Solution Brief

‘Trojanized’ Legitimate Software

Prevent infection and mitigate propagation with Intel® Security products

The mechanisms used for software distribution through the Internet can be turned into malware and virus attack vectors. There is a clear evolution from the original malicious binder exposed a decade ago to the sophisticated distribution of legitimate software that is “Trojanized” before or during the distribution phase.

Regardless of a Trojan’s sophistication, the fundamental steps are the same:

- “Weaponize” the software: Insert malware into a deliverable application.
- Delivery: Transmit undetected Trojanized software to the target.
- Exploitation: Trigger the Trojan’s code and attempt to remain undetected.
- Installation: Establish persistence and attempt lateral movement.

The latest attack technique is based on a sophisticated on-the-fly mechanism that injects code into a legitimate download to remain undetected. The attack principle is to merge the original application and the malicious code.

This attack technique might use two components to find a successful entry point into the target: a listener that catches and modifies the HTTP download request and a binder that infects and distributes the binaries.

Current algorithms deploy malware infection routines and network redirection attacks without modifying the application’s code. That opens a floodgate for weaponized commercial or open-source software and can include executable files with an embedded signature. The attack succeeds if the signature is not automatically and fully verified before any initial execution attempt.

Once the Trojanized application is launched in the target, a binder process creates its own file for additional embedded executables in which all the injected code is reconstructed for further execution, bypassing all security controls. Because the original application is intact, the malware might be attached to any file with any signature and still succeed.

intel Security

Policies and procedures

The latest Intel Security cyber defense best practices recommend the adoption of the following general threat mitigation strategies for network and endpoints:

- Use a virtual private network when connecting to an untrusted network. Administrators should keep security software up to date and rely on strong indicators of trust rather than those potentially forged in an attack. Applications should be signed and verified with a chain of trust. Forensic analysis should include correlating hashes with trusted sources.
- Security software should include dynamic analysis to flag rogue actions regardless of initial binary inspection because static scanning goes only so far. Behavioral monitoring, web and IP reputation, memory scanning, and application containment are valuable components of a complete solution.
- Vendor downloads should occur over secure connections and all code should be signed. This drastically reduces man-in-the-middle attacks. Software vendors should include self-validation in their applications, regularly audit their code, use static code analysis tools, and perform peer reviews. It is always good to have a central repository of trusted corporate applications and allow users to download only approved installers from that repository.
- Antimalware software should be configured to identify the presence of binders.
- Host intrusion detection and prevention applications should be used for packet inspections that can identify malicious payloads.
- Use only trusted virtualization architectures combined with proper network segmentation. Trusted virtualization architectures use a secure and verifiable boot process. Sound network segmentation can monitor traffic and keep applications isolated in the event of a successful exploit. This combination also protects against lateral malware movement.
- Identify the presence of malware delivered by Trojanized software by monitoring outbound traffic. It is possible to expose infected machines for further remediation by the traffic they attempt to send to the Internet.

Intel Security

Intel Security products can identify Trojanized legitimate software, identify and block embedded malware threats, expose compromises, and respond quickly:

McAfee VirusScan® Enterprise 8.8 or McAfee Endpoint Security 10

- Keep DAT files up to date.
- Ensure McAfee Global Threat Intelligence (McAfee GTI) is in use; it recognizes more than 600 million unique malware signatures.
- Develop Access Protection rules to stop installation and payloads of malware:
  - Refer to Access Protection rules Knowledge Base Article: KB81095 and KB54812.
  - Refer to configuration best practices for McAfee VirusScan 8.8 Enterprise: PD22940.
  - Refer to configuration best practices for McAfee Endpoint Security: KB86704.

McAfee Host Intrusion Prevention

- McAfee Host Intrusion Prevention can help prevent the spread of malware. Using custom IPS signatures, you can create rules to prevent malware-generated file operations (create, write, execute, read, etc.).
- Enable Host Intrusion Prevention Signature 3894, Access Protection—Prevent svchost.exe executing non-Windows executables.
- Enable Host Intrusion Prevention Signatures 6010 and 6011 to immediately block the injection.
- Two subrule types can accomplish this:

1. Create a custom IPS signature using the Files engine and a subrule with the following criteria:
   - Name: <insert name>
   - Rule type: Files
   - Operations: Create, Execute, Read, Write
   - Parameters: Include - Files - <path/filename of malware>
     - The filename must include a path. If you wish to wildcard the path, begin the filename with "**\" or "?:\" if you wish to wildcard the drive letter (for example: "**\filename.exe" or "?:\filename.exe").
     - You cannot use MD5 hashes with the "Files" parameter, only path/filename.
     - You can also use the drive type to limit the path to a specific drive (for example, hard drive, CD-ROM, USB, network, floppy).
   - Executables: Can be left blank, unless you want to limit the signature to specific processes that perform the file operation (for example, explorer.exe, cmd.exe, etc.).
2. Create a custom IPS signature using the Program engine and a subrule with the following criteria:
   - Name: <insert name>
   - Rule type: Program
   - Operations: Run target executable
   - Parameters: <leave blank>
   - Executables: Can be left blank, unless you wish to limit the signature to a specific process as the source executable (for example, if you want to block explorer.exe from running a Target Executable (such as notepad.exe)).
   - Target Executables: Define the executable properties for which you want to prevent execution (for example, if you want to block notepad.exe from running, specify the path/filename of the executable). The executable can be defined using one or more of the criteria (file description, filename, fingerprint, signer).

McAfee SiteAdvisor® Enterprise or McAfee Web Protection

- Use website reputations to prevent or warn users of websites that distribute Trojanized software.

McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense

- Threat Intelligence Exchange policy configuration:
  - Start with observation mode: As endpoints are discovered with suspected processes, use system tags to apply Threat Intelligence Exchange enforcement policies.
  - Clean at: known malicious.
  - Block at: most likely malicious (blocking at unknown would provide better protection but may also add initial administrative workload).
  - Submit files to McAfee Advanced Threat Defense at unknown and below.
  - Threat Intelligence Exchange Server policy: Accept Advanced Threat Defense reputations for files not yet seen by Threat Intelligence Exchange.
- Threat Intelligence Exchange manual intervention:
  - File reputation enforcement (subject to operation mode). Most likely malicious: clean/delete.
  - Might be malicious: Block.
- Enterprise (organizational) reputation can override McAfee GTI:
  - You can choose to block an undesired process, for example, an unsupported or vulnerable application.
  - Mark file as might be malicious.
- Or choose to allow an undesired process for "testing":
  - Mark file as might be trusted.

McAfee Advanced Threat Defense

- In-box detection capabilities:
  - Signature-based detection: Signatures maintained by McAfee Labs include more than 600 million signatures.
  - Reputation-based detection: McAfee GTI
  - Real-time static analysis and emulation: Used for signatureless detection
  - Custom YARA rules
  - Full static-code analysis: Reverse engineers file code to assess attributes and function sets and fully analyze source code without execution.
  - Dynamic sandbox analysis
- Create analyzer profiles where Trojanized software is likely to run:
  - Common OS, Windows 7, 8, 10
  - Install Windows applications (Word, Excel) and enable macros.
- Provide an analyzer to profile Internet access:
  - Many samples run a script from a Microsoft document that makes an outbound connection and might activate the malware. Providing an analyzer profiles an Internet connection and increases detection rates.

McAfee Network Security Platform

- Network Security Platform has signatures in its default policies to detect the TOR network, which may be used to transfer files associated with malware.
- Integrate with Advanced Threat Defense for new variants of attacks:
  - Configure Advanced Threat Defense integration in "advanced malware policy."
  - Configure Network Security Platform to send .exe, Microsoft Office, Java archive, and PDF files to Advanced Threat Protection for inspection.
  - Verify Advanced Threat Protection configuration is applied at the sensor level.
- Update callback detection rules (to combat botnets).

McAfee Web Gateway

- Enable McAfee Gateway antimalware inspection.
- Enable GTI for URL and file reputation.
- Integrate with Advanced Threat Defense for sandboxing and zero-day detection.

VirusTotal Convicter: Automated Intervention

- Convicter is a Python script triggered by the McAfee ePolicy Orchestrator® (McAfee ePO) automated response system to cross-reference with VirusTotal any file generating a McAfee Threat Intelligence Exchange threat event.
- It is possible to alter the script to reference other threat intelligence exchanges, such as GetSusp.
- If the threshold for trusting the community is met, the script will automatically set the enterprise reputation. Suggested conviction threshold: 30% of vendors and two majors must agree.
- Filter: "Target file name does not contain: McAfeeTestSample.exe."
- This is a free, community supported tool (not supported by Intel Security).

McAfee Endpoint Threat Defense & Response

- McAfee Endpoint Threat Defense & Response finds and responds to advanced threats. When used in association with threat feeds from McAfee Labs, Dell SecureWorks, or ThreatConnect, new threats can be searched for and eliminated before they have a chance to spread.
- Custom collectors allow you to build specific tools to find and identify indicators of compromise associated with Trojanized applications.
- Triggers and reactions are built by the user to define actions when specific conditions are met. For example, when hashes or filenames are found, a "delete" action can automatically run.

For Further Reading

Best Practices for how to use McAfee Host Intrusion Prevention rules for a malware outbreak: KB84507

This Knowledgebase article provides customers with detailed information about Trojan-Powelike: Infection and Propagation Vectors: PD25582

SIEM Orchestration: Orchestration Triggers Signs of Malware Infection and Anomalous Behaviors: PD24830

White paper: *Secure Beyond the Signature*

FAQs for Network Security Platform: Advanced Malware Detection: KB75269

McAfee Web Gateway Product Guide: Web Filtering: PD26339

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com