINS ‘TargetImage|12622590293378144023[lsass.exe]’
  + **Filter Component**
    - **Condition:** ‘SIG\_ID’ EQUALS ‘49190-3703360405’