

- [Trend Micro](#)
- [About TrendLabs Security Intelligence Blog](#)

- 
- 
- 
- 
- 



Search:

- [Home](#)
- [Categories](#)

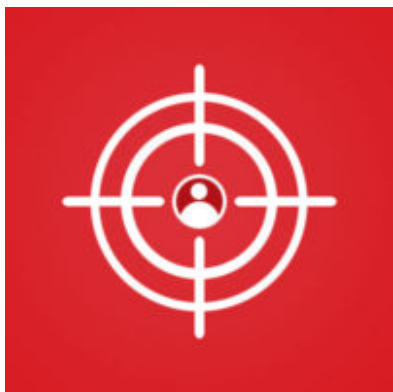
[Home](#) » [Malware](#) » BLACKGEAR Espionage Campaign Evolves, Adds Japan To Target List

BLACKGEAR Espionage Campaign Evolves, Adds Japan To Target List

- Posted on: [October 27, 2016](#) at 1:00 am
- Posted in: [Malware](#), [Targeted Attacks](#)
- Author: [Trend Micro](#)

0

 27   95  



By Joey Chen and MingYen Hsieh

BLACKGEAR is an espionage campaign which has targeted users in Taiwan for many years. Multiple papers and talks have been released covering this campaign, which used the ELIRKS backdoor when it was first discovered in 2012. It is known for using blogs and microblogging services to hide the location of its actual command-and-control (C&C) servers. This allows an attacker to change the C&C server used quickly by changing the information in these posts.

Like most campaigns, BLACKGEAR has evolved over time. Our research indicates that it has started targeting Japanese users. Two things led us to this conclusion: first, the fake documents that are used as part of its infection routines are now in Japanese. Secondly, it is now using blogging sites and microblogging services based in Japan for its C&C activity.

This post will discuss this C&C routine, the tools used in these attacks, and the connections between these tools.

C&C configuration retrieval

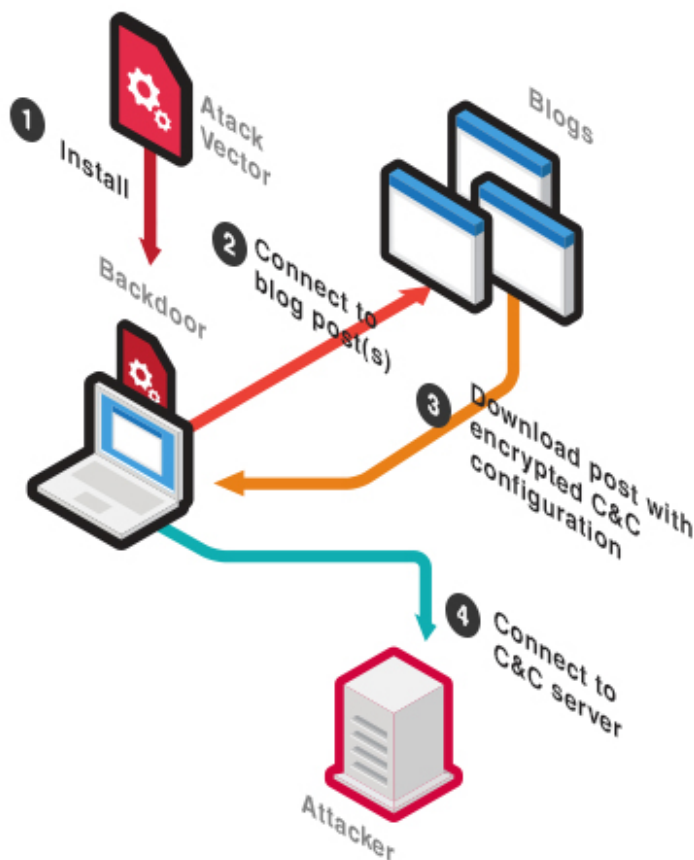


Figure 1. Overview of C&C configuration retrieval method

Backdoors used by BLACKGEAR share a common characteristic: they all retrieve encrypted C&C configuration information from blogs or microblogs. An attacker would register an account on these services and then create posts. The encrypted C&C information would be between two hardcoded tags, as seen below:

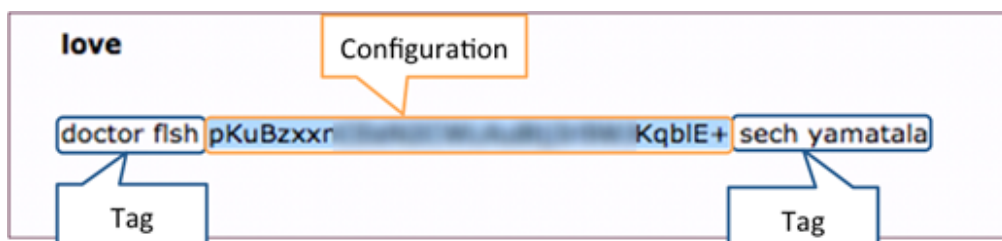


Figure 2. Encrypted configuration information between tags

There are two reasons BLACKGEAR would use this technique. First, the beacon traffic of the backdoor would look like normal traffic to blogs. Secondly, the threat actor would be able to quickly change the C&C servers used if these were blocked. A defender would be unable to block this change in server from reaching any affected machines unless the legitimate site was blocked as well.

Tools Used by BLACKGEAR

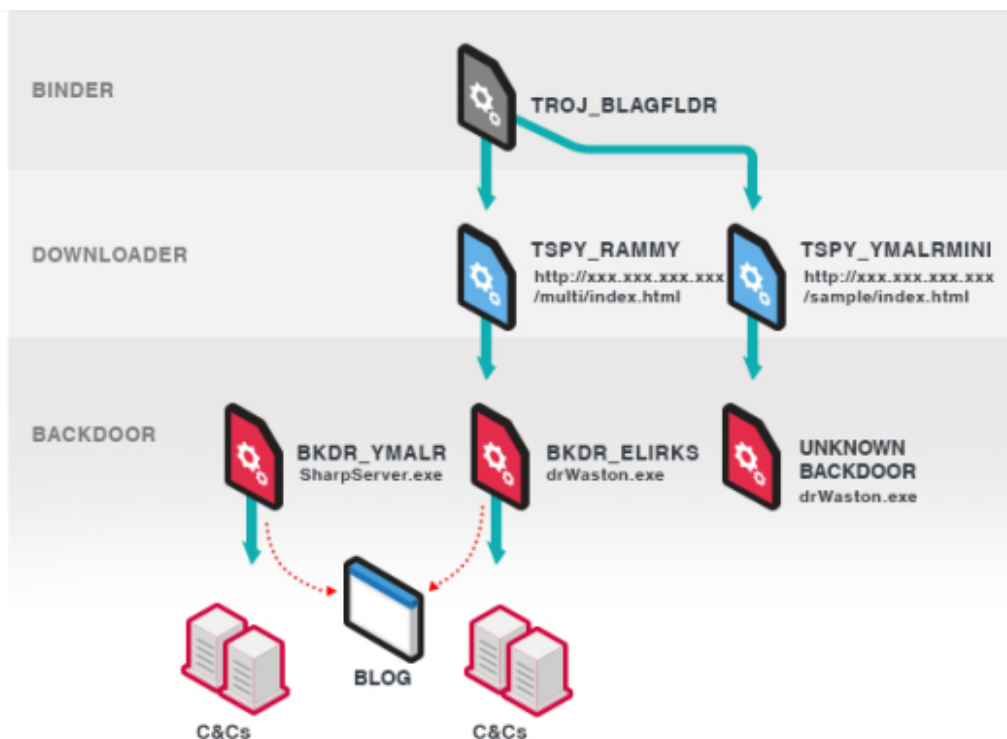


Figure 3. Tools used by BLACKGEAR campaign

The malware tools used by BLACKGEAR can be categorized into three categories: binders, downloaders and backdoors. Binders are delivered by attack vectors (such as phishing and watering hole attacks) onto a machine. These, in turn, drop decoys and downloaders. The latter connect to various sites under the control of the attacker and downloads backdoors. These use persistent methods to ensure that they remain present on the affected machines to give attackers access to the machine in question.

By separating the attack tools into three stages, threat actors are able to adapt quickly. If one component is detected and/or blocked, it can be replaced without disrupting the entire toolset.

Binder

The binder (which we detect as the TROJ_BLAGFLDR family) hides as a normal folder by changing its icon to a folder icon. Once the victim executes it, it executes the downloader in the background, drops a decoy folder that includes fake documents, then delete itself. This is so the victim won't notice that the malicious downloader has been executed.

Downloader

TSPY_RAMNY

TSPY_RAMNY is a downloader dropped by TROJ_BLAGFLDR malware. To remain persistent, it moves itself to the Windows *temp* folder and drops a **.lnk* (Windows Shortcut) file in the startup folder that points to itself. It also sends information about the compromised host (such as network settings) back to the download site.

The download link is formatted in the following format:

- `http://{IP address}/{folder name}/{webpage name}` (Example: `http://{IP address}/multi/index.html`)

This is done so that if someone looks solely at the URL, the download of the backdoor will appear to be an ordinary website.

TSPY_YMALRMINI

TSPY_YMALRMINI is another downloader that is dropped by TROJ_BLAGFLDR malware, which also sends information about compromised hosts back to the download site. We were unable to determine which payloads were used by this downloader. However, our research indicates

that some of these downloads are saved as *drWaston.exe* on the compromised host. This same file name is also used by some ELIRKS variants, indicating a possible connection. TSPY_YMALRMINI uses the same URL format as RAMNY.

TSPY_YMALRMINI has the same download link pattern as TSPY_RAMNY. The family name for this malware is because some variants have the PDB string “C:\toolson-mini\YmailerCreator – Debug\Binder\Binder\YMailer.pdb” . In addition, these variants also create a log file named *YmailerMini.log*.

Backdoors

BKDR_ELIRKS

BKDR_ELIRKS was the first family of backdoors tied to BLACKGEAR. It retrieves encrypted C&C configuration information from various blogging or microblogging services. Once decoded, it connects to these C&C servers and waits for commands given by a threat actor. To remain persistent, it moves itself to the Windows *temp* folder and drops a **.lnk* (Windows Shortcut) file in the startup folder that points to itself.

Its backdoor routines include getting information from the compromised host, downloading and running files, taking screenshots, and opening a remote shell.

BKDR_YMALR

BKDR_YMALR is a backdoor written using the .NET framework which is also known as LOGEDRUT. The detection name comes from a log file created by this malware family named *YMailer.log*. Its behavior is similar to ELIRKS – both in terms of C&C information retrieval and available commands to a threat actor.

Encryption and Decryption

BKDR_ELIRKS

Reverse analysis of ELIRKS allowed us to determine how to decrypt the C&C information, which is done in the following Python code:

```
#!/usr/bin/env python

from ctypes import *

def decipher(v, k):
    y=c_uint32(v[0])
    z=c_uint32(v[1])
    sum=c_uint32(0xC6EF3720)
    delta=c_uint32(0x61C88647)
    n=32
    w=[0,0]

    while(n>0):
        z.value -= (y.value + sum.value) ^ (y.value * 16 + k[2]) ^ (( y.value >> 5 ) + k[3])
        y.value -= (z.value + sum.value) ^ (z.value * 16 + k[0]) ^ (( z.value >> 5 ) + k[1])
        sum.value += delta.value
        n -= 1

    w[0]=y.value
    w[1]=z.value

    return w

if __name__ == '__main__':
    key = [0x8F3B39F1, 0x8D3FBD96, 0x473EAA92, 0x502E41D2]
    ciphertext = [ciphertext1, ciphertext2] # you can input cipher text here
    res = decipher(ciphertext, key)
    plaintext = "%X" % (res[0])
    c4 = str(int("0x"+plaintext[6:8],16))
    c3 = str(int("0x"+plaintext[4:6],16))
    c2 = str(int("0x"+plaintext[2:4],16))
    c1 = str(int("0x"+plaintext[:2],16))
    print c4+"."+c3+"."+c2+"."+c1
```

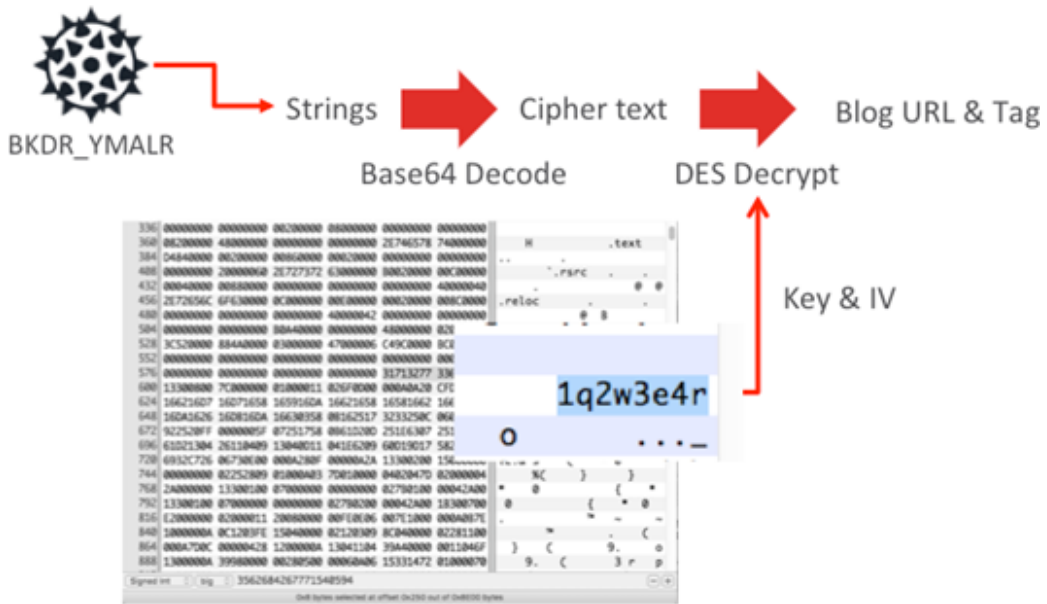



Figure 7. BKDR_YMALR decryption algorithm

Once these have been decoded, BKDR_YMALR uses the same algorithm as ELIRKS to obtain the C&C information.

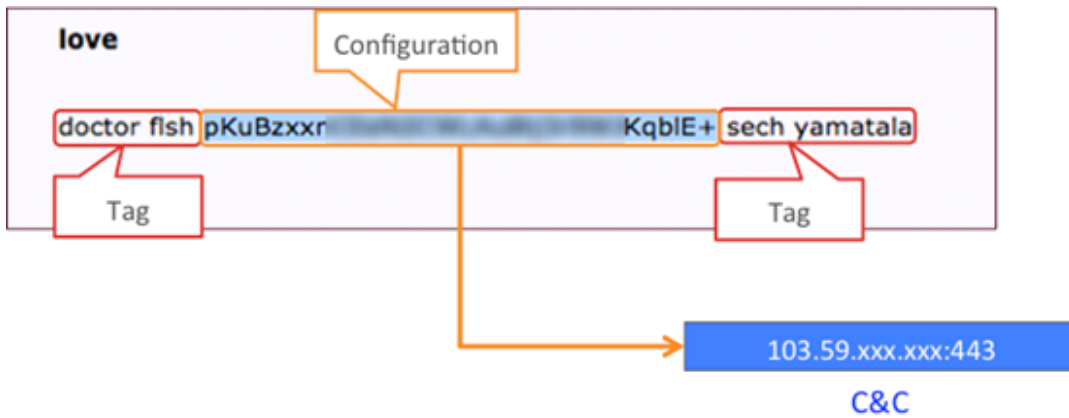


Figure 8. BKDR_YMALR configuration from the blog post blog

Connections between tools

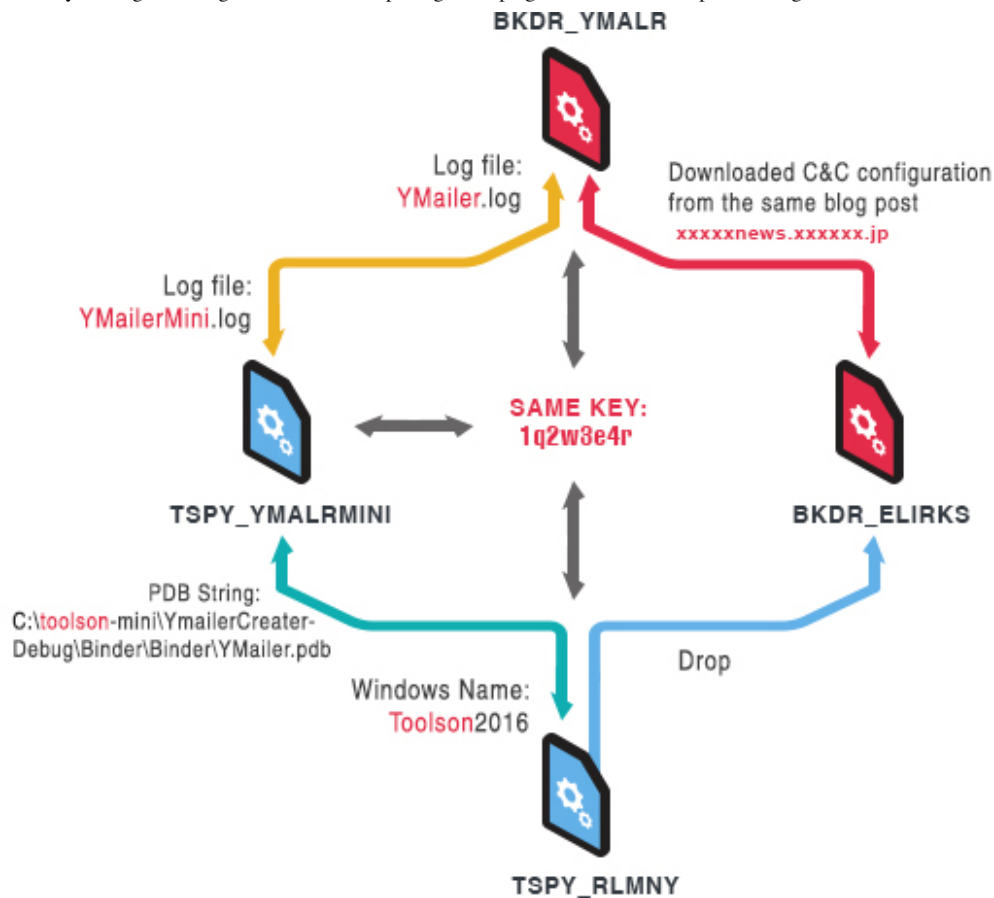


Figure 9. Connections between tools

More than just tools being used together, it appears that there are distinct connections between the different tools used by BLACKGEAR. The string “YMailer” shows up in the filenames of log files used by both BKDR_YMALR and TSPY_YMALRMINI, and it is in the PDB strings of the latter. The two downloaders TSPY_RLMNY and TSPY_YMALRMINI both use the string *toolson* in different places. Lastly, both downloaders and one backdoor share the same decryption key *1q2w3e4r*. The above illustration shows the connections between the families.

Conclusion

Malware threats need to evolve or otherwise become non-threats. Similarly, to stay relevant, BLACKGEAR has evolved with both new tools and new targets, and will continue to be a threat for the foreseeable future. We will continue to monitor its activities in order to protect our customers.

Indicators of Compromise (IOCs)

TROJ_BLAGFLDR

- 52d6b30bc578465d8079d9abd0d4c4826b51b25f
- 800c7d54280f5f35e3b58a6d4dfd4845f6ed9e15
- 8b6614562a79a13e60d100a88f1ba4eb601636db
- 98efee8dde7d493c0d35d02a2170b6d1b52987d3

TSPY_RAMNY

- 02785ebcb683a380c80958f3fe2a52f805c5c12d
- 74031e70ca3b4004c6b7a8197397882bc02c30cb
- b4c63a0ff9b8eb8cc1a53a4dd036e93f9eeceeca

TSPY_YMALRMINI

- 048790098a7c6b8405761b75ef2a2fd8bd0560b6
- 96f3b52460205f6ecc6b6d1a73f8db13c6634afc

BKDR_ELIRKS

- 17cacabc78c4b164bb0e7d9200289be9236e7bc
- 4157ecd252dc09b533fcf6a778aca2c376601354
- 4f54cfcf266b73ca3759b9cb0252c27094b5b330
- 521a9d73191c7740f969ae3c53e6abf70ffbedf9
- 533565f7953fb1648d437d14d007003c6343b9ae
- 80108d2aacb0a1f2a5350f71e7a04239fc5f96a9
- 8cad1bcbdd558802b34119fb57160cc748170133
- 9a768fae41ca7395b4257e85acef915e124c2981
- a70001c67e81d1dcf62f808760514b6df28a411a
- a9ea07caafeb63133e5131f7a56bc8da1bc3d72a
- dd0ceafbe7f4bf2905e560c3348545e32bc0f684

BKDR_YMALR

- 02fed8cae7f3986c1344dd75d869ba23cfc4073a
- 09d73b522f36786bb6e645b96f244bb51c3cc7ea
- 0a59d52367435bc22a92c27d60023accec575a5fb
- 0cc74332b1e213456693159d3ba12a3421036f68
- 1120f049dcb4a62809687dc277b42589d8d1caa6
- 12c8cc7e125572d614b708c056f7fd0ed49870c5
- 29b08d270ba6efcf57ca2ad33d8e3edd93d6b32a
- 2d3d7b9521aec637f2e99624e0489b9f140d463f
- 2de7d78615ec0bf2652790d53b50ddb0472292c
- 31de946255b240c0ae2f56786ac25183f3aeea5
- 3aa8509715c7f55bdee831d5f7db22a2c516db43
- 3d175b1defe7076e0fe56076dd0d5f438de43324
- 4000244b2cba78a45034bb6ab2bac46d6a8a79ea
- 4882735e8a465fac938fd04546a51efefb9806da
- 48d373bdb31dcecd7f59bd5a964d062c8b6bfce8
- 49f6eb7f8e4a27f574c9a3e8c0da0b7895df7e41
- 4c7df09012fc88d336467691acf0afce64f40341
- 551f9a60203bec904487113e8d42dea463ac6ca9
- 5a4b15fa5a615a93191ede4c75dd3e65e87586dc
- 5aa5117db6f420c81d2e1a7f036963a3c6ef02e9
- 5dc007d056513cba030ec16e15bdbb9ea5fe0e5a
- 628309a60ad1fbe240486519de1424f7ddc2df4d
- 636e7a9effb1a244697c880832e486de56260527
- 6bb5f51d03edd1acd7d38cca8095a237543c6a0d
- 6c4786b792f13643d408199e1b5d43f6473f5eea
- 6dd997409afec6fafbe54bd9d70d45ffff6a807
- 7142ca7079da17fa9871cbc86f7633b3253aeaed
- 7254b719fd3cf87c8ac8ed9327c8e1bf99abf7af
- 7329a789363f890c401c286dbaf3d2bf79ee14f7
- 7b2c4d14710cf2fd53486399ecc5af85cd75eca6
- 88e22933b76273793e4278c433562fb0b4fe125a
- 8917c582ab5c2e831de6eba33b4f19d6e3a2cb70
- 8c325e92bf21d0c3737dbbc596854bc12184eeaf
- 8f65cbde2f3b664bcde3822a19765bdb7f58099
- 9047b6b2e8fbaa8a06b2faaa30e038058444106a
- 93c3f23905599df78cd5416dd9f7c171b3f1e29e
- 94750bdae0fa190116a68e96d45f3d46c24b6cf1
- 9954a1c8e7b0e2f17841608f6b8c9d042b7a0780
- 9b96646d152583ff58c2c29191cb1672847d56b6
- 9f5a3b6db752d617f4d278d6531e2bbdb7faa977
- a30cc98ceb5d3379e80443f68a186326926f73ce
- a893896af5468ac6e04cdd13edff8cae04800848
- a8f461749c7fe2a21116b8390cf84a8300009321
- a9108bf3ce39cea40e46ac575247a9a7c077b2a8
- a9fd9ade807af4779f3eea39fed2c583a50c8497
- ac014e4c2d68f6c982ac58738857b698b9e46af5
- acaec2b0f86ec4262be5bb8bcebcc12093e071ba
- ad61c51b03022ef6bcb5e9738fe2f621e970ecb3
- b28f6ba3d6571c5d85cb5276cbcdce9adf49d5a9
- bc61f1b3c8eb3bda2071f6caf71ff23705128ca5
- c30b305a7bea9a2f61aca2dbcf596c2b0c0e4fa0
- c4c747f26f95fdbfc5bff04688dc76ae0bb48fff
- c58d6fc761dec675ab45ad5c3682ffc9936cf357

- c85f528900aa9d836abd88eb56902efd711491da
- ca163d6ae85edede87b271267918a0ffe98040c7
- cf629249fb4af86746059e638ccef5b8a43c6834
- cfd9a67b4b0eb3d756bb7e449b46687e6aef006b
- d107268bd767a2dfe1c8733b7da96c1a64f5d112
- d7cd079f8485ea55443ed497f055dbed5ae4a668
- d95c97f1525e9888571f498f2be584dda243da2a
- e01f9ba6355bc7ccf89261658bff9f965b8c21
- e05efde2b442dc4119179e3c39c74a973499e271
- e1acfed710f186d86a2bc8179ff38fdd21f9a1b6
- e1fb2e1866f332a5656bf55fde13ff57d5f0bbf6
- e77303d80968395eec008515ea9eb3c620b14255
- eb9e553524d414d862857297baf44da3b4072650
- eca06f3c535ba3b3463917974a79efc821fdbb6c
- eeb065a1963a8ad0496e61305c076c5946d77e12
- efa611262e6d4804ce9026d50bfa64f20d9271ca
- fb59481d153388d2ad3bb6321d0b2875cb07f4d3
- fbcbbc187e99317c5a36a3667592590a7f5a17d1



Related Posts:

- [Pawn Storm Campaign Adds Turkey To Its List of Targets](#)
- [Helper for Haima iOS App Store Adds More Malicious Behavior](#)
- [New Open Source Ransomware Based on Hidden Tear and EDA2 May Target Businesses](#)
- [BEBLOH Expands to Japan in Latest Spam Attack](#)



Say NO to ransomware.

Trend Micro has **blocked over 100 million** threats and counting

Learn how to protect Enterprises, Small Businesses, and Home Users from ransomware:

[ENTERPRISE >>](#)

[SMALL BUSINESS >>](#)

[HOME >>](#)

Tags: [BLACKGEARELIRKS](#)

Comments for this thread are now closed.



0 Comments TrendLabs

1 Login ▾

♥ Recommend Share

Sort by Best ▾

This discussion has been closed.

Subscribe Add Disqus to your site Add Privacy

Featured Stories

- [Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patched](#)
- [New Bizarro Sundown Exploit Kit Spreads Locky](#)
- [The Internet of Things Ecosystem is Broken. How Do We Fix It?](#)
- [CVE-2016-3298: Microsoft Puts the Lid on Another IE Zero-day Used in AdGholas Campaign](#)
- [FastPOS Updates in Time for the Retail Sale Season](#)

Business Email Compromise

- How can a sophisticated email scam cause more than \$2.3 billion in damages to businesses around the world?
[See the numbers behind BEC](#)

Latest Ransomware Posts

[Mobile Ransomware: How to Protect Against It](#)

[Mobile Ransomware: Pocket-Sized Badness](#)

[HDDCryptor: Subtle Updates, Still a Credible Threat](#)

[Businesses as Ransomware's Goldmine: How Cerber Encrypts Database Files](#)

[New Bizarro Sundown Exploit Kit Spreads Locky](#)

Recent Posts

- [Mobile Ransomware: How to Protect Against It](#)
- [Home Routers: Mitigating Attacks that can Turn them to Zombies](#)
- [Patch Tuesday of December 2016: Microsoft Releases 12 Bulletins, Six Critical](#)
- [Leaking Beeps: IT Systems Broadcasting Sensitive Info](#)
- [Mobile Ransomware: Pocket-Sized Badness](#)

Ransomware 101

- This infographic shows how ransomware has evolved, how big the problem has become, and ways to avoid being a ransomware victim.
[Check the infographic](#)

Popular Posts

[CEO Fraud Email Scams Target Healthcare Institutions](#)
[One Bit To Rule A System: Analyzing CVE-2016-7255 Exploit In The Wild](#)
[Hacking Team Flash Zero-Day Integrated Into Exploit Kits](#)
[Businesses as Ransomware's Goldmine: How Cerber Encrypts Database Files](#)
[Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patched](#)

Latest Tweets

- Common attack types and vulnerabilities in the network can be revealed through leaked pages. Find out how:… [twitter.com/i/web/status/8…](#)
[about 50 mins ago](#)
- Aside from HDDCryptor, other earlier discovered #ransomware families continue to make their presence felt. Details: [bit.ly/2gyB8f5](#)
[about 9 hours ago](#)
- What are the types of attacks do home networks usually contend with? Here's what we found out:… [twitter.com/i/web/status/8…](#)
[about 12 hours ago](#)

Stay Updated

Email Subscription

- [Home and Home Office](#)
- |
- [For Business](#)
- |
- [Security Intelligence](#)
- |
- [About Trend Micro](#)
- Asia Pacific Region (APAC): [Australia](#) / [New Zealand](#), [中国](#), [日本](#), [대한민국](#), [台灣](#)
- Latin America Region (LAR): [Brasil](#), [México](#)
- North America Region (NABU): [United States](#), [Canada](#)
- Europe, Middle East, & Africa Region (EMEA): [France](#), [Deutschland](#) / [Österreich](#) / [Schweiz](#), [Italia](#), [Р о с с и я](#), [España](#), [United Kingdom](#) / [Ireland](#)
- [Privacy Statement](#)
- [Legal Policies](#)
- Copyright © 2016 Trend Micro Incorporated. All rights reserved.