Interview with Sergey Ulasen, The Man Who Found The Stuxnet Worm

I'm very excited about today's guest. Very few industry experts know him by name, even though he's the guy who first discovered the notorious Stuxnet worm in 2010. His name is Sergey Ulasen.

Sergey UlasenFirst, a few background words about Sergey. I'm happy to say that he joined the company in August 2011, immediately starting to contribute to the ever growing expertise of our malware analysis team, which now consists of more than 100 experts around the world. He's a very professional and high spirited man, possessing the expert knowledge and experience for tackling even the most sophisticated threats.

Sergey graduated in 2006 from the Belorussian State Technical University with a B.Sc. in software development. He began his professional career with local anti-virus vendor VirusBlokAda as a programmer. Later Sergey joined the team that engineered the company's anti-virus engine, and in 2008 he became the team leader. He was also involved in developing anti-rootkit and system rescue technologies, and helped with solving the most sophisticated malware incidents.

Then he joined KL. Me very happy.

Sergey, let's go back to the moment when your team first discovered the Stuxnet sample. How did it all come about?

It was all quite simple, actually – far from how such things might be portrayed in the movies, I can tell you!

At the time I was working for a relatively small security company, and had quite a lot of different responsibilities. I was involved in software development, threat analysis, technical consulting, and dealing with incidents involving the most sophisticated malware as reported by our customers.

It all started when the technical support guys informed me about a rather unusual case: a customer in Iran reported arbitrary BSODs and computer reboots. They forwarded me the help-request together with info about their preliminary scanning reports.

What were your first impressions about the case?

My very first impression was that the anomalies found were due to some Windows misconfiguration or were the result of a conflict between installed applications. It's well-known of course that systems commonly get all in a tangle due to software conflicts.

So I recommended that the tech-support guys got as much info about the installed applications as possible. The penny dropped when I learned that the same anomalies had been found on many other computers in the customer's network – even on computers with freshly installed Windows after a thorough anti-junk-applications check. This was the moment I realized this was something more than just your average system malfunction – there was no doubt a malware infection was involved. And it most certainly had been expertly designed and constructed (that is, apart from its causing regular BSODs) since we couldn't detect it with regular detection means. Most probably a rootkit was involved too.

Luckily, our partner in Iran who first reported the issue is not just an experienced security expert but also a good friend and on my IM contact list. I just wonder how things would have turned out if we hadn't had this sort of connection...

My pal first tried to solve the matter himself, and then later with the help of technical support. To no avail. As persistent as ever, he then pings me for assistance.

This all happened on a sunny (in Iran) Saturday, which was a working day there. Meanwhile, up in an overcast Belarus, I was at a friend's wedding reception – some 400 km from Minsk. All the other guests were of course happily celebrating, dancing and drinking far too much, while I was there hanging on the telephone (my mobile) all the time delivering urgent technical – and psychological! – assistance to a dude near Tehran. Bubbly girls – bubbly in hand – dressed to the nines kept passing by to and fro (by this time the festivities had taken themselves outside into the woods; (don't ask)) wondering what on earth I was doing talking strange things in some strange language in the woods at a wedding. And of course judging me as some kinda bizarre geek-freak ("but if only they got to *know* me"). *ANY*way… before long my mate in Iran and I realized we couldn't make any more headway over the phone, so called it a night and decided to continue our investigation on Monday. I was hoping Mondays were working days in Iran as well as Saturdays…

Come Monday afternoon, first we solved some technical issues with getting remote access to the infected computer. I must say it took a great deal of effort to find the cause of the anomalies. But we got there in the end. We eventually found the malware, and figured out its stealthy nature, strange payload and spreading techniques.

The Stuxnet drivers were signed with genuine digital certificates from respected companies. Sort of like the multipasses in The Fifth Element! Digital certificates are things that (at least used to) guarantee that one can trust a file. Why did you decide nevertheless to delve into it?

Once we found the cause of the trouble we started more in-depth analysis with my colleagues in the virus lab. This involved lots of heated discussion and argument, and actually plenty of swearing too :) – since there's no textbook approach to something like this and we were learning as we went along. We kept on with it – brainstorming, drawing up schemes, and developing different idea threads. And with each step we were gradually getting more and more queasy as we started to understand just what we were dealing with.

We finally parsed the malware and worked out that it was using zero-day vulnerabilities that allowed Stuxnet to penetrate even well-patched Windows computers. And it was at this point we all agreed the digital certificate had been stolen. Additionally, the complexity of Stuxnet's code and extremely sophisticated rootkit technologies led us to conclude that this malware was a fearsome beast with nothing else like it in the world, and that we needed to inform the infosec industry and community of the details ASAP.

So what was the response from the industry and community?

Well, early on that was nothing short of shocking!

At first we decided not to go public and that it would be better to just inform the other parties involved. We tried to reach out both to Microsoft and Realtek – but got no proper response! In hindsight, I now understand that we shouldn't have done things quite that way; after all, what are the chances of an alert from a small Belarusian AV company getting through to the decision makers there?

So then I decided to go public and report the issue to the community. I published some details about Stuxnet on our website and also on the popular industry forum at wilderssecurity.com. A bit later, after carrying out some further analysis, I reassured myself about the seriousness of the incident and together with my colleague Oleg Kupreev published a more in-depth description of the malware along with an announcement about the zero-day vulnerability and stolen certificate.

And this was the point when things went ballistic!

Please, go on!!

The first person to post a note about the incident was the famed Brian Krebs. Then came Frank Boldewin, who was the first to make the connection tying Stuxnet to Siemens WinCC SCADA industrial control systems. A bit later we started getting theories connecting the malware to the Iranian nuclear program and the start of cyber warfare, no less.

Meanwhile, thanks to some heavyweight string pulling by Andreas Marx at AV-test.org, I got through to the guys at the Microsoft Security Response Center, who immediately started working on the case.

Again, looking back, I clearly understand now that we made some mistakes in going about things – mistakes that resulted in delays in getting to the root(kit!) of the issue. Unfortunately at that time VirusBlokAda had no knowledge of, or experience of how to deal with, such cases. Indeed, to handle them effectively you really need to know at least a couple of key people in the industry and have their personal e-mails at hand. We didn't.

The other problem was that the company had no resources to perform really thorough analysis of the threat. VirusBlokAda positions itself as a local niche player and invests primarily in customer service. If threat analysis ever took up too many resources, alas, we sometimes had to forego it.

Ultimately this incident confirmed to me that a security company needs strong threat analysis expertise. Dedicated teams need to concentrate on this analysis to ensure a company stays a step ahead of cybercriminals and at least keeps up with any cyber warfare going on – to be prepared to cope appropriately with either as and when it appears.

How did the Iranian officials respond to this… unpleasant news?

They just stonewalled us – no official response at all. Perhaps it's not the country's policy to make public comments on such things. Keeping cards close to one's chest seems to be the Iranian way though – my friend in Iran who helped uncover Stuxnet (on that Saturday – with me in the woods at the wedding) asked that his name never be mentioned in any reports on the matter, and refused to provide any comments on it.

Interestingly, later I met some high-ranking IT-dedicated Iranian officials in Minsk. They made like they didn't know anything at all about the incident. Yeah, right.

Like with many a hot news story that makes the headlines, Stuxnet received its fair share of mis-reporting…

Oh yes! Many of the stories and comments surrounding Stuxnet made me ROFL! Here are some selected foul-ups:

> *"The company developed the worm itself and then used it for self-promotion through the mass media".*

– Well, should we have had the opportunity to afford a dozen of the world's very best security experts to develop Stuxnet, I think we'd have come up with a more peaceful application.

> *"Sergey Ulasen traveled to Iran and helped the Iranians fish out the malware directly from the centrifuges".*

– Oh yeah, with me wearing one of those spaceman-like foil suits. Aye.

> *"Iranians deliberately asked for assistance from a Belorussian company because they don't trust anyone else".*

– Well, they were right about Belarusians being trustworthy. But their "choosing" us? And even if they had "chosen" us... No, sorry, this false statement simply can NOT be rationalized!

> *"The Iranians used the company to publicly accuse Western countries of starting a cyberwar".*

– Considering the Iranian authorities' cloak of silence thrown over the whole affair, I doubt they needed any more noise being made about this incident. Even if they did, they could have found more effective ways of doing so.

> *"Sergey Ulasen is an enemy of democracy and liberal values in the Middle East".*

– Oh sure, and I also built the Berlin Wall.

Let me state it clearly. Neither I nor the people I worked with on this investigation ever publicly expressed any conspiracy theories regarding the origin or aims of Stuxnet. I was never interested in spending my time trying to understand any political aspect to the story. I'm a malware expert delivering first-class protection against cyber threats, not producing thrillers.

Of late the Internet has been flooded with speculation about the recently discovered *Duqu* Trojan, which has already been christened Stuxnet's child/grandchild/stepbrother/cousin twice removed, etc. Indeed, they do have lots in common. What do you think about this?

There's still too much uncertainty about Duqu.

Considering the lack of concrete information about this malware I'd say what's going on now is pretty much a repeat of what we had with Stuxnet – assumptions, allegations, and pop-labeling by people who don't know what they're talking about, with the real facts of the matter buried among all the BS. Not to mention the pure hype and scaremongering, like this:

NEW THREAT:
"Stuxnet Lite"
W32/Duqu
DON'T LET STUXNET SHUT YOU DOWN!
Read more about this new threat
»

Honestly, I prefer not to speculate on this matter and wait until the dust settles to see the whole picture. I'll be carefully following Aleks Gostev's series of blog posts on Securelist re *Duqu*, and I'm pretty sure we'll soon have a full and accurate account of the malware's origin, aims, and technical aspects.

What I am sure of at the moment is that there *is* a clear connection between Duqu and Stuxnet as the former malware is based on the latter's source code and employs many of its techniques. Also, the way the teams behind both types of malware spawned their creatures to the world is also very similar. The only difference between them seems to be that the Duqu case is still shrouded in mystery.

I'm sure any security vendor would love to have you on board to strengthen their team's expertise. Why did you choose to join our company?

Actually Kaspersky Lab was the only option I was considering when thinking about quitting my previous job.

I've always admired the company's achievements and respected the people working here and the way they do their job. I was convinced – and this conviction's only increased since I started working here – that KL is the world's most technologically advanced anti-malware vendor, which has succeeded in gathering a unique team of security professionals doing just fantastic things. No doubt the company has even more great potential – it has so many new killer technologies under the hood yet to be introduced to the public…

When I heard for the first time that KL was planning on being the No. 1 anti-malware vendor in the world, I found it hard to take seriously. I'm sure ten years ago there weren't many who could have imagined the company becoming No. 4. But now, having seen that come about, I'd say becoming No. 1 is no pipe dream.

Anything else you'd like to add before we get to the traditional (for the "In the Spotlight" series) questions about personal and out-of-office stuff?

say six current and former employees

who declined to discuss the matter publicly because they feared reprisals

First of all, I'd like to announce that this is the very last talk I'm giving about Stuxnet.

Frankly, I've had my fill of this topic, which has been whirling around me now for 18 months. Sometimes I even get myself thinking that Stuxnet is a hindrance to my professional career. I've many things to be proud of besides this worm. Indeed, I've been involved in many other significant projects leveraging my intellectual and emotional efforts, which have delivered much more visible results for the company and for my personal development.

So I'd like to end the Stuxnet chapter once and for all, and head towards new horizons in fighting cybercrime.

Fair enough! Now – the non-work stuff…

I think people should continually develop themselves. And that of course includes me. So whenever I get a free moment I'm always trying to do something worthwhile to further myself. For example, when watching, say, an American movie, I always switch to the original audio track to practice my English comprehension skills. Also, in the past when getting to the office took quite a while, I used this time to listen to podcasts, training programs and foreign literature.

My favorite movies fall into the art-house, drama and comedy genres. I detest horror movies. In my opinion we see enough horror on the news. Nor am I a fan of thrillers…

I love my parents, sister and nephew, and also my friends – who sadly I don't see much of these days. However, each time we do get to meet it turns out to be a really cool shindig!

I relish visiting my grandma in the countryside. Conciliating ambience, a total absence of mobile coverage, and unity with nature take me away from the day-to-day stresses, and deliver the ultimate in relaxation and recuperation! Trust me – getting all the clutter out of a brain in just two days – I’ve got it down to an art-form. I should set up a speed-chill school :)

Sergey, thanks loads for chatting with me. I’m flattered to have taken the very last Stuxnet talk form the guy who discovered it! And what I can guarantee here at the company are many new challenges and extremely interesting work with talented people!