Incident Response: «Someone please call 3322»

Roland Sako, Security Researcher
Critical Infrastructure Defense Team
Kaspersky Lab, Switzerland
О себе

Роланд Сако

Женева, швейцария

Лабораторий Касперского; Критической инфраструктуры

Исследование безопасности и общение
Somewhere in the Middle East…
Several Issues with the PLCs

Sudden network outage and lose of network connectivity in manufacturing zone.
“Works on my machine” syndrome?

I DON'T ALWAYS CHECK IN BUGS

BUT WHEN I DO, I SAY "WORKS ON MY MACHINE"!
What’s going on..

Problems with PLCs

Information Gathering
Processes, Policies, Diagrams,..
Processes, Policies, Diagrams,..

- Brief access to the plant
- Went on site to collect network traffic
- Client didn’t have diagrams, policies, etc.
Working With Minimal Data

NETWORK TRAFFIC

.PCAP
Understanding .PCAP
What’s going on..

Problems with PLCs

Information Gathering

Actual Analysis

...
Some findings

1. DC directly connected to the Internet
2. Flat network without proper segmentation
3. Many servers including SCADA and SBM are served from the same host as DNS which might expose them to the Internet
4. OPC Server directly connected to DC and default gateway.
5. SMB allows blank user/pass
Just to name a few - Flat network
Just to name a few - DC to the outside
Just to name a few - Weak NTLM password

- NTLMv1 is vulnerable for password hash cracking
"3877418","101.505961","NBNS","92","Name query NB QQ2009.3322.ORG<00>"
"3877419","101.505961","NBNS","92","Name query NB QQ2009.3322.ORG<00>"
"3877420","101.505963","NBNS","92","Name query NB QQ2009.3322.ORG<00>"
"3877421","101.505963","NBNS","92","Name query NB QQ2009.3322.ORG<00>"

"DNS","75","Standard query 0xb527 A qq2009.3322.org"
"DNS","75","Standard query 0xb527 A qq2009.3322.org"
Just to name a few

And many more..
Someone call 3322
Someone call 3322
1. Chinese dynamic DNS service provider
2. Subdomains associated with Malware detected by CN-CERT and Microsoft
3. +70k malicious subdomains
4. A variety of malware
Of note, in the 16 days since we began collecting data on the 70,000 malicious subdomains, we have been able to block more than 609 million connections from over 7,650,000 unique IP addresses to those malicious 3322.org subdomains. In addition to blocking connections to the malicious domains, we have continued to provide DNS services for the unblocked 3322.org subdomains. For example, on Sept. 25, we successfully processed 34,954,795 DNS requests for 3322.org subdomains that were not on our block list.

- Microsoft, 2012

https://blogs.microsoft.com/blog/2012/10/02/microsoft-reaches-settlement-with-defendants-in-nitol-case/
Words on 3322.org

Distribution of malware using 3322.org

- Hupigon: 23.08%
- Zegost: 17.32%
- Other (556 Samples): 18.40%
- Startpage: 7.50%
- PCClient: 4.07%
- Agent: 4.29%
- Farfli: 3.29%
- DelfInject: 2.81%
- Obfuscator: 2.42%
- Small: 2.23%
- Delf: 2.31%
- Malagen: 1.71%
- Dedipros: 1.22%
- ServStart: 1.10%
- Redosdru: 1.01%
- Autorun: 0.96%
- Meredrop: 0.79%
- Malex: 0.74%
- Nitol: 0.71%
- Delfsnif: 0.71%

Figure 16: The above graph represents the distribution of malware currently utilizing 3322.org to retrieve C&C server IP addresses.

https://krebsonsecurity.com/tag/3322-org
What’s going on..

Problems with PLCs
Information Gathering
Actual Analysis
Report Writing & Delivery
Summary

1. Infection might have occurred before 2012
2. DC directly connected to the Internet
3. Straight connection from DC to File Sharing
4. PLC network interfaces used as hubs
5. Flat network without proper segmentation
6. Many servers including SCADA and SBM are served from the same host as DNS which might expose them to the Internet
7. SMB allows blank user/pass
Main Issues, part. 2

Malware infected DC, DNS, Admin servers, SMB, Network shares.
Conclusion

1. Non-ICS malware in ICS environment still hurts
2. No need for sophisticated malware like Stuxnet
3. We can still cause DOS ICS equipment with simple «stupid» malware
4. No way for the manufacturer to spot the issue
Questions?