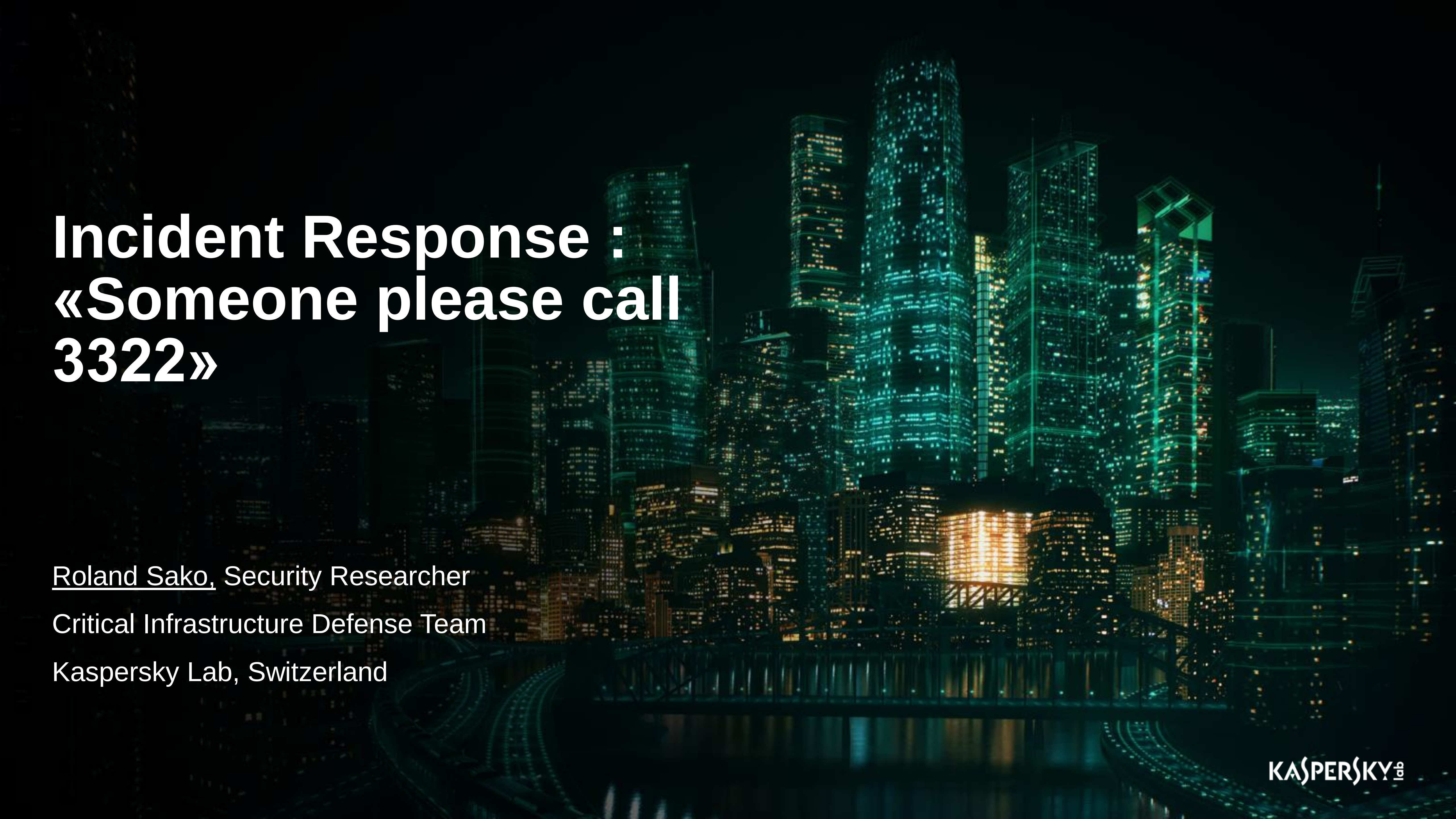


Incident Response : «Someone please call 3322»

Roland Sako, Security Researcher

Critical Infrastructure Defense Team

Kaspersky Lab, Switzerland

О себя

Роланд Сако

Женева, швейцария 🇨🇭

Лабораторий Касперского; Критической инфраструктуры

Исследование безопасности и обзчение

Somewhere in the Middle East…

Several Issues with the PLCs

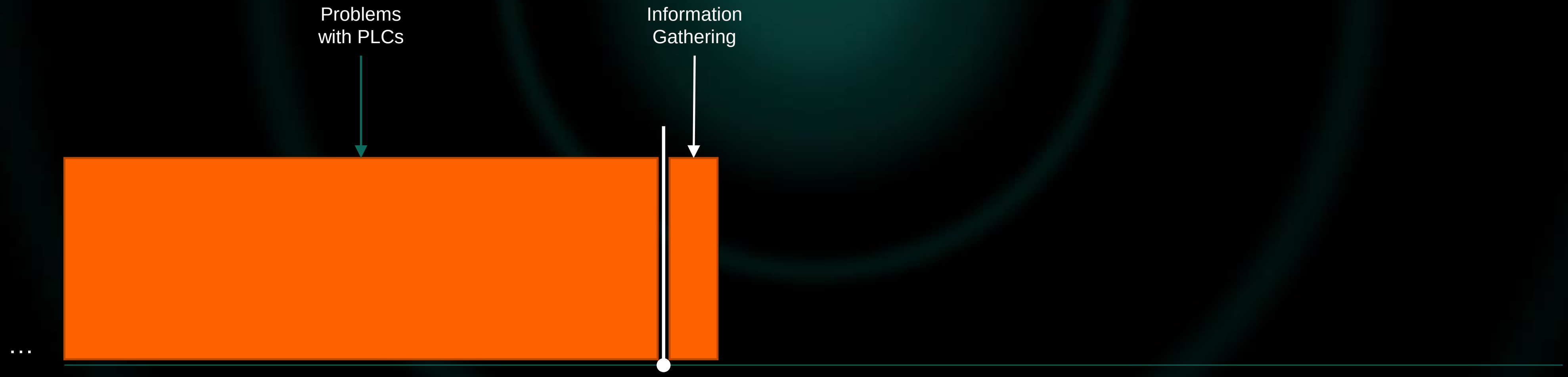
Sudden network outage and lose of network connectivity in manufactruring zone..

Looking for help

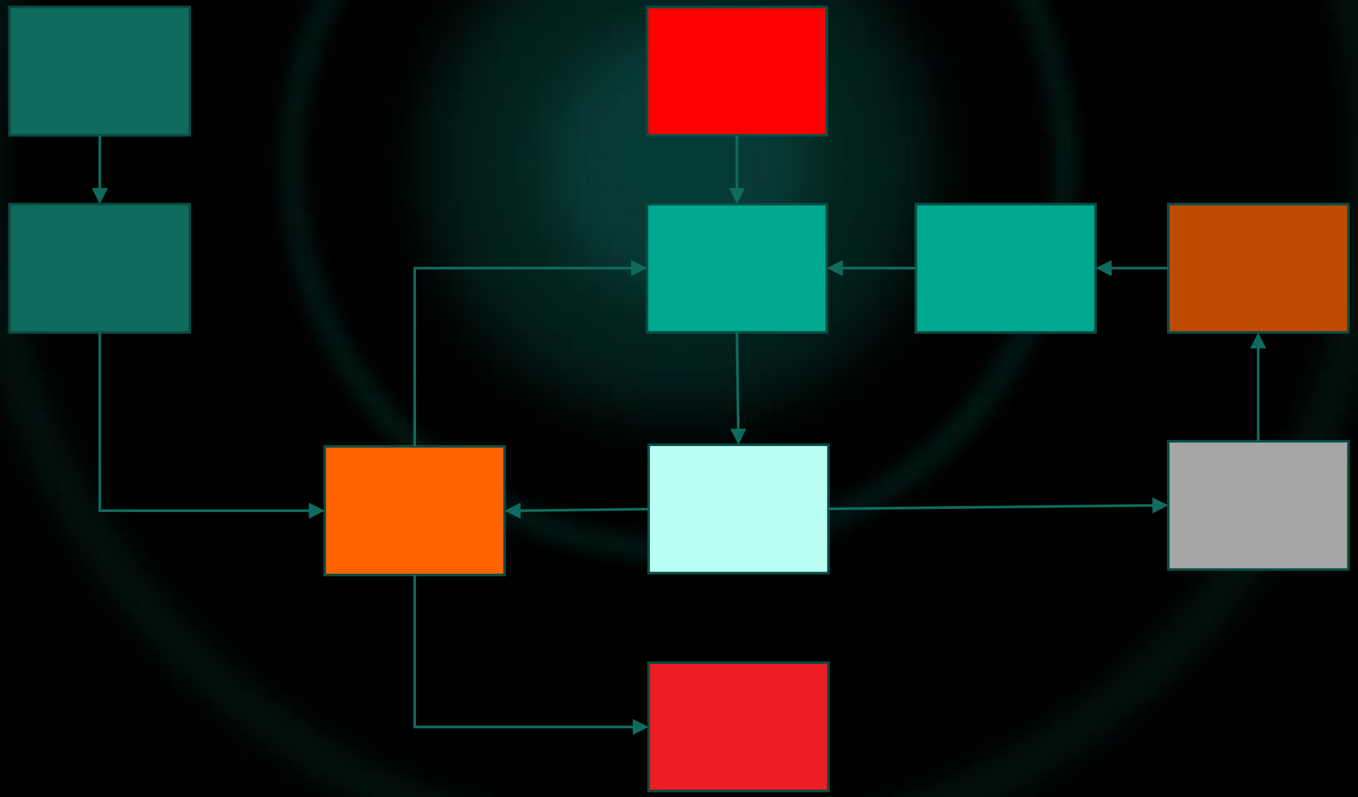
“Works on my machine” syndrome?

I DONT ALWAYS CHECK IN BUGS
BUT WHEN I DO, I SAY "WORKS ON MY MACHINE"!

What’s going on..



Processes, Policies, Diagrams,..



Processes, Policies, Diagrams,..

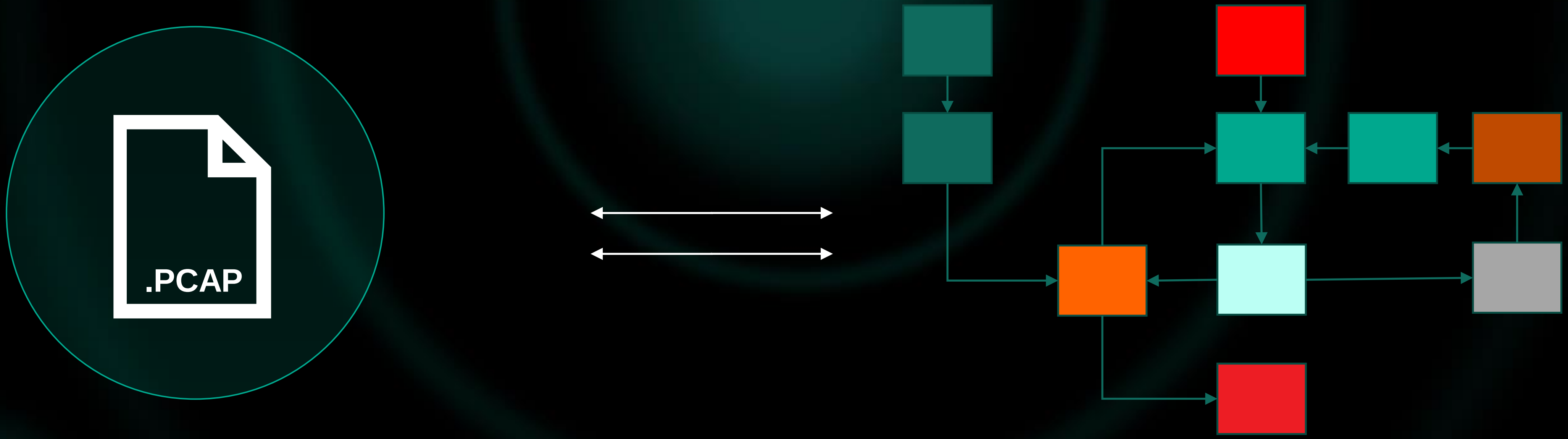
- Brief access to the plant
- Went on site to collect network traffic
- Client didn’t have diagrams, policies, etc.

Working With Minimal Data

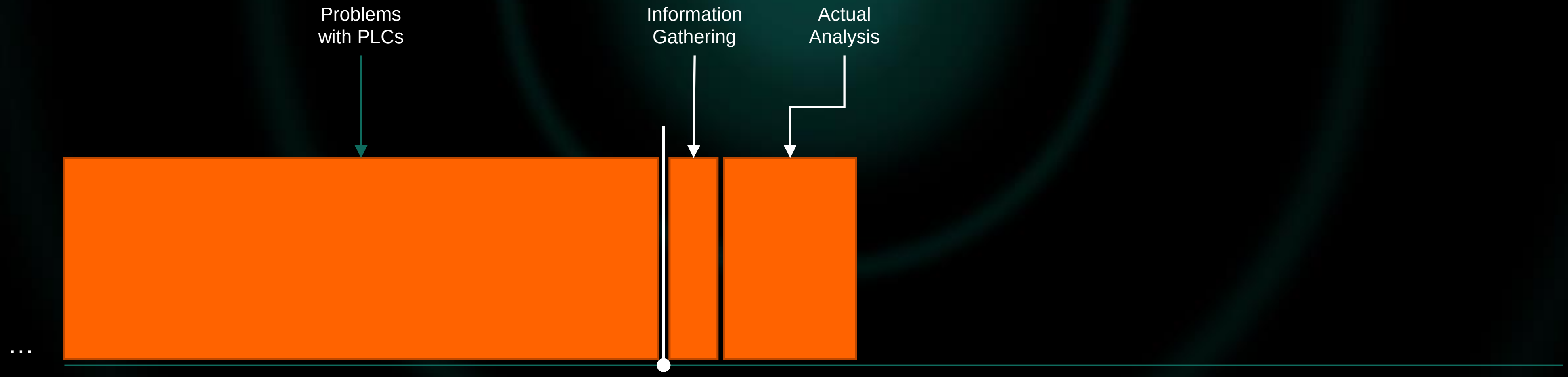
.PCAP

NETWORK TRAFFIC

Understanding



What’s going on..

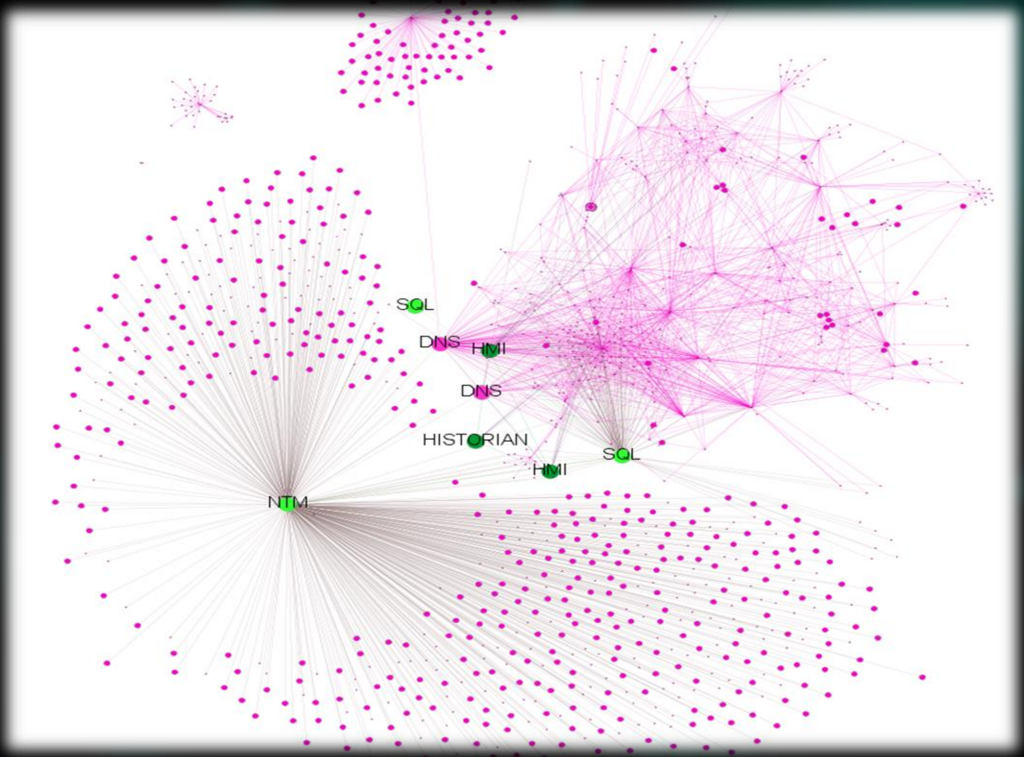


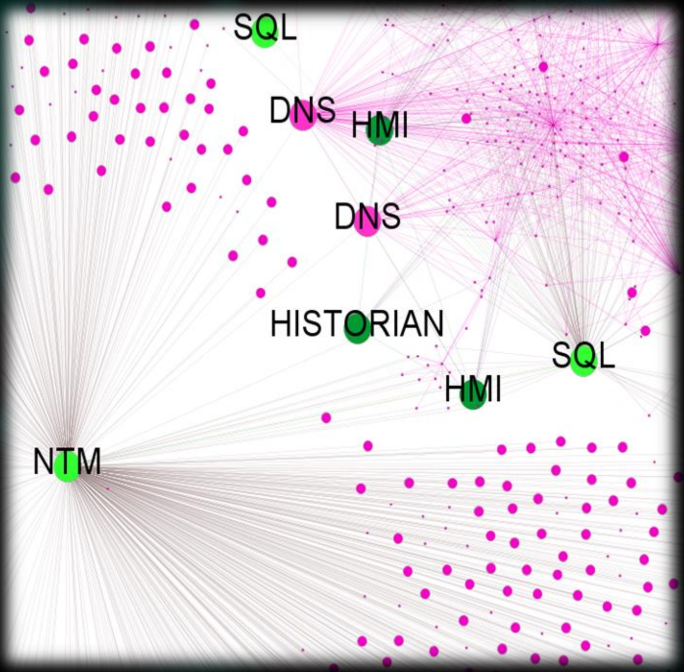
KASPERSKY lab

Some findings

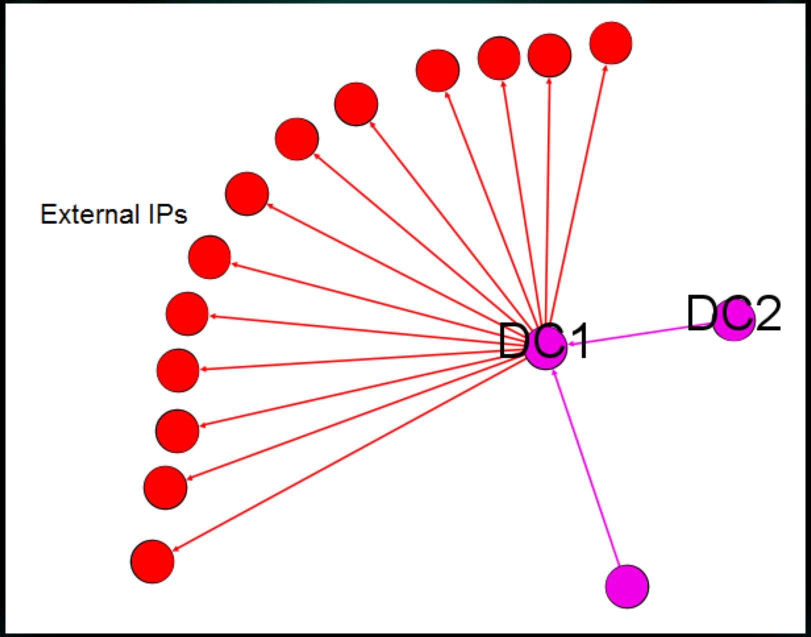
1. DC directly connected to the Internet
2. Flat network without proper segmentation
3. Many servers including SCADA and SBM are served from the same host as DNS which might expose them to the Internet
4. OPC Server directly connected to DC and default gateway.
5. SMB allows blank user/pass

Just to name a few - Flat network

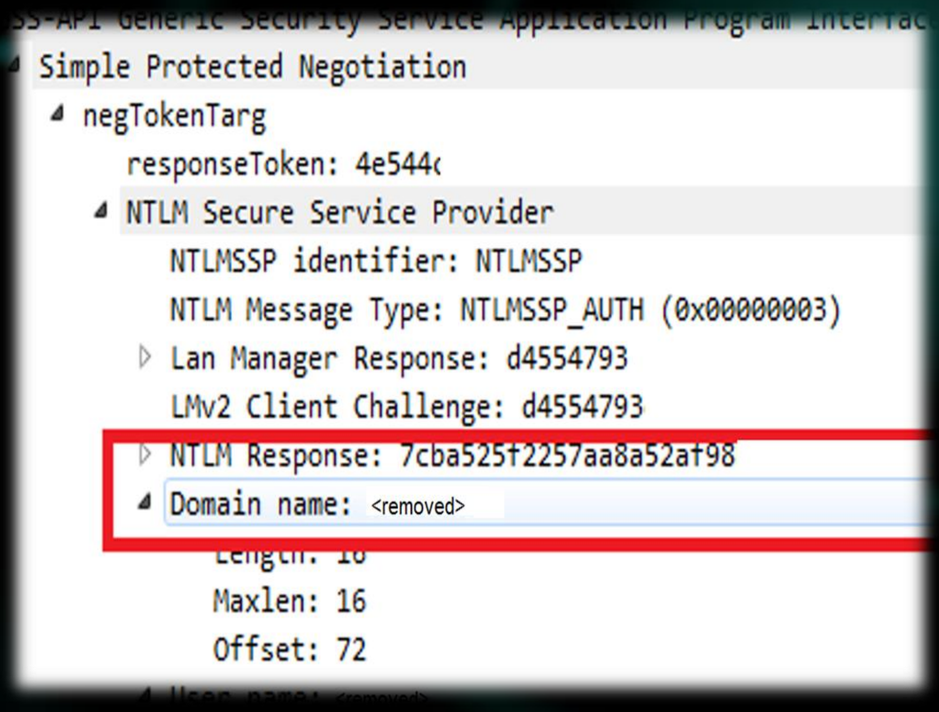




Just to name a few - DC to the outside



Just to name a few - Weak NTLM password



```
SS-API Generic Security Service Application Program Interfac
◢ Simple Protected Negotiation
  ◢ negTokenTarg
      responseToken: 4e544(
    ◢ NTLM Secure Service Provider
        NTLMSSP identifier: NTLMSSP
        NTLM Message Type: NTLMSSP_AUTH (0x00000003)
      ▷ Lan Manager Response: d4554793
        LMv2 Client Challenge: d4554793
      ▷ NTLM Response: 7cba525f2257aa8a52af98
      ◢ Domain name: <removed>
          Length: 16
          Maxlen: 16
          Offset: 72
      ◢ User name: <removed>
```

- **NTLMv1 is vulnerable for password hash cracking**

Just to name a few - Strange DNS requests

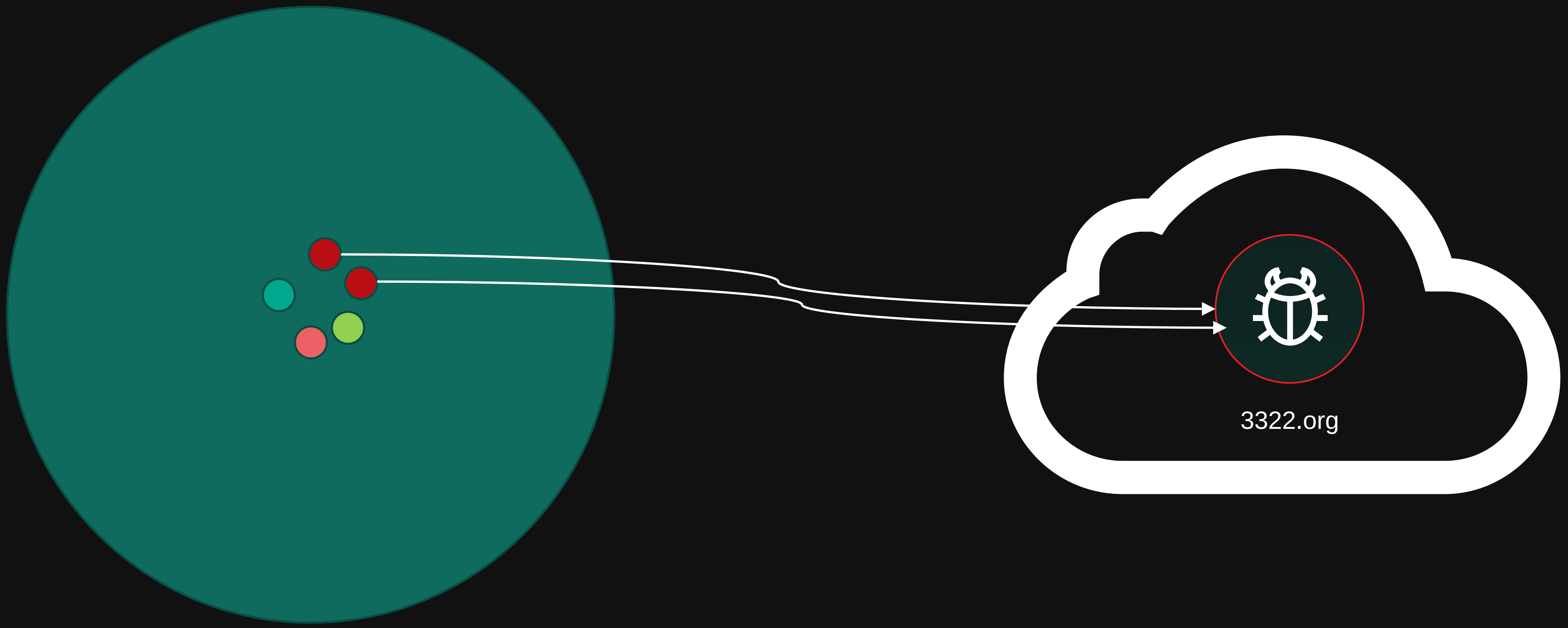
```
"3877418","101.505961","NBNS","92","Name query NB QQ2009.3322.ORG<00>"
"3877419","101.505961","NBNS","92","Name query NB QQ2009.3322.ORG<00>"
"3877420","101.505963",”NBNS","92","Name query NB QQ2009.3322.ORG<00>"
"3877421","101.505963",NBNS","92","Name query NB QQ2009.3322.ORG<00>"
```

```
"DNS","75","Standard query 0xb527 A qq2009.3322.org"
"DNS","75","Standard query 0xb527 A qq2009.3322.org"
```

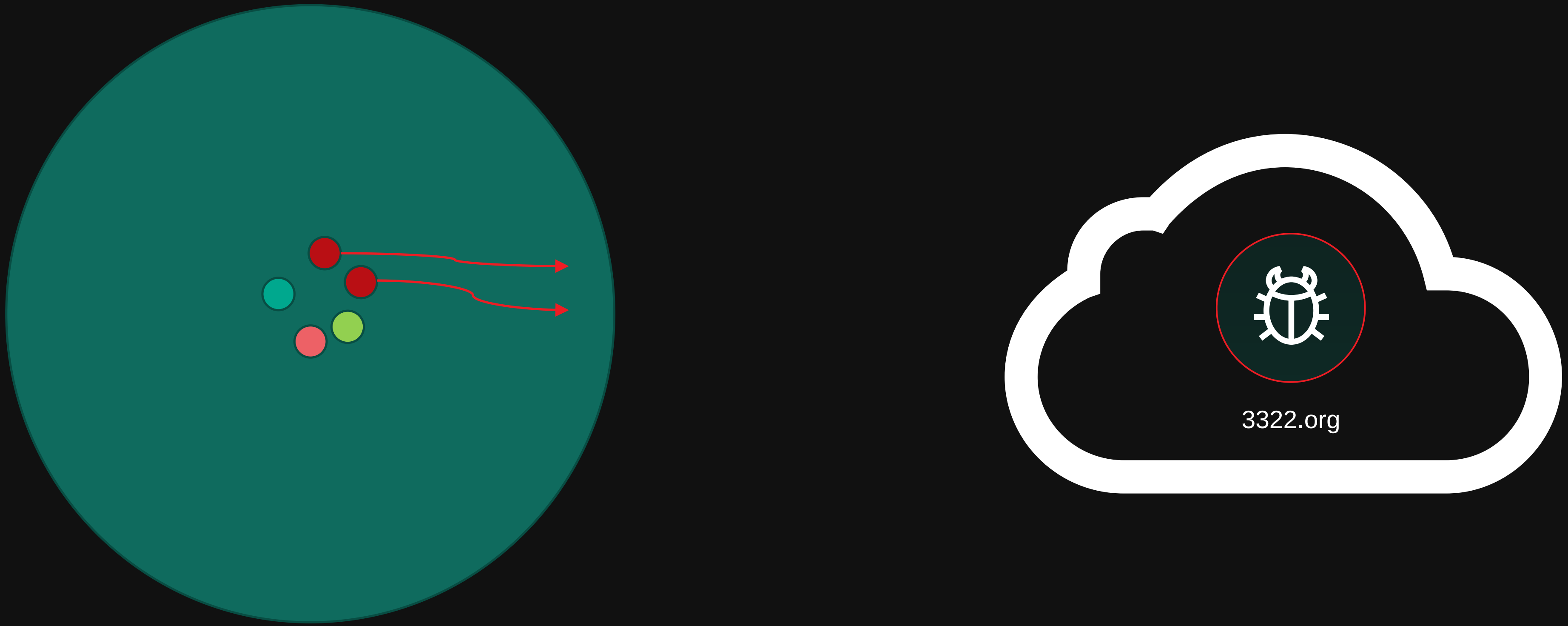
Just to name a few

And many more..

Someone call 3322



Someone call 3322



3322.org

Words on 3322.org

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

Words on 3322.org

”

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

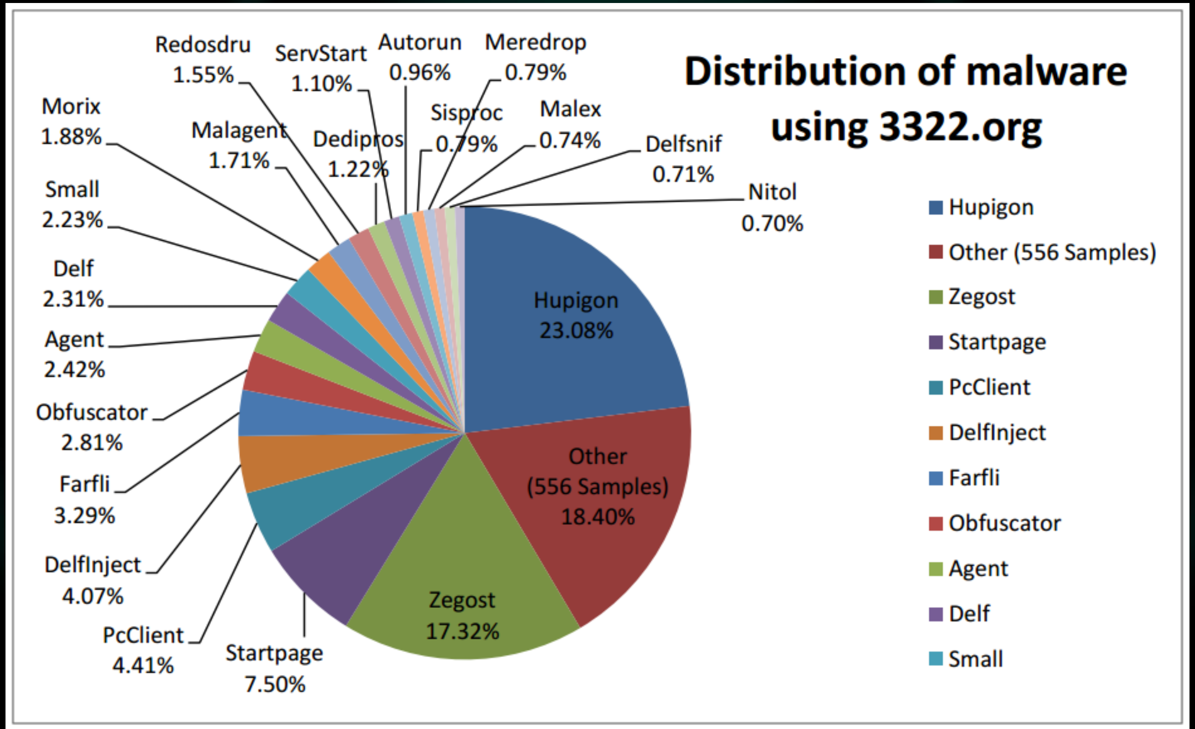
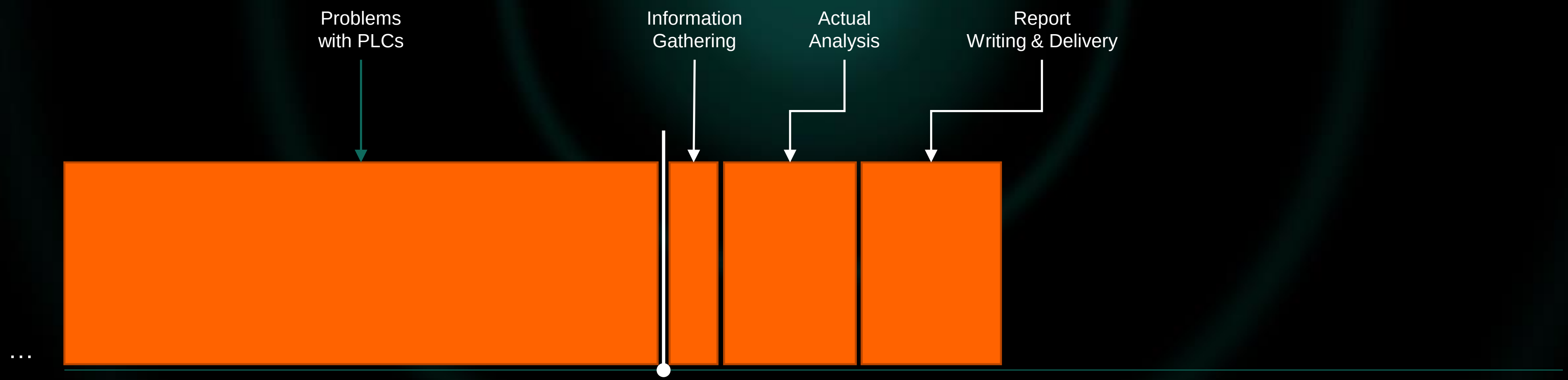


Figure 16: The above graph represents the distribution of malware currently utilizing 3322.org to retrieve C&C server IP addresses.

https://krebsonsecurity.com/tag/3322-org

What’s going on..



Summary

1. Infection might have occured 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 environement still hurts
2. No need for sofisticated 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?