[SANS ISC] Excel Recipe: Some VBA Code with a Touch of Excel4 Macro

September 23, 2021 Malware, SANS Internet Storm Center, Security Leave a comment

I published the following diary on isc.sans.edu: "*Excel Recipe: Some VBA Code with a Touch of Excel4 Macro*":

Microsoft Excel supports two types of macros. The legacy format is known as "Excel4 macro" and the new (but already used for a while) is based on VBA. We already cover both formats in many diaries. Yesterday, I spotted an interesting sample that implements... both!

The malicious file was delivered through a classic phishing email and is called "Document_195004540-Copy.xls" (SHA256:4f4e67dccb3dfc213fac91d34d53d83be9b9f97c0b75fbbce8a6d24f26549e1
The file is unknown on VT at this time. It looks like a classic trap... [Read more]

Excel4 Macro Malware SANS ISC VBA

« [SANS ISC] Malicious Calendar Subscriptions Are Back?

[SANS ISC] Keep an Eye on Your Users Mobile Devices (Simple Inventory) »

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Stay in Touch

Upcoming Events

Here is a list of events that I will attend and cover via Twitter and wrap-ups. Ping me if you want to meet! The list is regularly updated.

Recent Articles

Name *

Email *

Website

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Clipboard Swapper Delivered With Love

Popular Articles

- Keep an Eye on SSH Forwarding!
  41.7k views
- Show me your SSID's, I'll Tell Who You Are!
  40.9k views
- Sending Windows Event Logs to Logstash
  33.6k views
- Check Point Firewall Logs and Logstash (ELK) Integration
  30.5k views
- Socat, Another Network Swiss Army Knife
  29.7k views
- Forensics: Reconstructing Data from Pcap Files
  26.1k views
- dns2tcp: How to bypass firewalls or captive portals?
  24.6k views
- Vulnerability Scanner within Nmap
  20.4k views
- Bruteforcing SSH Known_Hosts Files
  20.3k views
- Bash: History to Syslog
  18.8k views

Recent Tweets

- [/dev/random] [SANS

ISC] Keep an Eye on Your Users Mobile Devices (Simple Inventory) blog.rootshell.be/2021/09/24/s...

About 9 hours ago

- [/dev/random] [SANS ISC] Excel Recipe: Some VBA Code with a Touch of Excel4 Macro blog.rootshell.be/2021/09/23/s...

September 23, 2021 11:22

- Expectations VS. Real Life #ransomware pic.twitter.com/g2GOiGFt4h

September 22, 2021 16:42

- Welcome #iOS15! 1st issue with iCloud Private Relay: when activated, I can't access my IMAPS accounts... Anyone else?

September 22, 2021 08:27

- Crazy to see how some companies (read: managers) did not realize yet that the way of working changed thanks to the #Pandemic...

September 20, 2021 08:50

Time Machine

Select Month

NVD Vulnerabilities Feed

- CVE-2021-38094 (ffmpeg) September 20, 2021
  Integer Overflow vulnerability in function filter_sobel in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.
- CVE-2021-38090 (ffmpeg) September 20, 2021
  Integer Overflow vulnerability in function filter16_roberts in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.
- CVE-2021-38091 (ffmpeg) September 20, 2021
  Integer Overflow vulnerability in function filter16_sobel in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.
- CVE-2021-38093 (ffmpeg) September 20, 2021
  Integer Overflow vulnerability in function filter_robert in

libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.

- CVE-2021-38089 (ffmpeg) September 20, 2021
  Buffer Overflow vulnerability in function config_input in libavfilter/vf_bm3d.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.
- CVE-2021-38092 (ffmpeg) September 20, 2021
  Integer Overflow vulnerability in function filter_prewitt in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.
- CVE-2021-37412 (techradar) September 15, 2021
  The TechRadar app 1.1 for Confluence Server allows XSS via the Title field of a Radar.
- CVE-2020-21127 (metinfo) September 15, 2021
  MetInfo 7.0.0 contains a SQL injection vulnerability via admin/?n=logs&c=index&a=dodel.