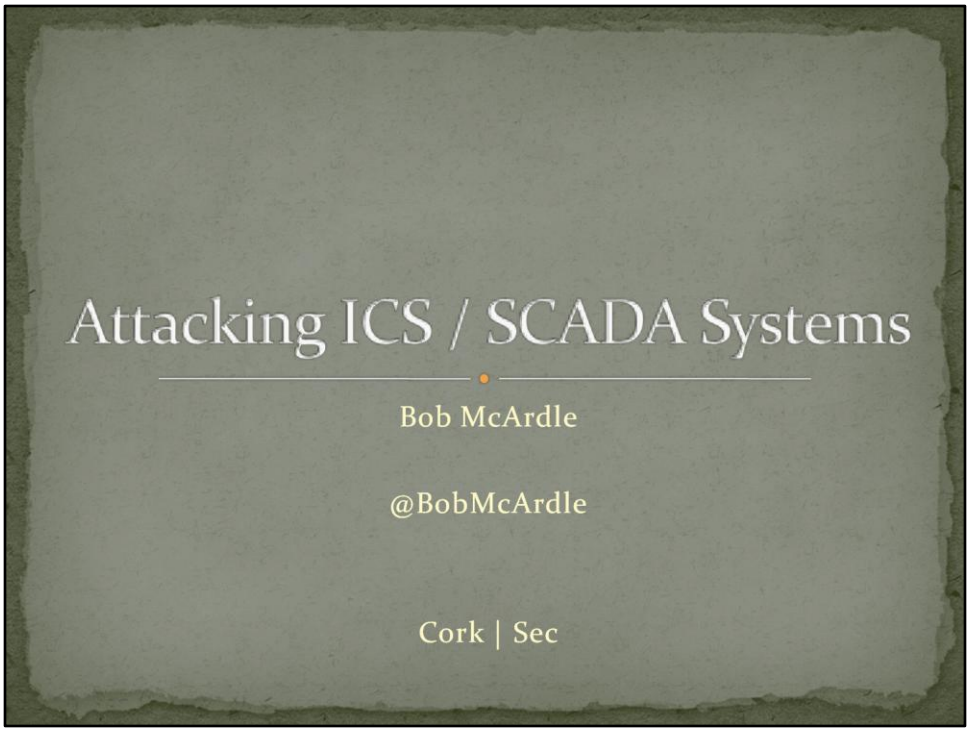
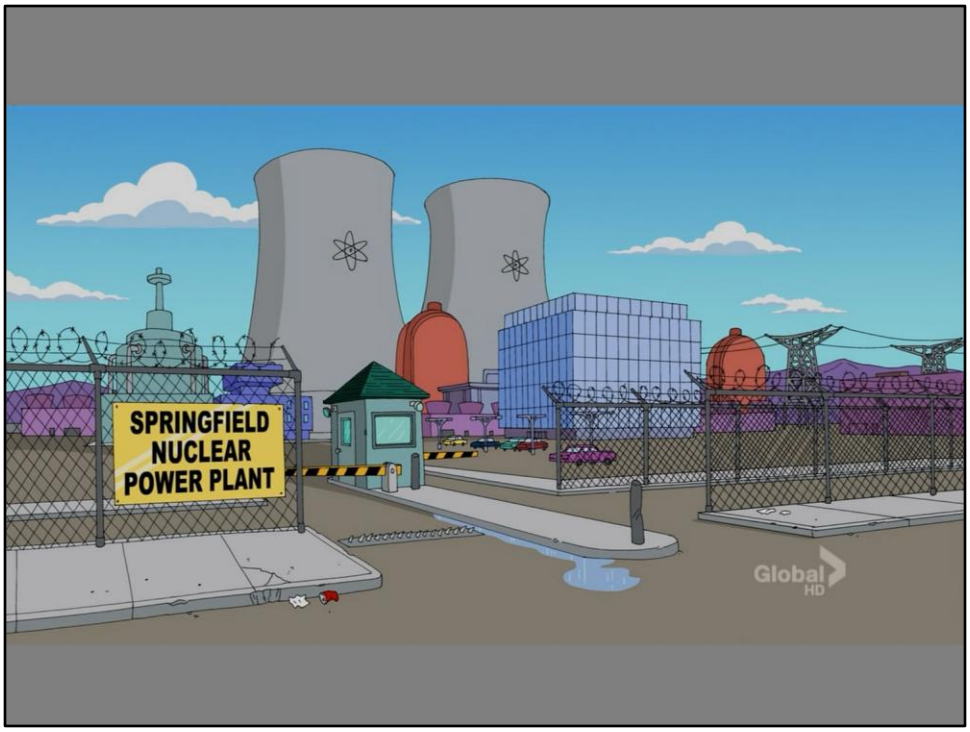
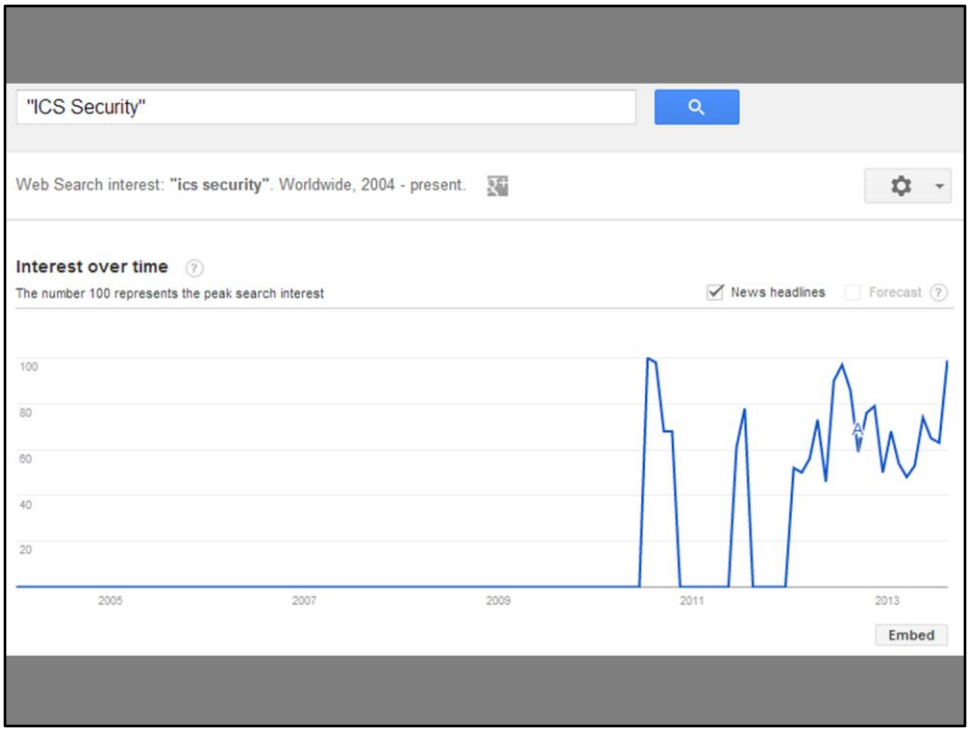


So - what I'm going to talk about for the next half hour is ICS and SCADA attacks. Before I start I want to be sure to give credit where credit is due, all of the research carried out here was from one of our team members in Trend Micro called Kyle Wilhoit. Kyle is travelling a lot these days talking about ICS and SCADA attacks, but if anyone wants to get in touch with him about this topic – just ask me later on.



So lets start with explaining those two terms – what does ICS or SCADA mean?

ICS stands for Industrial Control System, and SCADA which stands for Supervisory Control and Data Acquisition is a type of ICS. Essentially these two terms refer to devices that monitor and control industrial devices in the real world. These devices are used in the production of everything from water, gas, car manufacturing all the way to Nuclear facilities.



A couple of years ago nobody in the security industry was really talking about ICS or SCADA Security, as this Google Trends graph shows.

But in June 2010 all of that changed…

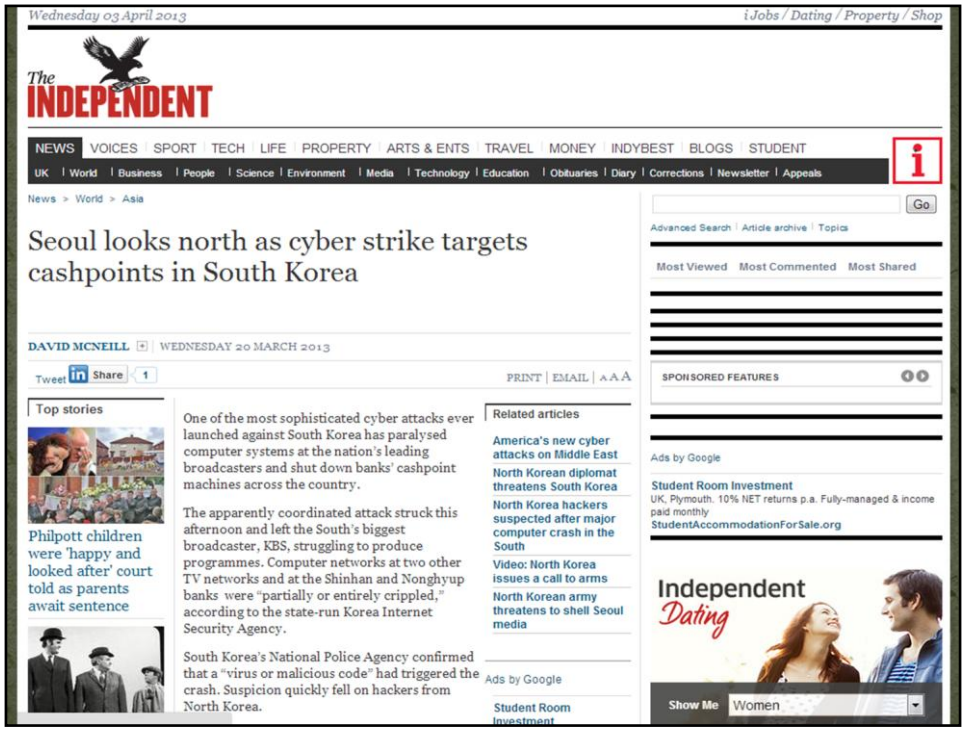
Because June 2010 was when the Stuxnet malware was discovered, which allegedly was targeted at the Uranium Enrichment facility at Natanz in Iran.

Now I don't think there is any need for me to describe Stuxnet to anyone in this room – but the incident did have a lot of interesting knock on effects…

For one it changed the way nations talked about the Cyber Offensive capabilities. For example - some nations that had originally being portraying themselves as unorganised on Cyber defence how started to push an image of strength, whereas others become more brazen in their attacks

Of course the media also had a great time with this story. Reporters who had never heard about the terms ICS and SCADA before where suddenly sticking the word Cyber in front of just about everything. In fact if you are already bored by my presentation and have smuggled some alcohol into the room, feel free to have a shot every time I mention Cyber – I'm pretty confident there is a doctor on site.

We have “Cyber Attacks” almost every day in the news (and no I have no idea what a girl smashing glass has to do with a CyberAttack)…



Wednesday 03 April 2013 — iJobs / Dating / Property / Shop

The INDEPENDENT

NEWS | VOICES | SPORT | TECH | LIFE | PROPERTY | ARTS & ENTS | TRAVEL | MONEY | INDYBEST | BLOGS | STUDENT

UK | World | Business | People | Science | Environment | Media | Technology | Education | Obituaries | Diary | Corrections | Newsletter | Appeals

News > World > Asia

Seoul looks north as cyber strike targets cashpoints in South Korea

DAVID MCNEILL | WEDNESDAY 20 MARCH 2013

Tweet | Share 1 | PRINT | EMAIL | A A A

Top stories

Philpott children were 'happy and looked after' court told as parents await sentence

One of the most sophisticated cyber attacks ever launched against South Korea has paralysed computer systems at the nation's leading broadcasters and shut down banks' cashpoint machines across the country.

The apparently coordinated attack struck this afternoon and left the South's biggest broadcaster, KBS, struggling to produce programmes. Computer networks at two other TV networks and at the Shinhan and Nonghyup banks were "partially or entirely crippled," according to the state-run Korea Internet Security Agency.

South Korea's National Police Agency confirmed that a "virus or malicious code" had triggered the crash. Suspicion quickly fell on hackers from North Korea.

Related articles

America's new cyber attacks on Middle East
North Korean diplomat threatens South Korea
North Korea hackers suspected after major computer crash in the South
Video: North Korea issues a call to arms
North Korean army threatens to shell Seoul media

Ads by Google

Student Room Investment

Go

Advanced Search | Article archive | Topics

Most Viewed | Most Commented | Most Shared

SPONSORED FEATURES

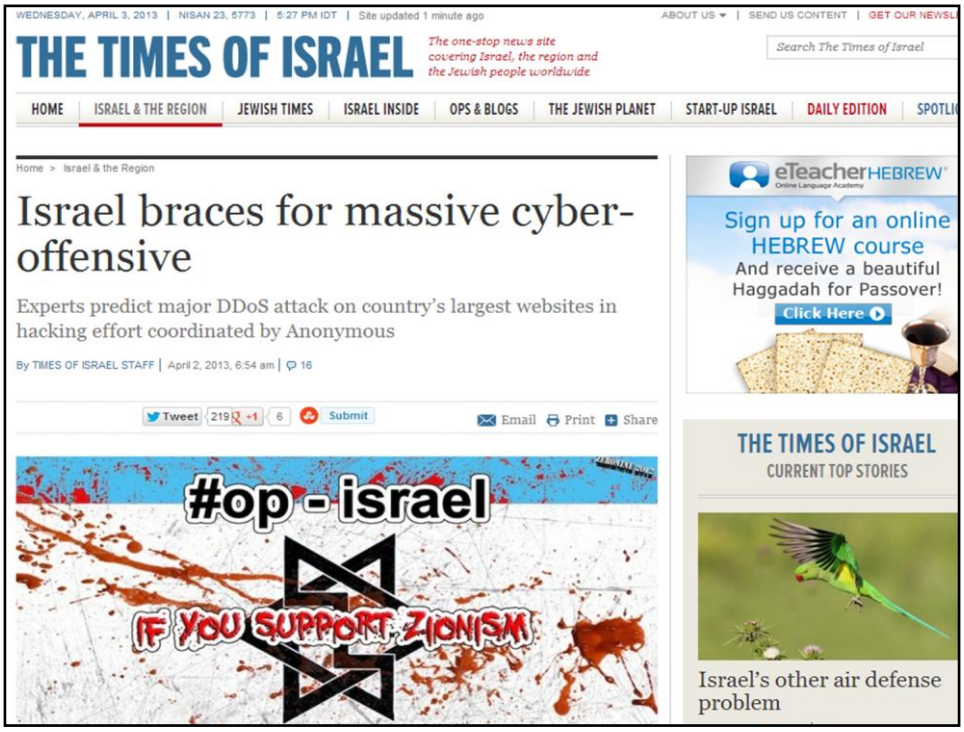
Ads by Google

Student Room Investment
UK, Plymouth. 10% NET returns p.a. Fully-managed & income paid monthly
StudentAccommodationForSale.org

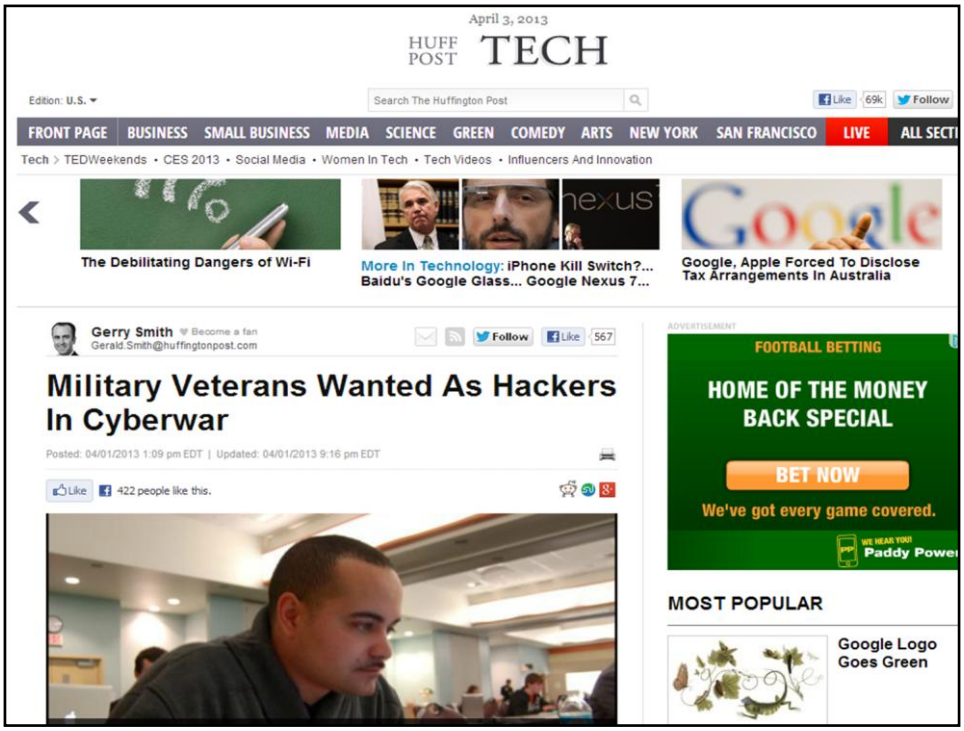
Independent Dating

Show Me Women

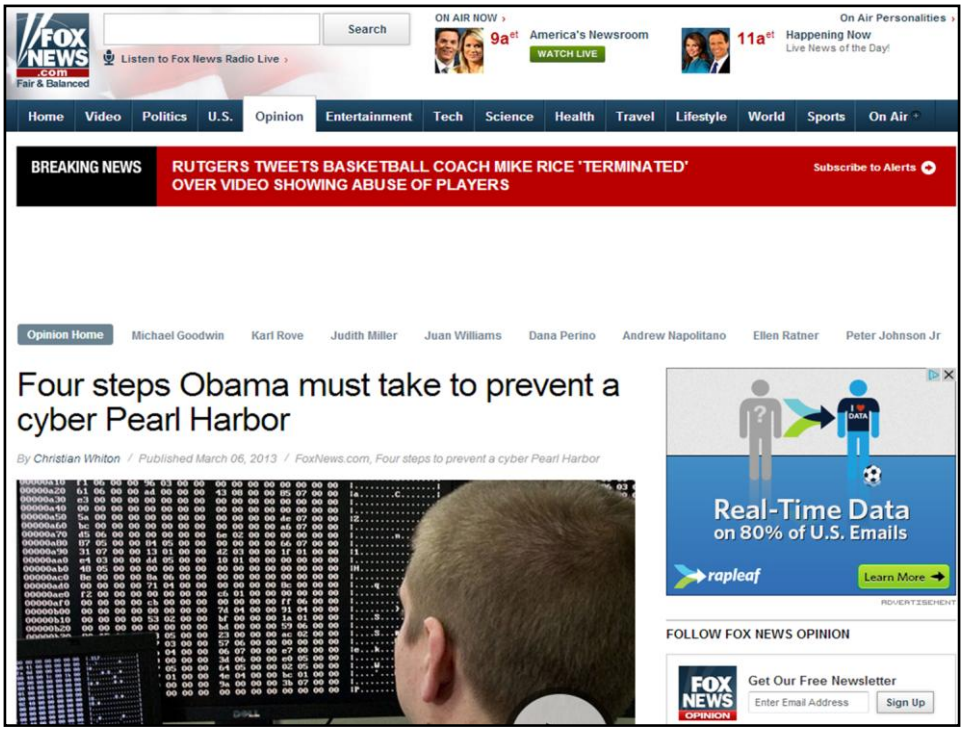
There are Cyber-Strikes carried out by countries on each other.



There are Cyber-Offensives.



Of course we have CyberWar…

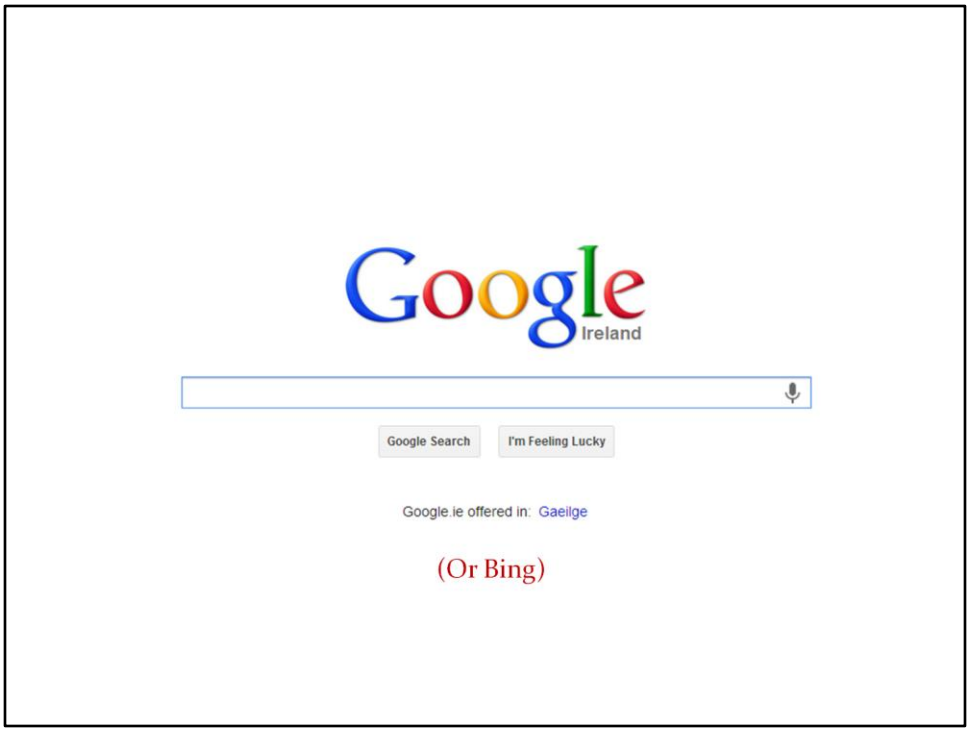


Cyber Pearl Harbours,… (what ever that means)

.. Cyber 9/11 .. (which makes even less sense)

And even the almighty Cyber Armageddon will soon be among us.

So with all of these talks about Cyber attacks against ICS and SCADA systems, just how easy is if for an attacker to find such as system. Well there are number of very powerful tools that attackers can use to quickly find potential targets, the first of these is to use …



Google – or of course Bing for the Microsoft fans in the room. Joking aside, Bing can actually be more powerful for these type of searches, with operators for searching IP ranges and other things. Lets look at a couple of examples of using Google to find ICS systems…

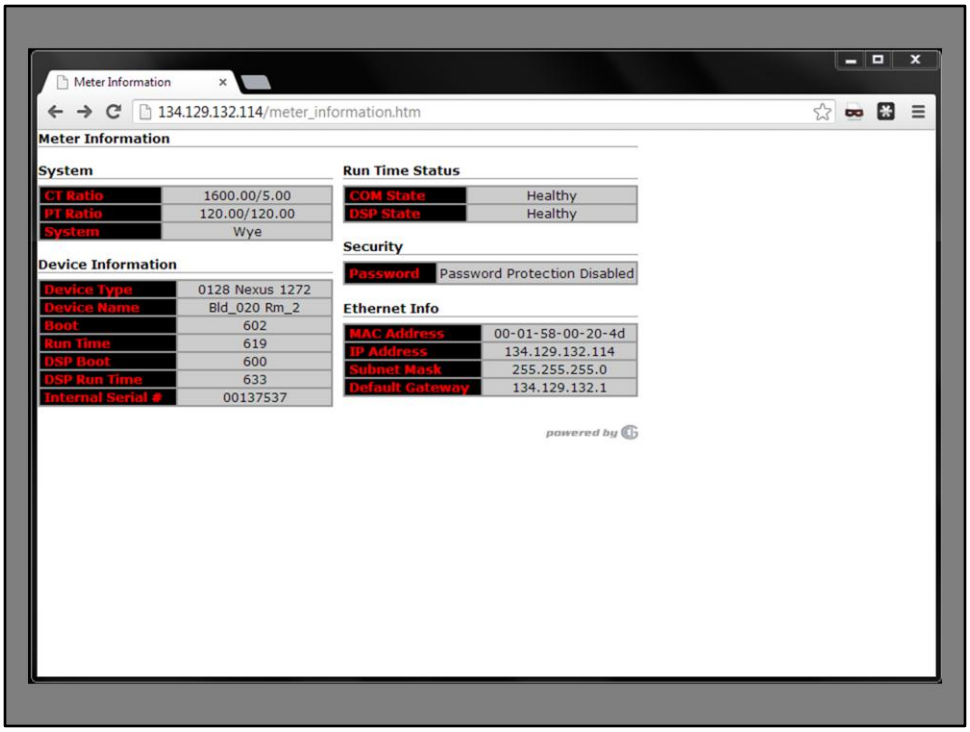
LIVE DEMO - SHOW:

inurl:meter_information.htm - Utility Energy Meter from Electro Industries/Gaugetech

SIMPLE GOOGLE DORK – IN FACT, THAT WOULD MAKE A GOOD TOPIC FOR A TALK IF ANYONE IS INTERESTED.

SHOW FIRST WEBCAM RESULT IN GOOGLE HACKS

More: http://www.exploit-db.com/google-dorks/

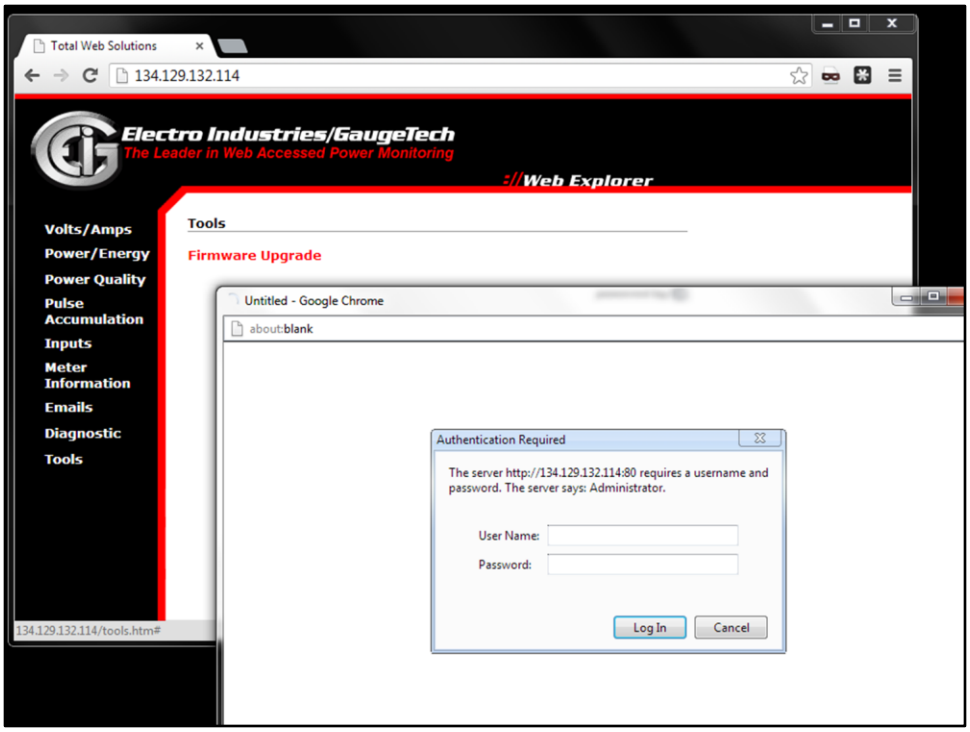


DEMO – HIDDEN BACKUP SLIDE IN CASE OF INTERNET ISSUES:

Searching for

inurl:meter_information.htm

will give you several results related to a Utility Energy Meter from Electro Industries/Gaugetech. Especially the results that have the meter_information.htm file directly on an IP are interesting, as these may be system that have been forgotten about by an Administrator. This panel is mostly just information – but still not information you want the entire world to have access to. However there are other more interesting panels in the same interface…



DEMO – HIDDEN BACKUP SLIDE IN CASE OF INTERNET ISSUES:

Under the tools menu you can do a Firmware Upgrade. This option is password protected but another quick Google will find you the install manual which contains the default username and password, or an attacker could simply brute force this.

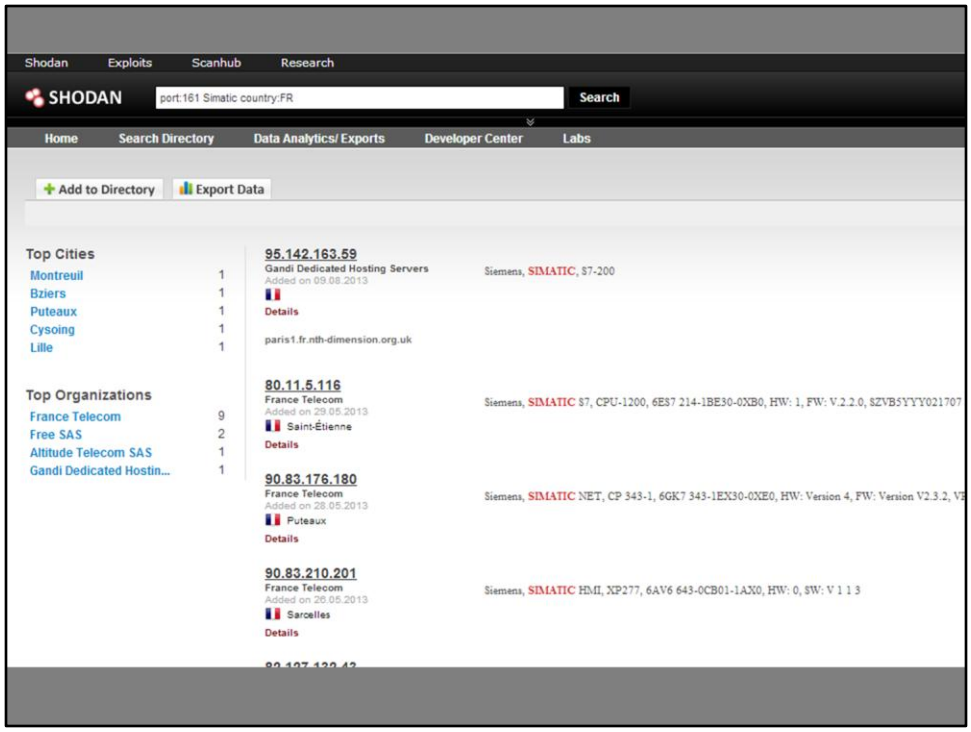
DEMO – HIDDEN BACKUP SLIDE IN CASE OF INTERNET ISSUES:

A more powerful tool available to attacker is Shodan. Unlike Google which is designed to help you find specific webpages, Shodan is a search engine that lets you find specific computers (routers, servers, etc). Think of it as a public port scan directory, or a search engine of banners.

There are many, many searches you can do to find ICS related machines – but just as a simple example I will search for the phrase

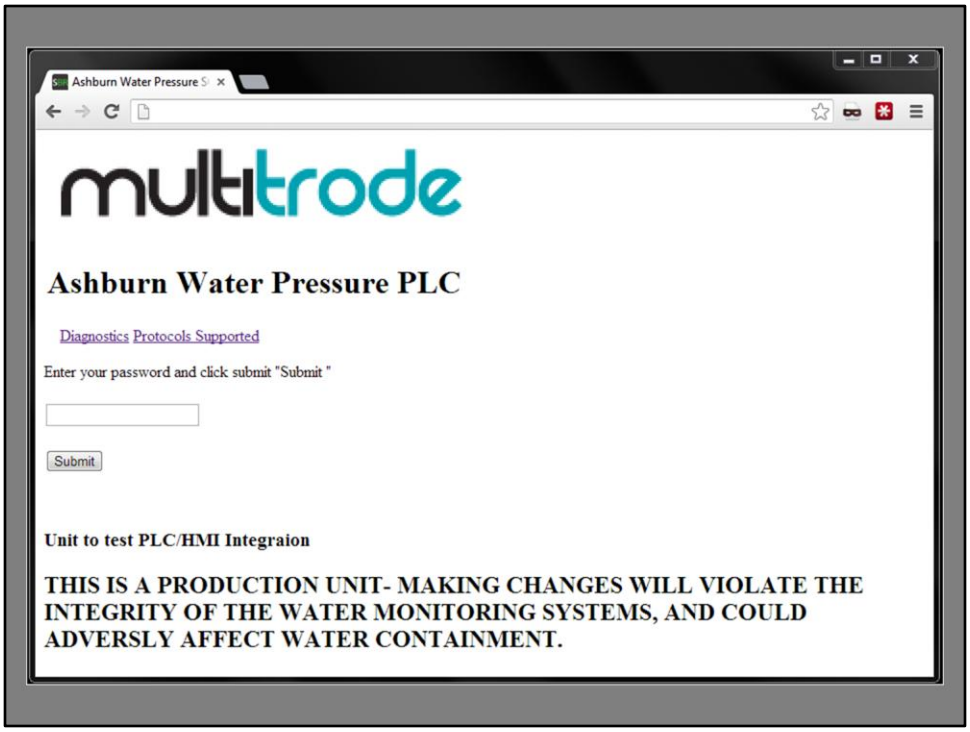
Port:161 Simatic country:FR

LIVE DEMO:



DEMO – HIDDEN BACKUP SLIDE IN CASE OF INTERNET ISSUES:

And here you can see the results. Simatic systems is a series of PLCs (Programmable Logic Controllers) from Siemens, commonly used in the control of process equipment and manufacturing machinery. I narrowed it down to French machines that have the SNMP port open. I picked that port as some Simatic systems have a DOS vulnerability on that service.

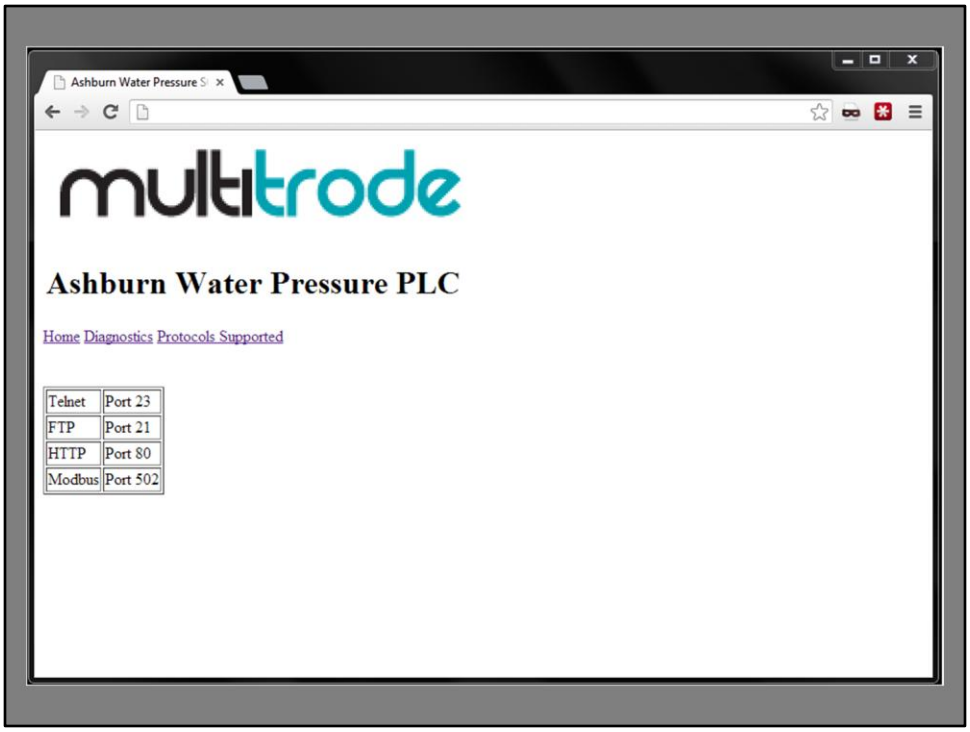


DEMO – HIDDEN BACKUP SLIDE IN CASE OF INTERNET ISSUES:

Speaking of ICS systems – here is one very good example I can across when researching this talk.

Here we see the main login page for Water Plant that is connected to the internet. The webpage is not much to look at, but they rarely are – this has been created by some admin to make his live easier – not to win any web design awards. You can see they where nice enough to include a warning banner

Right on the main page there are two links that require no authentication what so ever.

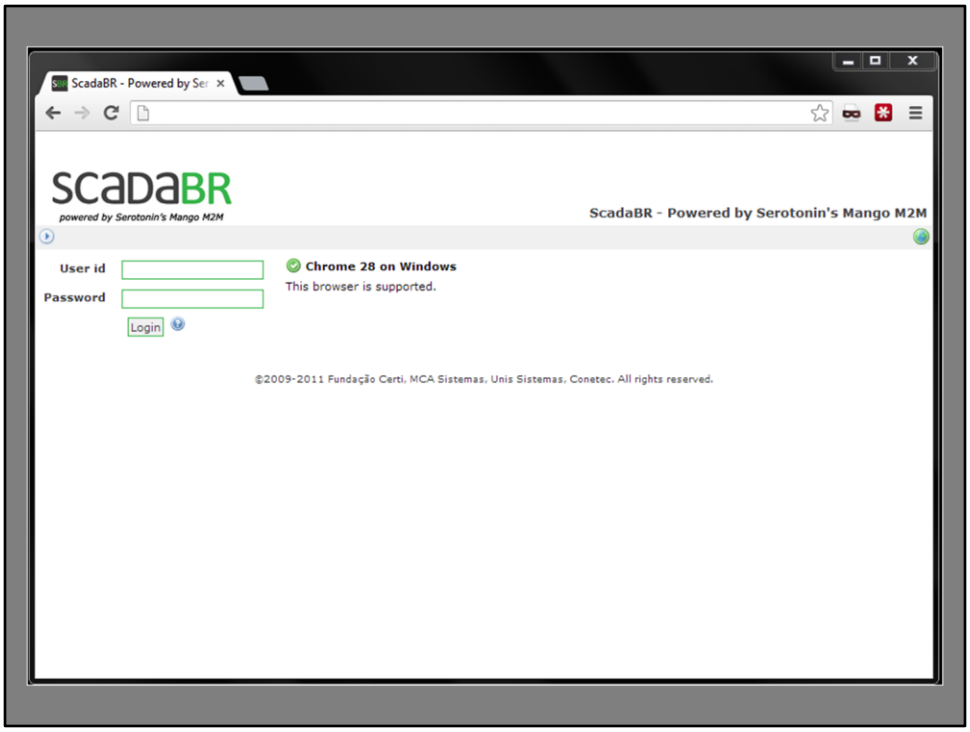


DEMO – HIDDEN BACKUP SLIDE IN CASE OF INTERNET ISSUES:

The “Protocols supported” link lets us know that the machine is running Telnet, FTP, HTTP and Modbus – which is a common communications protocol used by PLCs

DEMO – HIDDEN BACKUP SLIDE IN CASE OF INTERNET ISSUES:

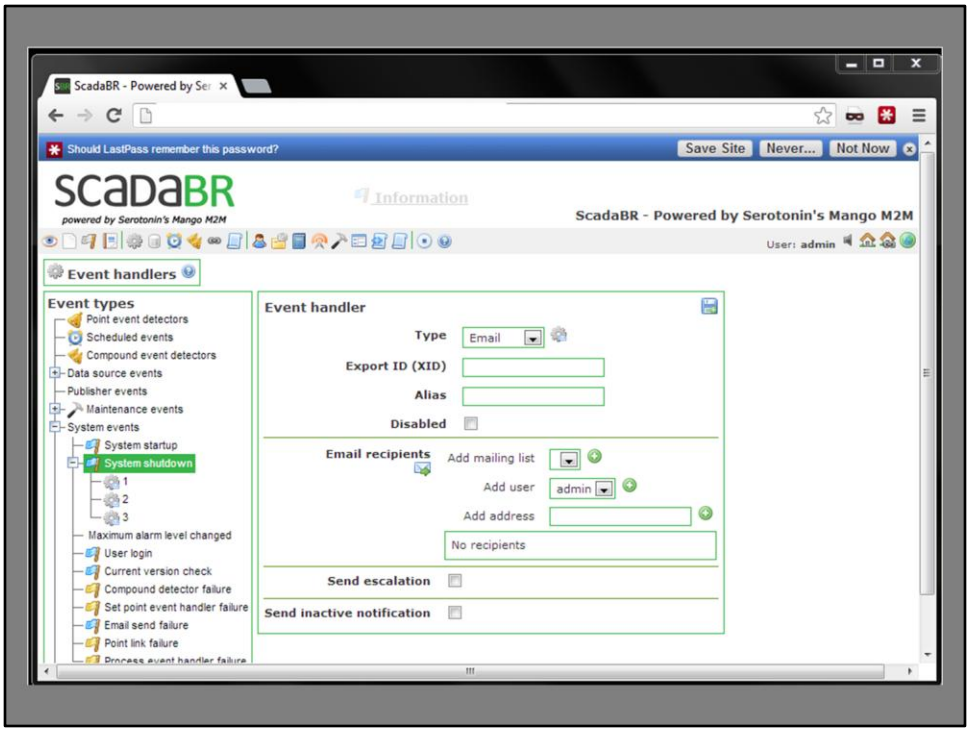
The “Diagnostics” page is already more interesting though – here is a very simple control panel created that lets a human actually input values and affect the running of the plant. The page even calls out that these changes may adversely affect systems.



DEMO – HIDDEN BACKUP SLIDE IN CASE OF INTERNET ISSUES:

When we did some more digging into the server we found that it was actually running a piece of software called “ScadaBR” on port 8080. We also later found out afterwards that using “scadabr” as the password on the main page will lead you to this same portal.

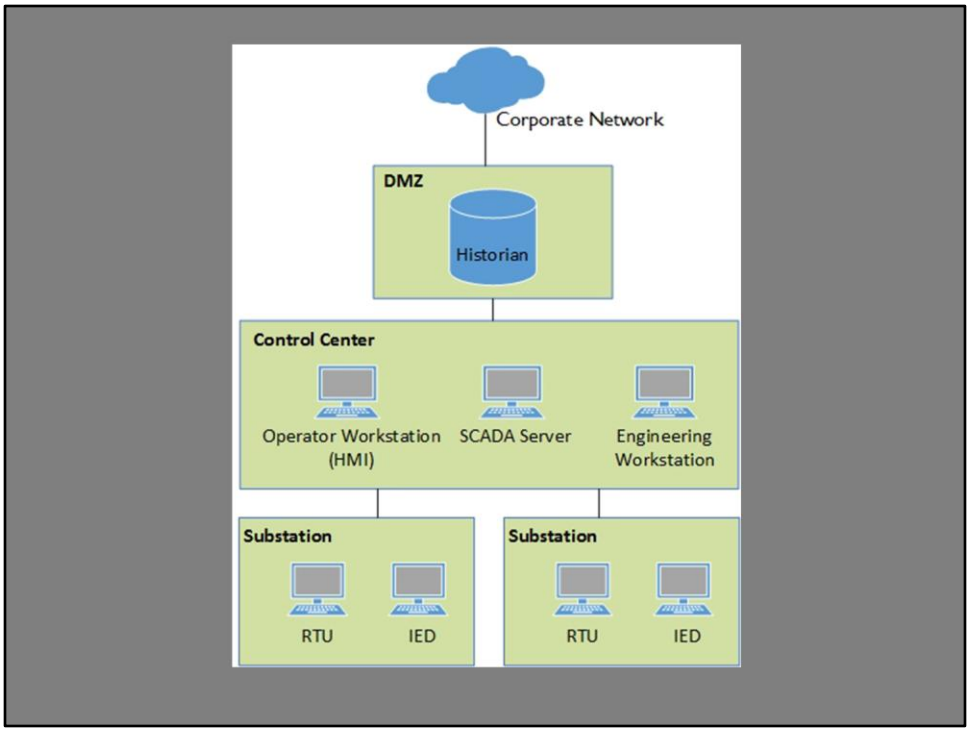
To make matters worse the ScadaBR software also comes with a default login and password – the old reliable admin/admin – and this machine had not changed that.



DEMO – HIDDEN BACKUP SLIDE IN CASE OF INTERNET ISSUES:

Logging into this panel in turn gives you much more options. It lets you see all sorts of interesting statistics such as Alerts – but more interestingly it lets you schedule commands in the water plant itself. Just as an example lets create a shutdown event. We fill out this form, and click submit. Next we add it to the scheduled job to run hourly. What will happen next is that at the next checkin time – which in this case is on the hour – this command will be pulled down by any connected PLC systems, and they will simply shut themselves down.

Don't worry though – I'm not going to let that happen, I have around 30 minutes to remove it – so I'm going to talk a bit more about how SCADA systems are setup and then later we can come back and remove it from the queue, before anything bad happens …



Heres a diagram of a standard enough ICS setup. The corporate network connects to the control center via a DMZ (Demilitarized zone) which normally also contains the Data Historian. This is essentially a database where all logs are backed up to for later query and analysis.

Within in the control center you will find Workstations that act as Human Machine Interfaces, they in turn communicate with the various Substations.

Each substation will have a Remote Terminal Unit (for local control) and an IED. For those of you with .mil in your email addresses, don't worry – that stands for Intelligent Electronic Device – this is the PLC that is actually doing all the work.

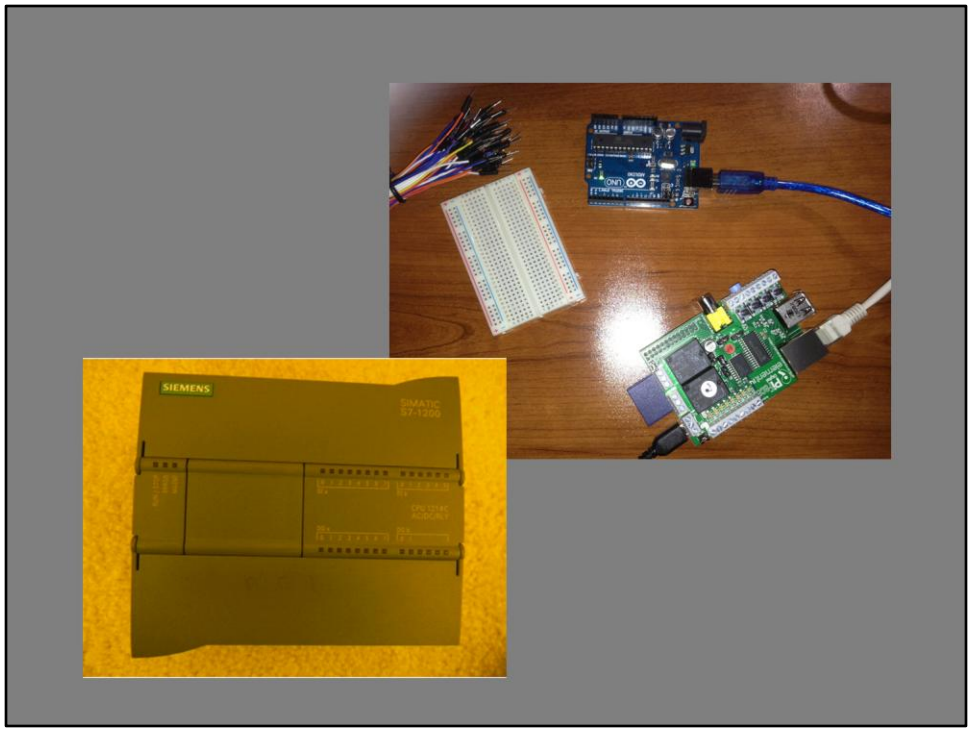
The communication between these devices tends to take place over two main communication protocols – Modbus and DNP3, and guess what – neither of these protocol have ANY encryption or authentication, and of course there have been vulnerabilities published for both ☹

So what about that Water Plant we looked at earlier – the one I was able to show was trivial to bypass and control?

Well it turns out this exact same water pump setup is being run by the same organisation in 7 other parts of the world , and I've marked the countries on the map. We have the US, Brazil, Ireland, Russia, China, Japan and Austrailia. When you combine the populations of the cities they are servicing you end up with 50 million people.

And we know that every single one of those systems has been attacked several times, over a period of several months. We know that attackers gained access, exfiltrated data, and even modified the system setups themselves.

And we know all this – because the entire setup…



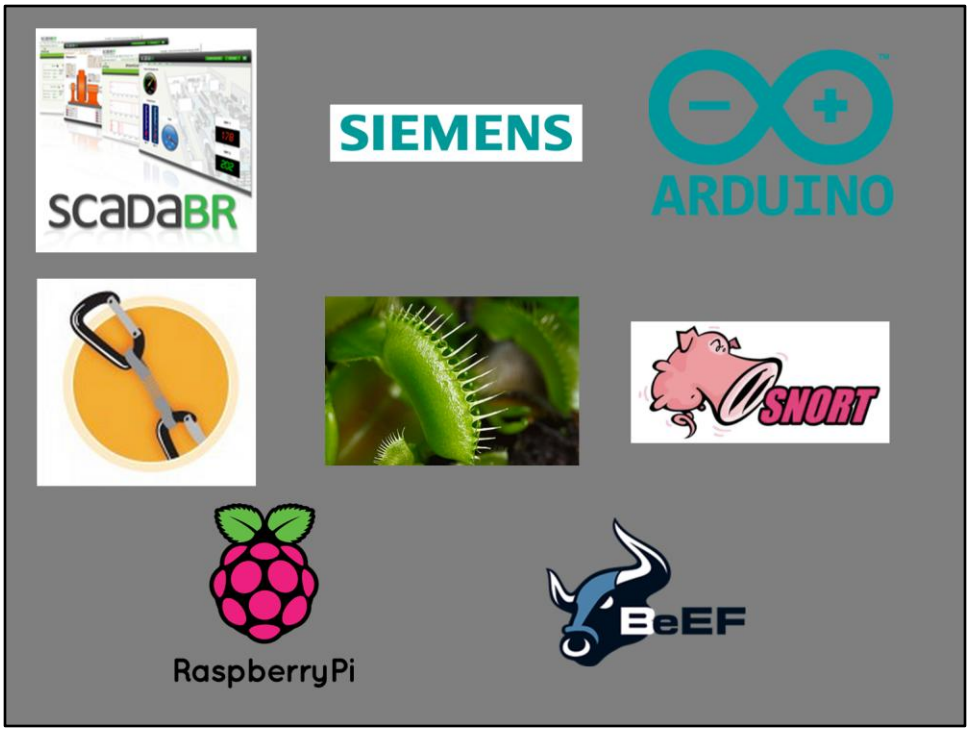
was being run from Kyles basement ☺

The FTR team has been operating 12 very realistic looking ICS Honeypots in 8 different countries since January 2013. These systems are not real Water plants – but attackers don't know that. The systems are in many cases making use of real hardware and PLCs, and we have two people on our team who previously worked with ICS systems all the time, so are well aware what these systems should look like.

We choose to mimic Water plants as these are traditionally less secure than other facilities such as a Nucleur facility for example.

Oh and don't worry – this also means that nothing bad is going to happen if I forget to cancel that shutdown event ☺

So let me first explain the briefly the setup we are using for our honeypots, and I'll then spend the rest of this presentation focusing on the most interesting part of all – who was attacking these systems



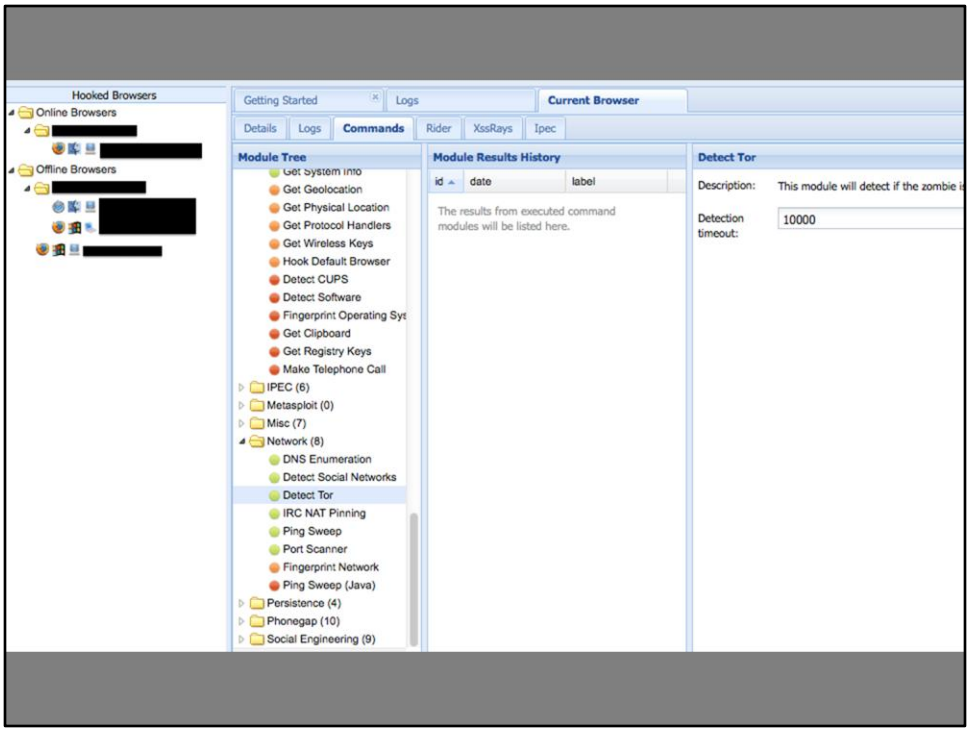
In our setup we used a variety of different Hardware and Software – which you can see on the slide. If anyone is interested in the exact architecture I can share that later on.

Briefly we used the

ScadaBR framework I showed
We used SIEMENS PLC
Arduino hardware devices
The Quickdraw SCADA IDS signatures from Digital Bond
Dionea – a malware collecting Honeypot
The SNORT IDS
A Raspberry Pi as some cheap hardware
And also BeEF – The Browser Exploit Framework

And on top of this there were several libraries for Modbus and DNP3 simulation.

Our use of BeEF in particular is worth calling out.

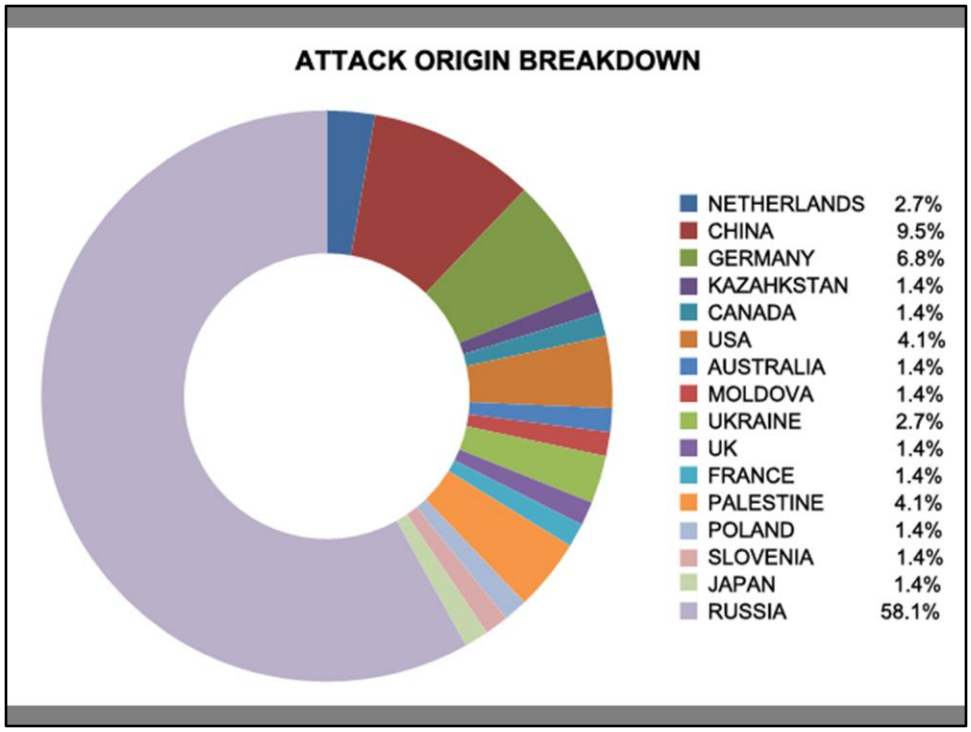


BeEF is a Penetration testing tool written in Javascript. You simply add a single piece of Javascript to any webpage you control and any person who visits that page will activate the BeEF plugin. BeEF then makes use of JavaScript and HTML5 functionality to offer a range of different functionality. You can see some of this on the slide, but there is everything from simple browser fingerprinting up to portscanning the network and social engineering the user.

In our case we where only interested in using BeEF to get a more accurate attribution of the person accessing our honeypots, and we deployed it in parts of the interface with banners that said that this system was being monitored. In total we used Beef to

Detect if TOR was being used
Get the Internal IP
Get the System Info
Get the Physical Location of the machine
And Get certain Registry Keys

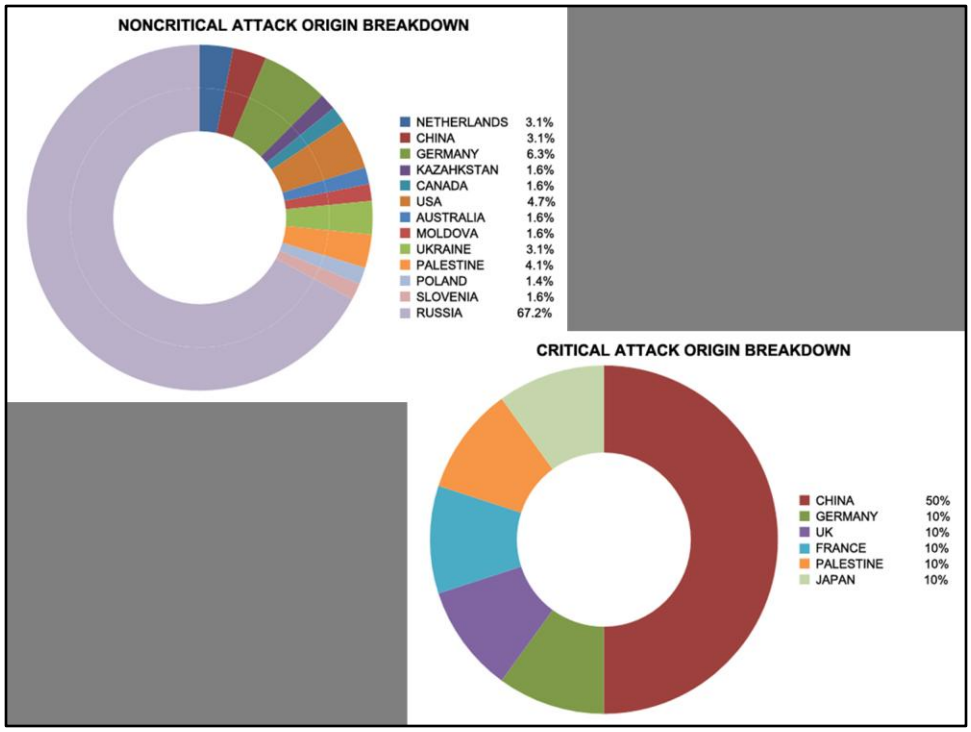
Its important to note that no exploits where used – this is just JavaScript, and in many ways less invasive than some of the tracking cookies advertisers use.



So who attacked us? In total we received over 32000 automated attacks over 5 months, coming from over 1200 Unique IP addresses.

Most of these are not really “attacks” though – they are just the normal background scans of the internet that goes on every day, port scans, vulnerability scans etc.

So instead we only considered “attacks” those that where considered targeted by virtue of the level of initial reconnaissance and fingerprinting the attackers carried out, before prior to the main attack. In total we observed 74 attacks originating from 16 different countries - as can be seen on the graph



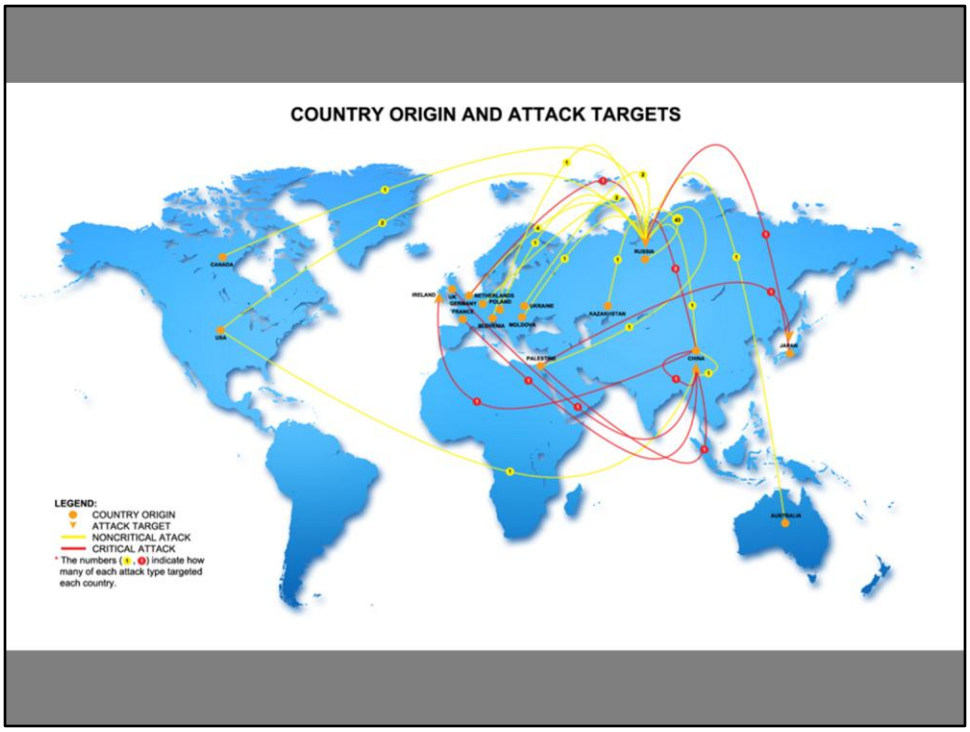
We then further broke these attacks down in Non-Critical and Critical attacks.

For a critical attack was any attack which would have caused catestrophic failures in the operation of the ICS device. The attacks considered non-critical included a variety of approachs – from dictionary attacks on logins, to SQL injection, to modbus attacks.

In total we had 64 non-critical attacks, and 10 critical ones. For Non-Critical Russia is clearly leading the way – with Germany, USA in 2nd place followed by China, Netherlands, the Ukraine and Palestine.

On the critical side however China is the clear leader – being responsible for 50%, but it is also interesting to see the origins of other countries that carried out critical attacks and that all Russian attacks where non-critical in nature.

Overall these results where already quite interesting , and not exactly what we expected – but what is perhaps more interesting is who is attacking who.



This visualisation might look a bit daunting at first but let me talk you through it. Also I have to apologise that we don't have the awesome Team Cmyru data visualisation wizards at our disposal.

On this slide Critical attacks are in red, and non-critical in yellow. Circles indicate the origin of an attack, and arrows the target. Also each line has a number to indicate the amount of attacks.

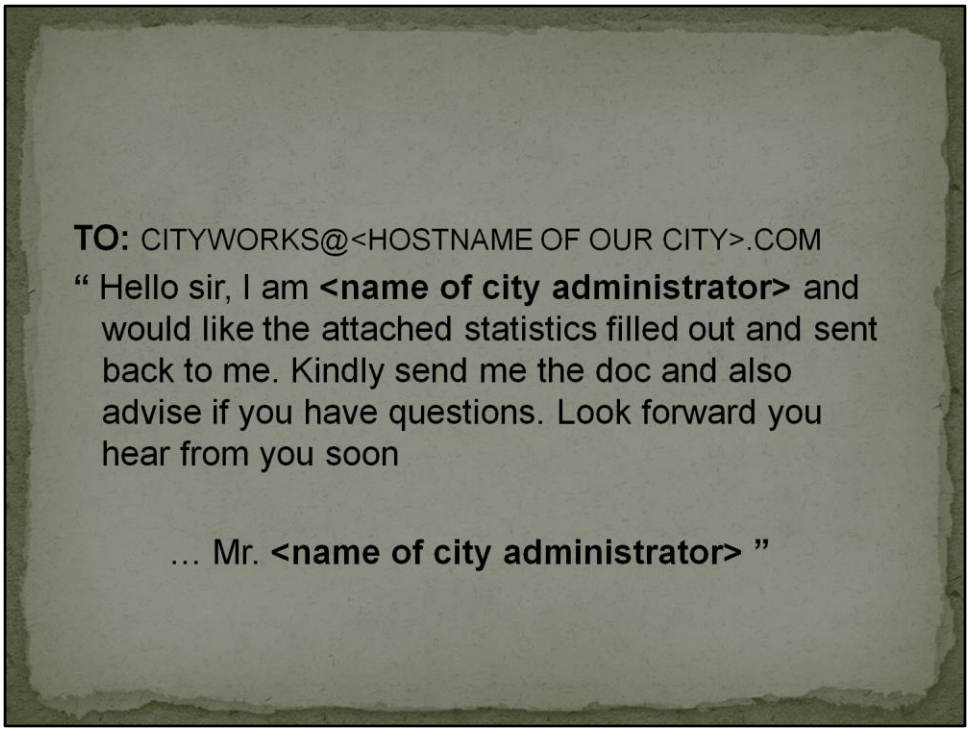
If you can't make it out, don't worry - there are a couple of interesting takeaways from this which I'll go over.

Russia was far and away the most attacked nation in our testing, followed by China. Russia received attacks from all over the world 5 of which where critical in nature. The main foreign countries attacking Russia where China (with 3 critical attacks), but also Germany with a total of 5 attacks. What even more interesting however is that we saw 43 attacks from Russia on Russia. We are still not entirely sure what the cause of this was – perhaps these are proactive internal security checks against SCADA systems in Russian IP space, or a criminal element with blackmail as a motive.

On the map you can see what we saw in the previous pie charts, that China is the source of most critical attacks – but they also received significant attacks themselves – being targeted by 4 critical attacks from the UK, France, Palestine and within China itself.

Further down the list we have critical attacks against Japan, and against my own home country of Ireland. The attacker IP who targeted Dublin also targeted one of our Honeypots in Russia.

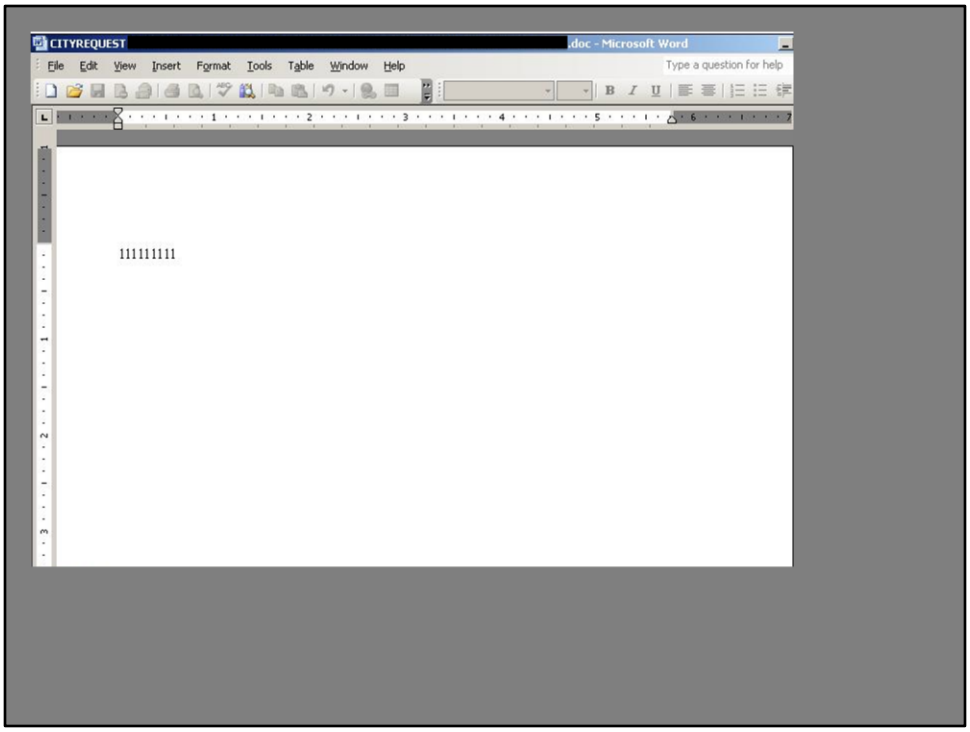
Of course this is just a snapshot of what we saw in OUR honeypots. Its really difficult for us to say who is attacking who in the real world, but its clear that attacks are happening.



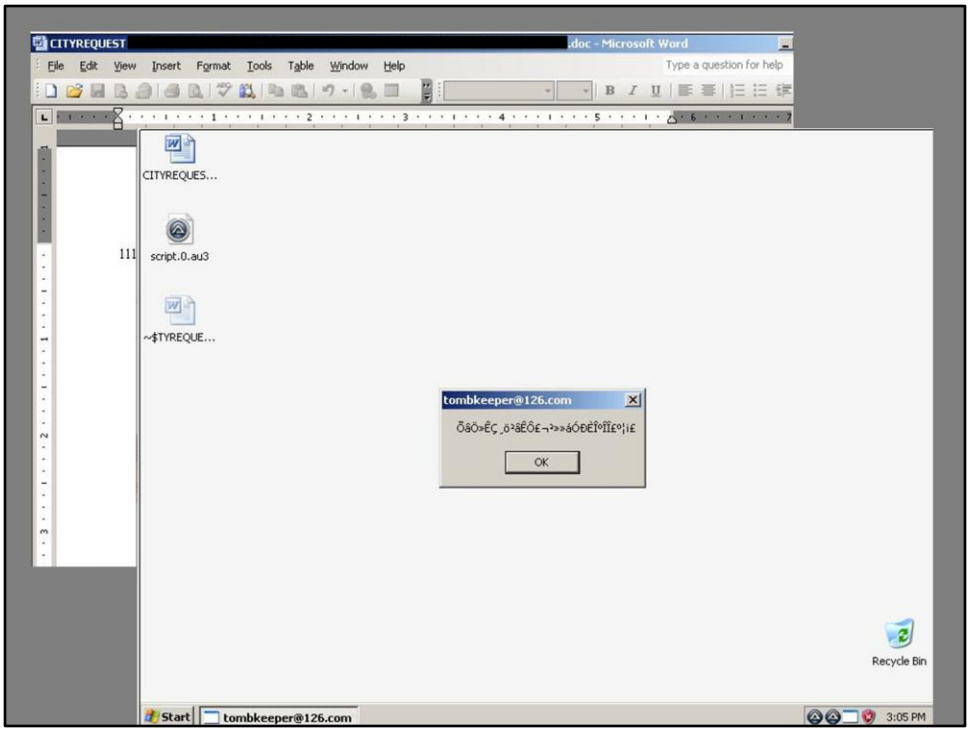
Now all of the attacks we talked about so far I personally find quite interesting, but there is one last attack I wanted to finish on before wrapping this talk up.

During our operating of these honeypots we witnessed a very targeted attack on one of our Honeypots in the US. This attack began with a phishing email sent to an email address we had seeded on the website of Honeypot that was compromised. The email address was created to closely mimic a legitimate one that a city government would normally have.

Like most phishing emails, this one contained a malicious attachment called CITYREQUEST.DOC



We setup a server complete with salted documents that would be believable for the target of this attack to have, and then opened the document on that machine. There was nothing much to see in the document itself. However once opened it did trigger an exploit for CVE 2012-0158.



And this in turn drops an executable on the machine, which displays a popup like the one shown on screen.

Excellent we thought – Malware! After all we are an AV company, so we feel a lot happier when we are pulling apart Windows binaries instead of wading through logs of malicious Modbus traffic ☺

This malware in turn drops two files to the system – gh.exe and ai.exe

Gh.exe is a standard password dumping tool. It simply dumps the contents of the local SAM passwords database. This is a standard functionality to help laterally move throughout a target network though remote logins or pass the hash attacks – and is seen in many targeted attacks.

Ai.exe is more interesting however. This component shovels a shell back to a C&C server in China or the US. Together these are quite simplistic for a first wave of attacks, which is more in keeping with what is commonly seen in attacks attributed to Chinese attackers – who normally follow up these initial beachhead infections with a more fully featured RAT if they have compromised a victim of interest.

In total we left the malware running for 5 days during which time the attackers exfiltrated

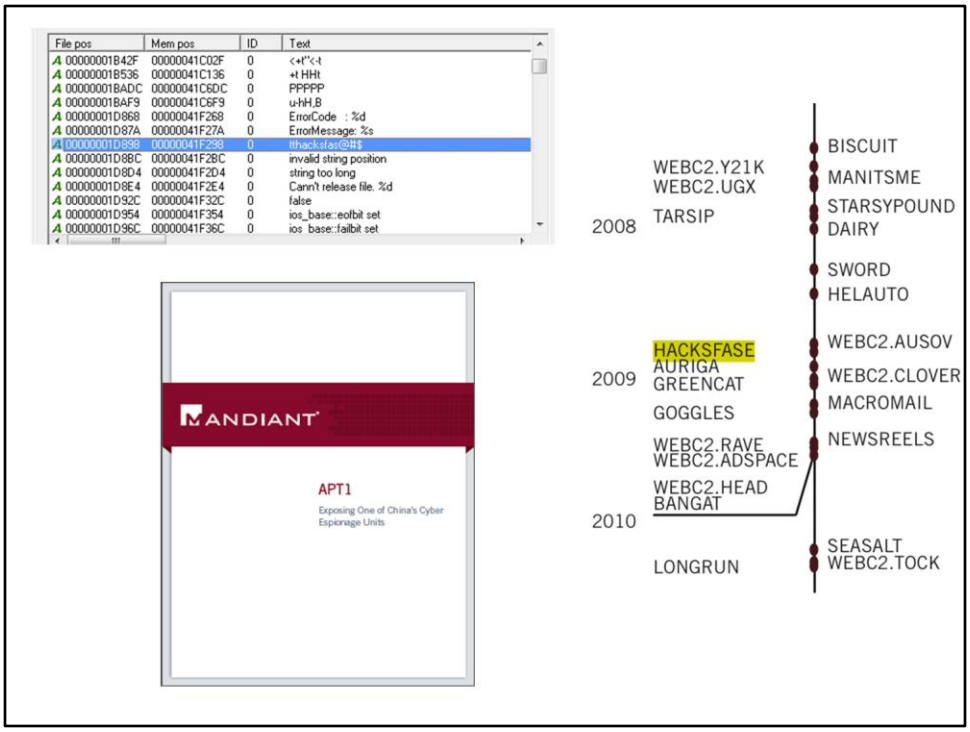
-Fake VPN config files

-Network Statistics

-SAM database

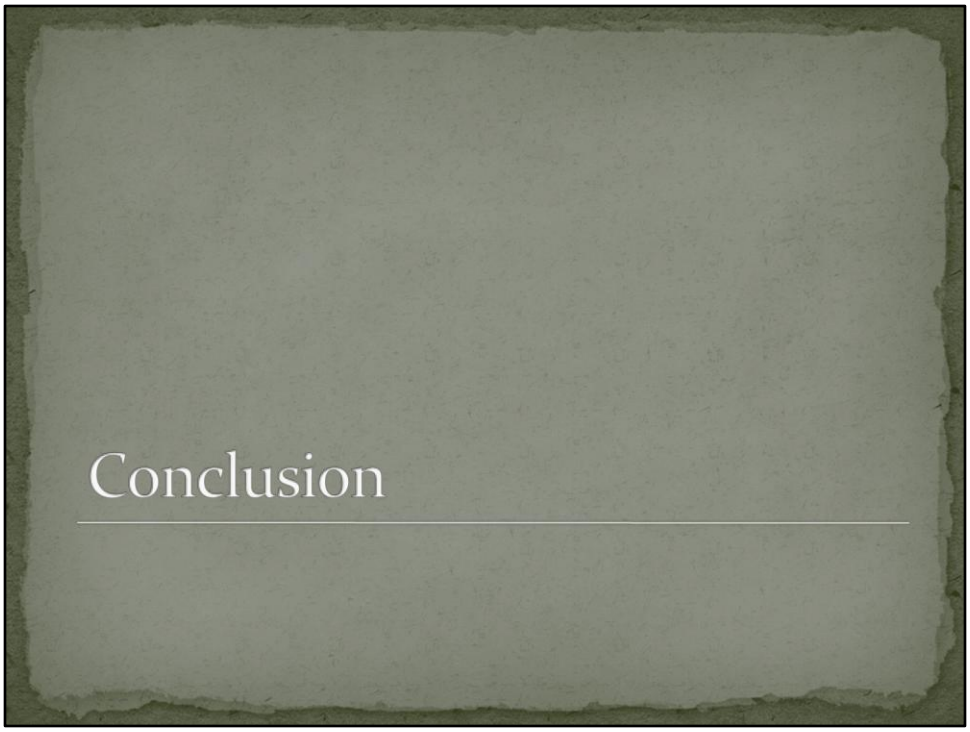
Also during that time they launched a lot of pings and traceroutes to map out the connected local network, disable Firewalls and AV on the machine, carried out some basic anti-forensics (delete prefetch) and tried to mount shared network drives – so a lot of evidence of maintaining persistance and attempting to move laterally.

What was most interesting of all with Ai.exe however was the human readable strings inside…



This malware contained an interesting string which I have highlighted here. This string associates it with a malware family called Hacksfase. Hacksfase in turn is one of the malware tools that Mandiant claim to have attributed to a specific unit of the Chinese PLA.

So it is possible that our Honeypot installation in America was also attacked by the same group behind the Mandiant APT1 report.



So to conclude – I won't go into details here on how we recommend people secure ICS system, although if you are interested Kyle covers this well in our paper.

But I think it is clear that these sorts of systems are under active attack, both by opportunistic attackers, and by people who know exactly what they are doing. And this is not only the case in the 8 countries we tested in, but most likely in most major countries as well.

Whats also clear is that you if you have not already you should definitely go checkout both Google Dorking / Hacking and Shodan. Combined these will let you find a hell of a lot more than just ICS and SCADA systems. I was tempted to do a whole talk on one of those two – but thought I should stick to the ICS part first – anyone else is welcome to do so though ☺

And don't worry – as soon as I'm off stage I will stop that shut down command before the water supply from some fake water plant to some fake people dries up ☺