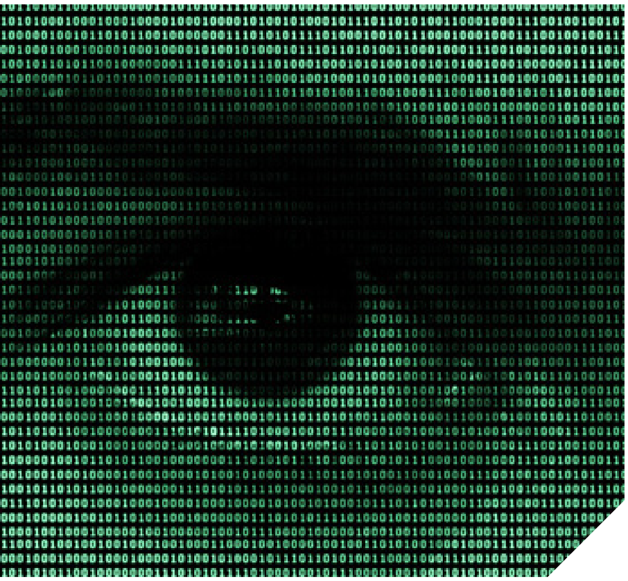


TEN CYBERTHREATS OUTSIDE THE FIREWALL

by Neustar Engineering

When most people think of cybersecurity, they think about passwords, firewalls, and hackers. However, the true nature of cybersecurity involves a far more sophisticated take on technology, intrusion detection, and data theft. Understanding these concerns and their nuances has become absolutely crucial for any organization that holds client data or credit card information, or has intellectual property on externally accessible servers.

Unfortunately for the IT Administrator, security vulnerabilities are not found exclusively in the cyber domain. Here is a list of ten current threats that can cause real damage to an organization's bottom line, brand, and reputation – all of which exist outside of a company's firewall.

1. Social Exploits

A huge percentage of other cyber-exploits start with some kind of social engineering that exposes a network to malware, exposes credentials or provides an open door for hackers to gain entry into a system. Some spoofed email scams (CEO Spoofing) can result in International wire transfers that are difficult to recover. Wire transfers should not be based on email instructions only.

There is no magic bullet to stop all social engineering. The most effective prevention is simple employee training to spot or be suspicious of social engineering exploits, such as: challenge unaccompanied visitors, be suspicious of thumb drives, don't leave your computer unlocked and never give out your password to anyone! The good news is there are ready-made training courses available online.

2. Phishing

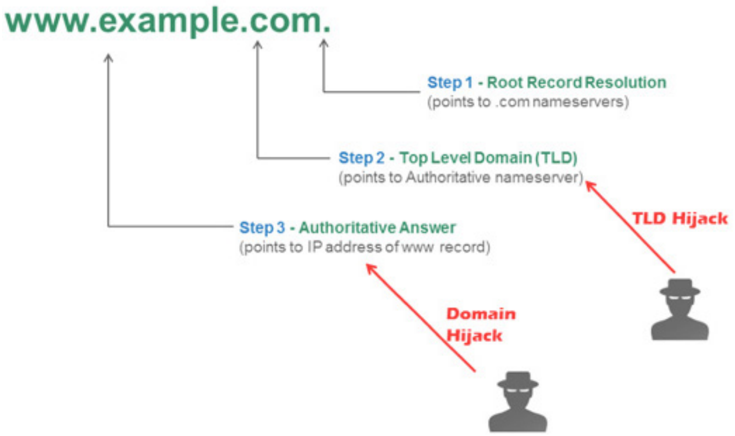
Spoofing email to appear from a trusted source is relatively simple. Most email servers don't actually block email that may be spoofed and may even fail authentication at some level. Phishing emails number in the millions per day. According to Symantec, in May 2014 one in every 395 emails was a phishing attempt. Furthermore, in May 2015, there were some 27 Billion spam emails sent every day!

A user that falls for a phishing email may expose a network to malware or spyware. Malicious emails may contain links to 'look-a-like' sites that fool visitors into exposing credentials or passwords. This may be the first step towards a broader cyberattack. Once again, training is critical. Firewalls and Recursive DNS servers can be used to block users from reaching malicious websites. Anti-virus software that checks all attachments can also be an effective measure against poisoned attachments. Not opening the email in the first place is your best bet. Agari makes software that can effectively block phishing emails from being delivered to the email Inbox in the first place.

3. TLD Hijacking

The DNS Recursion is a multi-step process. (Root, TLD, Authoritative). Unfortunately hackers have figured out how to hijack the DNS resolution and thereby redirect users to hacker controlled sites. Some well-known brands have fallen prey to such attacks (Huffington Post UK and The New York Times).

The TLD (top level domain) is vulnerable to being altered, thereby directing the DNS process to a hacker controlled nameserver for authoritative resolution and ultimate redirection to the hacker controlled website.


www.example.com.
Step 1 - Root Record Resolution
(points to .com nameservers)
Step 2 - Top Level Domain (TLD)
(points to Authoritative nameserver)
TLD Hijack
Step 3 - Authoritative Answer
(points to IP address of www record)
Domain Hijack

Several TLD operators (.com, .net) offer TLD Domain Locking, which makes it difficult to alter the TLD announcements. IT Administrators can also monitor the results of the TLD resolution and be notified in the results are changed. Neustar's Web Performance service includes DNS monitoring.

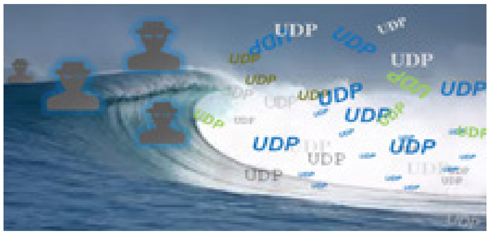
4. Domain Hijacking

Domain Hijacking is very similar to TLD Hijacking, just one step down on the DNS resolution tree. If a hacker can gain control of the DNS record for a website, it can easily be altered and users would be redirected to a hacked controlled website. Some DNS providers offered hardened portals that have built in security features such as:

Dual factor authentication
Access Control Lists
Domain Locking

You can also monitor the *results* of a DNS lookup and be alerted if the response from DNS were to be altered. Neustar's Web Performance service includes DNS monitoring.

5. UDP Flood



DDoS attacks have been growing in size and frequency. UDP floods are typically the largest attacks in both pure bandwidth (bits/second) and packets per second. UDP has several sub-protocols that can be exploited, such as: NTP, DNS, SSDP, Chargen and ICMP. These UDP amplification or reflection attacks are relatively simple to launch and can easily overwhelm a typical network environment with sheer volume.

In March 2013, the first 300 Gbps reflection attack was waged against Spamhaus. Then in February of 2014 a 400 Gbps NTP Reflection attack was reported against a French web hosting company. These massive attacks are not frequent or common, but they underscore the potential of UDP floods to overwhelm an enterprise network, hosting facility or even an ISP or cable company.

Consider a moderate UDP flood can be 25 Gbps. Most organizations don't have 25 Gbps of transit capacity, so their circuits become overwhelmed. Datacenters will typically black hole or null route the destination IP address that is under attack to protect their network integrity. This leaves the victim completely offline. No router, appliance or firewall can stop upstream circuit exhaustion.

The fundamental flaw with UDP is there is no 3-way handshake required, so the SOURCE of the packet can be easily spoofed. The attackers run a script that requests information from machines around the Internet, such as an NTP MON_GETLIST request. In turn, the machines reply not to the actual sender, but to the spoofed Source, aka the victim. The amplification of the attack occurs via the vulnerable machines out on the Internet (such as a router or printer) that send back a large response to a spoofed request. They flood the victim IP address with unwanted UDP packets. The attacks typically come from a widely distributed source pool.

IT Administrators need to be armed with both a detection and mitigation strategy. Typically detection of these large attacks can be accomplished with simple Netflow monitoring at the border router. This can be done in-house or outsourced to a third party. Mitigation is best left to a DDoS mitigation service. Traffic is redirected to a DDoS mitigation network for scrubbing. Once the attack has subsided, the redirection is unwound.

6. Slow and Low Denial of Service Attacks

The most well known of these attacks is called Slowloris, named after a small primate. Slowloris attacks a webserver by opening a large amount of sessions. Session capacity can be exhausted. Partial HTTP requests keep the sessions alive and can bind up thread/process capacity as well. These attacks can be difficult to detect, due to their low bandwidth volume. However, DDoS appliances or cloud based mitigation services can stop these attacks. Web Performance monitoring can identify when website performance begins to degrade. Lowering TCP Reset timer can be considered, but may produce collateral damage to some legitimate users.

7. SYN Floods

The SYN flood is the tried and true DDoS attack and still very popular. These attacks represent about 17% of the DDoS attacks that Neustar mitigates. Attacks are typically waged by a botnet of hundreds or thousands of compromised computers. With SYN floods, the botnet must generate the attack traffic without any amplification, so the total bandwidth of SYN floods tends to be lower than UDP floods. Most SYN floods have spoofed Source IP, which can be easily mitigated by the use of SYN Cookies. DDoS appliances, firewalls, CDNs and some proxy servers can protect against small-scale SYN floods. Large attacks are best handled by a DDoS mitigation service.

8. Click Fraud

In the world of online advertising and banner ads, a click from a legitimate user can trigger a payment to the referring website. This "click-thru" based pricing model has led to click fraud. Bots or machines are scripted to click away and run up phony charges. IP Reputation can help identify these malicious bots. In IP Reputation, a bot controlled IP address will score poorly on a Real User scale, which can then be rejected by the website.

9. Registration Fraud

Some online advertisers, search engines and referring websites have created incentives for click thru and registrations. These payments have led to Registration Fraud, in which a bot or script is designed to create phony registrations to drive up charge-back payments to the referrer. The CAPTCHA challenge is one attempt to combat these bogus bot-based Registrations. IP Reputation can also be used to reject IP addresses that have a high risk or are suspected of being controlled by a scripted bot.

10. WiFi Snooping

Most people don't realize that certain WiFi spots are relatively easy to exploit. There are hacker programs and even browser plug-ins that can allow a malicious actor to spy on WiFi neighbors in the local coffee shop or even takeover their current web sessions on certain websites, like Facebook. WEP WiFi is more vulnerable than WPA or WPA2. Corporate users should use a VPN, which adds a layer of encryption to their session on the web. Keep an eye on your browser and use with caution if you don't see the lock symbol indicating an encrypted https session.

For more information visit:
www.neustar.biz/it-security-services

©2015 Neustar, Inc. All rights reserved.