MALICIOUS

Classifications: Banking Trojan

Threat Names: Ursnif

Verdict Reason: -

Sample Type	**Windows DLL (x86-32)**
File Name	**e609894b274a6c42e971e8082af8fd167ade4aef5d1a3816d5acea04839f0b35.dll**
ID	#6769998
MD5	85fa54c2a97ad3a1f8bd64af62450511
SHA1	db92c0a81e8b27d222607e093ccc9d00485db119
SHA256	e609894b274a6c42e971e8082af8fd167ade4aef5d1a3816d5acea04839f0b35
File Size	592.00 KB
Report Created	2023-01-24 00:00 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (4 rules, 6 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Banking Trojan
	• Rule "Ursnif_Gen_C2_Format" from ruleset "Malware" has matched on the function strings for (process #1) hpdlipgxs.exe. • Rule "Ursnif_Gen_C2_Format" from ruleset "Malware" has matched on a memory dump for (process #1) hpdlipgxs.exe.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #1) hpdlipgxs.exe has a thread which sleeps more than 5 minutes.			
1/5	User Data Modification	Uses encryption API	1	-
	• (Process #1) hpdlipgxs.exe uses above average number of encryption APIs.			
1/5	Obfuscation	Resolves API functions dynamically	2	-
	• (Process #1) hpdlipgxs.exe resolves 135 API functions by name. • (Process #3) wmiprvse.exe resolves 77 API functions by name.			
-	Trusted	Known clean file	1	-
	• Embedded file "" is a known clean file.			

Mitre ATT&CK Matrix

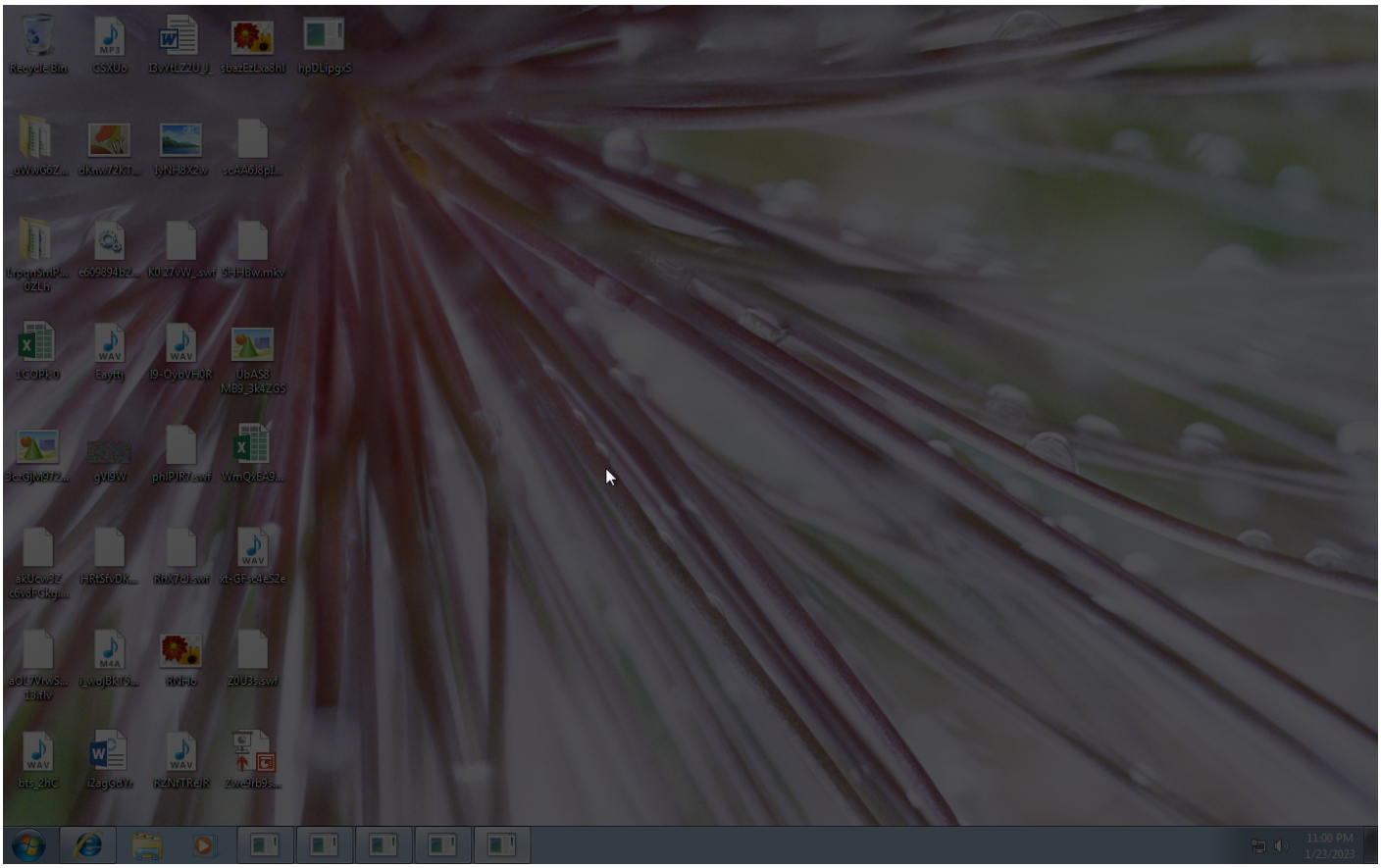
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing							

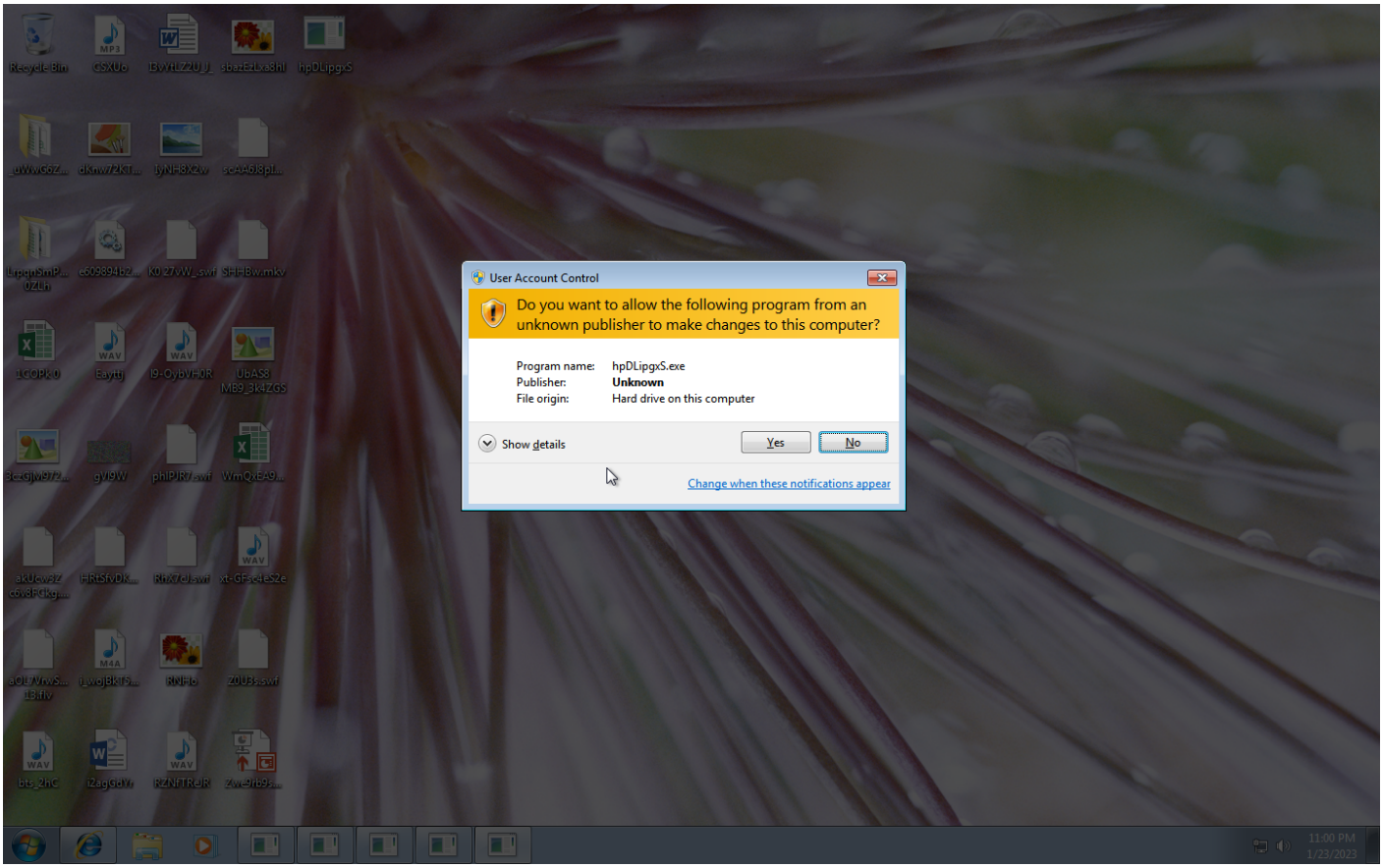
Sample Information

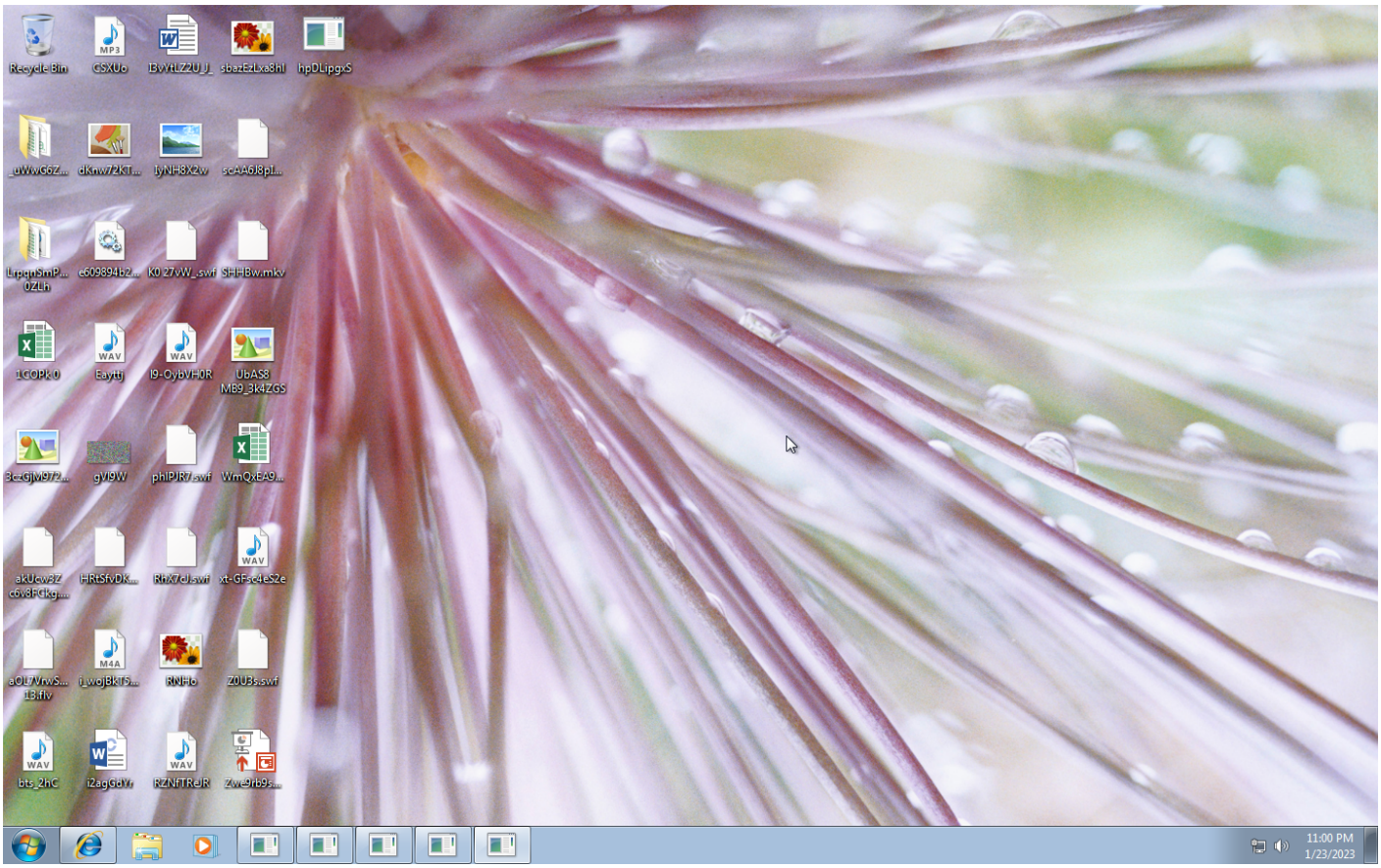
ID	#6769998
MD5	85fa54c2a97ad3a1f8bd64af62450511
SHA1	db92c0a81e8b27d222607e093ccc9d00485db119
SHA256	e609894b274a6c42e971e8082af8fd167ade4aef5d1a3816d5acea04839f0b35
SSDeep	12288:cysmuJC4fktsdyjJGL44Clz8JwsWydYo9NRl:cT7IoyjXTKdlnz
ImpHash	78b4b07ec49eab1076c53a1a1cf86078
File Name	e609894b274a6c42e971e8082af8fd167ade4aef5d1a3816d5acea04839f0b35.dll
File Size	592.00 KB
Sample Type	Windows DLL (x86-32)
Has Macros	✔

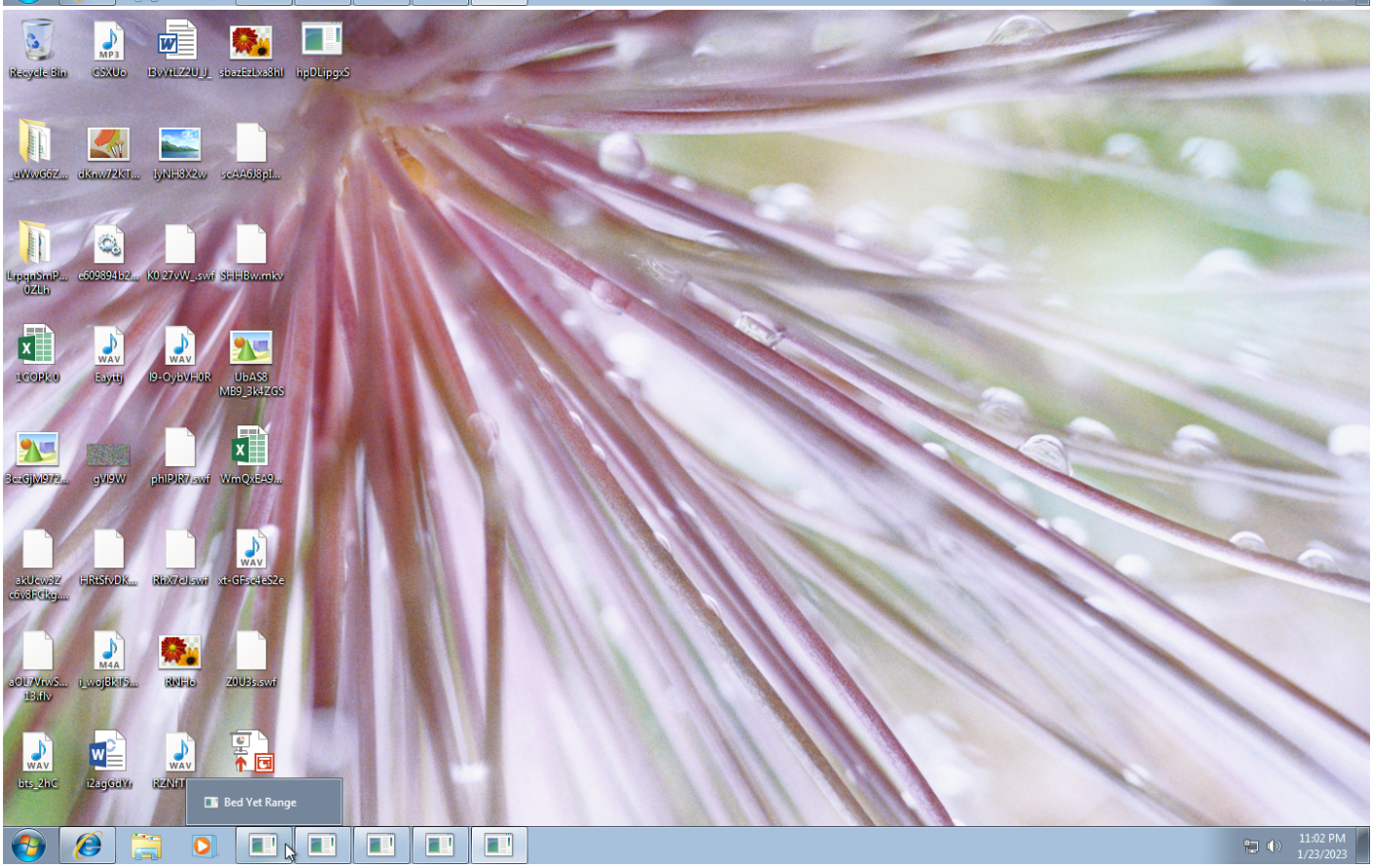
Analysis Information

Creation Time	2023-01-24 00:00 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	2




User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: hpDLipgxS.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

5.10 KB total sent

8.68 KB total received

2 ports 80, 53

5 contacted IP addresses

8 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

2 total requests returned errors

HTTP/S

7 URLs contacted, 4 servers

7 sessions, 4.94 KB sent, 8.34 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://protectioon.cdn4.mozilla.net/fonts/GFNmN_2Fv/EB_2Ff35lBSV9ApL3S13/G00GZOEr8CgP4EwtbN3/s_2FJAPFrn1C7uk3Q35fZ2/_2FODD0k3TH2G/... .../tvhdghxhwrnXxzKs/mOPzS1lFDfKozh2/s5luF_2B9XJC17m8rz/dS5t8BRD5/NYmPJyeFBNTn_2BWZJqY/U4n0QAEAHOesDgNVXEl/8TzOlXbGz2uqAgrLT/r_2F.bak	-	-		0 bytes	NA
GET	http://protectioon.cdn4.mozilla.net/fonts/isRVJBv0mXSMa2Ji_2F/GT82FMxGoymkAZ3E_2BNb5/YriH7PZEE1caw/WrKjEwg8/xdPtbXs4_2FisFBMWyUFwI... ...fYuCXx9PE/f74q9Grv2cO3R0JbpB/39D78cO3N/w032fpABBDDcRw2d50Uk/pmbTrlDBV3w8iuVmDFf/dg9FpqHt2l7yiqYCtC5Sqn/im_2B8JDZcDyHJ67E/f_2Bz.bak	-	-		0 bytes	NA
GET	http://protectioon.cdn4.mozilla.net/fonts/5lPJZCWvu_2FSlFe3sg0/SfpJ_2Fw87KnDk4pxI6/uM9uh5TWjfwKZS3l2AnPIU/IGG0VzmwR3UdR/JOGZv9Ly/1... ...uCTOp/pQTZW6fSMQGINNG/gL3gPJ1GlAg9A5Fuah/oOgIOZAIE/BF_2FVS8Vb0nC36_2Fr_/2F8HbGQ_2FpwvePkBZQ/NRS92Zc5auHhOwt07hfydG/_2Fe1VCXj/5.bak	-	-		0 bytes	NA
GET	http://protectioon.cdn4.mozilla.net/fonts/wIGcS0YfmDDIfDzUwG/1Cd4dnsAO/K7aWTy6svk4_2FY6Jpfs/Tsil0VJchR3VcH7dOWM/O96BotPUs4wYb5cwcL... ...9Ci1x/ihS7H0laDo1v6HVOnCV46/2ho918HxZXDeYyyK/ntwqEOazxTX8GJk/lyyx6rojyJ_2BiKZll/aTpQUK9Ur/Ccq58iKeFIzpNZqywwyz/N2sHckONr_2/FkJ.bak	-	-		0 bytes	NA
GET	http://trackingg-protectioon.cdn4.mozilla.net/fonts/L3wYuAHI2rRuLwvILLog81/z8ABmqSJCyFQY/dz32cLsE/FIlmf3Di1_2BAKEcPKjfN5L/DYWtPUwT... ...5OcYpdFmO/d_2FCoisB/Eyc1JOyN6ncqTV6_2Ff_/2BPeQp3fqrucB91i4Me/3ZSAryawWqX0NuyeeCGRDe/wpWiBTDHlWj7r/2F3dLkmE/ILI56iRQE5_2Bq5/OZS.bak	-	-		0 bytes	NA
GET	http://trackingg-protectioon.cdn4.mozilla.net/fonts/anvl4DF57tb/vO3Ek6luLQbT8h/JCj0Cwe5R_2FsSEW_2F6m/AdqS_2FBQBTM3A38/e16lxOdem_2F... ...VOTpMLOHoXai/9eH1oFs5el/mjlJCAa7Te7xSKclV/A3itFTqdSvr6/bMZ2mKJNhDP/nfDlpWVt5zhXu_/2BiWPl8pSWHhoQsLr0Vpy/L6TtA5O7rEool8FvAWp/ms.bak	-	-		0 bytes	NA

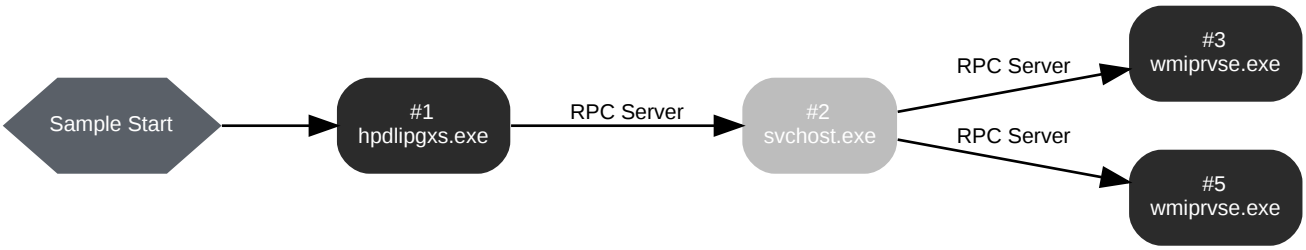
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://trackingg-protectioon.cdn4.mozilla.net/fonts/HW8zAOY4KqE_2BIBQxXqiK/_2Bgg1jsDn7Rs/cb8bpux3/NVaRJ9pAMaxXxFteTQq43_2/BASePvZI... ...1FlfqiEpdBr3N9UHoDR/EEpetG_2BDp_2BXIN_2/F9Eaoun3dHQfmur59xnuKY/rGslP6nXCrcwT/9okpWrFT/wIa7Tho_2BbO0_2BdGNglJP/Y9Xk_2Fyq/CTe_2B.bak	-	-		0 bytes	NA
GET	http://trackingg-protectioon.cdn4.mozilla.net/fonts/FFu8QJqgB45OXgFmN1i/qmUxw2HBsgltuiWx_2Ffn6/yA8FahHjwziTP/Khum2D9f/BKyX7ozBxQKl... ...VhPP/DwdQhvoLu3_2Fq15rt/R0l1huLjj/YSOT6JSN0BrR_2B0LEXN/LC53k4blksPVMK24DeD/BHKgRxewTpOp0ZG_2FDdTD/DZbFE840hFpoB/7V_2BenfrMNo/H.bak	-	-		0 bytes	NA
GET	http://80.77.23.77/fonts/RjqLyclOWEhHUdn38dGd/TJCs4UupBl44_2BJ/xC22XKe2asuLoAS/D_2FkWTlB2CPxx5z8U/OafMYpcsy/3XXWSzGHJhvkLNs7LSzA/... ...yepklAl2MJ/_2BtLKv048od/jwcGh_2FvIh/wUXbSfMuLVZlaP/DqNGioFU4Qm1m2wf_2BX9/AIMGj2dpge6b4Oxz/QdeJrRKLulJCzF5/nrAQ5KzWmBMvmgJ/xych.bak	-	-		0 bytes	NA
GET	http://80.77.25.109/fonts/8epz1t_2Fn86AmrKA6_2B0/W9YmJPHIkhA0u/bgXtp7Ab/74sKTQ7xl27y9uBY0Kym1KE/0KP9ZHZkOe/oipurPeUiJBR4hFhF/H5sWv... ...e8/3H5tTsdwnZhcNo_2FdF5/b2knUq434OgN_2F3UwS/VkjNEn0D50Bs_2Fdl_2B0C/6GuC_2F3ajDTM/VyeFrLlp/dfKml2JZpM9yiF0_2BiDzuU/oQiEg2ek3E/e.bak	-	-		0 bytes	NA
GET	http://80.77.25.109/fonts/EPT9utPC1ladvBEuonHxwK/lNcjSGbwWslTS/cLE1URuF/SvZrRnzfl4cVD6EZGIwOD7h/w_2Fh6Rfkj/aCc1q17nn_2FetFWv/rLVlo... ..._2B4t6C/adtn6wJZB/ueE9CH3hWw0flxnVXcg_/2FK3HoSlvPyqCV67J_2/F2DIbEZPX0guDzr6dMqlh5/TFCQuEuGljiH3/8lcLV2o7/8PzQAmuDCT9arsq/Maetc.bak	-	-		0 bytes	NA
GET	http://170.130.165.182/fonts/YxWT4AU8gIKfD5nz82G_2Bx/Gf1XohqLXX/TWvPpHPW4oiV4l5NF/A_2FgmLjWqql/s_2BPi8ekE0/Y4S97WsDdTOeV2/p4zvOgzH... ...2F/98OHY3kqREKLzdTlXTYbk_/2BuJAfTyqQy_2/F9TvlrYK/jP6X5ZM7HYulxceF1JwCYQZ/EQ0AjezZSs/4QJXSsnHSvkWadq0X/Le5kL4HSw_2F5qPv_/2FssgT.bak	-	-		0 bytes	NA
GET	http://80.77.23.77/fonts/zWYgGwSPxxE9nwQ_2B/i1TCRbNzT/ahU_2FdYHsT80OF0JT4x/3Libq0uC_2F2DIcpEpk/vyL0xu368G6kxNp37v4Rs2/_2BO8_2FsDBt... ...Wdsz_2FlcsBIOzbQ8/p_2Fht9nYzZfbgbA/20xdaOqNywuc2Yw/OkfLwTw7LI42xDsnAx/qAKKPknbS/kKUIpYK5h8wEg91fFMUU/TcyMVgY5ouZuMpreVtl/FHg8l.bak	-	-		0 bytes	NA
GET	http://80.77.25.114/fonts/mHtZyjI0/Iw6fkq0l08toJRZty2tDaiJ/4jQnUzz6uR/_2FafMnyZ6W1khq_2/BQkGIs95Yx3t/ImqphNUXfCV/EuuOqWDRoZCpN3/qv... ...L/N7W3NcEQJ4Kwt0zDjCU/ZG8sa_2FTT7PsDpO0cGczi/K4nD3eZHnHw4T/5zzRwOli/JDc8olgeEdux2SUumV3FIZU/Gyhb2_2BWC/mQseCoK0QJ2dktFxd/D2pcj.bak	-	-		0 bytes	NA
GET	http://170.130.165.182/fonts/f0VSlh4ZY0Jd0FgWTdUdOzU/h8l_2F5ZNl/w3MzTlY17IDO7mrj_/2FGXddeQjt1X/rj5Bf8MKPfL/_2Fr3r2T3BFijF/742_2B_2... ...8zvtcfZ5HqpTT3uP4RtWr_/2FoZU_2F6_2B7/fM8tUsXU/VO76RHiFe2N7vu_2FRVTaHH/_2BcRPm9uL/9mO_2FWPwGjOS6kHE/nwd3tRU0QlpM/zjxeettI7CY/Sz.bak	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	protectioon.cdn4.mozilla.net	NX_DOMAIN			NA
A	trackingg-protectioon.cdn4.mozilla.net	NX_DOMAIN			NA

BEHAVIOR

Process Graph



Process #1: hpdlipgxs.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\hpdlipgxs.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\hpDLipgxS.exe" /dll="C:\Users\KEECFM~1\Desktop\e609894b274a6c42e971e8082af8fd167ade4aef5d1a3816d5acea04839f0b35.dll"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 38460, Reason: Analysis Target
Unmonitor End Time	End Time: 278533, Reason: Terminated by timeout
Monitor duration	240.07s
Return Code	Unknown
PID	3800
Parent PID	1888
Bitness	32 Bit

Host Behavior

Type	Count
System	240
Module	232
File	3
Environment	1
-	42
User	42
COM	1
-	25

Network Behavior

Type	Count
HTTP	15
TCP	8

Process #2: svchost.exe

ID	2
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 46745, Reason: RPC Server
Unmonitor End Time	End Time: 278533, Reason: Terminated by timeout
Monitor duration	231.79s
Return Code	Unknown
PID	872
Parent PID	3800
Bitness	64 Bit

Process #3: wmiprvse.exe

ID	3
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 46745, Reason: RPC Server
Unmonitor End Time	End Time: 278533, Reason: Terminated by timeout
Monitor duration	231.79s
Return Code	Unknown
PID	3180
Parent PID	872
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	83
System	28
Registry	3
File	2

Process #5: wmiprvse.exe

ID	5
File Name	c:\windows\syswow64\wbem\wmiprvse.exe
Command Line	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 48001, Reason: RPC Server
Unmonitor End Time	End Time: 128121, Reason: Terminated
Monitor duration	80.12s
Return Code	0
PID	3852
Parent PID	872
Bitness	32 Bit

Host Behavior

Type	Count
System	8
Mutex	1
Module	23
Registry	17
File	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e609894b274a6c42e971e8082af8fd167ade4aef5d1a3816d5acea04839f0b35	C:\Users\kEecfMwgj\Desktop\e609894b274a6c42e971e8082af8fd167ade4aef5d1a3816d5acea04839f0b35.dll, C:\Users\KEECFM~1\Desktop\e609894b274a6c42e971e8082af8fd167ade4aef5d1a3816d5acea04839f0b35.dll	Sample File	592.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
d4651721750d35d493fb1633e237700022bd849fa123164790b168b8318acb090	-	Downloaded File	548 bytes	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\e609894b274a6c42e971e8082af8fd167ade4aef5d1a3816d5acea04839f0b35.dll	Accessed File, Sample File	Access	MALICIOUS
C:\Windows\system32\OemLogo.Bmp	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\hpDLipgxS.exe	Accessed File	Access	CLEAN
c:\lsarpc	Dropped File, Modified File	-	CLEAN
c:\srvsvc	Dropped File, Modified File	-	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\system32\WBEM\Logs\	Accessed File	Access	CLEAN
\??\C:\Windows\system32\OemInfo.Ini	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://80.77.25.109/fonts/EPT9utPC1ladvBEuonHxwK/INcjSGbwWslTS/cLE1URuF/SvZrRnzfl4cVD6EZGIwOD7h/w_2Fh6Rfkj/aCc1q17nn_2FetFWv/rLVIo.../_2B4t6C/adtn6wJZB/ueE9CH3hWw0flxnVXcg_/2FK3HoSlvPyqCV67J_2/F2DIbEZPX0guDzr6dMqlh5/TFCQuEuGljiH3/8lcLV2o7/8PzQAmuDCT9arsq/Maetc.bak	-	80.77.25.109	-	GET	CLEAN
http://170.130.165.182/fonts/f0VSlh4ZY0Jd0FgWTdUdOzU/h8l_2F5ZNI/w3MzTlY17lDO7mrj_/2FGXddeQjt1X/rj5Bf8MKPfL/_2Fr3r2T3BFijF/742_2B_2... ...8zvtcfZ5HqpTT3uP4RtWr_/2FoZU_2F6_2B7/fM8tUsXU/VO76RHiFe2N7vu_2FRVTaHH/_2BcRPm9uL/9mO_2FWPwGjOS6kHE/nwd3tRU0QlpM/zjxeettI7CY/Sz.bak	-	170.130.165.182	-	GET	CLEAN
http://trackingg-protectioon.cdn4.mozilla.net/fonts/anvl4DF57tb/vO3Ek6luLQbT8h/JCj0Cwe5R_2FsSEW_2F6m/AdqS_2FBQBTM3A38/e16lxOdem_2F.../VOTpMLOHoXai/9eH1oFs5el/mjlJCAa7Te7xSKcIV/A3itFTqdSvr6/bMZ2mKJNhDP/nfDIpWVt5zhXu_/2BiWPl8pSWHhoQsLr0Vpy/L6TtA5O7rEool8FvAWp/ms.bak	-	-	-	-	CLEAN
http://trackingg-protectioon.cdn4.mozilla.net/fonts/FFu8QJqgB45OXgFmN1i/qmUxw2HBsgltuiWx_2Ffn6/yA8FahHjwziTP/Khum2D9f/BKyX7ozBxQKl... ...VhPP/DwdQhvoLu3_2Fq15rt/R0l1huLjj/YSOT6JSN0BrR_2B0LEXN/LC53k4blksPVMK24DeD/BHKgRxewTpOp0ZG_2FDdTD/DZbFE840hFpoB/7V_2BenfrMNo/H.bak	-	-	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://80.77.23.77/fonts/zWYgGwSPxxE9nwQ_2B/i1TCRbNzT/ahU_2FdYHsT80OF0JT4x/3Libq0uC_2F2DIcpEpk/vyL0xu368G6kxNp37v4Rs2/_2BO8_2FsDBt...Wdsz_2FlcsBIOzbQ8/p_2Fht9nYzZfbgbA/20xdaOqNywuc2Yw/OkfLwTw7Ll42xDsnAx/qAKKPknbS/kKUIpYK5h8wEg91fFMUU/TcyMVgY5ouZuMpreVtl/FHg8l.bak	-	80.77.23.77	-	GET	CLEAN
http://80.77.25.109/fonts/8epz1t_2Fn86AmrKA6_2B0/W9YmJPHIkhA0u/bgXtp7Ab/74sKTQ7xl27y9uBY0Kym1KE/0KP9ZHZkOe/oipurPeUiJBR4hFhF/H5sWv...e8/3H5tTsdwnZhcNo_2FdF5/b2knUq434OgN_2F3UwS/VkjNEn0D50Bs_2Fdl_2B0C/6GuC_2F3ajDTM/VyeFrLlp/dfKml2JZpM9yiF0_2BiDzuU/oQiEg2ek3E/e.bak	-	80.77.25.109	-	GET	CLEAN
http://trackingg-protectioon.cdn4.mozilla.net/fonts/HW8zAOY4KqE_2BIBQxXqiK/_2Bgg1jsDn7Rs/cb8bpux3/NVaRJ9pAMaxXxFteTQq43_2/BASePvZI... ...1FlfqiEpdBr3N9UHoDR/EEpetG_2BDp_2BXIN_2/F9Eaoun3dHQfmur59xnuKY/rGsIP6nXCrcwT/9okpWrFT/wIa7Tho_2BbO0_2BdGNgIJP/Y9Xk_2Fyq/CTe_2B.bak	-	-	-	-	CLEAN
http://protectioon.cdn4.mozilla.net/fonts/isRVJBv0mXSMa2Ji_2F/GT82FMxGoymkAZ3E_2BNb5/YriH7PZEE1caw/WrKjEwg8/xdPtbXs4_2FisFBMWyUFwI... ...fYuCXx9PE/f74q9Grv2cO3R0JbpB/39D78cO3N/w032fpABBDDcRw2d50Uk/pmbTrIDBV3w8iuVmDFf/dg9FpqHt2l7yiqYCtC5Sqn/im_2B8JDZcDyHJ67E/f_2Bz.bak	-	-	-	-	CLEAN
http://trackingg-protectioon.cdn4.mozilla.net/fonts/L3wYuAHI2rRuLwvILLog81/z8ABmqSJCyFQY/dz32cLsE/FIlmf3Di1_2BAKEcPKjfN5L/DYWtPUwT... ...5OcYpdFmO/d_2FCoisB/Eyc1JOyN6ncqTV6_2Ff_/2BPeQp3fqrucB91i4Me/3ZSAryawWqX0NuyeeCGRDe/wpWiBTDHIWj7r/2F3dLkmE/ILI56iRQE5_2Bq5/OZS.bak	-	-	-	-	CLEAN
http://protectioon.cdn4.mozilla.net/fonts/5IPJZCWvu_2FSlFe3sg0/SfpJ_2Fw87KnDk4pxI6/uM9uh5TWjfwKZS3l2AnPIU/IGG0VzmwR3UdR/JOGZv9Ly/1... ...uCTOp/pQTZW6fSMQGINNG/gL3gPJ1GlAg9A5Fuah/oOgIOZAIE/BF_2FVS8Vb0nC36_2Fr_/2F8HbGQ_2FpwvePkBZQ/NRS92Zc5auHhOwt07hfydG/_2Fe1VCXj/5.bak	-	-	-	-	CLEAN
http://protectioon.cdn4.mozilla.net/fonts/GFNmN_2Fv/EB_2Ff35lBSV9ApL3S13/G00GZOEr8CgP4EwtbN3/s_2FJAPFrn1C7uk3Q35fZ2/_2FODD0k3TH2G/... .../tvhdghxhwrnXxzKs/mOPzS1IFDfKozh2/s5luF_2B9XJC17m8rz/dS5t8BRD5/NYmPJyeFBNTn_2BWZJqY/U4n0QAEAHOesDgNVXEl/8TzOIXbGz2uqAgrLT/r_2F.bak	-	-	-	-	CLEAN
http://80.77.25.114/fonts/mHtZyjI0/lw6fkq0l08toJRZty2tDaiJ/4jQnUzz6uR/_2FafMnyZ6W1khq_2/BQkGIs95Yx3t/ImqphNUXfCV/EuuOqWDRoZCpN3/qv... ...L/N7W3NcEQJ4Kwt0zDjCU/ZG8sa_2FTT7PsDpO0cGczi/K4nD3eZHnHw4T/5zzRwOli/JDc8olgeEdux2SUumV3FIZU/Gyhb2_2BWC/mQseCoK0QJ2dktFxd/D2pcj.bak	-	80.77.25.114	-	GET	CLEAN
http://80.77.23.77/fonts/RjqLycIiOWEhHUdn38dGd/TJCs4UupBl44_2BJ/xC22XKe2asuLoAS/D_2FkWTlB2CPxx5z8U/OafMYpcsy/3XXWSzGHJhvkLNs7LSzA/...yepklAI2MJ/_2BtLKv048od/jwcGh_2Fvlh/wUXbSfMuLVZlaP/DqNGioFU4Qm1m2wf_2BX9/AIMGj2dpge6b4Oxz/QdeJrRKLulJCzF5/nrAQ5KzWmBMvmgJ/xych.bak	-	80.77.23.77	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://protectioon.cdn4.mozilla.net/fonts/wIGcS0YfmDDIfDzUwG/1Cd4dnsAO/K7aWTy6svk4_2FY6Jpfs/Tsil0VJchR3VcH7dOWM/O96BotPUs4wYb5cwcL... ...9Ci1x/ihS7H0laDo1v6HVOnCV46/2ho918HxZXDeYyyK/ntwqEOazxTX8GJk/Iyyx6rojyJ_2BiKZll/aTpQUK9Ur/Ccq58iKeFIzpNZqywwyz/N2sHckONr_2/FkJ.bak	-	-	-	-	CLEAN
http://170.130.165.182/fonts/YxWT4AU8gIKfD5nz82G_2Bx/Gf1XohqLXX/TWvPpHPW4oiV4l5NF/A_2FgmLjWqql/s_2BPi8ekE0/Y4S97WsDdTOeV2/p4zvOgzH...2F/98OHY3kqREKLzdTlXTYbk_/2BuJAfTyqQy_2/F9TvlrYK/jP6X5ZM7HYulxceF1JwCYQZ/EQ0AjezZSs/4QJXSsnHSvkWadq0X/Le5kL4HSw_2F5qPv_/2FssgT.bak	-	170.130.165.182	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
protectioon.cdn4.mozilla.net	-	-	-	CLEAN
trackingg-protectioon.cdn4.mozilla.net	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
80.77.25.114	-	Germany	HTTP, TCP	CLEAN
80.77.23.77	-	Germany	HTTP, TCP	CLEAN
80.77.25.109	-	Germany	HTTP, TCP	CLEAN
170.130.165.182	-	United States	HTTP, TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	access	wmiprvse.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version	read, access	wmiprvse.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main	access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer	access	wmiprvse.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\IE10RunOnceLastShown	access, write	wmiprvse.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\IE8RunOnceLastShown_TIMESTAMP	access, write	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management	access	wmiprvse.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\IE8RunOnceLastShown	access, write	wmiprvse.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\IE10RunOnceLastShown_TIMESTAMP	access, write	wmiprvse.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\Check_Associations	access, write	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM	access, create	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM\EnableObjectValidation	read, access	wmiprvse.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PagingFiles	read, access	wmiprvse.exe	CLEAN

Process

Process Name	Commandline	Verdict
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
hpdlipgxs.exe	"C:\Users\kEecfMwgj\Desktop\hpDLipgxS.exe" /dll="C:\Users\KEECFM~1\Desktop\e609894b274a6c42e971e8082af8fd167ade4aef5d1a3816d5acea04839f0b35.dll"	CLEAN
wmiprvse.exe	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	Ursnif_Gen_C2_Format	C2 format string of multiple Ursnif variants	Function Strings	-	Banking Trojan	5/5
Malware	Ursnif_Gen_C2_Format	C2 format string of multiple Ursnif variants	Memory Dump	-	Banking Trojan	5/5

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.7.1
Dynamic Engine Version	4.7.1 / 11/21/2022 04:40
Static Engine Version	4.7.1.0 / 2022-11-21 03:00:41
AV Exceptions Version	4.7.2.20 / 2022-12-15 11:43:19
Link Detonation Heuristics Version	4.7.2.20 / 2022-12-15 11:43:19
Smart Memory Dumping Rules Version	4.7.2.20 / 2022-12-15 11:43:19
Config Extractors Version	4.7.2.22 / 2023-01-05 11:05:11
Signature Trust Store Version	4.7.2.21 / 2023-01-03 15:44:56
VMRay Threat Identifiers Version	4.7.2.23 / 2023-01-07 18:36:42
YARA Built-in Ruleset Version	4.7.2.21

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp

System Root	C:\Windows