THREAT TRENDS OF 2017
Operation Cloud Hopper: China-based Hackers Target Managed Service Providers

By Kevin Townsend on April 06, 2017

A widespread campaign known to be targeting managed service providers (MSPs) in at least fourteen countries has been tied to the group known as APT10 and is thought to be operating out of China. These are the conclusions of a new report published this week by PwC UK and BAE Systems.
ВНИМАНИЮ ПОЛЬЗОВАТЕЛЕЙ!

27.06.2017 | 4422

Внимание!

На наши сервера осуществляется вирусная атака.

Просим прощения за временные неудобства!

Operation Cloud Hopper: China-based Hackers Target Managed Service Providers

By Kevin Townsend on April 06, 2017

A widespread campaign known to be targeting managed service providers (MSPs) in at least fourteen countries has been tied to the group known as APT10 and is thought to be operating out of China. These are the conclusions of a new report published this week by PwC UK and BAE Systems.
Ukranian company that spread Petya could face criminal charges for vulnerability

*The hack was easier than we thought*

by Russell Brandom | @russellbrandom | Jul 3, 2017, 3:00pm EDT

---

Operation Cloud Hopper: China-based Hackers Target Managed Service Providers

By Kevin Townsend on April 06, 2017

A widespread campaign known to be targeting managed service providers (MSPs) in at least fourteen countries has been tied to the group known as APT10 and is thought to be operating out of China. These are the conclusions of a new report published this week by PwC UK and BAE Systems.
Ukrainian company that spread Petya could face criminal charges for vulnerability

The hack was easier than we thought
by Russell Brandom | @russellbrandom | Jul 3, 2017, 3:00pm EDT

CCleaner accidentally includes Flouxif malware to its latest version

Mark Padin | Published 02 October 2017 | 11:07 PM

Operation Cloud Hopper: China-based Hackers Target Managed Service Providers

By Kevin Townsend on April 06, 2017

A widespread campaign known to be targeting managed service providers (MSPs) in at least fourteen countries has been tied to the group known as APT10 and is thought to be operating out of China. These are the conclusions of a new report published this week by PwC UK and BAE Systems.
INTERNET OF THINGS

Report: Mirai Botnet DDoSed 17 Dyn Data Centers Globally

That's all but three of the DNS service provider's sites.

Yevgeniy Sverdlik | Oct 26, 2016
Friday's DDoS attack came from 100,000 infected devices

DNS service provider Dyn says Mirai-powered botnets were the primary source for Friday's disruption

By Michael Kan
U.S. Correspondent, IDG News Service | OCT 27, 2016 5:01 AM PT

Dyn Data Centers Globally

That's all but three of the DNS service provider's sites.

Yevgeniy Sverdlik | Oct 26, 2016
**NEWS**

Friday's DDoS attack came from 100,000 infected devices

DNS service provider Dyn says Mirai-powered botnets were the primary source for Friday's disruption

By Michael Kan
U.S. Correspondent, IDG News Service | OCT 27, 2016 5:01 AM PT

Dyn Data Center

That's all but three of the DNS

Yevgeniy Sverdlik | Oct 26, 2016

root/xc3511
admin/admin
root/default
root/S4321
admin/password
user/user
admin/admin1234
admin/1111
root/1234
service/service
guest/12345
administrator/1234
ubnt/ubnt
root/hi3518
root/zlxx.
root/system
root/user
admin/1111111
admin/54321
admin/1234
tech/tech
root/vixxv
root/888888
root/juantech
support/support
root/root
admin/(none)
root/1111
root/666666
root/klv123
supervisor/supervisor
guest/12345
666666/666666
root/klv1234
root/jvbdz
root/7ujMko0vixxv
root/ikwb
root/realtek
admin/1234
admin/123456
admin/pass
mother/meric

Mirai's built-in password dictionary.
Friday's DDoS attack came from 100,000 infected devices

DNS service provider Dyn says Mirai-powered botnets were the primary source for Friday's disruption.

New Reaper IoT Botnet Leaves 378 Million IoT Devices Potentially Vulnerable to Hacking

BullGuard CEO Calls on the Security Industry and Device Manufacturers to Address the Growing Cyber Threat from Unprotected Smart Devices: Dojo by BullGuard Stops Reaper Botnet Dead
BREACHES IN 2017

- DBs and systems in public Internet
- PoS malware scraping credit card data
- Private information leaks primarily (90%):
  - Misconfigurations (e.g. poor passwords)
  - Security patches not installed
- Just US statistics: GDPR

Type of stolen information

- Credit card data
- Private information
Hi John,

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.
Hi John,

Someone just used your password! 
john.podesta@gmail.com

Details:
Saturday, 19 March, 8:34:30 U 
IP Address: 134.249.139.239 
Location: Ukraine 

Google stopped this sign-in attempt

CHANGE PASSWORD

Best, 
The Gmail Team

---

Please find attached invoice no: 892261

Attached is a Print Manager form. 
Format = Portable Document Format File (PDF) 

Disclaimer

This email/fax transmission is confidential and intended solely for the person or organisation to whom it is addressed. If you are not the intended recipient, you must not copy, distribute or disseminate the information, or take any action in reliance of it. Any views expressed in this message are those of the individual sender, except where the sender specifically states them to be the views of any organisation or employer. If you have received this message in error, do not open any attachment but please notify the sender (above) deleting this message from your system. For email transmissions please rely on your own virus check no responsibility is taken by the sender for any damage arising out of any bug or virus infection.
Good day to you, Toby.

I am bothering you for a very critical cause. Though we are not familiar, but I have a lot of data about you. The matter is that, most probably by mistake, the data of your account has been dispatched to me. For instance, your address is:

```
RESPONSE
NE3 4YD
```

I am a law-abiding citizen, so I decided to warn you that that was emailed to me, that you could explore what data has become available for deceivers. File password is - 1848.

Regards,

[Attached Print Manager form, PDF format, 47 KB]
INTERNET IS NOT FIT FOR NON-SECURED SERVICES