SIMCommander K-SOC Advisory – Conficker Worm

Last Updated: 10 April 2009

Aliases:

- Net-Worm.Win32.Kido (Kaspersky)
- Net-Worm.Win32.Kido.bt (Kaspersky)
- Net-Worm.Win32.Kido.dv (Kaspersky)
- Net-Worm.Win32.Kido.fx (Kaspersky)
- WORM_GIMMIV.A (TrendMicro)
- TSPY_GIMMIV.A (TrendMicro)
- WORM_DOWNAD.A (TrendMicro)
- Trojan.Moo (Symantec)
- W32.Downadup (Symantec)
- TrojanSpy:Win32/Gimmiv.A (Microsoft)
- TrojanSpy:Win32/Gimmiv.A.dll (Microsoft)
- W32/Conflicker.worm (McAfee)

Also Known as:

Microsoft Security Bulletin MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution Vulnerability

Description:

Conficker is believed to be the most widespread computer worm infection since SQL Slammer in 2003 [1]. CNN reported over eight million computers infected on Jan 8, 2009 [2]. Up to this moment, there are 5 known variants - Conficker A, B, C, D and E, they were discovered 21 November 2008, 29 December 2008, 20 February 2009, 4 March 2009 and 7 April 2009, respectively. One announcement in CNN on 9 April, 2009, the situation is going worse because the infection channel extends to P2P [3]. The 60 minutes mentioned that over millions of worm living mainly in the enterprise computers, waiting for arbitrary code execution through the Conficker [4].

[1] http://www.nytimes.com/2009/01/23/technology/internet/23worm.html?_r=1&em

[2] http://edition.cnn.com/2009/TECH/ptech/01/16/virus.downadup/?iref=mpstoryview

[3] http://edition.cnn.com/2009/TECH/04/09/conficker.activated/index.html

[4[http://www.cbsnews.com/stories/2009/03/27/60minutes/main4897053.shtml

How Conficker spreads

The worm propagation is based on NetBIOS or removable media. After a computer is infected, the worm propagates to other computers by the following channels.

- NetBIOS push
- HTTP pull/push
- P2P pull/push

Infection Symptoms:

An infected computer will have the following abnormal performance.

- Users are unable to reach the AntiVirus Software websites or the Microsoft Windows Updates
- Account lockout policies being reset automatically
- Certain Microsoft Windows services such as Automatic Updates, Background Intelligent Transfer Service (BITS), Windows Defender and Error Reporting Services are disabled
- Domain controllers responding slowly to client requests
- Congestion on local area networks.

According to US-CERT [5], the presence of a Conficker infection may be detected if a user is unable to surf to the following websites:

http://www.symantec.com/norton/theme.jsp?themeid=conficker_worm&inid=us_ghp_link_conficker_worm

http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx

http://www.mcafee.com

http://www.kaspersky.com

If a user is unable to reach either of these websites, a Conficker infection may be indicated (the most current variant of Conficker interferes with queries for these sites, preventing a user from visiting them).

[5] http://www.us-cert.gov/current/#conficker_worm_information

Impact to Enterprises:

According to Kaspersky, when a computer infected by Conficker, it cannot access to the Kaspersky website and download the latest antivirus database. In other words, when the infected computer is Kaspersky Administration Kit server, the Administration Kit cannot update the virus database and distribute the virus database to all its client computers.

In a large enterprise environment, the Administration Kit servers can be infected easily under the following circumstances and the infected Administration Kit servers generate the 'virus database update failed' events.

i) Administration Kit servers not patched the Microsoft vulnerability MS08-067

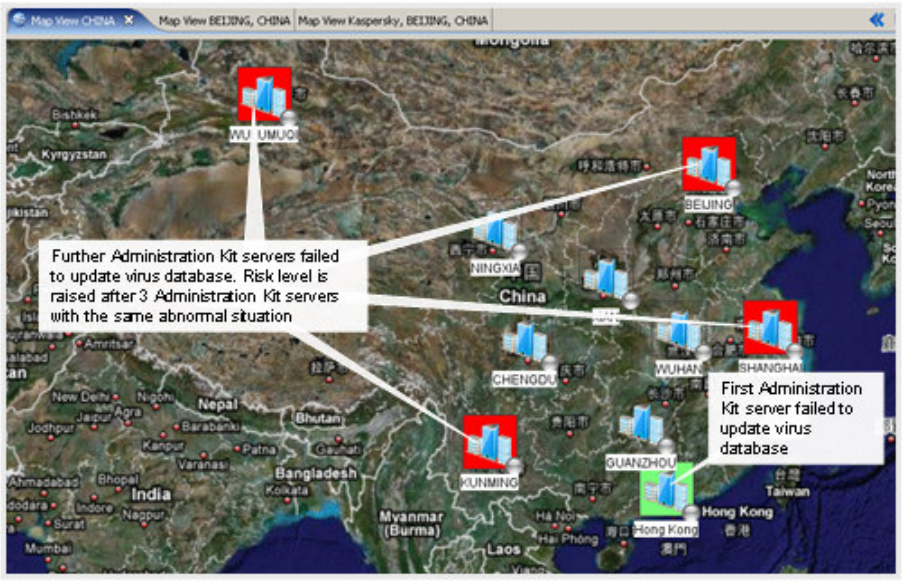
ii) KAV of the Administration Kit server is not using the updated virus database

iii) Variant of the Conficker has appeared but the Administration Kit server is waiting for the virus database update

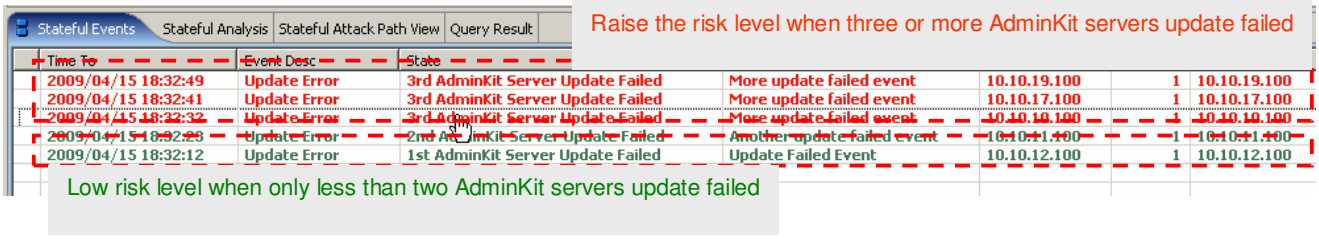
SIMCommander K-SOC provides additional layer of detection to prevent Conficker outbreak

As mentioned above, an easy way to verify the Conficker worm infection is to access the Kaspersky web site to update virus database. However, in a large enterprise environment, the virus database update is distributed through the Administration Kit to multiple KAV clients. Thus, the focusing point is to ensure the Administration Kit servers able to update the virus database from Kaspersky web site but not the endpoints.

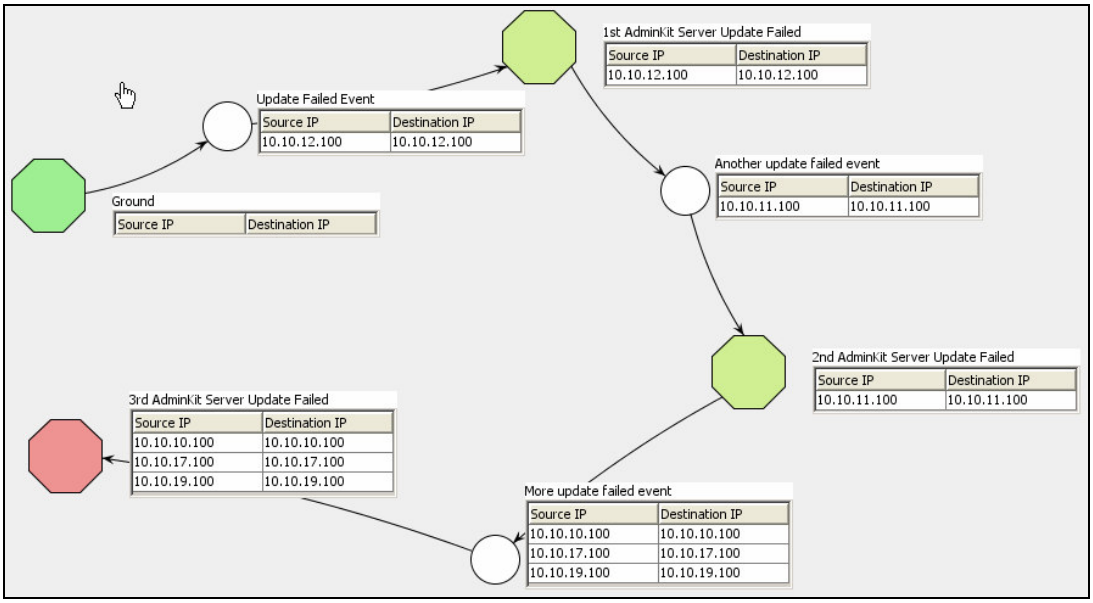
In a large enterprise, it is difficult to control and verify if all the Administration Kit servers are installed up-to-date Microsoft patches and Kaspersky virus database. Nonetheless, K-SOC adds value to provide additional layer of protection to monitor the Administration Kit server behavior proactively and automatically. When the Administration Kit server is infected by Conficker, the Administration Kit cannot update the virus database and generate the 'virus database update failed' event as aforesaid. By using K-SOC, you can create a monitoring rule to detect the 'antivirus database update failed' in Administration Kit servers via the intelligent Abnormal Behavior Detection technology. The detail procedures to create the rule are documented in next section. When the Conficker worm is spreading among the Administration Kit servers, you can receive real-time notification and see the following screen in the K-SOC console.



During the virus outbreak, time-to-respond is the most critical factor to contain the situation. K-SOC allows you to drill down the detail for quick virus response. As shown in the below figure, the events from different Administration Kit servers are consolidated by the K-SOC Advanced Detection Technology.



You can also conduct the infection path analysis by accessing the Stateful Path in the K-SOC console to present the Conficker infection graphically. This Stateful Path presentation is to simulate the analysis flow of the rule defined above with the victim IP address. Hence, it is easy for you to identify which Administration Kit servers are under infection as shown below.



Create intelligent Abnormal Behavior Detection rule to prevent Conficker worm

Prior to the rule creation, you have to define the parameters according to your enterprise security policy or requirements. This document uses the following criteria to define the abnormal behavior detection rule.

The abnormal event used in this case: *AntiVirus database update failed*

The number of Administration Kit servers with 'AntiVirus database update failed' is considered as abnormal: *3*

Timeout value of the detection: *90 minutes*

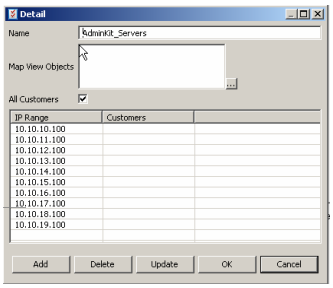
The risk level before the abnormal situation happened: *2*

The risk level after the abnormal situation happened: *7*

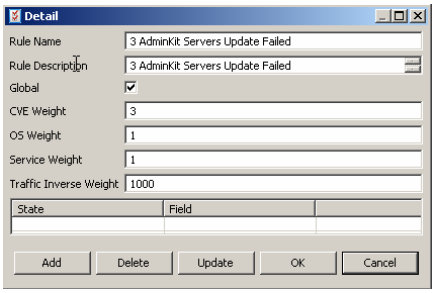
After defined the criteria, the next step is to following the procedures below to create the rule in K-SOC.

1. Launch the K-SOC console and click the Alert Configuration.

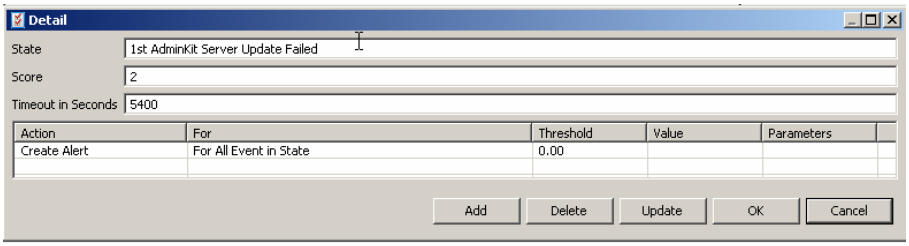
2. Create a Network Object Administration Kit_Servers. Then, you can input all the Administration Kit servers IP address to the object.

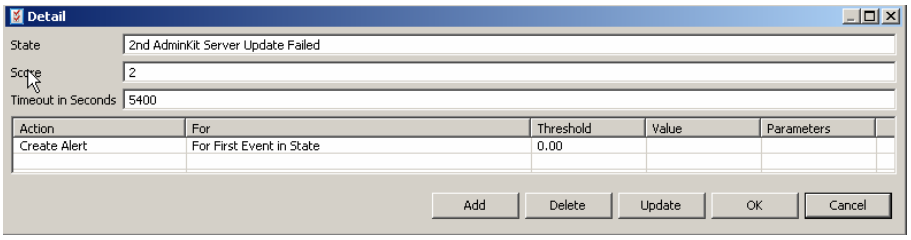


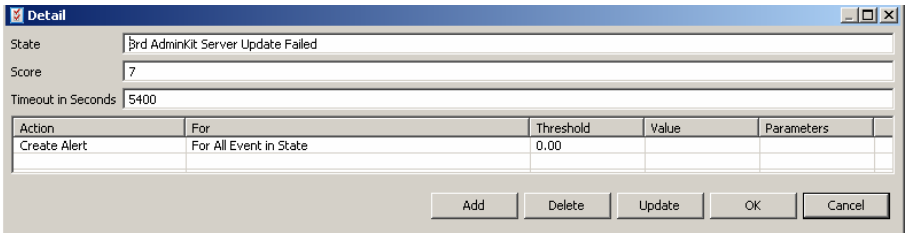
3. Create a new rule to detect the abnormal situation of '3 Administration Kit servers failed to update virus database'.



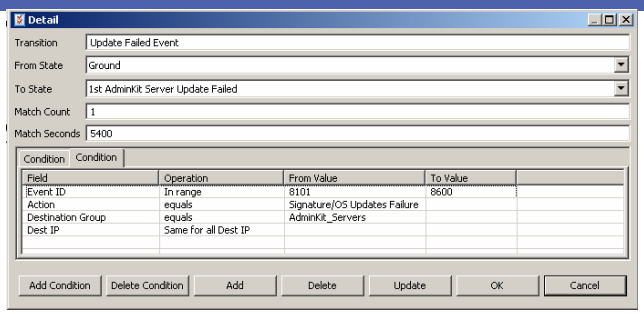
4. Create three states for this detection – the 'update failed situation' for the first, second, third and further Administration Kit servers. The first two states of the State Score is assigned to '2' and the last State Score is assigned to '7'.

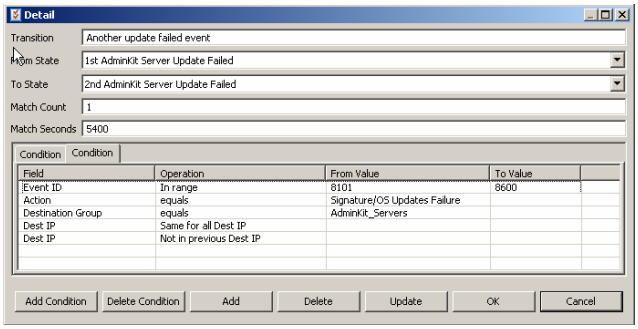


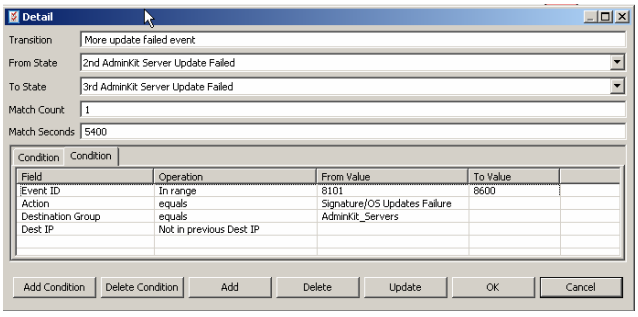




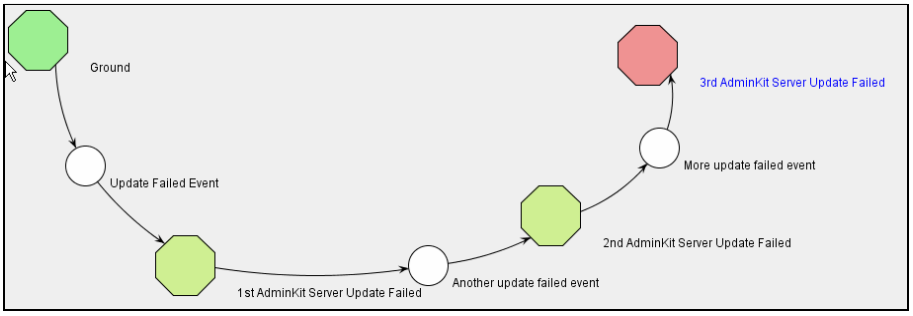
5. After created the States, the next step is to create the Transitions as shown below. Input the parameter as defined the match count = 1 and the timeout = 5400, select the condition as action = 'Signature/OS update failure'. Because we want to limit the detection only for Administration Kit Servers, so we have to add the condition Destination Group = 'Administration Kit Servers' where this is the network object created in step 1. In the second and third Transition, we have to add the condition 'Destination IP address' is 'not in previous Dest IP' to differentiate the same Administration Kit Servers sending multiple update failed events.







6. After completed the above steps, you can be able to see the following analysis rule. The last step is to save this rule to take effect.

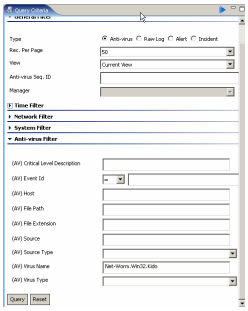


Verification:

After defined the correlation rule, if you want to confirm the Conficker virus out of the network, you can perform the following steps.

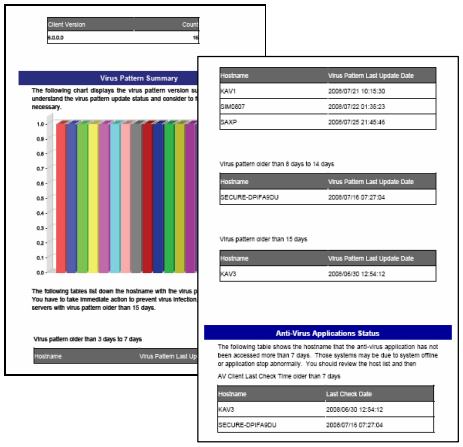
1. By Query

The purpose of query is to confirm if any computer detected the Conficker worm appeared in the network. You can launch the Query view in the K-SOC console and search for the computers with the virus 'Net-Worm.Win32.Kido' or 'Net-Worm.Win32.Kido.bt' or 'Net-Worm.Win32.Kido.dv' or 'Net-Worm.Win32.Kido.fx' detected.



2. By Report

You generate the report 'AntiVirus Client Status Report' from the K-SOC to have the overview picture of which computers are using outdated virus database. According to the Kaspersky Viruslist information, the last Conficker worm information is added to the Kaspersky virus database on 16 March, 2009. That means, all the computers using the virus database older than 16 March, 2009, they are in the risk of Conficker (aka Kido) worm infection. You have to force the update from the Kaspersky Administration Kit to those computers to prevent Conficker worm infection.



Resolution Procedures:

In case of Conficker infected, you can follow the procedures to clear the worm.

1. Follow the instruction in the Viruslist to clear the Windows registry and files in the following link

   http://www.viruslist.com/en/viruses/encyclopedia?virusid=21782725

2. Apply a patch as described in Microsoft Security Bulletin MS08-067.
3. Update latest antivirus software and signature pattern.
4. Perform online scan by Kaspersky when necessary, you can visit the Kaspersky scanner under http://www.kaspersky.com/virusscanner.

Enquiry:

For any feedback or enquiry to this document, please send email to advisory@simc-inc.com.

Additional Resources:

CBS News

- http://www.cbsnews.com/stories/2009/03/27/60minutes/main4897053.shtml

CNN News

- http://edition.cnn.com/2009/TECH/ptech/01/16/virus.downadup/index.html
- http://edition.cnn.com/2009/TECH/03/24/conficker.computer.worm/

Microsoft Security Bulletin MS08-067

- http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
- http://support.microsoft.com/kb/958644

Kaspersky Lab Viruslit

- http://www.kaspersky.com/technews?id=203038750
- http://www.viruslist.com/en/alerts?alertid=203996089
- http://www.viruslist.com/en/viruses/encyclopedia?virusid=21782725
- http://www.viruslist.com/en/viruses/encyclopedia?virusid=21782733

TrendMicro Security Advisories

- http://us.trendmicro.com/us/threats/conficker-worm/?WT.mc_id=2009HP_Hero_Conficker&WT.ac=2009HP_Hero_Conficker

Symantec Security Response

- http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99&tabid=2
- http://www.symantec.com/norton/theme.jsp?themeid=conficker_worm&inid=us_hhobanner_conficker

McAfee Threat Advisories

- http://www.mcafee.com/us/threat_center/conficker.html

Computer Associates

- http://www.ca.com/us/securityadvisor/vulninfo/vuln.aspx?id=36809

CERT Vulnerability Note and Alert

- http://www.kb.cert.org/vuls/id/827267
- http://www.us-cert.gov/cas/techalerts/TA09-088A.html