

 CounterStorm™  
Targeted Attack  
Technical Brief

CounterStorm, Inc.  
15 West 26<sup>th</sup> Street, 7<sup>th</sup> Floor  
New York, NY 10010

212-206-1900  
[info@counterstorm.com](mailto:info@counterstorm.com)  
[www.counterstorm.com](http://www.counterstorm.com)

## Executive Summary

Targeted attacks are real. Gartner estimates that although fewer than 10 percent of all current attacks are targeted against a particular company, the financial impact of a single successful targeted attack will be 50 to 100 times greater than that of a successful mass attack worm or virus.<sup>i</sup> Forrester also stated that with increasing organized crime involvement we will see more targeted attacks.<sup>ii</sup>

Targeted attacks are an enormous threat to an organization's security and its operation. Depending on who the victim is, targeted attacks can affect critical infrastructure and have the potential of putting the general public at risk. Because of their sophistication and surgically precise impact area, targeted attacks are almost impossible to detect by traditional security products. Because targeted attacks have very specific victims, when a company suffers a targeted attack, it is all alone. Few know about the attack, and the company itself may not detect it until after the damage is done.

Most successful targeted attacks in recent years have often involved a combination social engineering, breakdown in processes, technical vulnerabilities, and insider abuse. To properly mitigate targeted attacks, companies must not rely on security devices that simply look for a predefined set of conditions, like matching attack signatures or comparing network activity to known vulnerabilities. Organizations need to deploy security devices inside the network interior that can accurately detect and shut down attacks in seconds without relying on signatures. The device must be able to adjust to future threats including slow and stealthy attacks. Because targeted attacks can affect different areas of the network, the security devices must also offer a variety of response options which include stopping attacks automatically to initiating an emergency response for a specific condition. Furthermore, this device needs to provide the security administrator with extreme visibility into the network.

## Attack Classes

There are two broad classes of attacks: mass attacks and targeted attacks. Mass attacks, such as viruses and worms, have traditionally been the most common attacks. Targeted attacks are attacks that are launched against specific industries or companies.

Targeted attacks are very different from opportunistic or mass attacks. The most obvious difference between a targeted and a mass attack is that a mass attack has no specific victim in mind, but rather attacks whomever and wherever it can. Examples of mass attacks include worms like Slammer and Blaster, which used pseudo-random number generators to choose IP addresses to attack.

Targeted attacks, on the other hand, have very specific victims. The UK Ministry of Defense, the Recording Industry Association of America (RIAA), eGold,<sup>iii</sup> and the US Defense Department have all recently fallen prey to targeted attacks. When hit by MyDoom.F, the RIAA website suffered several days of intermittent outages before being forced offline for a period of more than 24 hours.<sup>iv</sup> The financial loss of RIAA was huge—and so was the damage to its reputation. In another case, the UK's National Infrastructure Security Coordination Center (NISCC) reported a sophisticated targeted Trojan attack on the UK Ministry of Defense and other government

---

<sup>i</sup> John Pescatore, "Management Update: Prevent Targeted Attacks," ID Number:G00130609

<sup>ii</sup> Paul Stamp, Jonathan Penn, Merv Adrian, and Benjamin Gray, "Increasing Organized Crime Involvement Means More Targeted Attacks"

<sup>iii</sup> E-Gold targeted by worm. Source: <http://www.financialcryptography.com/mt/archives/000060.html>

<sup>iv</sup> MyDoom.F drives RIAA web site offline. Source: <http://thewhir.com/marketwatch/myd022704.cfm>

agencies.<sup>v</sup> Attacks on computer networks at the Defense Department and other U.S. agencies are currently being launched through Internet sites in China. These targeted attacks against Defense Department and other U.S. agencies began two to three years ago and have been code-named Titan Rain by U.S. investigators.<sup>vi</sup> Thus far, hundreds of unclassified networks have been successfully breached.

Motivation is another differentiating factor between targeted and mass attacks. Mass attacks are often launched for no other reason than to gain bragging rights in the hacker community. Targeted attacks, however, can be politically or financially motivated, and are generally launched by more knowledgeable and sophisticated attackers. Because their intent is to delete, steal or hijack critical information assets, they cause far more extensive damage to the enterprises that they have targeted.

## External vs. Internal Targeted Attacks

Targeted attacks are launched through two broad methods: external attacks and internal attacks.

- External attacks, where an attack is launched from outside the network of an organization. Vulnerability exploitation is the most common form of external attacks. Vulnerability exploitation takes advantage of software flaws or configuration errors to bypass access controls and existing security tools.
- Internal attacks where the attack is launched from within the trusted network of the organization. One of the common forms of internal attacks is malware insertion, where a malicious executable is installed on internal systems and is used to collect information and forward it to an external attacker.

Perpetrators of mass attacks “cast a wide net” in an attempt to infect as many networks as possible. This makes it relatively simple for security vendors to develop countermeasures, such as scanning the network for common attack signatures or developing security patches to address known vulnerabilities. But targeted attacks are often based on insider information, and their level of customization makes them almost impossible to detect through traditional security products.

## The Impact of Targeted Attacks

Mass attacks receive more media attention, but in many events targeted attacks cause much greater damage to an individual business. In the UK, the National Hi-Tech Crime Unit (NHTCU) reported that more than 50 UK companies had been hit by targeted attacks in 2004, and last summer they arrested members of a Russian crime gang who had netted 1.3 million dollars in 90 days via the targeted Zombie bot attack.<sup>vii</sup>

Gartner estimates that although fewer than 10 percent of all current attacks are targeted against a particular company, the financial impact of a single successful targeted attack will be 50 to 100 times greater than that of a successful mass attack worm or virus. Forrester also states that with increasing organized crime involvement we will see more targeted attacks. Gartner further estimates that through 2009, businesses can expect to see the financial damages caused by targeted attacks grow at least five times more quickly than damages caused by mass attacks.<sup>viii</sup>

---

<sup>v</sup> National Infrastructure Security Co-ordination Center (NISCC) Briefing 08/2005 Issue 16 June 2005, <http://www.niscc.gov.uk/niscc/docs/ttea.pdf>

<sup>vi</sup> Online attacks aimed at U.S. traced to China/Pentagon’s a top target, but brass unable to put the blame on Peking or global hackers. Source: [http://www.chron.com/CDA/archives/archive.mpl?id=2005\\_3897760](http://www.chron.com/CDA/archives/archive.mpl?id=2005_3897760)

<sup>vii</sup> Russian Internet extortion gang cracked. Source: <http://www.newscientist.com/article.ns?id=dn6196>

<sup>viii</sup> John Pescatore, “Prevent Targeted Attacks,” ID Number: G0013303

## Protection Against Targeted Attacks

Most successful targeted attacks in recent years have often involved a combination social engineering, breakdown in process, technical vulnerability, and insider abuse.

People are usually the weakest but most important element in a security program. During a social engineering experiment at the IRS, auditors posing as network technicians managed to trick one-third of users into giving their passwords over the phone.<sup>ix</sup> Improperly defined processes or badly enforced policies are also often a factor in security breaches. For example, ChoicePoint failed to properly check the background of criminals posing as business customers who stole identify data of up to 145,000 users.<sup>x</sup> Furthermore, many of the most successful attacks are the results of authorized users abusing their access privileges. Business partners also often have access to sensitive corporate information. In 2002, credit reporting company Experian reported that 13,000 customer records were stolen using an authorization code belonging to Ford Motor Company.<sup>xi</sup>

Most of the “human security issue” can be improved to reduce the possibility of targeted attacks succeeding though they have been proven largely ineffective. Educating employees, encouraging them to notice and report the suspicious behavior of co-workers, properly define processes and enforce policies should be done to cover all bases. In general, people will be people, and technology solutions that can detect and prevent damaging behavior are where most security improvements will come from in preventing targeted attacks from succeeding.

### Technical Solutions

To properly mitigate targeted attacks, companies first have to move away from security devices that simply look for a predefined set of conditions, like matching attack signatures or comparing network activity to known vulnerabilities. An organization needs to deploy security devices inside its network interior that can accurately detect and shut down attacks in seconds without relying on signatures. The device must be able to adjust to future threats including slow and stealthy attacks. Because targeted attacks can affect different areas of the network, the security devices must also offer a variety of responses, from stopping attacks automatically to initiating an emergency response for a specific condition. Furthermore, this device needs to provide its users extreme security visibility into the network.

Because the perpetrators of targeted attacks devote both time and resources to learning about their potential victims, targeted attacks can use custom-created executables that are rarely detected by signature-based security techniques like IDS and IPS (whether network-based or host-based). Furthermore, targeted attacks have very specific victims, when a company suffers a targeted attack, it is all alone. No one else will know about the attack, and the company itself may not detect it for some time.

A targeted attacker will spend a lot of time probing the victim's network. This type of attacker is discrete. He or she will not bombard the target with portscans, but rather will rely on slow and stealthy techniques such as sending occasional packets, each from a different source address and each with a specific purpose in mind. These probe packets will blend in with normal network behavior, making them indistinguishable from background scans and rendering most network behavior analysis (NBA) systems useless since most NBA systems analyze network traffic based on IP flow generated by network elements.

---

<sup>ix</sup> <http://www.treas.gov/tigta/auditreports/2005reports/200520042fr.html>

<sup>x</sup> ChoicePoint: More ID theft warnings. Source: <http://money.cnn.com/2005/02/17/technology/personaltech/choicepoint/index.htm>

<sup>xi</sup> Experian, Ford Still Unsure How Hacker Stole 13,000 Credit Reports. Source: <http://lists.jammed.com/ISN/2002/05/0161.html>

A targeted attack may involve exploiting other networks in order to gain access to the victim's site. One way of gaining access into a victim's network is by probing partner networks for weaknesses. The networks of many large organizations have peering points with the networks of their business partners through VPN tunnels or leased lines. If partner organizations do not have identical or stronger security policies than the targeted organization, the partner networks become the logical point of entry for attackers. For example, in a recent industrial espionage scandal that involved several Israeli telecommunications and software companies, targeted Trojans were distributed to partner networks through marketing CDs.<sup>xii</sup> Because the attacks originated from the internal network rather than the network perimeter, traditional network perimeter devices—firewalls, IDS/IPS, and similar technologies—were unable to detect it.

## CounterStorm

CounterStorm, Inc. provides immediate internal network security against targeted, known, and zero-day attacks. CounterStorm's internal network security offering, CounterStorm-1, is an integrated internal network security solution that employs revolutionary technology to accurately identify and stop targeted and zero-day attacks within seconds. CounterStorm-1 employs a multi-tiered approach using three proprietary attack detection engines to search for non-standard traffic profiles. With a unique patent-pending correlation engine, Counterstorm-1 synthesizes data gathered without the use of signatures to detect attacks and shut them down within seconds. Furthermore, CounterStorm-1 adjusts to future threats—including slow and stealthy attacks—where other solutions fail.

CounterStorm-1 provides:

- **Accuracy:** CounterStorm-1 maintains an extremely low incidence of false positives. This eliminates the “boy who cried wolf” syndrome.
- **Speed:** CounterStorm-1 detects and stops attacks within seconds. Today's attacks have an extremely high velocity. In many cases, whole networks can be infected within minutes.
- **Flexible Response:** CounterStorm-1 provides several response methods to malicious activities: Automatic Response, Emergency Response, and Manual Response.
  - An automated response allows for instant action, stops attacks automatically, and provides the fastest and most effective protection.
  - When network administrators become aware of an on going attack, they can immediately trigger preconfigured emergency responses.
  - Manual response provides immediate notification when an attack occurs, and the network administrator need only push a button in order to block the attack. Manual response can be easily customized for any security environment.
- **Targeted visibility:** CounterStorm-1 provides its users extreme visibility into security information of his network over the layer 3 boundary. CounterStorm enables its users to drill down on events provided to the packet level.
- **Adaptation to future threats:** CounterStorm-1 employs proprietary machine-learning techniques and adjusts to future security threats as they manifest themselves.

---

<sup>xii</sup> Several high-level employees at Israel firms have been implicated in an industrial espionage scandal involving targeted Trojans. Source: <http://www.msnbc.msn.com/id/8145520>

## Conclusion

Targeted attacks are real. Targeted attacks are an enormous threat to an organization's security and its operation. Law enforcement agencies are already reporting significant increases in their frequency and their maliciousness. Security intelligence experts have also detected the tell-tale signs of organized crime gangs and government espionage in targeted attacks, and a hacker community much more motivated by financial gain than personal or political fulfillment.

To protect against targeted attacks, businesses need to acknowledge the risks of targeted attacks and prepare for them. Organizations need to educate employees, encourage them to notice and report the suspicious behavior of co-workers, properly define processes and enforce policies. Organizations also need to deploy effective, adaptive internal network security technologies that can accurately detect attacks and contain targeted and zero-day attacks.

CounterStorm-1 provides its users unparalleled accuracy. It detects and quarantines attacks in seconds—with no time-consuming false positives—and it equips its users with flexible response methods to neutralize malicious activities. CounterStorm-1 also adjusts to future security threats as they manifest themselves. CounterStorm has successfully detected and blocked multiple targeted and zero-day attacks at a Fortune 1000 company, halted a recent attack that targeted education and media organizations, and prevented a compromised medical device from sending confidential medical information to Russian hackers.

To learn more about CounterStorm, please visit <http://www.counterstorm.com>.