

Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon

The idea behind the Stuxnet computer worm is actually quite simple. We don't want Iran to get the Bomb. Their major asset for developing nuclear weapons is the Natanz uranium enrichment facility. The gray boxes that you see, these are real-time control systems. Now if we manage to compromise these systems that control drive speeds and valves, we can actually cause a lot of problems with the centrifuge. The gray boxes don't run Windows software; they are a completely different technology. But if we manage to place a good Windows virus on a notebook that is used by a machines engineer to configure this gray box, then we are in business. And this is the plot behind Stuxnet.

So we start with a Windows dropper. The payload goes onto the gray box, damages the centrifuge, and the Iranian nuclear program is delayed -- mission accomplished. That's easy, huh? I want to tell you how we found that out. When we started our research on Stuxnet six months ago, it was completely unknown what the purpose of this thing was. The only thing that was known is very, very complex on the Windows part, the dropper part, used multiple zero-day vulnerabilities. And it seemed to want to do something with these gray boxes, these real-time control systems. So that got our attention, and we started a lab project where we infected our environment with Stuxnet and checked this thing out. And then some very funny things happened. Stuxnet behaved like a lab rat that didn't like our cheese -- sniffed, but didn't want to eat. Didn't make sense to me. And after we experimented with different flavors of cheese, I realized, well, this is a directed attack. It's completely directed. The dropper is prowling actively on the gray box if a specific configuration is found, and even if the actual program that it's trying to infect is actually running on that target. And if not, Stuxnet does nothing.

So that really got my attention, and we started to work on this nearly around the clock, because I thought, well, we don't know what the target is. It could be, let's say for example, a U.S. power plant, or a chemical plant in Germany. So we better find out what the target is soon. So we extracted and decompiled the attack code, and we discovered that it's structured in two digital bombs -- a smaller one and a bigger one. And we also saw that they are very professionally engineered by people who obviously had all insider information. They knew all the bits and bites that they had to attack. They probably even know the shoe size of the operator. So they know everything.

And if you have heard that the dropper of Stuxnet is complex and high-tech, let me tell you this: the payload is rocket science. It's way above everything that we have ever seen before. Here you see a sample of this actual attack code. We are talking about -- round about 15,000 lines of code. Looks pretty much like old-style assembly language. And I want to tell you how we were able to make sense out of this code. So what we were looking for is first of all is system function calls, because we know what they do.

And then we were looking for timers and data structures and trying to relate them to the real world -- to potential real world targets. So we do need target theories that we can prove or disprove. In order to get target theories, we remember that it's definitely hardcore sabotage, it must be a high-value target, and it is most likely located in Iran, because that's where most of the infections had been reported. Now you don't find several thousand targets in that area. It basically boils down to the Bushehr nuclear power plant and to the Natanz fuel enrichment plant.

Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon

So I told my assistant, "Get me a list of all centrifuge and power plant experts from our client base." And I phoned them up and picked their brain in an effort to match their expertise with what we found in code and data. And that worked pretty well. So we were able to associate the small digital warhead with the rotor control. The rotor is that moving part within the centrifuge, that black object that you see. And if you manipulate the speed of this rotor, you are actually able to crack the rotor and eventually even have the centrifuge explode. What we also saw is that the goal of the attack was really to do it slowly and creepy -- obviously in an effort to drive maintenance engineers crazy, that they would not be able to figure this out quickly.

The big digital warhead -- we had a shot at this by looking very closely at data and data structures. So for example, the number 164 really stands out in that code; you can't overlook it. I started to research scientific literature on how these centrifuges are actually built in Natanz and found they are structured in what is called a cascade, and each cascade holds 164 centrifuges. So that made sense, it was a match.

And it even got better. These centrifuges in Iran are subdivided into 15, what is called, stages. And guess what we found in the attack code? An almost identical structure. So again, that was a real good match. And this gave us very high confidence for what we were looking at. Now don't get me wrong here, it didn't go like this. These results have been obtained over several weeks of really hard labor. And we often went into just a dead-end and had to recover.

Anyway, so we figured out that both digital warheads were actually aiming at one and the same target, but from different angles. The small warhead is taking one cascade, and spinning up the rotors and slowing them down, and the big warhead is talking to six cascades and manipulating valves. So in all, we are very confident that we have actually determined what the target is. It is Natanz, and it is only Natanz. So we don't have to worry that other targets might be hit by Stuxnet.

Here's some very cool stuff that we saw -- really knocked my socks off. Down there is the gray box, and on the top you see the centrifuges. Now what this thing does is it intercepts the input values from sensors -- so for example, from pressure sensors and vibration sensors -- and it provides legitimate code, which is still running during the attack, with fake input data. And as a matter of fact, this fake input data is actually prerecorded by Stuxnet. So it's just like from the Hollywood movies where during the heist, the observation camera is fed with prerecorded video. That's cool, huh?

The idea here is obviously not only to fool the operators in the control room. It actually is much more dangerous and aggressive. The idea is to circumvent a digital safety system. We need digital safety systems where a human operator could not act quick enough. So for example, in a power plant, when your big steam turbine gets too over speed, you must open relief valves within a millisecond. Obviously, this cannot be done by a human operator. So this is where we need digital safety systems. And when they are compromised, then real bad things can happen. Your plant can blow up. And neither your operators nor your safety system will notice it. That's scary.

Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon

But it gets worse. And this is very important, what I'm going to say. Think about this. This attack is generic. It doesn't have anything to do, in specifics, with centrifuges, with uranium enrichment. So it would work as well, for example, in a power plant or in an automobile factory. It is generic. And you don't have -- as an attacker -- you don't have to deliver this payload by a USB stick, as we saw it in the case of Stuxnet. You could also use conventional worm technology for spreading. Just spread it as wide as possible. And if you do that, what you end up with is a cyber weapon of mass destruction. That's the consequence that we have to face. So unfortunately, the biggest number of targets for such attacks are not in the Middle East. They're in the United States and Europe and in Japan. So all of the green areas, these are your target-rich environments. We have to face the consequences, and we better start to prepare right now.

Thanks.

(Applause)

Chris Anderson: I've got a question. Ralph, it's been quite widely reported that people assume that Mossad is the main entity behind this. Is that your opinion?

Ralph Langner: Okay, you really want to hear that? Yeah. Okay. My opinion is that the Mossad is involved, but that the leading force is not Israel. So the leading force behind that is the cyber superpower. There is only one, and that's the United States -- fortunately, fortunately. Because otherwise, our problems would even be bigger.

CA: Thank you for scaring the living daylights out of us. Thank you Ralph.

(Applause)

Translation:

Die Idee hinter dem Stuxnet Computerwurm ist eigentlich ganz einfach. Wir wollen nicht der Iran die Bombe bekommen. Ihr großes Plus für die Entwicklung von Atomwaffen ist die Urananreicherungsanlage Natanz. Die grauen Felder, die Sie sehen, sind diese in Echtzeit Steuerungssysteme. Nun, wenn es uns gelingt, diese Anlagen, die Kontrolle Fahrgeschwindigkeiten und Ventile, wir tatsächlich dazu führen können eine Menge Probleme mit der Zentrifuge Kompromiss. Die grauen Felder werden nicht ausgeführt Windows-Software, sie sind eine ganz andere Technik. Aber wenn wir eine gute Windows-Virus auf einem Notebook, dass durch eine Maschinen-Ingenieur wird verwendet, um diese graue Box konfigurieren Ort, zu verwalten, dann sind wir im Geschäft. Und dies ist das Grundstück hinter Stuxnet.

So beginnen wir mit einem Windows-Dropper. Die Nutzlast geht auf das graue Feld, Schäden der Zentrifuge und das iranische Atomprogramm wird verzögert - Mission erfüllt. Das ist einfach, oder? Ich möchte Ihnen sagen, wie wir herausgefunden. Wenn wir unsere Forschung begann am Stuxnet vor sechs Monaten war es völlig unbekannt, was der Zweck dieser Sache war. Das einzige, was bekannt war, ist sehr, sehr komplex in der Windows-Teil der Pipette Teil verwendet mehrere Zero-Day-Schwachstellen. Und es schien, dass etwas mit dieser grauen Kisten, diese in Echtzeit Kontrollsysteme zu tun. Damit haben unsere Aufmerksamkeit, und wir begannen ein Labor Projekt, wo wir mit unserer

Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon

Umwelt infiziert Stuxnet und überprüft diese Sache aus. Und dann ein paar sehr lustige Dinge passiert. Stuxnet benahm sich wie eine Laborratte, die nicht mochte unsere Käse - Schnupfen, aber wollte nicht essen. Hat keinen Sinn für mich. Und nachdem wir mit verschiedenen Geschmacksrichtungen von Käse experimentierte, wurde mir klar, gut, das ist ein Angriff gerichtet ist. Es ist völlig gerichtet. Der Dropper aktiv streifen auf das graue Feld, wenn eine bestimmte Konfiguration gefunden wird, und selbst wenn das eigentliche Programm, es versucht zu infizieren ist tatsächlich ausgeführt wird auf dieses Ziel. Und wenn nicht, tut nichts Stuxnet.

Damit bekam wirklich meine Aufmerksamkeit, und wir fingen an zu dieser Arbeit fast rund um die Uhr, weil ich dachte, gut, wir wissen nicht, was das Ziel ist. Es könnte sein, lassen Sie uns zum Beispiel sagen, ein US-Kraftwerk oder einer Chemiefabrik in Deutschland. Also haben wir besser herausfinden, was das Ziel ist bald. Also haben wir gewonnen und dekompiert den Angriff Code, und wir entdeckten, dass es in zwei digitale Bomben's strukturiert - ein kleineres und ein größeres. Und wir sahen auch, dass sie sehr professionell sind Leute, die offensichtlich hatten alle Insider-Informationen entwickelt. Sie wussten alle Bits und beißt, dass sie zum Angriff hatte. Wahrscheinlich haben sie einmal die Schuhgröße des Betreibers. Und sie wissen alles.

Und wenn Sie habe gehört, dass die Pipette von Stuxnet komplex und High-Tech ist, lassen Sie mich Ihnen sagen: Die Nutzlast ist Hexenwerk. Es ist weit über alles, was wir noch nie gesehen. Hier sehen Sie eine Probe dieses eigentlichen Attacke Code. Wir sprechen über - rund rund 15.000 Zeilen Code. Sieht ziemlich genau wie im alten Stil Assembler. Und ich möchte Ihnen sagen, wie wir in der Lage, Sinn zu machen aus diesem Kodex wurden. Also, was wir gesucht haben ist in erster Linie ist System-Funktion aufruft, weil wir wissen, was sie tun.

Und dann waren wir für Timer und Datenstrukturen und versucht, sie in die reale Welt beziehen suchen - mögliche Ziele der realen Welt. Also brauchen wir Theorien Ziel, dass wir beweisen oder widerlegen können. Um Ziel Theorien zu bekommen, wir erinnern uns, dass es definitiv Hardcore-Sabotage, muss es ein hochwertiges Ziel sein, und es ist sehr wahrscheinlich, das sich in den Iran, weil dort die meisten Infektionen gemeldet worden seien. Jetzt müssen Sie nicht finden mehrere tausend Ziele in diesem Bereich. Im Grunde läuft alles auf das Kernkraftwerk Bushehr und die Treibstoff Natanz Anreicherungsanlage.

Also erzählte ich meiner Assistentin, "Get me eine Liste aller Zentrifuge und Kraftwerk Experten aus unserem Kundenstamm." Und ich rief sie abgeholt und ihr Gehirn in dem Bemühen, ihr Know-how mit, was wir gefunden in Code und Daten übereinstimmen. Und das funktionierte ziemlich gut. So konnten wir verbinden die kleinen digitalen Sprengkopf mit dem Rotor steuern. Der Rotor besteht darin, dass bewegliche Teil in der Zentrifuge, dass schwarze Objekt, das Sie sehen. Und wenn man die Geschwindigkeit dieser Rotor zu manipulieren, sind Sie eigentlich in der Lage, knacken Sie den Rotor und schließlich sogar die Zentrifuge explodieren. Was wir sahen auch, dass das Ziel des Angriffs war wirklich zu langsam und gruselig zu tun - offenbar in dem Bemühen, Instandhalter verrückt, dass sie nicht in der Lage wäre, diese Zahl schnell zu fahren.

Die große digitale Sprengkopf - wir hatten eine Chance auf diese, indem Sie sehr genau auf Daten und Datenstrukturen. So zum Beispiel, das Heft 164 steht

Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon

wirklich in diesem Code, kann man nicht übersehen. Ich fing an, wissenschaftliche Literatur, wie diese Zentrifugen sind tatsächlich in Natanz gebaut und fanden sie in einer so genannten Kaskade strukturiert sind, und jeder Kaskade hält 164 Zentrifugen Forschung. Damit machte Sinn, es war ein Spiel.

Und es sogar noch besser. Diese Zentrifugen in Iran sind in 15, was heißt, Stufen unterteilt. Und raten Sie mal, was wir im Angriff Code gefunden? Eine nahezu identische Struktur. Also noch einmal, war, dass ein wirklich gutes Spiel. Und das hat uns sehr hohes Vertrauen für das, was wir suchten. Jetzt wollen Sie mich nicht falsch hier, es hat nicht so weitergehen. Diese Ergebnisse wurden über mehrere Wochen wirklich harte Arbeit erhalten. Und wir gingen oft in nur einer Sackgasse und hatte sich zu erholen.

Jedenfalls, so dass wir herausgefunden, dass sowohl digitale Sprengköpfe waren eigentlich darauf abzielen ein und dasselbe Ziel, aber aus unterschiedlichen Blickwinkeln. Die kleinen Sprengkopf ist unter einer Kaskade und Spinnen bis die Rotoren und verlangsamt werden, und die großen Gefechtskopf ist auf sechs Kaskaden und Manipulieren von Ventilen reden. Also in allem sind wir sehr zuversichtlich, dass wir eigentlich bestimmt, was das Ziel ist. Es ist Natanz, und es ist nur Natanz. So haben wir nicht zu befürchten, dass andere Ziele Stuxnet könnten betroffen sein.

Hier gibt's einige sehr coole Sachen, die wir gesehen haben - wirklich klopfte meine Socken aus. Dort unten ist das graue Feld, und auf der Oberseite sehen Sie die Zentrifugen. Nun, was dieses Ding tut, ist es fängt die Eingabewerte von Sensoren - so zum Beispiel von Drucksensoren und Schwingungssensoren - und es gibt legitime Code, der noch läuft während des Angriffs, mit gefälschten Eingabedaten. Und da in der Tat, das ist fake Eingangsdaten tatsächlich Stuxnet bespielte. Also ist es genauso wie von den Hollywood-Filmen, wo während der heist, die Beobachtung mit Kamera aufgezeichnete Video eingespeist wird. Das ist cool, huh?

Die Idee ist hier offensichtlich nicht nur für die Betreiber in der Leitwarte Narr. Es ist eigentlich viel gefährlicher und aggressiver. Die Idee ist, eine digitale Sicherheitssystem zu umgehen. Wir müssen digitale Sicherheitssysteme, wo einem menschlichen Operator nicht handeln konnte schnell genug. So zum Beispiel, in einem Kraftwerk, wenn der große Dampfturbine wird auch über Geschwindigkeit, müssen Sie Entlastungsventile innerhalb einer Millisekunde zu öffnen. Offensichtlich kann dieser nicht durch einen menschlichen Bediener durchgeführt werden. Also das ist, wo wir digitale Sicherheitssysteme müssen. Und wenn sie gefährdet sind, dann kann wirklich schlimme Dinge passieren. Ihre Anlage kann die Luft sprengen. Und weder Sie noch Ihr Unternehmen Sicherheit System wird es bemerken. Das ist beängstigend.

Aber es kommt noch schlimmer. Und das ist sehr wichtig, was ich sagen werde. Denken Sie darüber nach. Dieser Angriff ist generisch. Es hat nichts zu tun, in Einzelheiten, mit Zentrifugen, die Anreicherung von Uran. So würde es auch funktionieren, zum Beispiel in einem Kraftwerk oder in einer Autofabrik. Es ist generisch. Und Sie müssen nicht - wie ein Angreifer - müssen Sie nicht auf diesen Nutzlast von einem USB-Stick zu liefern, wie wir sie sah im Falle der Stuxnet. Sie können auch herkömmliche WORM-Technologie für die Verbreitung. Nur breitete es so breit wie möglich. Und wenn Sie das tun, was Sie am Ende mit ein Cyber Massenvernichtungswaffe. Das ist die Konsequenz, dass wir uns stellen

Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon

müssen. Also leider sind die größte Anzahl von Zielen für solche Angriffe nicht in den Nahen Osten. Sie sind in den Vereinigten Staaten und Europa und in Japan. Also alle grünen Bereiche sind diese Ihr Ziel-reiche Umgebungen. Wir müssen die Konsequenzen tragen, und wir besseren Start sich jetzt vorbereiten.

Dank.

(Beifall)

Chris Anderson: Ich habe eine Frage. Ralph, es ist recht ausführlich berichtet, dass die Menschen davon ausgehen, dass die wichtigsten Unternehmen Mossad dahinter ist. Ist das Ihre Meinung?

Ralph Langner: Okay, Sie wirklich wollen, das gehört? Yeah. Okay. Meine Meinung ist, dass der Mossad beteiligt ist, sondern daß die führende Kraft ist nicht Israel. Also die führende Kraft dahinter ist die Cyber-Supermacht. Es gibt nur einen, und dass die Vereinigten Staaten ist - zum Glück, zum Glück. Denn sonst würden unsere Probleme auch größer sein.

CA: Vielen Dank für erschrecken den helllichten Tag von uns. Danke Ralph.

(Beifall)

Quelle:

http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber_weapon.html?utm_source=newsletter_weekly_2011-03-30&utm_campaign=newsletter_weekly&utm_medium=email