Malware Analysis Report

Executive Summary

This report details the analysis of a loader malware, a type of malicious software used to infiltrate devices and deliver further payloads, such as trojans or stealers. The malware was distributed through phishing emails using social engineering tactics. Once executed, the loader collects system information from the victim's device and installs additional threats. It employs advanced evasion techniques to bypass detection and persistence strategies to maintain its foothold within the infected system. Mitigation measures focus on email security, user awareness, and continuous monitoring to detect malicious activity.

General Information

Filename:	INVOICE PACKAGE LINK TO DOWNLOAD.docm
Verdict:	Malicious activity
Threats:	**Loader** A loader is malicious software that infiltrates devices to deliver malicious payloads. This malware is capable of infecting victims' computers, analyzing their system information, and installing other types of threats, such as trojans or stealers. Criminals usually deliver loaders through phishing emails and links by relying on social engineering to trick users into downloading and running their executables. Loaders employ advanced evasion and persistence tactics to avoid detection.

MIME:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
File info:	Microsoft Word 2007+
MD5:	F2D0C66B801244C059F636D08A474079
SHA1:	C62129FFF128817B5AF62AA0051C082F9992112E
SHA256:	08D4FD5032B8B24072BDFF43932630D4200F68404D7E12FFEEDA2364C8158873
SSDEEP:	384:/iMIoinwt9VRFPZ1AZy8WNxt/ZtNN6wyMDv6js2ZzoP6Yv:/7u651AQrxllN6wyMOAOUPPv

Behavior activities

MALICIOUS

Unusual execution from MS Office
WINWORD.EXE (PID: 1116)

Microsoft Office executes commands via PowerShell or Cmd
WINWORD.EXE (PID: 1116)
Malicious document has been detected
WINWORD.EXE (PID: 1116)
Starts POWERSHELL.EXE for commands execution
WINWORD.EXE (PID: 1116)

SUSPICIOUS

Obfuscated call of IEX
powershell.exe (PID: 5688)

Static information

TRiD

.docm	|	Word Microsoft Office Open XML Format document (with Macro) (53.6)
.docx	|	Word Microsoft Office Open XML Format document (24.2)
.zip	|	Open Packaging Conventions container (18)
.zip	|	ZIP compressed archive (4.1)

EXIF

ZIP

ZipRequiredVersion:	20
ZipBitFlag:	0x0006
ZipCompression:	Deflated
ZipModifyDate:	1980:01:01 00:00:00
ZipCRC:	0x7aec387e
ZipCompressedSize:	391
ZipUncompressedSize:	1453
ZipFileName:	[Content_Types].xml

XMP

Title:	-
Subject:	-
Description:	-

XML

Keywords:	-

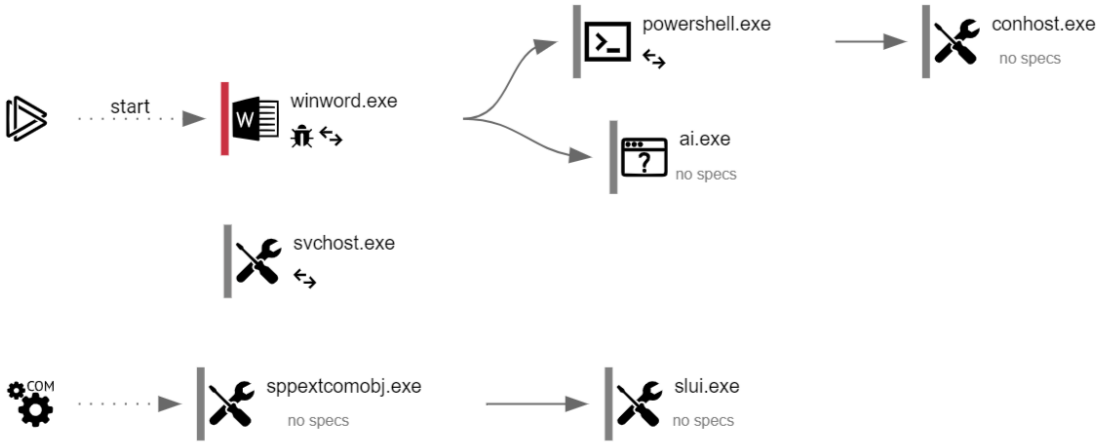
RevisionNumber:	1
CreateDate:	2021:03:13 11:14:00Z
ModifyDate:	2021:03:13 11:21:00Z
Template:	Normal.dotm
TotalEditTime:	7 minutes
Pages:	1
Words:	13
Characters:	75
Application:	Microsoft Office Word
DocSecurity:	None
Lines:	1
Paragraphs:	1
ScaleCrop:	No
Company:	-
LinksUpToDate:	No
CharactersWithSpaces:	87
SharedDoc:	No
HyperlinksChanged:	No
AppVersion:	16

File Preview

INVOICE PACKAGE LINK TO DOWNLOAD

in order to view the content, please enable the macro

Behavior graph



Process information

PID	CMD	Path	Parent process
1116	"C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\admin\AppData\Local\Temp\INVOICE PACKAGE LINK TO DOWNLOAD.docm" /o ""	C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE	explorer.exe

Information

User:
admin

Company:
Microsoft Corporation

Integrity Level:
MEDIUM

Description:
Microsoft Word

Version:
16.0.16026.20146

Files activity

Executable files-11 Suspicious files-121 Text files-39 Unknown types-2

Network activity

HTTP(S) requests-15 TCP/UDP connections-116 DNS requests-29 Threats-0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size
1328	svchost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–
1116	WINWORD.EXE	GET	200	23.53.40.178:80	http://crl.microsoft.com/pki/crl/products/MicCodSigPCA_08-31-2010.crl	unknown	–	–
1116	WINWORD.EXE	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHI3O1J0%3D	unknown	–	–
1116	WINWORD.EXE	GET	200	23.53.40.178:80	http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl	unknown	–	–
4196	svchost.exe	GET	200	23.52.120.96:80	http://www.microsoft.com/pkiops/crl/MicS	unknown	–	–

					ecSerCA2011_2011-10-18.crl			
—	—	GET	200	23.52.120.96:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	—	—
2120	MoUsoCoreWorker.exe	GET	200	23.52.120.96:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	—	—
1116	WINWORD.EXE	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEA77flR%2B3w%2FxBpruV2lte6A%3D	unknown	—	—
2476	SIHClient.exe	GET	200	23.52.120.96:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	—	—
2476	SIHClient.exe	GET	200	23.52.120.96:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—
1116	WINWORD.EXE	GET	200	23.53.40.178:80	http://crl.microsoft.com/pki/crl/products/MicrosoftTimeStampPCA.crl	unknown	—	—
1116	WINWORD.EXE	GET	200	23.52.120.96:80	http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl	unknown	—	—
1116	WINWORD.EXE	GET	200	23.53.40.178:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	—	—
1116	WINWORD.EXE	GET	200	23.53.40.178:80	http://crl.microsoft.com/pki/crl/products/MicTimStaPCA_2010-07-01.crl	unknown	—	—
2508	backgroundTaskHost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHl3O1J0%3D	unknown	—	—

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3888	svchost.exe	239.255.255.250:1900	—	—	—	whitelisted
7116	svchost.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:137	—	—	—	whitelisted

—	—	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
2120	MoUsoCoreWorker.exe	23.52.120.96:80	www.microsoft.com	AKAMAI-AS	DE	unknown
4196	svchost.exe	23.52.120.96:80	www.microsoft.com	AKAMAI-AS	DE	unknown
—	—	23.52.120.96:80	www.microsoft.com	AKAMAI-AS	DE	unknown
1116	WINWORD.EXE	52.109.89.18:443	officeclient.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	unknown
1116	WINWORD.EXE	52.113.194.132:443	ecs.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
1116	WINWORD.EXE	52.109.76.243:443	roaming.officeapps.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
1116	WINWORD.EXE	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
1116	WINWORD.EXE	23.53.40.169:443	omex.cdn.office.net	Akamai International B.V.	DE	unknown
3260	svchost.exe	40.113.103.199:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
1328	svchost.exe	20.190.159.68:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
1328	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
1116	WINWORD.EXE	23.213.164.137:443	fs.microsoft.com	AKAMAI-AS	DE	unknown
2032	svchost.exe	23.213.166.81:443	go.microsoft.com	AKAMAI-AS	DE	unknown
1116	WINWORD.EXE	52.111.243.8:443	messaging.engagement.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	unknown
1116	WINWORD.EXE	52.109.32.47:443	nleditor.osi.office.net	MICROSOFT-CORP-MSN-AS-BLOCK	GB	unknown
5688	powershell.exe	188.114.97.3:443	filetransfer.io	CLOUDFLARENET	NL	unknown
1116	WINWORD.EXE	13.89.179.10:443	self.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2476	SIHClient.exe	20.12.23.50:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
2476	SIHClient.exe	23.52.120.96:80	www.microsoft.com	AKAMAI-AS	DE	unknown
2476	SIHClient.exe	13.95.31.18:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
1116	WINWORD.EXE	23.53.43.59:443	metadata.templates.cdn.office.net	Akamai International B.V.	DE	unknown
1116	WINWORD.EXE	23.53.41.242:443	binaries.templates.cdn.office.net	Akamai International B.V.	DE	unknown
1116	WINWORD.EXE	23.53.40.178:80	crl.microsoft.com	Akamai International B.V.	DE	unknown
1116	WINWORD.EXE	23.52.120.96:80	www.microsoft.com	AKAMAI-AS	DE	unknown
4324	svchost.exe	4.231.128.59:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
2508	backgroundTaskHost.exe	20.223.35.26:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
2508	backgroundTaskHost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
7116	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	4.231.128.59 20.73.194.208	whitelisted
google.com	142.250.185.78	whitelisted
www.microsoft.com	23.52.120.96	whitelisted
officeclient.microsoft.com	52.109.89.18	whitelisted
ecs.office.com	52.113.194.132	whitelisted
roaming.officeapps.live.com	52.109.76.243	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted
omex.cdn.office.net	23.53.40.169 23.53.41.90	whitelisted
client.wns.windows.com	40.113.103.199	whitelisted
login.live.com	20.190.159.68 40.126.31.69 20.190.159.2 20.190.159.4 40.126.31.71 20.190.159.64 20.190.159.23 40.126.31.67	whitelisted
fs.microsoft.com	23.213.164.137	whitelisted
go.microsoft.com	23.213.166.81	whitelisted
messaging.engagement.office.com	52.111.243.8	whitelisted
messaging.lifecycle.office.com	52.111.243.8	whitelisted
nleditor.osi.office.net	52.109.32.47 52.109.32.38 52.109.32.39 52.109.32.46	whitelisted
filetransfer.io	188.114.97.3 188.114.96.3	unknown
self.events.data.microsoft.com	13.89.179.10	whitelisted
slscr.update.microsoft.com	20.12.23.50	whitelisted
fe3cr.delivery.mp.microsoft.com	13.95.31.18	whitelisted
metadata.templates.cdn.office.net	23.53.43.59 23.53.43.83	whitelisted
binaries.templates.cdn.office.net	23.53.41.242 23.53.42.8	whitelisted
crl.microsoft.com	23.53.40.178 23.53.40.176	whitelisted
arc.msn.com	20.223.35.26	whitelisted
fd.api.iris.microsoft.com	20.223.35.26	whitelisted

Threats

PID	Process	Class	Message
2256	svchost.exe	Potentially Bad Traffic	ET INFO Commonly Abused File Sharing Domain in DNS Lookup (filetransfer .io)
5688	powershell.exe	Potentially Bad Traffic	ET INFO Commonly Abused File Sharing Domain (filetransfer .io in TLS SNI)

Recommendations

Strengthen Defense-in-Depth Strategies:

- **Email Security Enhancements**:
  - Implement Advanced Threat Protection (ATP) to block malicious attachments and links.
  - Utilize sandboxing technologies to detonate and inspect attachments before delivering them to the end-user.
- **Endpoint Detection & Response (EDR)**:
  - Deploy EDR solutions to detect and block suspicious behavior in real-time, such as unauthorized PowerShell execution or unusual process creations.
  - Regularly update endpoint security solutions with the latest malware signatures and behavioral analysis data.
- **Network Segmentation**:
  - Implement network segmentation to isolate critical infrastructure from end-user environments, reducing the risk of malware spreading laterally.

User Awareness and Training:

- **Phishing Simulation**: Conduct regular phishing simulations to test employee awareness and ensure they can identify and report suspicious emails.
- **Security Awareness Programs**: Provide ongoing training to help users recognize suspicious behavior such as unsolicited email attachments or requests for sensitive information.

Advanced Monitoring & Logging:

- **SIEM (Security Information and Event Management) Solutions**:
  - Integrate SIEM tools to monitor, correlate, and analyze logs from across the network and endpoints in real-time.

    - Set up alerts for key indicators of compromise (IoCs) related to the malware, such as PowerShell command execution or unauthorized network connections.
- **DNS Traffic Monitoring**:
    - Enable DNS logging and filtering to detect domain name queries to known malicious domains. Use threat intelligence feeds to flag and block these queries.

Threat Hunting and Incident Response:

- **Proactive Threat Hunting**: Set up proactive threat hunting activities to look for indicators of compromise (IOCs) tied to the malware or other emerging threats in the environment.
- **Incident Response (IR) Playbook**: Create or update incident response playbooks specific to malware attacks. Include step-by-step actions such as containment, eradication, and recovery measures.

Patching and Vulnerability Management:

- **Patch Management**: Ensure all systems, including operating systems and third-party applications like Office, Adobe Reader, and browsers, are up to date with the latest security patches.
- **Vulnerability Scanning**: Implement regular vulnerability scans to identify and remediate unpatched systems that could be exploited by the malware or similar threats.

Disable Macros by Default:

- Ensure that macros are **disabled by default** in Office applications, and only enable them for trusted documents.
- Consider deploying **Group Policy settings** to block macros in documents downloaded from the internet or from untrusted sources.

Backup and Recovery:

- **Frequent Backups**: Ensure regular backups of critical data are performed and stored offline or in a secure, segregated environment.
- **Backup Testing**: Periodically test backup restoration processes to confirm data can be reliably recovered in the event of a ransomware attack or malware-induced corruption.

Zero Trust Architecture:

- **Zero Trust Implementation**: Adopt a Zero Trust model, where each user and device must be authenticated and authorized, regardless of their location within the network.
- **Least Privilege Access**: Apply the principle of least privilege, ensuring users and applications only have the access they absolutely need, reducing the impact if a user is compromised.

Review and Strengthen Remote Access Policies:

- **Multi-Factor Authentication (MFA)**: Ensure MFA is enabled for all remote access, particularly for services like VPNs and RDP (Remote Desktop Protocol).
- **Conditional Access Policies**: Implement conditional access policies based on user behavior, device health, or geographic location to prevent unauthorized access.

Review and Update Incident Response Plan:

- Develop and regularly update an incident response plan to quickly respond to similar threats.
- Perform post-incident reviews to learn from each event and update policies accordingly.