# Security Considerations in Public Sector 2016


## Ondrej Stahlavsky

**Regional Director CEE**


FORTINET

# První svého druhu: Setmění na Ukrajině 23.12.2015

| ZNÁMÝ CÍL # 1 | |
|---|---|
| Společnost | Prykarpattya Oblenergo |
| Dopad | Výpadek v 8 provinciích Ivano-Frankivsk regionu |

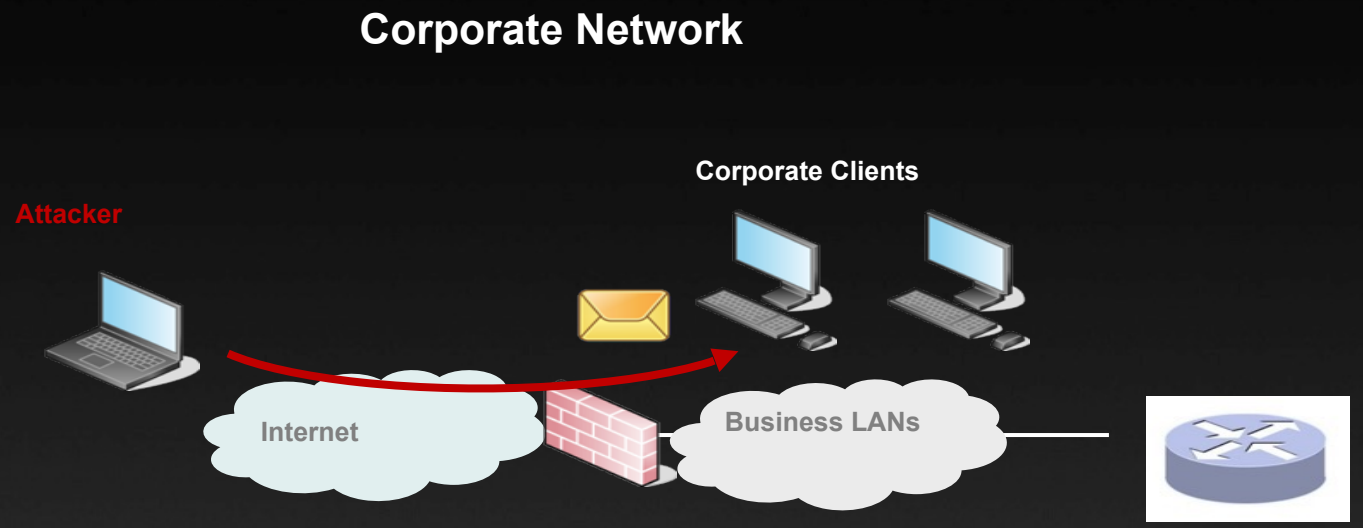
| ZNÁMÝ CÍL # 2 | |
|---|---|
| Společnost | Kyivoblenergo |
| Dopad | Odpojení 30 elektrických stanic = přerušení dodávek elektřiny pro cca 80 000 zákazníků |

*"The big lesson here is that…someone actually brought down a power system through cyber means. That is an historic event, it has never occurred before."*

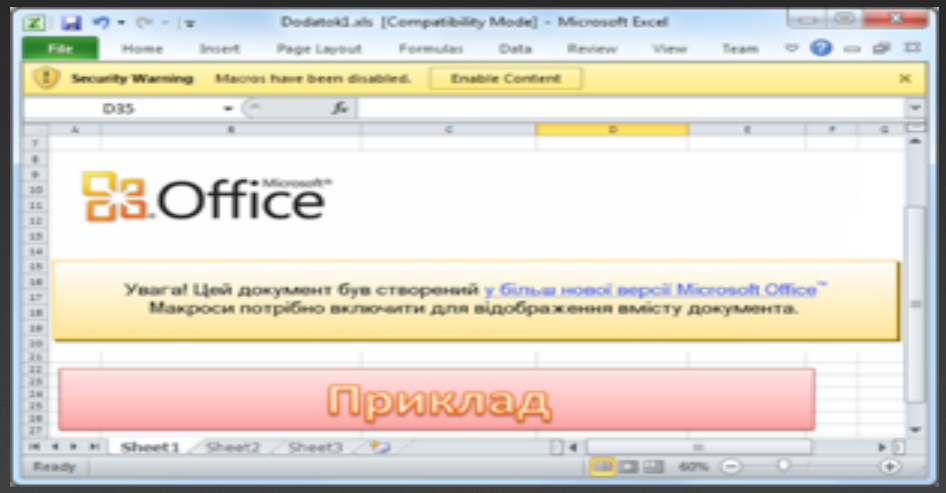
*- Robert M. Lee, Cyber Warfare Operations Officer for the US Air Force*

FORTINET

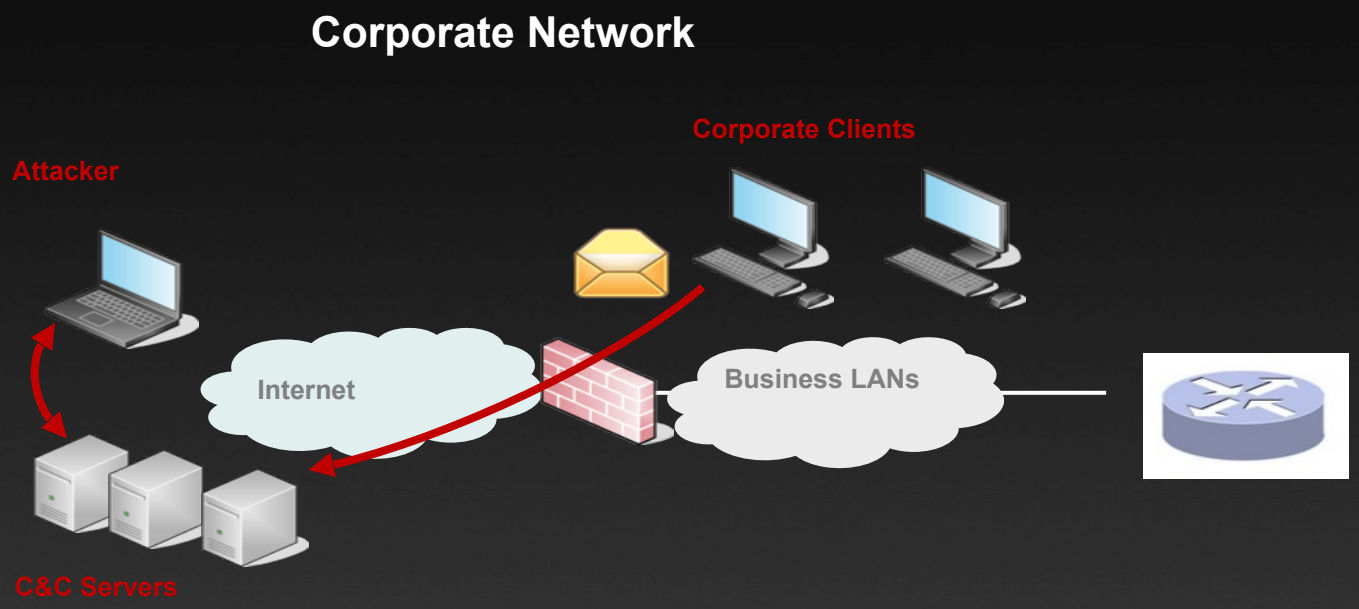
# 1. Spear Pishing Email




*The target gets a spear-phishing email that contains an attachment with a malicious document. The attackers spoofed the sender address to appear to be one belonging to Rada (the Ukrainian parliament) and the document itself contains text trying to convince the victim to run the macro in the document*

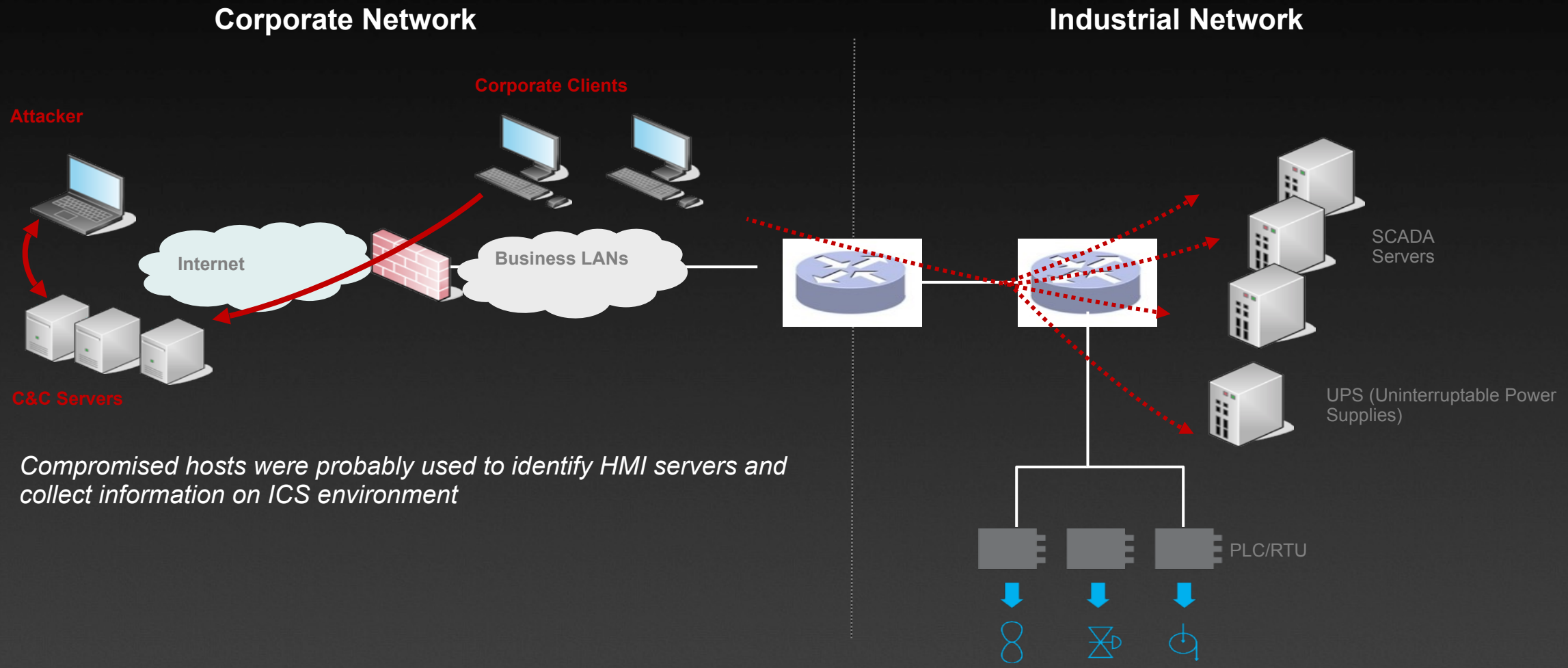


# 2. Information Gathering



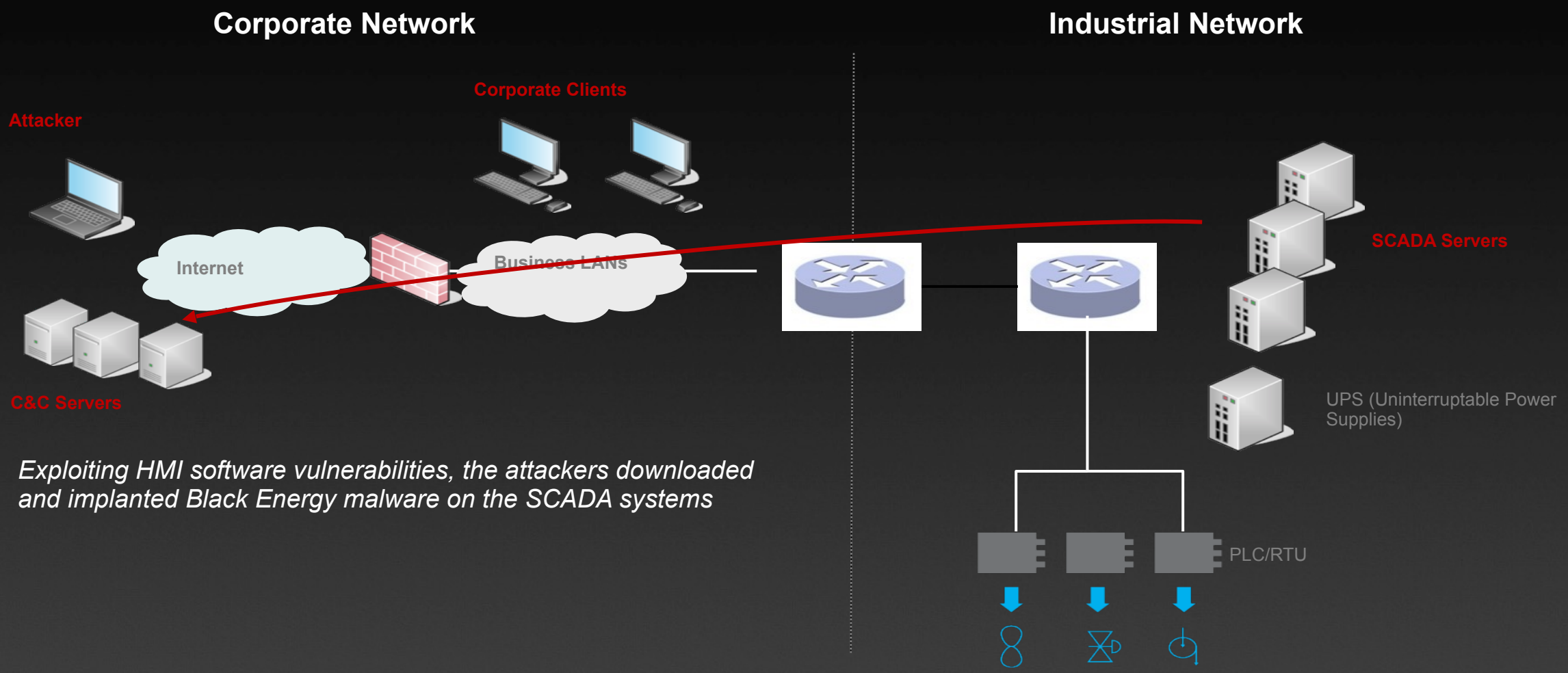

*The victims, successfully tricked, executed malicious code to interact with remote Command and Control (C&C) servers. System information was sent to C&C servers, and was used by attackers to gather additional information about targets. Ultimate goal was to execute commands on the victim's hosts or to gain remote access to the target network*

# 3. Lateral Movement



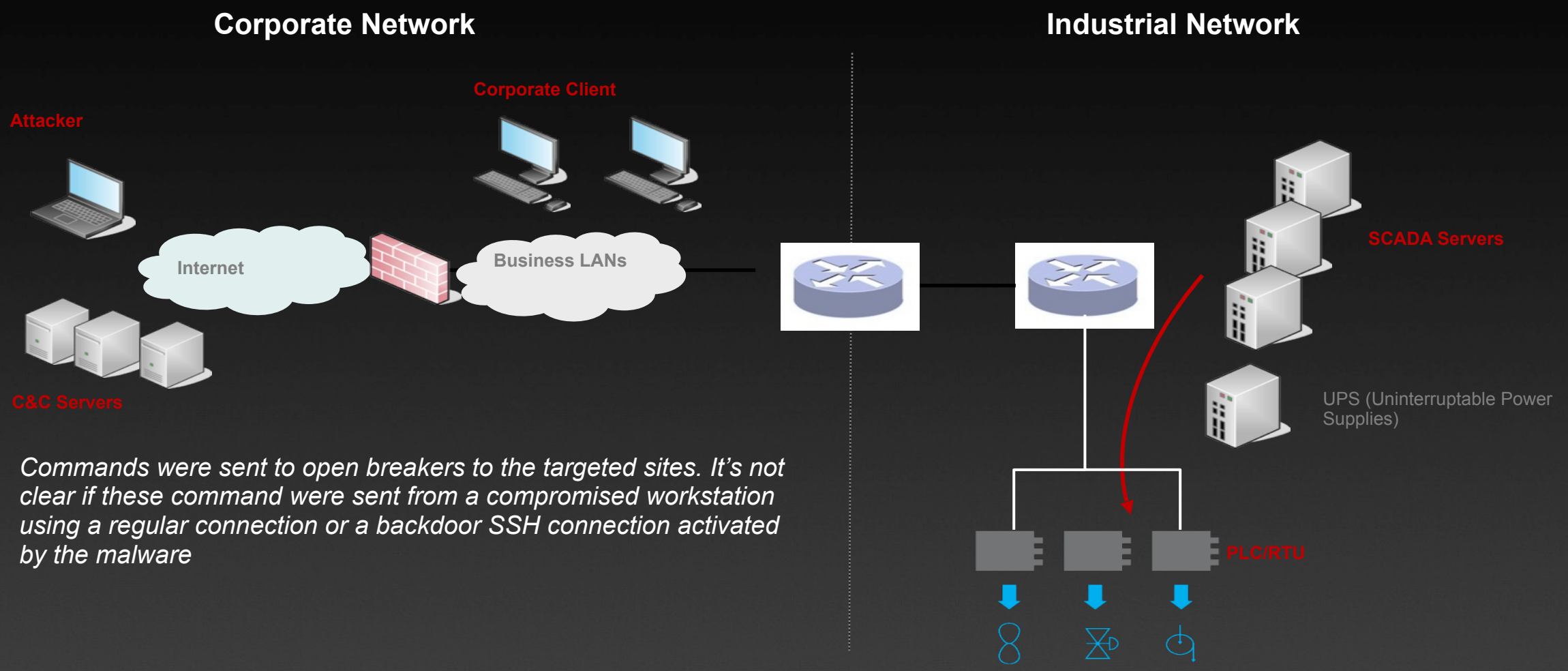

*Compromised hosts were probably used to identify HMI servers and collect information on ICS environment*

# 4. SCADA Infiltration



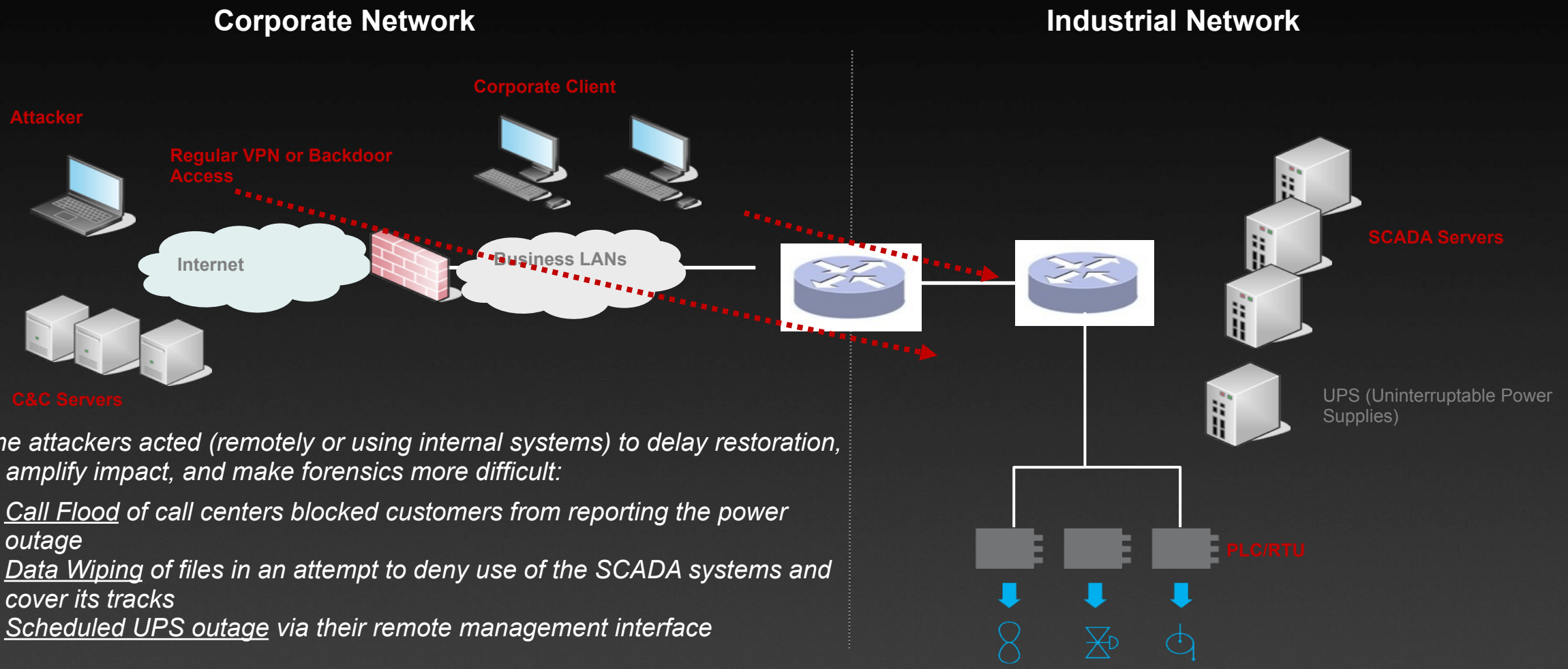

*Exploiting HMI software vulnerabilities, the attackers downloaded and implanted Black Energy malware on the SCADA systems*

# 5. Electric Outage




*Commands were sent to open breakers to the targeted sites. It's not clear if these command were sent from a compromised workstation using a regular connection or a backdoor SSH connection activated by the malware*

# 6. Actions to hinder incident response

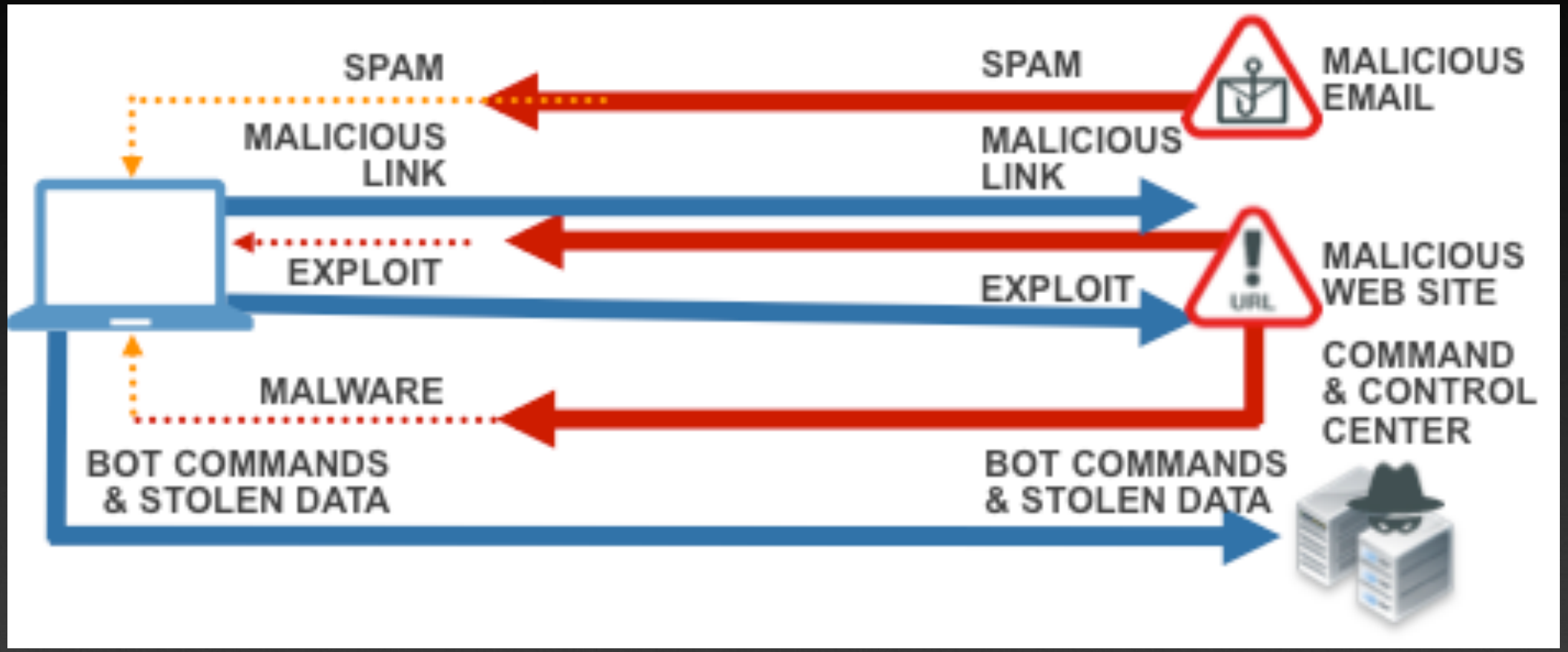



*The attackers acted (remotely or using internal systems) to delay restoration, to amplify impact, and make forensics more difficult:*

- *Call Flood of call centers blocked customers from reporting the power outage*
- *Data Wiping of files in an attempt to deny use of the SCADA systems and cover its tracks*
- *Scheduled UPS outage via their remote management interface*

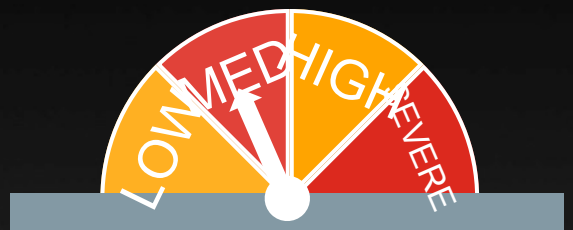
# Portable media attack vector

# Attack Anatomy – INTERNET vector

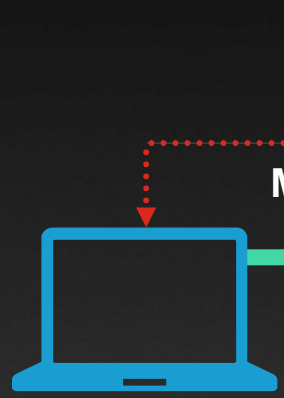


# Delivery

Goal: Choose the best delivery mechanism as possible to deliver the exploit.




- SOCIAL ENGINEERING / PHISHING
- DRIVE-BY-MALWARE (WEBSITE)
- MALVERTISING



SPAM

MALICIOUS LINK

- ANTI-SPAM
- WEB FILTERING
- INTRUSION PREVENTION
- ANTIVIRUS
- APP CONTROL/ IP REPUTATION

SPAM

MALICIOUS LINK

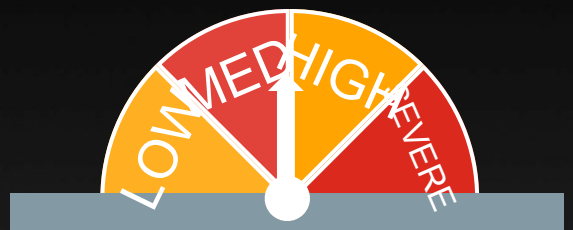
MALICIOUS EMAIL


MALICIOUS WEB SITE

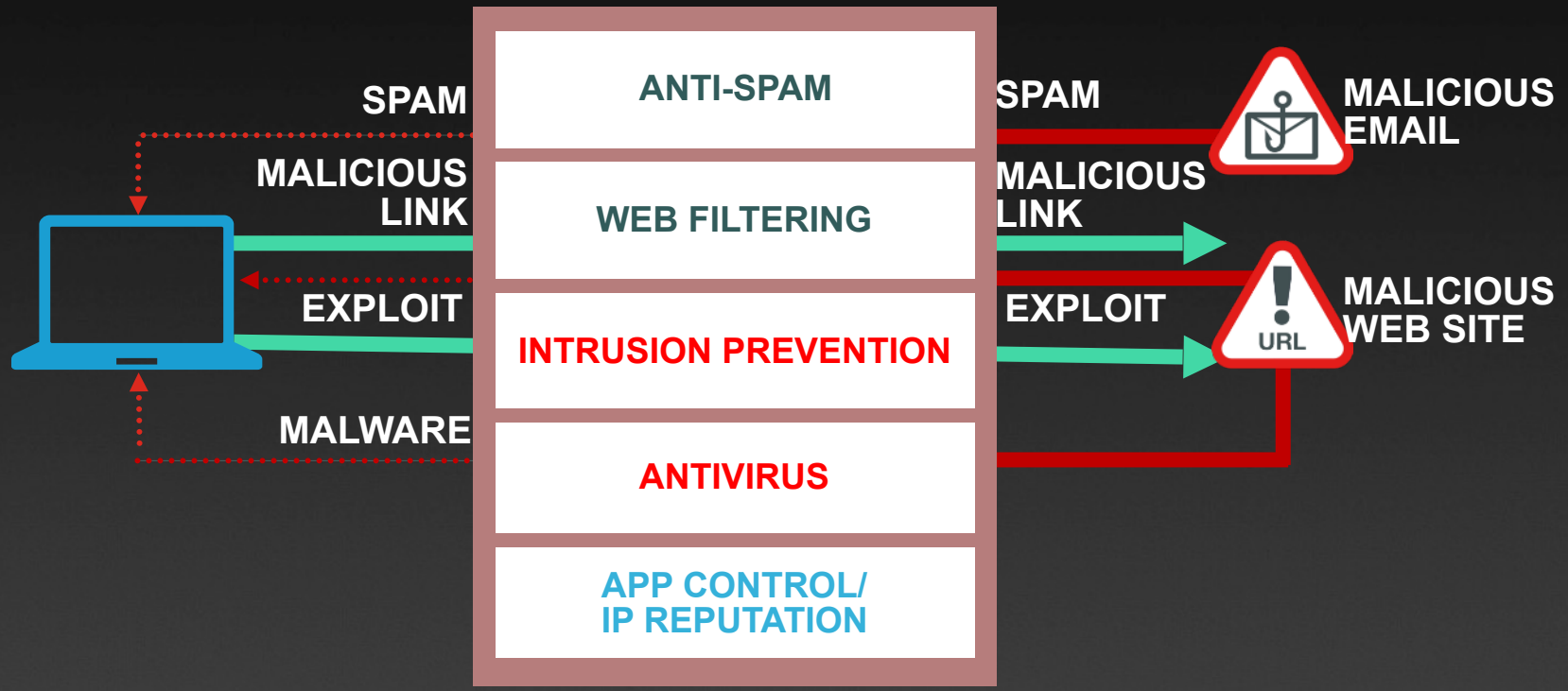
FORTINET

# Exploitation

Goal: Successful, stable exploitation of the system without being detected.



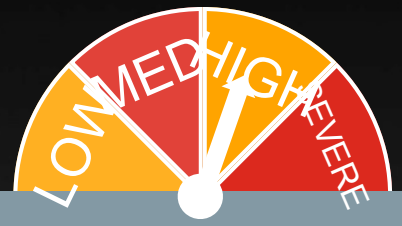

- BROWSER PLUGINS – FLASH, JAVA
- MALICIOUS ADOBE
- OFFICE DOCUMENTS - MACROS




FORTINET

# Command and Control

Goal: Communicate undetected back to malicious infrastructure to  and download other tools.




- DNS TUNNELING
- TUNNELING USING ICMP, TOR, ETC
- FAST FLUX

**Identity&Access Management**

**Security Information and Event Management (SIEM)**

ALICIOUS MAIL

ALICIOUS EB SITE

OMMAND CONTROL ENTER

FORTINET

# Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti (č. 181/2014 Sb.) byl schválen s účinností od 1.1.2015. Firmy a organizace, kterých se zákon týká, měly dostatek času se připravit a sladit své bezpečnostní procesy a infrastrukturu se zněním zákona. Přesto mnoho subjektů zákon do dnešního dne nesplňuje a hrozí jim tak nápravná opatření a sankce od NBÚ.

Zákon určuje, jak má být kybernetická bezpečnost zajištěna a definuje, jakým způsobem se má reagovat na hrozby a řešit vzniklé bezpečnostní události. Další podrobnosti k zákonu jsou stanoveny v prováděcích vyhláškách a to včetně technických požadavků na jednotlivé systémy.

Subjekty, kterých se zákon týká, jsou v zákoně jasně definované. Rozhodně to ale neznamená, že ostatní mohou na zákon zapomenout. Ochrana dat, uživatelů a komunikace se dnes týká úplně všech. Zákon pak slouží jako určité doporučení a metodika, jak přistupovat ke kybernetické bezpečnosti.

Pokrytí jednotlivých částí zákona konkrétními řešeními výrobců nemusí být vůbec snadné a přímočaré. Užití produktů od mnoha výrobců komplikuje integraci celého řešení do funkčního a bezpečného celku a vede k nepřiměřené zátěži pracovníků při provozu podobného řešení. Fortinet Vám nabízí řešení, které pokryje značné množství kapitol zákona a bude snadno integrovatelné.

## ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

- §16 FYZICKÁ BEZPEČNOST
- §17 OCHRANU INTEGRITY KOMUNIKAČNÍCH SÍTÍ
- §18 OVĚŘOVÁNÍ IDENTITY UŽIVATELŮ
- §19 ŘÍZENÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ
- §20 OCHRANA PŘED ŠKODLIVÝM KÓDEM
- §21 ZAZNAMENÁVÁNÍ ČINNOSTÍ SYSTÉMU A UŽIVATELŮ
- §22 DETEKCE BEZPEČNOSTNÍCH UDÁLOSTÍ
- §23 SBĚR A VYHODNOCENÍ BEZPEČNOSTNÍCH UDÁLOSTÍ
- §24 APLIKAČNÍ BEZPEČNOST
- §25 KRYPTOGRAFICKÉ PROSTŘEDKY
- §26 ZAJIŠŤOVÁNÍ ÚROVNĚ DOSTUPNOSTI
- §27 BEZPEČNOST PRŮMYSLOVÝCH A ŘÍDICÍCH SYSTÉMŮ

# Cyber Threat Assesment Program


csr_sales@fortinet.com