Security Considerations 2016

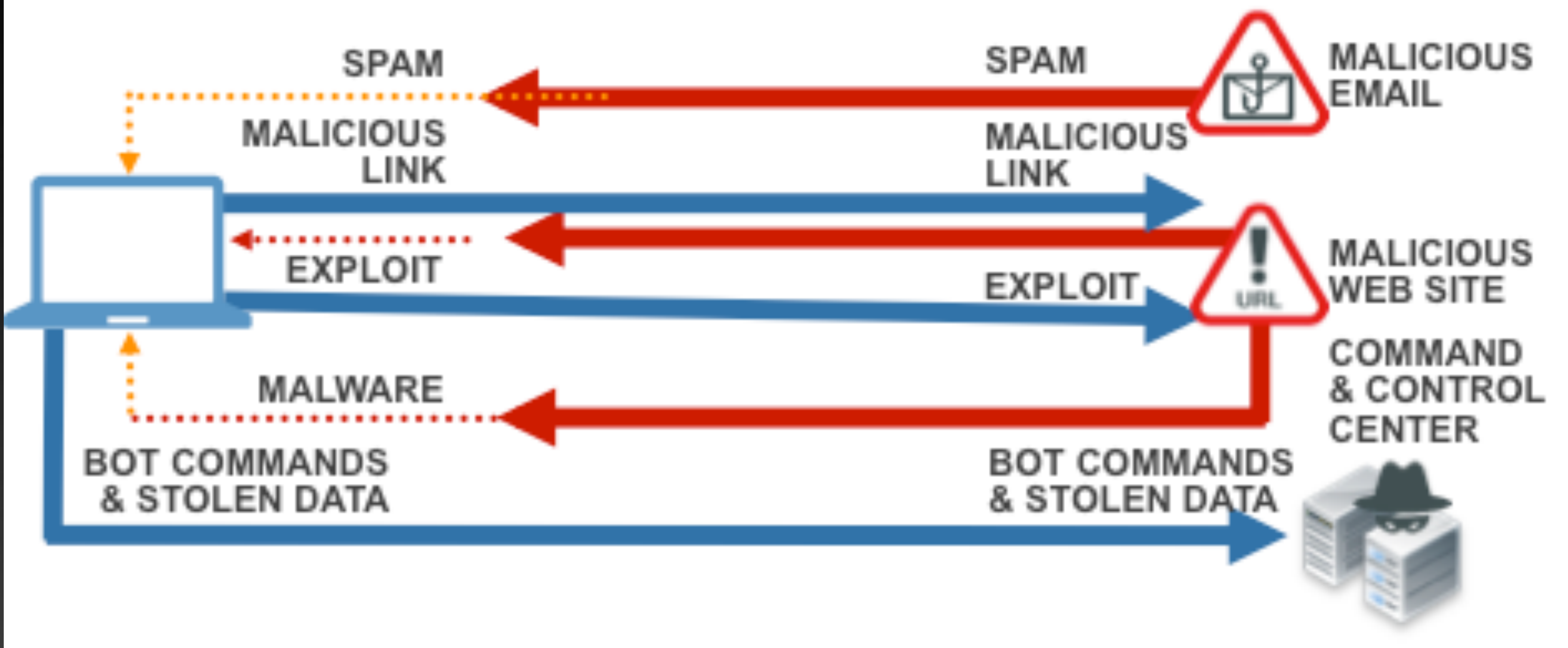
Ondrej Stahlavsky

Regional Director CEE

FORTINET

Portable media attack vector

Attack Anatomy – INTERNET vector



První svého druhu: Setmění na Ukrajině 23.12.2015

ZNÁMÝ CÍL # 1

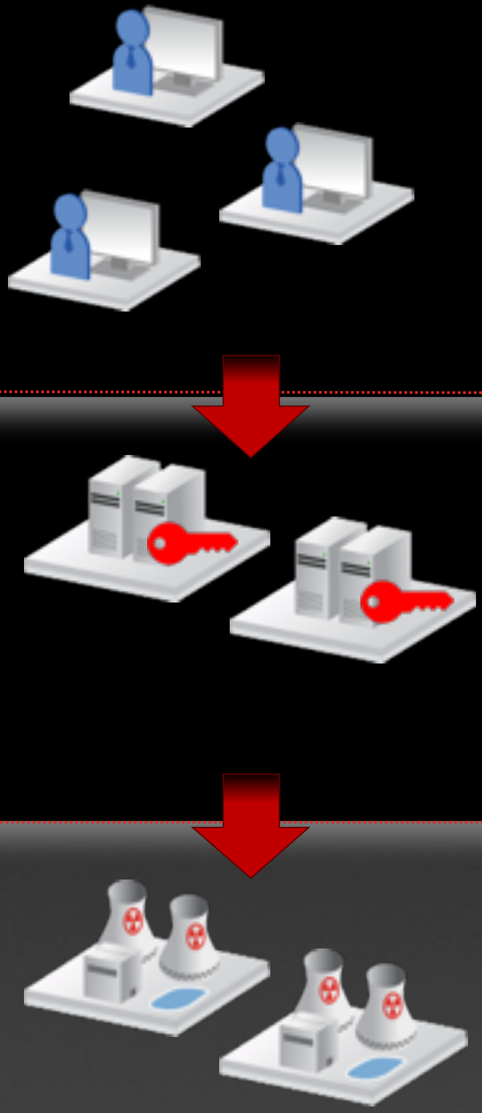
Společnost	*Prykarpattya Oblenergo*
Dopad	*Výpadek v 8 provinciích Ivano-Frankivsk regionu*

ZNÁMÝ CÍL # 2

Společnost	*Kyivoblenergo*
Dopad	*Odpojení 30 elektrických stanic = přerušení dodávek elektřiny pro cca*

> *“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*

BlackEnergy 3



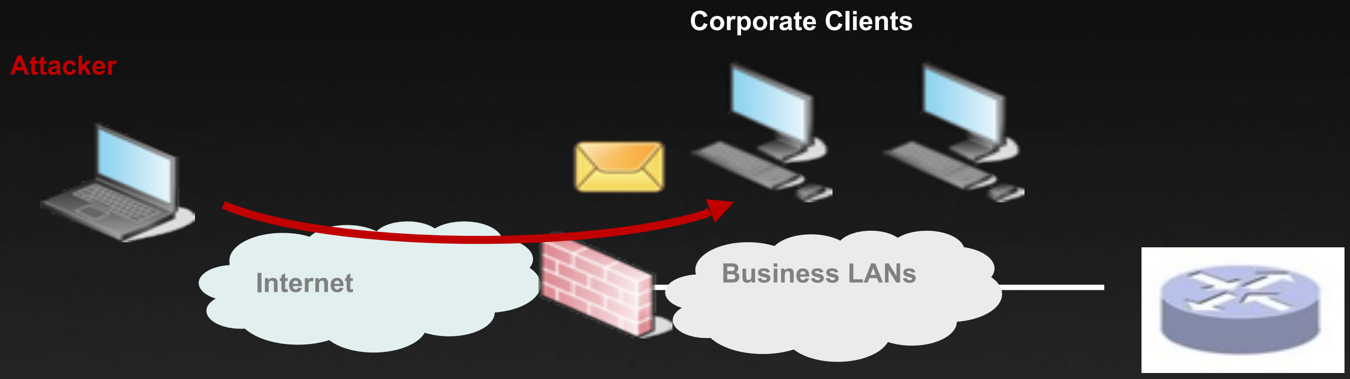
- Umožňuje spojení s Command and Control (C&C) serverem
- Odesílá informace o systému na C&C server
- Instaluje KillDisk malware – sleep state
- ➢ *Poskytuje zadní vrátka útočníkům a získává přístupové údaje administrátorů*

- Využívá síťové připojení k dalšímu šíření na připojené systémy
- ➢ *Umožňuje útočníkům instalovat SSH backdoor pro trvalý přístup*
- ➢ *Umožňuje útočníkům laterální pohyb s využitím získaných přístupových údajů*

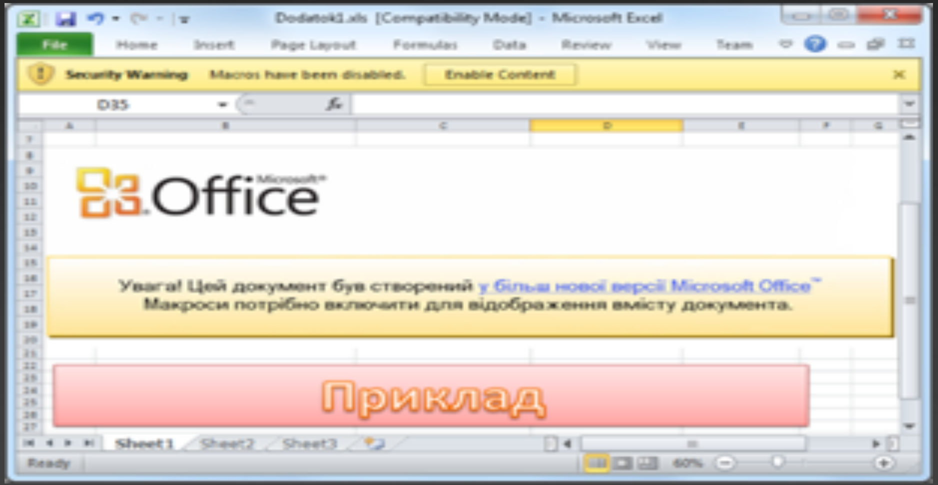
- Využívá síťové připojení k přesunu z IT do ICS prostředí
- ➢ *Umožňuje útočníkům instalovat RATs na kritické systémy*

1. Spear Pishing Email

Corporate Network



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

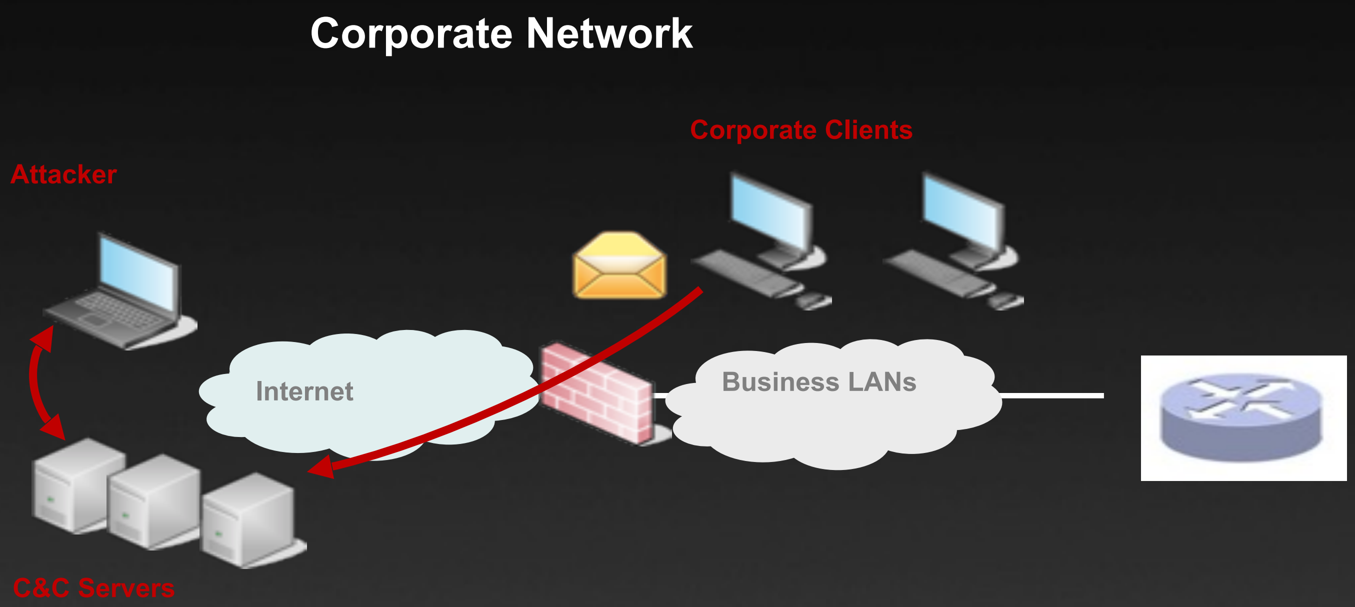


Security Warning Macros have been disabled. Enable Content

Увага! Цей документ був створений у більш новоі версіі Microsoft Office™
Макроси потрібно включити для відображення вмісту документа.

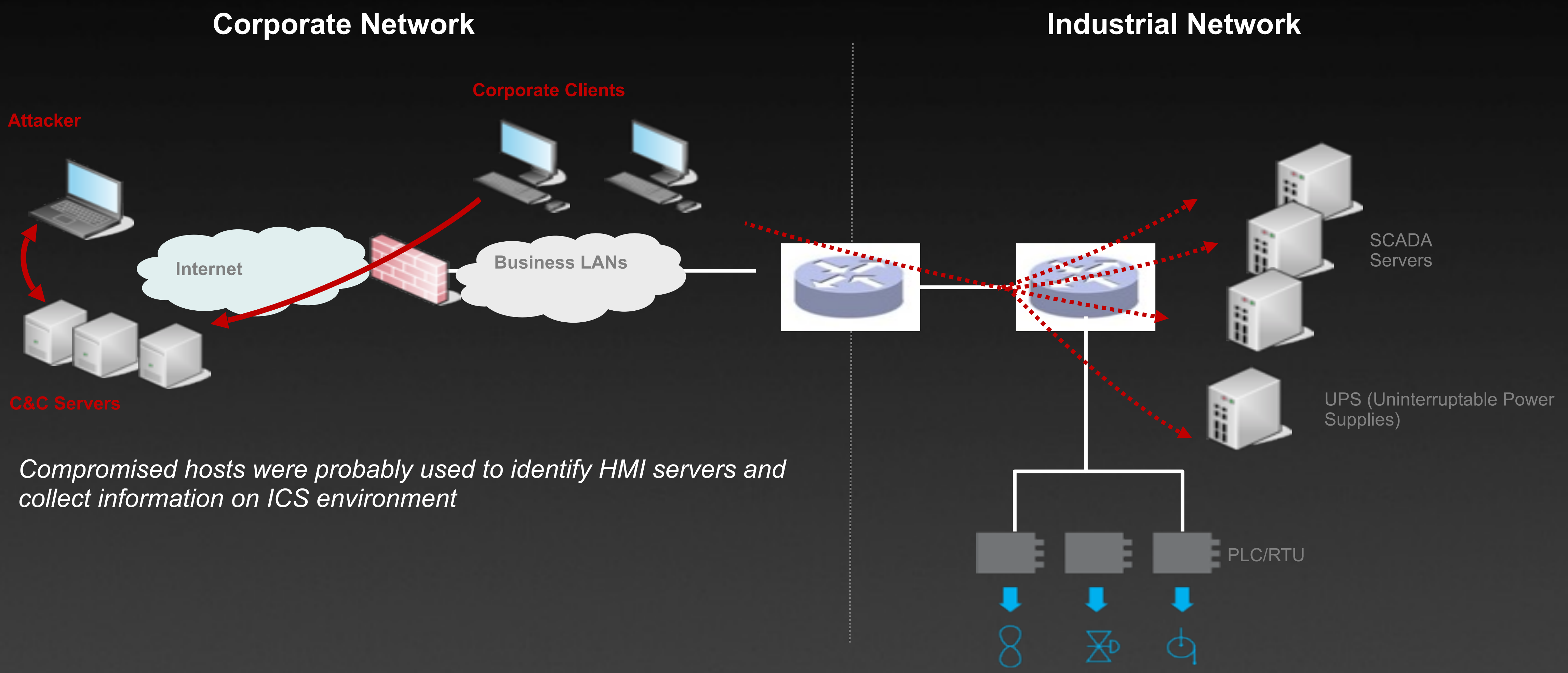
Приклад

2. Information Gathering



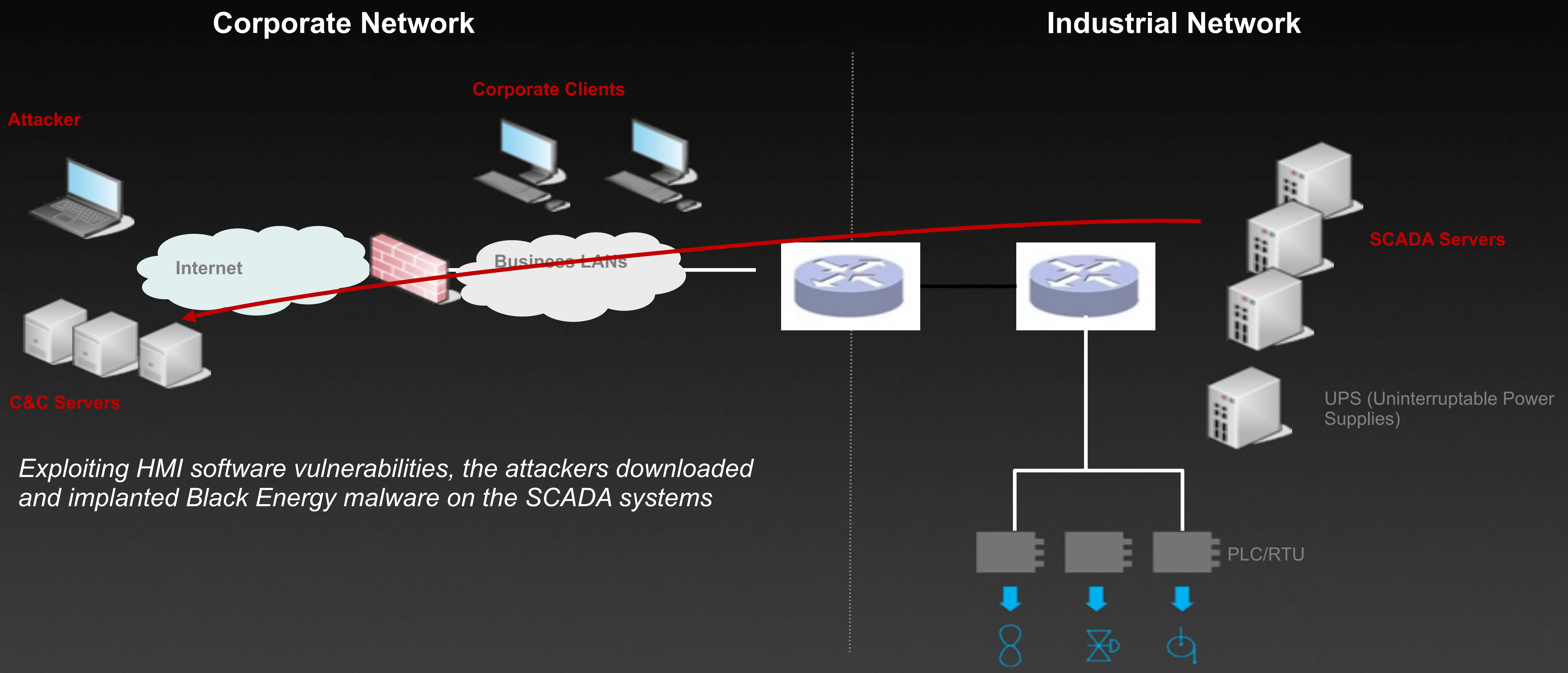
The victims, successfully tricked, executed malicious code to interact with remote Command and Control (C&C) servers. System information was sent to C&C servers, and was used by attackers to gather additional information about targets. Ultimate goal was to execute commands on the victim's hosts or to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

3. Lateral Movement



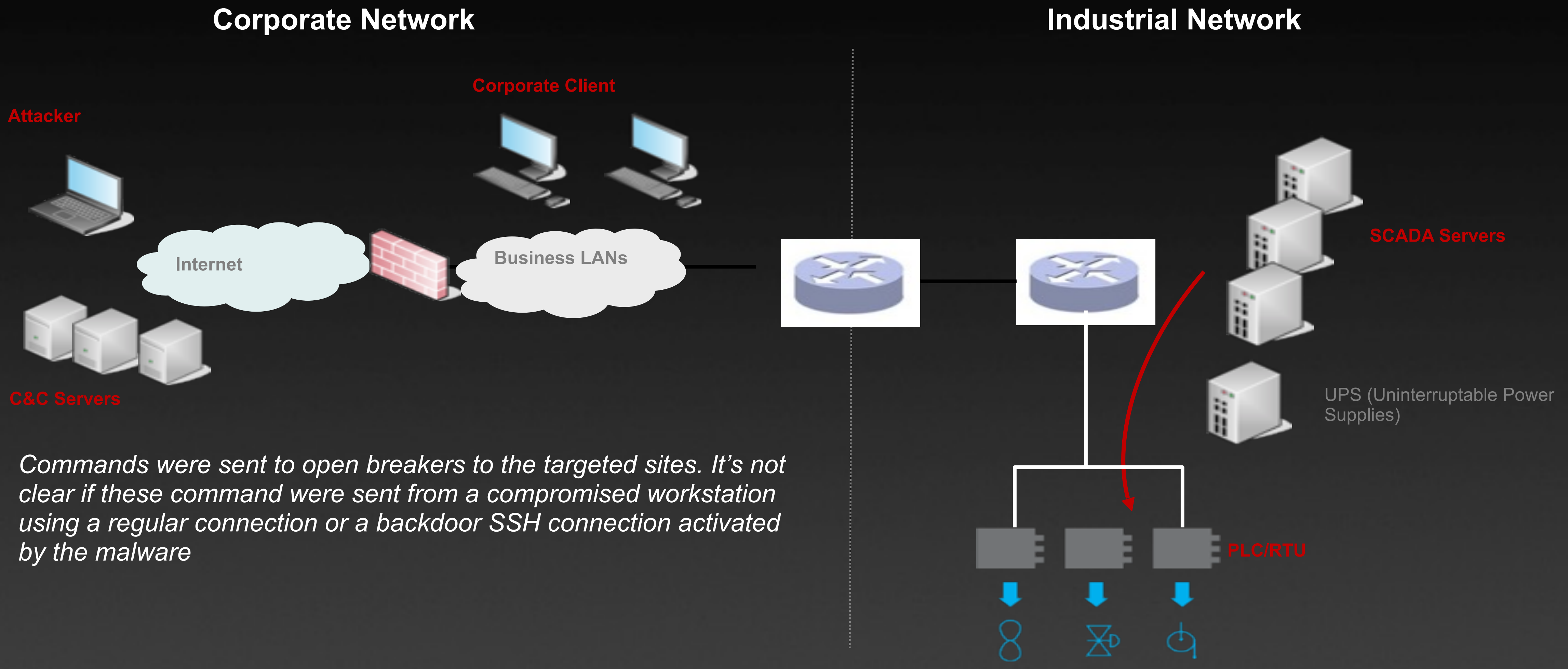
Compromised hosts were probably used to identify HMI servers and collect information on ICS environment

4. SCADA Infiltration



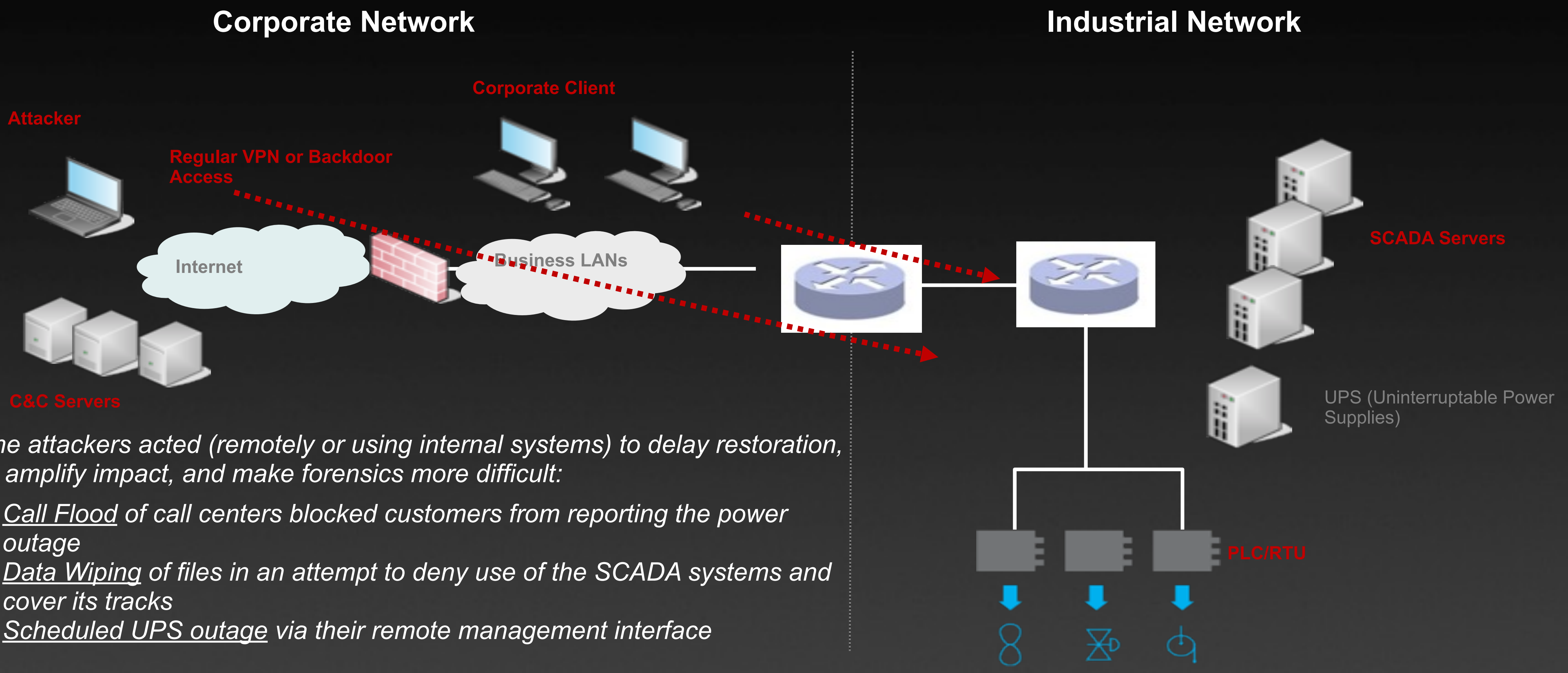
Exploiting HMI software vulnerabilities, the attackers downloaded and implanted Black Energy malware on the SCADA systems

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

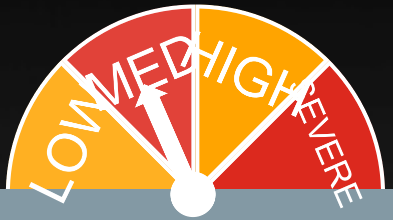


The attackers acted (remotely or using internal systems) to delay restoration, to amplify impact, and make forensics more difficult:

- *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*

Delivery

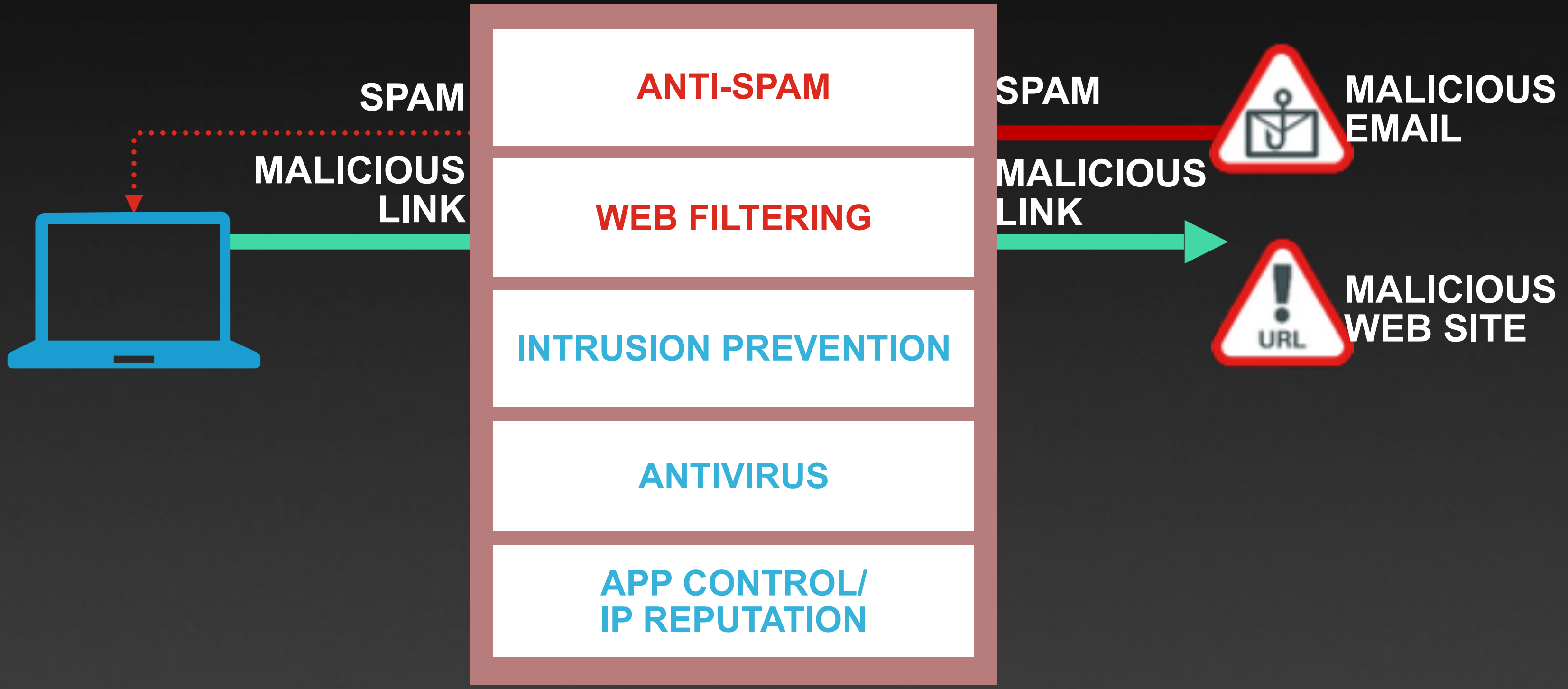
Goal: Choose the best delivery mechanism as possible to deliver the exploit.



SOCIAL ENGINEERING / PHISHING

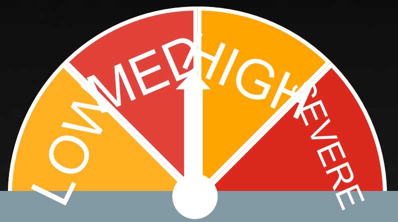
DRIVE-BY-MALWARE (WEBSITE)

MALVERTISING



Exploitation

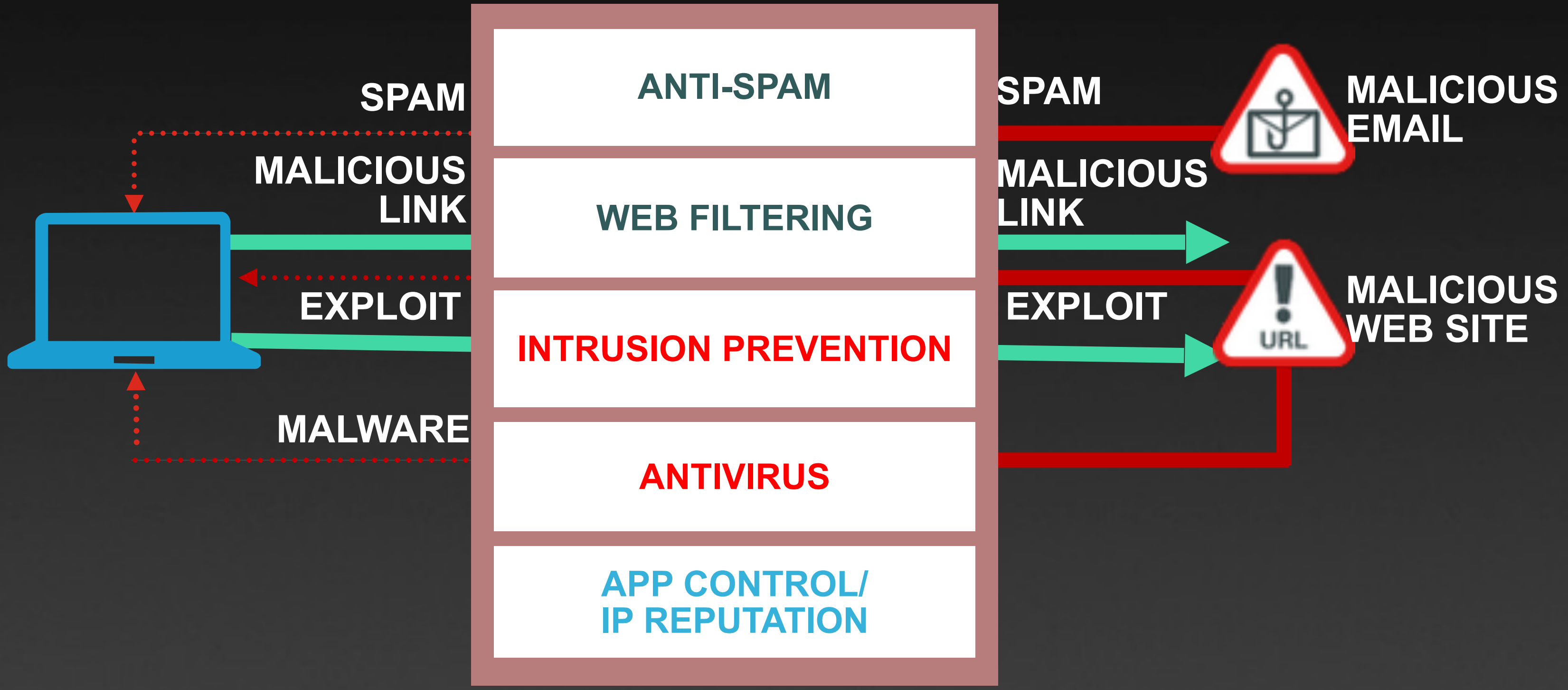
Goal: Successful, stable exploitation of the system without being detected.



BROWSER PLUGINS – FLASH, JAVA

MALICIOUS ADOBE

OFFICE DOCUMENTS - MACROS


SPAM

MALICIOUS LINK

EXPLOIT

MALWARE

ANTI-SPAM

WEB FILTERING

INTRUSION PREVENTION

ANTIVIRUS

APP CONTROL/ IP REPUTATION

SPAM

MALICIOUS LINK

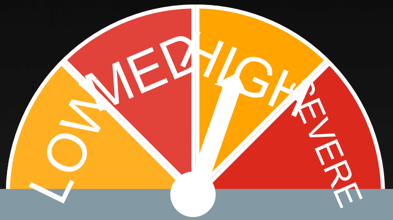
EXPLOIT

MALICIOUS EMAIL

MALICIOUS WEB SITE

Command and Control

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



DNS TUNNELING

TUNNELING USING ICMP, TOR, ETC

FAST FLUX

SPAM
ANTI-SPAM
MALICIOUS LINK
WEB FILTERING
INTRUSION PREVENTION
MALWARE
IP REPUTATION
ALICIOUS
MAIL
ALICIOUS
EB SITE
MMAND
CONTROL
ENTER

Identity&Access Management

Security Information and Event Management (SIEM)

Cyber Threat Assesment Program

FORTINET

csr_sales@fortinet.com