radware

FIVE WAYS
Modern Malware Defeats Your Defenses… …And What You Can Do About It

Malware is a key vector for data breaches. Research shows that 51% of data breaches include the usage of malware, whether for initial breach, expansion within the network or heisting data[1]. Yet despite malware being a pivotal attack vector, companies are unable to defend against data-theft malware running wild in their network. In fact, some of the biggest and most well-publicized breaches ever were the result of undetected malware.

The reason is that modern malware is built to evade traditional anti-malware defenses. Today's malwares are sophisticated multi-vector attack weapons designed to elude detection using an array of evasion tools and camouflage techniques. In the game of chess between attackers and defenders, hackers constantly find new ways to stay one step ahead of existing defenses.

Below are five common evasion techniques used by modern malware and how they beat traditional anti-malware defenses:

1. Polymorphic malware: many traditional anti-malware defenses operate using known malware signatures. Modern data-theft malware counteracts this by constantly morphing or shapeshifting. By making simple changes to the code, attackers can easily generate an entirely new binary signature for the file.

Shapeshifting, zero-day malware beats signature-based defenses such as anti-virus, email filtering, IPS/IDS, and sandboxing.

1 2017 Verizon Data Breach Investigations Report (DBIR) - http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

2. File-less malware: Many anti-malware tools focus on static files and operating-systems (OS) processes to detect malicious activity. However, an increasingly common technique by attackers is to use file-less malware which is executed in runtime memory only, leaves no footprint on the target host and is therefore transparent to file-based defenses.

File-less malware beats IPS/IDS, UEBA, anti-virus, and sandboxing.

3. Encrypted payloads: Some anti-malware defense use content scanning to block sensitive data leakage. Attackers get around this by encrypting communications between infected hosts and Command & Control (C&C) servers.

Encrypted payloads beat DLP, EDR, and secure web gateways (SWG).

4. Domain generation algorithm (DGA): Some anti-malware defenses include addresses of known C&C servers, and block communication with them. However, malwares with domain generation capabilities get around this by periodically modifying C&C address details and using previously unknown addresses.

Beats secure web gateways (SWG), EDR, and sandboxing.

5. Host spoofing: spoofs header information to obfuscate the true destination of the data, thereby bypassing defenses that target the addresses of known C&C servers.

Beats secure web gateways (SWG), IPS/IDS and sandboxing.

WHAT CAN YOU DO?

Beating zero-day evasive malware is not easy, but there are several key steps you can take to severely limit its impact:

1. **Apply multi-layer defenses**: Protecting your organization against evasive malware is not a one-and-done proposition. Rather, it is an ongoing effort that requires combining endpoint defenses (such as anti-virus software) with network-layer protection such as firewalls, secure web gateways and more. Only multi-layered protection ensures complete coverage.

2. **Focus on zero-day malware**: Zero-day malware accounts for up to 50% of malware currently in circulation. Zero-day malware frequently goes unrecognized by existing anti-malware defenses and is a major source of data loss. Anti-malware defense mechanisms that focus squarely on identifying and detecting zero-day malwares is a must have.

3. **Implement traffic analysis**: Data theft malware attacks take aim at the entire network to steal sensitive data. Although infection might originate from user endpoints, it is typically the aim of attackers to expand to network resources as well. As a result, it is important for an anti-malware solution to not just focus on one area of the network or resource type, but maintain a holistic view of the entire network and analyze what is happening.

4. **Leverage big data**: A key ingredient in detecting zero-day malware is the ability to collect data from a broad information base amassed over time. This allows defenders to detect malware activity on a global scale and correlate seemingly unrelated activities to track malware development and evolution.

RADWARE CLOUD MALWARE PROTECTION SERVICE

The Radware Cloud Malware Protection Service is the last line of defense against data-stealing zero-day malware. Radware's service takes a different approach than traditional malware defenses by focusing specifically on detecting and blocking evasive zero-day malware activity and employing artificial intelligence using machine learning to detect communication anomalies indicative of malware. Cloud Malware Protection Service protects a large community of more than 2 million enterprise users worldwide and detects over 500 zero-day malwares weekly by analyzing more than 2 billion communications daily and over 3 TB of data each week.

Radware's Cloud Malware Protection Service is a 100% cloud-based solution which does not require the user to install any software or hardware on-premise.

Selecting Radware's Cloud Malware Protection Service helps customers enjoy the following capabilities:

Detect Zero-Day Malware
using Radware's machine-learning technology that detects communication anomalies indicative of zero-day evasive malwares

Block Malware Activity
using API integration with defense mechanisms such as SIEM systems, Secure Web Gateways (SWGs) and Next Generation Firewalls (NGFWs)

Report on Malware Activity
in the network and get immediate alerts when new malware is detected in your network

Audit the Network's Defenses
against zero-day evasive malware activity on a continuous basis using Radware's Javelin Auditor

LEARN HOW THE RADWARE CLOUD MALWARE PROTECTION SERVICE CAN HELP YOUR ORGANIZATION DEFEND AGAINST THE RISK OF DATA BREACH.

About Radware

Radware® (NASDAQ: RDWR), is a global leader of cyber security and application delivery solutions for physical, cloud, and software defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application, and corporate IT protection services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.