



Managed Security In Action White Paper Series – Nuspire Networks

Michigan’s Premier Global Managed Security Provider

Keeps Thousands Of Geographically Dispersed Locations

Secure From Conficker Virus

**By Markus Davis, Brian Klumpp, Saylor Frase, Dan Hoban
w/Jim Hebler**

©®Nuspire Networks, May, 2009

Table of Contents

- I. Introduction**
- II. About Nuspire**
- III. Conficker Virus – A Brief Background**
- IV. Parallels – Pandemics, Network Security and Viral Botnets**
- V. Nuspire Network Team Identifies Conficker and Its Effects**
- VI. Identifying the Symptoms – Nuspire Team’s Holistic Approach**
- VII. Protecting the Enterprise – Nuspire Closes The Gaps Through Myriad of Industries**
- VIII. Managed Remote Detection, Elimination and Seamless Removal**
- IX. Continuing the Vigilance – Like Swine Flu, Conficker Can Continue Moving Forward**
- X. Closing Thoughts – Conclusion**

Introduction

In late November, 2008, the Global Managed Security experts at Nuspire Networks noticed and identified the real-time symptoms, effects and perversely ingenious tactics of a network based pandemic quick to be known as the Conficker Virus. In its role as a Managed Security Monitoring Services provider for global, geographically dispersed organizations in Manufacturing, Supply Chain, Distribution, Retail, Health Care and Telecommunications-Data provisioning, Nuspire's real-time Network Operations Center enabled a unique initial view of this resilient virus.

Early versions and variants of the Conficker Virus were network based, infecting vulnerabilities on Microsoft Windows versions 2000, XP, Vista, Server 2003, Server 2008 and Windows Server 2008 R2 Beta, according to Microsoft. On October 23, 2008, Microsoft released an emergency "out of band" patch to close the vulnerability. However, as of January 2009, an estimated 30% of affected Windows PCs remained vulnerable. The hackers responsible for Conficker (Russian and or Eastern European authorship is suspected) provided the ability for the virus to propagate over Local Area Networks (LANs) through removable media and network shares, enabling the virus to sustain, reproduce and infest ever-more-rapidly through varying network enterprises. Between 9 and 15 million PCs were estimated to be infected with exponential facilitation possible at appointed times as determined by the hacker-authors responsible.

For the purposes of the confidentiality and customer relationships Nuspire will keep its references to Conficker afflicted networks, infrastructure and associated enterprises nameless, only referring to industry, type and individual situation.

The purpose of this White Paper is to chronicle Nuspire Networks experience and real-time management of the Conficker Virus, as well as its tactical ability to remove and destroy it via both remote and on-site management and its continuing monitoring of its symptoms as its authors continue to launch it on a timed basis.

About Nuspire

Nuspire Networks is an over a decade old Global Managed Security and Real-Time Network Monitoring firm with its Network Operations Centers based in Michigan.

Nuspire's technical specialty is managing the network enterprise and mission-critical information assets of Geographically Dispersed facilities in most every industry vertical.

Nuspire excels at helping its customers manage multiple locations for customers in Health Care, Major Retail, Telecommunications, Manufacturing, Supply Chain, Vehicle Dealerships, Food Distribution, Grocery Store, Chain Restaurants and any and all organizations who want to keep its information Secure, Compliant and Secure.

Nuspire's highly trained team is lead by some of the best Information Security experts in the industry today. Simply put, Nuspire's highly talented and intuitive team brings hundreds of years of collective Managed Services experience within the discipline of Real-Time Monitoring, Information Security and Mission-Critical data asset control. Nuspire also helps organizations manage and filter content flow, data acceleration, infrastructure implementation and management and data storage-disaster recovery.

Nuspire Network solutions are comprised of Best-Of-Science technologies developed internally and from a who's who of partners within the Network Security, Information Technology and Professional Services industries today.

Conficker Virus & Nuspire – Background

In late 2008 into January-March 2009, the Nuspire Networks' Security Team lead by Brian Klumpp, Marcus Davis, and David Skimin all were being alerted to the development and implementation of virtual *sandboxes* or *botnets* comprised of groups of eight to 16 machines attempting to gain access behind customer firewalls. And, thanks to its ability to morph and confuse end-users, some locations were inadvertently helping Conficker nestle and settle into Customer Target environments under the guise of "solving" the initial problem.

Marcus Davis and the team at Nuspire quickly isolated and assessed Conficker in early 2009, utilizing a secure, standalone Windows server as a "Conficker Laboratory" so as to understand its various forms, templates and variants while also enabling Nuspire Managed Services team-members the ability to identify, isolate and securely detonate the virus in real-time while preventing loss of any mission-critical data, identity theft and information loss.

In Nuspire's managed network infrastructure of thousands upon thousands of locations, Conficker reared its ugly capabilities and survivability throughout North America. Fortunately, the Nuspire team – after alerting its major-player security partners – had quarantined the virus and was helping its customers ward off its effects while killing it in real-time beginning in November, 2008 when it infected a group of varying Manufacturer Dealerships (both American and Japanese) throughout the Greater Midwest and along the Eastern Seaboard. It was at this point that Nuspire Networks was working closely with leading Security OEM Providers in helping the Network Security industry identify these similar and disparate threat tactics as Conficker.

Parallels – Pandemics, Network Security and Viral Botnets

"Conficker is probably the most amazing and resilient virus I have seen to date," said Marcus Davis, Nuspire's frontline team manager in its battle against Conficker. "We think it originates from Russia and Eastern Europe. It's authors have disguised it so it will launch or reinvent itself under the guise of downloading anti-Conficker virus protection software. It will lie dormant and then launch out of a pop-up under the form of an attack ad server. Its authors can launch security breaches and have it hit everywhere, or, target specific locations, gathering one, 10 or hundreds of signatures. When we saw it attacking our locations or attempting to attack our retail firewalls, it blocked our initial attempts to remotely launch the software built to remove it. In a dark, perverse way, it's a brilliant worm that has infected millions of personal computers and thousands of servers."

And, by spreading computer-by-computer, server-by-server and through regionalized network clusters, Conficker enables savvy hackers to develop a virtual infrastructure to impose its own code to gather and secure identities, credit card numbers, mission-critical information, proprietary and confidential code – and any number of items at the author's discretion.

And, when considering that the Conficker Virus has been developed to morph into a myriad of formats once it exploits a vulnerability, without services such as Nuspire's constant monitoring and real-time identification, management and destruction, the spread of this virus could have been much more devastating to Nuspire's clients., this Worm

Nuspire Network Team Identifies Conficker & Its Effects

To sit on the inside of the Nuspire Networks' Operation Center replicates the effect one might feel when witnessing Mission Control at NASA. Network transmissions, activity and security events in increments of the millions– from PCs, PDAs, Cell Phones, Point-of-Sale Devices in each and every global location it serves – are monitored and managed in real time. Hot spots and suspect transmissions are identified. Customers are notified in real-time. When Conficker began to appear in its unique and resilient forms, slowing network transmissions, web-traffic congestion and slow performance all coalesced to provide the initial evidence of this worm-viruses' manifestation – it was sole dedicated viral awareness, isolation and detonation team at Nuspire who cornered Conficker in Virtual Servers at the Network Operations Center laboratory.

“We were seeing the slow performance of some of our distribution centers, web supply chain providers and vehicle dealerships; we immediately got on the phone with these customers,” Davis recalls. “And, when these customers tried to go out to Microsoft to access necessary patches or any of the major security providers, Conficker would block their attempts to access.”

In real-time, Nuspire could see the virus attempting to attack customers' servers. And, in real-time, the Nuspire team worked closely with its dealer-supply chain and affected retail customers to take infected machines off-line while ensuring that customer identities, social security numbers, credit check and credit card information were not exposed or infected as the team quarantined and destroyed the virus, Davis said.

“In some instances, we could see the attempts for created botnets to somehow communicate with remote servers while awaiting further instruction,” Davis said. “We also could see this thing trying to communicate everywhere as we received reports from our customer contacts. The ingenious way this threat subverted many anti-virus software and firewall prevention programs by subtly changing its signature or simply laying low in the background masked as a Microsoft Windows component was a challenge to counter.

Nuspire Desktop NuVu Painting the Threat Picture

When Nuspire circulated its NuVu Desktop Monitoring tool enabling customers to see real time Network threats, the Virus detection team didn't realize how effective it would become in assessing the threat early, often and consistent....frankly, the tool was built to reduce unnecessary customer calls and to increase the efficiency of proactive communication to corporate customer contacts. By being more transparent and pro-active, customer IT managers at media centers, health care facilities, distribution centers or retail facilities with PCI compliance concerns could assure their executives in advance of concern – ensuring less stress and increased security at every turn.

As Conficker botnets quietly built its silent embedded army from three-to-10 million PCs, exploiting vulnerability gaps in Microsoft Windows platforms created over the past decade, Nuspire's NuVu enabled its customer end-users to align its prevention servers with a dedicated army that was two and three steps ahead in identifying the Conficker characteristics, strains, disguises and isolation-prevention tactics remotely from the Nuspire NOC – freeing up the customer to focus on the core business at hand....

“Back in the November and December timeframe, we were working with our Security partners in unison with diligence and vigilance to surround the threat while anticipating what its overseers in Russia, Eastern Europe and China had in mind,” said David Skimin, part of Nuspire's threat monitoring team. “We all knew that many corporate networks and end-users had ignored Microsoft's effort to alleviate Conficker back in late October; the patch went out on the 23rd of that month and yet many people at corporate offices, their “work” –

focusing on closing the deal or getting the latest task done – had hit ‘ignore’ or ‘apply later’ thinking ‘IT will take care of it.’

“Once it’s embedded, it’s up to us to isolate and detonate this problem remotely ourselves or to walk our customer through alleviating the threat,” Skimin continues. “As long as we can take the affected system off-line while ensuring that customer data or financial information isn’t affected, then our efforts could be saving millions of dollars and the customer’s reputation in the marketplace.”

The entire industry has seen what’s happened at T.J. Max or Heartland Payment Systems – major retailers and the Credit Card industries fourth largest provider to see how millions of dollars and thousands of financial records are all squandered and vulnerable. Each massive breach has affected hundreds of thousands of citizens and cost each organization hundreds of millions in lost revenue along with irreparable damage to their reputations.

Managing The Real-Time Impact – Nuspire Security Expertise In Action

The Nuspire Networks team, due to its unique technology and 24 x 7 x 365 Managed Monitoring services model – was out in front of the Conficker Virus situation. Nuspire Networks continues to be vigilant in its isolation, management and detonation of Conficker and other future yet-to-be-cleverly-named threats.

In late fall 2008 into the First Quarter of 2009, Nuspire Networks and its dedicated Virus Identification and Monitoring teams utilized Virtual Servers to assess, analyze and unravel Conficker’s characteristics, symptoms and strategies – making sure Nuspire’s unified and thorough understanding could be aligned, accurate and efficient to ensure that its Customers would be spared potentially damaging effects.

“Conficker is one of the most clever and difficult Trojan-virus we’ve ever seen,” Nuspire’s Markus Davis said. “It would be very difficult for a single IT staff or multi-tasking IT professional to be able to isolate and identify Conficker on their own. At Nuspire, we had dedicated teams working on analyzing and understanding Conficker and getting back with our security partners and customers in real time with the information we continued to find.

“And as Conficker lays dormant waiting for its next round of instructions, Nuspire will continue to monitor this situation with vigilance and due diligence,” Davis said.

(SEE ATTACHED E-MAILS and NUSPIRE BULLETINS)

Nuspire Networks Communication Examples

“Nuspire Networks has utilized VMware environment to replicate Windows 2000 SP 4 and Windows XP SP 2 machines. Here is what we found:

- 1) Win2000 w/l.E. 5 no anti-virus – code not able to execute.
- 2) Win2000 w/l.E. 6 no anti-virus – code not able to execute without install of gdiplus.d11
- 3) Win2000 w/l.E. 6 no anti-virus – code not able to execute with .Net installed – Code is dependent on the JRE platform to utilize its advanced JAVA scripts.
- 4) Win2000 w/l.E. 6 Anti-Virus LEADING SECURITY PROVIDER (NAME WITHELD) did not detect malicious code – not removed. LEADING SECURITY PROVIDER (NAME WITHELD) did not detect malicious code – not removed. LEADING SECURITY PROVIDER (NAME WITHELD) Detected malicious code, not removed – safe mode included.
- 5) WinXP w/l.E. 6 no anti-virus – (Conficker) code was able to execute almost entirely silently. LEADING SECURITY PROVIDER (NAME WITHELD) did not detect malicious code, not removed. LEADING SECURITY PROVIDER (NAME WITHELD) did not detect

malicious code – not removed. LEADING SECURITY PROVIDER (NAME WITHELD) detected malicious code, not removed, safe mode included....”

As Nuspire’s army of Security experts continued its analysis of Conficker while concurrently working with its customers, it also was monitoring and transmitting daily media briefings to its client list, too.

Examples Attached, highlights include:

“TrafficConverter.biz is a notorious pay-per-install affiliate programs (sic) was dismantled this week after media attention caused VISA and Mastercard to shut down the group’s payment operations. The action comes just a few days after a report by The Washington Post that showed some affiliates were making more than \$100,000 US a week installing rogue anti-virus software. The credit card industry may have been spurred by the fact that the first version of the Conficker worm told infected systems to download a file from Traffic Converter, although the story posits that this could have an attempted Joe Job rather than a blatant attempt to drum up more installs.” Source: SlashDot

And, as media heavyweights like USA Today and CBS 60 Minutes weighed in (See Attached – quotes to follow), Markus Davis communicated real-time solutions and mission-critical instructions to keep Nuspire Networks’ customers safe and secure, as outlined in this Q1 E-Mail:

“Below are images taken of a website that can OPEN ITSELF during normal web browsing. Please be aware that clicking anywhere within the first image can execute a virus....<http://protectionskim.com>”

Davis and his pro-active team were busy finding the fraudulent web addresses and identifying their symptoms while getting the information out to Nuspire’s customers in real-time....continuing:

“If a computer displays any of these images or pop-ups simply terminate the web browser by finding the item in the taskbar and right clicking to close....”

Meanwhile, Nuspire’s International Security Partners were also sharing data, tactics and information:

“This virus can and will shutdown your clients, morph, change, morph again and is set to possibly raise havoc on April 1....” INDUSTRY LEADING SECURITY PROVIDER, NAME WITHELD.

Why Nuspire Network Solutions Matter – Virus Team In Action Continued...

In the weeks prior to this story, Nuspire Networks’ customers were being protected as the ever-vigilant Virus team led by Brian Klumpp and Markus Davis continued its assault on Conficker. These excerpts from Nuspire March 2009 e-mails demonstrate Nuspire’s value:

- 1) Alert comes from normal browsing of the web – unknown amount of hijacked sites are presently at Conficker’s author disposal.
- 2) JAVA Script activates Host machine – detects operating system, browser and display settings to correctly fill the whole screen with an image of what the user would see having opened “MY COMPUTER.”
- 3) The alert uses several different Trojans which have small changes in the signature to allow a more successful pass through of the Anti-Virus application.

- 4) A web search for assistance on removing/stopping the malicious application results in more misleading sites than helpful ones that provide remediation.
- 5) This alert has the potential to turn the host computer into a bot to further the propagation of said malicious application.

Portions of this malware use the Trojan.zlob.g which writes information to Winsock, Registry and BHOs (Browser Helper Objects) and copies itself to the system restore point....instructions below for remedy....

Davis went on to provide detailed Virus elimination instructions. Nuspire's NuSecure Security package has successfully identified each and every instance of Conficker across hundreds of thousands of Access Points geographically dispersed across the Globe. Nuspire Networks is aware that Conficker is still out there – ready, silent and dormant – awaiting for its next round of instructions to gather identities, credit cards, bank information or millions of dollars, incrementally and quietly one devastating transaction at a time....

Conclusion: Business Needs Superb, Active, Vigilant Network Monitoring-Security More Than Ever

Any business entity that deals in on-line financing, ordering or mission-critical data truly needs to incorporate 24 x 7 x 365 ultra-secure solutions as a necessary provision. As 24 x 7 x 365 servers overseen by hackers and Internet pirates throughout the Globe, it only makes sense to invest in your own "Network Traffic Cop" to ensure a solution that can and will prevent Worms and Malicious software like Conficker to infest business systems while ruining an organization's reputation. No matter what security solutions are deployed nothing can match the accompaniment of full time human analytics to sense, review and act on security events.

As global, web based information systems display its collective vulnerabilities, organizations like Heartland Systems and TJ Max – and their Customers – are compromised and damaged irrevocably.

Nuspire Networks will continue to provide vigilant monitoring, around-the-clock isolation and continued protection of Mission-Critical information, assets and customer-relationships, period.

As its customers in Health Care, Broadcast, Manufacturing, Retail, Telecommunications and Global Supply Chain distribution have learned – the cost-effective value provided by Nuspire's unique team, its Network Operations Center and its desk-top monitoring and alerting solutions are second-to-none.

Please go to www.nuspirenetworks.com to learn more or call 248.896.6150 if you would like Nuspire's Security Experts to present, educate or add value to your organization.

Source Material For This Whitepaper

USA Today, CBS, Inc. Magazine, Fortune Magazine, Microsoft, Juniper, Cisco, Fortinet, McAfee, Norton, Newsweek Magazine, Time Magazine, The New York Times, Washington Post and Information Week.