TOFINO™

tofinosecurity.com/blog

Shamoon Malware and SCADA Security – What are the Impacts?

Published September 25, 2012

The latest post-Stuxnet discovery of advanced threats is a malicious malware known as Shamoon. Like Stuxnet, Duqu and Flame, it targeted energy companies in the Middle East, this time Saudi Aramco and likely other oil and gas concerns in the region including Qatar's RasGaz. It is a new species however, because it did not disrupt an industrial process as Stuxnet did, nor did it stealthily steal business information as Flame and Duqu did. Instead it removed and overwrote the information on the hard drives of 30,000 (yes that number is correct1) workstations of Saudi Aramco (and who knows how many more at other firms).

Nothing this damaging has been seen in a while. As a Kaspersky Lab expert commented "Nowadays, destructive malware is rare; the main focus of cybercriminals is financial profit. Cases like the one here do not appear very often."

What does Shamoon mean for SCADA and ICS Security? Hold that thought for a few paragraphs...

Saudi Aramco's headquarters complex. This is one of the sites where workstation hard drives were wiped clean by the Shamoon virus. Photo: Wikipedia

What is Shamoon?

First publicized on August 16, 2012 by Symantec, Kaspersky Labs, and Seculert, Shamoon took control of an Internet connected computer at Saudi Aramco. It then used that computer to communicate back to an external Command-and-Control server and to infect other computers running Microsoft Windows that were not Internet connected.

The name Shamoon comes from a folder name within the malware executable:

“c:\shamoon\ArabianGulf\wiper\release.pdb”

While the significance of the word “Shamoon” is not known, it is speculated that it is the name of one of the malware authors. Shamoon is the equivalent of Simon in Arabic.

Symantec describes Shamoon as having 3 components:

1. Dropper – the main component and source of the original infection. It drops components 2 and 3 onto the infected computer, copies itself to network shares, executes itself and creates a service to start itself whenever Windows starts.
2. Wiper – this is the destructive module. It compiles a list of files from specific locations on the infected computers, erases them, and sends information about the files back to the attacker. The erased files are overwritten with corrupted jpeg files, “obstructing any potential file recovery by the victim”2.
3. Reporter – this module sends infection information back to the attacker’s central computer.

While all of this sounds sophisticated, expert analysis (Kaspersky Labs) concluded, due to a number of errors found in the code, that the developers of Shamoon are “skilled amateurs”. They are not in the same league as the sophisticated coders of Stuxnet and Flame.

What Damage did Shamoon do?

On August 15, 2012 Saudi Aramco posted on its Facebook page that

“...the company has isolated all its electronic systems from outside access as an early precautionary measure that was taken following a sudden disruption that affected some of the sectors of its electronic network. The disruption was suspected to be the result of a virus that had infected personal workstations without affecting the primary components of the network."

They later told Reuters

"Shamoon [the virus] spread through the company's network and wiped computers' hard drives clean. Saudi Aramco says damage was limited to office computers and did not affect systems software that might hurt technical operations."

However, as CIO blogger Constantine von Hoffman stated:

“You don’t destroy 30,000 workstations without causing a vast amount of damage. It might be possible that the attack didn’t directly hit oil production or harm the flow of oil out of the ground. No one I’ve spoken to has suggested it did, but it’s clear that if the company's statement is true then Aramco used a very strict reading of the phrase “oil production.”

Mr. von Hoffman went on to question the Saudi Aramco statement that all damage had been repaired by Aug 26th. He also wonders, in the days of oil and gas projects being dominated by joint ventures, how other energy companies' computers could not have been damaged by Shamoon.

Saudi Aramco's Uthmaniyah gas plant, like other of the companies production sites were apparently unaffected by the Shamoon malware. Photo courtesy of: Saudi Aramco.

Who Created Shamoon? Why did they do it?

Recently the Shamoon attack has been reported to have been initiated by an insider, "an extraordinary development in a country where open dissent is banned".

It may have been the work of a group called the "Cutting Sword of Justice" who claimed responsibility for the attack. In this case the motive seems to be to disrupt the Saudi government's main source of income because of Riyadh's support for Sunni leaders in Bahrain and Sunni rebels in Syria.

If this group is behind Shamoon, it could be a milestone in computer hacking. It would be the first time a group of hobbyists and hacktivists have achieved results similar to what allegedly government's cyber warfare teams have accomplished.

Another clue about the motivations of the creators of Shamoon could be the part of its code that includes a portion of an image of a burning U.S. flag, which is presumed to have been taken from the Wikipedia image. The angle in this case is presumably that disrupting Saudi Aramco would ultimately disrupt U.S. energy supplies.

What does Shamoon have to do with SCADA and ICS Security?

Shamoon was a destroyer of data on workstations of energy companies in the Arabian Gulf. There is no evidence that it had any impact on ICS or SCADA systems.

What does it mean for automation professionals? The good news is that like Stuxnet, Flame and Duqu, Shamoon was highly targeted. But the bad news is that it is another indicator that industry, especially the energy industry is now a target.

Even more concerning is the fact that the bar for effective disruption of a business has been lowered to the level of enthusiastic amateurs. Copycats penetrated a well protected network and destroyed data. This is a bit like the fear we have when we think of terrorists getting their hands on nuclear weapons. No rules of engagement apply!

Call it “cyber warfare” or “cyber hype”, the bottom line is that the information / networked world is facing increased threats and ICS and SCADA systems are part of that world.

What are your thoughts on Shamoon? Does its discovery impact your security strategy?

[1] That is the number quoted by Wikipedia, nationalpost.com, zdnet.com, cio.com and others

[2] http://www.bbc.co.uk/news/technology-19293797

Since this blog was originally published in September 2012, it has been updated. Visit this page for the up-to-date version of this blog.

Related Content to Download

Presentation - "Unicorns and Air Gaps - Do They Really Exist?"

Related Links

- Wikipedia.org, Webpage: Shamoon
- Saudiaramco.com Webpage: Saudi Aramco Restores Network Services
- Securelist.com, Blog: Shamoon the Wiper Copycats at Work
- Symantec Blog: The Shamoon Attacks
- NYTimes.com, Webpage: Saudi Oil Producer’s Computers Restored After Virus Attack
- Nationalpost.com, Webpage: Insiders suspected in massive Shamoon virus cyber-attack that wiped 30K Saudi oil company computers
- Securelist.com, Blog: Shamoon The Wiper: further details (Part II)
- CIO.com, Webpage: 'Shamoon' Virus That Devastated Saudi Oil Co. Likely to Have Done More Damage
- Webpage: Shamoon News Coverage
- Amazon.com: Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power

Comments

Submitted by Tim Altick (not verified) on Wednesday, September 26, 2012.

Heather, Continue the good

Heather,

Continue the good work in relaying this information to the field. Customer's need to know since the press will not convey the message (with the exception of CBS 60 Minutes on hte Stuxnet virus).

Submitted by Heather MacKenzie on Wednesday, September 26, 2012.

30,000 workstations affected

@zyber_zorro has provided an interesting link pertaining to the 30,000 number:
http://pastebin.com/cTJeeTat

If real, then the 30,000 number is real.

Submitted by Zyber_zorro (not verified) on Friday, September 28, 2012.

Shamoon recovery

What is the best approach to recover from this security incident? ip map is published, server names are published, all good stuff for planning a next attack.

Is the best approach to change all this or just continue?

Submitted by Sinclair Koelemij (not verified) on Tuesday, September 25, 2012.

Shamoon

Good summary of the Shamoon malware, though formally the link between Shamoon and the Aramco / Rasgas attacks has never been confirmed by either company.

I think Shamoon is the most worrying event in security, not so much because Shamoon is very advanced malware - it isn't, but the destructive nature of the malware.

We see several very good malware development tools in the market, combining these capabilities with an intention to cause as much damage as possible to the infected computer is a frightning world if we also realize that AV has several shortcomings. Too many malware slipped through the defenses in the last two years.

See also http://insecurity.honeywellprocess.com/