Analysis Report YEKk7T2avj.xlsx

Sample Name: YEKk7T2avj.xlsx
Filesize: 126305
MD5: 5f97c5ea28c0401abc093069a50aa1f8
SHA1: 15053a986dc12c9f353f4940d7d918871d337aed
SHA256: 14c58e3894258c54e12d52d0fba0aafa258222ce9223a1fdc8a946fd169d8a12
AIML: 0 **(UNKNOWN)**
Static: **(CLEAN)**
MultiAV: **(MALICIOUS)**
Dynamic Analysis Using Sandboxing: 48 **(MAL)**

MITRE ATT&CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Process Injection 1	Masquerading 3	Virtualization/Sandbox Evasion 1	Process Injection 1	Security Software Discovery 1	Process Discovery 1	Virtualization/Sandbox Evasion 1	File and Directory Discovery 1	System Information Discovery 1					
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder	Process Injection 1	Masquerading 3	OS Credential Dumping	System Information Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder	Software Packing	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Carrier Billing	Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Risk Summary

- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion

Static Summary

- Yara
- oletools

AV Engines Scan Summary

- clamav (Swf.Trojan.Rokrat-6443186-0)
- comodo
- mcafee (Generic Exploit.cp trojan)
- node32 (SWF/Exploit.CVE-2018-4878.B/Trojan)
- sophos
- microsoft (File not scanned. There might be issue in file path or something els)
- cyren (SWF/CVE-2018-4878.B!Camelot)
- kaspersky
- avast

BEHAVIOUR ANALYSIS

SYSTEM STARTUP PROCESS

-> **EXCEL.EXE** (PID: 2404, CMD: "C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" /automation -Embedding, MD5: 9A625295E52E2F220209FEEEBCEE0C46)

-> **splwow64.exe** (PID: 4888, CMD: C:\Windows\splwow64.exe 12288, MD5: 7FE20527607797A8DADE19838B8B1573)

URL ANALYSIS

FOUND URLS IN SOURCE

https://autodiscover.in/autodiscover/autodiscover.xml

@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.com.br/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.es/autodiscover/autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.uk/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.xyz/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.sg/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.com.br/autodiscover/autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.in/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.com/autodiscover/autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.it/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

http://www.dylboiler.co.kr/admincenter/files/boad/4/manager.php
@Source : activeX1.bin

https://autodiscover.xyz/autodiscover/autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.online/autodiscover/autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.com.cn/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.com/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.it/autodiscover/autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.fr/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.online/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.es/Autodiscover/Autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.com.cn/autodiscover/autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.fr/autodiscover/autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.uk/autodiscover/autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

https://autodiscover.sg/autodiscover/autodiscover.xml
@Source : excel.exe_Rules.xml.1.dr

IP ANALYSIS

IP FOUND IN SOURCE

192.168.56.1
@Source : C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE

DOMAINS ANALYSIS

DOMAIN FOUND IN SOURCE

Not Found

BEHAVIOUR

FOUND INLINED NOP INSTRUCTIONS (LIKELY SHELL OR OBFUSCATED CODE)

Filetype : Microsoft Excel 2007+

Entropy : 7.961208356093016

Trid :
@arraytag : def
Def : ['Excel Microsoft Office Open XML Format document (40004/1) 83.33%', 'ZIP compressed archi ve (8000/1) 16.67%']

Filename : YEKk7T2avj.xlsx

Submissionpath : C:\Users\user\desktop\

Filesize : 126305

Md5 : 5f97c5ea28c0401abc093069a50aa1f8

Sha1 : 15053a986dc12c9f353f4940d7d918871d337aed

Sha256 : 14c58e3894258c54e12d52d0fba0aafa258222ce9223a1fdc8a946fd169d8a12

Sha512 : 94f5d406e822a9b9ff330d8046e56a8f76a24ba6745fd90e67458c7dea94363fe0900c1db5db87d1ee9d15ddfc 8549d990cf791597ec57ebc59a200ffc3e14c3

Ssdeep : 3072:C5lW1fxM3zZcv/Bx05ieYvKrUUpUZqf6NhoaMqmzrEh:Cyq3eXBx05i5KrloqiToaM1E

Tlsh : 17C31224993D316ECDE08CBE236245D2D30475D176C2B89E2642FF0D0AD59DE3EA71D9

Preview : PK.....!.....[Content_Types].xml ...(..... ....

Ole :
@doctype : OpenXML
@olefiles : 0
@arraytag : olefile
Signature :
Archive