Threat Research

Sandworm Team and the Ukrainian Power Authority Attacks

January 08, 2016 | by John Hultquist

UKRAINE CYBER TARGETING | SANDWORM TEAM | DISRUPTIVE MALWARE

Update 1.11.16 - SANS ICS Team Connects Dots

Updating the blog entry to bring attention to the recent analysis published by Mike Assante from the SANS ICS team.

"After analyzing the information that has been made available by affected power companies, researchers, and the media it is clear that cyber attacks were directly responsible for power outages in Ukraine. The SANS ICS team has been coordinating ongoing discussions and providing analysis across multiple international community members and companies. We assess with high confidence based on company statements, media reports, and first-hand analysis that the incident was due to a coordinated intentional attack."

Read the full SANS post here - and see below for iSIGHT

iSIGHT Partners Analyst Comment

The SANS ICS blog confirms conclusions previously reached by iSIGHT regarding the nature of the Ukrainian attacks (specifically the role of destructive malware and phone disruption) and attribution to Sandworm Team. iSIGHT Partners believes this incident is a milestone because it is the first major cyber attack to substantially affect the civilian population and because of the overwhelming importance of the grid to multiple reliant sectors. Furthermore, Sandworm Team's previous interest in US and European critical systems underscores the threat they pose (see below for more on Sandworm Team.)

Sandworm Team - Historical Targeting of Ukraine and Interest in SCADA Systems

Since last week, iSIGHT Partners has worked to provide details on the power outage in Ukraine to our global customers. We have analyzed the forensic evidence we have been able to obtain from the region, contextualizing it within our knowledge of cyber espionage actors. Many details of the event remain unknown, and given the nature of the incident, especially the use of destructive malware, we do not anticipate every detail will be exposed.

However, we have linked Sandworm Team to the incident, principally based on BlackEnergy 3, the malware that has become their calling card.

iSiGHT Partners has tracked Sandworm Team for some time - and we publicly reported on some of their activities in October 2014, when we discovered their use of a zero-day exploit, CVE-2014-4114. In that campaign, we saw targeting of Ukrainian government officials, members of the EU and NATO. Shortly after releasing information on their espionage operations, our friends at TrendMicro found evidence that the operators were not only conducting classic strategic espionage but targeting SCADA systems as well. Evidence of this accumulated, and iSIGHT Partners released a follow-up blog were we assessed that activity was reconnaissance for attack - a preparation for cyber attack to be carried out in the long term. ICS-CERT released a separate advisory as well.

Sandworm Team Activity - Late 2014 to Current Day

Sandworm Team went to ground shortly after being exposed in October of 2014, and malware with Dune references (the genesis for the 'Sandworm' moniker) which we had previously used to track them disappeared entirely. However, the unique malware variant, BlackEnergy 3, reemerged in Ukraine early in 2015, where we had first found Sandworm Team. Throughout 2015 we saw increased intrusion activity using BlackEnergy 3. We warned our clients of new features suggesting an increased focus on European targets - though verification of targets was not possible at the time. Additionally, we warned our customers about the targeting of both media and regional power authorities in the Ukraine, sectors later affected by cyber attacks. Some of this information was recently shared by the folks at ESET, who have also been following Sandworm Team very closely for quite some time.

On the Ukrainian Power Authority Incidents

Last week iSIGHT's sources provided us with the same KillDisk malware published by Rob Lee of SANS and Dragos Security. As ESET has, we place this malware within the greater context of activity tied to BlackEnergy 3, which we believe is Sandworm Team. We believe this KillDisk malware is related to the destructive malware leveraged during Ukrainian elections in October. At the time, CERT-UA connected that incident to BlackEnergy 3. Symantec has since verified those claims. Furthermore, iSIGHT's own sources indicate that BlackEnergy 3 malware was deployed on at least one of the Ukrainian power systems affected by KillDisk.

iSIGHT Partners is still collecting information on the mechanics of the power outage and what role the KillDisk malware played in the greater event. We cannot confirm that the KillDisk malware caused the outage. It may have been used following steps to manipulate power in order to impede restoration efforts or operator visibility. It is noteworthy that technical support numbers associated with the power authorities were allegedly flooded with calls, which may have been an effort to further overwhelm responders. On their official website, the Ukrainian security service, SBU, made this claim.

Outlook

A cyber attack of this nature is a milestone -although a predictable one. The aggressive nature of Sandworm Team's previous activity in Europe and the United States exposed their interest in targeting critical systems and indicated preparation for cyber attack. Targeting of critical entities in Ukraine throughout 2015, during a time of war, further presaged a desire to disrupt infrastructure.

PREVIOUS POST NEXT POST

Recent Posts

17 Mar 2020
Six Facts about Address Space Layout Randomization on Windows >

16 Mar 2020
They Come in the Night: Ransomware Deployment Trends >

09 Mar 2020
Crescendo: Real Time Event Viewer for macOS >

RSS FEED: STAY CONNECTED