EXPOSED: Russia is a proxy for the digital underworld

Russia is an easy scapegoat. As we explain in Splitting Pennies – the world is not as it seems. The US Government spent billions of dollars creating the false narrative of Russia as an 'enemy' as the post WW2 "War Department" knew very well based on focus groups and RAND reports that unless they could come up with enemies that scared the public at large, getting those billions and hundreds of billions wouldn't be so easy.

(Another photo of a Military "Storage Site" in Arizona with billions of unused planes 'just in case)

First let's quickly look at Russia as a proxy state. As we saw with KimDotCom, there are few places in the world one can hide. Russia is one such place. It is possible to go to Russia and the Stans and vanish. No one will ask questions, if you have a little money. No one will care to ask. So that's one thing to consider. You are a hacker based in NYC. It really is only a matter of time before you will be caught. The web of surveillance is so deep in the west, it's electronic, it's physical – you can't exist without eventually leaving a trace somewhere. Or to put it differently, the only way to stay hidden here is to not exist, that means no working or communicating with people or the 'system' – possible but if you need money or get bored then it presents a problem (as you will reveal yourself to the system). Russia is not the only country in the world to hide, but presents some interesting advantages due to the political conflicts they have with most

countries, and who wants to live in Africa, really.

Second, Russia is a great proxy for hiding your IP. Many hackers will traceroute their signal through Russian servers, which can be rented cheaply. Many IP obfuscation software such as HideMyAss will offer Russia as an option, such that users can 'appear' that they are in Russia. So the 'digital mafia' if you will, or 'hackers for hire' will often mask themselves as "Russian Hackers" when in fact there is nothing Russian about them at all. The CIA does this, the NSA does this, and hackers do it too. A Russian IP can be the difference between being caught and not. Causing a political scandal is a bonus "Those pesky Russians are at it again!"

The fact is Russia is very backward. Just recently a shopping mall burned and more than 70 children died. It's a travesty, a horror. They have no building codes, no fire escape requirements, people jumped out of windows like during 911. Russia doesn't have an internal system to 'catch' hackers nor do they have any interest in doing so, they have much bigger priorities. Russia has real problems (but, they are not caused by Putin, contrary to media reports). There are no bankruptcy laws in Russia, no consumer protection. The last thing they are worried about are hackers or DMCA. The point is there are many reasons that Russia is used as a proxy both technically and jurisdictionally..

Third, there are actual Russian hackers and 'hack for hire' groups and individuals that work globally from Almaty, Moscow, and many other places. They travel globally but when they are working you can bet they aren't doing it from NYC. That's the irony of modern Russia, legit Entrepreneurs like Pavel Durov are forced to live like global digital Bedouins. "Only in Russia"

Almaty, Kaz – great place to hide from the FBI.

So for example it would be quite possible for the DNC, or any US based group for that matter, to hire “Russians” to do

"hacking" or "security analysis" may be what they are telling their accountants now to book the transaction as.

Russia is a black hole. So as the expression goes, all roads lead to Rome – **All roads that lead to Russia lead to nowhere.** It's a digital dead end, perhaps the only one left in the world (not counting poor undeveloped countries) which is perhaps why many are so irritated that Russia stays independent and grows internally so vibrantly.

So next time you read or hear about how "Russians" hacked this or "Russians" did that electronically, replace "Russians" with "Anyone".

To learn more about how the world really works, checkout Splitting Pennies – **visit our sponsor Ubuy.me @ www.ubuy.me**

CIA hack job(s) EXPOSED

Finally, we have a 'snowden' event for the CIA and the inner workings of how the agency operates in the digital 'cyber' sphere. Wikileaks released "Vault7" – a treasure trove of documents pertaining to their 'cyberwarfare' or in layman's terms, hacking operations. Since we've released Splitting Pennies, in the hope of explaining how the world 'really' works – we've received mostly positive feedback, but many mainstream readers have accused us of being 'conspiracy theorists' – well now we have the proof. The CIA has spent millions of dollars, hired the best computer experts in the world, and developed a series of world class hacking tools. These aren't just your normal Ion Cannon or 'scripts' – these are the most sophistocated and powerful hacking tools in the world. So sophistocated, they fooled software titans like Google and Microsoft (who have their own in-house security

experts). More alarmingly, the CIA allowed this information to be proliferated into unclassified hands and eventually to end up in Wikileaks:

> ***Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.***

What's not clear yet at this point, if the 'source' was a lone ranger, or it was a coordinated release. Or, the source may have been one of the unclassified users who accidentally received these files or access to them in a breach, and felt obligated to forward them to wikileaks. Possibly we'll never know, but it doesn't really matter. Like previous leaks, these documents are an inner working 'blueprint' of CIA's modern internet operations.

Side note: **Interestingly, the author of this article just ordered this must read book: Dark Alliance: Movie Tie-In Edition: The CIA, the Contras, and the Cocaine Explosion** .. An agent for the public defender's office told me that when he worked for the DEA they did a huge cocaine import bust and turned out they almost arrested CIA agents who flashed their badges and told them 'get out of here, this is not for you' .. The book starts out with a bang; Gary Webb interviews the largest drug dealer of all time, Freeway Ricky Ross. What does Crack-Cocaine, the CIA, and all this have to do with FX and markets? They go where the money is, and as we've exposed in previous articles – the CIA manipulates FX markets more than the Fed. Actually, the Fed has a rough time manipulating any currency other than the USD, which is where the CIA comes in handy.

So the point here is that, running drugs was something that served a purpose in the 80s. In the 90s it was all about privitization and seizing assets in previously communist countries, setting up shop in South America, planting the trojan horse(s) in Asia, etc. Last 10 years has been all

about social media and the physical monitoring of citizens, including but not limited to genius designs like Pokemon GO which quite literally, will film and record your every move. The designers probably wish there was a mobile penetration like Russia (99%) in USA there are still those who don't use or have Mobile Phones.

Anyway, this release shows the massive budgetary and man-force efforts the CIA has been undergoing to create what is quite possibly the largest and most powerful hacking enterprise ever to exist on the face of the earth. Criminal hackers, mafia, and other players – they don't have the budget, they don't have the CIA and entire DOD aparatus behind them. This is quite frankly, a "White Elephant" for a number of reasons, and ironically, the poor operational security led to a leak exposing and thus nullifying the entire operation (as is stated in the documents). Who knows, maybe there are 2 operations, one in VA and one in Singapore, or in a Volcano in Indonesia..

Also ironically, the CIA has been jumping like a Jack Russell clamoring for the investigation into the "Russian Hacking" into the elections. Well, maybe it's not so ironic, maybe it was the CIA hacking all along, using the UMBRAGE group to paint Russia as the perpetrator, using cheaply designed stolen Malware from Ukraine.

> *The CIA's Remote Devices Branch's UMBRAGE group collects and maintains a substantial library of attack techniques 'stolen' from malware produced in other states including the Russian Federation.*

At the end of the day, this is really a waste of taxpayer money. The fact that they have these tools shouldn't surprise anyone, they are after all, a SPY agency. It was a surprise that the intelligence aparatus got behind the anti-Trump campaign but there was a reason why – Trump didn't agree with their decades long 'deep state' agenda, and they know a threat when they see it. Government workers are very skilled at getting more money from a budget and keeping their jobs with continued benefits and raises (at least, at that level – this isn't your local DMV!)

For those with good security, this is a non-issue. The Malware and other 'tools' described in the documents mostly rely on exploitation of security glitches or poor IT

configurations. I mean who uses Mega, when you can use Dropbox (should be called NSAdropbox) where the apparatus can easily see your files without going through all this trouble of infecting your PC with Malware. And let's be softy lefties, at least they invested in technology innovation and not weapons and torture devices, I mean they were't strapping people to chairs and poking their eyes out.
To learn more about how the CIA manipulates markets – and how you can too! Checkout Splitting Pennies – Understanding Forex – your guide to world domination. Muhuahahahaaaa

---

ALERT: Point of Sale RAM scraper malware

Advances in technology have led to more sophisticated crimes by exploiting security vulnerabilities of new technologies. This is exacerbated by the fact that understanding of these technologies and their use is only by a few, while the majority of end-users are unaware. Generally speaking, following standard security practices will thwart 95% of electronic crimes such as phishing, hacking, etc. This includes using complex passwords (Sf9$fpq%f82bsS), using network firewalls, encrypted emails, etc. But the new POS RAM scraper is dangerous because the vendors are not the victims of their bad security, and you may never know where your credit card or other information was scraped from.

A look at Point of Sale RAM

scraper malware and how it works

From Sophos:

A special kind of malware has been hitting the headlines recently – that which attacks the RAM of Point of Sale (PoS) systems.

Although it's been getting quite a bit of publicity recently, we actually first identified it as a threat back in December 2009 and wrote about it in an article on Naked Security entitled Will RAM scraping loosen the sky and make it fall?.

Answering that question today, it just might!

Actually, the situation isn't that bad – yet – but this malware family has definitely become more complex and far-reaching. In this article, we take a step back from the technical details and look at the evolution of PoS RAM scrapers.

What do PoS RAM scrapers do?

In a nutshell, PoS RAM scrapers steal payment data – such as credit card track one and track two data – from the RAM of PoS systems.

The payment card industry has a set of data security standards known asPCI-DSS. These standards require end-to-end encryption of sensitive payment data when it is transmitted, received or stored.

This payment data is decrypted in the PoS's RAM for processing, and the RAM is where the scraper strikes. Using regular expression searches, they harvest the clear-text payment data and send that information to rogue callhome servers.

Why do we care about PoS RAM scrapers? How does it hurt me?

I believe this malware family has a higher probability of burning a hole in your pocket compared to other prevalent malware families.

In today's plastic money economy people are carrying cash a lot less than before. Aside from a handful of stores, the majority of retailers accept debit or credit cards. Payment cards are convenient, quick, supposedly-secure, and you don't have change jingling around in your pockets.

PoS RAM scrapers target the systems which process debit and credit card transactions and steal the sensitive payment information. Your home computer might be super secure, but there is no guarantee the PoS system at your neighborhood grocery store has the same level of security. You might end up losing your credit card data buying a candy bar!

How have PoS RAM scrapers evolved?

Sophos detects PoS RAM scraper malware under the family name *Trackr*(e.g. Troj/Trackr-Gen, Troj/Trackr-A) Other AV vendors detect this malware family with a variety of names, the most common name being *Alina*.

Some of the earliest variants of Trackr had simple functionality that worked like this:

1. Install as a service
2. Use a legitimate-looking name
3. Scan RAM for credit card track one and track two data
4. Dump the results into a text file. This text file was then probably accessed remotely or manually.

Over the years Trackr has become more industrialized, with some cosmetic changes and added bot and network functionality.

Our friends at Trustwave SpiderLabs have written two excellent articles,Alina: Casting a Shadow on PoS and Alina: Following

The Shadow, about the inner workings of the Trackr family.

Till now we have observed the following types of Trackr:

- Basic version (not packed, scrapes RAM for credit card information)
- Complex version (added socially-engineered filenames, bot and network functionality)
- Installed DLL version (the DLL is registered as a service and performs the RAM scraping)
- Versions one and two packed with a commercially-available packer
- Versions one and two packed with a custom packer

Most recently, SophosLabs discovered the highly-prevalent Citadel crimeware targeting PoS systems.

The Citadel malware uses screen captures and keylogging instead of the RAM-scraping technique used by Trackr. Citadel's focus on PoS systems demonstrates that this avenue is fast becoming a point of serious concern.

Who do PoS RAM scrapers target?

One of the earliest serious PoS RAM scraper attacks that we observed was back in November 2011 when we found that a university and several hotels had their PoS systems compromised. Later we saw varied targets including an auto dealership in Australia infected with Trackr.

To better understand the threat we gathered statistics about the various industries targeted by Trackr during the past 6 months (as observed using Sophos Live Protection):

It doesn't come as a surprise that the biggest targeted industries are:

- Retail

- Service
- Healthcare
- Food services
- Education
- Hotel and tourism

In these industries there's a high volume of credit and debit card transactions taking place, meaning they have goldmines of payment data that can be harvested.

Compromising a single PoS system (e.g. in a fast food outlet) may yield thousands of credit cards per week, cheaply – much easier to gather 10,000 credit card details from one PoS system then attempt to infect 10,000 PCs, hoping to grab the data from there.

If not protected properly, PoS systems become easy targets – a single point of failure that can affect thousands of people.

In addition to the breakdown of industries targeted, we also looked at the countries where we saw Trackr infections over the same time period:

Again, no surprises that the developed countries top this chart with the US, where credit cards are abundant, taking the #1 spot.

In fact, the Trackr infection numbers match up closely with the credit card country usage statistics published by Visa.

So how does Trackr get on a PoS system?

We have used the term PoS quite generally throughout this article. PoS is the place where a retail transaction is completed. So a PoS could be some custom hardware/software solution, a regular PC running PoS software, a credit card transaction server, or something similar.

Big box retailers and chain stores have security-hardened PoS systems, and we have not seen any major evidence of these large organizations getting compromised with Trackr.

The victims tend to be mostly small to medium sized organizations who will typically have less investment in defensive counter-measures.

Based on our analysis there were two main methods of infection:

Insider job

Someone with active knowledge of the payment processing setup installs a RAM scraper to gather data. The early Trackr samples dropped their harvested data in a plain text file which we suspect was manually retrieved or remotely accessed.

The malware had no network functionality and we found no evidence of a top-level dropper/installer.

Phishing/Social Engineering

These are the common infection vectors with the more complex versions of Trackr. The socially engineered filenames we have observed includeTaskmgr.exe, windowsfirewall.exe, sms.exe, java.exe, win-firewall.exe, andadobeflash.exe. This suggests that the files were delivered as part of a phishing campaign, or social engineering tricks were used to infect the system.

Importantly however, Trackr is not seen regularly in the mass-spammed malware campaigns that we observe daily. Rather it is highly targeted towards a group of relevant businesses.

To conclude, it is not always a safe solution to pay for everything with cards.

Everyone should follow computer security best practices and consumers should proactively sign-up for credit monitoring

services so they don’t becomes victims of credit or identity theft.

Businesses big and small need to make investments to protect their critical PoS infrastructure. Just like they wouldn’t keep their cash registers unlocked for someone to grab money out of them, PoS systems need proper protection.

Inside TAO: Documents Reveal Top NSA Hacking Unit

More leaked documents reveal a secret NSA hacking operation, with techniques ranging from physical implants of malware (sometimes hardware) to infiltrating Telecom networks, and even exploiting Microsoft updates to infect the target machine. TAO has existed since 1997, but recently interest in the program is exploding, as seen by the drastic increase in the number of TAO operation facilities, and the number of employees.

> *The NSA’s TAO hacking unit is considered to be the intelligence agency’s top secret weapon. It maintains its own covert network, infiltrates computers around the world and even intercepts shipping deliveries to plant back doors in electronics ordered by those it is targeting… One example of the sheer creativity with which the TAO spies approach their work can be seen in a hacking method they use that exploits the error-proneness of Microsoft’s Windows. Every user of the operating system is familiar with the annoying window that occasionally pops up on screen when an internal problem is detected, an automatic message that prompts the user to*

> *report the bug to the manufacturer and to restart the program. These crash reports offer TAO specialists a welcome opportunity to spy on computers. The technique can literally be a race between servers, one that is described in internal intelligence agency jargon with phrases like: "Wait for client to initiate new connection," "Shoot!" and "Hope to beat server-to-client response." Like any competition, at times the covert network's surveillance tools are "too slow to win"..*

Read the full article here – Inside TAOs_ Documents Reveal Top NSA Hacking Unit – SPIEGEL ONLINE Considering TAO is an NSA sponsored hacking program, it wouldn't be a stretch to see Spiegel soon hacked, so we are keeping this article here on Global Intel Hub.