THE CASE FOR NETWORK-BASED MALWARE DETECTION

THE NEED FOR AN ADDITIONAL LAYER OF PROTECTION

STRATEGIC WHITE PAPER

Client-based anti-malware software is important in any approach to Internet security. Unfortunately, most users do not keep their security software, applications and operating systems up to date – and with significant money to be made from fraud and identity theft, malware authors are constantly finding new ways to bypass or disable security barriers. For an 'always-on' solution that cannot be disabled and is constantly aware of the latest threats, service providers should consider a network-based approach to malware detection – one that can detect command-and-control signatures within network traffic to identify specific types of malware and reduce the incidence of false positives.

Alcatel·Lucent

TABLE OF CONTENTS

THE LIMITATIONS OF CLIENT-BASED SECURITY

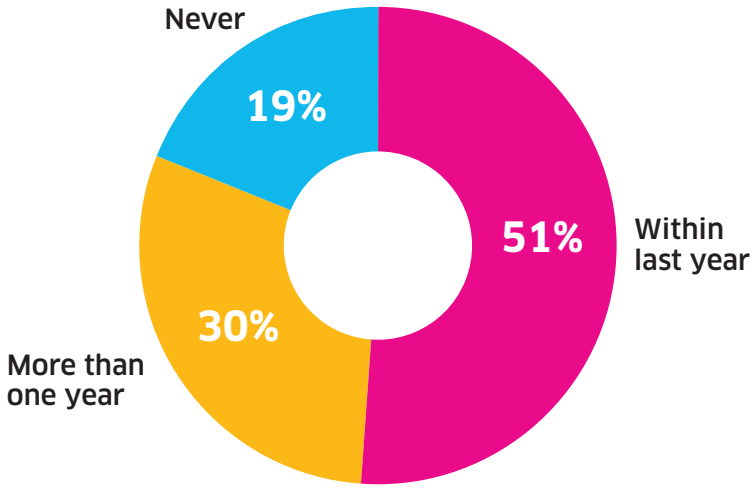
Malware has changed considerably since the 1990s. In the early days it consisted mainly of pranks designed by programmers to show off vulnerabilities they had discovered in Windows. The current generation of malware, however, focuses on fraud, identity theft and distributed denial of service (DDoS) attacks — making it a much more serious problem for service providers and their subscribers.

Despite billions of dollars invested in R&D to combat malware and the fact that upwards of 94 percent of PCs are equipped with anti-virus software, Kindsight Security Labs has found that approximately 15–20 percent of home networks consistently show signs of being infected by malware such as Trojans, botnets, spambots and keyloggers. While client-based anti-virus software is an important piece of the overall security puzzle, it simply isn't capable of addressing the growing malware problem on its own.

How Malware avoids the anti-virus barrier

In a survey conducted by Kindsight, despite the fact 83 percent of web users were running up-to-date anti-virus software, 51 percent had been infected with at least one piece of malware during the previous year.

Figure 1. Time period since last infection



Source: Kindsight Survey, 2010

How does malware slip through the barrier created by traditional, PC-based anti-virus systems? In fact it has many paths — most of which are user-created:

- **Anti-virus software is not operational:** The impact of real-time anti-virus protection on a device's battery, memory and processor can be more than the average consumer is willing to accept. As a result, many infections are contracted by users who turn off anti-virus software because they perceive it to negatively affect the performance of the games and applications they want to use.
- **Anti-virus software is not up to date:** Many web users overestimate the effectiveness of their anti-virus software, unaware that it is only as good as the latest updates provided by the security vendor. Depending on the source, only 50–80 percent of people have up-to-date anti-virus software installed on their PCs. Beyond this, it's not just security software that needs to be kept up to date — older versions of applications, plug-ins and operating systems can all be exploited by malware.

- **Software is not configured correctly:** As malware becomes more sophisticated, so does the security software designed to protect against it — making it increasingly difficult for the average user to know if the software is actually doing its job. In many cases, the differences between on-demand scans, scheduled scans, email scans, download scans and on-use scans are not made clear. As a result, users are not capable of configuring these options correctly or are unsure of the impact certain features will have on the security of their system.
- **Software is not completely effective:** Malware authors use automated tools to constantly repackage and obfuscate their malware to evade detection by anti-virus software. And with security vendors having to contend with thousands of new malware samples on a daily basis, studies have shown that client-based anti-virus software is capable of detecting only 50–75 percent of malware, leaving a potentially large proportion completely undetected. Some anti-virus software also cannot identify spyware or adware infections; in many cases, entirely different programs are required for this purpose.
- **More devices, more connections:** Both fixed and mobile service providers are now faced with a multi-directional flow of malware. For example, Internet service providers are subject to smartphone/tablet malware when these devices are connected to home WiFi routers; similarly, mobile operators are subject to malware coming from laptops tethered to smartphones or connected to mobile Internet sticks or 3G/WiFi hotspots. Devices running Google's Android operating system have become particularly vulnerable in recent months, with Kindsight Security Labs reporting a 400 percent increase in infections from early September to late November 2011.

THE ILLUSION OF PROTECTION

Although anti-virus software is installed on 94% of PCs, only

- 51% of users keep their anti-virus software up to date
- 64% have a firewall enabled
- 55% have anti-spyware software installed

Source: National Cyber Security Alliance

Even with the most up-to-date software installed and security properly enabled on their PCs, users are still not completely safe from infection. In early 2012, the Zeus Tracker site reported that the average anti-virus detection rate was only 36% for binaries of the Zeus Trojan — malware specifically designed for banking-based identity theft. Likewise, in 2011, research from SurfRight found that 32 percent of users with up-to-date software were actually infected with malware.

The new reality: Malware for profit

A paradigm shift in malware authors' primary motivation has led to the creation of malware that is increasingly difficult to detect and remove. The first generation of malware was created to spread through a network quickly, causing as much trouble as possible while garnering notoriety for the author. However, authors have since learned there is significant money to be made by gaining control of a computer — and more to be made with more computers controlled. Botnets, in particular, have been used extensively by criminal organizations for phishing, bank fraud, identity theft, extortion, spam distribution and DDoS attacks. Botnet owners have also been known to rent access to the devices under their control to other criminal organizations for substantial sums of money.

As the motivation for creating malware has shifted from notoriety to profit, there is considerable incentive for authors to ensure their malware can bypass client-based security. Rather than openly announce its presence, malware now operates in stealth mode and aggressively protects itself from removal by client-based anti-malware software. It conceals itself in the operating system using rootkit technology, disables existing anti-malware software, takes control of network access, and even protects its territory by removing competing malware.

NETWORK-BASED SECURITY: AN ADDITIONAL LAYER OF PROTECTION

Although client-based security has its strengths, given the number of factors that can reduce the effectiveness of security software installed on PCs and mobile devices, infection detection integrated directly into the service provider's network offers a much-needed additional layer of protection.

Rather than directly scanning a user's PC, smartphone or tablet for installed malware, network-based detection systems analyze fixed and mobile Internet traffic for specific malware communications. Such an approach is effective because, in order to realize its goals, malware must engage in network activity to communicate with controllers, transmit stolen information, deliver illicit network services, and spread from one device to the next. Each of these activities is easily observed at the network level — and can provide conclusive evidence of malware infection.

Network-based detection also serves to simplify the security process. In their ongoing 'arms race' with security vendors, criminals are continuously updating and repackaging their malware — but very rarely do they change their malware's difficult-to-modify communication protocols. For example, whereas client-based security software needs to keep track of hundreds or even thousands of signatures related to the variations of the Zeus Trojan, a network- based system needs only to monitor for the signatures of fewer than 10 distinct communication protocols. Network security vendors are also better equipped to handle zero-day attacks because even if the malware is considered to be 'new', it is likely to be using existing communication protocols.

Network-based security vs. client-based security

In general, network-based security systems offer the following advantages over client-based systems:

- **Cannot be disabled:** Network-based systems are not susceptible to the techniques modern malware uses to defeat and bypass client-based security measures. Because the detection system is embedded within the service provider network itself, it is practically invisible to cybercriminals — and the only way to turn it off is through the service provider's management datacenter.
- **Always-on monitoring:** Client-based anti-virus software can be deactivated at will by the end user (to improve gaming performance, for example). However, some users will inadvertently forget to turn it back on — making them vulnerable to infection. Because a network-based system cannot be shut off by the user, it is always on and always doing its job.
- **Always-current detection:** Because service providers maintain the equipment, it is easier to ensure the network-based security system remains up to date and aware of the latest threats.

It should be noted that network-based security is not intended to replace client-based services such as anti-virus software and firewalls, but rather to significantly enhance their effectiveness by providing immediate notification when something slips through. Increasingly, service providers are coming to the conclusion that security is not an 'either/or' proposition; both client-based and network-based solutions are important layers of an overall security strategy. The ideal case for consumers and service providers alike would be an interworking of solutions — for example, where network-based detection alerts the subscriber to use a device-based app or online scanner to remove the malware.

SIGNATURE-BASED DETECTION

One specific technique that can be leveraged for a network-based security system is signature-based detection, which analyzes Internet traffic to look for a specific traffic pattern — the signature — known to be associated with malware command-and-control (C&C) activity. If a computer is seen to be communicating with a traffic pattern that matches a known signature, it can be determined with great certainty that the user is infected with the specific bot that uses that C&C protocol.

Creating and maintaining a robust signature set is critical to ensuring a network- based system's effectiveness in detecting malware infections in consumer devices. Signatures are developed by capturing samples of malware in a lab or via a 'honeypot' (for more information, see the section on alternative detection methods later in this report), and then observing the C&C protocol activity exhibited by the malware. Activities such as specific messages/payload, unusual use of ports, etc., can then be associated with a particular infection, allowing that piece of malware to be incontrovertibly identified within the network.

Typically, a detected malware signature triggers an alert in the network when the characteristic traffic pattern is observed. But before notifying users that their computers are infected and leading them through the remediation process, service providers must be extremely confident the devices are actually infected — and that they know for sure which type of malware is infecting each user's system.

That's why each signature is tested, both in a lab and in a live network deployment, to ensure it identifies an infection without generating false positives — if the signature definition is too broad or imprecise, it may trigger on legitimate network activity instead of just the malware. Minimizing false positives is extremely important; if users are provided with too many alerts and asked to perform remediation on non-existent threats, they will eventually become immune to the entire process and refuse to act should their systems actually become infected. Through field trials and deployments completed over the past couple years, Kindsight has reached the following conclusions about signature-based detection:

- It is one of the most effective techniques to detect malware C&C traffic coming from a service provider's customers.
- With the correct signature set, malware can be detected with far greater accuracy than competing techniques, providing indisputable evidence that a customer is infected.
- The notification and remediation process is much more effective when the malware has been positively identified and the remediation can be customized for specific malware.

EVIDENCE OF A MALWARE

Signature-based detection techniques look for unequivocal evidence that a user's computer is infected and being exploited by an attacker. This evidence includes:

- Malware C&C communications
- Backdoor connections
- Attempts to infect others
- Hijacked browsers and spyware infections
- Excessive email
- DDoS and hacking activity

ALTERNATIVE DETECTION METHODS

Service providers can also use other malware-detection techniques in their network-based systems, some of which can be combined with signature-based techniques to improve their effectiveness.

Honeypots

Honeypot computers and networks are intentionally configured to attract infection. Based on the premise that malware scanning the network will find these vulnerable systems and attack them, honeypots provide very strong evidence that the attacker is infected or operated by a hacker. Unfortunately, honeypots are only effective at detecting malware that spreads through network vulnerabilities — a relatively small percentage of the malware ecosystem.

Blacklists

Much of the research in botnet detection is devoted to finding C&C sites. A common technique is to capture a sample of the bot in a honeypot; when it inevitably tries to connect to its C&C server, that IP address or domain name can be added to one of the many available blacklists. While common sense would dictate that a user connecting to a blacklisted IP address or domain is part of a botnet, this is not always the case:

- Some botnet C&C sites are actually located on servers that also host legitimate services; this is particularly true of botnets that use web or IRC protocols for command and control.
- Some are hosted on legitimate sites that have been compromised and subsequently fixed, but have not yet been removed from the blacklist.
- Some use 'fast-flux' DNS rallying techniques to vary the C&C IP address faster than the blacklists can keep up.

Because of these issues, blacklists provide too many false positives and are not always accurate. However, accuracy can be improved when combined with other detection techniques (including signature-based detection).

Sinkholing

Through the use of DNS sinkholing techniques, traffic intended for known botnet C&C locations can be redirected to a sinkhole server operated by the service provider; accordingly, anyone who visits the sinkhole server is likely to be infected. The main advantage over a simple blacklist is that the sinkhole server can verify the visitor is using the botnet's C&C protocol. This methodology provides accurate detection and can identify specific malware; the downside is that it can be quite labor-intensive and costly to maintain.

DNS

Several techniques involve the analysis of DNS traffic to detect botnet activity, the simplest of which is to observe the domain names used by malware to contact C&C servers to create a blacklist of infected computers or servers. Another technique is to look for characteristic patterns in the DNS traffic that indicate malware infection. This method can be very effective against specific bots that use a variety of fast-flux DNS techniques for rallying, but is not generally applicable against most types of malware. In addition, DNS-based systems will miss malware that bypasses the service provider's DNS (as seen by the recent DNSChanger attack). They also do not detect infections among subscribers who use third-party DNS services (such as Google DNS) instead of the service provider's DNS.

Scanning

Although scanning for vulnerable systems could be useful in botnet detection, it does not provide any level of confidence that a user is actually infected. In addition, there are significant legal and technical issues associated with scanning a user's home computer.

Netflow

The increased network activity associated with DDoS attacks and the propagation of spam can be easily identified in the network and attributed to botnet activity. However, while network flow ('netflow') statistics can be useful for identifying that an incident is occurring, they do not usually provide the information required to determine which malware is actually responsible. As such, this technique does not meet the criteria for low false positives and the positive identification of malware.

Behavioral Profiling

Whereas signature-based detection tracks what malware 'says', behavior-based approaches look at what malware actually does, monitoring the actions of a program to determine whether it is malicious or not. Using this approach, profiles are created that outline normal program behavior; any deviations from that profile (for example, scanning the network for computers with open ports that are vulnerable to exploits, suddenly sending huge quantities of email, etc.) are flagged as suspicious. Unfortunately, program behavior can be very complicated, making profile construction particularly challenging. If the profile of normal behavior for a program is too narrow in its definition, behavior-based detection systems are capable generating a large number of false positives.

In general, behavioural profiling is ideal for uncovering larger, more generic security issues; signature-based detection, on the other hand, is better at detecting very specific security issues and types of malware. For optimal malware detection, service providers should utilize a combination of the two approaches.

THE BUSINESS CASE FOR NETWORK-BASED DETECTION

By leveraging their role in the network, service providers are ideally positioned to offer network-based security to their subscribers. Not only can the service be delivered without having subscribers install an additional device in their home networks, it can also be offered at an attractive price point that appeals to subscribers.

For service providers, deploying a network-based security platform that uses signature-based malware-detection techniques provides four key benefits:

- Reduced risk: Protecting subscribers by identifying the specific types of malware infecting the subscriber base and supporting the development of policies to address each type.
- Resource conservation: Eliminating the consumption of network resources due to malware infection.
- Reduced churn: By taking actions to detect and block malware, service experience is improved — resulting in more satisfied and loyal subscribers.
- Greater returns: Creating opportunities for revenue generation through the provision of network-based security offerings as a value-added service.

Network-based security as a value-added service

Many technologies and processes can be used to protect the network and subscribers from malware — all of which come at a cost to the service provider. This means there are some business decisions to be made vis-a-vis the cost- benefit analysis of managing the risk/impact of malware and the extent to which subscribers should fund malware detection, notification and remediation.

Market research and evidence from Kindsight deployments find that consumers value the additional layer of protection service providers can offer via network-based malware detection — and are willing to pay a few dollars each month for it.

By making network-based malware security a fee-based service, it becomes a more complex solution for service providers to implement and maintain (for example, due to the processes required to enable subscribers to order the service, or the coordination of billing for the service). However, the elimination of the impact of malware on the network through this additional layer of protection has significant value for the subscriber — and leveraging this opportunity makes perfect business sense for service providers.

In addition to implementing network-based security as a fee-based service, service providers can also utilize creative financing mechanisms to generate revenue while providing value to their subscribers — for example, by offering the service to subscribers at no cost if they opt in to relevant advertising.

Some operators consider security to be a substantial differentiator over their competitors, choosing to forego the opportunity to generate fee-based revenue or ad monetization in exchange for market differentiation and leadership.

Whether delivered on a paid, no-cost, or used to upsell other services (e.g., premium technical support for a one- time virus/malware cleaning fee or as a monthly subscriptions), effective remediation service should include some of the following elements:

- Portals that give self-service, step-by-step instructions on removing the malware
- Easy-to-use tools known to be effective in removing specific malware infections
- Options for telephone/email/chat support with technicians who can either walk the subscriber through remediation steps or remotely log into the subscriber's device to perform the remediation

A BETTER APPROACH TO MALWARE DETECTION

An 'always-on', 'always up-to-date' solution that cannot be disabled (either by malware or the user), network-based malware detection gives subscribers additional protection that complements and strengthens traditional, device-based security software. Using techniques such as signature-based detection, a network-based approach zeros in on malware communication patterns to identify specific infections and reduce false positives.

Kindsight offers a security and analytics platform to help service providers implement network-based detection capabilities to better protect their network and subscribers — with Security Analytics providing a signature-based, offline platform to measure malware-infection statistics across both fixed and mobile networks, and Security Services notifying users when their home networks or mobile devices have been attacked.

REFINING THE SIGNATURE SET

Deployments conducted with major service providers in North America and Europe have allowed Kindsight to test specific classes of signatures and execute a detailed false-positive analysis based on real-world network traffic. Through these deployments, Kindsight has been able to follow the progress of notable malware such as Conficker, Koobface, Zeus, Torpig, Palevo/Mariposa and Lethic, allowing the company to verify the effectiveness of its signature set while further refining it as the malware evolves.

At any given time, Kindsight's signature set tracks between 2,000 and 2,500 signatures for a wide range of malware – and this set is updated weekly to reflect newly discovered malware.

ABOUT KINDSIGHT SECURITY LABS

Kindsight Security Labs focuses on the behavior of malware communications to develop network signatures that specifically and positively detect current threats. This approach enables the detection of malware in the service provider network and the signatures developed form the foundation of Kindsight Security Analytics, Kindsight Broadband Security and Kindsight Mobile Security solutions.

To accurately detect that a user is infected, our signature set looks for network behavior that provides unequivocal evidence of infection coming from the user's computer. This includes:

- Malware command and control (C&C) communications
- Backdoor connections
- Attempts to infect others (e.g. exploits)
- Excessive e-mail
- Denial of Service (DoS) and hacking activity

There are four main activities that support our signature development and verification process.

1. Monitor information sources from major security vendors and maintain a database of currently active threats.
2. Collect malware samples (>20,000/day), classify and correlate them against the threat database.
3. Execute samples matching the top threats in a sandbox environment and compare against our current signature set.
4. Conduct a detailed analysis of the malware's behavior and build new signatures if a sample fails to trigger a signature

As an active member of the security community, Kindsight Security Labs also shares this research by publishing a list of actual threats detected and the top emerging threats on the Internet and this report.

Kindsight is a network-based security product line within Alcatel-Lucent's Platform Business. The Kindsight portfolio enables Internet service providers and mobile network operators to detect threats, send alerts, block infected devices and protect subscribers. It also analyzes Internet traffic for malware and pinpoints infected devices to identify risks and take action. To generate revenue and increase brand loyalty, Kindsight also enables communication providers to launch differentiated, value-added services that combine network-based and device-based security for complete protection.

Kindsight™

Alcatel·Lucent