NCCIC NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER | US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10124171

2017-05-14

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

Three files were submitted to US-CERT for analysis. All files are confirmed as components of a ransomware campaign identified as "WannaCry", a.k.a "WannaCrypt" or ".wnCry". The first file is a dropper, which contains and runs the ransomware, propagating via the MS17-010/EternalBlue SMBv1.0 exploit. The remaining two files are ransomware components containing encrypted plug-ins responsible for encrypting the victim users files. Displayed below is a YARA signature that can be used to detect the ransomware:

```
ruleWanna_Cry_Ransomware_Generic{
meta:
      description = "Detects WannaCryRansomware on Disk and in Virtual Page"
      author = "US-CERT Code Analysis Team"
      reference = "not set"
      date = "2017/05/12"
      hash0 = "4DA1F312A214C07143ABEEAFB695D904"
strings:
      $s0 = {410044004D0049004E0024}
      $s1 = "WannaDecryptor"
      $s2 = "WANNACRY"
      $s3 = "Microsoft Enhanced RSA and AES Cryptographic"
      $s4 = "PKS"
      $s5 = "StartTask"
      $s6 = "wcry@123"
      $s7 = {2F6600002F72}
      $s8 = "unzip 0.15 Copyrigh"
      $s9 = "Global\\WINDOWS_TASKOSHT_MUTEX"
      $s10 = "Global\\WINDOWS_TASKCST_MUTEX"
      $s11 = {7461736B736368652E65786500000005461736B5374617274000000742E776E7279000069636163}
      $s12 = {6C73202E202F6772616E742045766572796F6E653A46202F54202F43202F5100617474726962202B68}
      $s13 = "WNcry@2ol7"
      $s14 = "wcry@123"
      $s15 = "Global\\MsWinZonesCacheCounterMutexA"
condition:
      $s0 and $s1 and $s2 and $s3 or $s4 and $s5 and $s6 and $s7 or $s8 and $s9 and $s10 or $s11 and $s12 or $s13 or $s14 or $s15
}
```

Files

Processed	39 0252d45ca21c8e43c9742285c48e91ad (m_chinese (simplified).wnry) 025ac29fc5b5257ca0a031de71f201bf (s.wnry) 08b9e69b57e4c9b966664f8e1c27ab09 (m_filipino.wnry) 17194003fa70ce477326ce2f6deeb270 (m_croatian.wnry) 2c5a3b81d5c4715b7bea01033367fcb5 (m_danish.wnry) 2efc3690d67cd073a9406a25005f7cea (m_chinese (traditional).wnry)

	30a200f78498990095b36f574b6e8690 (m_italian.wnry) 313e0ececd24f4fa1504118a11bc7986 (m_romanian.wnry) 35c2f97eea8819b1caebd23fee732d8f (m_finnish.wnry) 3788f91c694dfc48e12417ce93356b0f (m_indonesian.wnry) 3d59bbb5553fe03a89f817819540f469 (m_german.wnry) 3e0020fc529b1c2a061016dd2469ba96 (r.wnry) 452615db2336d60af7e2057481e4cab5 (m_russian.wnry) 4da1f312a214c07143abeeafb695d904 (4da1f312a214c07143abeeafb695d904) 4e57113a6bf6b88fdd32782a4a381274 (m_french.wnry) 4fef5e34143e646dbf9907c4374276f5 (taskdl.exe) 531ba6b1a5460fc9446946f91cc8c94b (m_turkish.wnry) 537efeecdfa94cc421e58fd82a58ba9e (m_czech.wnry) 5bef35496fcbdbe841c82f4d1ab8b7c2 (5bef35496fcbdbe841c82f4d1ab8b7c2) 5dcaac857e695a65f5c3ef1441a73a8f (t.wnry) 6735cb43fe44832b061eeb3f5956b099 (m_korean.wnry) 7a8d499407c6a647c03c4471a67eaad7 (m_dutch.wnry) 7bf2b57f2a205768755c07f238fb32cc (u.wnry) 8419be28a0dcec3f55823620922b00fa (m_vietnamese.wnry) 8495400f199ac77853c53b5a3f278f3e (taskse.exe) 86721e64ffbd69aa6944b9672bcabb6d (tasksche.exe) 8d61648d34cba8ae9d1e2a219019add1 (m_spanish.wnry) 95673b0f968c0f55b32204361940d184 (m_bulgarian.wnry) ae08f79a0d800b82fcbe1b43cdbdbefc (c.wnry) b77e1221f7ecd0b5d696cb66cda1609e (m_japanese.wnry) c17170262312f3be7027bc2ca825bf0c (b.wnry) c33afb4ecc04ee1bcc6975bea49abe40 (m_latvian.wnry) c7a19984eb9f37198652eaf2fd1ee25c (m_swedish.wnry) c911aba4ab1da6c28cf86338ab2ab6cc (m_slovak.wnry) e79d7f2833a9c2e2553c7fe04a1b63f4 (m_polish.wnry) fa948f7d8dfb21ceddd6794f2d56b44f (m_portuguese.wnry) fb4e8718fea95bb7479727fde80cb424 (m_greek.wnry) fe68c2dc0d2419b38f44d83f2fcf232e (m_english.wnry) ff70cc7c00951084175d12128ce02399 (m_norwegian.wnry)

Domains	
Identified	6 iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com gx7ekbenv2riucmf.onion 57g7spgrzlojinas.onion xxlvbrloxvriy2c5.onion 76jdd2ir2embyv47.onion cwwnhwhlz52maqm7.onion

Files

5bef35496fcbdbe841c82f4d1ab8b7c2

Details	
Name	5bef35496fcbdbe841c82f4d1ab8b7c2
Size	3723264
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	5bef35496fcbdbe841c82f4d1ab8b7c2
SHA1	50049556b3406e07347411767d6d01a704b6fee6
ssdeep	98304:wDqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3R:wDqPu1Cxcxk3ZAEUadzR8yc4gB
Entropy	7.9642512073

Antivirus	
MicroWorld-eScan	Trojan.GenericKD.5055387
nProtect	Ransom/W32.Wanna.3723264
CAT-QuickHeal	Ransom.WannaCryBot
ALYac	Trojan.Ransom.WannaCryptor
Malwarebytes	Ransom.WanaCrypt0r
AegisLab	Ml.Attribute.Gen!c
K7GW	Exploit (0050d7a31)
K7AntiVirus	Exploit (0050d7a31)
Arcabit	Trojan.Generic.D4D239B
Invincea	virtool.win32.injector.eg
Baidu	Win32.Worm.Rbot.a
Cyren	W32/Trojan.AHAZ-1193
Symantec	Ransom.Wannacry
Paloalto	generic.ml
ClamAV	Win.Trojan.Agent-6313878-0
GData	Win32.Trojan-Ransom.WannaCry.D
Kaspersky	Trojan-Ransom.Win32.Wanna.m
BitDefender	Trojan.GenericKD.5055387
NANO-Antivirus	Trojan.Win32.Wanna.eorfmq
Avast	Win32:WanaCry-A [Trj]
Rising	Ransom.FileCryptor!8.1A7 (cloud:pN1yUsg5xNU)
Ad-Aware	Trojan.GenericKD.5055387
Emsisoft	Trojan-Ransom.WanaCrypt0r (A)
Comodo	TrojWare.Win32.Ransom.WannaCryptor.a
F-Secure	Trojan.GenericKD.5055387
DrWeb	Trojan.Encoder.11432
VIPRE	Trojan.Win32.Generic!BT
TrendMicro	WORM_WCRY.A
McAfee-GW-Edition	Ransom-WannaCry!86721E64FFBD
Sophos	Troj/Wanna-E
Ikarus	Trojan.Win32.Filecoder
F-Prot	W32/WannaCrypt.D
Jiangmin	Trojan.WanaCry.i
Webroot	W32.Ransom.Wannacry
Avira	BDS/Agent.ilyda
Endgame	malicious (high confidence)
ViRobot	Trojan.Win32.S.WannaCry.3723264.I[h]
ZoneAlarm	Trojan-Ransom.Win32.Wanna.m

Microsoft	Ransom:Win32/WannaCrypt.A!rsm
AhnLab-V3	Trojan/Win32.WannaCryptor.R200572
McAfee	GenericR-JTA!5BEF35496FCB
AVware	Trojan.Win32.Generic!BT
VBA32	suspected of Trojan.Downloader.gen.h
ESET-NOD32	Win32/Exploit.CVE-2017-0147.A
Tencent	Win32.Trojan.Ransomware.Auto
SentinelOne	static engine - malicious
Fortinet	W32/WannaCryptor.D!tr
AVG	Ransom_r.CGA
Panda	Trj/RansomCrypt.I
CrowdStrike	malicious_confidence_100% (W)
Qihoo-360	Win32/Trojan.Ransom.50f
MicroWorld-eScan	Trojan.GenericKD.5055387
nProtect	Ransom/W32.Wanna.3723264
CAT-QuickHeal	Ransom.WannaCryBot
ALYac	Trojan.Ransom.WannaCryptor
Malwarebytes	Ransom.WanaCrypt0r
AegisLab	Ml.Attribute.Gen!c
K7GW	Exploit (0050d7a31)
K7AntiVirus	Exploit (0050d7a31)
Arcabit	Trojan.Generic.D4D239B
Invincea	virtool.win32.injector.eg
Baidu	Win32.Worm.Rbot.a
Cyren	W32/Trojan.AHAZ-1193
Symantec	Ransom.Wannacry
Paloalto	generic.ml
ClamAV	Win.Trojan.Agent-6313878-0
GData	Win32.Trojan-Ransom.WannaCry.D
Kaspersky	Trojan-Ransom.Win32.Wanna.m
BitDefender	Trojan.GenericKD.5055387
NANO-Antivirus	Trojan.Win32.Wanna.eorfmq
Avast	Win32:WanaCry-A [Trj]
Rising	Ransom.FileCryptor!8.1A7 (cloud:pN1yUsg5xNU)
Ad-Aware	Trojan.GenericKD.5055387
Emsisoft	Trojan-Ransom.WanaCrypt0r (A)
Comodo	TrojWare.Win32.Ransom.WannaCryptor.a
F-Secure	Trojan.GenericKD.5055387
DrWeb	Trojan.Encoder.11432
VIPRE	Trojan.Win32.Generic!BT
TrendMicro	WORM_WCRY.A
McAfee-GW-Edition	Ransom-WannaCry!86721E64FFBD
Sophos	Troj/Wanna-E
Ikarus	Trojan.Win32.Filecoder
F-Prot	W32/WannaCrypt.D
Jiangmin	Trojan.WanaCry.i
Webroot	W32.Ransom.Wannacry
Avira	BDS/Agent.ilyda
Endgame	malicious (high confidence)
ViRobot	Trojan.Win32.S.WannaCry.3723264.I[h]
ZoneAlarm	Trojan-Ransom.Win32.Wanna.m

Microsoft	Ransom:Win32/WannaCrypt.A!rsm
AhnLab-V3	Trojan/Win32.WannaCryptor.R200572
McAfee	GenericR-JTA!5BEF35496FCB
AVware	Trojan.Win32.Generic!BT
VBA32	suspected of Trojan.Downloader.gen.h
ESET-NOD32	Win32/Exploit.CVE-2017-0147.A
Tencent	Win32.Trojan.Ransomware.Auto
SentinelOne	static engine - malicious
Fortinet	W32/WannaCryptor.D!tr
AVG	Ransom_r.CGA
Panda	Trj/RansomCrypt.I
CrowdStrike	malicious_confidence_100% (W)
Qihoo-360	Win32/Trojan.Ransom.50f

PE Information

Compiled	2010-11-20T09:03:08Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	2ed157e77d0d2252c36eedfb2e2d3784	4096	0.726699793774
.text	c7613102e2ecec5dcefc144f83189153	36864	6.13459082812
.rdata	d8037d744b539326c06e897625751cc9	4096	3.50361558618
.data	22a8598dc29cad7078c291e94612ce26	159744	6.10031814517
.rsrc	aa250ba035b78129d983f27904848732	3518464	7.99522172756

Packers

Name	Version	Entry Point
Microsoft Visual C++ v6.0	NA	NA

Relationships

(F) 5bef35496fcbdbe841c82f4d1ab8b7c2 (5bef3)	Connected_To	(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
(F) 5bef35496fcbdbe841c82f4d1ab8b7c2 (5bef3)	Dropped	(F) tasksche.exe (86721)

Description

This artifact is a malicious PE32 executable that has been identified as a WannaCry ransomware dropper. Upon execution, the dropper attempts to connect to the following hard-coded URI:

http[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.

Displayed below is a sample request observed:

--Begin request—

```
GET / HTTP/1.1
Host: www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Cache-Control: no-cache
```

--End request--

If a connection is established, the dropper will terminate execution. If the connection fails, the dropper will infect the system with ransomware. When executed, the malware is designed to run as a service with the parameters “-m security”. During runtime, the malware determines the number of arguments passed during execution. If the arguments passed are less than two, the dropper proceeds to install itself as the following service:

--Begin service--

```
ServiceName = "mssecsvc2.0"
DisplayName = "Microsoft Security Center (2.0) Service"
StartType = SERVICE_AUTO_START
```

BinaryPathName = "%current directory%5bef35496fcbdbe841c82f4d1ab8b7c2.exe -m security"

--End service--

Once the malware starts as a service named mssecsvc2.0, the dropper attempts to create and scan a list of IP ranges on the local network and attempts to connect using UDP ports 137, 138 and TCP ports 139, 445. If a connection to port 445 is successful, it creates an additional thread to propigate by exploiting the SMBv1 vulnerability documented by Microsoft Security bulliten MS17-010. The malware then extracts & installs a PE32 binary from it's resource section named "R". This binary has been identified as the ransomware component of WannaCrypt. The dropper installs this binary into "C:\WINDOWS\tasksche.exe." The dropper executes tasksche.exe with the following command:

--Begin command--

"C:\WINDOWS\tasksche.exe /i"

--End command—

Note:
=====
When this sample was initially discovered, the domain "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com" was not registered, allowing the malware to run and propigate freely. However within a few days, researchers learned that by registering the domain and allowing the malware to connect, it's ability to spread was greatly reduced. At this time, all traffic to "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" is re-directed to a monitored, non-malicious server, causing the malware to terminate if it is allowed to connect. For this reason, we recommend that administrators and network security personnel not block traffic to this domain.

tasksche.exe

Details	
Name	tasksche.exe
Size	3514368
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	86721e64ffbd69aa6944b9672bcabb6d
SHA1	8897c658c0373be54eeac23bbd4264687a141ae1
ssdeep	98304:QqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3x:QqPu1Cxcxk3ZAEUadzR8yc4gB
Entropy	7.99546693739

Antivirus	
MicroWorld-eScan	Trojan.Ransom.WannaCryptor.A
nProtect	Ransom/W32.Wanna.3514368
CAT-QuickHeal	Ransom.WannaCryBot
ALYac	Trojan.Ransom.WannaCryptor
Malwarebytes	Ransom.WanaCrypt0r
K7GW	Trojan (0050d7171)
K7AntiVirus	Trojan (0050d7171)
Arcabit	Trojan.Ransom.WannaCryptor.A
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9973
F-Prot	W32/WannaCrypt.D
Symantec	Ransom.Wannacry
TrendMicro-HouseCall	Ransom_WCRY.J
Paloalto	generic.ml
ClamAV	Win.Ransomware.WannaCry-6313787-0
GData	Win32.Trojan-Ransom.WannaCry.A
Kaspersky	Trojan-Ransom.Win32.Wanna.b
BitDefender	Trojan.Ransom.WannaCryptor.A
NANO-Antivirus	Trojan.Win32.Wanna.eorfmq
AegisLab	Dropped.Generic.Ransom.Hydracrypt!c
Avast	Win32:WanaCry-A [Trj]
Tencent	Win32.Trojan.Ransome.Vdfa
Ad-Aware	Trojan.Ransom.WannaCryptor.A

Emsisoft	Trojan.Ransom.WannaCryptor.A (B)
Comodo	TrojWare.Win32.Ransom.WannaCryptor.a
F-Secure	Trojan.Ransom.WannaCryptor.A
DrWeb	Trojan.Encoder.11432
VIPRE	Trojan.Win32.Generic!BT
TrendMicro	Ransom_WCRY.J
McAfee-GW-Edition	BehavesLike.Win32.Backdoor.wc
Sophos	Mal/Wanna-A
Cyren	W32/Trojan.AHAZ-1193
Jiangmin	Trojan.WanaCry.b
Webroot	W32.Ransomware.Wcry
Avira	TR/AD.RansomHeur.aexdn
Antiy-AVL	Trojan[Ransom]/Win32.Scatter
ViRobot	Trojan.Win32.S.WannaCry.3514368.O[h]
ZoneAlarm	Trojan-Ransom.Win32.Wanna.b
Microsoft	Ransom:Win32/WannaCrypt
AhnLab-V3	Trojan/Win32.WannaCryptor.R200571
McAfee	Ransom-WannaCry!86721E64FFBD
AVware	Trojan.Win32.Generic!BT
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
Rising	Malware.Heuristic!ET#89% (cloud:vZkqDj6QDKF)
Ikarus	Trojan.Win32.Filecoder
Fortinet	W32/WannaCryptor.D!tr
AVG	Ransom_r.CFY
Panda	Trj/RansomCrypt.F
CrowdStrike	malicious_confidence_69% (W)
Qihoo-360	Win32/Trojan.Ransom.50f
MicroWorld-eScan	Trojan.Ransom.WannaCryptor.A
nProtect	Ransom/W32.Wanna.3514368
CAT-QuickHeal	Ransom.WannaCryBot
ALYac	Trojan.Ransom.WannaCryptor
Malwarebytes	Ransom.WanaCrypt0r
K7GW	Trojan (0050d7171)
K7AntiVirus	Trojan (0050d7171)
Arcabit	Trojan.Ransom.WannaCryptor.A
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9973
F-Prot	W32/WannaCrypt.D
Symantec	Ransom.Wannacry
TrendMicro-HouseCall	Ransom_WCRY.J
Paloalto	generic.ml
ClamAV	Win.Ransomware.WannaCry-6313787-0
GData	Win32.Trojan-Ransom.WannaCry.A
Kaspersky	Trojan-Ransom.Win32.Wanna.b
BitDefender	Trojan.Ransom.WannaCryptor.A
NANO-Antivirus	Trojan.Win32.Wanna.eorfmq
AegisLab	Dropped.Generic.Ransom.Hydracrypt!c
Avast	Win32:WanaCry-A [Trj]
Tencent	Win32.Trojan.Ransome.Vdfa
Ad-Aware	Trojan.Ransom.WannaCryptor.A
Emsisoft	Trojan.Ransom.WannaCryptor.A (B)
Comodo	TrojWare.Win32.Ransom.WannaCryptor.a

F-Secure	Trojan.Ransom.WannaCryptor.A
DrWeb	Trojan.Encoder.11432
VIPRE	Trojan.Win32.Generic!BT
TrendMicro	Ransom_WCRY.J
McAfee-GW-Edition	BehavesLike.Win32.Backdoor.wc
Sophos	Mal/Wanna-A
Cyren	W32/Trojan.AHAZ-1193
Jiangmin	Trojan.WanaCry.b
Webroot	W32.Ransomware.Wcry
Avira	TR/AD.RansomHeur.aexdn
Antiy-AVL	Trojan[Ransom]/Win32.Scatter
ViRobot	Trojan.Win32.S.WannaCry.3514368.O[h]
ZoneAlarm	Trojan-Ransom.Win32.Wanna.b
Microsoft	Ransom:Win32/WannaCrypt
AhnLab-V3	Trojan/Win32.WannaCryptor.R200571
McAfee	Ransom-WannaCry!86721E64FFBD
AVware	Trojan.Win32.Generic!BT
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
Rising	Malware.Heuristic!ET#89% (cloud:vZkqDj6QDKF)
Ikarus	Trojan.Win32.Filecoder
Fortinet	W32/WannaCryptor.D!tr
AVG	Ransom_r.CFY
Panda	Trj/RansomCrypt.F
CrowdStrike	malicious_confidence_69% (W)
Qihoo-360	Win32/Trojan.Ransom.50f

PE Information

Compiled	2010-11-20T09:05:05Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	d95b2ee2a80c00ca7d29c40b18c99393	4096	0.708880451742
.text	920e964050a1a5dd60dd00083fd541a2	28672	6.4042351061
.rdata	2c42611802d585e6eed68595876d1a15	24576	6.66357096841
.data	83506e37bd8b50cacabd480f8eb3849b	8192	4.45574950787
.rsrc	7e152ea77186bbe06de1f254ecd4e02e	3448832	7.99986707519

Packers

Name	Version	Entry Point
Microsoft Visual C++ v6.0	NA	NA

Relationships

(F) tasksche.exe (86721)	Related_To	(S) res11.PNG
(F) tasksche.exe (86721)	Related_To	(F) b.wnry (c1717)
(F) tasksche.exe (86721)	Related_To	(F) c.wnry (ae08f)
(F) tasksche.exe (86721)	Related_To	(F) t.wnry (5dcaa)
(F) tasksche.exe (86721)	Related_To	(F) m_bulgarian.wnry (95673)
(F) tasksche.exe (86721)	Related_To	(F) m_chinese (simplified).wnry (0252d)
(F) tasksche.exe (86721)	Related_To	(F) m_chinese (traditional).wnry (2efc3)
(F) tasksche.exe (86721)	Related_To	(F) m_croatian.wnry (17194)
(F) tasksche.exe (86721)	Related_To	(F) m_czech.wnry (537ef)
(F) tasksche.exe (86721)	Related_To	(F) m_danish.wnry (2c5a3)
(F) tasksche.exe (86721)	Related_To	(F) m_dutch.wnry (7a8d4)

(F) tasksche.exe (86721)	Related_To	(F) m_english.wnry (fe68c)
(F) tasksche.exe (86721)	Related_To	(F) m_filipino.wnry (08b9e)
(F) tasksche.exe (86721)	Related_To	(F) m_finnish.wnry (35c2f)
(F) tasksche.exe (86721)	Related_To	(F) m_french.wnry (4e571)
(F) tasksche.exe (86721)	Related_To	(F) m_german.wnry (3d59b)
(F) tasksche.exe (86721)	Related_To	(F) m_greek.wnry (fb4e8)
(F) tasksche.exe (86721)	Related_To	(F) m_indonesian.wnry (3788f)
(F) tasksche.exe (86721)	Related_To	(F) m_italian.wnry (30a20)
(F) tasksche.exe (86721)	Related_To	(F) m_japanese.wnry (b77e1)
(F) tasksche.exe (86721)	Related_To	(F) m_korean.wnry (6735c)
(F) tasksche.exe (86721)	Related_To	(F) m_latvian.wnry (c33af)
(F) tasksche.exe (86721)	Related_To	(F) m_norwegian.wnry (ff70c)
(F) tasksche.exe (86721)	Related_To	(F) m_polish.wnry (e79d7)
(F) tasksche.exe (86721)	Related_To	(F) m_portuguese.wnry (fa948)
(F) tasksche.exe (86721)	Related_To	(F) m_romanian.wnry (313e0)
(F) tasksche.exe (86721)	Related_To	(F) m_russian.wnry (45261)
(F) tasksche.exe (86721)	Related_To	(F) m_slovak.wnry (c911a)
(F) tasksche.exe (86721)	Related_To	(F) m_spanish.wnry (8d616)
(F) tasksche.exe (86721)	Related_To	(F) m_swedish.wnry (c7a19)
(F) tasksche.exe (86721)	Related_To	(F) m_turkish.wnry (531ba)
(F) tasksche.exe (86721)	Related_To	(F) m_vietnamese.wnry (8419b)
(F) tasksche.exe (86721)	Related_To	(F) r.wnry (3e002)
(F) tasksche.exe (86721)	Related_To	(F) s.wnry (025ac)
(F) tasksche.exe (86721)	Related_To	(F) taskdl.exe (4fef5)
(F) tasksche.exe (86721)	Related_To	(F) taskse.exe (84954)
(F) tasksche.exe (86721)	Related_To	(F) u.wnry (7bf2b)
(F) tasksche.exe (86721)	Dropped_By	(F) 5bef35496fcbdbe841c82f4d1ab8b7c2 (5bef3)

Description

This artifact is a malicious PE32 executable that has been identified as the WannaCrypt ransomware component, named "tasksche.exe". Installed by the dropper component during run-time, "tasksche.exe" installs itself as a service with the following attributes:

--Begin service--

ServiceName = "wipqhztnxh610"
DisplayName = "wipqhztnxh610"
BinaryPathName = "cmd.exe /c "C:\ProgramData\wipqhztnxh610\tasksche.exe""

--End service--

The malware creates the following registry key:

--Begin registry key--

HKEY_LOCAL_MACHINE
Subkey = "Software\WanaCrypt0r"
ValueName = "wd"
ValueData= "<malware working directory>"

--End registry key--

The file "tasksche.exe" contains a password protected zip archive in its resource section named "XIA". During runtime, the malware extracts the archive contents using the password "WNcry@2ol7" and installs the files on the victim's hard drive. Displayed below are the files in the archive and their functionality:

-- Begin archive file list --

msg folder: == Contains multiple user manuals on different languages in RTF file format
b.wnry == Ransom message image file used to replace user's wallpaper

c.wnry == It contains the C2 servers hidden in the network TOR:
r.wnry == It explains what has happened and how to pay the ransom
t.wnry == It has AES encrypted plug-in which is responsible for encrypting the victim users files.
s.wnry == TOR library that is imported by u.wnry
u.wnry == Interactive TOR client which will enable a victim user to submit payment to the hackers via a secure TOR session.
taskdl.exe == supportive file used to search for the string "\$RECYCLE*.WNCRYT"
taskse.exe == supportive file for Remote Desktop Services

--End archive files--

Screenshots

- **res11.PNG**

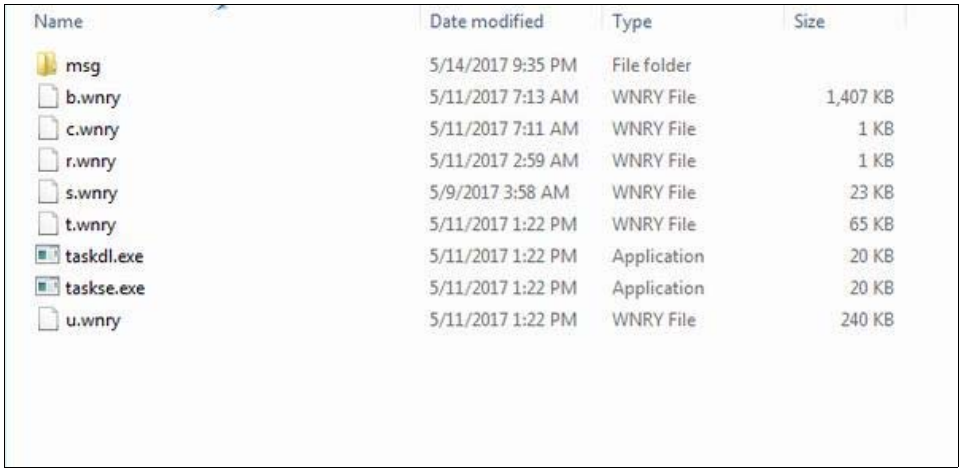

Image 2: Files contained in this embedded archive in the resource section named "XIA"

4da1f312a214c07143abeeafb695d904

Details

Name	4da1f312a214c07143abeeafb695d904
Size	4497408
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	4da1f312a214c07143abeeafb695d904
SHA1	b629f072c9241fd2451f1cbca2290197e72a8f5e
ssdeep	98304:zcI8HbSxeeqe5hXlpIyS+PiwTNl/iZ102q7O3cOtgP5HYPNtNO8 /l04miT4RTMpK:zD28tqeDNPLTmZR4Ou5H8NbOR04g5MpK
Entropy	7.99683684716

Antivirus

Bkav	W32.Clod284.Trojan.e098
MicroWorld-eScan	Trojan.GenericKD.4829301
CAT-QuickHeal	Ransom.Genasom
ALYac	Trojan.Ransom.WannaCryptor
Malwarebytes	Ransom.WannaCrypt
AegisLab	Backdoor.W32.Farfli!c
K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9995
Cyren	W32/Trojan.ZEBS-1630
Symantec	Ransom.Wannacry
ESET-NOD32	a variant of Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	Ransom_WCRY.F117DB
Paloalto	generic.ml
ClamAV	Win.Trojan.Agent-6258665-0

Kaspersky	Backdoor.Win32.Farfli.atmr
BitDefender	Trojan.GenericKD.4829301
NANO-Antivirus	Trojan.Win32.Farfli.enstjk
Avast	Win32:Malware-gen
Ad-Aware	Trojan.GenericKD.4829301
Sophos	Mal/Wanna-A
Comodo	TrojWare.JS.Trojan.Download.~
F-Secure	Trojan.GenericKD.4829301
DrWeb	Trojan.Encoder.10718
VIPRE	Trojan.Win32.Generic!BT
TrendMicro	Ransom_WCRY.F117DB
McAfee-GW-Edition	BehavesLike.Win32.Downloader.rc
Emsisoft	Trojan-Ransom.WannaCryptor (A)
F-Prot	W32/WannaCrypt.H
Jiangmin	Backdoor.Farfli.bde
Webroot	W32.Trojan.Gen
Avira	TR/Dropper.gafex
Fortinet	W32/Filecoder_WannaCryptor.B!tr
Antiy-AVL	Trojan[Backdoor]/Win32.Farfli
Endgame	malicious (high confidence)
Arcabit	Trojan.Generic.D49B075
ViRobot	Trojan.Win32.WannaCryptor.4497408[h]
ZoneAlarm	Backdoor.Win32.Farfli.atmr
Microsoft	Ransom:Win32/Genasom
AhnLab-V3	Trojan/Win32.WCrypto.R199610
McAfee	Ransom-WannaCry!4DA1F312A214
AVware	Trojan.Win32.Generic!BT
VBA32	Backdoor.Farfli
Tencent	Win32.Trojan.Raas.Auto
Yandex	Trojan.Filecoder!gRTNEfeDeo4
Ikarus	Trojan.Win32.Filecoder
GData	Trojan.GenericKD.4829301
AVG	FileCryptor.OUA
Panda	Trj/CI.A
CrowdStrike	malicious_confidence_62% (W)

PE Information

Compiled	2017-04-08T21:36:48Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	c4af8d472d9b961126c879510fc137a1	4096	0.710572941802
.text	d09045cdfcf8ee598beaf3391623aec5	28672	6.11147819166
.rdata	9ec77c0e054f493084d66f0939e94d7e	24576	6.54607243406
.data	297a4b644479ae0224207d6a96b81c49	8192	4.0949667335
.rsrc	f4b80cdf5638bcabc3292ee19e7e528f	4431872	7.9999601862

Packers

Name	Version	Entry Point
Microsoft Visual C++ v6.0	NA	NA

Relationships

(F) 4da1f312a214c07143abeeafb695d904	Related_To	(S) res22.PNG

(4da1f)		
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) b.wnry (c1717)
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) c.wnry (ae08f)
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) t.wnry (5dcaa)
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) s.wnry (025ac)
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) r.wnry (3e002)
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) u.wnry (7bf2b)

Description

This artifact is a malicious PE32 executable that has been identified as the WannaCrypt ransomware component, normally named "tasksche.exe" when dropped. The dropper component that installs this file was not part of the submission. It contains an embedded resource named "PK". This resource is a compressed archive that is protected with the password “wcr@123”. This compressed archive contains the following files:

--Begin Files Within PK Archive—
Name: b.wry
MD5: 99AE8326B4BC406DAF54DDC7C5E43ABE

Name: c.wry
MD5: 725BF255D114B71AACB9E610BB92027A

Name: m.wry
MD5: 54C0E4AA798CE82886A96BA4BB449188

Name: r.wry
MD5: 880E6A619106B3DEF7E1255F67CB8099

Name: s.wry
MD5: 7CF776F898D58F8BE1C44F254FC00643

Name: t.wry
MD5: 48099908E66D81901EB2076702AFD73C

Name: u.wry
MD5: B27F095F305CF940BA4E85F3CB848819

--End Files Within PK Archive—

During runtime, the malware decrypts the Windows DLL contained in t.wry by reading the first 8 bytes and comparing the data to the ASCII value "WANNACRY". If it matches, the malware then reads 256 bytes of the file starting at byte 12. The malware then decrypts these 256 bytes using a hard coded private RSA2 key. This produces the following 16-byte value.

--Begin 128 Bit AES Key—

896F1BB014E66A6DC5ED5DD687D305A4

--End 128 Bit AES Key—

These 16-bytes will be used by an embedded AES algorithm to decrypt the actual data contained within the encrypted file, beginning at byte 280. This reveals the embedded DLL, which will be utilized to encrypt the victim's files. It is important to note that this newly decrypted DLL contains two hard coded RSA1 keys. During the encryption process, this DLL will generate a new pseudo random AES 128-bit key for each file it encrypts.The target file is then encrypted with this AES key. Next the AES key is encrypted using the hardcoded RSA1 key and tacked to the beginning of the file. This DLL will attempt to encrypt files on the victim's primary hard drive, as well as attached physical and network drives. Encrypted files are appended with a .WCRY extension.

These encrypted files have a similar format to the file "t.wry", in that the first 8 bytes will contain the ASCII value WANNACRY. After this value there will be a four byte marker "0x00 0x01 0x00 0x00", followed by 256 bytes with the end marker "0x40 0x00 0x000x00". This marked, 256 byte sequence contains the 128 bit AES key, encrypted by RSA, which may be used to decrypt the victim's data within the file.

Screenshots

- **res22.PNG**

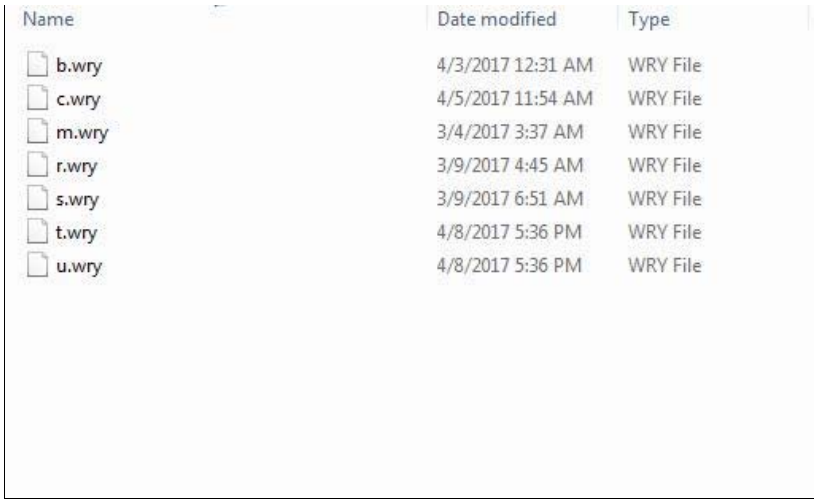

Image 3: Files contained in this embedded archive in the resource section named "PK"

---

b.wnry

Details

Name	b.wnry
Size	1440054
Type	PC bitmap, Windows 3.x format, 800 x 600 x 24
MD5	c17170262312f3be7027bc2ca825bf0c
SHA1	f19eceda82973239a1fdc5826bce7691e5dcb4fb
ssdeep	384:zYzuP4tiuOub2WuzvqOFgjexqO5XgYWTIWv/+:sbL+
Entropy	0.336339312356

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Ikarus	Trojan.Win32.Filecoder
GData	Generic.Trojan.Agent.TFW01J
Qihoo-360	Trojan.Generic
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Ikarus	Trojan.Win32.Filecoder
GData	Generic.Trojan.Agent.TFW01J
Qihoo-360	Trojan.Generic

Relationships

(F) b.wnry (c1717)	Related_To	(S) Ooops.PNG
(F) b.wnry (c1717)	Related_To	(F) tasksche.exe (86721)
(F) b.wnry (c1717)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)

Description

This file is a bitmap image file depicting the ransom message and replaces the victim's wallpaper.

Screenshots

- **Ooops.PNG**

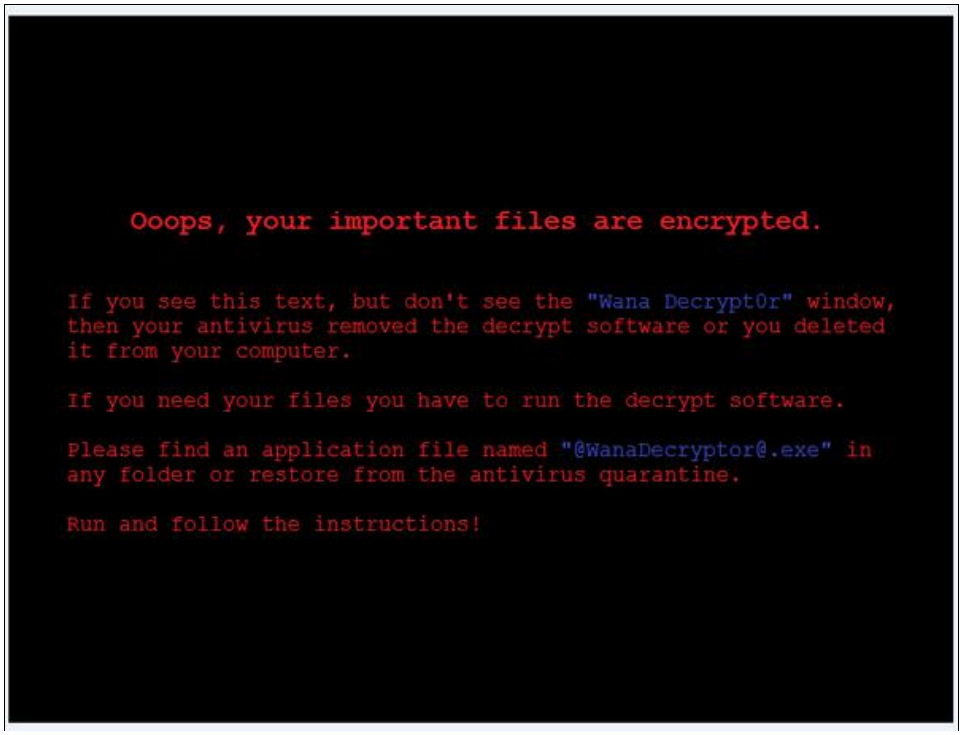

Image 1: Ransom message image file used to replace user's wallpaper

c.wnry

Details	
Name	c.wnry
Size	780
Type	data
MD5	ae08f79a0d800b82fcbe1b43cdbdbefc
SHA1	f6b08523b1a836e2112875398ffefffde98ad3ca
ssdeep	6:cL+qaHqHgVcKKfF9mHRMMPRGS37LlN/sUQqGUSGeTsdEC:cjaRVcKKfm2MYS3sUQqGLGeTEV
Entropy	1.9906166083

Antivirus	
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Microsoft	Ransom:Win32/WannaCrypt.A!rsm

Relationships

(F) c.wnry (ae08f)	Related_To	(F) tasksche.exe (86721)
(F) c.wnry (ae08f)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)
(F) c.wnry (ae08f)	Contains	(D) gx7ekbenv2riucmf.onion
(F) c.wnry (ae08f)	Contains	(D) 57g7spgrzlojinas.onion
(F) c.wnry (ae08f)	Contains	(D) xxlvbrloxvriy2c5.onion
(F) c.wnry (ae08f)	Contains	(D) 76jdd2ir2embyv47.onion
(F) c.wnry (ae08f)	Contains	(D) cwwnhwhlz52maqm7.onion

Description

This is a data file, which contains the C2 servers hidden within the TOR network. Displayed below are samples observed during analysis:

--Begin C2--

gx7ekbenv2riucmf.onion
57g7spgrzlojinas.onion
xxlvbrloxvriy2c5.onion

76jdd2ir2embyv47.onion
cwwnhwhlz52maqm7.onion

--End C2--

t.wnry

Details	
Name	t.wnry
Size	65816
Type	data
MD5	5dcaac857e695a65f5c3ef1441a73a8f
SHA1	7b10aaeee05e7a1efb43d9f837e9356ad55c07dd
ssdeep	1536:am+vLII5ygV8/tuH+P9zxqDKvARpmKiRMkTERU:a9LAg4tXPTEKvADmFgRU
Entropy	7.99727613788

Antivirus	
MicroWorld-eScan	Trojan.GenericKD.5057663
Symantec	Trojan.Gen.8!cloud
TrendMicro-HouseCall	Suspicious_GEN.F47V0513
BitDefender	Trojan.GenericKD.5057663
Ad-Aware	Trojan.GenericKD.5057663
F-Secure	Trojan.GenericKD.5057663
Emsisoft	Trojan.GenericKD.5057663 (B)
Arcabit	Trojan.Generic.D4D2C7F
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Ikarus	Ransom.Win32.WannaCrypt
GData	Trojan.GenericKD.5057663
Qihoo-360	Trojan.Generic
MicroWorld-eScan	Trojan.GenericKD.5057663
Symantec	Trojan.Gen.8!cloud
TrendMicro-HouseCall	Suspicious_GEN.F47V0513
BitDefender	Trojan.GenericKD.5057663
Ad-Aware	Trojan.GenericKD.5057663
F-Secure	Trojan.GenericKD.5057663
Emsisoft	Trojan.GenericKD.5057663 (B)
Arcabit	Trojan.Generic.D4D2C7F
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Ikarus	Ransom.Win32.WannaCrypt
GData	Trojan.GenericKD.5057663
Qihoo-360	Trojan.Generic

Relationships		
(F) t.wnry (5dcaa)	Related_To	(F) tasksche.exe (86721)
(F) t.wnry (5dcaa)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)

Description

This artifact is a malicious PE32 executable containing the primary component responsible for performing the encryption of the victim's files. Importantly, this file appears to be encrypted in the same manner in which the ransomware encrypts the victim's files. This would suggest the “decryptor” if purchased from the adversary via paid ransom, would decrypt the victim's files in the same way.

m_bulgarian.wnry

Details	
Name	m_bulgarian.wnry

Size	47879
Type	Rich Text Format data, version 1, unknown character set
MD5	95673b0f968c0f55b32204361940d184
SHA1	81e427d15a1a826b93e91c3d2fa65221c8ca9cff
ssdeep	768:Shef3jHdCG28Eb1tyci8crbEw6/5+3xFkbP0vyzbZrS14e:SheU5De
Entropy	4.95061166753

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_bulgarian.wnry (95673) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Bulgarian.

m_chinese (simplified).wnry

Details

Name	m_chinese (simplified).wnry
Size	54359
Type	Rich Text Format data, version 1, unknown character set
MD5	0252d45ca21c8e43c9742285c48e91ad
SHA1	5c14551d2736eef3a1c1970cc492206e531703c1
ssdeep	768:SWjkSFwwlUdcUG2HAmDTzpXtgmDNQ8qD7DHDqMtgDdLDMaDoKMGzD0DWJQ8/QoZ4:SWcwiqDB
Entropy	5.01509344454

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_chinese (simplified).wnry (0252d) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Chinese (simplified).

m_chinese (traditional).wnry

Details

Name	m_chinese (traditional).wnry
Size	79346
Type	Rich Text Format data, version 1, unknown character set
MD5	2efc3690d67cd073a9406a25005f7cea
SHA1	52c07f98870eabace6ec370b7eb562751e8067e9
ssdeep	768:SDwtkzjHdLG2xN1fyvnywUKB5lylYlzlJpsbuEWeM/yDRu9uCuwyInIwDOHEhm/v:SDnz5Rt4D4
Entropy	4.90189108744

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_chinese (traditional).wnry (2efc3) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Chinese (traditional).

m_croatian.wnry

Details	
Name	m_croatian.wnry
Size	39070
Type	Rich Text Format data, version 1, unknown character set
MD5	17194003fa70ce477326ce2f6deeb270
SHA1	e325988f68d327743926ea317abb9882f347fa73
ssdeep	384:SheftipUENLFsPzy3EFHjHdb2YG2+d18Scgn8c8/868H1F8E8/8Z3m8VdAm86a8n:Shef3jHd3G2n+p/mZrS14A
Entropy	5.03796878473

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_croatian.wnry (17194) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Croatian.

m_czech.wnry

Details	
Name	m_czech.wnry
Size	40512
Type	Rich Text Format data, version 1, unknown character set
MD5	537efeecdfa94cc421e58fd82a58ba9e
SHA1	3609456e16bc16ba447979f3aa69221290ec17d0
ssdeep	384:SheftipUENLFsPzy3EFHjHdg2yG2gv8n8+8zfB8k8F8i8k1Z8M8I818E838C8A8s:Shef3jHd2G26nyMZrS14g
Entropy	5.03594913469

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_czech.wnry (537ef) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Czech.

m_danish.wnry

Details	
Name	m_danish.wnry
Size	37045
Type	Rich Text Format data, version 1, unknown character set
MD5	2c5a3b81d5c4715b7bea01033367fcb5
SHA1	b548b45da8463e17199daafd34c23591f94e82cd
ssdeep	384:SheftipUENLFsPzy3EFHjHd02wG2roqni2Jeo75Y3kmA31dv61QyU:Shef3jHd4G2M5bZrS14Q
Entropy	5.02868302371

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_danish.wnry (2c5a3) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Ddanish.

m_dutch.wnry

Details

Name	m_dutch.wnry
Size	36987
Type	Rich Text Format data, version 1, unknown character set
MD5	7a8d499407c6a647c03c4471a67eaad7
SHA1	d573b6ac8e7e04a05cbbd6b7f6a9842f371d343b
ssdeep	384:Sw3BHSj2cLeT+sPzy3EFHjHdp2oG2/CzhReo75Y3kmA31dv61Qyz:Sw3BHSWjHdBG2/UhsZrS14f
Entropy	5.03616020597

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_dutch.wnry (7a8d4) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Dutch.

m_english.wnry

Details

Name	m_english.wnry
Size	36973
Type	Rich Text Format data, version 1, unknown character set
MD5	fe68c2dc0d2419b38f44d83f2fcf232e
SHA1	6c6e49949957215aa2f3dfb72207d249adf36283
ssdeep	384:S93BHSj2cguALeT+sPzy3EFHjHdM2EG2YLC7O3eo75Y3kmA31dv61QyW:S93BHSTjHd0G2YLCZrS14y
Entropy	5.04061161642

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_english.wnry (fe68c) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in English.

A sample of the text is shown below:

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so

enough time.You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.You only have 3 days to submit the payment.
After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to
recover your files forever.We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.Please check
the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window. After your payment,
click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday. Once the payment
is checked, you can start decrypting your files immediately.

Contact
If you need our assistance, send a message by clicking <Contact Us>.We strongly recommend you to not
remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed.
If your anti-virus gets updated and removes this software automatically, it will not be able to recover
your files even if you pay!

m_filipino.wnry

Details

Name	m_filipino.wnry
Size	37580
Type	Rich Text Format data, version 1, unknown character set
MD5	08b9e69b57e4c9b966664f8e1c27ab09
SHA1	2da1025bbbfb3cd308070765fc0893a48e5a85fa
ssdeep	384:Sw3BHSj2cLeT+sPzy3EFHjHdi2MG2AGsi6p07i/eo75Y3kmA31dv61QyR:Sw3BHSWjHdGG2Axa7iGZrS14N
Entropy	5.04581932168

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_filipino.wnry (08b9e) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Filipino.

m_finnish.wnry

Details

Name	m_finnish.wnry
Size	38377
Type	Rich Text Format data, version 1, unknown character set
MD5	35c2f97eea8819b1caebd23fee732d8f
SHA1	e354d1cc43d6a39d9732adea5d3b0f57284255d2
ssdeep	384:SheftipUENLFsPzy3EFHjHdg2oG2l1glOmeo75Y3kmA31dv61QyB:Shef3jHdMG2l1AO3ZrS14l
Entropy	5.03093847336

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_finnish.wnry (35c2f) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Finnish.

m_french.wnry

Details	
Name	m_french.wnry
Size	38437
Type	Rich Text Format data, version 1, unknown character set
MD5	4e57113a6bf6b88fdd32782a4a381274
SHA1	0fccbc91f0f94453d91670c6794f71348711061d
ssdeep	384:SheftipUENLFsPzy3EFHjHdtW2IG2sjqMeo75Y3kmA31dv61Qyg:Shef3jHd0G2smJZrS14M
Entropy	5.03112667661

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_french.wnry (4e571) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in French.

m_german.wnry

Details	
Name	m_german.wnry
Size	37181
Type	Rich Text Format data, version 1, unknown character set
MD5	3d59bbb5553fe03a89f817819540f469
SHA1	26781d4b06ff704800b463d0f1fca3afd923a9fe
ssdeep	384:SheftipUENLFsPzy3EFHjHdN26G2VSA1Ieo75Y3kmA31dv61QyU:Shef3jHdfG2oe1ZrS14w
Entropy	5.03973926795

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_german.wnry (3d59b) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in German.

m_greek.wnry

Details	
Name	m_greek.wnry
Size	49044
Type	Rich Text Format data, version 1, unknown character set
MD5	fb4e8718fea95bb7479727fde80cb424
SHA1	1088c7653cba385fe994e9ae34a6595898f20aeb
ssdeep	384:SheftipUENLFsPzy3EFHjHdc2oG2WWDFFG5BwKeo75Y3kmA31dv61QyM:Shef3jHdoG2NHG5BwLZrS14Q
Entropy	4.91009563462

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_greek.wnry (fb4e8) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Greek.

m_indonesian.wnry

Details

Name	m_indonesian.wnry
Size	37196
Type	Rich Text Format data, version 1, unknown character set
MD5	3788f91c694dfc48e12417ce93356b0f
SHA1	eb3b87f7f654b604daf3484da9e02ca6c4ea98b7
ssdeep	384:Sw3BHSj2cLeT+sPzy3EFHjHdY2oG2pq32eo75Y3kmA31dv61Qys:Sw3BHSWjHdUG2pq3nZrS14I
Entropy	5.03926854193

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_indonesian.wnry (3788f) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Indonesian.

m_italian.wnry

Details

Name	m_italian.wnry
Size	36883
Type	Rich Text Format data, version 1, unknown character set
MD5	30a200f78498990095b36f574b6e8690
SHA1	c4b1b3c087bd12b063e98bca464cd05f3f7b7882
ssdeep	384:SheftipUENLFsPzy3EFHjHdR2AG2c/EnByeo75Y3kmA31dv61Qy9:Shef3jHdJG2cQZrS14R
Entropy	5.02804819173

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_italian.wnry (30a20) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Italian.

m_japanese.wnry

Details

Name	m_japanese.wnry
Size	81844
Type	Rich Text Format data, version 1, unknown character set
MD5	b77e1221f7ecd0b5d696cb66cda1609e
SHA1	51eb7a254a33d05edf188ded653005dc82de8a46
ssdeep	384:SXZ0j2cKKwd1lksPzy3EFHjHdI2MG275rQeo75Y3kmA31dv61Qyr:SXZ0qbjHd4G2RNZrS14P
Entropy	4.8502578701

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	TROJ_RANSOMNOTE.RTF
Tencent	Win32.Trojan.Filecoder.Pfte
Ikarus	Trojan.Win32.Filecoder
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	TROJ_RANSOMNOTE.RTF
Tencent	Win32.Trojan.Filecoder.Pfte
Ikarus	Trojan.Win32.Filecoder

Relationships

(F) m_japanese.wnry (b77e1) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Japanese.

m_korean.wnry

Details	
Name	m_korean.wnry
Size	91501
Type	Rich Text Format data, version 1, unknown character set
MD5	6735cb43fe44832b061eeb3f5956b099
SHA1	d636daf64d524f81367ea92fdafa3726c909bee1
ssdeep	768:Shef3jHdUG2NQcbxfSVZiG9jvi3//ZVrMQr7pEKCHSI2DsY78piTDtTa6BxzBwdY:SheiaDq
Entropy	4.84183050451

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_korean.wnry (6735c) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Korean.

m_latvian.wnry

Details	
Name	m_latvian.wnry
Size	41169
Type	Rich Text Format data, version 1, unknown character set
MD5	c33afb4ecc04ee1bcc6975bea49abe40
SHA1	fbea4f170507cde02b839527ef50b7ec74b4821f
ssdeep	384:SheftipUENLFsPzy3EFHjHdcqH24G2ZN1EDCv3Apb0WD5gYV/S4L3rnzdeo75Y3f:Shef3jHdcMG2NpZrS14F
Entropy	5.0306952962

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_latvian.wnry (c33af) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Latvian.

m_norwegian.wnry

Details	
Name	m_norwegian.wnry
Size	37577
Type	Rich Text Format data, version 1, unknown character set
MD5	ff70cc7c00951084175d12128ce02399
SHA1	75ad3b1ad4fb14813882d88e952208c648f1fd18
ssdeep	384:SheftipUENLFsPzy3EFHjHdy2MG2D7mgwroXeo75Y3kmA31dv61Qy5:Shef3jHdGG23KrDZrS14N
Entropy	5.02583682362

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_norwegian.wnry (ff70c) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Norwegian.

m_polish.wnry

Details	
Name	m_polish.wnry
Size	39896
Type	Rich Text Format data, version 1, unknown character set
MD5	e79d7f2833a9c2e2553c7fe04a1b63f4
SHA1	3d9f56d2381b8fe16042aa7c4feb1b33f2baebff
ssdeep	384:SheftipUENLFsPzy3EFHjHdD2SG2gA8w8OJ6868jy8/8w8m8T848f8y858l8j8yv:Shef3jHdxG2KhuZrS14G
Entropy	5.04854100247

Antivirus	
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_polish.wnry (e79d7) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Polish

m_portuguese.wnry

Details

Name	m_portuguese.wnry
Size	37917
Type	Rich Text Format data, version 1, unknown character set
MD5	fa948f7d8dfb21ceddd6794f2d56b44f
SHA1	ca915fbe020caa88dd776d89632d7866f660fc7a
ssdeep	384:SheftipUENLFsPzy3EFHjHdy2QG2xgk5eo75Y3kmA31dv61QyV:Shef3jHdCG2EZrS14p
Entropy	5.02787228176

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
Ikarus	Win32.Outbreak
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
Ikarus	Win32.Outbreak

Relationships

(F) m_portuguese.wnry (fa948) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Portuguese.

m_romanian.wnry

Details

Name	m_romanian.wnry
Size	52161
Type	Rich Text Format data, version 1, unknown character set
MD5	313e0ececd24f4fa1504118a11bc7986
SHA1	e1b9ae804c7fb1d27f39db18dc0647bb04e75e9d
ssdeep	768:Shef3jHdXG2Cz2/vBAOZsQO0cLfnF/Zhcz7sDsYZBB/0gBjL+IU/hbhMVDtsR49P:ShehlrGR1m4dx9mjVyAvg7ouDT
Entropy	4.96430694991

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_romanian.wnry (313e0) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Romanian.

m_russian.wnry

Details

Name	m_russian.wnry
Size	47108
Type	Rich Text Format data, version 1, unknown character set
MD5	452615db2336d60af7e2057481e4cab5
SHA1	442e31f6556b3d7de6eb85fbac3d2957b7f5eac6

ssdeep	384:SheftipUENLFsPzy3EFHjHdg2qG2aUGs0K6lyZqmfGGHRblldORZeo75Y3kmA31L:Shef3jHdeG2lGsDOcZxbP7ZrS14K
Entropy	4.95277769168

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	TROJ_RANSOMNOTE.RTF
TrendMicro	TROJ_RANSOMNOTE.RTF
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Tencent	Win32.Trojan.Filecoder.Palq
Ikarus	Trojan.Win32.Filecoder
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	TROJ_RANSOMNOTE.RTF
TrendMicro	TROJ_RANSOMNOTE.RTF
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Tencent	Win32.Trojan.Filecoder.Palq
Ikarus	Trojan.Win32.Filecoder

Relationships

(F) m_russian.wnry (45261) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Russian.

m_slovak.wnry

Details

Name	m_slovak.wnry
Size	41391
Type	Rich Text Format data, version 1, unknown character set
MD5	c911aba4ab1da6c28cf86338ab2ab6cc
SHA1	fee0fd58b8efe76077620d8abc7500dbfef7c5b0
ssdeep	384:SheftipUENLFsPzy3EFHjHd4Yb2YG2gNZ8a8zV/8j8U8l8x838Z8Q808m8d8T8hw:Shef3jHdZvG23AZrS14f
Entropy	5.02773096628

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_slovak.wnry (c911a) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Slovak.

m_spanish.wnry

Details

Name	m_spanish.wnry
Size	37381
Type	Rich Text Format data, version 1, unknown character set
MD5	8d61648d34cba8ae9d1e2a219019add1
SHA1	2091e42fc17a0cc2f235650f7aad87abf8ba22c2
ssdeep	384:SheftipUENLFsPzy3EFHjHdf24G2/ezV6YQUdZYlujeMQ9RXmhRweo75Y3kmA31S:Shef3jHdrG2fuhZrS14T
Entropy	5.02443306661

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_spanish.wnry (8d616) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Spanish.

m_swedish.wnry

Details

Name	m_swedish.wnry
Size	38483
Type	Rich Text Format data, version 1, unknown character set
MD5	c7a19984eb9f37198652eaf2fd1ee25c
SHA1	06eafed025cf8c4d76966bf382ab0c5e1bd6a0ae
ssdeep	384:SheftipUENLFsPzy3EFHjHdb24G2ZKLVdDeo75Y3kmA31dv61QyE:Shef3jHd/G2w6ZrS14w
Entropy	5.02297273663

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_swedish.wnry (c7a19) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Swedish.

m_turkish.wnry

Details

Name	m_turkish.wnry
Size	42582
Type	Rich Text Format data, version 1, unknown character set
MD5	531ba6b1a5460fc9446946f91cc8c94b
SHA1	cc56978681bd546fd82d87926b5d9905c92a5803
ssdeep	384:SheftipUENLFsPzy3EFHjHds42WG2mzGu/eo75Y3kmA31dv61QyZ:Shef3jHdsiG2moZrS149
Entropy	5.01072237707

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
ESET-NOD32	Win32/Filecoder.WannaCryptor.D

Relationships

(F) m_turkish.wnry (531ba) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Turkish.

m_vietnamese.wnry

Details

Name	m_vietnamese.wnry
Size	93778
Type	Rich Text Format data, version 1, unknown character set
MD5	8419be28a0dcec3f55823620922b00fa

SHA1	2e4791f9cdfca8abf345d606f313d22b36c46b92
ssdeep	384:SheftipUENLFsPzy3EFHjHdW2YG22cViQj3KiG8dpcH8iEriG8E8O83Jz52sxG8h:Shef3jHdWG2+oPZrS14i
Entropy	4.762061349

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	TROJ_RANSOMNOTE.RTF
TrendMicro	TROJ_RANSOMNOTE.RTF
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Tencent	Win32.Trojan.Filecoder.Dxmn
Ikarus	Trojan.Win32.Filecoder
GData	Script.Trojan.Agent.54KIMR
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	TROJ_RANSOMNOTE.RTF
TrendMicro	TROJ_RANSOMNOTE.RTF
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Tencent	Win32.Trojan.Filecoder.Dxmn
Ikarus	Trojan.Win32.Filecoder
GData	Script.Trojan.Agent.54KIMR

Relationships

(F) m_vietnamese.wnry (8419b) Related_To (F) tasksche.exe (86721)

Description

This artifact is an RTF formatted ransom note containing payment instructions, written in Vietnamese.

---

r.wnry

Details

Name	r.wnry
Size	864
Type	ASCII text, with CRLF line terminators
MD5	3e0020fc529b1c2a061016dd2469ba96
SHA1	c3a91c22b63f6fe709e7c29cafb29a2ee83e6ade
ssdeep	24:ptrPzDVR5Gi3OzGm0Ei5bnBR7brW8PNAi0eEprY+Ai75wRZce/:DZD36W5/vWmMo+m
Entropy	4.53351847801

Antivirus

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	TROJ_RANSOMNOTE.AUSCQT
TrendMicro	TROJ_RANSOMNOTE.AUSCQT
AegisLab	Troj.Ransomnote.Auscqt!c
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Tencent	Win32.Trojan.Filecoder.Lkds
Ikarus	Trojan.Win32.Filecoder
GData	Script.Trojan.Agent.98XDFC
Qihoo-360	Trojan.Generic
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	TROJ_RANSOMNOTE.AUSCQT
TrendMicro	TROJ_RANSOMNOTE.AUSCQT
AegisLab	Troj.Ransomnote.Auscqt!c
Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Tencent	Win32.Trojan.Filecoder.Lkds
Ikarus	Trojan.Win32.Filecoder

GData	Script.Trojan.Agent.98XDFC
Qihoo-360	Trojan.Generic

Relationships

(F) r.wnry (3e002)	Related_To	(F) tasksche.exe (86721)
(F) r.wnry (3e002)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)

Description

This is a data file that explains what has happened and how to pay the ransom

s.wnry

Details

Name	s.wnry
Size	22667
Type	Zip archive data, at least v1.0 to extract
MD5	025ac29fc5b5257ca0a031de71f201bf
SHA1	55edb34545871def9a4b6599484ad781fa583407
ssdeep	384:RpyPhUnOidCa1feM+Oyua4nMmK4kOW2JpHLHBOQnbNOMLlk:7yaJnFe9uaq7W2JdBOQpOM5k
Entropy	7.98860680988

Antivirus

No matches found.

Relationships

(F) s.wnry (025ac)	Related_To	(F) tasksche.exe (86721)
(F) s.wnry (025ac)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)

Description

TOR library that is imported by "u.wnry"

taskdl.exe

Details

Name	taskdl.exe
Size	20480
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	4fef5e34143e646dbf9907c4374276f5
SHA1	47a9ad4125b6bd7c55e4e7da251e23f089407b8f
ssdeep	96:Udocv5e0e1wWtaLYjJN0yDGgI2u9+w5eOIMviS0jPtboyn15EWBwwWwT:6oL0edtJN7qvAZM6S0jP1oynkWBwwWg
Entropy	3.16648454088

Antivirus

MicroWorld-eScan	Trojan.GenericKD.5057554
nProtect	Ransom/W32.WannaCry.20480
CAT-QuickHeal	TrojanRansom.Agent
McAfee	Ransom-O
Malwarebytes	Ransom.WanaCrypt0r
VIPRE	Trojan.Win32.Generic!BT
K7GW	Trojan (0001140e1)
K7AntiVirus	Trojan (0001140e1)
TrendMicro	Ransom_WCRY.I
F-Prot	W32/WannaCrypt.C
Symantec	Ransom.Wannacry

ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	Ransom_WCRY.I
Paloalto	generic.ml
Kaspersky	Trojan-Ransom.Win32.Agent.aapw
BitDefender	Trojan.GenericKD.5057554
NANO-Antivirus	Trojan.Win32.Agent.eopwdw
ViRobot	Trojan.Win32.S.WannaCry.20480[h]
Avast	Win32:WannaCry-B [Trj]
Ad-Aware	Trojan.GenericKD.5057554
Sophos	Troj/Wanna-C
Comodo	UnclassifiedMalware
F-Secure	Trojan.GenericKD.5057554
DrWeb	Trojan.Encoder.11432
McAfee-GW-Edition	Ransom-O
Emsisoft	Trojan.GenericKD.5057554 (B)
Cyren	W32/Trojan.NFAB-4202
Jiangmin	Trojan.WanaCry.j
Webroot	W32.Ransom.Wanacryptor
Avira	TR/FileCoder.724611
Fortinet	W32/Agent.AAPW!tr
Antiy-AVL	Trojan/Win32.TGeneric
Arcabit	Trojan.Generic.D4D2C12
AegisLab	Troj.Ransom.W32.Agent!c
ZoneAlarm	Trojan-Ransom.Win32.Agent.aapw
Microsoft	Ransom:Win32/WannaCrypt
AhnLab-V3	Trojan/Win32.HDC.C61115
ALYac	Trojan.Ransom.WannaCryptor
AVware	Trojan.Win32.Generic!BT
Tencent	Win32.Trojan.Ransomlocker.Nmmb
Ikarus	Trojan.Win32.Filecoder
GData	Trojan.GenericKD.5057554
AVG	FileCryptor.OYG
Panda	Trj/RansomCrypt.I
Qihoo-360	Trojan.Generic
MicroWorld-eScan	Trojan.GenericKD.5057554
nProtect	Ransom/W32.WannaCry.20480
CAT-QuickHeal	TrojanRansom.Agent
McAfee	Ransom-O
Malwarebytes	Ransom.WanaCrypt0r
VIPRE	Trojan.Win32.Generic!BT
K7GW	Trojan (0001140e1)
K7AntiVirus	Trojan (0001140e1)
TrendMicro	Ransom_WCRY.I
F-Prot	W32/WannaCrypt.C
Symantec	Ransom.Wannacry
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	Ransom_WCRY.I
Paloalto	generic.ml
Kaspersky	Trojan-Ransom.Win32.Agent.aapw
BitDefender	Trojan.GenericKD.5057554
NANO-Antivirus	Trojan.Win32.Agent.eopwdw

ViRobot	Trojan.Win32.S.WannaCry.20480[h]
Avast	Win32:WannaCry-B [Trj]
Ad-Aware	Trojan.GenericKD.5057554
Sophos	Troj/Wanna-C
Comodo	UnclassifiedMalware
F-Secure	Trojan.GenericKD.5057554
DrWeb	Trojan.Encoder.11432
McAfee-GW-Edition	Ransom-O
Emsisoft	Trojan.GenericKD.5057554 (B)
Cyren	W32/Trojan.NFAB-4202
Jiangmin	Trojan.WanaCry.j
Webroot	W32.Ransom.Wanacryptor
Avira	TR/FileCoder.724611
Fortinet	W32/Agent.AAPW!tr
Antiy-AVL	Trojan/Win32.TGeneric
Arcabit	Trojan.Generic.D4D2C12
AegisLab	Troj.Ransom.W32.Agent!c
ZoneAlarm	Trojan-Ransom.Win32.Agent.aapw
Microsoft	Ransom:Win32/WannaCrypt
AhnLab-V3	Trojan/Win32.HDC.C61115
ALYac	Trojan.Ransom.WannaCryptor
AVware	Trojan.Win32.Generic!BT
Tencent	Win32.Trojan.Ransomlocker.Nmmb
Ikarus	Trojan.Win32.Filecoder
GData	Trojan.GenericKD.5057554
AVG	FileCryptor.OYG
Panda	Trj/RansomCrypt.I
Qihoo-360	Trojan.Generic

PE Information

Compiled	2009-07-14T00:12:07Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	517be0783885b48f9e129f76f2906642	4096	0.647544716167
.text	c9aa64fe8d9efc3e7be627442c0172f0	4096	4.92282748815
.rdata	e98eaa78f8b3d90a99454c5d64db86ba	4096	2.66441166404
.data	d71c25cb529fed9abe0ee5d3d6264cd5	4096	0.105612474489
.rsrc	a5fbafb18686e9366dc75c2e1920c441	4096	3.71611137019

Packers

Name	Version	Entry Point
Microsoft Visual C++ v6.0	NA	NA

Relationships

(F) taskdl.exe (4fef5)	Related_To	(F) tasksche.exe (86721)

Description

This artifact is a PE32 executable designed to search for the string "\$RECYCLE*.WNCRYT" on all installed drives on the system.

taskse.exe

Details

Name	taskse.exe

Size	20480
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	8495400f199ac77853c53b5a3f278f3e
SHA1	be5d6279874da315e3080b06083757aad9b32c23
ssdeep	96:UjpvOHheaCDCNIOgTegoddPtboyX7cvp0EWy1HlWwr:UjVWEam7ofP1oyX7olWUHlW0
Entropy	2.52525096181

Antivirus

MicroWorld-eScan	Trojan.GenericKD.5057859
nProtect	Ransom/W32.Zapchast.20480.B
CAT-QuickHeal	Trojanransom.Zapchast
McAfee	Ransom-O
Malwarebytes	Ransom.WanaCrypt0r
K7GW	Trojan (0001140e1)
K7AntiVirus	Trojan (0001140e1)
TrendMicro	Ransom_WCRY.I
F-Prot	W32/WannaCrypt.B
Symantec	Ransom.Wannacry
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	Ransom_WCRY.I
Paloalto	generic.ml
GData	Trojan.GenericKD.5057859
Kaspersky	Trojan-Ransom.Win32.Zapchast.i
BitDefender	Trojan.GenericKD.5057859
NANO-Antivirus	Trojan.Win32.Zapchast.eopvwc
ViRobot	Trojan.Win32.S.WannaCry.20480.A[h]
AegisLab	Troj.Ransom.W32!c
Sophos	Troj/Wanna-C
Comodo	UnclassifiedMalware
F-Secure	Trojan.GenericKD.5057859
DrWeb	Trojan.Encoder.11432
VIPRE	Trojan.Win32.Generic!BT
McAfee-GW-Edition	Ransom-O
Emsisoft	Trojan.GenericKD.5057859 (B)
Cyren	W32/Trojan.FXSJ-2552
Jiangmin	Trojan.Zapchast.eo
Webroot	W32.Ransom.Wanacryptor
Avira	TR/FileCoder.724649
Antiy-AVL	Trojan/Win32.TGeneric
Arcabit	Trojan.Generic.D4D2D43
ZoneAlarm	Trojan-Ransom.Win32.Zapchast.i
Microsoft	Ransom:Win32/WannaCrypt
AVG	FileCryptor.OYH
AhnLab-V3	Trojan/Win32.WannaCryptor.C1951306
ALYac	Trojan.Ransom.WannaCryptor
AVware	Trojan.Win32.Generic!BT
Ad-Aware	Trojan.GenericKD.5057859
Panda	Trj/RansomCrypt.C
Tencent	Win32.Trojan.Ransomlocker.Ozmy
Ikarus	Trojan.Win32.Filecoder
Fortinet	W32/Zapchast.D!tr

Avast	Win32:WannaCry-A [Trj]
Qihoo-360	Trojan.Generic
MicroWorld-eScan	Trojan.GenericKD.5057859
nProtect	Ransom/W32.Zapchast.20480.B
CAT-QuickHeal	Trojanransom.Zapchast
McAfee	Ransom-O
Malwarebytes	Ransom.WanaCrypt0r
K7GW	Trojan (0001140e1)
K7AntiVirus	Trojan (0001140e1)
TrendMicro	Ransom_WCRY.I
F-Prot	W32/WannaCrypt.B
Symantec	Ransom.Wannacry
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	Ransom_WCRY.I
Paloalto	generic.ml
GData	Trojan.GenericKD.5057859
Kaspersky	Trojan-Ransom.Win32.Zapchast.i
BitDefender	Trojan.GenericKD.5057859
NANO-Antivirus	Trojan.Win32.Zapchast.eopvwc
ViRobot	Trojan.Win32.S.WannaCry.20480.A[h]
AegisLab	Troj.Ransom.W32!c
Sophos	Troj/Wanna-C
Comodo	UnclassifiedMalware
F-Secure	Trojan.GenericKD.5057859
DrWeb	Trojan.Encoder.11432
VIPRE	Trojan.Win32.Generic!BT
McAfee-GW-Edition	Ransom-O
Emsisoft	Trojan.GenericKD.5057859 (B)
Cyren	W32/Trojan.FXSJ-2552
Jiangmin	Trojan.Zapchast.eo
Webroot	W32.Ransom.Wanacryptor
Avira	TR/FileCoder.724649
Antiy-AVL	Trojan/Win32.TGeneric
Arcabit	Trojan.Generic.D4D2D43
ZoneAlarm	Trojan-Ransom.Win32.Zapchast.i
Microsoft	Ransom:Win32/WannaCrypt
AVG	FileCryptor.OYH
AhnLab-V3	Trojan/Win32.WannaCryptor.C1951306
ALYac	Trojan.Ransom.WannaCryptor
AVware	Trojan.Win32.Generic!BT
Ad-Aware	Trojan.GenericKD.5057859
Panda	Trj/RansomCrypt.C
Tencent	Win32.Trojan.Ransomlocker.Ozmy
Ikarus	Trojan.Win32.Filecoder
Fortinet	W32/Zapchast.D!tr
Avast	Win32:WannaCry-A [Trj]
Qihoo-360	Trojan.Generic

PE Information

Compiled	2009-07-13T23:15:28Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	bf20072e3afa57f58ac8c40e0f9d162b	4096	0.627317954157
.text	27ba7eebe222f1f600c05d356fdd3f20	4096	3.29976908335
.rdata	95ab42776493299c34c1e0c609c3d165	4096	1.05105359822
.data	5a849268f8bc1bf35214e328323b8793	4096	0.79975850341
.rsrc	f7bd6aed27ba347f17f0fa5893d895d6	4096	3.72171470037

Packers

Name	Version	Entry Point
Microsoft Visual C++ v6.0	NA	NA

Relationships

(F) taskse.exe (84954) Related_To (F) tasksche.exe (86721)

Description

This artifact is a PE32 executable designed to support Remote Desktop Services.

---

u.wnry

Details

Name	u.wnry
Size	245760
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	7bf2b57f2a205768755c07f238fb32cc
SHA1	45356a9dd616ed7161a3b9192e2f318d0ab5ad10
ssdeep	3072:Rmrhd5U1eigWcR+uiUg6p4FLlG4tlL8z+mmCeHFZjoHEo3m:REd5+IZiZhLlG4AimmCo
Entropy	6.27892040839

Antivirus

MicroWorld-eScan	Trojan.GenericKD.5057856
nProtect	Ransom/W32.Wanna.245760
CAT-QuickHeal	TrojanRansom.Wanna
McAfee	Ransom-O
Malwarebytes	Ransom.WanaCrypt0r
VIPRE	Trojan.Win32.Generic!BT
CrowdStrike	malicious_confidence_60% (D)
K7GW	Trojan (0001140e1)
K7AntiVirus	Trojan (0001140e1)
Cyren	W32/Trojan.FSSE-8992
Symantec	Ransom.Wannacry
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	RANSOM_WCRY.I
Avast	Win32:WanaCry-A [Trj]
ClamAV	Win.Trojan.Agent-6312824-0
Kaspersky	Trojan-Ransom.Win32.Wanna.c
BitDefender	Trojan.GenericKD.5057856
NANO-Antivirus	Trojan.Win32.Wanna.eottwl
Paloalto	generic.ml
ViRobot	Trojan.Win32.S.WannaCry.245760[h]
Tencent	Win32.Trojan.Ransomlocker.Mvmh
Ad-Aware	Trojan.GenericKD.5057856
Emsisoft	Trojan.GenericKD.5057856 (B)
Comodo	TrojWare.Win32.Ransom.WannaCryptor.~
F-Secure	Trojan.GenericKD.5057856

DrWeb	Trojan.Encoder.11432
TrendMicro	RANSOM_WCRY.I
McAfee-GW-Edition	Ransom-O
F-Prot	W32/WannaCrypt.A
Jiangmin	Trojan.WanaCry.a
Webroot	W32.Ransom.Wannacry
Avira	TR/FileCoder.724645
Fortinet	W32/GenKryptik.1C25!tr
Antiy-AVL	Trojan/Win32.Deshacop
Arcabit	Trojan.Generic.D4D2D40
AegisLab	Uds.Dangerousobject.Multi!c
ZoneAlarm	Trojan-Ransom.Win32.Wanna.c
Microsoft	Ransom:Win32/WannaCrypt
Sophos	Troj/Wanna-D
AhnLab-V3	Trojan/Win32.WannaCryptor.R200589
ALYac	Trojan.Ransom.WannaCryptor
AVware	Trojan.Win32.Generic!BT
Rising	Malware.Generic.5!tfe (cloud:7SfzBq30iMV)
Ikarus	Trojan.Win32.Filecoder
GData	Win32.Trojan-Ransom.WannaCry.E
AVG	Generic_r.SSZ
Panda	Trj/RansomCrypt.K
Qihoo-360	Win32/Trojan.Multi.daf
MicroWorld-eScan	Trojan.GenericKD.5057856
nProtect	Ransom/W32.Wanna.245760
CAT-QuickHeal	TrojanRansom.Wanna
McAfee	Ransom-O
Malwarebytes	Ransom.WanaCrypt0r
VIPRE	Trojan.Win32.Generic!BT
CrowdStrike	malicious_confidence_60% (D)
K7GW	Trojan (0001140e1)
K7AntiVirus	Trojan (0001140e1)
Cyren	W32/Trojan.FSSE-8992
Symantec	Ransom.Wannacry
ESET-NOD32	Win32/Filecoder.WannaCryptor.D
TrendMicro-HouseCall	RANSOM_WCRY.I
Avast	Win32:WanaCry-A [Trj]
ClamAV	Win.Trojan.Agent-6312824-0
Kaspersky	Trojan-Ransom.Win32.Wanna.c
BitDefender	Trojan.GenericKD.5057856
NANO-Antivirus	Trojan.Win32.Wanna.eottwl
Paloalto	generic.ml
ViRobot	Trojan.Win32.S.WannaCry.245760[h]
Tencent	Win32.Trojan.Ransomlocker.Mvmh
Ad-Aware	Trojan.GenericKD.5057856
Emsisoft	Trojan.GenericKD.5057856 (B)
Comodo	TrojWare.Win32.Ransom.WannaCryptor.~
F-Secure	Trojan.GenericKD.5057856
DrWeb	Trojan.Encoder.11432
TrendMicro	RANSOM_WCRY.I
McAfee-GW-Edition	Ransom-O

F-Prot	W32/WannaCrypt.A
Jiangmin	Trojan.WanaCry.a
Webroot	W32.Ransom.Wannacry
Avira	TR/FileCoder.724645
Fortinet	W32/GenKryptik.1C25!tr
Antiy-AVL	Trojan/Win32.Deshacop
Arcabit	Trojan.Generic.D4D2D40
AegisLab	Uds.Dangerousobject.Multi!c
ZoneAlarm	Trojan-Ransom.Win32.Wanna.c
Microsoft	Ransom:Win32/WannaCrypt
Sophos	Troj/Wanna-D
AhnLab-V3	Trojan/Win32.WannaCryptor.R200589
ALYac	Trojan.Ransom.WannaCryptor
AVware	Trojan.Win32.Generic!BT
Rising	Malware.Generic.5!tfe (cloud:7SfzBq30iMV)
Ikarus	Trojan.Win32.Filecoder
GData	Win32.Trojan-Ransom.WannaCry.E
AVG	Generic_r.SSZ
Panda	Trj/RansomCrypt.K
Qihoo-360	Win32/Trojan.Multi.daf

PE Information

Compiled	2009-07-13T23:19:35Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	143b3fc179777c5b2f2e0ff974ebd7b7	4096	0.763356728671
.text	c9ede1054fef33720f9fa97f5e8abe49	81920	6.24100602272
.rdata	5a89aac6c8259abbba2fa2ad3fcefc6e	40960	5.87183534271
.data	05da32043b1e3a147de634c550f1954d	12288	4.72665302653
.rsrc	8e97637474ab77441ae5add3f3325753	106496	5.63519234495

Packers

Name	Version	Entry Point
Microsoft Visual C++ v6.0	NA	NA

Relationships

(F) u.wnry (7bf2b)	Related_To	(F) tasksche.exe (86721)
(F) u.wnry (7bf2b)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)

Description

This artifact is an interactive TOR client which will enable a victim to submit payment to the hackers via a secure TOR session.

Domains

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

URI

- http[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Ports

- 80

HTTP Sessions

- GET / HTTP/1.1

Host: www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Cache-Control: no-cache

Whois

Domain Name: IUQERFSODP9IFJAPOSDFJHGOSURIJFAEWRWERGWEA.COM
Registrar: NAMECHEAP INC.
Sponsoring Registrar IANA ID: 1068
Whois Server: whois.namecheap.com
Referral URL: http[:]//www[.]namecheap.com
Name Server: NS1.SINKHOLE.TECH
Name Server: NS2.SINKHOLE.TECH
Name Server: NS3.SINKHOLE.TECH
Name Server: NS4.SINKHOLE.TECH
Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProhibited
Updated Date: 12-may-2017
Creation Date: 12-may-2017
Domain name: iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Registry Domain ID: 2123519849_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http[:]//www[.]namecheap.com
Updated Date: 2017-05-12T15:08:10.00Z
Creation Date: 2017-05-12T15:08:04.00Z
Registrar Registration Expiration Date: 2018-05-12T15:08:04.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse[@]namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https[:]//icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name: Botnet Sinkhole
Registrant Organization:
Registrant Street: Botnet Sinkhole
Registrant City: Los Angeles
Registrant State/Province: CA
Registrant Postal Code: 00000
Registrant Country: US
Registrant Phone: +0.00000000000
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: BotnetSinkhole[@]gmail.com
Registry Admin ID:
Admin Name: Botnet Sinkhole
Admin Organization:
Admin Street: Botnet Sinkhole
Admin City: Los Angeles
Admin State/Province: CA
Admin Postal Code: 00000
Admin Country: US
Admin Phone: +0.00000000000
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: BotnetSinkhole[@]gmail.com
Registry Tech ID:
Tech Name: Botnet Sinkhole
Tech Organization:
Tech Street: Botnet Sinkhole
Tech City: Los Angeles
Tech State/Province: CA
Tech Postal Code: 00000
Tech Country: US
Tech Phone: +0.00000000000
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:

Tech Email: BotnetSinkhole[@]gmail.com
Name Server: ns1.sinkhole.tech
Name Server: ns2.sinkhole.tech
Name Server: ns3.sinkhole.tech
Name Server: ns4.sinkhole.tech
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
>>> Last update of WHOIS database: 2017-05-14T11:56:55.96Z <<<

Relationships

(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Related_To	(U) http[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Related_To	(P) 80
(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Related_To	(H) GET / HTTP/1.1
(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Characterized_By	(W) Domain Name: IUQERFS
(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Connected_From	(F) 5bef35496fcbdbe841c82f4d1ab8b7c2 (5bef3)

gx7ekbenv2riucmf.onion

Relationships

(D) gx7ekbenv2riucmf.onion	Contained_Within	(F) c.wnry (ae08f)

57g7spgrzlojinas.onion

Relationships

(D) 57g7spgrzlojinas.onion	Contained_Within	(F) c.wnry (ae08f)

xxlvbrloxvriy2c5.onion

Relationships

(D) xxlvbrloxvriy2c5.onion	Contained_Within	(F) c.wnry (ae08f)

76jdd2ir2embyv47.onion

Relationships

(D) 76jdd2ir2embyv47.onion	Contained_Within	(F) c.wnry (ae08f)

cwwnhwhlz52maqm7.onion

Relationships

(D) cwwnhwhlz52maqm7.onion	Contained_Within	(F) c.wnry (ae08f)

Relationship Summary

(F) 5bef35496fcbdbe841c82f4d1ab8b7c2 (5bef3)	Connected_To	(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
(F) 5bef35496fcbdbe841c82f4d1ab8b7c2 (5bef3)	Dropped	(F) tasksche.exe (86721)
(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Related_To	(U) http[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Related_To	(P) 80
(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Related_To	(H) GET / HTTP/1.1

(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Characterized_By	(W) Domain Name: IUQERFS
(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Connected_From	(F) 5bef35496fcbdbe841c82f4d1ab8b7c2 (5bef3)
(F) tasksche.exe (86721)	Related_To	(S) res11.PNG
(F) tasksche.exe (86721)	Related_To	(F) b.wnry (c1717)
(F) tasksche.exe (86721)	Related_To	(F) c.wnry (ae08f)
(F) tasksche.exe (86721)	Related_To	(F) t.wnry (5dcaa)
(F) tasksche.exe (86721)	Related_To	(F) m_bulgarian.wnry (95673)
(F) tasksche.exe (86721)	Related_To	(F) m_chinese (simplified).wnry (0252d)
(F) tasksche.exe (86721)	Related_To	(F) m_chinese (traditional).wnry (2efc3)
(F) tasksche.exe (86721)	Related_To	(F) m_croatian.wnry (17194)
(F) tasksche.exe (86721)	Related_To	(F) m_czech.wnry (537ef)
(F) tasksche.exe (86721)	Related_To	(F) m_danish.wnry (2c5a3)
(F) tasksche.exe (86721)	Related_To	(F) m_dutch.wnry (7a8d4)
(F) tasksche.exe (86721)	Related_To	(F) m_english.wnry (fe68c)
(F) tasksche.exe (86721)	Related_To	(F) m_filipino.wnry (08b9e)
(F) tasksche.exe (86721)	Related_To	(F) m_finnish.wnry (35c2f)
(F) tasksche.exe (86721)	Related_To	(F) m_french.wnry (4e571)
(F) tasksche.exe (86721)	Related_To	(F) m_german.wnry (3d59b)
(F) tasksche.exe (86721)	Related_To	(F) m_greek.wnry (fb4e8)
(F) tasksche.exe (86721)	Related_To	(F) m_indonesian.wnry (3788f)
(F) tasksche.exe (86721)	Related_To	(F) m_italian.wnry (30a20)
(F) tasksche.exe (86721)	Related_To	(F) m_japanese.wnry (b77e1)
(F) tasksche.exe (86721)	Related_To	(F) m_korean.wnry (6735c)
(F) tasksche.exe (86721)	Related_To	(F) m_latvian.wnry (c33af)
(F) tasksche.exe (86721)	Related_To	(F) m_norwegian.wnry (ff70c)
(F) tasksche.exe (86721)	Related_To	(F) m_polish.wnry (e79d7)
(F) tasksche.exe (86721)	Related_To	(F) m_portuguese.wnry (fa948)
(F) tasksche.exe (86721)	Related_To	(F) m_romanian.wnry (313e0)
(F) tasksche.exe (86721)	Related_To	(F) m_russian.wnry (45261)
(F) tasksche.exe (86721)	Related_To	(F) m_slovak.wnry (c911a)
(F) tasksche.exe (86721)	Related_To	(F) m_spanish.wnry (8d616)
(F) tasksche.exe (86721)	Related_To	(F) m_swedish.wnry (c7a19)
(F) tasksche.exe (86721)	Related_To	(F) m_turkish.wnry (531ba)
(F) tasksche.exe (86721)	Related_To	(F) m_vietnamese.wnry (8419b)
(F) tasksche.exe (86721)	Related_To	(F) r.wnry (3e002)
(F) tasksche.exe (86721)	Related_To	(F) s.wnry (025ac)
(F) tasksche.exe (86721)	Related_To	(F) taskdl.exe (4fef5)
(F) tasksche.exe (86721)	Related_To	(F) taskse.exe (84954)
(F) tasksche.exe (86721)	Related_To	(F) u.wnry (7bf2b)
(F) tasksche.exe (86721)	Dropped_By	(F) 5bef35496fcbdbe841c82f4d1ab8b7c2 (5bef3)
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(S) res22.PNG
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) b.wnry (c1717)
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) c.wnry (ae08f)
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) t.wnry (5dcaa)
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) s.wnry (025ac)

(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) r.wnry (3e002)
(F) 4da1f312a214c07143abeeafb695d904 (4da1f)	Related_To	(F) u.wnry (7bf2b)
(F) b.wnry (c1717)	Related_To	(S) Ooops.PNG
(F) b.wnry (c1717)	Related_To	(F) tasksche.exe (86721)
(F) b.wnry (c1717)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)
(S) Ooops.PNG	Related_To	(F) b.wnry (c1717)
(S) res11.PNG	Related_To	(F) tasksche.exe (86721)
(S) res22.PNG	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)
(F) c.wnry (ae08f)	Related_To	(F) tasksche.exe (86721)
(F) c.wnry (ae08f)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)
(F) c.wnry (ae08f)	Contains	(D) gx7ekbenv2riucmf.onion
(F) c.wnry (ae08f)	Contains	(D) 57g7spgrzlojinas.onion
(F) c.wnry (ae08f)	Contains	(D) xxlvbrloxvriy2c5.onion
(F) c.wnry (ae08f)	Contains	(D) 76jdd2ir2embyv47.onion
(F) c.wnry (ae08f)	Contains	(D) cwwnhwhlz52maqm7.onion
(D) gx7ekbenv2riucmf.onion	Contained_Within	(F) c.wnry (ae08f)
(D) 57g7spgrzlojinas.onion	Contained_Within	(F) c.wnry (ae08f)
(D) xxlvbrloxvriy2c5.onion	Contained_Within	(F) c.wnry (ae08f)
(D) 76jdd2ir2embyv47.onion	Contained_Within	(F) c.wnry (ae08f)
(D) cwwnhwhlz52maqm7.onion	Contained_Within	(F) c.wnry (ae08f)
(F) t.wnry (5dcaa)	Related_To	(F) tasksche.exe (86721)
(F) t.wnry (5dcaa)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)
(F) m_bulgarian.wnry (95673)	Related_To	(F) tasksche.exe (86721)
(F) m_chinese (simplified).wnry (0252d)	Related_To	(F) tasksche.exe (86721)
(F) m_chinese (traditional).wnry (2efc3)	Related_To	(F) tasksche.exe (86721)
(F) m_croatian.wnry (17194)	Related_To	(F) tasksche.exe (86721)
(F) m_czech.wnry (537ef)	Related_To	(F) tasksche.exe (86721)
(F) m_danish.wnry (2c5a3)	Related_To	(F) tasksche.exe (86721)
(F) m_dutch.wnry (7a8d4)	Related_To	(F) tasksche.exe (86721)
(F) m_english.wnry (fe68c)	Related_To	(F) tasksche.exe (86721)
(F) m_filipino.wnry (08b9e)	Related_To	(F) tasksche.exe (86721)
(F) m_finnish.wnry (35c2f)	Related_To	(F) tasksche.exe (86721)
(F) m_french.wnry (4e571)	Related_To	(F) tasksche.exe (86721)
(F) m_german.wnry (3d59b)	Related_To	(F) tasksche.exe (86721)
(F) m_greek.wnry (fb4e8)	Related_To	(F) tasksche.exe (86721)
(F) m_indonesian.wnry (3788f)	Related_To	(F) tasksche.exe (86721)
(F) m_italian.wnry (30a20)	Related_To	(F) tasksche.exe (86721)
(F) m_japanese.wnry (b77e1)	Related_To	(F) tasksche.exe (86721)
(F) m_korean.wnry (6735c)	Related_To	(F) tasksche.exe (86721)
(F) m_latvian.wnry (c33af)	Related_To	(F) tasksche.exe (86721)
(F) m_norwegian.wnry (ff70c)	Related_To	(F) tasksche.exe (86721)
(F) m_polish.wnry (e79d7)	Related_To	(F) tasksche.exe (86721)
(F) m_portuguese.wnry (fa948)	Related_To	(F) tasksche.exe (86721)
(F) m_romanian.wnry (313e0)	Related_To	(F) tasksche.exe (86721)
(F) m_russian.wnry (45261)	Related_To	(F) tasksche.exe (86721)
(F) m_slovak.wnry (c911a)	Related_To	(F) tasksche.exe (86721)

(F) m_spanish.wnry (8d616)	Related_To	(F) tasksche.exe (86721)
(F) m_swedish.wnry (c7a19)	Related_To	(F) tasksche.exe (86721)
(F) m_turkish.wnry (531ba)	Related_To	(F) tasksche.exe (86721)
(F) m_vietnamese.wnry (8419b)	Related_To	(F) tasksche.exe (86721)
(F) r.wnry (3e002)	Related_To	(F) tasksche.exe (86721)
(F) r.wnry (3e002)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)
(F) s.wnry (025ac)	Related_To	(F) tasksche.exe (86721)
(F) s.wnry (025ac)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)
(F) taskdl.exe (4fef5)	Related_To	(F) tasksche.exe (86721)
(F) taskse.exe (84954)	Related_To	(F) tasksche.exe (86721)
(F) u.wnry (7bf2b)	Related_To	(F) tasksche.exe (86721)
(F) u.wnry (7bf2b)	Related_To	(F) 4da1f312a214c07143abeeafb695d904 (4da1f)
(U) http[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Related_To	(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
(P) 80	Related_To	(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
(H) GET / HTTP/1.1	Related_To	(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
(W) Domain Name: IUQERFS	Characterizes	(D) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Mitigation Recommendations

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov/malware (anonymous)

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

TLP:WHITE