

SANS Industrial Control Systems Security Blog

01 Jan 2016

Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered

[1 comments](#) Posted by [robertmlee](#)

Filed under [Security Awareness](#)

The SANS ICS team recently gained access to a sample of malware that came from the network of the [Ukrainian site](#) targeted in the cyber attack that led to a power outage. I want to offer a few caveats to this blog post up front.



- First, this is all developing and the next few days and weeks will add clarity to the situation.
- Second, with this type of analysis there's not much that can be definitively stated in terms of attribution or impact. Take everything here as informative only.
- Third, SANS ICS is not in the business of releasing highly detailed technical analysis of malware. The purpose of this blog is to focus on lessons learned and education for the community. Therefore, I am not going to be sharing the hash of the sample we have but instead talking about the takeaways. There are at least 3 major cybersecurity and threat intelligence vendors I am aware of that have the sample and will be releasing detailed analyses. I do not want us at SANS ICS to impede that by releasing the sample to the wider community right now. However, to any of the major players and researchers that want a sample feel free to reach out to us via the [SANS ICS Alumni email distribution](#) and we will provide it to verified sources.□

Here I'll detail the facts, speculation, and takeaways for the community.

The Facts

The SANS ICS team has been researching the cyber attack on the Ukrainian power grid since the event occurred with a mix of interest and a critical viewpoint. The interest was due to the seriousness of the event and the critical viewpoint was taken because while threats are active against ICS there are often otherwise good case-studies that get spun [out of control by the media](#). The idea of a cyber attack on infrastructure that leads to an impact to operations is very serious in nature and must be handled with care, especially when there is geopolitical tension in an area such as Ukraine.

Through trusted contacts in the community the SANS ICS team came across a lot of amplifying information about the attack, how it could have occurred, and the seriousness of this incident to the Ukrainian government and the focus they are putting on the investigation that increases the credibility of their reporting. The SANS ICS team was also passed a sample of malware from trusted sources taken from the impacted network by responders in country.

The hash for the malware can also be found on VirusTotal where a user in Ukraine submitted the sample on the 23rd of December. The timing and unique nature of the sample adds some credibility to the sources that collected and passed us the sample of the malware.

The malware is a 32 bit Windows executable and is modular in nature indicating that this is a module of a more complex piece of malware. I passed the malware sample to Kyle Wilhoit, a Senior Threat Researcher at Trend Micro who has done [great work](#) in the ICS community before, who confirmed through static analysis that the malware itself has a wiping routine that would impact the infected system. After that I passed the sample to Jake Williams, founder of Rendition Security and a fellow SANS Instructor, who has been [analyzing](#) this incident as

RSS

 Search

Categories

- [Courses](#) (2)
- [Defense Use Cases](#) (1)
- [ICS Survey](#) (2)
- [Instructors](#) (3)
- [Internet of Things](#) (2)
- [IT-OT Convergence](#) (3)
- [NERC CIP v5](#) (1)
- [Security Awareness](#) (7)
- [Summit](#) (1)
- [Uncategorized](#) (0)

Recent Posts

- [Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered](#)
- [Current Reporting on the Cyber Attack in Ukraine Resulting in Power Outage](#)
- [Takeaways from Reports on Iranian Activity Against the Power Grid and a Dam](#)
- [The Rise of the Things #2](#)
- [The Rise of The Things!](#)

Recent Comments

Popular Posts

Archives

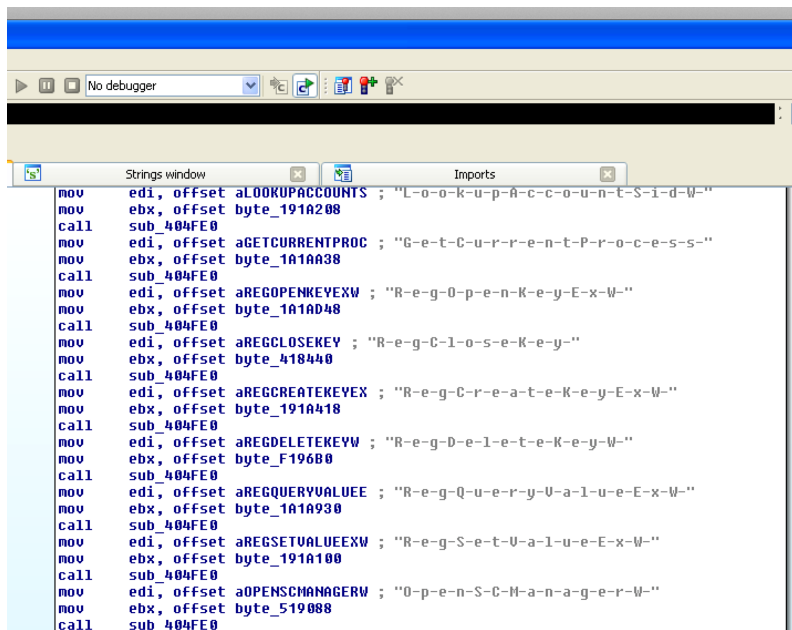
Select Month

Links

- [Log in](#)
- [Entries RSS](#)
- [Comments RSS](#)

well for further support. Below is his analysis:

Note that this analysis is based on an extremely limited static analysis of the malware and further analysis may impact these findings. The code appears modular in nature. The attackers take steps to obscure some notable suspicious APIs (e.g. OpenSCManager) from the imports table, but not others (e.g. CreateToolhelp32Snapshot). The string "obfuscation" method is crude and obvious upon manual examination, but effective to thwart string matching. Any of these hyphen separated strings would make an excellent Yara rule.



```
Strings window
Imports
mov edi, offset aLOOKUPACCOUNTS ; "L-o-o-k-u-p-a-c-c-o-u-n-t-s-i-d-w-"
mov ebx, offset byte_191A208
call sub_404FE0
mov edi, offset aGETCURRENTPROC ; "G-e-t-C-u-r-r-e-n-t-P-r-o-c-e-s-s-"
mov ebx, offset byte_1A1A38
call sub_404FE0
mov edi, offset aREGOPENKEYEXW ; "R-e-g-o-p-e-n-K-e-y-E-x-W-"
mov ebx, offset byte_1A1A48
call sub_404FE0
mov edi, offset aREGCLOSEKEY ; "R-e-g-C-l-o-s-e-K-e-y-"
mov ebx, offset byte_418440
call sub_404FE0
mov edi, offset aREGCREATEKEYEX ; "R-e-g-C-r-e-a-t-e-K-e-y-E-x-W-"
mov ebx, offset byte_191A418
call sub_404FE0
mov edi, offset aREGDELETEKEYW ; "R-e-g-D-e-l-e-t-e-K-e-y-W-"
mov ebx, offset byte_F196B0
call sub_404FE0
mov edi, offset aREGQUERYVALUEE ; "R-e-g-Q-u-e-r-y-U-a-l-u-e-E-x-W-"
mov ebx, offset byte_1A1A930
call sub_404FE0
mov edi, offset aREGSETVALUEEXW ; "R-e-g-S-e-t-U-a-l-u-e-E-x-W-"
mov ebx, offset byte_191A100
call sub_404FE0
mov edi, offset aOPENSCMANAGERW ; "O-p-e-n-S-C-H-a-n-a-g-e-r-W-"
mov ebx, offset byte_519088
call sub_404FE0
```

Notably, the malware does not appear to use all of the functions it imports. Specifically, there are no cross references to service related calls. While this may be due to dynamic call targets, there are significant numbers of cross references to other dynamically resolved APIs (e.g. RegDeleteKey).

The resolution of APIs that are not used elsewhere in the code probably means that some of the code was borrowed from another program. This hints at a development shop with a code base from which to piece modules together. Although the string obfuscation was crude, it was sufficient for the task. The crude string obfuscation should not be taken as an indication that the attacks came from a non-state actor.

Another possible interesting note is the compile timestamp of the executable. It is set to January 6, 1999.

TimeStamp	0x3693DD58 (Wed Jan 06 17:02:00 1999)
-----------	---------------------------------------

This was likely modified by the attackers, but whether this date is significant in historical context is unknown at this time. It may simply be a random modification.

There are at least 3 major cybersecurity vendors working on the piece of malware right now in their own analysis and I will simply state that I'm impressed with the quality of work from them I have seen so far. Additionally, folks at the ICS-CERT and E-ISAC are doing great analysis as well and will likely be pushing out information through government sharing channels soon. Simply put, a lot will be known about this in the community soon to further support the analysis or help move on to a better understanding.

The Speculation

It is not currently possible right now to state that the malware recovered caused the loss of power in Ukraine. Additionally, the wiping functionality of the module recovered is likely for the purposes of cleanup after the attack; it itself does not appear to have been capable of causing the outage. This is important to note as the wiping capability is not similar in nature to the Shamoon attack but instead an anti-forensics technique.

Also, it is possible that the incident caused responders to look at the network where they found the malware. The

malware could be new and yet not be related to the incident. At this time I believe the malware is related to the incident though from analysis by the SANS ICS team and others around the community but this should be categorized as a low-confidence assessment currently.□

There has also been speculation that the malware is related to, and potentially a module for, BlackEnergy2. The previous statement should not be taken as a standalone soundbite. There is very little to support this conclusion right now. If true though this would add credibility to Ukraine's SBU who [reported](#) that the malware was launched by Russian security services. Because of the sources concluding the BlackEnergy2 connection I feel it is important to share the (potentially overstated) speculation with the community as there were many organizations around the global community who were impacted by that campaign. Just because a campaign is reported on publicly does not mean it is no longer active. Security personnel in ICS organizations should be actively looking for threats — the Ukrainian incident should not be seen as an incident that only impacts one site in a foreign country although no panic or alarm should be taken, only due diligence towards defense.

The Takeaways

- There is a lot of great analysis going on in the community by a number of companies, government organizations, and individual researchers. Each have been contributing some unique aspects to the analysis. Defenders must always work together like this and build off of each other's strengths. Information sharing in this manner is critical to security.
- The Ukrainian power outage is more likely to have been caused by a cyber attack than previously thought. Early reporting was not conclusive but a sample of malware taken from the network bolsters the claims. The unique nature of the malware indicate some level of targeting may be possible but much more information is needed to confirm that targeting of ICS or this specific facility was intended.□
 - If the malware does end up being related to the BlackEnergy2 campaign then this adds to the possibility that the facility and ICS was specifically targeted□
 - Technical data alone is very rarely enough to conclude the intention of an adversary
- ICS facilities around the world need to take an [active defense](#) approach to monitoring ICS networks and responding to threats. Additionally, each should have an ability, or at least contacts to request help from, to perform basic threat and malware analysis to know when to reach out for help to the larger community (my one plug: the identification of, response to, and analysis of threats is the type of skill set we teach in SANS□ [ICS515](#) and I would encourage organizations to find this or similar type of training for security personnel□ onsite. Firewalls and boxes on the network alone will not protect an ICS fully).

This incident is an important case-study for the ICS community. If the analysis and follow on information is validated about the malware and attack then this will also be a significant event for the international community.□ The precedence that this event sets is far reaching past the security community and will need to be analyzed and understood fully. The response by countries to this type of attack and any attribution obtained will also be significant in establishing the precedence of these types of events moving forward in the international community.□

Lastly, Michael Assante, SANS ICS Director, and I will be discussing these and other takeaways from this event and other recently reported case-studies in an upcoming webcast on Jan 5th. We will update everyone with anything we find out between now and then during the webcast, free to [join us](#).

Bio: Robert M. Lee is the course author of ICS515 - Active Defense and Incident Response and the co-author of FOR578 - Cyber Threat Intelligence. He is also the Founder, CEO of Dragos Security and gained his start in cyber security in the U.S. Intelligence Community as a Cyber Warfare Operations officer. He may be found on□ Twitter [@RobertMLee](#)



[Permalink](#) | [Comments](#) | [RSS Feed](#) - [Post a comment](#) | [Trackback URL](#)

1 Comments

Posted January 04, 2016 at 6:48 AM | [Permalink](#) | [Reply](#)

Vytautas

Wish it was possible to cross reference and compare this event with what happened at German steel mill in 2014. Perhaps some data about what was reported by the German government last year will come forth?

Post a Comment

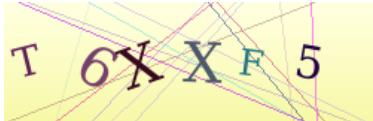
*Name

*Email

Website

*Comment

Captcha



*Response

Post Comment

* Indicates a required field.□

Latest Tweets @SANSICS

[New from #SANSICS: DUC #4 "Analysis of the Recent Reports of \[...\]](#)

January 5, 2016 - 8:16 PM

[The webcast on the reports on Iranian activity and the Ukrai \[...\]](#)

January 5, 2016 - 7:14 PM

[Thank you for everyone who joined the webcast dissecting the \[...\]](#)

January 5, 2016 - 7:13 PM

Latest Papers

[Burp Suite\(up\) with fancy scanning mechanisms](#)

By Zoltan Panczel

[Applying Data Analytics on Vulnerability Data](#)

By Yogesh Dhinwa

[Web Application File Upload Vulnerabilities](#)

By Matthew Koch

"The depth of knowledge I'm taking away from the SCADA conference would have taken two or three other training conferences offered from other providers."

- Tony Risinger, Westar Energy

"The SCADA Summit series provide a valuable combination of discussion on real world challenges and suggestions on how to resolve them."

- John Mathias, Owens Corning

"This was a great opportunity to gain knowledge on securing a control system from external threats"

- Danny Carlsen, MacAulay-Brown



[Resources](#) | [Courses](#) | [Events](#) | [Certification](#) | [Instructors](#) | [About](#)

© 2011 - 2016 SANS™ Institute