

Diary of a "RAT" (Remote Access Tool)

A five-year history lesson directly from the source

McAfee® Labs™ researchers recently gained access to the history log files of an attacking command and control (C&C) server and uncovered details of five years of attacks propagated by the Shady RAT advanced persistent threat (APT). Learn about what the remote access tool's (RAT's) diary revealed.

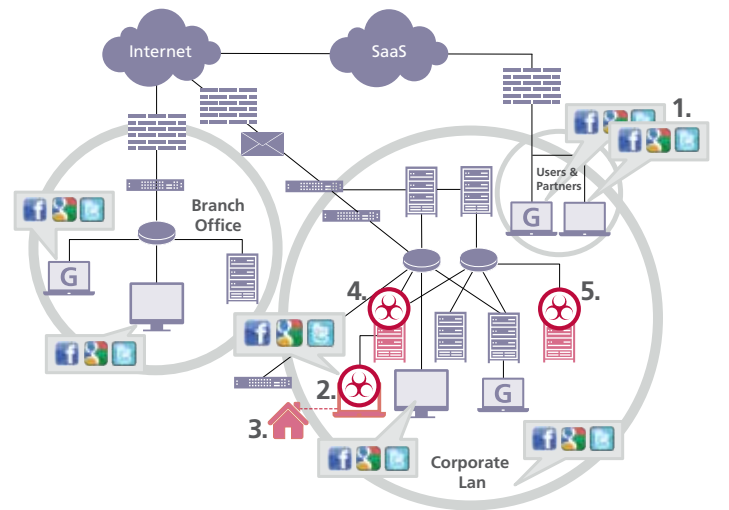
McAfee Portfolio for Connected Security

No single technology can provide connected security against targeted, persistent attacks. Consider the following McAfee security products for complete multi-layered security:

- McAfee® Application Control
- McAfee® Data Loss Prevention
- McAfee® Database Activity Monitoring
- McAfee® Email Protection
- McAfee® Endpoint Security Suites
- McAfee® Enterprise Mobility Management
- McAfee® ePolicy Orchestrator®
- McAfee® Firewall Enterprise
- McAfee® Network Behavior Analysis
- McAfee® Network Security Platform
- McAfee® SiteAdvisor®
- McAfee® Vulnerability Manager
- McAfee® Web Protection

1. Spear phishing does work. This is the first and most successful attack vector, giving attackers access with privileges.
2. Many types of data are coveted. Over many years of investigations into cyber espionage intrusions, the McAfee Labs team discovered that the following vital information has been stolen by hackers from organizations:
 - Closely guarded national secrets
 - Source code
 - Bug databases
 - Email archives
 - Negotiation plans
 - Exploration details for new oil/gas field auctions
 - Document stores
 - Legal contracts
 - Supervisory control and data acquisition (SCADA) configurations
 - Design schematics
3. Attackers have a variety of motivations. In the case of the Shady RAT exploit, these were largely financial and political.
4. Stolen data now reaches into petabytes (1 quadrillion or 1,000 terabytes) of content—as far as we know.
5. We don't know where all of that information has gone, who has accessed it, or what they have done with it.

Anatomy of a RAT APT Attack



1. Reconnaissance
2. Social Engineering Targeted Malware
3. Establish Covert Backdoor
4. Establish Command and Control Infrastructure
5. Complete Objectives and Maintain Persistence

6. Every geography is affected.
7. Every type of business (public, private, government) is affected.
8. Every size of business (government agencies to nonprofits) is affected.
9. Attacks are long-lived and persistent. The longest attack duration was 28 months (the average of 71 companies identified was 8.75 months).
10. All of the Fortune Global 2,000 can now be divided into two categories: those who have been compromised and know it and those who have been compromised and don't know it yet.

APTs Hide in Plain Sight

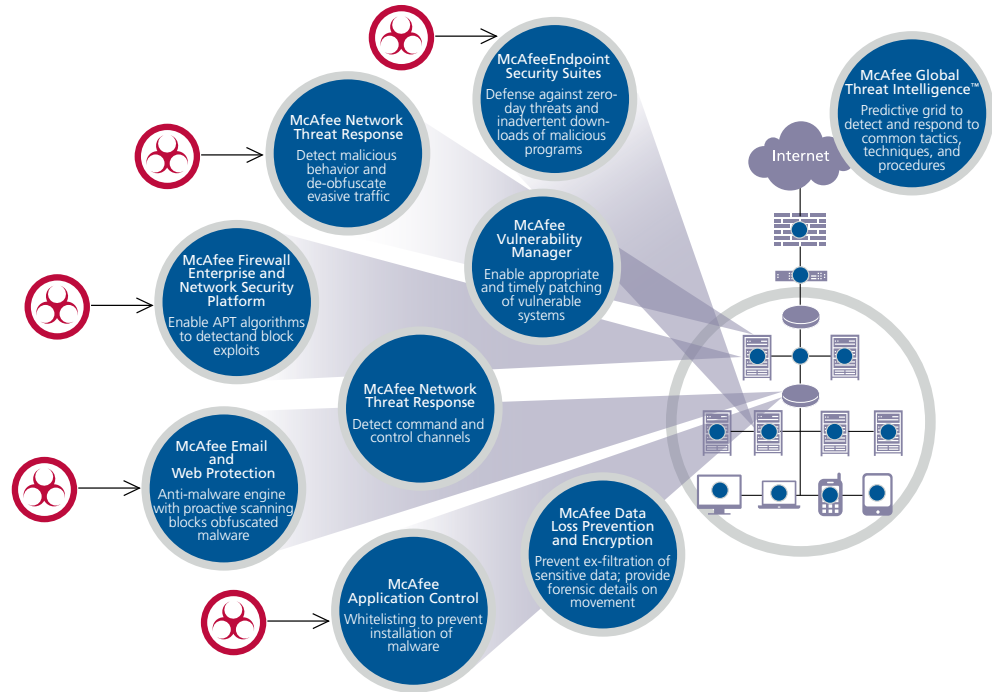
APTs avoid detection by using common network ports, process injection, and Microsoft Windows service persistence. APTs generally only initiate outbound network connections. So, unless an enterprise network is specifically monitoring outbound network traffic for APT-related anomalies, it will not identify the APT malware outbound beaconing attempts.

Some pertinent statistics about APT malware:

- Average file size: 121.85 Kb
- Most common APT file names:
 - » Svchost.exe (most common)
 - » lexplore.exe
 - » lprinp.dll
 - » Wiinzf21.dll
- Avoids anomaly detection through:
 - » Outbound HTTP connections
 - » Process injection
 - » Service persistence
- Communications:
 - » 100 percent of APT backdoors make only outbound connections
 - » 83 percent use TCP port 80 or 443
 - » 17 percent used another port

Because APT malware is so difficult to detect, simple malware signatures such as MD5 hashes, filenames, and traditional anti-virus methods usually yield a low rate of true positives.

McAfee Security Connected Portfolio Blocks APT Attack Vectors



Don't Become a Victim

There are five steps that you can take to protect your enterprise, whether or not you've been targeted:

1. Block unwanted infiltration.
 - Email security helps detect spear-phishing messages before they hit users' inboxes
 - Web security helps detect and stop users from going to malicious or infected URLs
 - Comprehensive endpoint protection helps detect and stop inadvertent downloads of malicious programs
 - Firewall and intrusion prevention systems (IPS) block the downloads of malware and deny unauthorized access by command and control servers
2. Block unauthorized changes.
 - Application whitelisting blocks unauthorized changes from being made
 - Database activity monitoring stops unauthorized access to critical databases
3. Avoid sensitive data from being harvested and exfiltrated.

- Data encryption denies access to data even if it has been stolen
- Data loss prevention identifies sensitive content and controls its movement throughout the network
- 4. Know what's going on inside your network.
 - Network behavior analysis can identify compromised systems based on traffic behavior anomalies
 - Centralized management and vulnerability assessment allow you to enable appropriate and timely patching of vulnerable systems
- 5. Achieve a global perspective.
 - Knowing just your own network isn't sufficient—you need a global understanding of all threats worldwide to protect yourself

For more information, please contact your McAfee sales representative, or visit www.mcafee.com. Detailed information on advanced persistent threats like Operation Aurora and Shady RAT can be found at <http://www.mcafee.com/us/mcafee-labs.aspx>. Our McAfee Labs team has also released its complete report on Shady RAT which can be found at www.mcafee.com/shadyrat.

