Denial, anger, bargaining, depression and acceptance: reporting 0-days to Russian vendors

Vladimir Dashchenko
Kaspersky Lab ICS CERT

Hello world

Kaspersky Lab ICS CERT team member

ICS Security researcher

1. Intro
2. What's happening with 0days?
3. Case studies + Denial, anger, bargaining, depression and acceptance (DABDA) stages for RU and Non-RU
4. Why so?
5. Outro

INTRO

Conditions:

1. No IT giants (classical software guys)

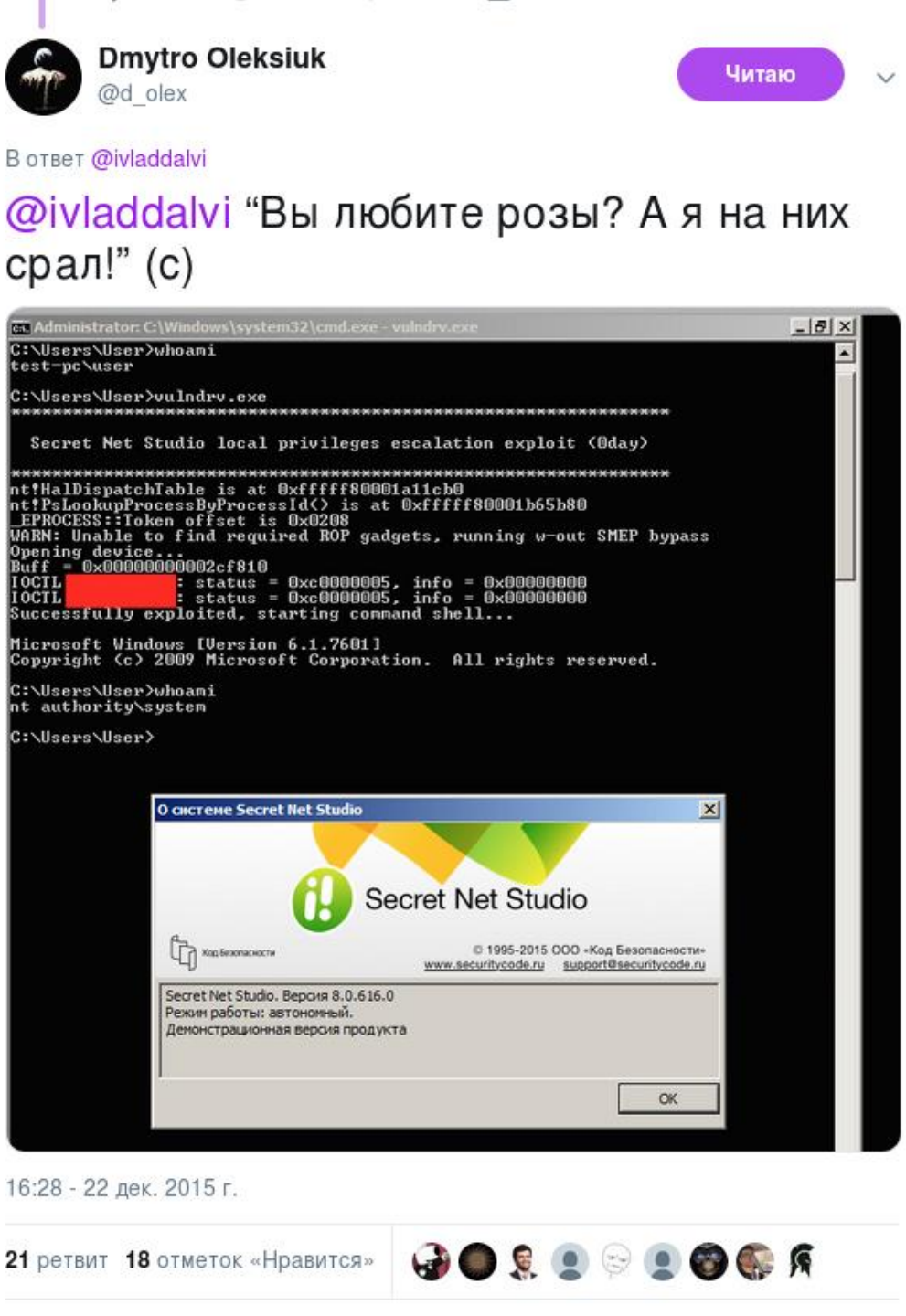
2. Hardware, ICS vendors only

2³ EDITION

Epigraph:

Cr4sh:

https://twitter.com/d_olex/status/679247132851757057



2^3 EDITION

+

0days

The ‘Importozameschenie’

ZERO NIGHTS 2018

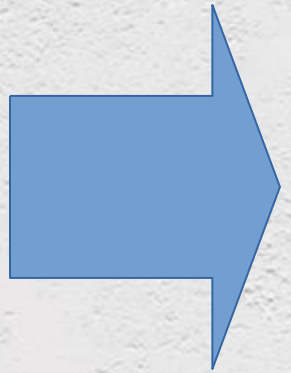
2^3 EDITION

LOCALS ONLY

2018.ZERONIGHTS.ORG

Industrial sectors:

- **Oil& Gas**
- **Chemicals**
- **Vehicles and transportation production**
- **Mechanical Engineering**
- **Etc...**



Critical infrastructure

Doing ‘Importozameschenie’ for Services+products+software+hardware+other stuff...

Why is it important to compare ‘there’ and ‘here’:

- Chance for a local players
- Stimulate market
- A lot of attention to it
- A great responsibility

Couple things could not be replaced – experience and responsibility

There:

- ✓ CERTs
- ✓ PSIRTs
- ✓ Regulations
- ✓ Money!

Here:

- ✗ CERTs
- ✗ PSIRTs
- ✗ Regulations (in terms of vulnerability disclosure)
- ✓ FSTEK vulnerability database (great start, but has to be updated)

Here Here Here There

2^3 EDITION

How we reach vendors

Kaspersky Lab ICS CERT Experience

ZERO NIGHTS 2018

2^3 EDITION

The next moment after bug is discovered.

Contact person:

There:

1) PSIRTs
2) Security mail-box
3) Friends who knows someone from vendor
4) Twitter/LinkedIn
5) Phone calls
6) CERTs

Here:

1) Any email you can find; usually you need to find a senior developer
2) Phone calls

Communications:

There:

1) PGP

Here:

1) PGP

The next moment after bug is discovered

Reporting the bug

Artifacts :

1)Short summary
2)Detailed explanation
3)PoC
4)…
5)Video
6)Demo
7)Screen shots
8)Audio explanation
9)Etc…

Case studies. Here.

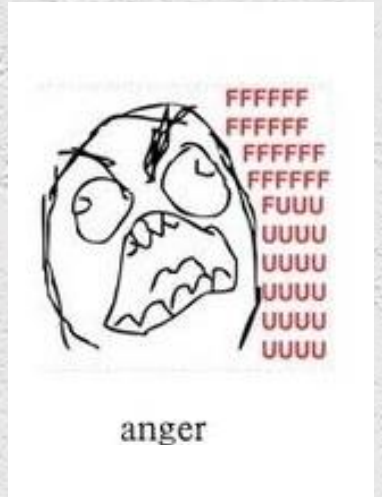
PLC Vendor. Popular brand on ICS market. Arbitrary file reading

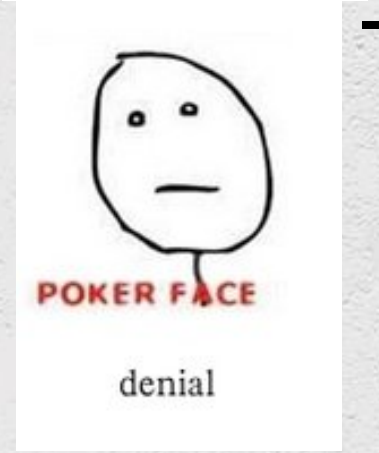
denial

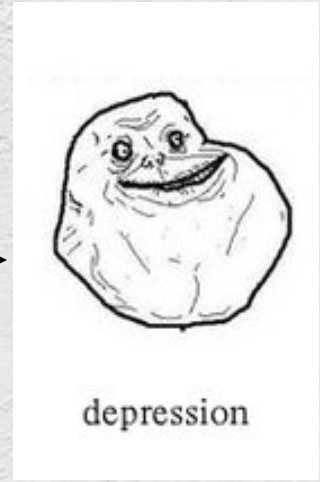
bargaining

acceptance

The same PLC vendor. Remote Code Execution with root privileges (no sandbox/container isolation for byte-code like in other PLCs)





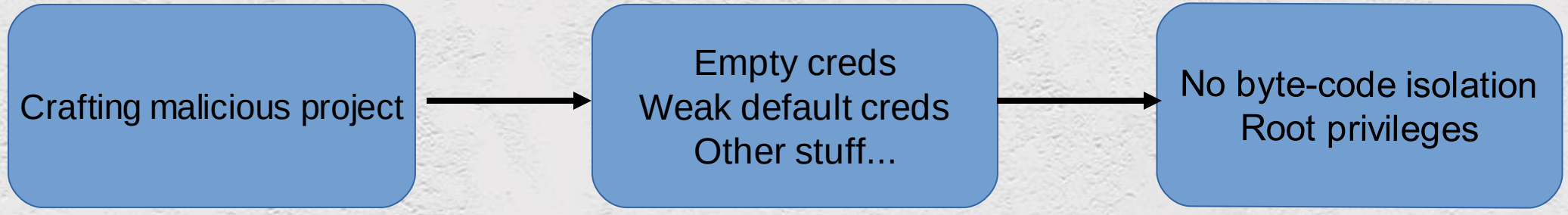


…

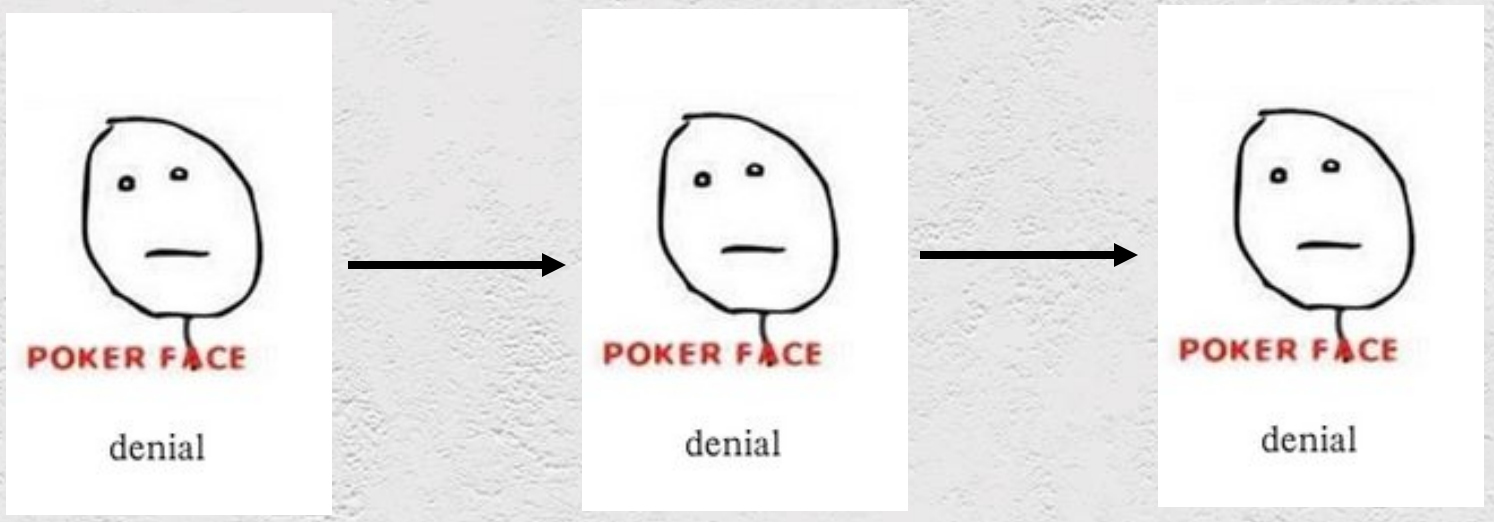
4 month already

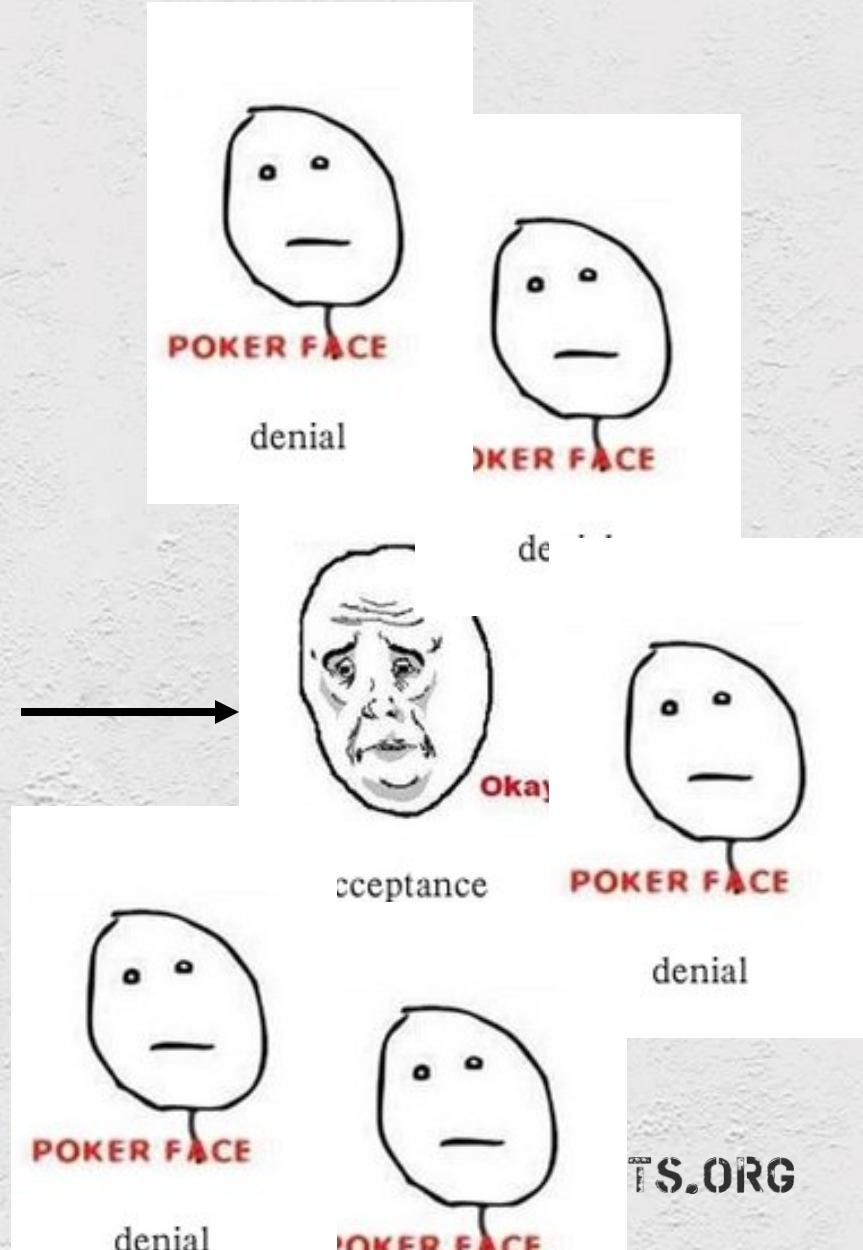
The same PLC vendor. Remote Code Execution via crafted/modified project

Architectural issue



Industrial router vendor





1+ year story. Still do not know. CVEs assigned

TS.ORG

Industrial router vendor. Multiple bugs

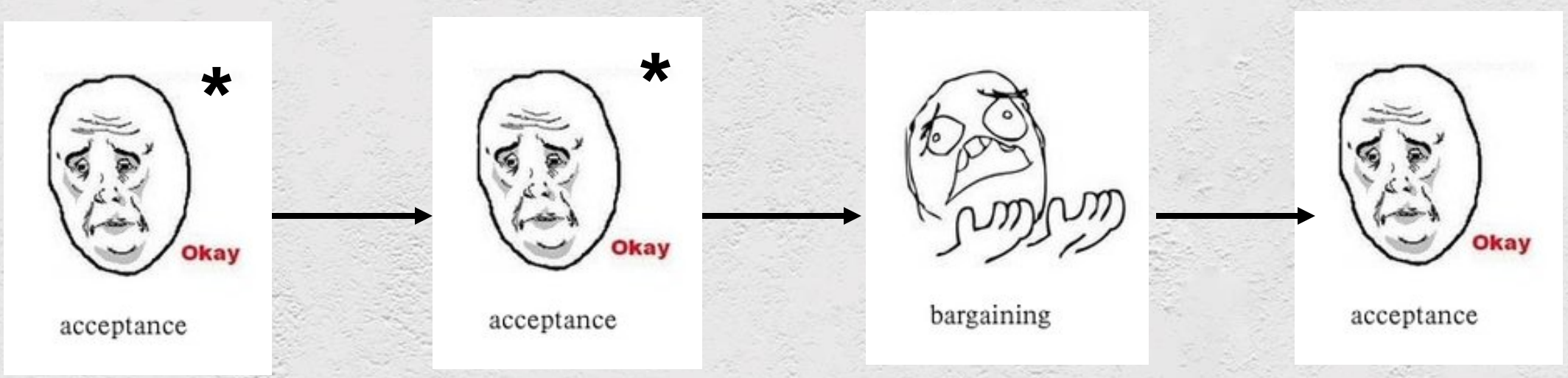
Gray box: docs, installation image, other useful stuff
Timing: Three weeks

Passwords issues
Insecure sudo Configuration
Build-in user with highest privileges
Information Disclosure
Command injection

Require authentication

2³ EDITION

Industrial router vendor (other one). Multiple bugs



A bit less than one year

Industrial router vendor (other one)

Gray box: docs, installation image, other useful stuff
Timing: Three weeks

Cert issue
DoS x 3
RCE (via POST)
Credential issues

Remotely

Case studies. There.

2³ EDITION

Exceptional cases

[redacted]@meau.com>

Reply all

Tue 12/15/2015, 4:28 PM

Vladimir Dashchenko

MITSUB
ELECTR
ges for the B

Download

Vladimir,

A direct email from you to me Is secure enough. Please let me know the specific details of your finding. I appreciate you contacting Mitsubishi Electric with this information.

Respectfully,

[redacted]

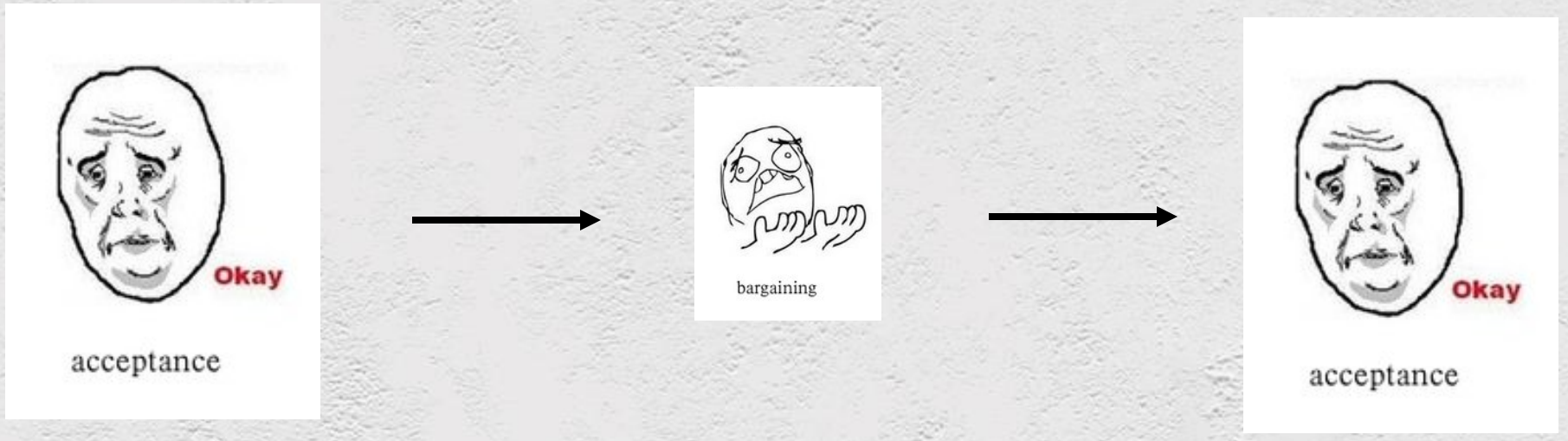
Exceptional cases

Establish TCP connection


ZERO
NIGHTS
2018


2 3
EDITION

Most cases


Okay
acceptance
bargaining
Okay
acceptance

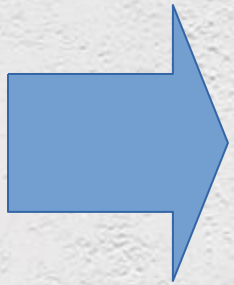
Most of cases. There

90-day policy does not work

In ICS world it takes years (example – 2015 report)

Lowering number of vulnerabilities

No security patch. Only a version update



A new level of ‘maturity’

“Your IT vs Our OT”

Possible reasons. ‘Here’ and ‘There’

Here:

Sense of Invulnerable/Immortal solutions

“Who even needs us except these guys (customers)?!”

There:

Okay, vulnerabilities exist

It’s too risky to show how vulns we’ve had

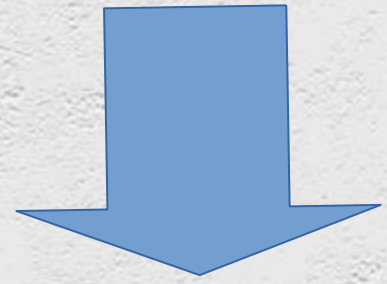
Not that easy to update/upgrade (why no patches available)

ICS Security ‘Balkanization’?

ICS CVSS is coming to ya!

First notice – Jul 2015 by Reid Wightman

2019 – S4X19 ‘A New CVSS For ICS’. Practical testing of methodology



Maybe use both to take into account ICS specifics and cyber-physical effect?

Conclusions

For vendors

Make a vulnerability report procedure transparent and easy

Inform all of your customers that security issue was patched

A security researcher is your friend

Any bounty matters – stickers, public advisory, t-shirt!

Resolved and disclosed bug is better than not reported at all

If you don’t receive bug reports – does not mean that they do not exist

For researchers

How solutions are secured – depends on us

Be patient. Sometimes they need time to realize and to react

Explain possible business impact. Or at least try

If you're not sure that it's a good idea to report a bug (punishment?) ask us! Or other ICS security guys

Quick Hall of Thanks

Kaspersky Lab ICS CERT family

ICS Vendors

@cyberpunkych

And these little guys:

CVE-2016-8368
CVE-2016-8370
CVE-2018-15360
CVE-2018-15359
CVE-2018-15358
CVE-2018-15357
CVE-2018-15356
CVE-2018-15355
CVE-2018-15354
CVE-2018-15353
CVE-2018-15352
CVE-2018-15351
CVE-2018-15350

THANKS FOR ATTENTION

Vladimir.Dashchenko@Kaspersky.com