Modern Malware Demands Modern Defense

Robert M. Lee & Tim Conway

ICS.SANS.ORG
Learning
Defending
Leading
Automation of Cyber-physical Systems and the Internet of Things

2011

SEP 2011

DEC 2011

2012

MAY 2012

SEP 2012

JUN 2014

Duqu malware discovered

APT attacks on gas pipeline sector

Houston water system compromise

Flame malware discovered

Telvent intrusion, company warns ICS customers (ICS supplier)

Havex Trojan is discovered in ICS-focused water-holing attacks – observed capability to locate OPC servers and attempts to exfiltrate collected data
Defending
<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICS Opportunistic (General Purpose)</td>
<td>Conficker, PETYA, ENLPROX</td>
</tr>
<tr>
<td>ICS Themed (Delivery Techniques)</td>
<td>Dragonfly 2.0</td>
</tr>
<tr>
<td>ICS Tailored-Access (Exploits &amp; Modules)</td>
<td>BlackEnergy2, Havex Dragonfly 1.0</td>
</tr>
<tr>
<td>ICS Tailored-Effects (Payloads/Manipulation)</td>
<td>STUXNET, CRASHOVERRIDE</td>
</tr>
</tbody>
</table>
Major Public ICS Incidents & Access Campaigns

**High**
- ICS Payload
- ICS Exploits
- ICS Delivery
- ICS Targeting
- ICS Recon

**Low**
- ICS IMPACTS
- (Nuisance)
- (Lost Productivity/Data)
- (Lost Value)
- (Loss of Safety, Reliability, Assets)

**ICS IMPACTS**
- Critical Infrastructure Data Exfiltration
- NY Dam Intrusion
- BlackEnergy 2 (various ICS modules)
- Havex (OPC module)

**Stage One**
- Dec 2016 Ukraine Power Outage
- BE3
- Unspecified German Facility

**Stage Two**
- Stuxnet (all versions)
- TRISIS
- Dec 2015 Ukraine Power Outage
- NY Dam Intrusion
ICS Attacks

225k
Ukraine 2015
Three electric utilities attacked through a cyber means resulting in 225k customers out of power

200 MW
Ukraine 2016
Electric transmission substation attacked through a cyber means

SIS
Middle East Facility 2017
Safety Instrumented System, targeted and impacted

Combination
Safety or protection system manipulation followed by intentional control system misuse to cause equipment damage and human health and safety impact
LITTLE BOBBY

I need you to ensure no attacks occur.

Okay--what's the security budget?

OH, WE HAD TO CUT IT ALL.

I assure you we will never see any attacks.

Defending   Learning   Leading
ics-community.sans.org

Join the Community that is defending our Critical Infrastructure