# The wild world of malware: Keeping your company safe inside

Threats are continuously evolving but your firewall protection may not. Now is the time to look beyond traditional network security and incorporate protection against malware and exploits that pass through PCs and mobile devices when users browse the Internet, send or receive email and download applications.

As the number and severity of cyber crimes continues to grow, it's important to understand the various types of malware involved and how they work. This applies specially to small and medium businesses that are not likely to have IT personnel whose sole focus is network security. This paper examines the current drivers of malware development, details the characteristics of each, discusses how they manifest themselves on the network, and points to how each can be remedied.

While the names of many forms of malware might be familiar, they continue to evolve as countermeasures to eliminate them force adaptation. Today, the adaptation is driven by professional criminals. Yes, there are still amateurs out there who try to impress their friends or just act out by coding and releasing malware of various kinds. But far more dangerous are the organized, transnational criminal gangs who distribute malware for profit. These schemes include:

- Extortion - Locking up or disrupting computers, then charging money to have the disruption undone. Often, these attacks take the form of a worthless computer scan and the sale of equally worthless "antivirus" software. This technique can be used to harvest credit card information. Sometimes the purchased software is "scareware" which drives additional purchases or continues to exact "subscription" payments.
- Theft - Stealing electronic assets. These can include: personally identifiable information (identity theft) from employee or customer records; financial account information and passwords; proprietary trade and business assets which can be sold to competitors; email accounts, including address books, to be used for spam mailings (from seemingly trusted sources); and even computer resources themselves (zombies) which are controlled by the criminals for everything from spam mailing to hosting pornography.

The software which enables these crimes is categorized as malware. As worrisome as malware is, and it continues to get worse, there are straightforward and extremely effective ways to address it. But first, know your enemy. Typical malware consists of six main types: viruses, worms, Trojans, spyware, adware and rootkits.

## Viruses

Probably the best known type of malware is the virus. Computer viruses have been around for decades; however the basic premise has remained constant. Typically designed to inflict damage against the end user, computer viruses can purge an entire hard disk, rendering data useless in a matter of moments.

Just as biological viruses replicate themselves when infecting a host cell, computer viruses will often replicate and spread themselves through an infected system. Other types of viruses are used for 'seek and destroy' where specific files types or portions of the hard disk are targeted. Criminals conducting cyber thefts will often unleash a virus on penetrated systems after extracting the desired information as a means of destroying forensic evidence.

Computer viruses were originally spread through the sharing of infected floppy disks. As technology evolved so too did the distribution method. Today, viruses are commonly spread through file sharing, web downloads and email attachments. In order to infect a system, the virus must be executed on the target system; dormant computer viruses which have not been executed do not pose an immediate threat. Viruses typically do not possess any legitimate purposes and in some countries are illegal to possess.

## Worms

Computer worms have existed since the late 1980s, but were not prevalent until networking infrastructures within organizations became common. Unlike computer viruses, worms have the capability of spreading themselves through networks without any human interaction. Once infected by a worm, the compromised system will begin scanning the local network in an attempt to locate additional victims. After locating a target, the worm will exploit software vulnerabilities the in remote system, injecting it with malicious code in order to complete the compromise. Due to its means of attack, worms are only successful at infecting systems on the network which are running specific operating systems. Worms are often viewed more as a nuisance than a real threat. However, they may be used to spread other malware or inflict damage against target systems.

## Trojans

Like viruses, Trojans typically require some type of user interaction in order to infect a system. However unlike most worms and viruses, Trojans often try to remain undetected on the compromised host. Trojans are small pieces of executable code embedded into another application. Typically the infected file is an application the victim would use regularly (such as Microsoft Word or Calculator). The goal is for the victim to unknowingly execute the malicious code when launching an otherwise innocent program. This often results in Trojans infecting a system without triggering any type of notification. There are several types of Trojans, each fulfilling a different purpose. Some Trojans are designed specifically to extract sensitive data from the infected system; these types of Trojans typically install keyloggers or take screenshots of the victim's computer and automatically transmit the information back to the attacker. Other, more dangerous "remote access Trojans" (RATs), will take control of the infected system, opening up a back door for an attacker to later access. Remote access Trojans are typically used in the creation of botnets.

## Spyware / Adware

Like some types of Trojans, spyware is used to collect and relay sensitive information back to its distributor. Spyware typically is not malicious in nature. However, it is a major nuisance, typically infecting web browsers, making them nearly inoperable. Spyware is often used for deceitful marketing purposes, such as monitoring user activity without their knowledge. At times, spyware may be disguised as a legitimate application, providing the user with some benefit while secretly recording behaviour and usage patterns.

Like spyware, adware is a major nuisance for users. But it is usually not malicious in nature. Adware, as the name implies, is typically used to spread advertisements providing some type of financial benefit to the attacker.

After becoming infected by adware, the victim becomes bombarded by pop-ups, toolbars and other types of advertisements when attempting to access the Internet. Adware usually does not cause permanent damage to a computer. However, it can render the system inoperable if not removed properly.

## Rootkits

Arguably the most dangerous type of malware is the rootkit. Like remote access Trojans, rootkits provide the attacker with control over an infected system. However, unlike Trojans, rootkits are exceptionally difficult to detect or remove. Rootkits are typically installed into low level system resources (below the operating system). Because of this, rootkits often go undetected by conventional antivirus software. Once infected with a rootkit, the target system may be accessible by an attacker providing unrestricted access to the rest of the network.

## Knowing when you've got one

Malware in network traffic or on a computer makes its presence known one of three ways:

- "signature" is a fingerprint or pattern in the file that can be recognized by a network security system like a firewall even before it gets to a computer. If such a file actually gets to a computer, the antivirus/anti-malware software on the machine should catch it.
- suspect file types appearing out of context, like an executable (.exe) or registry value hidden in a compressed file like a .zip.
- Behaviour; even a rootkit may reveal itself when it "phones home" to the operator who controls it. If this behaviour is abnormal, for instance in volume or time of day, this can be an indicator of a compromised system.

The standard security measures of having anti–virus software installed and constantly updated on all machines will address the most common culprits. Their signatures give them away. Network security companies maintain "honeypots" around the world, like Dell SonicWALL's Collaborative Cross-vector GRID Network, which deliberately attract each new release of malware so its signature can be identified and distributed with routine anti-malware updates. With the signature on file, the security software can identify the malware as soon as it shows up and remediate it. More sophisticated security companies take this a step further. For example, Dell SonicWALL's GRID Network populates a cloud database with all new threat signatures immediately upon identification anywhere in the world. Dell SonicWALL security appliances backstop the tens of thousands of threat signatures stored locally with this cloud database. Scanned files are compared against this exhaustive database of malicious executables in real time for even more comprehensive protection.

Recognizing a hidden file type is slightly more difficult. Some companies have blanket rules regarding the file types that can transit the network. For example, some companies will not allow any compressed files inside their firewall. But this can be disruptive to normal traffic flows. A more sophisticated and less disruptive approach is to perform Reassembly-Free Deep Packet Inspection ® (RFDPI) on every packet of data transiting the network. This is performed by the superior brands of firewalls, like Dell SonicWALL, that literally look inside the data payload to see what is there. This process spots hidden threats and removes them from the flow.

Behaviour is the hardest indicator to recognize. If some form of malware gets through, most people are unaware of it until the performance of the infected machine becomes unacceptably slow or erratic. Next - Generation Firewalls (NGFWs) can identify suspicious behaviour even before it gets that far. By recognizing unusual network activity, like huge volumes of email being sent from an individual machine, a NGFW can help administrators isolate the malware for removal. The intelligence of such security systems can be adjusted to enforce policies for network activities just as a company would have policies for the behaviour of their employees. For example, a policy could say that instant messaging is permitted, but transmission of files by instant message is not. If there is no need for such activity, the fact that a computer is attempting such behaviour suggests that the machine is being controlled by someone other than an employee, a red flag for the presence of malware. Just as importantly, the dangerous activity would be automatically blocked.

## Never getting one in the first place

As with biological infections, the best medicine is prevention. Proper security measures provide this. Next - Generation Firewalls with the functionality described above can identify a huge majority of the malware attempting to enter a company’s network. This includes attacks that involve spam email, phishing (fake) websites, and “drive-by downloads” that inject malware during a visit to a seemingly safe website. Each of these methods of infection uses a different approach requiring different methods of identification. NGFWs can apply all these methods simultaneously from a single security appliance. A “best in class” NGFW device, like Dell SonicWALL’s, offers optional capabilities to identify threats in spam email, in hidden files, and in drive-by downloads according to their signatures or their behaviour. This last category, drive-by downloads, is especially worth noting since so many transactions are now performed online, like accessing remote information or conducting purchases. What looks like a legitimate Web 2.0 transaction can disguise malware delivery. A solid NGFW solution scans Internet traffic to spot exactly these kinds of application behaviours.

When the security solution employs RFDPI, files attempting to enter the network only need to be scanned once to address all the potential threats. This means network traffic can move more smoothly, yielding a better user experience and more productivity. This has the follow on advantage of getting the most value from a high-speed connection and possibly reducing the need for more expensive bandwidth.

The consolidated technologies in NGFWs also eliminate the need for multiple devices like firewalls and spam and content filters. Taken together, this is a powerful economic argument for a Next Generation Firewall.

## Summary

Malware continues to plague the business network landscape. But even as the criminals producing malware have become larger and more sophisticated, the technology to thwart them has grown equally sophisticated.

Now even the smallest companies can enjoy levels of protection that essentially inoculate them from many forms of malware. And these companies can do so cost effectively. By recognizing the threat contemporary malware represents, and by implementing a contemporary security solution, the wild world of malware can be left in the wild. And business can proceed safely, efficiently, and profitably.

## About Dell SonicWALL

Dell™ SonicWALL™ provides intelligent network security and data protection solutions that enable customers and partners - around the world – to dynamically secure, control, and scale their global networks. Built upon a shared network of millions of global touch points, Dell SonicWALL Dynamic Security begins by leveraging the Dell SonicWALL Global Response Intelligent Defense (GRID) Network and the Dell SonicWALL Threat Center that provide continuous communication, feedback and analysis regarding the nature and changing behaviour of threats worldwide. Dell SonicWALL Research Labs continuously processes this information, proactively delivering defences and dynamic updates that defeat the latest threats.

Leveraging its patented Reassembly-Free Deep Packet Inspection technology in combination with a high speed, multi-core parallel hardware architecture, Dell SonicWALL enables simultaneous, multi-threat scanning and analysis at wire speed and provides the technical framework that allows the entire solution to scale for deployment in high bandwidth networks. Solutions are available for the SMB through the enterprise, and are deployed in large campus environments, distributed enterprise settings, government, retail point of sale and healthcare segments, as well as through service providers.