# XII STIC CCN-CERT CONFERENCES

Cybersecurity,
towards effective response and deterrence

TRITON: Autopsia de un caso real de seguridad de control industrial

ccn-cert
centro criptológico nacional

ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN

David GROUT
CTO EMEA & Director PreSales South EMEA

FireEye

David.grout@fireeye.com

Index

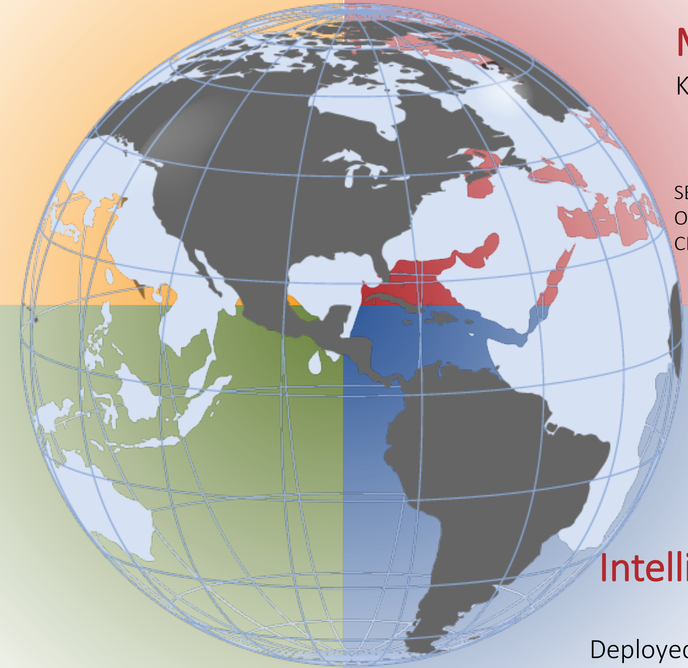
1. How are we collecting information

2. ICS / SCADA – The Race to the Botton

3. Triton Case :

   A. Approach
   B. Technical differences
   C. Attribution
   D. Outcomes

How are we collecting information ?



Sensors Telemetry

Global awareness of campaigns

4,400+
CUSTOMERS

250+
OF THE FORTUNE 500

Managed Services

Know active events for managed defense

6
SECURITY OPERATIONS CENTERS

200+
CLIENTS

Incident Response

Understand the most devastating attacks

1,200+
CUSTOMERS

200+
OF THE FORTUNE 500

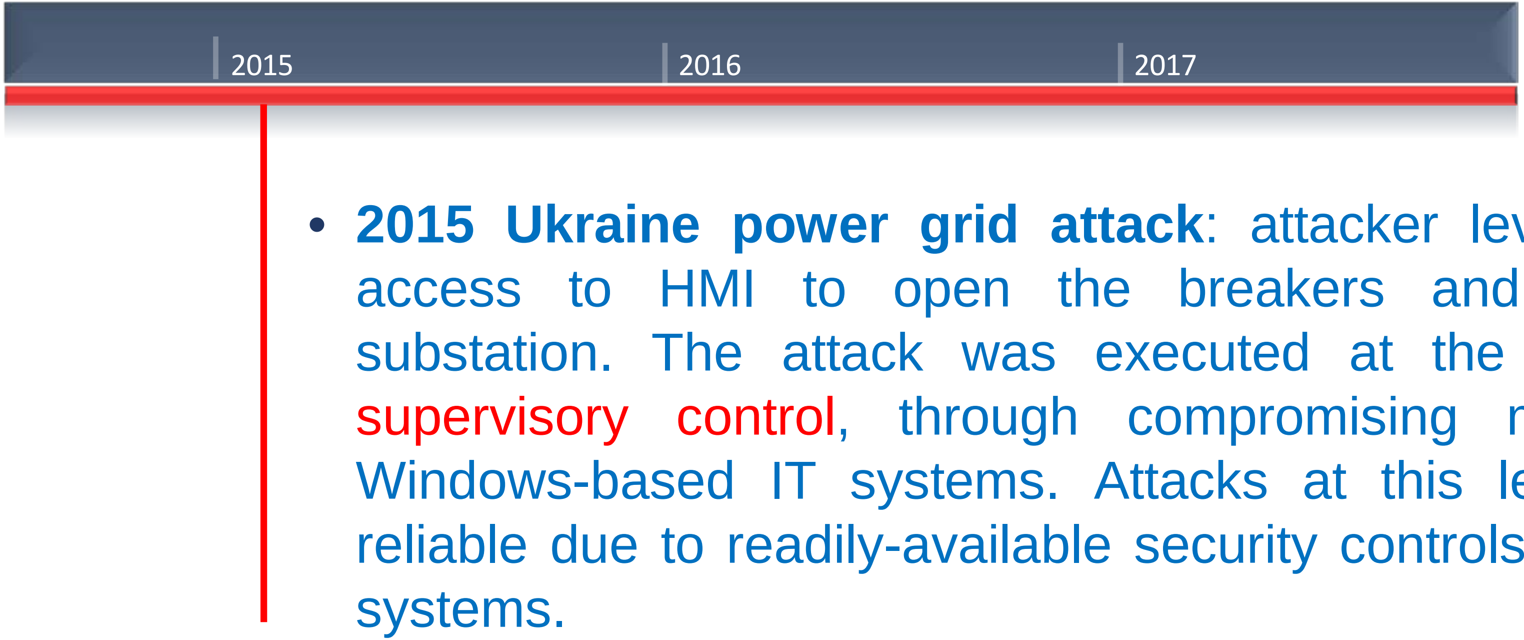
Intelligence Analysis

Deployed global researchers with local knowledge

18
COUNTRIES

100+
ANALYSTS AND RESEARCHERS

The race to the bottom



2015

2016

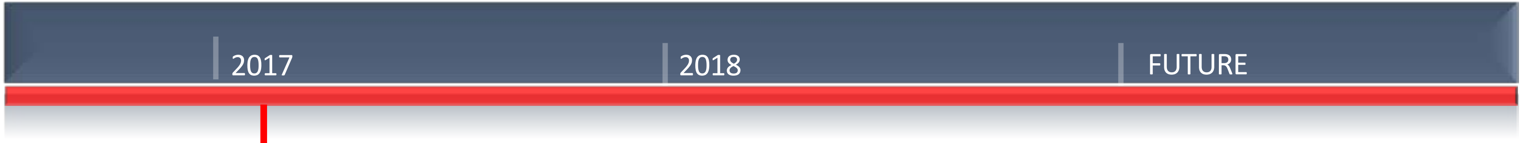
2017

- **2015 Ukraine power grid attack**: attacker leveraged VNC access to HMI to open the breakers and de-energize substation. The attack was executed at the level of the supervisory control, through compromising more familiar Windows-based IT systems. Attacks at this level are less reliable due to readily-available security controls for Windows systems.

The race to the bottom

- **2016 Ukraine power grid**: attacker achieved the same goal at the industrial protocol layer. Very few industrial organizations have visibility into their control network traffic. However, this is slowly changing as more utilities recognize the value and necessity for control traffic monitoring for both improving operational efficiency and security.

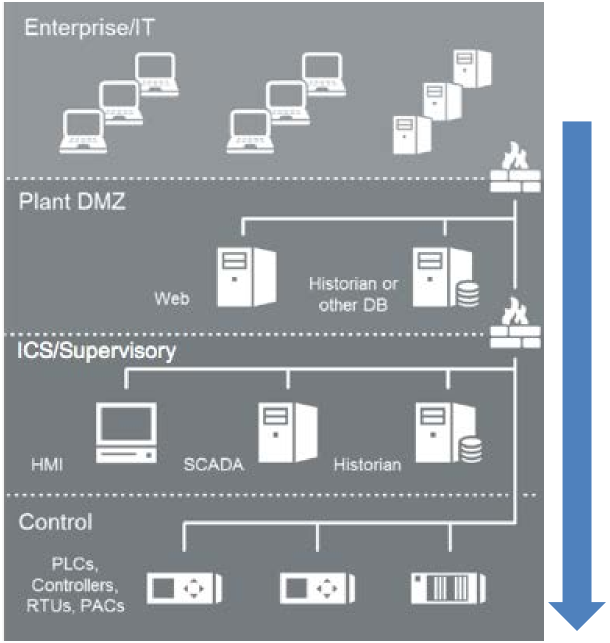
The race to the bottom



- **2017 TRITON**: Attacker moved their exploit all the way into the control equipment, to the regulatory control level. Exploits at this level are unchallenged by defenders because embedded systems typically lack any on-device security protections and there are currently no commercial solutions to detect compromised systems.

The race to the bottom

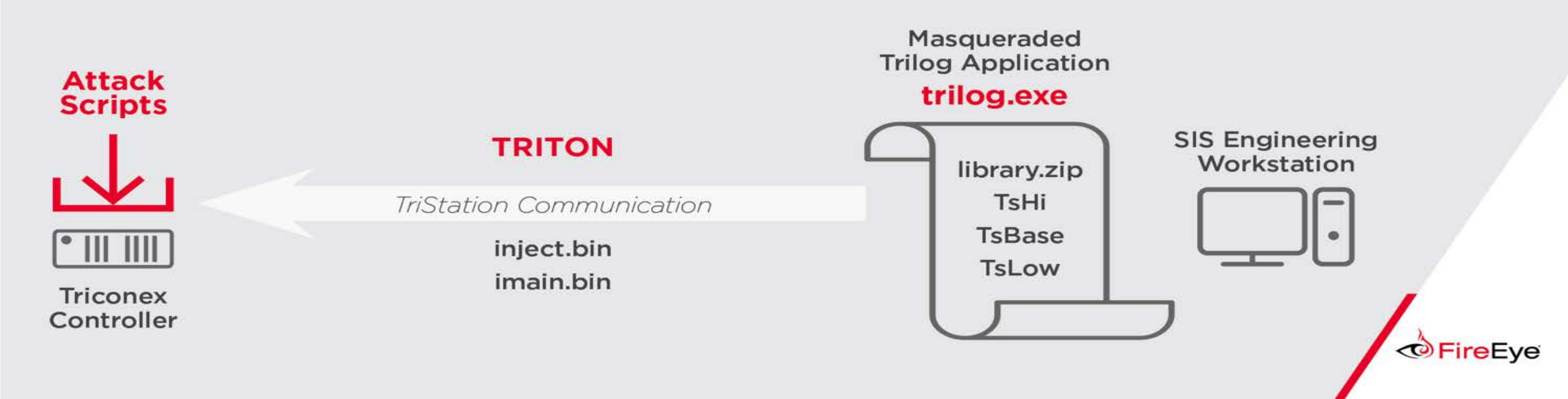
- This trend refers to the tendency of attackers to move **their exploits one layer down as soon as security controls are introduced at some layer** of computer architecture abstraction.
- While a small fraction of asset owners are slowly embracing ICS network monitoring solutions, the attackers are already moving their exploits one layer lower **– into the control equipment, where there are no defenses**.



The Purdue Model

Triton The Approach

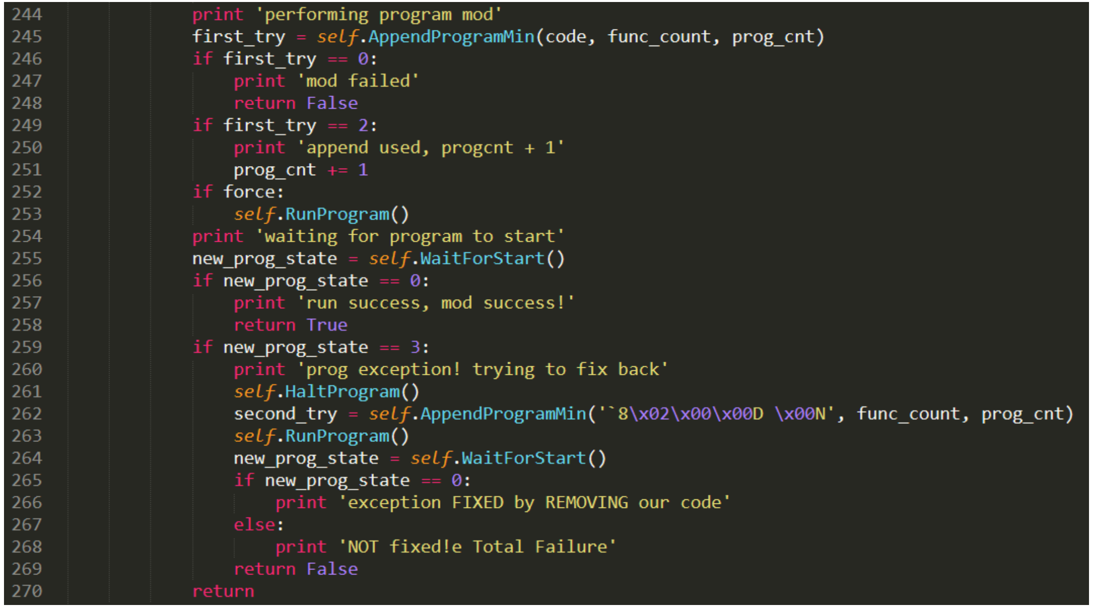
- In 2017, Mandiant responded to an incident at a critical infrastructure organization where threat actors deployed an attack framework, which we call TRITON, designed to manipulate Industrial Safety System
- We assess with moderate confidence that the attackers' final goal was to use their control over the SIS to allow them to cause an incident with physical consequence.
- Another possibility is that this intrusion was training or a proof of concept (POC) exercise.



Technical differences – Attackers were advanced

FRAMEWORK APPROACH – Part1 Modular Model

- TRITON includes extensive debugging messaging in its code that informs users about code execution results, it confirms a targeted & professional approach

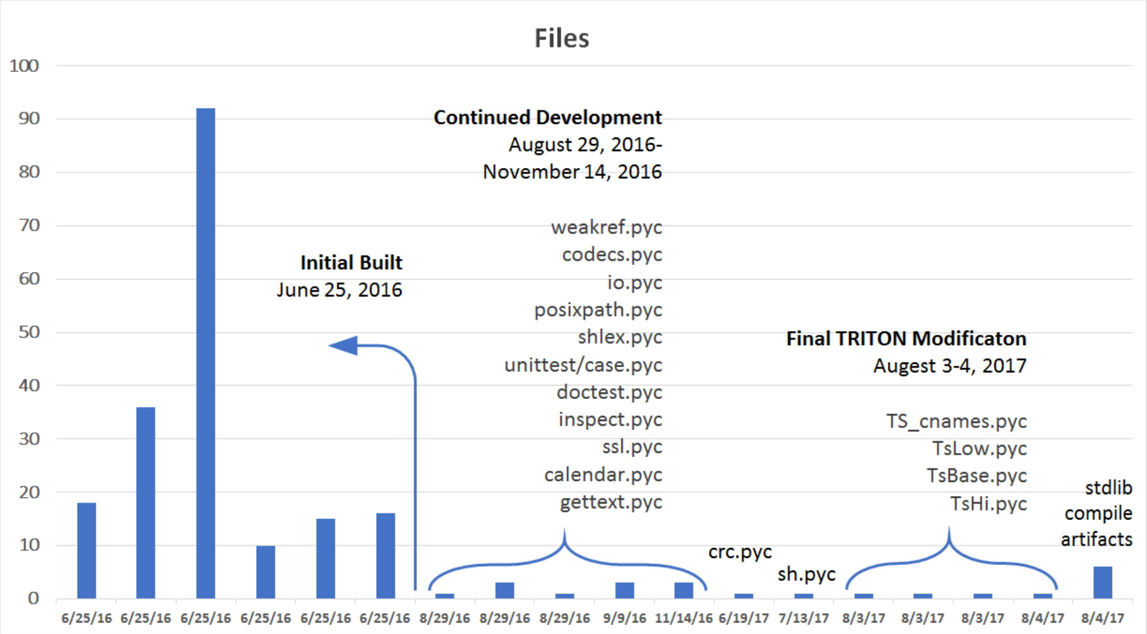


```
        print 'performing program mod'
        first_try = self.AppendProgramMin(code, func_count, prog_cnt)
        if first_try == 0:
            print 'mod failed'
            return False
        if first_try == 2:
            print 'append used, progcnt + 1'
            prog_cnt += 1
        if force:
            self.RunProgram()
        print 'waiting for program to start'
        new_prog_state = self.WaitForStart()
        if new_prog_state == 0:
            print 'run success, mod success!'
            return True
        if new_prog_state == 3:
            print 'prog exception! trying to fix back'
            self.HaltProgram()
            second_try = self.AppendProgramMin('`8\x02\x00\x00D \x00N', func_count, prog_cnt)
            self.RunProgram()
            new_prog_state = self.WaitForStart()
            if new_prog_state == 0:
                print 'exception FIXED by REMOVING our code'
            else:
                print 'NOT fixed!e Total Failure'
            return False
        return
```

Technical differences – Attackers were advanced

FRAMEWORK APPROACH – Part2 Debugging

- TRITON is designed with an easily understood modular architecture with descriptive function names
- The compilation times of the python codes of library.zip suggest the development of the framework started as early as June 25, 2016



Initial Built
June 25, 2016

Continued Development
August 29, 2016-
November 14, 2016

weakref.pyc
codecs.pyc
io.pyc
posixpath.pyc
shlex.pyc
unittest/case.pyc
doctest.pyc
inspect.pyc
ssl.pyc
calendar.pyc
gettext.pyc

crc.pyc

sh.pyc

Final TRITON Modificaton
Augest 3-4, 2017

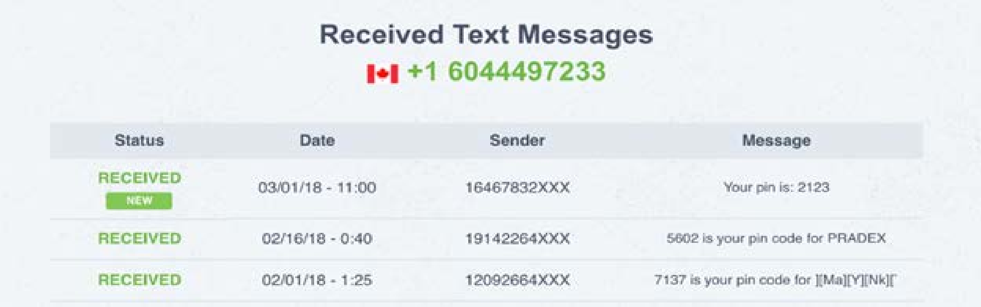
TS_cnames.pyc
TsLow.pyc
TsBase.pyc
TsHi.pyc

stdlib
compile
artifacts

Technical differences – Attackers were advanced

FRAMEWORK APPROACH – Part3 A set of customs tools

- The TRITON attacker used dozens of custom-built and modified off-the-shelf tools while active in the target environment
  - Persistence over scheduled tasks → CryptCat and Plink reverse shell backdoors
  - Port knocking mechanism → for backdoors
  - Mirroring knows malware tools→ SecHack ←→ Mimikatz
  - Use of public SMS utility to bypass OTP for OT VPN



Received Text Messages

+1 6044497233

Status	Date	Sender	Message
RECEIVED NEW	03/01/18 - 11:00	16467832XXX	Your pin is: 2123
RECEIVED	02/16/18 - 0:40	19142264XXX	5602 is your pin code for PRADEX
RECEIVED	02/01/18 - 1:25	12092664XXX	7137 is your pin code for][Ma][Y][Nk][

Outcomes

Why did they failed ?

- We assess with moderate confidence that the attackers' inability to successfully inject the backdoor was due to having access to a single main processor test controller.
- The controller used with a Triple Main Processor and an error during the application code checks between processors results in a safe shutdown.

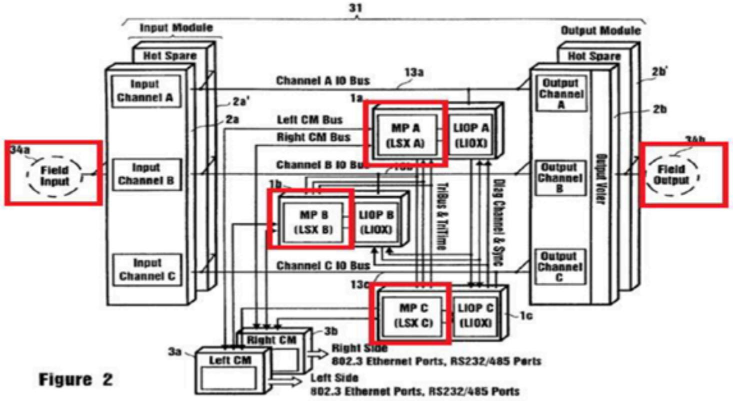


Figure 2

Overall Block diagram of the system -> triple redundant controller (from the patent)

Attribution

Assessment

- The team who developed TRITON had access for sure to the material to test their customs tools and fine tuned their functions.
- The lack of prior reconnaissance on the target controller confirmed that attackers had access to similar material in a lab.
- TRITON was designed to avoid detection and deter forensic examination with specific custom build able to remove traces
- At least part of the group has been operating since at least 2014
  - We discovered VT samples uploaded in 2014 for cyrptcat.exe, Several tools have been compiled in 2014 – Netcat Backdoor , napupdatedb.exe, a PLINK-based backdoor, was scheduled to run daily from April 28, 2014, at 14:21:36 UTC, 15:21:36 UTC and 17:21:36 UTC.

Attribution

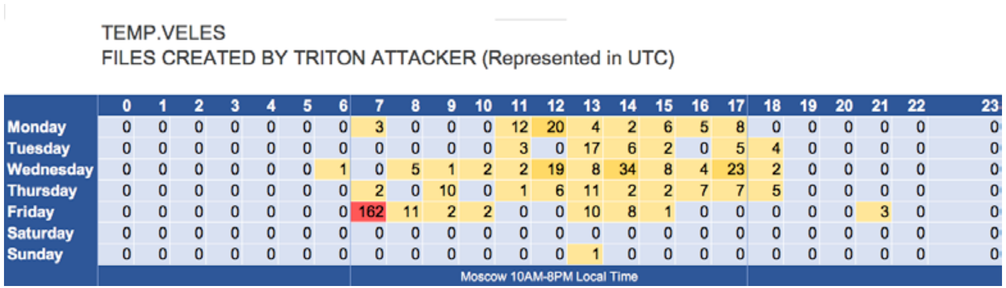
Technical Artefact

- Metadata associated with tested files indicates the user(s) have consistently come from **Russian IP space.**
- Multiple files **have Cyrillic names** and content.
- A PDB path contained in a tested file revealed a string that appears to be a unique handle or user name. This moniker can be linked to a **Russia-based person** active in Russian information security communities since at least 2011.
- We recovered CATRUNNER binaries used in TEMP.Veles activity that were compiled on Aug. 12, 2014. Historical records made available by SourceForge indicate an unknown **Russian IP address** downloaded this source code on Aug. 11, 2014, and Aug. 12, 2014.
- Throughout multiple investigations, FireEye iSIGHT Intelligence has observed a distinct IP address that further **ties TEMP.Veles activity to CNIIHM**

Attribution

Conclusion

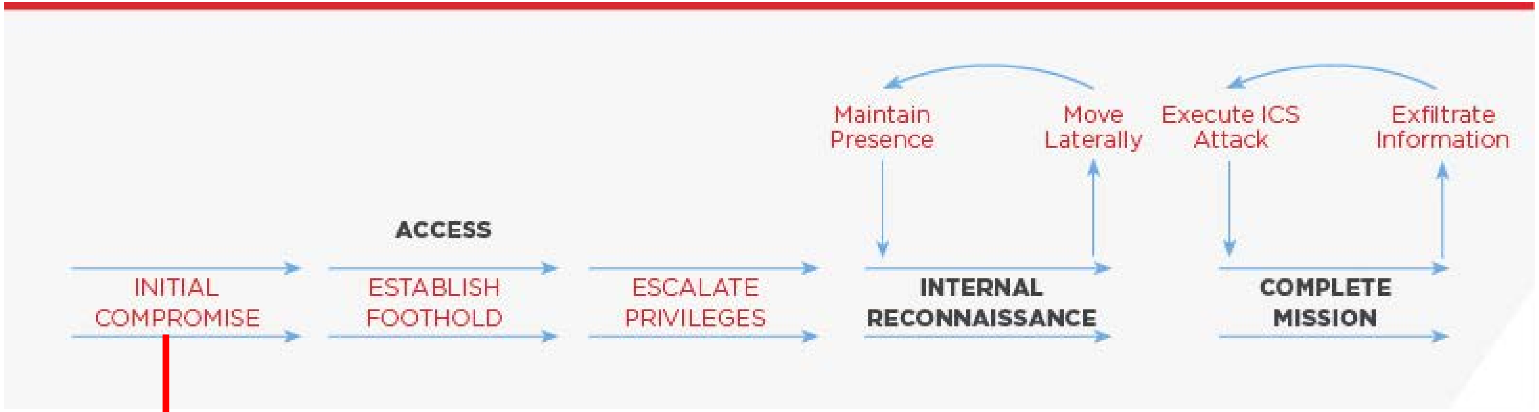
- We assesse with high confidence that intrusion activity that led to TRITON use was supported by the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM aka TsNIIKhM, TsNII), a Russian Government-owned technical research institution in Moscow.



TEMP.VELES
FILES CREATED BY TRITON ATTACKER (Represented in UTC)

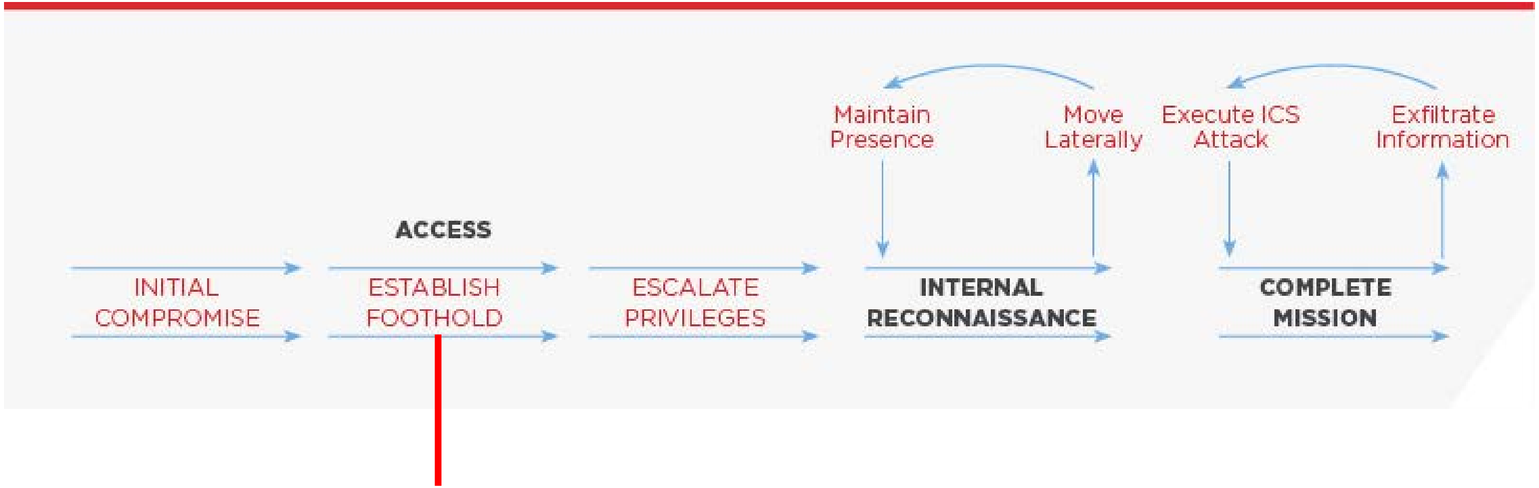
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Monday	0	0	0	0	0	0	0	3	0	0	0	12	20	4	2	6	5	8	0	0	0	0	0	0
Tuesday	0	0	0	0	0	0	0	0	0	0	0	3	0	17	6	2	0	5	4	0	0	0	0	0
Wednesday	0	0	0	0	0	0	1	0	5	1	2	2	19	8	34	8	4	23	2	0	0	0	0	0
Thursday	0	0	0	0	0	0	0	2	0	10	0	1	6	11	2	2	7	7	5	0	0	0	0	0
Friday	0	0	0	0	0	0	0	162	11	2	2	0	0	10	8	1	0	0	0	0	0	3	0	0
Saturday	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sunday	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
								Moscow 10AM-8PM Local Time																

Remediation



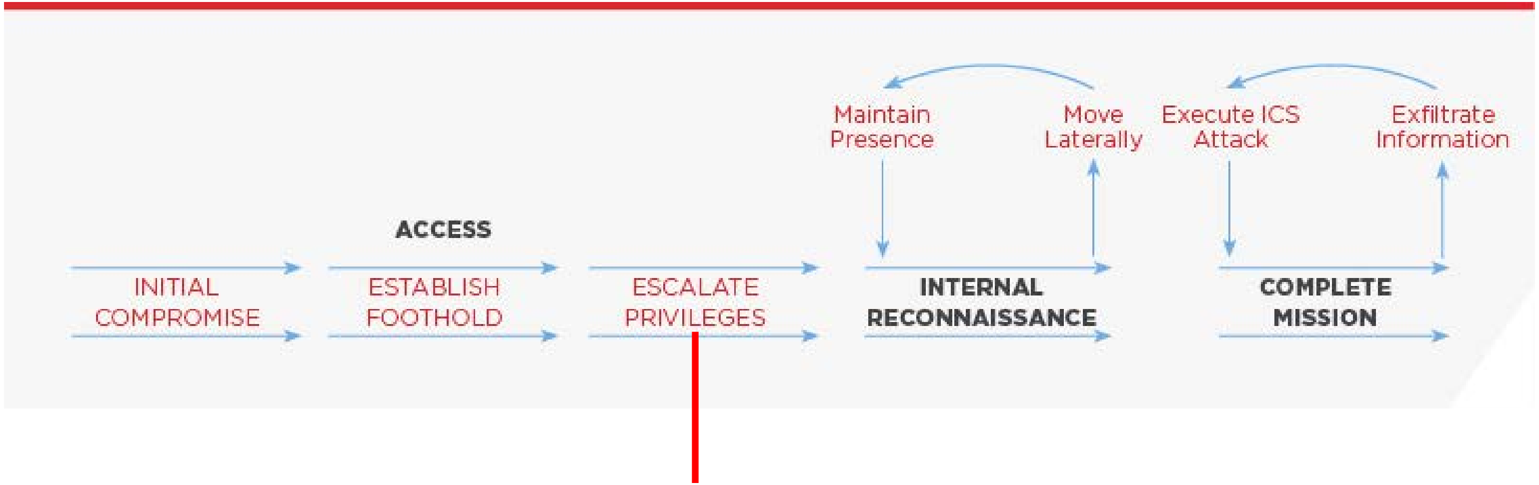
- **TTPS**: Spear-phishing, waterholes, leverage vulnerabilities
- **Mitigations:** Email Sandboxes, Security Awareness Program, Best Practices in vulnerability management and updates.

Remediation



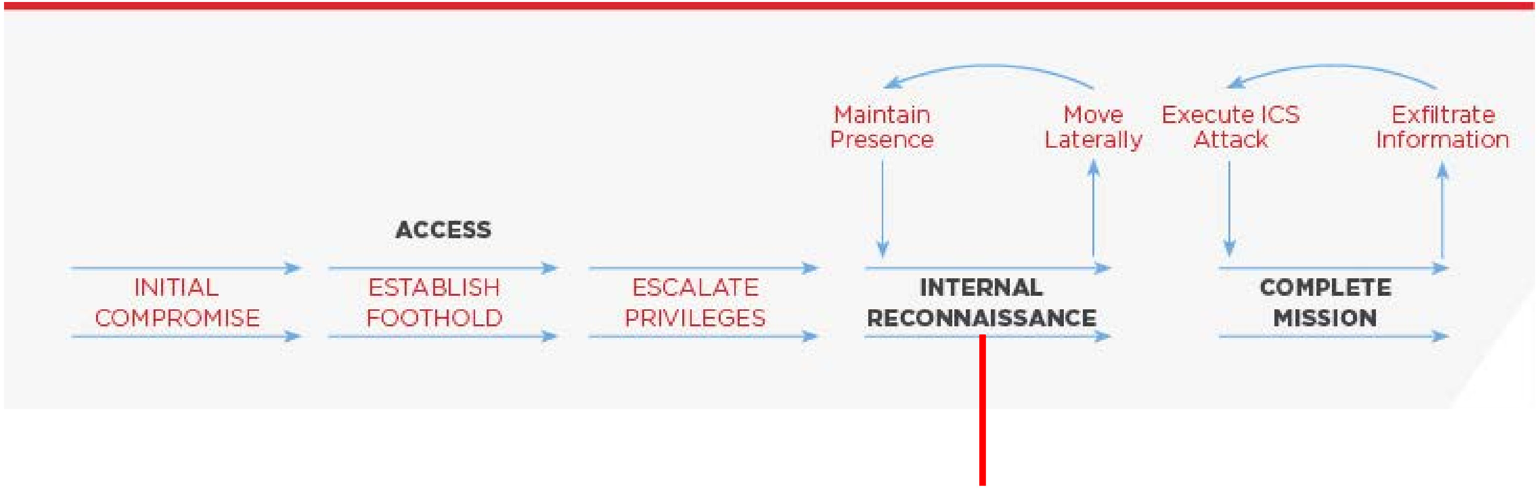
- **TTPS**: Backdoors installation to enable outbound connection
- **Mitigations:** IPS/IDS to focus on network behavior analysis, harden application and traffic authorization, network VISIBILITY, Host based Agent for system persistence detection, Enable powershell Login.

Remediation



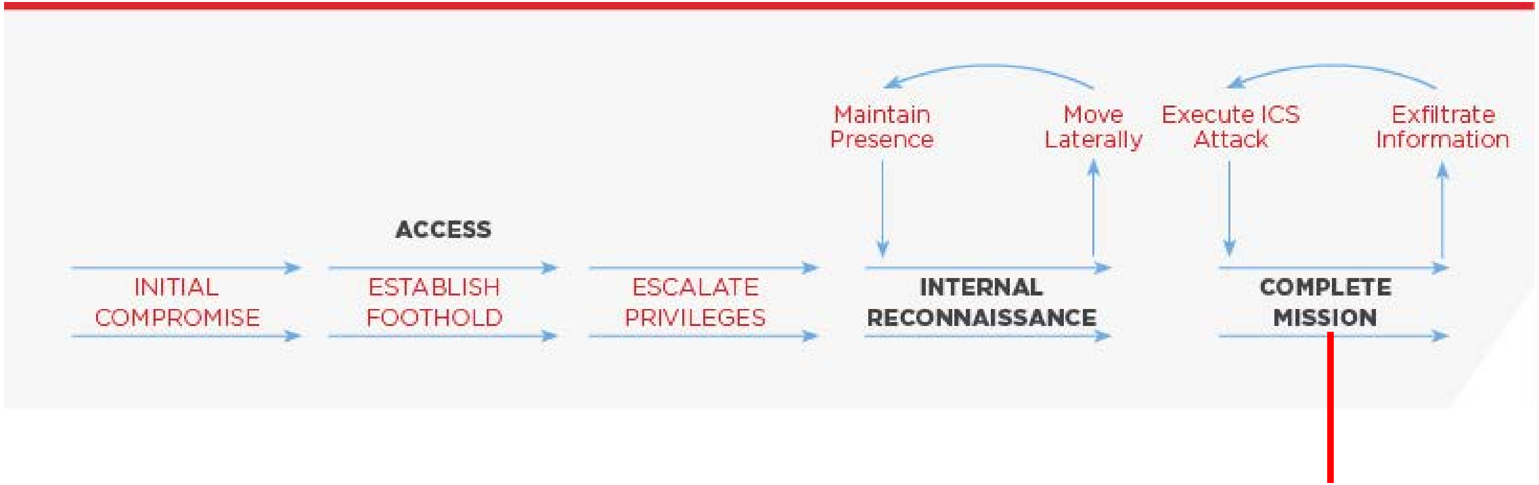
- **TTPS**: Credential harvesting for execution of remote commands
- **Mitigations:** Analyze host and network behaviors such as data exfiltration and introduction of attacker tools.

Remediation



- **TTPS**: Use compromise VPN account, remote connection to backdoors
- **Mitigations:** Manage user right access as needed, do not store ICS credential in IT network, multi factor authentication, deactivate unnecessary ports, whitelisting and access control on DCS and SIS.

Remediation



- **TTPS**: Lateral movement from OT DMZ to the DCS network to implant malware on SIS engineering station
- **Mitigations:** Network segregation, No dual homed computer, use unidirectional gateways or data diodes, Monitor TriStation network traffic – VISIBILITY, use physically locks.

References and documentation

Some documents are accessible through specific subscription

- https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
- https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html
- https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html
- https://intelligence.fireeye.com/reports/18-00016550
- https://intelligence.fireeye.com/reports/18-00012760

# XII STIC CCN-CERT CONFERENCES

Cybersecurity,
towards effective response and deterrence

- **Email**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es

  Websites
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Folow us on**

ccn-cert
centro criptológico nacional