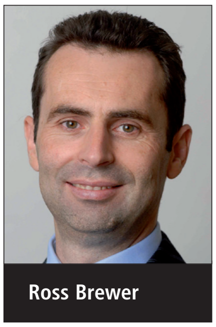
Advanced persistent threats: minimising the damage



Ross Brewer

Ross Brewer, LogRhythm

According to the Office of Cyber Security and Information Assurance, 93% of large corporations and 87% of small businesses reported some form of cyber breach in 2013.[1] Furthermore, a recent Ponemon Institute study found that, in 2013, the average annual cost of cybercrime globally was $7.22m per organisation, representing a 30% increase on the previous year's study.[2] As we move forward with more objects becoming Internet enabled and more services moving online, the cybercrime problem is only likely to worsen. In fact, analyst firm Gartner recently stated that it is becoming impossible to prevent targeted attacks and organisations should instead focus their security spending on monitoring and response techniques. With this in mind, analysts have predicted that, by 2020, 60% of security budgets will be spent on rapid detection and response approaches, up from less than 10% in 2013.[3]

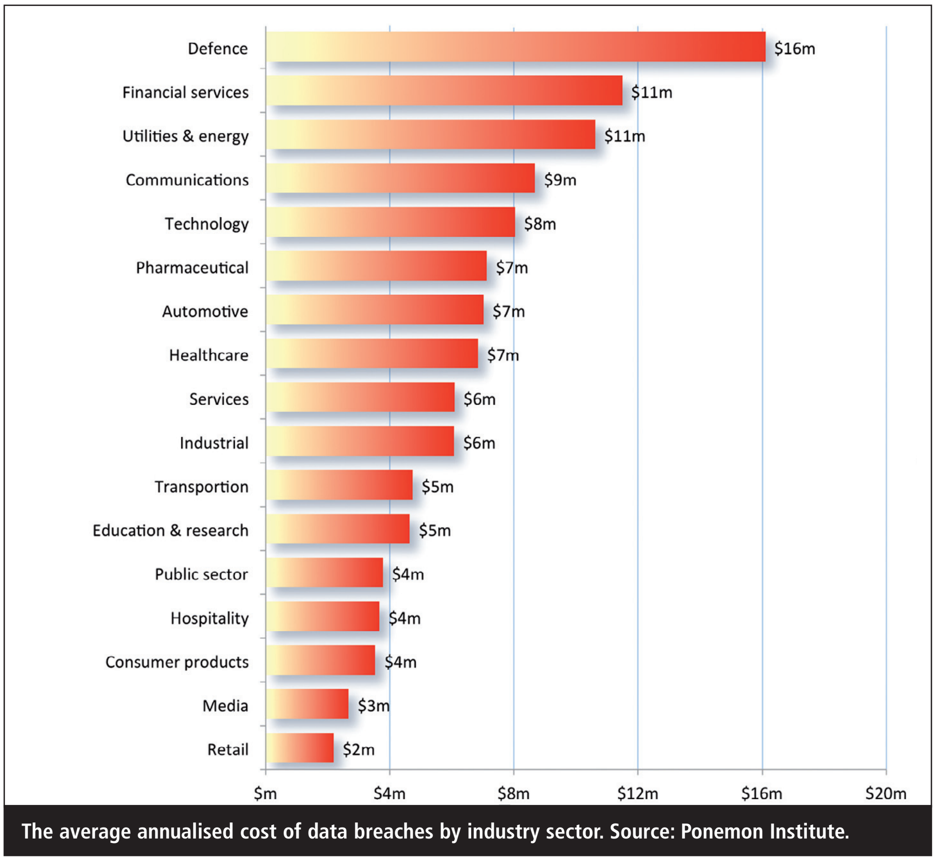
Security professionals are therefore facing an uphill battle in defending their networks as attacks become increasingly sophisticated, particularly when it comes to Advanced Persistent Threats (APTs). APTs present a challenge due to their unique and complex nature. Designed to subvert IT security measures, they frequently combine malware with well-planned physical theft and clever social engineering techniques in order to harness the full spectrum of logical, physical and social attack vectors. Given there is no single attack vector used by APTs and no single activity pattern, there is no easy way for an organisation to protect itself from an APT. A defence-in-depth strategy across logical, physical, and social boundaries is fundamental.

Defining an APT?

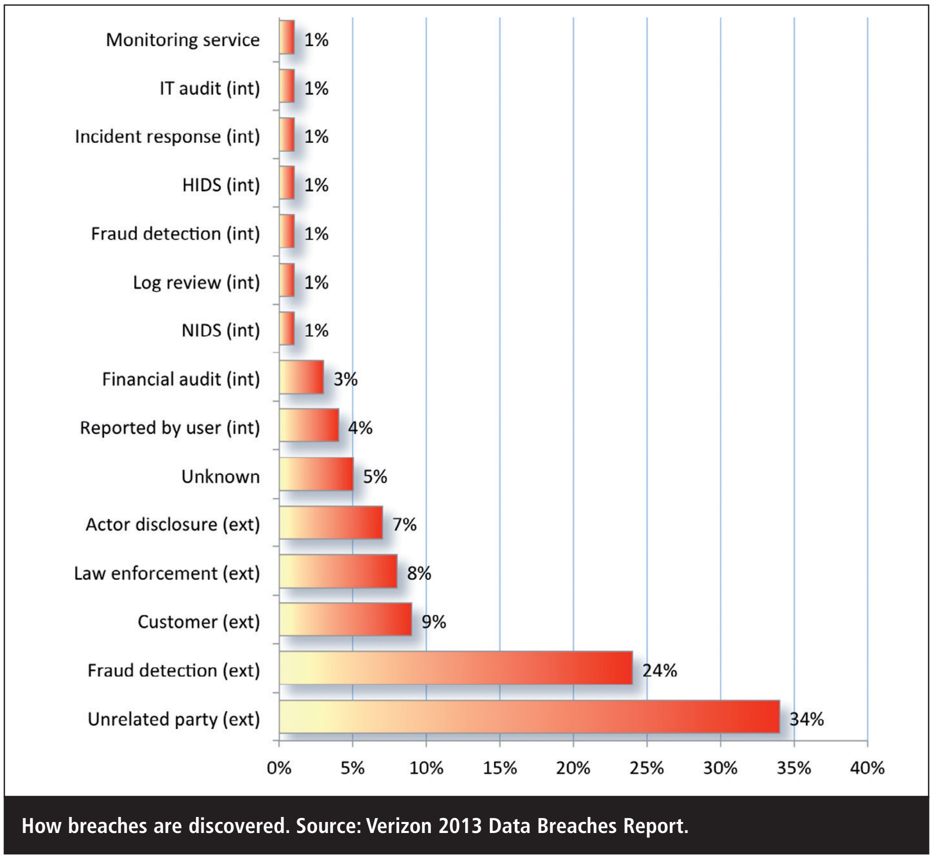
There is some argument over how an APT can be precisely defined. While APTs differentiate themselves from other forms of attack as they target a specific organisation, with a very precise goal (often to extract or destroy highly valuable data), the fact that they utilise more traditional techniques causes some to conclude that it is not the means that defines them, but the perpetrator.

There is yet to be an official definition of an APT, however the National Institute of Standards and Technology (NIST) describes the threat as: "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (eg, cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organisations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, programme, or organisation; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives."[4]

While this definition goes some way to explaining what an APT is, the basic overview provides little assistance for those looking to defend against these



The average annualised cost of data breaches by industry sector. Source: Ponemon Institute.



How breaches are discovered. Source: Verizon 2013 Data Breaches Report.

kinds of attacks. In order to be able to do so, organisations need a truer understanding of exactly how an APT works and each phase of its lifecycle.

"With the target so well defined, an APT will continue attempting to reach its goal until it is successful – no matter how long it takes"

The APT lifecycle

APTs are 'advanced' as the attacker usually writes custom, zero-day malware and exploits, designed to target a specific organisation. They will also frequently launch advanced social engineering and phishing attacks in an attempt to exploit users' systems. The 'persistent' element is explained by the fact that these attacks are extremely patient and methodical in their approach.

With the target so well defined, an APT will continue attempting to reach its goal until it is successful – no matter how long it takes. Verizon's 2013 Data Breach Report revealed that 66% of attacks in 2012 lay dormant for months before discovery and the vast majority of breaches (70%) were discovered by external parties, who then informed the victim.[5] APTs are particularly renowned for lying dormant like this for months and waiting for the opportunity to strike, such as the Stuxnet worm that was deployed to attack Iranian nuclear facilities and went undetected for almost two years.

It is therefore evident that the traditional security tools organisations have long relied on to protect their networks – anti-virus, Intrusion Preventions Systems (IPSs), firewalls and so on – cannot keep up with the rapid escalation of these sophisticated threats. While these solutions still provide businesses with a level of protection in today's fast-changing world, they must be used in conjunction with systems that provide security intelligence. With this increased level of defence, an attack can be identified and remediated far earlier, particularly when the vast majority of APTs involve the use of zero-day malware – which point security tools often miss.

However, before any attempt at stopping an APT can be made, it is essential that an organisation can determine where in the 'lifecycle' it resides. While no two APTs are the same, most follow a common pattern, and understanding the specific phases can help organisations protect themselves. Typically, there are five separate stages.

The reconnaissance phase

To begin the process of deploying an APT, the attacker needs to find a point of entry into the system and, while much of the reconnaissance done against the APT's target is passive in nature, eventually the actual infrastructure needs to be touched. Unfortunately, the weakest link in many organisations is its people and at this stage the attackers will be researching targets within the organisation, as well as scanning the network in an attempt to identify possible points of entry.

The compromise phase

Once the attackers have completed reconnaissance and decided upon their entry point and method, they now need to gain access into the network perimeter. While there are a number of ways this can be achieved, the most common method is through the delivery of custom malware via a spear-phishing campaign – usually targeting a zero-day vulnerability for exploitation.

"The perpetrators are usually sophisticated enough to ensure that their emails appear legitimate and the custom-written malware ensures that traditional, signature based defences will be by-passed"

Social engineering techniques, such as phishing, can often be scoffed at given their frequent lack of sophistication, leading many to believe that either their spam filters will identify suspicious content or people are unlikely to fall for tactic. However, when in the context of an APT, the perpetrators are usually sophisticated enough to ensure that their emails appear legitimate and the custom-written malware ensures that traditional, signature based defences will be by-passed. Add to this the fact that the use of zero-day malware will ensure that the target can be compromised, irrespective of patch level, and the compromise has a very real chance of success.

When the target user opens the malicious attachment, or follows a malicious hyperlink, the exploit is then launched. Due to the nature of writing exploits, there are often size limitations around the amount of code that can be injected at one time and, because of this, the malware will generally communicate with a command and control (C&C) infrastructure to download and install the rest of the payload, immediately after a process is exploited.

Maintaining access

It goes without saying that once the host has been compromised, for the attack to be successful, the APT has to maintain access to the systems. The most common way to do this is by stealing valid access credentials and, in fact, Verizon discovered that in 2012, 76% of breaches involved the use of weak or stolen user credentials. Once access has been gained this way, the APT will usually install a Remote Access Trojan (RAT) on a number of hosts within the infrastructure. By extending the footprint past the initial compromised host, the APT can maintain access even if one or more of the original breaches are detected.

However, the process of staying within the infrastructure often takes an even more sophisticated route. Often, RATs will install themselves as a service on the compromised host which allows constant access to the target – particularly out-of-hours when hackers believe their activity is less likely to be detected. From there, the RAT may be instructed to download more modules, disguising its packages, installing and configuring elsewhere on the system. The original threat can then either remove itself, or cover its tracks – leaving the newly installed modules in place. This, effectively, provides the APT with uninterrupted 'backdoor' access and allows the attacker to enter and exit the system as and when required over any length of time.

The lateral movement phase

Once it is in and is able to move around the system as it chooses, the APT then tries to identify where the target data resides. At this stage, malware becomes unnecessary as the attacker is in possession of various user credentials. By using these compromised credentials, it is less likely the APT's movements will be detected if they are being carried out by a 'valid' user.

During the reconnaissance stage, the attacker will generally have monitored users' behaviour in an attempt to try and mimic 'normal' activity at this stage, as there is clearly a risk that the stolen credentials will be identified and access blocked. However it should be noted that, while the path the APT takes will attempt not to deviate too heavily from a user's behaviour, it is incredibly difficult to precisely match it. While the use of RATs may, in some cases, make the APT more difficult to detect, without the ability to precisely mimic an insider's actions they are also left with vulnerabilities.

> ***"While the path the APT takes will attempt not to deviate too heavily from a user's behaviour, it is incredibly difficult to precisely match it"***

The data exfiltration phase

This final phase of an APT is when the attackers realise their goal and begin to identify, gather and move the target data outside of the network. Various forms of data are often gathered and combined into a single host to move it all in one go, which usually involves aggregating the data into an encrypted set of RAR files. This approach allows the attacker to store several files in a compressed form in the data container and ensures any data loss prevention tools cannot inspect the information as it passes through the perimeter.

It must be noted that the exfiltration method and point of exit is unlikely to be in the same area of the architecture as the entry point of the initial compromise. Consider also that the exit strategy may not be completed online, but may in fact involve a physical human extracting the data, whereby they collect the payload from a known, hidden location. This becomes a 'dead letter box' where the data may reside legitimately. The RAR file may be placed into an online data host, FTP or external facing server where files and data frequently traverse. Or, in other circumstances, the payload may be packaged into an RAR, but using stenography to rename it so the file appears as an image. If, for example, a .jpg file was placed on a web server, the web browser could quite legitimately call it an image and it will appear as conventional web traffic or activity.

Identifying an APT

The complex nature and attack path of APTs means that, traditionally, it took months, or in some cases years, for victims of the attacks to realise they were impacted. Given this, it is likely that are still many organisations where an APT is currently active and they are simply not aware.

The unfortunate fact is that traditional security tools will never offer the protection required to identify and block an APT. However, there is a way to ensure that the network stands more of a chance. Throughout the journey of an APT it will leave behind a trail of log data and, as it does, this data provides context along with cross-phase correlation and corroboration to determine what is taking place, how and when. For each of the aforementioned phases, different evidence can be gathered to help determine if an APT is within the system. The clues are in the digital finger prints left behind

Reconnaissance: the log and audit trails

It is possible to identify any potential reconnaissance taking place. If, for example, a port scan is run against a public IP address, the firewall should log a 'deny' for each event. If multiple denies are seen against unique destination ports from the same origin host within a small window of time, it is safe to assume that some sort of port scanning activity is taking place. An active defence approach can be taken here, by identifying the origin of the IP addresses performing the reconnaissance

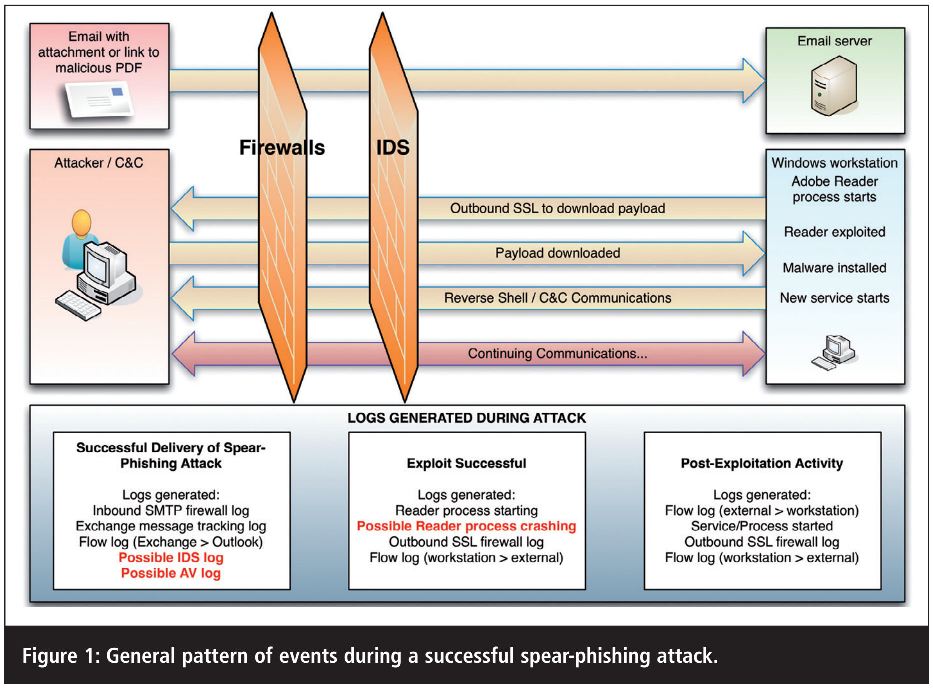

Email with attachment or link to malicious PDF
Email server
Attacker / C&C
Firewalls
IDS
Windows workstation
Adobe Reader process starts
Reader exploited
Malware installed
New service starts
Outbound SSL to download payload
Payload downloaded
Reverse Shell / C&C Communications
Continuing Communications...
LOGS GENERATED DURING ATTACK
Successful Delivery of Spear-Phishing Attack
Logs generated:
Inbound SMTP firewall log
Exchange message tracking log
Flow log (Exchange > Outlook)
Possible IDS log
Possible AV log
Exploit Successful
Logs generated:
Reader process starting
Possible Reader process crashing
Outbound SSL firewall log
Flow log (workstation > external)
Post-Exploitation Activity
Logs generated:
Flow log (external > workstation)
Service/Process started
Outbound SSL firewall log
Flow log (workstation > external)

Figure 1: General pattern of events during a successful spear-phishing attack.

activity and automatically adding them to a 'suspicious IP' watch list. It is imperative here that both the suspicious activity identified and the 'watch list' are recorded in a centralised tool with analytics capabilities in order to ensure correlative analysis can be run at later phases.

However, internal reconnaissance activities can often look similar to those being carried out by an APT at the perimeter. For example, if SQL server instances are being calculated, the IP range might be probed for port 1433 or, if network shares are being searched, ports 135-139 may be probed. In order to ensure that security teams are not chasing false positives, it is essential to ensure real-time analytics is taking place, with rules defined to detect any internal reconnaissance activity.

Compromise: the log and audit trails

Spear-phishing campaigns often leave behind logs that can, when correlated with other activity, alert systems administrators to the suspicious behaviour – as depicted in Figure 1.

Furthermore, it is often the case that part of the malware application or its code will have been embedded using stenography. Through this technique, the malware is hidden within a .jpg or other file, making it even more difficult to detect. Once it has been allowed into the network, the malware will then slowly build itself up, running the code as the C&C demands. Although the logistics of the payload delivery can vary, data is still traversing the network, and behavioural anomaly detection techniques can be used to identify whether or not the traffic is abnormal.

Maintaining access: the log and audit trails

At the stage where a RAT is installed, several approaches can be taken to detect it. In order to make its way through the firewall and hide the traffic, the RAT will initiate outbound TCP connections – more often than not encrypted with a SSL/TLS over port 443, which ensures they appear as normal web traffic. However, if a suspicious watchlist has already been generated during identification of the reconnaissance phase, it will alert to the fact an internal host is communicating with an external IP address on that list.

By using behavioural analytics to examine a user's web browsing activity against a behavioural whitelist, the RAT's communications can be identified as abnormal to that user's normal activity. In order to ensure that this happens, web browsing should be tracked based on the unique websites usually visited and the volume of normal online activity on a per host as well as per user basis. If changes occur within both of these parameters within a short period of time, an investigation should be instigated.

Lateral movement: the log and audit trails

While it can be difficult to detect compromised credentials – particularly when they are being carefully used – there are a number of ways they might be exposed. Often the stolen details will be used to simply gain access through a Virtual Private Network (VPN) and real-time analytics tools can raise an alert if one VPN is being used from two separate geographical locations within a timeframe that is unrealistic.

> ***"In order to identify the suspicious activity, network behavioural anomaly detection is required. This method will allow baselines of 'normal' activity to be built-up, and anything that deviates from this baseline examined"***

Multi-dimensional behavioural analytics can also be used to identify if credentials have been used anomalously. There are a number of dimensions of a user's 'normal' behaviour that can be tracked, such as the processes normally run, hosts normally authenticated to, areas of the system normally accessed and so on. If there is a variation in any of these activities, then it may be an indication that access credentials have been compromised and an investigation can ensue.

Data exfiltration: the log and audit trails

Once the APT has reached the exfiltration stage it is almost impossible to detect without advanced analytics as, in order to identify the suspicious activity, network behavioural anomaly detection is required. This method will allow baselines of 'normal' activity to be built-up, and anything that deviates from this baseline examined. For example, if a workstation is not normally used for anything other than sending emails and browsing the web, but suddenly begins sending data outbound to a single server fairly frequently, it is possible to assume that nefarious activity is taking place.

A whitelist of normal behaviour can be built-up over a long period of time, which will assist in identifying the 'low and slow' exfiltration attempts.

Identifying a payload that has been concealed using stenography can seem difficult, but when logic and context are applied, it becomes relatively easy. Within log files, the hidden data would be an image call: however this would be out of context unless the image was created within a crafted HTML web page. When it has a pixel size of 0x0 it would not appear on the page but could still be browsed for, downloaded and finally, delivered to the APT attacker. Simply, it is unlikely a .jpg image would be referenced without being delivered by an HTML page in a browser session and the chances are, therefore, that it is part of a payload.

Conclusion

While APTs are designed to be highly elusive, with the right mechanisms in place they can be identified and removed. However, in order to do so, advanced security intelligence that combines 360-degree visibility into all network activity and an analytics driven defence is required.

It is imperative to have an in-depth understanding of 'normal' activity on the network, along with the ability to understand events in relation to each other. By analysing richer sets of data, and applying context, it is not only more likely that irregular activity will be flagged immediately, but it will also reduce the number of false positives. Through this level of pervasive visibility it is possible to spot anomalous activity – such as suspicious data transfers or excess network usage – and stop an APT in its tracks. Given that very few organisations can say with full confidence that they have not been compromised by an APT now, or at any other point, it is imperative that the correct tools and systems are put in place now so the potential damage of a successful attack is minimised.

About the author

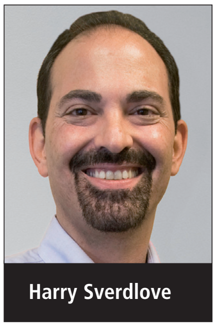
Ross Brewer is vice president and managing director for international markets at LogRhythm, a position he has held since 2008. Brewer has more than two decades' experience within sales and management, with more than 10 years spent in the information security sector where he has had a successful track record of building and managing international operations. Prior to joining LogRhythm, Brewer was vice president and managing director for EMEA at LogLogic.

References

1. 'Keeping the UK safe in cyber space'. Gov.uk, 23 Jan 2014. Accessed Feb 2014. https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace.
2. '2013 Cost of Cybercrime Study: Global Report'. Ponemon Institute, Oct 2013. Accessed Feb 2014. www.hpenterprisesecurity.com/collateral/report/Ponemon2013CyberCrimeReport_Global_1013.pdf
3. 'Prevention Is Futile in 2020: Protect information Via Pervasive Monitoring and Collective Intelligence'. Gartner, May 2013.
4. 'Managing Information Security Risk: Organisation, Mission, and Information System View. National Institute of Standards and Technology, Mar 2011. Accessed Feb 2014. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.
5. '2013 Data Breach Investigations Report'. Verizon, Apr 2013. Accessed Feb 2014. www.verizonenterprise.com/DBIR/2013/.

The Java vulnerability landscape

Harry Sverdlove, Bit9



Harry Sverdlove

Java has been a trending security concern for several years. Recently, however, there has been a significant rise in Java-related vulnerabilities and attacks.

According to Kaspersky Lab, in 2012 Java surpassed Adobe Reader as the most exploited endpoint software in real-world attacks. Specifically, the 2012 annual Kaspersky Security Bulletin noted that: "Throughout the year Kaspersky Lab's experts registered both large-scale and targeted attacks utilising vulnerable software, with Oracle Java being the most frequently targeted (50% of attacks). Adobe Reader ranked second (28%) and Adobe Flash player occupies the fourth place with only 2% share, thanks to efficient automatic updating system that promptly closes security holes."

In August 2013, F-Secure anti-malware analyst Timo Hirvonen reported finding an in-the-wild exploit actively targeting an unpatched vulnerability in Java 6. According to vulnerability information provider Secunia, the bug could be "exploited by malicious local users to disclose certain sensitive information, manipulate certain data, and gain escalated privileges and by malicious people to conduct spoofing attacks, disclose certain sensitive information, manipulate certain data, cause a DoS (denial of service), bypass certain security restrictions, and compromise a vulnerable system." No doubt, Java has become a primary gateway for hackers to enter today's businesses.