Anatomy of a cyber-attack

The strategies and tools of cyber-criminals—and how to stop them

Table of contents

Introduction

As the number and severity of cyber-crimes continues to grow, it's important to understand the steps cyber-criminals take to attack your network, the types of malware they use, and the tools you need to stop them. The basic steps of a cyber attack include reconnaissance (finding vulnerabilities); intrusion (actual penetration of the network); malware insertion (secretly leaving code behind); and clean-up (covering tracks).

Malware comes in various forms, some more nefarious than others, ranging from annoying sales pitches to potentially business-devastating assaults. Dell SonicWALL offers comprehensive solutions to counter every stage of cyber attacks and eliminate every type of malware from disrupting your business network.

You need to understand the enemy before you can defeat them.

Attack step 1: Reconnaissance and enumeration

The goal of reconnaissance is to learn about vulnerabilities in the targeted network and systems, including credentials, software versions, and misconfigured settings. One method for gathering this information is through social engineering cons, which fool end users into surrendering data. This is often perpetrated through phishing (fraudulent email), pharming (fraudulent web sites) and drive-by pharming (redirected DNS settings on hijacked wireless access points).

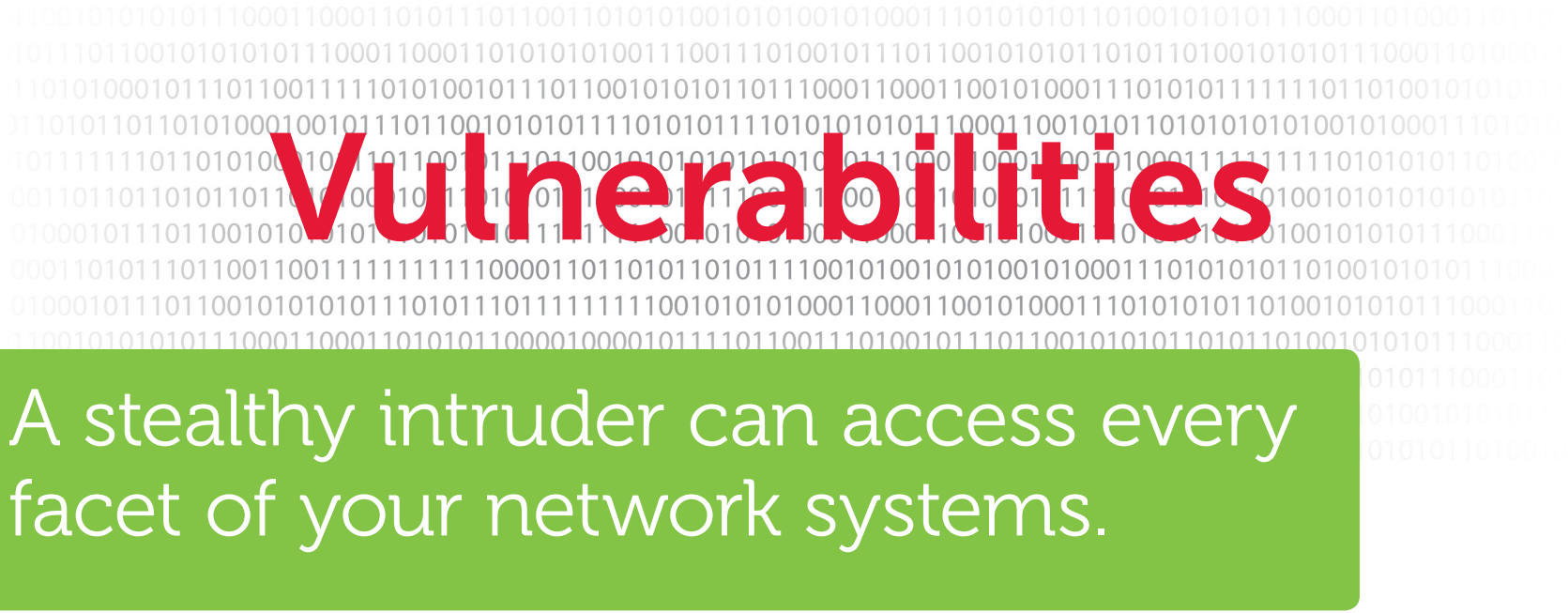
Enumeration, the second step in any type of cyber-attack, surreptitiously expands the knowledge and data gained during reconnaissance. Service scanning and war dialing are popular during the enumeration phase. Service scanning identifies network systems and correlates known bugs and software weaknesses. War dialing involves using an automated system to call each of the telephone numbers owned by a company in hopes of finding a modem which may provide direct access to internal company resources.

Cyber-criminals will do anything to find and exploit your weaknesses.

Attack step 2: Intrusion and advanced attacks

Once attackers have identified and correlated known vulnerabilities, they can exploit them to penetrate the network. Even more dangerous are sophisticated "zero-day" attacks, which exploit software weaknesses that, while not publically disclosed, may have been distributed on the black market among attackers ranging from petty criminals to transnational organized criminal gangs.

Another advanced form of malicious intrusion is the denial-of-service (DoS) attack, which aims to render networks inoperable by bombarding them with external communications requests. Common DoS attacks include smurf attacks, ping flood attacks, ping-of-death attacks and SYN flood attacks.



A stealthy intruder can access every facet of your network systems.

Attack step 3: Malware insertion

After infiltrating a network, the next step in an attack is to secretly insert malware in order to maintain ongoing remote control over systems, and ultimately, execute code within the network to achieve a particular goal.

Inserted malware can be a nuisance (e.g., marketing driven); controlling (to provide back door access or remote control), or destructive (to cause intentional harm or to cover the tracks of the attacker).

Hidden malware gives your attacker the keys to your network.

Malware type 1: Nuisance malware

Some types of malware are not overly malicious in nature, but can cause annoyance and affect system performance and productivity. Spyware, used to collect and relay sensitive information back to its distributor, also can be a major nuisance, typically infecting web browsers rendering them nearly inoperable. Spyware is often used for deceitful marketing purposes, such as monitoring user activity without their knowledge.

Adware, as the name implies, is typically used to spread advertisements, providing some type of financial benefit to the attacker. After becoming infected by adware, the victim becomes bombarded by pop-ups, toolbars and other types of advertisements when attempting to use the infected computer.

Nuisance adware can render a system inoperable if not removed properly.

Malware type 2: Controlling malware

Other malware hides in wait to issue controls or execute attacks. Trojans—executable code embedded into another (typically commonly-used) application—are often designed to be unknowingly launched by a trusted user. Remote-access Trojans (RATs) create back doors for remote control.

Rootkits are even more insidious. They hide in low-level, sub-OS system resources to provide attackers with unrestricted network access, and can even go undetected by conventional anti-virus solutions. Trojans and rootkits are often used in creating zombie systems, from which criminals can launch outbound botnet attacks.

Hidden malware gives your attacker the keys to your network.

Malware type 3: Destructive malware

Typically designed to inflict damage, computer viruses can purge an entire hard disk, rendering data useless in a matter of moments. Commonly spread through shared files, web downloads or email attachments, viruses must be executed on the target system before they actually pose a threat. Once activated, viruses often replicate themselves throughout the infected system. Seek-and-destroy viruses target specific files types or portions of the hard disk.

Unlike viruses, worms can spread themselves throughout networks without user activation. Once infected by a worm, the compromised system will begin scanning the local network in an attempt locate additional target systems. After locating a target, the worm will exploit vulnerabilities in its operating system, injecting it with malicious code. While sometimes viewed as a nuisance, worms can also spread other malware and inflict damage.

Viruses and worms can devastate your network—and your business.

Attack step 4: Clean-up

The final stage of the attack cycle is to rid the infected system of forensic evidence. A proactive element to this step is for attackers to be as inconspicuous as possible in the earlier steps. For example, an attacker may commandeer the credentials of a trusted network user that would not raise alarms by accessing the targeted systems, or use commonplace applications, such as instant messaging, to insert malicious files or extract information.

A primary goal of this step is to erase any traces of the attack from the system. This can be done by the manual or automated deletion of command line or event logs, deactivation of alarms, and the upgrade or patching of outdated software after the attack has been accomplished. Additionally, hackers and cyber thieves often unleash viruses and worms to destroy potentially incriminating evidence.

A skilled criminal can compromise your network without you ever knowing.

Dell SonicWALL Next-Generation Firewall

Dell™ SonicWALL™ offers a comprehensive line of defenses against all forms of cyber attack and malware.

- Dell SonicWALL Next-Generation Firewalls, featuring Reassembly-Free Deep Packet Inspection® (RFDPI) technology and multi-core parallel architecture, scan and analyze inbound and outbound traffic to identify multiple threats, applications and protocols, at wire speed and without file size limitations.

- Using input from millions of shared touch points in the Dell SonicWALL Global Response Intelligent Defense (GRID) Network, the Dell SonicWALL Threat Center provides continuous communication, feedback, and analysis on the nature and changing behavior of threats. Dell SonicWALL Research Labs continuously processes this information, proactively delivering countermeasures and dynamic updates to stop the latest threats.

- The Dell SonicWALL SuperMassive E10800 running SonicOS 6.0 is the highest overall protection Next-Generation Firewall to earn the "Recommend" rating from NSS Labs, the recognized leader in independent security product testing. This single code base for SonicOS is at the core of every Dell Dell SonicWALL firewall, from the TZ 105 to the Dell Dell SonicWALL SuperMassive E10800.

Dell SonicWALL Next-Generation Firewall

- The Dell SonicWALL **Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service** delivers intelligent, real-time network security protection against the latest blended threats, including viruses, spyware, worms, Trojans, software vulnerabilities and other malicious code.
  - **Intrusion prevention service (IPS)** prevents attackers from exploiting known vulnerabilities (Step 2 of the attack cycle)
  - **Gateway anti-virus and anti-spyware** prevents attackers from installing or uploading malware to a compromised system (Step 3 of the attack cycle)
  - **Application intelligence and control** prevents attackers from being able to use commonplace applications to transmit data to or from the compromised system (Step 4 of the attack cycle)
- Working in conjunction with Dell SonicWALL firewalls, **Dell SonicWALL Enforced Client Anti-Virus and Anti Spyware** software provides comprehensive gateway-enforced virus and spyware protection for desktops and laptops. Dell SonicWALL firewalls ensure that all of the computers accessing the network have the latest version of anti-virus and anti-spyware software installed and active.

Dell SonicWALL comprehensive integrated security solutions

- Dell SonicWALL **Clean Wireless™** integrates Dell SonicWALL firewalls with universal 802.11 a/b/g/n wireless access points, to deliver advanced security features such as WiFiSec, Virtual APs (VAP), and wireless intrusion detection services (WIDS).

- When combined with Dell SonicWALL Secure Remote Access (SRA) solutions, Dell SonicWALL firewalls create a **Clean VPN™** that decrypts and scans all authorized SSL VPN traffic for malware before it enters the network, and adds enforced authentication, data encryption, and granular access policy.

- The Dell SonicWALL **Email Security** Series provides comprehensive email threat protection for organizations of all sizes, stopping email-borne spam, virus, and phishing attacks, while contributing to internal policy and regulatory compliance.

- Dell SonicWALL **Application Traffic Flow Analytics**, including the Dell SonicWALL Global Management System 7.0, Scrutinizer and Analyzer solutions, increases threat awareness through real time and historical traffic analysis and provides powerful insight into application traffic, bandwidth utilization and security threats along with powerful troubleshooting and forensics capabilities.

How can I learn more?

- Download the whitepaper "The Wild World of Malware: Keeping Your Company Safe"
- View the webinar "Exploring the Digital Underworld: Botnets, Zero Day Threats and Phishing"
- Opt-in to receive Dell SonicWALL newsletters

For feedback on this e-book or other Dell SonicWALL e-books or whitepapers, please send an email to feedback@sonicwall.com.

About Dell SonicWALL

Dell™ SonicWALL™ provides intelligent network security and data protection solutions that enable customers and partners to dynamically secure, control, and scale their global networks. Securing any organization with multi-threat scanning based on global input at wire speed, Dell SonicWALL is recognized as an industry leader by Gartner and NSS Labs. For more information, visit the web site at **www.sonicwall.com**.

05/13 DS 0090L