Rickey Gevers

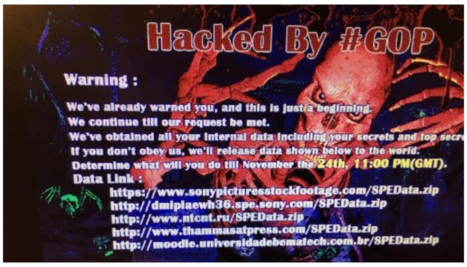
| Criminal brought to justice! | Twitter | Job |

IT | Politiek | Travel

vrijdag 19 december 2014

Commonalities between the different wiper viruses

In this blog post I will describe details about several attacks that, as of today, are not directly linked to each other. But in my opinion share very important commonalities that should not be unnoticed.



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secr
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Data Link :
https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip

The main hacking attacks I will talk about are the Dark Seoul cyberattacks, the Shamoon wiper virus and the Destover malware used to attack Sony. All have their own Wikipedia page, which proves their extend.

Below I will describe some remarkable events in which wiping/erasing malware functionality plays a key role, the events are in chronological order. (some political events are mentioned as well).

July 8, 2009Malware is used to launch a large scale DDoS attack and eventually corrupts the systems by placing the text: "Memory of the Independence Day" in the Master Boot Record (MBR) to prevent the compromised computer from restarting. The malware used hardcoded command and control ip addresses.

March 4th, 2011Malware is used to launch DDoS attacks, encrypt files and corrupt the MBR. Bytes are written to the MBR to prevent the system from booting normally, thus breaking the system. Another functionality is that the malware is able to encrypt documents. Hard coded command and control ip addresses are embedded in the malware.

April, 2012The Iranian oil ministry is hit by a cyber-attack. The malware effectively wipes whole computers leaving no traces. Security researches from Kaspersky who are called in to investigate the attack only find some traces of the malware, slightly linking in to Duqu and Stuxnet.

> July 2012
> Oil Embargo Sanctions against Iran set to squeeze the country, effectively starting in July 2012, $133 million in losses a day.

August 15, 2012
News struck Saudi Aramco was hit by a cyber attack. It suffered from a virus that effectively destroyed the MBR crippling the computer network. In the MBR a small portion of a JPG image was displayed. It later turned out to be a burning American flag. The attackers claimed to belong to the group "The Cutting Sword of Justice" and promised another present on August 25th.

August 25, 2012Hackers from "The Cutting Sword of Justice" made their promise and crippled the network of Qatari based firm RasGas.

> Sept 1, 2012
> Iran and North Korea sign a scientific and technological cooperation agreement, bringing the two nations deeply at odds with the US closer together.

March 20, 2013Hard drive wiping malware hit South Korea. Banks and television stations were reportedly crippled. Computers failed to boot up properly, and displayed an image of three skulls alongside a message claiming that the systems had been "hacked by Whois Team".

February 11th, 2014The Sands Casino was hit by a cyber attack. Their public website and internal network infrastructure was defaced and effectively wiped. The hacker group "Anti WMD Team" claimed responsibility.http://www.sandsinfo.com/index.htmlhttp://i1-news.softpedia-static.com/images/news2/No-Credit-Card-Data-Compromised-in-Las-Vegas-Sands-Casino-Company-Hack-AP-426875-2.jpg

November 24, 2014Sony Pictures falls victim to a devastating cyber attack. All internal data is leaked and computers destroyed. The attackers are known only by their collective name, the "Guardians of Peace". Once again the malware deletes the MBR. **Commonalities**If we quickly point a perpetrator in all of the above cases it looks like this:
North Korea
North KoreaUS/IsraelIranIranNorth KoreaIranNorth Korea

Blogarchief

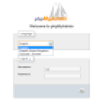
Populaire berichten

Hijack Whatsapp with your iPhone
Hijack (someone else's) Whatsapp with your iPhone If you want to hijack someone else's Whatsapp and receive messages addressed to that pers...

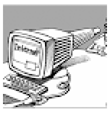
Whatsapp kapen met je iPhone
De filmpjes hoe je Whatsapp kan kapen met een Nokie N97 staan op interne t. Hier is een beschrijving dit te doen met de iPhone. Via de iPh...

Whatsapp security weaknesses
The facts of whatsapp and all the drama. In case of an iPhone if you open the Whatsapp application the following occurs: - The applicatio...

Videoconference systemen van Defensie eenvoudig te hacken
Maandag de 20ste werd ik getipt door hacker @ntisec . Hij vertelt me iets bizars te hebben gevonden en weet niet wat hij ermee aan moet. Hij...



Complete details of the Dorifel servers, including its 'master' server in Austria
Below are my findings of the two servers used in the (targetted) attack mainly taking place in the Netherlands. We have 2 server setups t...



26 Alternatives for Megaupload
Internet censorship does not work . It's that easy. Today people connected to megaupload.com have been arrested and are facing trial ....

KPN hack debacle -LIVEBLOG
Website security.nl kwam als eerste met een link naar pastebin waarop de klant gegevens van KPN gebruikers zouden staan. Hoewel eerst in...

International -ongoing- BlackShades customers raid -Summary

The first attack clearly used highly technical malware and could possibly addressed to America and/or Israel as there is reason to believe it is connected to Duqu and Stuxnet. It is the first appearance of "wiping" malware.

Quickly after this first attack another devastating "wiping" malware struck Saudi Aramco. This time the malware was not very technical, but proved its capability to destroy computers. It was highly effective in its job.The malware itself moved on a lateral basis throughout the network, had preconfigured Command andControl addresses, used compromised account credentials and sended a notifying message to an internal proxy server whom in turn forwarded that information to the internet. The attackers apparently wanted to know how much damage their attack had cost. Through pastebin posts the world was updated about the success of the malware. A group no one ever heard of claimed responsibility: "TheCutting Sword of Justice". In order to improve the impact the malware used a signed driver from the company ElDos.The malware contained several typing errors that made some parts of the malware malfunction.Although claiming to be from Saudi origin the hackers communicated in English.In the MBR the hackers left a small portion of an image. This image turned out to be a burning American flag. The hacker actively approached the press, said to bring another gift and promised to be back.The malware was compiled 5 days in advance of the attack.Shortly after the attack on Saudi Aramco the hackers delivered what could be assumed was the present mentioned in some of the statements of "The Cutting Sword of Justice". This time the Qatari based firm RasGas fell victim to a wiper virus.The malware spread lateral throughout the network, had preconfigured user account credentials, contained a lot of coding errors and also used the ElDos driver.

Then in 2013 South Korea fell victim to a large scale attack on its nation’s infrastructure. Computers from banks and television stations were wiped. This time a group again no one ever heard of called "Whois Team" claimed responsibility.The malware had a Linux component in it and credentials were retrieved from a very specific path: http://www.symantec.com/security_response/writeup.jsp?docid=2013-032014-2531-99&tabid=2 Indicating the malware was specifically designed for this attack.
The malware was compiled 2 days before the attack.

In February 2014 The Sands casino fell victim to another wiping malware. As I have no sample of this malware I cannot draw any conclusions so far. But the attackers claimed to be from the unknown group "Anti WMD Team" and communicated in English. Via messages directed at the casino and through video posts the attackers made clear they stole 828 Gb of data and have it in their possession. They actively approached the press, promised a gift and said to be back soon.

In November Sony fell victim to the devastating wiping malware. The malware used the ElDosdriver again, moved throughout the internal network via lateral movement, had hardcoded Command and Control IP addresses in it, had hardcoded credentials in the code, contained typo errors in the malware and showed a picture with their demands. The hackers were once again from an unknown team called "Guardians of Peace", communicated in English and well yes, they promised a Christmas gift and said to be back soon. In the mean time they slowly release all the data they had stolen to the public and actively approached the press.
The malware was compiled just a few days before the actual attack.

Some of the commonalities shared between these attacks are the following:
Political MessagesElDos driver
Actively approached press
Promised gift/Said to be backCommunication in English
English group name
Former unknown group
Use of images in MBRSpecific timingCompilation few days before attack

There definitely is no smoking gun here, but the circumstantial evidence is of such similarity it, in my opinion, cannot be ignored.

Political Messages
Political messages were to be found in all elements. Burning flags, detonation on specific dates and statements made by the group always had a political tone.

ElDos driver
The returning usage of the ElDos driver is one shared commonality in the malware. As malware with the main purpose of completely destroying hard drives is unique is even more unique a same driver is used. And it is specifically remarkable that in some of the attacks the driver wasn't even necessary for the purpose it was supposed to serve. Apparently the driver was just there and available to the attackers, and because of this they decided to include it in their malware. Maybe because they were just used to doing it?

Actively approaching the press

Rumours within the cybercrime underground started to appear early May about people getting arrested and their equipment getting seized. Not...

Blokkade The Pirate Bay omzeilen

Door de verplichte blokkade van The Pirate Bay wordt ONZE vrijheid afgepakt. Ik ga even niet in op de discussie hierover. Dit Artikel gaa...

Why I think the Linkedin password file is fake

Well first of all, there is no connection to LinkedIn other then the suspected 'hacker' saying it is from LinkedIn. There are 6.5 ...

In some attacks the attackers specifically targeted the press. They didn't just choose one newspaper, or one favorite journalist like often happens with lone wulfs or small groups. No they were highly informed about what press is influential and distributed their massage an mass towards all these organizations. Chances of getting unmasked by accidentally exposing more information to the journalist that opposed apparently didn't pose a threat to the hackers.

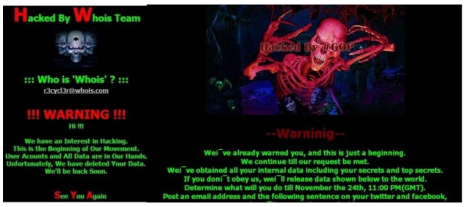
Promising Gifts and Said to be back
In some of these cases the hackers said they had a present waiting. The presents promised were thus far always met. Promising something and keeping that promise causes extra fear at the victim’s side.

Communication in English
While this clearly doesn't seem important it is remarkable though that an attack carried out by supposedly attackers from Saudi origin, attacking a Saudi company communicate in English whilst both of their first languages is Arabic. The attackers stuck to English as their way to cummunicate with their victims, and clearly wanted to world to be able to read and understand it as well. This slightly proves the attacks were not targeted at the company, but to the public.

English group names
In all cases English group names were used. In attacks of which Iran is the main subject one group called itself "The Cutting Sword of Justice" and in the attack on the Sands Casino the attackers said: "Don't let your tongue cut your throat.” On the other hand the attacks of which North Korea is the main suspect group names where "The WHOIS team" and "Guardians of Peace". By causing havoc these attackers apparently want to establish world peace.

Unknown groups
Often hackers and hacktivists join groups, known groups. Groups that claim responsibility because the hackers are proud of what they have achieved. They want people to know it was them again. They want to prove to the public they are capable of doing it again. In these cases the attacking groups have never been seen before, and are thus far never seen after the events.

The use of images.
In the first attack on the Saudi Aramco, a small portion of a JPG image was left in the MBR. This image eventually turned out to be a burning American flag. Although according to the initial message the attack had to do with the country of Saudi Arabia apparently something of America had stung the creators of the malware. The images used in the DarkSeoul attack and the Sony attack have remarkable commonalities in their layout and structure.



Hacked By Whois Team

::: Who is 'Whois' ? :::
r3cycl3r@whois.com

!!! WARNING !!!
Hi !!!

We have an Interest in Hacking.
This is the Beginning of Our Movement.
User Acounts and All Data are in Our Hands.
Unfortunately, We have deleted Your Data.
We'll be back Soon.

See You Again

Hacked By #GOP

--Warninig--

Wei¯ve already warned you, and this is just a beginning.
We continue till our request be met.
Wei¯ve obtained all your internal data including your secrets and top secrets.
If you doni¯t obey us, wei¯ll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Post an email address and the following sentence on your twitter and facebook,

Specific timing
During the attacks and during statements made by the different group very specific timing was used. The malware at Saudi Aramco was set to specifically detonate at a certain time and the promised present was set at again a very specific time. This is also the case in the DarkSeoul attack, as was in the Sony attack. The usage of very specific timing is not uncommon for programmers. It is less common though in an ongoing attacks. This is because once an attack is launched the attackers usually lose control over the situation. In these cases the attackers apparently were very confident in their succeeding’s.

Compilation times
Specifically in the Shamoon, DarkSeoul and Destover malware the compilation time was right before the attack. The attackers apparently waited till the last moment to compile their weapon and deploy it out in the open.

As a side note it is probably remarkable that Keith Alexander on numerous occasions specifically named the adversaries described in the above attacks. Some of the video's below:
http://www.afr.com/p/technology/interview_transcript_former_head_51yP0Cu1AQGUCs7WAC9ZVN
http://www.slideshare.net/afcea/gen-keith-alexander-commander-us-cyber-command-director-national-security-agencychief-central-security-service

See: 15:58

As the usage of destructive malware is uncommon, so is the modus operand of the described attacks. Based on these facts I can imagine the presence of an APT group that is funded and supported by the Iranian and North Korean government specifically tasked with targeting common enemies.

Samples:
Destover, md5: 6467c6df4ba4526c7f7a7bc950bd47eb
Shamoon, md5: b14299fd4d1cbfb4cc7486d978398214 & d214c717a357fe3a455610b197c390aa
DarkSeoul,
md5: 5fcd6e1dace6b0599429d913850f0364 & 0a8032cd6b4a710b1771a080fa09fb87 & 50e03200c3a0becbf33b3788dac8cd46 & 5fcd6e1dace6b0599429d913850f0364 & db4bbdc36a78a8807ad9b15a562515c4 & e4f66c3cd27b97649976f6f0daad9032 & f0e045210e3258dad91d7b6b4d64e7f3

Geplaatst door Rickey Gevers op 03:29

Geen opmerkingen:

Een reactie plaatsen

Voer je opmerking in...

Reageer als: Google-account

Publiceren Voorbeeld

Startpagina Ouder bericht

Abonneren op: Reacties plaatsen (Atom)