Newly Nasty*

The Economist, May 26, 2007

Imagine that agents of a hostile power, working in conjunction with organised crime, could cause huge traffic jams in your country's biggest cities—big enough to paralyse business, the media, government and public services, and to cut you off from the world. That would be seen as a grave risk to national security, surely?

Yes—unless the attacks came over the internet. For most governments, defending their national security against cyberwarfare means keeping hackers out of important government computers. Much less thought has been given to the risks posed by large-scale disruption of the public internet. Modern life depends on it, yet it is open to all comers. That is why the world's richest countries and their military planners are now studying intensively the attacks on Estonia that started four weeks ago, amid that country's row with Russia about moving a Soviet-era war memorial.

Even at their crudest, the assaults broke new ground. For the first time, a state faced a frontal, anonymous attack that swamped the websites of banks, ministries, newspapers and broadcasters; that hobbled Estonia's efforts to make its case abroad. Previous bouts of cyberwarfare have been far more limited by comparison: probing another country's internet defences, rather as a reconnaissance plane tests air defences.

At full tilt, the onslaught on Estonia was also of a sophistication not seen before, with tactics shifting as weaknesses emerged. "Particular 'ports' of particular mission-critical computers in, for example, the telephone exchanges were targeted. Packet 'bombs' of hundreds of megabytes in size would be sent first to one address, then another," says Linnar Viik, Estonia's top internet guru. Such efforts exceed the skills of individual activists or even organised crime; they require the co-operation of a state and a large telecoms firm, he says. The effects could have been life-threatening. The emergency number used to call ambulances and the fire service was out of action for more than an hour.

For many countries, the events of the past weeks have been a loud wake-up call. Estonia, one of the most wired nations in Europe, actually survived pretty well. Other countries would have fared worse, NATO specialists reckon.

National security experts used to dealing with high-explosives and body counts find cyberwarfare a baffling new theatre of operations. In Estonia's case, "botnets" (swarms of computers hijacked by surreptitiously placed code, usually spread by spam) swamped sites by deluging them with bogus requests for information. Called a "distributed denial of service" (DDOS) attack, this at its peak involved more than 1m computers, creating traffic equivalent to 5,000 clicks per second on some targets. Some parts were highly co-ordinated—stopping precisely at midnight, for example. Frank Cilluffo, an expert formerly at the White House, says that the attack's signature suggests that more than one group was at work, with small-time hackers following the initial huge sorties.

Most countries have been complacent about guarding information infrastructure. In America, a congressional committee for computer security has given failing grades to many of the federal bodies it scrutinises. The Department of Homeland Security supposedly has a "cybersecurity czar" but the throne has not yet found a steady occupant.

Private firms have had more experience in fighting off internet attacks. Organised crime gangs, often from Eastern Europe, extort money from gambling and pornography sites by using botnets to make them unreachable. Last week a large DDOS attack hit YLE, Finland's public broadcaster. This week Britain's *Daily Telegraph* was hit. No political or financial motive was apparent. A Romania-based hacker led the Finnish attack.

Firms of varying competence and credibility peddle technical solutions. The typical protection against DDOS attacks is to buy lots of extra computers and bandwidth to handle an unexpected spike in traffic. "Mirroring" content across several servers means the cyber-attackers must hit many more targets simultaneously before disrupting anything. A system's architecture helps too: Estonia's open approach, with its built-in flexibility and resilience, and co-operation between the state, business and academics, worked well. Mr Viik hopes this will deter those trying to build cyberdefences on a military or state monopoly model.

Counterattacks are possible, but tricky. Security firms' staff can pose as hackers to infiltrate cybergangsterdom. This used to be a mere battle of wits. Now there are real fears of violence. "It's changed now that big money is involved. It is not beyond the realm of imagination that someone might be targeted," says Mikko Hyppönen of F-Secure, an internet security firm.

But technology and sleuthing offer only a partial fix. The real question facing industrialised countries is how to create a legal environment that counts cyberaggression not as a kind of practical joke, but a grave breach of the legal order, akin to terrorism, international organised crime, or aggression against another state.

NATO is rethinking its position. It is designed to protect members against physical attack. When Estonia appealed for help it could only send an observer to Tallinn to monitor the attacks. For now, informal alliances are more useful.

Internet companies in friendly countries such as Sweden headed off many of the attacks before they even reached Estonia. Ken Silva, the security chief at VeriSign, which runs big chunks of the internet's domain-name system, advocates defences at the core of the network to tackle malicious data-packets before they reach their target. But finding agreement among the world's privately run internet networks is hard.

The urgent need is for an international legal code that defines cybercrimes more precisely, and offers the basis for some remedies. The Council of Europe, a continent-wide talking-shop that is the guardian of many international legal conventions, has a treaty on cybercrime dating from 2001. Acceptance has been partial. From overseas, America and Japan have signed up; Russia so far hasn't.

The International Telecommunication Union, which unites all 191 countries that use the world telephone system, hopes to take the lead in pushing for a global convention against cybercrime. Alexander Mtoko, its expert on cyberwarfare, says the key issue is anonymity: "We are in an industry where there is no control, no rules, no identities—it's the wild west. But for critical applications you have to know who you are dealing with." NATO experts agree. At a minimum, any international cybercrime convention is likely to oblige internet service providers to co-operate in blocking DDOS attacks coming from their subscribers' computers.

Yet the underlying problem is the internet itself. Wreaking havoc with anonymous telephone calls is hard. The internet's inherent openness allows hackers to hide. Yet that also helps make it cheap and innovative. Some countries may be more willing than others to trade freedom for security.

Mr Viik thinks a new global cybersecurity treaty may be reached by 2012. But victory will never be complete, thanks to the asymmetry between cat and mouse, notes Bruce Schneier, a security expert. "It is easier to come up with a new attack than with a new defence," he says. The strongest defence, says Mr Cilluffo, may be resilience: "the ability to reconstitute quickly, recover and absorb."

Browsers*

The New Threat Landscape

By Andrew Garcia
eWeek, August 4, 2008

With web-borne threats and drive-by downloads becoming the most troublesome form of malware today, enterprise IT administrators and users alike need to reconsider the tools and practices they prescribe and employ to protect computers and data—particularly as otherwise legitimate Web sites become the primary vector for malware transmission.

We've seen a twofold approach to malware as evildoers attempt to monetize their evildoings.

The first form stems from the phishing business, where malware authors create new domains and Web sites so fast that URL filtering and signature databases cannot keep up. The goal here is to score a few victims before the security companies can generate new signatures.

The second form consists of hijacked Web sites—sites that are otherwise legitimate but have been corrupted in a way that leads their visitors to malicious content.

An example of the interplay between these two types of Web threats is the Asprox botnet. The botnet originally derived from phishing attempts to draw unwitting users to malware via short-lived Web sites, but, in the last few months, Asprox has morphed into SQL injection attacks against legitimate sites. In automated fashion, the botnet leverages Google to find and exploit Web sites with vulnerable Active Server Pages, injecting an IFrame into the assailable site that redirects site visitors to exploit code elsewhere on the Web.

According to some sources, legitimate Web sites now comprise the majority of pages currently hosting malware. In its July 2008 Security Threat Report Update, Sophos Labs declared that 90 percent of the infected Web pages it detected in the first half of 2008 originated from legitimate Web sites that were hacked in some

form. The report also stated that Sophos Labs found, on average, more than 16,000 new infected pages each day during that time.

The changes in the way malware is propagated necessitate changes in the way IT managers secure corporate assets and give advice to users on keeping safe.

If the legitimate Web sites a user visits regularly, such as banks, merchants or social networks, can no longer be trusted to be clean, the old "spam-oriented" rule—not clicking on links in e-mail—becomes less relevant.

Indeed, when legitimate Web sites are the major source of malware, and users cannot readily tell whether a site is trustworthy by looking at it, there needs to be a technological solution to fill the breach and provide some assurance to users that the sites they visit are safe at this very moment—not five months ago, not an hour ago, but now.

Security providers have been trying out many new technologies to combat the problem of Web threats, as older, signature-based detections of the file system performed by anti-virus platforms have proven ineffective against new types of threats.

Newer technologies layer on Web reputation validation, in-line Web traffic scanning and script-blocking technologies to a browser's extended capability set, while anti-virus vendors augment their own platforms with more heuristic and behavioral analysis features.

Most of these browser add-on technologies have been targeted squarely on the Wild West that is the consumer's Microsoft Windows-based PC. Corporate customers, to date, have not suffered as much from Web threats, as enterprise administrators have deployed a tiered phalanx of both network- and host-based security solutions to combat all types of threats.

For example, intrusion prevention appliances or an in-line Web gateway appliance can detect and block both outbound traffic that looks like botnet activity and inbound, malware-laden Web traffic. However, network-based solutions will not protect users as they go mobile, outside the corporate network perimeter.

Makers of security solutions geared toward enterprise customers have made strides to improve their built-in detection and analysis of Web network traffic—blocking code from touching a protected system by examining the way it behaves or identifying its similarities to known threats before it touches the file system.

There are different approaches that administrators will need to evaluate before making any kind of deployment decision. Some products plug into the browser to specifically examine how things such as ActiveX or JavaScript behave, while others perform a more holistic HTTP scan that determines whether a Web request was made from a browser, e-mail application or other source. Other solutions, meanwhile, are baked into enterprise security platforms.

Some security companies are also changing the model by which malware is identified. Trend Micro, for example, is moving from a signature push model—where signatures need to be updated frequently all over the network—to a request-time pull for threat information from the cloud.

FIX MIX

Enterprise IT may be tempted to delve into consumer-oriented tools to augment the security of their most exposed, remote workers. However, such experiments will be fraught with complications. With most of these products, there is no central management component, so each instance is managed and updated on a one-off basis. Also, the products vary in their support for different browsers, which could interfere with the operation of outdated but mission-critical Web applications.

The best practical, vendor-neutral advice I can offer to avoid Web threats is to keep your systems patched—and by this I mean the operating system, the browser and its add-ons, as well as applications. That said, browser updates can sometimes cause incompatibilities with legacy Web applications.

Security software itself can even punish companies that don't keep fully up-to-date. For example, one of my favorite Web site validation and scanning tools—the stand-alone version of AVG's LinkScanner Pro—does not yet support Firefox 3.0, more than a month after the release of Mozilla's latest browser.

In cases such as these, administrators must weigh the use of a security program versus the productivity gained by using the application itself (and productivity usually wins). But if a security company has been known to be slow to adapt to browser improvements, the security solution will likely be a bad fit for corporate use on an ongoing basis.

WEB 2.0 Security*

Getting Collaborative Peace of Mind

By Marji McClure
Econtent, November 2008

Web 2.0 applications have opened up a lot of communication channels—and opportunity—for business professionals. They can, more than ever before, reach out to individuals from across the globe and share content and web applications. Through blogs, wikis, and social networking sites such as Facebook and Linked In, people are becoming more and more electronically intertwined. "There's a sense of security in a Web 2.0 world where people trust their personal information to others," says Jordan Frank, VP of sales and marketing for Traction Software. "They trust these sites."

Frank points out that some people trust such systems just because their friends do, and because sites such as Facebook haven't let people down—yet. He cautions that a breach could cause a backlash against such networks. "Ensuring success in Web 2.0 means that trust doesn't get broken," says Frank.

Most companies don't want to inhibit the collaborative flow that Web 2.0 has brought with it; they don't want it to hinder their overall operations and they want to continue to build on their Web 2.0 platforms. A Gartner Executives Programs survey of 1,500 CIOs from across the globe revealed that half of the respondents expected to invest in Web 2.0 technologies for the first time in 2008.

Internet experts agree that part of that investment must include security measures to protect organizations' intellectual property. One reason that Web 2.0 garners more attention for security safeguards than its predecessors is that its open nature makes it naturally more vulnerable to breaches. "The fact that security is becoming an issue speaks to the growth that Web 2.0 applications are having in the business world," says Isaac Garcia, CEO and co-founder of Central Desktop, which offers a web-based business collaboration platform.

Companies need to recognize the fact that the benefits that new technologies afford are typically accompanied by challenges. Web 2.0 is no different in this regard than any other technology offering. "The key thing is that when you're rolling out new technologies, these new technologies bring new vulnerabilities, as well as renew old vulnerabilities," according to John Pescatore, VP of internet research at Gartner, Inc. "It's an important time to build security features."

THE IMPLICATIONS

Web 2.0 security goes beyond the content that users find on the web and share with others within their network. It also involves preventing data leakage; that is, ensuring that that content doesn't find its way out, notes William "Sandy" Bird, CTO for Q1 Labs. The main vulnerabilities can be found directly in the collaboration applications such as wikis and blogs, in syndication (from RSS feeds and mashups), as well as Rich Interface Applications (RIA) and AJAX-enabled websites. Web 2.0 applications are vulnerable to a variety of threats, from cookie tampering to cross-site scripting (XSS) attacks.

Oftentimes, when such attacks occur, the user is unaware that his computer—and important data—has been compromised. It's a different world from years ago when viruses would wreak immediate (and very obvious) havoc on computer users. The threat may be imperceptible, and potentially even more dangerous.

The potential for security breaches caused by Web 2.0 technology is not likely to go away on its own. As more and more individuals use these applications (especially in the workplace), the risk of suffering from security breaches will likely increase considerably. In fact, companies are facing security issues on both the client side and the server side, says Danny Allan, director of security research for IBM Rational. Both can have devastating effects on companies, their employees, and their customers when the data created and stored in these Web 2.0 environments is compromised.

"Web 1.0 was a static page. With Web 2.0, you've got more client-side processes, like AJAX and widgets. Technically, there's more going on," says Doug Camplejohn, CEO and founder of Mi5 Networks, which focuses on the client side of the security issue.

DON'T DROP YOUR GUARD

This collaborative environment seems to be one in which users have let their guards down. "People don't read licensing agreements, they'll add a widget or they'll click on a link," adds Camplejohn, noting that the "bad guys" have gotten better at making harmful applications look legitimate. What has also changed, notes Camplejohn, is that when a virus and spam infected a system, their effects

were noticed immediately. "The new threats are silent," says Camplejohn. "They sneak in under the radar."

Mi5 Networks provides companies with Webgate appliances that help prevent vulnerabilities from occurring as well as helping to clean up any problems that do occur. The Webgate solutions don't require any installation and immediately monitor and block vulnerabilities. "Companies use us for two reasons: to see what employees are doing and what they are not doing; and to see what applications are okay and not okay," explains Camplejohn.

Imperva stresses the importance of having security measures in place on the server side when explaining its security solutions to customers. "What we talk to customers about is the need to apply security on the server side because that's where you have control," says Mark Kraynak, Imperva's director of strategic marketing. Still, with this approach, the goal is to prevent future problems. "We can show how the applications are working and we use the model to prevent attacks," explains Kraynak. Imperva's SecureSphere monitors the activity in its customers' applications and databases to prevent vulnerabilities. By using dynamic profiling, Imperva creates profiles of applications and databases, so changes and possible malicious activity can be more easily noticed.

Experts agree that such a proactive approach is the best approach, and one of the most popular solutions seems to be the technology that enables its clients to closely monitor its Web 2.0 systems and send alerts when a security breach is detected.

It's also helpful for companies to identify exactly who caused a security breach, and Q1 Labs' flagship product offers clients that visibility. QRadar enables its clients to uncover the source of a security problem and protect themselves against any security threats before they cause problems. "It's providing visibility to the incident as a whole," says Bird.

Most often, violators don't have malicious intentions, notes Camplejohn. However, safeguards still need to be in place to prevent users from accessing harmful websites and applications. Mi5 Networks has technologies that will block users from visiting a webpage that is identified as a risk. They receive a message that informs them that the particular page violates company policy. "We can also block a portion of a page and still deliver the good content," adds Camplejohn.

Pescatore notes that many organizations seek solutions that have security features already built in. He points to IBM and HP, which both purchased companies last year that offer security tools. IBM acquired Watchfire and HP bought SPI Dynamics. (Allan actually joined Watchfire in 2000 and transitioned to IBM with the acquisition.)

Within a few months, IBM released IBM Rational AppScan, which is a complete suite of automated web application security tools that scan and test web applications for security vulnerabilities. It also offers recommendations for how to fix problems that are identified, which helps organizations close the loop on their security issues.