Solution Brief

# Protecting Against Password Stealers

As we depend ever more on personal electronic devices and businesses move valuable information to the cloud, the value of access credentials has risen. Today, attackers use stolen passwords in the early stages of nearly all major advanced persistent threats.

Password stealers focus on breaching network and system security to obtain critical access credentials. The Fareit password stealer's robust capabilities have made it the most popular password-stealing malware for more than five years. Since its discovery in 2012, Fareit has continued to change to elude the latest cyber-defense strategies.

Initially, Fareit focused on stealing login credentials from web browsers to gain access to applications such as online banking, email accounts, and for identity theft. Since then, Fareit has evolved into a more aggressive information stealer that hides using mimetic tactics such as changing its file hash with each infection. In 2016, a new generation of Fareit password-stealing malware appeared, using an infected network asset to perform distributed denial of service attacks. Further, Fareit is now offered as a pay-per-infection service, which means that cybercriminals are now earning money to distribute malware. The more infections they can achieve, the more they are paid.

Phishing attacks that deliver password stealers such as Fareit are among the top initial attack vectors during the past decade.

## Policies and procedures to protect against password-stealer attacks

McAfee recommends that organizations take the following steps to protect against password-stealer attacks:

- Password stealers are often distributed by malware, so as a standard security principle always keep antimalware products up to date.
- Malware can be downloaded by unaware users while browsing. Keep web browsers and add-ons up to date to add an extra layer of protection.

McAfee™
Together is power.

- Run applications as a user with limited privileges instead of with administrator rights.
- Keep the network perimeter secure. Firewalls can prevent external attackers from gaining access to internal applications that have been previously compromised by successful password-stealer attacks.
- Use enterprise authentication credentials (such as those for web proxies for Internet browsing, database applications, shared folders, etc.) only when using corporate assets. Do not allow systems in the trusted corporate network that are not distributed and certified by the corporate IT security group.
- Malware that could contain password stealers may be embedded inside legitimate software which has been Trojanized by an attacker. To prevent a successful attack of this type, we highly recommend you tighten the software delivery and distribution mechanisms. It is always a good idea to have a central repository of corporate applications from which users can download approved software.
- In case users are authorized to install applications that are not previously validated by the IT security group, educate them to install only applications with trusted signatures from known vendors. It is very common for "harmless" applications offered online to have embedded password stealers, or other malware.
- Avoid application downloads from non-web sources. The likelihood of downloading malware from Usenet groups, IRC channels, instant messaging clients, or peer to peer systems is very high. Links to websites in IRC and instant messages also frequently point to infected downloads.
- Implement an educational program to prevent phishing attacks. Password stealers are commonly distributed through phishing.

If you believe that systems have been compromised by a password stealer, some best practices will help contain the lateral movement of the infection:

- Reduce the attack surface by enabling two-factor authentication on applications that support it. The attacker may have a stolen password, but the second factor will stop the infiltration.
- Using an endpoint firewall will curtail the expansion of intrusions with stolen passwords if the infected computer has limited inbound and outbound traffic enforced by firewall rules.

## How McAfee products can protect against password-stealer attacks

### McAfee VirusScan® Enterprise 8.8 or McAfee Endpoint Security 10

- Keep endpoint antimalware software up to date with the latest patch, DAT version, and scanning engine. Ensure McAfee Global Threat Intelligence (McAfee GTI) is in use.
- Develop Access Protection rules to stop installation and payloads of malware:
  - Refer to Access Protection Rules Knowledge Base Articles: 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

Intrusion prevention tools are not effective to expose a successful password-stealer attack. However, McAfee Host Intrusion Prevention can help prevent the lateral movement of the malware payload, which may contain a password stealer.

- 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 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, use, 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, 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 sites that distribute password stealers.

### 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 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:
  - 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-the-box detection capabilities:
  - Signature-based detection: McAfee Labs malware "zoo" maintains 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 in which password-stealing malware is likely to run:
  - Common operating systems such as 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 activates the malware. Providing an analyzer profiles an Internet connection and increases the 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 password stealers.
- 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 Defense configuration is applied at the sensor level.
- Update callback detection rules (to combat botnets).

### McAfee Web Gateway

- Enable McAfee Web Gateway antimalware inspection.
- Enable McAfee 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 Threat Intelligence Exchange threat event.
- You may 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 McAfee).

### McAfee Active Response

- McAfee Active Response finds and responds to advanced threats. When used in association with threat feeds from McAfee Labs, SecureWorks, or ThreatConnect, new threats can be searched for and eliminated before they have a chance to spread.
- Custom collectors can be used to build specific tools to find and identify indicators of compromise associated with password stealers.
- 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

Phishing Attacks Employ Old but Effective Password Stealer

Fareit Virus Profile

Fareit Virus Profile

McAfee
Together is power.

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "as is," without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance. McAfee and the McAfee logo are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee LLC. 3185_0617_brf-protecting-against-password-stealers
June 2017

**McAfee**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com