GLASSWALL

Threat Intelligence Bulletin:

The Primary Role of Windows Documents in Fileless Malware Attacks – And How to Stop It

April 2019

By Lewis Henderson

Glasswall's Threat Intelligence reports exclusively on evasive malware that has managed to bypass the various security layers attempting to protect an organisation. This bulletin focusses on Fileless Malware Attacks that are one of the most effective and damaging evasive threats; they certainly paint a bleak future for those who are in a defensive position.

GLASSWALL

The Primary Role of Windows Documents in Fileless Malware Attacks – And How to Stop It

Glasswall FileTrust™ Threat Intelligence reports focus on evasive malware that bypasses the various security layers designed to protect an organization. This bulletin focuses on Fileless Malware Attacks, emerging as one of the most effective and damaging evasive threats that are painting a bleak future for those tasked with defending their organizations.

Microsoft	Malware Bytes
"File-based inspection is ineffective against fileless malware"	"…fileless malware attacks are estimated to account for 35 percent of all attacks in 2018"

Fileless Malware techniques have been around for a couple of years, but in 2018 it felt like attackers were done testing, had completed their proofs of concept and had then moved aggressively to using it as the means to deploy a number of devastating cyber-attacks.

So what is it, how does it evade defenses and what can be done to get ahead of attackers?

As the name 'Fileless' indicates, the malicious part of this multi-stage style of attack is particularly problematic to defend against because there is no file. Maybe that is a little misleading: In attacks that use email attachments, there is a file at the beginning of the process, but no malicious payload. There are just Powershell scripts that launch when a recipient opens the file. 'Fileless' refers to what happens next, since after that attachment gets opened, things get interesting…and challenging.

Scripts used in Fileless Malware Attacks are launched by macros or DDE-enabled Microsoft Office files and they all look totally legitimate and benign to AV and Sandboxes. But then it gets really clever. These Powershell scripts write instructions directly to memory, encrypted malware is downloaded, the payload executes only in memory, and once the damage is done and the attacker's objectives are achieved, it deletes any trace of its existence. In attempting to identify the source of the attack, you'll be chasing ghosts.

These attacks are specifically designed to trick users on endpoints. Preventive steps would require doing ALL of the following:

- Restrict Admin privileges
- Disallow unapproved applications
- Prevent the Run registry keys from being modified
  AND
- Apply all security patches

Unfortunately, a lot of endpoint management and security software simply can't tackle that full list simultaneously and at scale in large organizations. It is possible to specifically block Microsoft Word from running PowerShell, but doing so will also block users from any legitimate use cases, which admittedly are few and far between for normal users. Clearly these are sub-optimal options.

Fileless Malware Attacks will continue to leave organizations exposed unless innovative alternatives to traditional protection methodologies are deployed, Content Disarm and Reconstruction (CDR) is one such technology that makes the difference between a breach in the headlines or business as usual. The Glasswall FileTrust™ suite of products sanitizes content from documents that trigger Fileless Malware Attacks and stops any code from being activated, ensuring our customers are protected when they're targeted by exploits hidden and evasive threats.

In 2019, we expect to see new Fileless Malware Attacks that are even harder to stop. But should attackers shift to other file types or features, Glasswall customers will be well ahead of them.

Recommendations for Customers

ENGAGE WITH THE BUSINESS:
Raise Macro enabled legacy Word formats as a high risk

MEASURE THE RISK:
Who are sending and receiving these high risk file types?

MONITOR THE RISK:
Are trusted supply chain file high risk profile?

CONTROL THE RISK:
Configure Glasswall to sanitise Macro content from legacy Word files from unknown senders

UK: +44 (0) 203 814 3900
USA: +1 (866) 823 6652
sales@glasswallsolutions.com
glasswallsolutions.com
Glasswall Solutions Limited
@glasswallnews