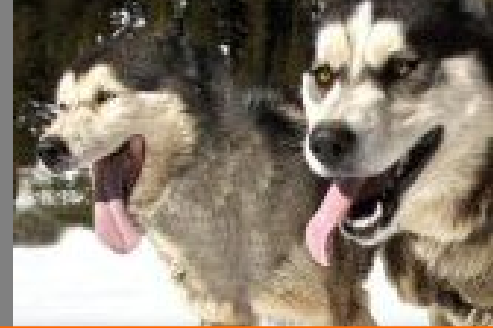


CYBERGATEKEEPER



CYBERGATEKEEPER PROACTIVELY COMBAT CONFICKER & OTHER MALWARE INFECTIONS

June, 2009

Network Utilities (Systems) Limited

Liberty House, 516 Walton Road,

West Molesey, Surrey KT8 2QF

Tel: 020 8783 3800

Web: www.netutils.com

Email: info@netutils.com



© 2009 InfoExpress, Inc.

The information contained herein is the property of InfoExpress, Inc. and may not be copied, used or disclosed on whole or in part, stored in a retrieval system or transmitted in any form or by any means (electronic, mechanical, reprographic, recording or otherwise) without the prior written permission of InfoExpress, Inc.

CyberArmor, CyberGatekeeper Remote and CyberGatekeeper LAN are registered trademarks of InfoExpress Inc. All other product names are registered trademarks of their respective owners.

Document ID: WP09-0623-01NU

 **infoexpress**

www.infoexpress.com

INDEX

Forward 2

Executive Overview 3

How can Conficker be detected and how easy is it to do so? 5

Detect - Positively Establish PC Infection..... 5

Respond - Notify and Report 6

Respond - Automatic Clean-up..... 6

Proactive Protection..... 6

Conclusion 7

Extending Capability - Generic Malware Detection 8

Closing the Vulnerability & Threat Gap..... 10

About InfoExpress??..... 13

About Network Utilities (Systems) Limited..... 13

Forward

This document anticipates that the Reader understands the threat that Conficker and many similar malware attacks pose. For that reason, the author feels a discussion regarding the threat is not required in the context of this document.

Executive Overview

Conficker is a well publicised computer worm that propagates itself around networked desktops to collect and steal data: sending it to the originator of the attack.

As it infects a desktop, it also protects itself by disabling or turning off key services and security software. This makes it more virulent and difficult to detect. *[Conficker is not the only malware exploit to act in this manner].*

Anti-virus, spyware and the Microsoft Security Update process combat malware exploits, but only after the vulnerability has been characterised. This leaves a protection void which can be taken advantage of by the likes of Conficker and other malware threats thereby altering the security paradigm by raising questions that include:

- Are we actually infected?
- How can I find out?
- What is extent of the infection?
- Which PCs are actually infected?
- How do we go about the clean-up?

It leaves Security & IT Professionals faced with a number of technical and operational challenges to identify the extent of an infection, to remove it effectively and economically and stop re-infections.

CyberGatekeeper works for the professionals by answering the questions and overcoming the resultant challenges. Its use will rapidly identify infected machines, work to keep them off the network and prevent them from infecting more machines. Furthermore, it provides an effective solution that will efficiently remove infections without the need to physically visit every contaminated machine. It then protects against re-infections, achieved by constantly checking every desktop and denying network access to any remaining infected machines until they have been cleansed by the CyberGatekeeper process.

[Security posture checks must continue after logon and that is a standard function of CyberGatekeeper].

Security and IT Professionals list the following challenges where Conficker is concerned:

1. How to determine whether the company is infected or not?
2. Having established an infection the excessive time and effort it took to locate which other desktops were actually infected.
3. The time needed to perform the clean-up operation. *[Points 1 & 2 have financially, proved very costly].*
4. Having a reliable mechanism to eliminate re-infections.

5. Lack of the ability to affirm that every company Desktop is security patched to combat the threat, in a timely manner.
6. Lack of reference data that assists the improvement of "Incident Response" procedures and heighten user awareness.

CyberGatekeeper overcomes these challenges by:

- A. Inspecting every PC across the Enterprise and identifying whether the malware profile was found, isolating any infected PC and also writing a record to log each action, against User and PC name, for reporting purposes. [With this process in place it takes only a few man minutes to search and run a report that lists infected machines with User and PC name identifiers].
- B. Providing the tool that isolates infected PCs from all others.
- C. Providing the mechanism to clean up infections from a central location without the need to despatch qualified personnel to visit and manually disinfect every infected PC..
- D. Delivering the tool that can be easily and quickly configured by administration to specifically inspect for the now known exploit or malware and not allow network connectivity to infected PCs until that infection has been removed; thereby immediately preventing re-infections. *(N.B. CyberGatekeeper can be setup to automatically remove an infection either when detected at the point of connection, or when infected whilst being network connected without manual intervention.)*
- E. By monitoring and policing all PCs to positively affirm that required security patches have been applied. Also that Spyware, Antivirus protection software etc. is always properly up-dated with their latest vaccine [DAT] files applied.

[This is by far the best way to stop infections in the first place and in a production environment reported as the most difficult to guarantee.]

How can Conficker be detected and how easy is it to do so?

Below is an overview of the Conficker profile footprint:-

Conficker sets this Registry Entry
<ul style="list-style-type: none">▶ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL CheckedValue = 0
Conficker can be found using this Registry Entry
<ul style="list-style-type: none">▶ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\dl
Conficker Stops and Disables these services
<ul style="list-style-type: none">▶ wuau serv – “Automatic Updates”▶ BITS – “Background Intelligent Transfer Service”▶ WinDefend – “Windows Defender”▶ wscsvc – “Security Center”▶ ERSvc – “Error Reporting Service”▶ WerSvc – “Windows Error Reporting Service”
Conficker Deletes these Registry Keys/Entries
<ul style="list-style-type: none">▶ HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Windows Defender▶ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot▶ HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\ShellServiceObjects\{FD6905CE-952F-41F1-9A6F-135D9C6622CC}

It can be clearly seen from this profile that “check for conditions” can be found on an infected PC. These conditions are used by CyberGatekeeper to detect the presence of Conficker.

Detect - Positively Establish PC Infection

A CyberGatekeeper test exists to inspect for the Conficker registry and process changes. If true the PC is positively certified as Conficker infected. Detection therefore is easily achieved!

CyberGatekeeper will make this determination when the PC first attempts to network connect and within seconds during the session if the PC becomes infected while network connected. *[The latter*

is most valuable because such infections can equally occur whilst network connected]. In either case, the infected PC is immediately isolated from the network and from all other machines. It remains in that state until it has been disinfected [cleansed].

Respond - Notify and Report

On detecting an anomaly or infection CyberGatekeeper can immediately message the User. The notice may be specific to the condition detected. Simultaneously, an audit entry will be written and those details can be reviewed using the Report Tool.

The User Notice [*pop-up message*] should contain the helpdesk number to call, a fault title (i.e. Suspected Conficker Infection), the Incident Response Code (IRC) and any appropriate short footnote you may wish to add. It could include a link to an Intranet web page if needed.

CyberGatekeeper collects and references the User and Host name in the Report Tool, plus which Inspect condition failed and then all the other details that the policy inspection process collected.

This is your centralised audit record that can be searched, filtered or exported as is required. Through its use all the infected PC's can be collated into a single report for the Incident Response Team or, later, for regulatory review. It can also be used as a reference to confirm the accuracy of the incident reported by the User.

Messaging the user and including an Incident Response Code is an excellent approach because it defines the procedure that tells Helpdesk staff exactly how they are to respond to the incident reported.

Respond - Automatic Clean-up

Once the cure for Conficker has been positively identified an automated clean-up process can be established and then initiated under CyberGatekeeper control. Clean-up can take the following forms:

1. Detect and download a clean-up programme to run on the PC
2. Detect and run a clean-up programme from a remote location
3. Detect and target deletion of infected or anomalous elements
4. Detect and then run or download an uninstall programme
5. Detect and download security patches and security software updates

These processes can be automated and applied the moment the infection is detected. There are options available to make the process known to the User, or not, according to the system administrators preference.

Proactive Protection

Please refer back to the Conficker profile on page 5. It is noticeable that Conficker protects itself by turning off certain processes and services. By monitoring those processes CyberGatekeeper

becomes a first line of defence and a proactive protector. Used with our automated remediation process, disabled services can be re-initialised and turned back on and if they cannot be for any reason, the PC in question can be removed from the network pending further investigation. Once again the User can be appropriately notified and failure details are easily found in the Report tool.

Another proactive function delivered by CyberGatekeeper is to assure every PC is kept current with the latest Microsoft OS Security Patches. CyberGatekeeper can inspect for those required and “kick off” the download process of your choice when the Desktop connects or while it’s network connected. That activity is achieved without disrupting the Users login process and is governed by your requirements and the configuration of CyberGatekeeper.

Similarly, verifying that the Anti-spyware and Antivirus programmes are functioning and their latest virus definition files are applied is another proactive way CyberGatekeeper acts to provide enhanced protection. After all, you’ve made a significant investment in desktop security protection, so it’s vital and logical that it be maintained in best working order.

Monitoring security protection software and applying security patches in a timely manner is the best practice method of combating the continuing attack strategies used by today’s Hackers. This is a factor recognised by Gartner in its latest NAC survey.

N.B. It is suggested that Conficker could also be detected by running a specially crafted network scan.. This should be the case, however, and equally realistic, the “Scan” could be blocked by the PC firewall, a complication in the process you can well do without. And in many instances, there’s no guarantee that the PC is connected when the scan occurs or protection afforded should the PC become infected between scans.

Conclusion

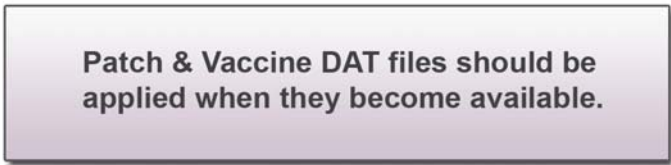
CyberGatekeeper delivers proactive protection against Conficker and other malware. It combats the real issues of infection by:-

- ▶ Providing early notification that there is an infection,
- ▶ Identifying all machines affected, saving the time, effort and cost to discover those,
- ▶ Saving time, effort and cost of clean-up: enabling an automated, swift clean-up from one central location, or several strategic locations,
- ▶ Putting in place a mechanism that combats chances of re-infection,
- ▶ Putting in place a mechanism to positively affirm every company PC is security patched to combat all such threats,
- ▶ Helping to improve “Incident Response” procedures and heighten User Security Awareness.

Extending Capability - Generic Malware Detection

To recap, more modern malware when infecting a PC protects itself by disabling or turning off certain protection functions and services, some of which have been specifically implemented to protect against malware infections.

Microsoft, as well as Anti-virus and Anti-spyware vendors are vigilant in providing security patches and DAT file updates. Generally they are retrospectively applied and designed to deal with product vulnerabilities that may have, or had been, exploited and if possible to identify and cleanse from the system or patch the vulnerability exploited. It is certainly a vital security practice that unfortunately is still no guarantee that future exploits will not circumvent.



Patch & Vaccine DAT files should be applied when they become available.

CyberGatekeeper can be configured to inspect for the symptoms of an infection and respond as directed by the Threat Management or Incident Response strategies you have adopted. It introduces a “behavioural” element to the protection process.

As explained earlier, CyberGatekeeper is set-up to inspect for specified conditions and if those are altered, respond by bringing them back to a “compliant” working state. *[As an example, check that Windows Update is on and if turned off respond by turning it back on.]* In each case the policy rule is distinct in searching out symptoms, and the response *[including whether the user is notified or not]* is specific to the violation of symptoms making up that rule.

With CyberGatekeeper a rule combination can be applied to a “policy” and if an inspected condition is violated separate response actions for each violation can occur. By making use of this CyberGatekeeper feature, policy rules may be constructed to differentiate between one condition violated and a group of conditions violated altogether. The group of conditions failing together is really a **behavioural** change and serves as a warning that something unusual has occurred that should be immediately investigated.

Consider that a PC is successfully connected having passed inspection. While on the network its AV software becomes disabled, Windows update service is turned off and the Windows Error Reporting Service is disabled. The PC now fails inspection because a series of conditions have been violated together and its detection rule activated. In this case the User would be warned that their PC maybe malware infected and to contact helpdesk. Even if the PC is not infected, this combination of faults should be investigated: so our behavioural process has not created unnecessary work.

Should the PC prove to be malware infected, you’ve caught it at a very early stage and can

respond as dictated by the Company's incident response procedures.

Once the investigation has been completed a CyberGatekeeper rule which positively identifies the infection can be added to the policy [with or without a clean-up remediation action] to positively combat the infection throughout the Enterprise, and catch the infection stragglers and to prevent possibilities of re-infections as well.

Finally, you will also have an audit trail for reporting purposes.



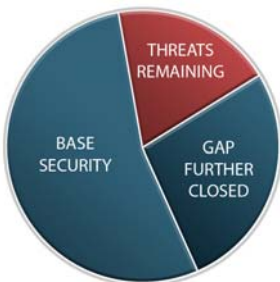
CyberGatekeeper also introduces greater proactive security because:

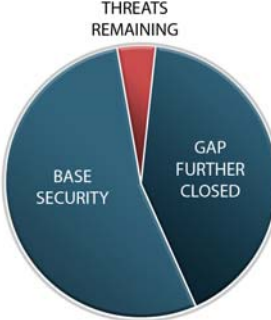
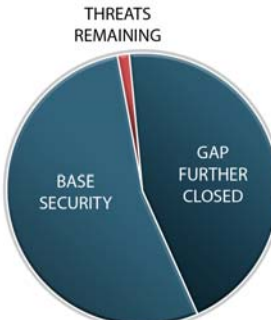
1. Every PC is constantly surveyed as compliant when it connects and throughout its session.
2. Patching stragglers are caught and immediately dealt with when they connect, no matter how short the duration of that connection.
3. If a protection resource is missing or turned off, it's immediately turned back on without constant Admin or User intervention.
4. Conditions not sanctioned are immediately resolved.

Closing the Vulnerability & Threat Gap

When CyberGatekeeper is used as an integral part of a protection strategy it certainly closes the vulnerability and threat gap by boosting your Company’s security protection posture. The table that follows explains how.

Strategic Protection	Graphical Closing the Gap	How CyberGatekeeper Delivers
<p>Base Protection</p>		<p>Antivirus & Spyware Software plus Personal Firewalls</p>
<p>Positively confirm only your own desktops network connect.</p> <p>All alien computers are kept off the network.</p>		<p>The CyberGatekeeper agent on the desktop exclusively belongs to your CyberGatekeeper implementation. It defines the desktop as a true company PC.</p> <p>To supplement that, a required rule in the “policy” can be added. That rule specifically checks for your own “digital certificate” if used, a specific hidden parameter of your choice or certain elements that define your PC build characteristics.</p> <p>Ours is a back-end authorising process where no evidence exists on the desktop that can pinpoint what is being checked. This makes it extremely difficult to circumvent our protection process.</p>
<p>Monitor security software packages are functioning to maximum efficiency.</p>		<p>Have a required rule in the “policy” that constantly checks that the required software programme has in fact started, is patched to required version and is using the most up-to-date virus definition file.</p> <p>Those checks constantly occur while network connected as well, with negligible impact on link bandwidth.</p>

Strategic Protection	Graphical Closing the Gap	How Delivered
<p>Monitor that key services have started and remain started while the PC is network connected.</p>		<p>Have a required rule in the “policy” that specifically checks that each mandatory service has in fact started.</p> <p>If not found invoke an automated response to restart that service.</p>
<p>Monitor that Operating System and Microsoft product security patches have been applied.</p>		<p>Have a required or desired rule in the “policy” that constantly checks that the mandatory patches are present, applied and running. If missing, an automated response can be invoked to kick-off the adopted procedure and the necessary update is then applied.</p> <p>If a desire rule is used the User logon process would not be interrupted.</p> <p>Infoexpress provides regular rule updates that include critical Microsoft security patch tests.</p>
<p>Monitor that prohibited programmes, or criteria like USB use, multiple NIC interfaces etc. are not active while network connected.</p>		<p>Have a prohibit rule in the “policy” that specifically checks for Windows registry settings, processes or services for these factors.</p> <p>If they alter, because the process has started, or the device is used, or network connectivity initiated through a second NIC interface, the offending PC is removed from the network.</p> <p>When the policy is breached Users can be notified and corrective actions taken.</p> <p>The action CyberGatekeeper takes is governed by your settings, policies and procedures.</p>

Strategic Protection	Graphical Closing the Gap	How Delivered
<p>Automate the patch download process at point and time of connectivity.</p> <p>Automatically reverse a monitored condition and return it to its correct state.</p>		<p>Such remediation actions are initiated from the policy test, and the remediation action may be explicit to each test.</p> <p>Failure of test calls a script from the back-end Remediation server. These scripts can be downloaded and run on the offending PC or run directly from the server itself. Scripts can be designed to perform a wide range of “fix” actions, including deleting files or un-installing for example peer-to-peer programmes.</p> <p>Infoexpress can provide remedy scripts or the client can build their own.</p>
<p>Monitor for a combination of anomalous conditions indicative of malware infection.</p>		<p>CyberGatekeeper tests can be configured to check for factors like AV & Windows update disabled or desktop firewall turned off, amongst many other criteria. Each would have its own unique remediation action linked with that test failing.</p> <p>In addition a test can be designed to look at a combination of anomalies and when the combination is detected, message the User. This pop-up warns that a possible malware infection is present and notifies whom to contact, plus contact details.</p> <p>Remember, DNAC creates zones of Computer Host “Friends”. Until any connecting PC is declared a “Friend”, i.e. successfully passed audit, it has no ability to communicate with peer host machines or, uncontrolled, with the default gateway. Hence DNAC controls the peer-to-peer communications process using a special IM shim making it more difficult for worm style infections to propagate</p>

CyberGatekeeper significantly improves desktop protection

As with any security solution it is irresponsible to claim 100% protection is achieved

About InfoExpress??

CAN WE DETERMINE WHETHER WE ARE USING Infoexpress OR InfoExpress? Which is correct?

Infoexpress is a privately owned company that has provided network security solutions for enterprises since 1996. The headquarters are in Mountain View, California, with offices throughout the United States, Canada, AsiaPAK and UK. InfoExpress has a strong product base with 15 years experience delivering its own VPN, Firewall, and NAC technologies.

The first product was VTCP/Secure and is a Proxy VPN technology that is still supported and in used by many large customers. It was the first VPN in the market to check for endpoint compliance before allowing the PC to join the network.

The second product CyberArmor was released was in 1999. CyberArmor is a centrally managed personal firewall and is widely deployed. Key features: small footprint with true enterprise scalability; Environmentally Sensitive Policies (ESP) that allow for smart policy configurations; Network and Application controls; and Central management and reporting features.

CyberGatekeeper was released in 2002 as in-line technology that enforced remote endpoint policies. In 2004 the technology was extended to enforce endpoint policies for the internal LAN. In 2006, along with version 5, DNAC – Dynamic Network Access Control was introduced. The value proposition for DNAC is that it can be deployed quickly without any network changes, is vendor agnostic and requires no hardware upgrades.

InfoExpress continues to lead the market with innovative solutions in this space.

InfoExpress' installed base includes many global organizations that have deployed up to hundreds of thousands of seats.

View video demonstration of DNAC at: <http://www.infoexpress.com/pads/demovideo.php>

About Network Utilities (Systems) Limited

Network Utilities is an Infoexpress premier partner.

Established in 1992, Network Utilities is a privately owned company with many years of experience in the IT sector, working across multiple verticals. Our speciality is our genuine ability to align technology with business objectives and goals. Our focus is built upon a foundation of four diverse but complementary elements; Availability, Security, Speed and Compliance. Our solutions and services are based upon the leading products in the industry and support some of the largest and most complex networks in the world. Our clients span all industry sectors and sizes from local and central public sector organisations through to large multi-national enterprises.

Visit www.netutils.com for information and customer testimonials.

To contact Network Utilities please call:

Network Utilities (Systems) Limited

Liberty House, 516 Walton Road,

West Molesey, Surrey KT8 2QF

Tel: 020 8783 3800

Web: www.netutils.com

Email: info@netutils.com

