

[Home \(/connect/\)](#) > [Blogs \(/connect/blogs\)](#)> [Security Response \(/connect/symantec-blogs/symantec-security-response\)](#)

## Security Response

<https://twitter.com/threatintel><http://www.symantec.com/connect/item-feeds/blog/2261/feed/all/en/all>**+1**

1 Votes

### Symantec Official Blog

## The Hackers Behind Stuxnet

By: [Patrick Fitzgerald \(/connect/user/patrick-fitzgerald\)](/connect/user/patrick-fitzgerald)

SYMANTEC EMPLOYEE

Created 21 Jul 2010

0 Comments

 : [日本語 \(/connect/ja/blogs/stuxnet-7\)](/connect/ja/blogs/stuxnet-7)

0

<http://en-us.reddit.com/submit?url=http://www.symantec.com/connect/blogs/hackers-behind-stuxnet> [\(/connect/forward?path=node/1395001\)](/connect/forward?path=node/1395001)

W32.Stuxnet has received a lot of media attention over the last few days. This incident provides almost a complete case study of how these attacks succeed and how they will probably be used in the future. A successful attack allowed the attacker to steal confidential SCADA design and usage documents.

Let's start by saying we don't know who is behind the attack, and historically discovering this is very rare. However, if someone proposed this type of attack a month ago, while we would have agreed it was theoretically possible, most would have dismissed such an attack as a movie-plot scenario. Furthermore, attacks of this nature are rarely disclosed publicly.

We know that the people behind this attack aren't amateurs, but their final motive is unclear.

The principal facts in this case are:

- The attackers discovered and used a zero-day vulnerability affecting all versions of Microsoft Windows.

1 of 5 • They developed and used a rootkit to hide their presence.

16/05/2019, 20:19

- They targeted software which is used to control industrial assets and processes; deep

- The hackers were able to sign their files using a legitimate digital certificate from an innocent third party. This digital certificate expired in June but a new driver appeared in July; it was also digitally signed using a digital certificate from another company. Both of these companies have offices in Taiwan. The hackers either stole private keys or were able to get their files signed. The attackers may have more compromised digital signatures.
- The hackers did not use a targeted means of attack. Instead, the threat replicates to USB keys and can infect any Windows computer.

The zero-day vulnerability, rootkit, main binaries, stolen digital certificates, and in-depth knowledge of SCADA software are all high-quality attack assets. The combination of these factors makes this threat extremely rare, if not completely novel.

### **The Lone Wolf**

One possibility is that this attack was perpetrated by the archetypal hacker sitting in his mother's basement. His motives may be driven by a thirst for notoriety. By stealing intellectual property, the lone wolf may want to demonstrate his hacking skills or he may have possibly done it for monetary gain. While possible, the attacker has stolen two digital certificates, used a zero-day exploit, and has an incredibly deep knowledge of a SCADA product. The resources to gather these assets would require a very patient and determined hacker. This threat was not put together in a weekend. The attacker as a lone wolf is unlikely.

### **Disgruntled Employee**

The deep knowledge of the SCADA product have led some to conclude that the attack may have been conducted by an insider, perhaps a disgruntled employee of a company using the software. However, the likelihood of an average disgruntled employee who was also able to discover a zero-day vulnerability and steal two digital certificates is low.

### **Commercial Competitors**

Another possibility is that a competitor of one of the compromised companies is looking to gain an advantage by any means necessary. They may use industrial design documents to learn and emulate the manufacturing process secrets or even cause a denial of service against their competitors. In these cases, historically the attack would have been done by hackers for hire. However, attacks of this nature are typically targeted. In this case, the threat spreads blindly to any Windows computer, whether it belongs to the targeted company or not, and whether or not the system has SCADA software installed. If this is a case of commercial espionage, the attackers may have only been able to get near their targeted systems and created the USB key replication as a means to eventually infect the targeted SCADA systems. They considered the fact that many other computers around the world would eventually be infected as collateral damage, with the hopes that their attack would be completed by the time the threat showed up on the

## State-sponsored Espionage

We have seen recent cases where governments have been accused of sanctioning hacking outside of their borders. A government may be trying to steal state or military secrets. If this attack was state-sanctioned, their motives may be similar to commercial competitors, including potentially gaining military secrets. The complexity and quality of the attack assets lead some to believe only a state would have the resources to conduct such an attack. However, the usage of the second digital certificate is a bit odd. One could make the case that once the first attack succeeded, a state would take cover and not waste the second digital certificate. Instead, by signing a very similar binary, security companies were immediately able to detect the second stolen certificate, making it useless in further compromises.

## Nationalistic, Political, Religious, and Related Motivations

Often attacks attributed to states may actually be conducted by citizens who are simply nationalistic or driven by political, religious, or other causes. Hackers bound by a common cause may target another country, organization, or company that they feel are their enemies. Such hacking groups often have the patience and expertise to gather such attack assets. Further, their goals of continued attack may lead them to continue to refine their attack as they are thwarted or discovered, such as resigning their driver files with a newly stolen digital certificate, modifying their binaries to avoid security product detection, and moving their command-and-control hosts as they are decommissioned.

## Terrorism

One of the darker possibilities is that this attack is motivated by terrorism. If the attacker gained control of a power station or another critical facility, they could wreak havoc, shutting down the facility or causing damage by disrupting the normal operations within the facility. This scenario is like something out of movie and, while for most attacks we'd immediately dismiss this as a possibility, given the amount and quality of the attack assets, terrorism even seems within the realms of possibility in this case.

## Conclusion

Most security professionals that watch action movies where a skilled hacker holds an organization or even a country for ransom will simply dismiss it as fantasy. However, the case of Stuxnet easily reads as if it were the latest Hollywood blockbuster. This is the first publicly widespread threat that has shown a possibility of gaining control of industrial processes and placing that control in the wrong hands. It also shows that in this interconnected world, IT security is more important than ever and that even the unthinkable must now be considered.

The "Myrtus Behind Stuxnet.ky8613860guava.pdb" appears in one of the drivers. Guava belongs to the myrtus plant family. Why guava or myrtus? Let the speculation begin.

Written by Patrick Fitzgerald and Eric Chien

Tags: Products (/connect/search?filters=im\_vid\_31:691), Endpoint Protection (/connect/product/endpoint-protection), Security Response (/connect/search?filters=im\_vid\_51:2261), W32.Stuxnet (/connect/search?filters=im\_vid\_111:11761)

Subscriptions (0)



[\(/connect/user/patrick-fitzgerald\)](/connect/user/patrick-fitzgerald)

**Patrick Fitzgerald (/connect/user/patrick-fitzgerald)**

[View Profile \(/connect/user/patrick-fitzgerald\)](/connect/user/patrick-fitzgerald)

**[Login \(/connect/user/login?destination=blogs%2Fhackers-behind-stuxnet\)](/connect/user/login?destination=blogs%2Fhackers-behind-stuxnet) or [Register \(/connect/user/register?destination=blogs%2Fhackers-behind-stuxnet\)](/connect/user/register?destination=blogs%2Fhackers-behind-stuxnet) to post comments.**

## About Your Community

**A Message From Your Community Manager: [RGMDonaldson \(/connect/user/rgmdonaldson\)](/connect/user/rgmdonaldson)**



**[\(/connect/user/rgmdonaldson\)](/connect/user/rgmdonaldson)**

Welcome to the Security Community on Symantec Connect.

The Security Community covers many different security products from Symantec and provides valuable technical information for each.

Please feel free to contact me via private message with any questions you may have.

I look forward to hearing from you and answering any questions about the Community.

[Send a private message to the Community Manager \(/connect/messages/new/4100651?destination=user%2F4100651\)](/connect/messages/new/4100651?destination=user%2F4100651)




### Top 5 Contributors: All Time

MEMBER






REWARD POINTS

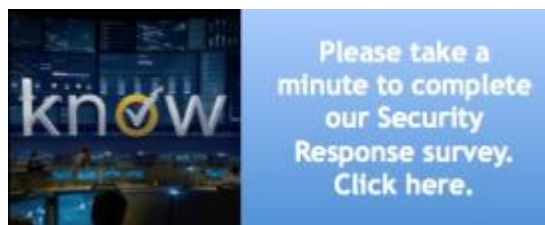
[Brian \(/connect/user/riai\)](/connect/user/riai) **147515**

4 of 5 [Vikram Kumar-SAV to SEP \(/connect/user/vikram-kumar-sav-sep\)](/connect/user/vikram-kumar-sav-sep) **77376**

 <a href="/connect/user/mithun-sanghavi">(/connect/user/mithun-sanghavi)</a> Mithun Sanghavi <a href="/connect/user/mithun-sanghavi">(/connect/user/mithun-sanghavi)</a>	<b>77018</b>
 <a href="/connect/user/rafeeq">(/connect/user/rafeeq)</a> Rafeeq <a href="/connect/user/rafeeq">(/connect/user/rafeeq)</a>	<b>68839</b>
 <a href="/connect/user/pk-1">(/connect/user/pk-1)</a> P K <a href="/connect/user/pk-1">(/connect/user/pk-1)</a>	<b>53536</b>

### Top 5 Contributors: Last 30 Days

MEMBER	REWARD POINTS
 <a href="/connect/user/aravind-ghosh">(/connect/user/aravind-ghosh)</a> Aravind Ghosh <a href="/connect/user/aravind-ghosh">(/connect/user/aravind-ghosh)</a>	<b>700</b>
 <a href="/connect/user/aboonaim-golandaz">(/connect/user/aboonaim-golandaz)</a> Aboonaim Golandaz <a href="/connect/user/aboonaim-golandaz">(/connect/user/aboonaim-golandaz)</a>	<b>650</b>
 <a href="/connect/user/tony-sutton">(/connect/user/tony-sutton)</a> Tony Sutton <a href="/connect/user/tony-sutton">(/connect/user/tony-sutton)</a>	<b>200</b>
 <a href="/connect/user/riai">(/connect/user/riai)</a> Brian <a href="/connect/user/riai">(/connect/user/riai)</a>	<b>200</b>
 <a href="/connect/user/aayan-p">(/connect/user/aayan-p)</a> Aayan P <a href="/connect/user/aayan-p">(/connect/user/aayan-p)</a>	<b>200</b>



<https://www.surveymonkey.com/r/G7KVZWQ>

[Contact Us \(/connect/contact\)](/connect/contact) [Privacy Policy \(http://www.symantec.com/about/profile/policies/privacy.jsp\)](http://www.symantec.com/about/profile/policies/privacy.jsp) [Earn Rewards \(/connect/points\)](/connect/points) [Rewards Terms and Conditions \(/connect/blogs/symantec-connect-rewards-program-terms-and-conditions\)](/connect/blogs/symantec-connect-rewards-program-terms-and-conditions)

© 2019 Symantec Corporation

[Twitter \(https://twitter.com/symantec\)](https://twitter.com/symantec) [Facebook \(https://www.facebook.com/Symantec\)](https://www.facebook.com/Symantec) [LinkedIn \(https://www.linkedin.com/company/symantec\)](https://www.linkedin.com/company/symantec)