Cybersecurity (Security+) and P4 Programmable Switches

Social Engineering Attacks

Elie Kfoury, Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 20th, 2023

Outline

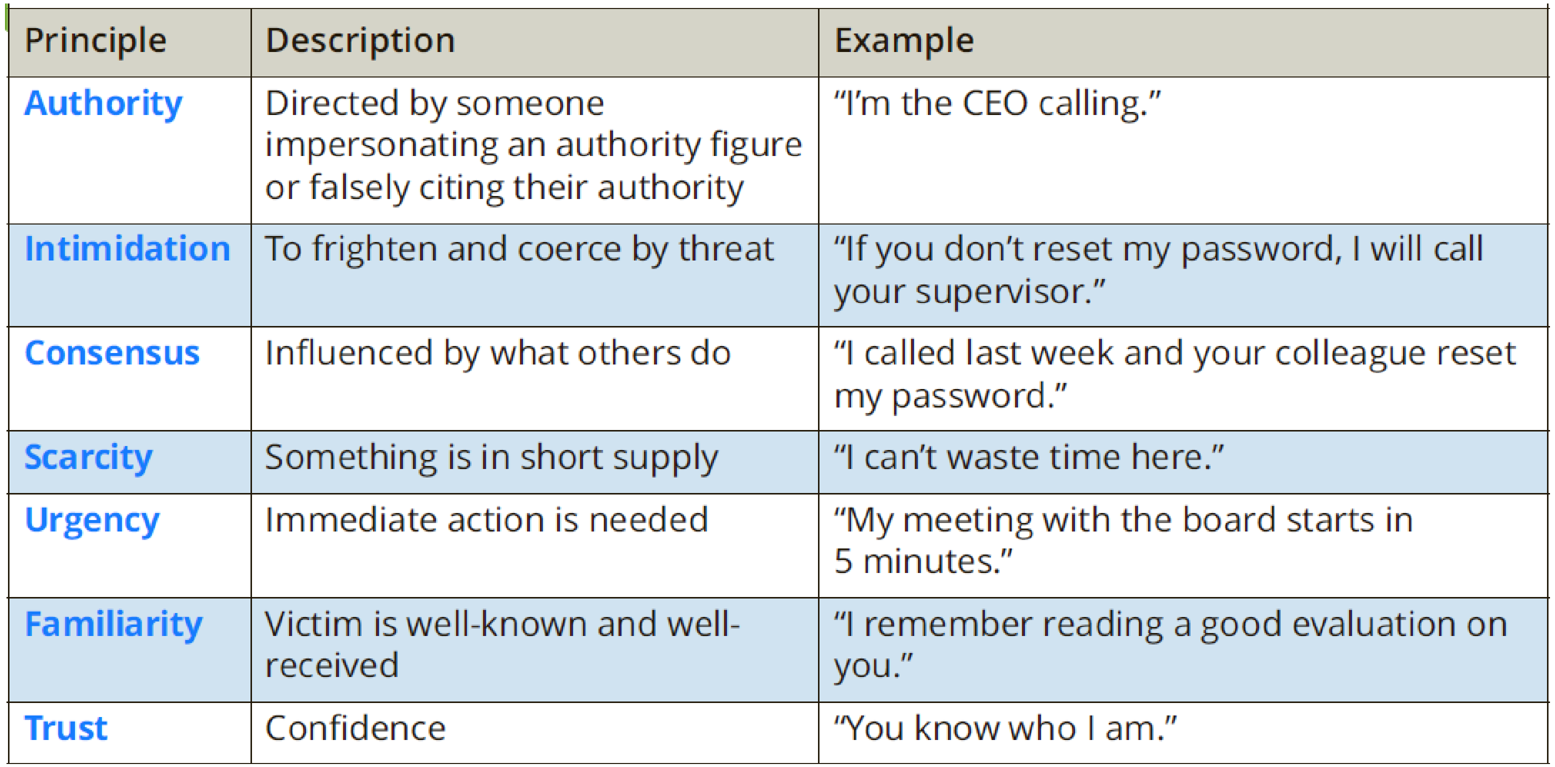
- Social engineering attacks definition
- Social engineering techniques
- Phishing emails
- Credentials harvesting
- Reverse shell

Social Engineering

- Technology is not always needed for attacks on IT
- Social engineering gathers information by relying on the weaknesses of individuals
- It relies on the psychological approaches to persuade a victim

Social Engineering

- Technology is not always needed for attacks on IT
- Social engineering gathers information by relying on the weaknesses of individuals
- It relies on the psychological approaches to persuade a victim



Principle	Description	Example
Authority	Directed by someone impersonating an authority figure or falsely citing their authority	"I'm the CEO calling."
Intimidation	To frighten and coerce by threat	"If you don't reset my password, I will call your supervisor."
Consensus	Influenced by what others do	"I called last week and your colleague reset my password."
Scarcity	Something is in short supply	"I can't waste time here."
Urgency	Immediate action is needed	"My meeting with the board starts in 5 minutes."
Familiarity	Victim is well-known and well-received	"I remember reading a good evaluation on you."
Trust	Confidence	"You know who I am."

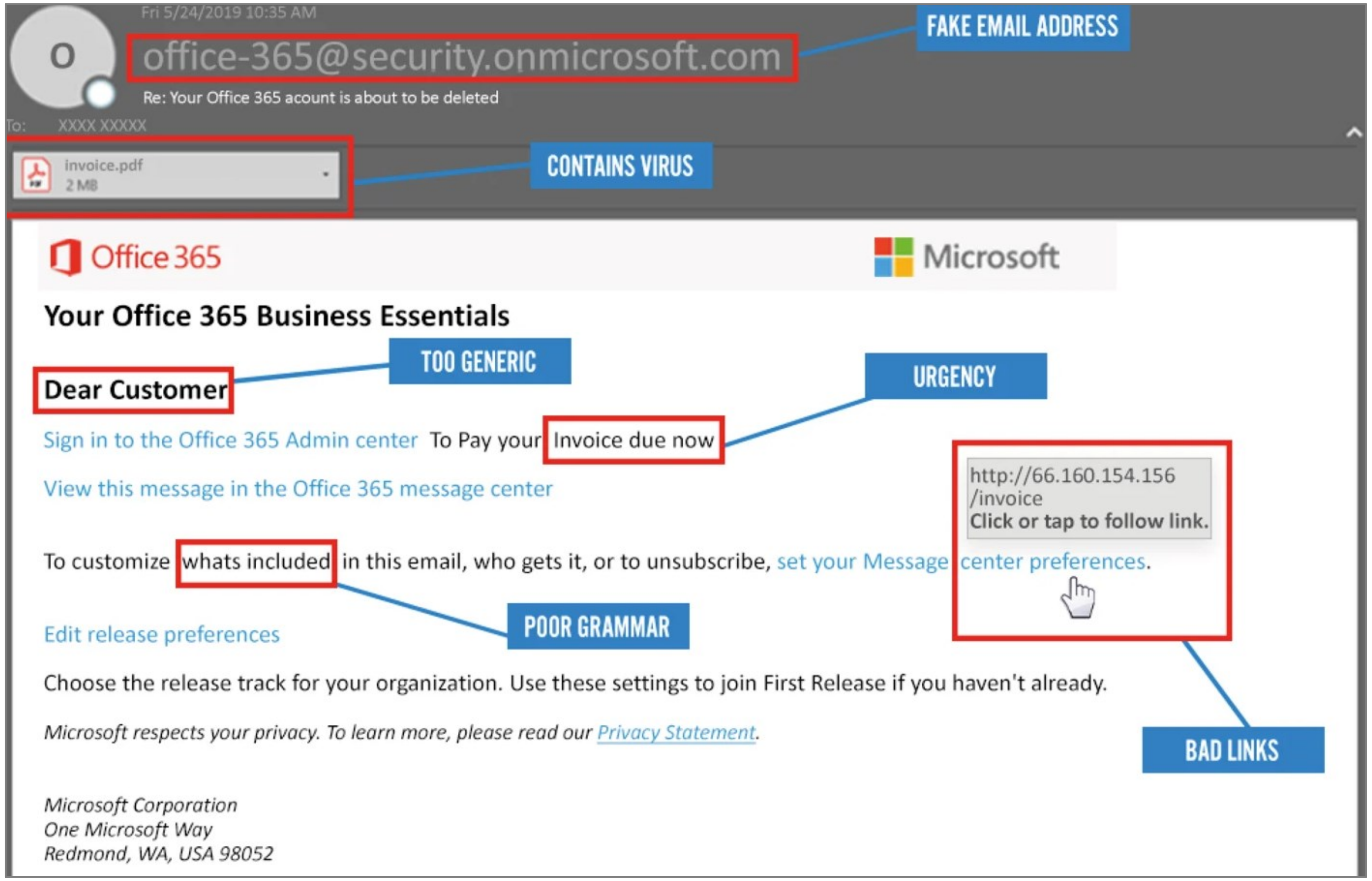
Ciampa, Mark. *CompTIA security+ guide to network security fundamentals*. Cengage Learning, 2021.

Social Engineering

- Impersonation
  - Masquerade as a real or fictitious character
  - Play out the role of that person on a victim
  - Impersonated parties include IT support, manager, trusted third party
- Phishing
  - Sending (millions) email claiming to be from legitimate source
  - Trick user into giving private info: password, credit card number, etc.
- Variation of phishing attacks
  - Pharming: automatically redirects the user to the fake site
  - Spear phishing: targets only specific users; emails are customized
  - Whaling: spear phishing targeting “big fish,” (wealthy individuals)
  - Vishing: Instead of using email, a phone call can be used instead (voice phishing)

Phishing Emails

- Phishing emails are hard to distinguish from legitimate ones
- Attacker uses logos and colors identical to those provided by a legitimate entity



Fri 5/24/2019 10:35 AM

office-365@security.onmicrosoft.com

Re: Your Office 365 acount is about to be deleted

To: XXXX XXXXX

invoice.pdf
2 MB

Office 365 Microsoft

Your Office 365 Business Essentials

Dear Customer

Sign in to the Office 365 Admin center To Pay your Invoice due now

View this message in the Office 365 message center

http://66.160.154.156/invoice
Click or tap to follow link.

To customize whats included in this email, who gets it, or to unsubscribe, set your Message center preferences.

Edit release preferences

Choose the release track for your organization. Use these settings to join First Release if you haven't already.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

Microsoft Corporation
One Microsoft Way
Redmond, WA, USA 98052

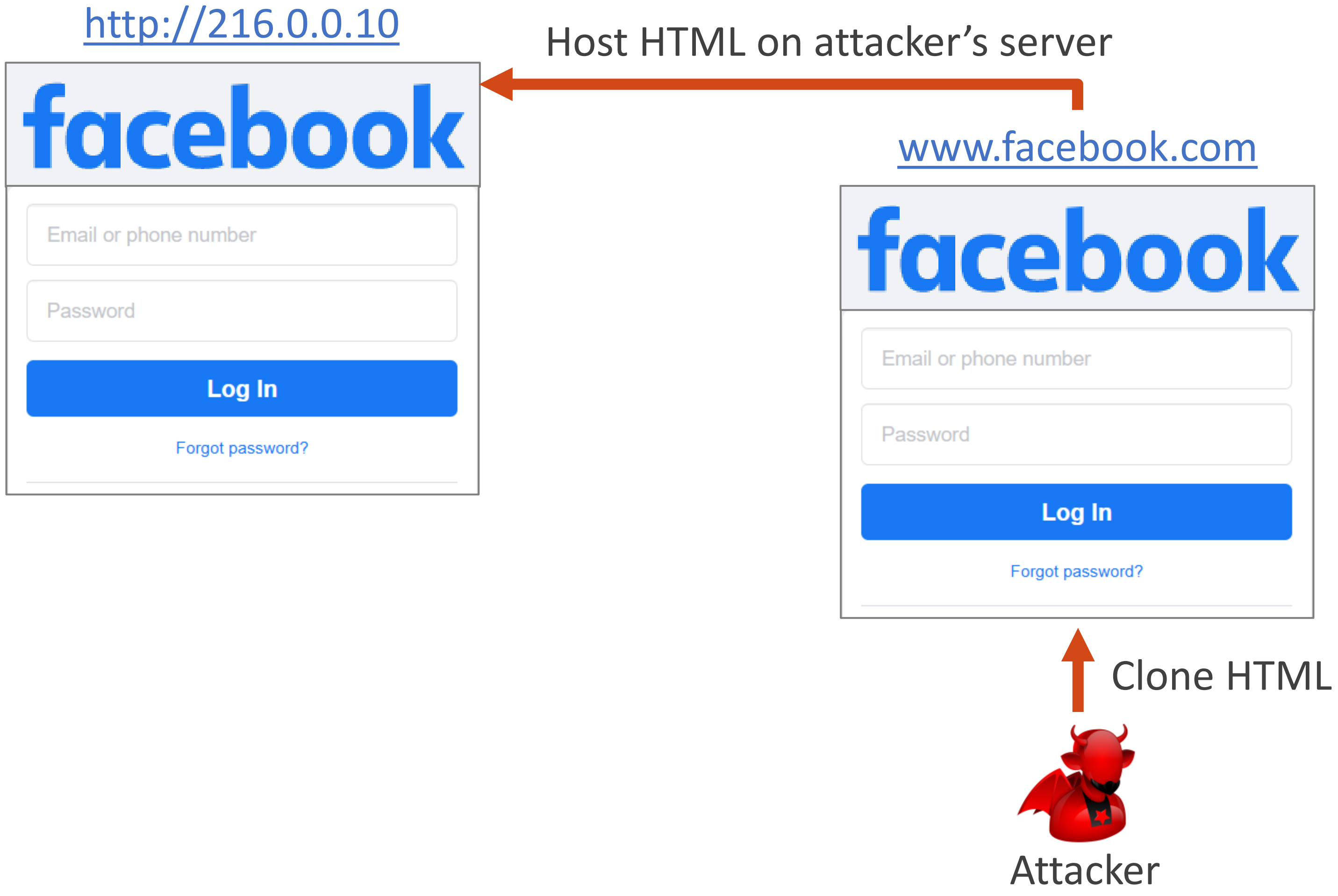
https://www.newcmi.com/blog/tips-for-detecting-a-phishing-email

Credentials Harvesting

- Gathering sensitive user credentials, such as usernames and passwords, with the intent of unauthorized access to systems or accounts

Credentials Harvesting

- Gathering sensitive user credentials, such as usernames and passwords, with the intent of unauthorized access to systems or accounts



http://216.0.0.10

Host HTML on attacker’s server

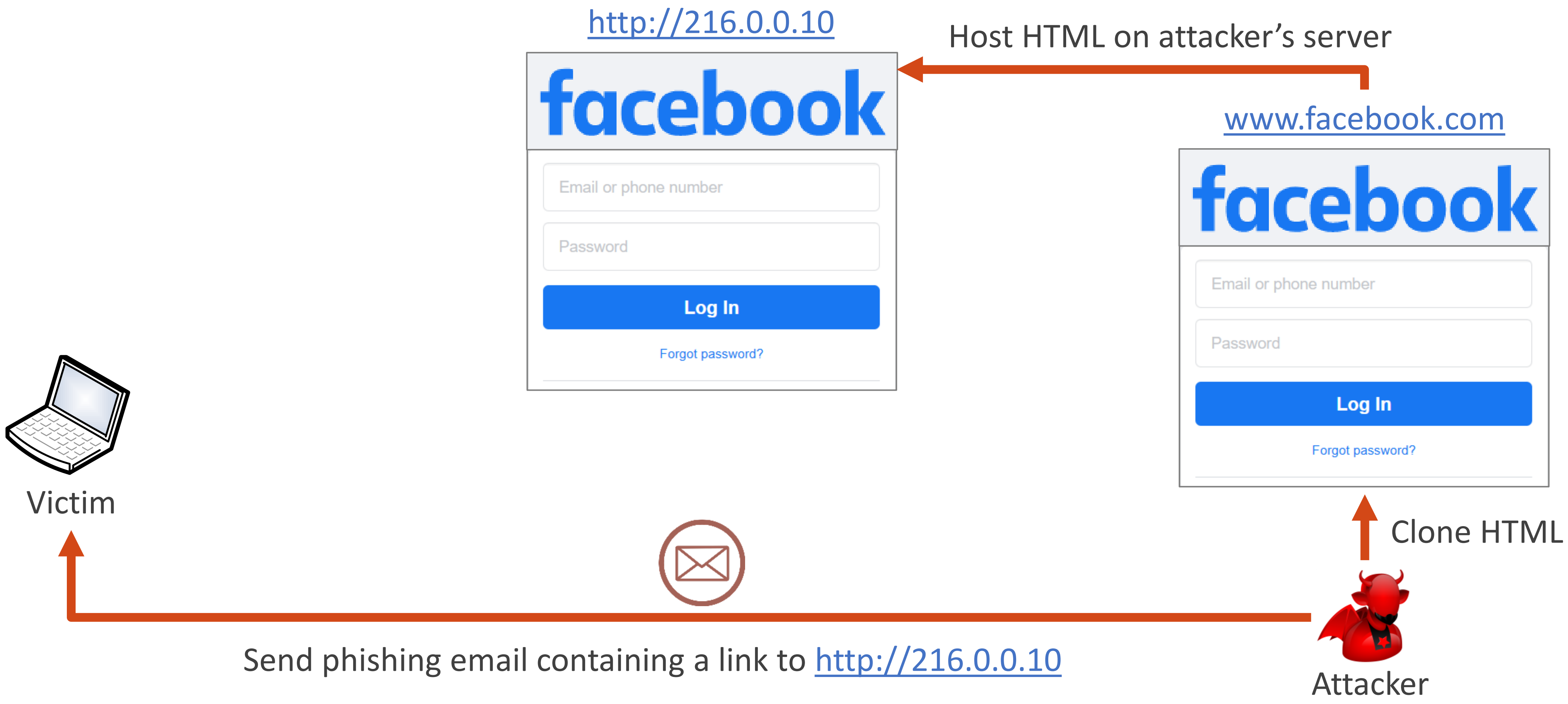
www.facebook.com

Clone HTML

Attacker

Credentials Harvesting

- Gathering sensitive user credentials, such as usernames and passwords, with the intent of unauthorized access to systems or accounts



http://216.0.0.10

Host HTML on attacker’s server

www.facebook.com

Clone HTML

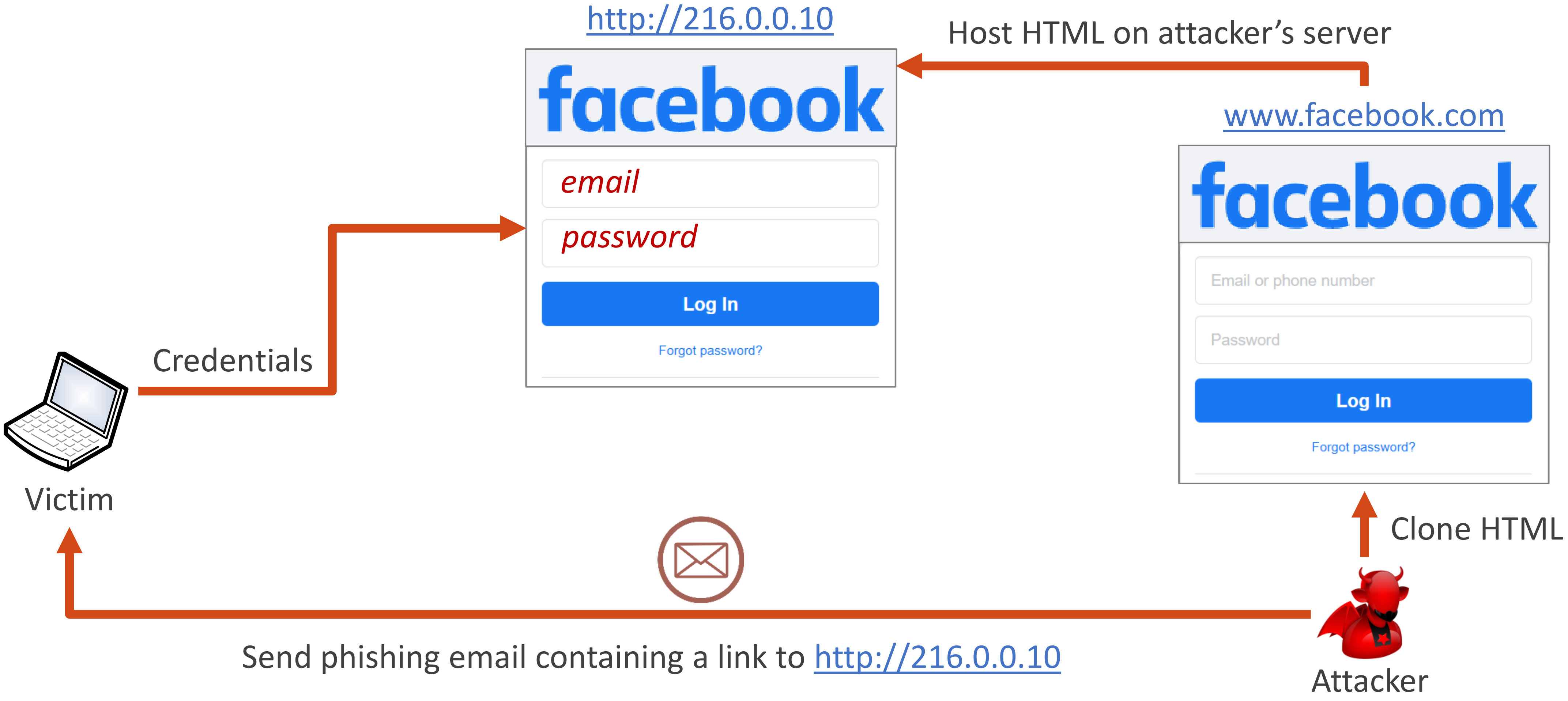
Victim

Send phishing email containing a link to http://216.0.0.10

Attacker

Credentials Harvesting

- Gathering sensitive user credentials, such as usernames and passwords, with the intent of unauthorized access to systems or accounts



http://216.0.0.10

Host HTML on attacker's server

www.facebook.com

Credentials

Victim

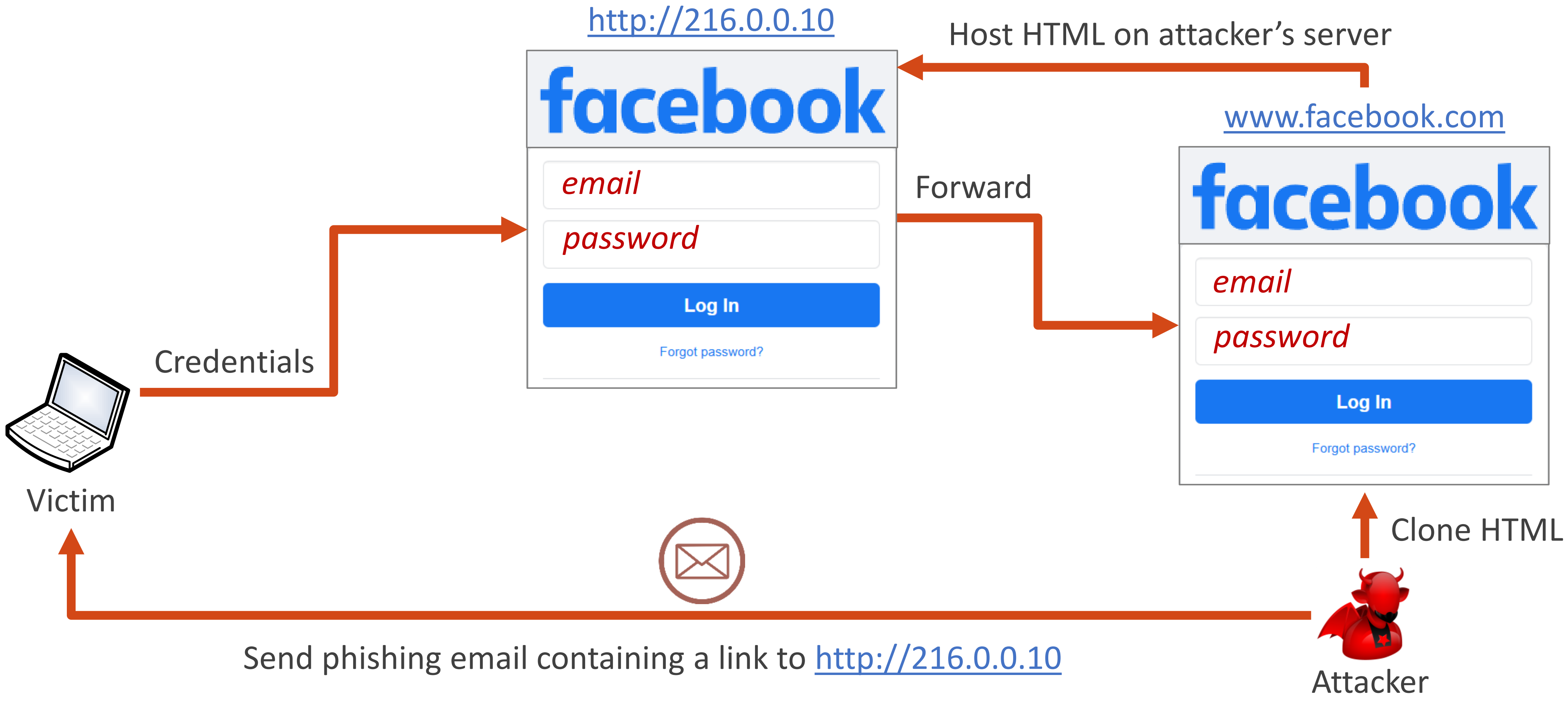
Clone HTML

Send phishing email containing a link to http://216.0.0.10

Attacker

Credentials Harvesting

- Gathering sensitive user credentials, such as usernames and passwords, with the intent of unauthorized access to systems or accounts



http://216.0.0.10

facebook

email

password

Log In

Forgot password?

Host HTML on attacker's server

www.facebook.com

facebook

email

password

Log In

Forgot password?

Forward

Credentials

Victim

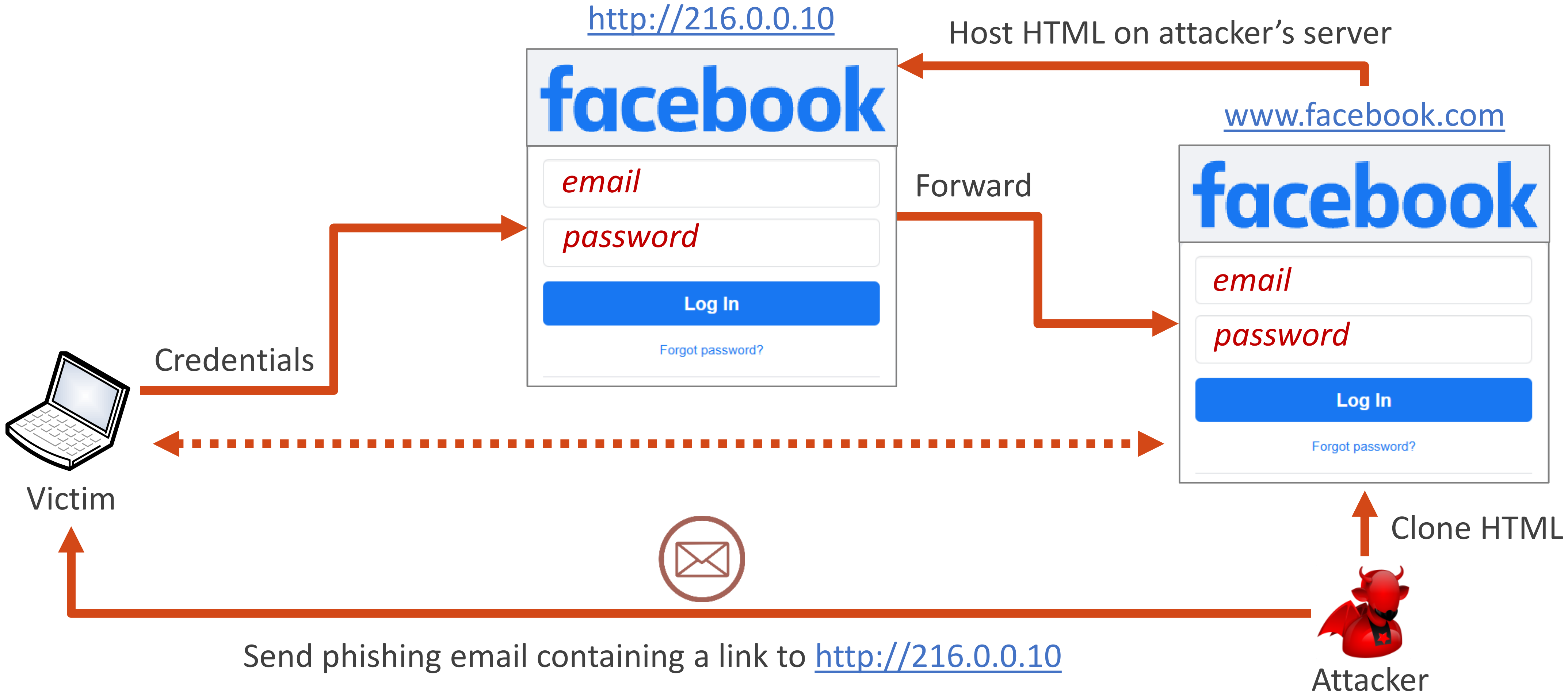
Clone HTML

Attacker

Send phishing email containing a link to http://216.0.0.10

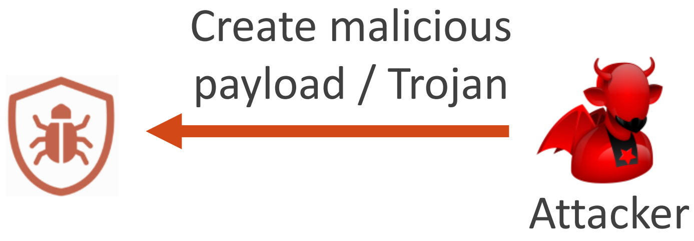
Credentials Harvesting

- Gathering sensitive user credentials, such as usernames and passwords, with the intent of unauthorized access to systems or accounts



Reverse Shell

- Attacker establishes a connection from the victim to their own system
- Gain full shell access to the victim’s machine

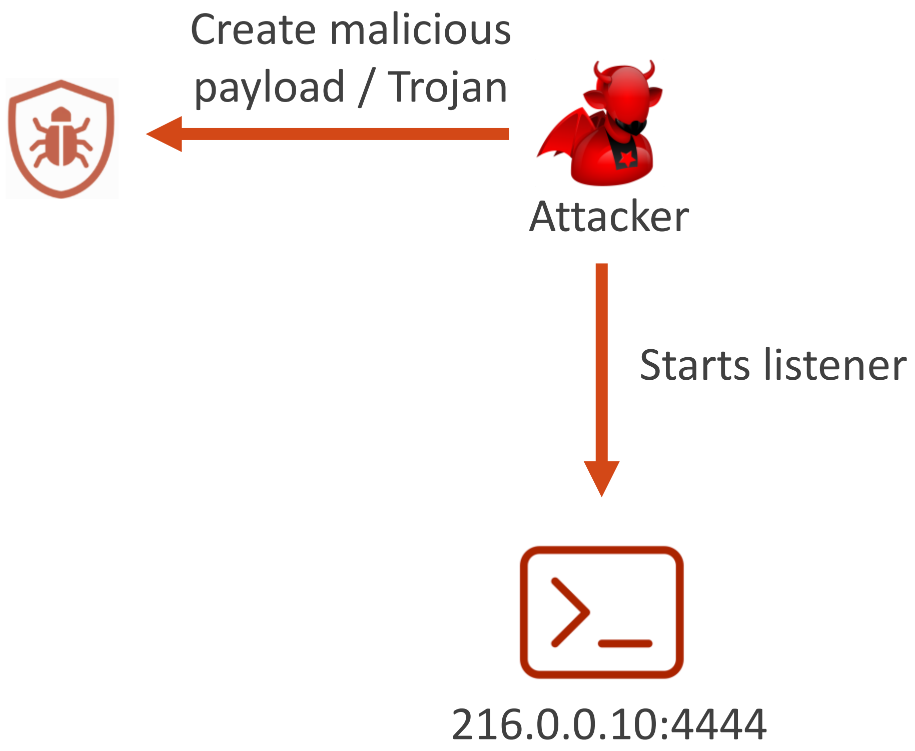


Create malicious payload / Trojan

Attacker

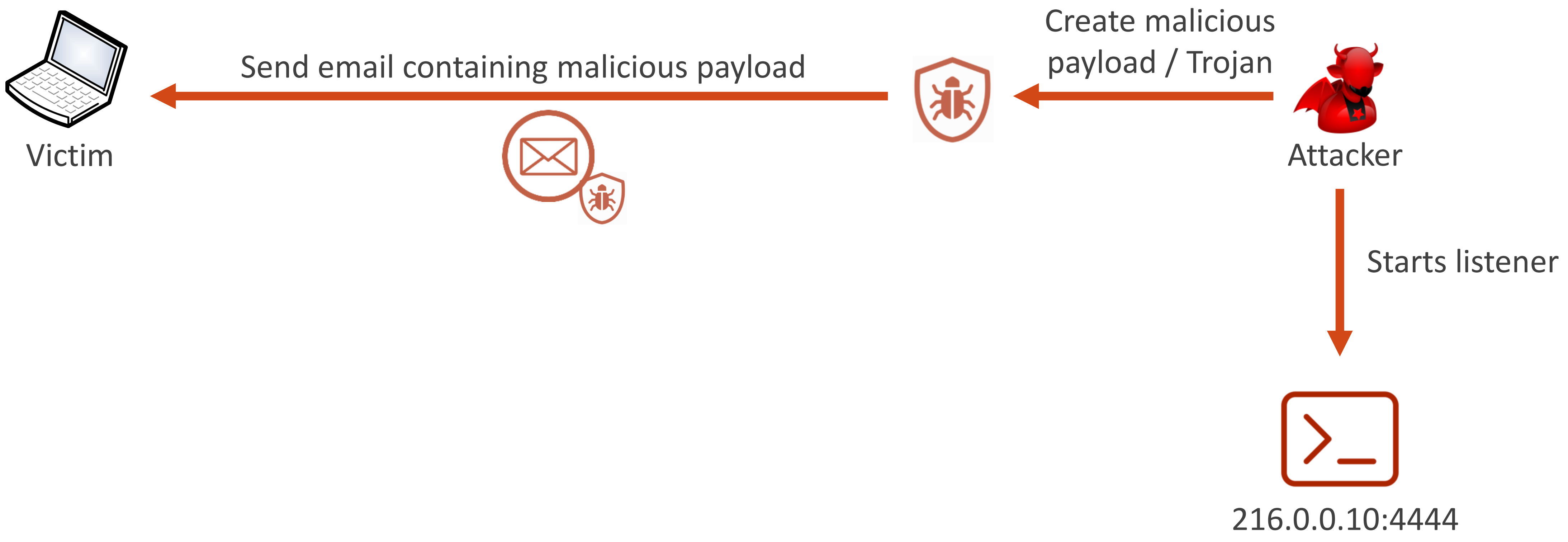
Reverse Shell

- Attacker establishes a connection from the victim to their own system
- Gain full shell access to the victim's machine



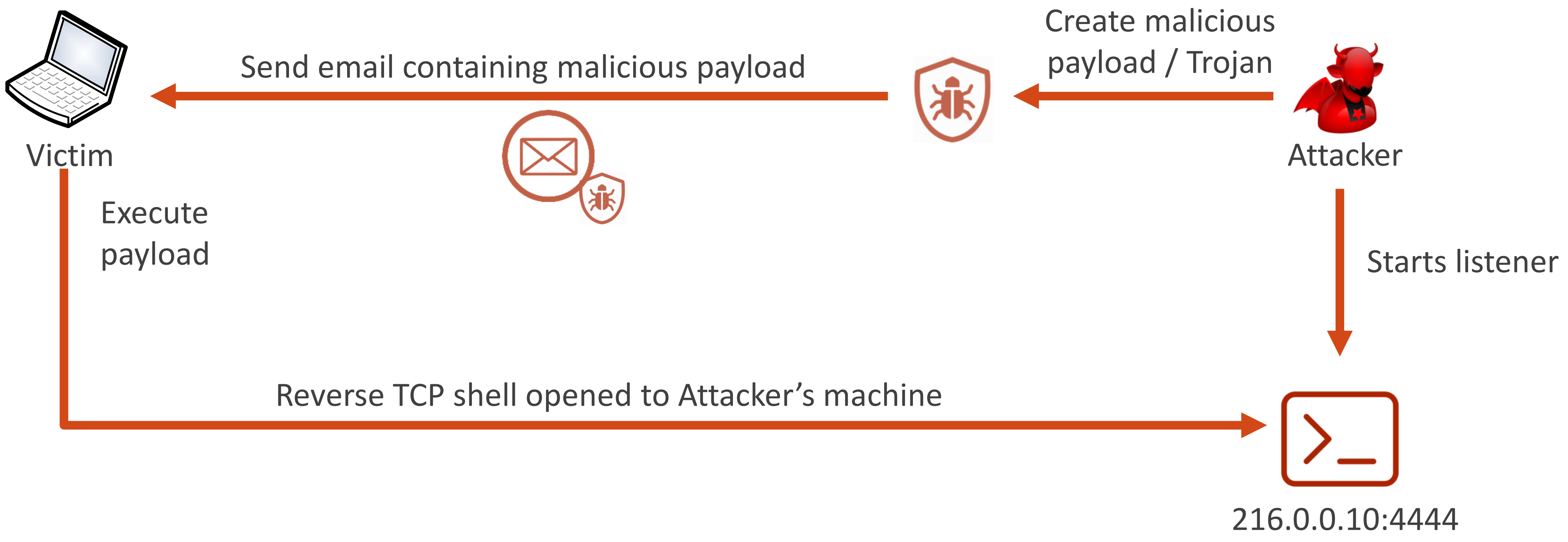
Reverse Shell

- Attacker establishes a connection from the victim to their own system
- Gain full shell access to the victim's machine


Create malicious payload / Trojan
Send email containing malicious payload
Victim
Attacker
Starts listener
216.0.0.10:4444

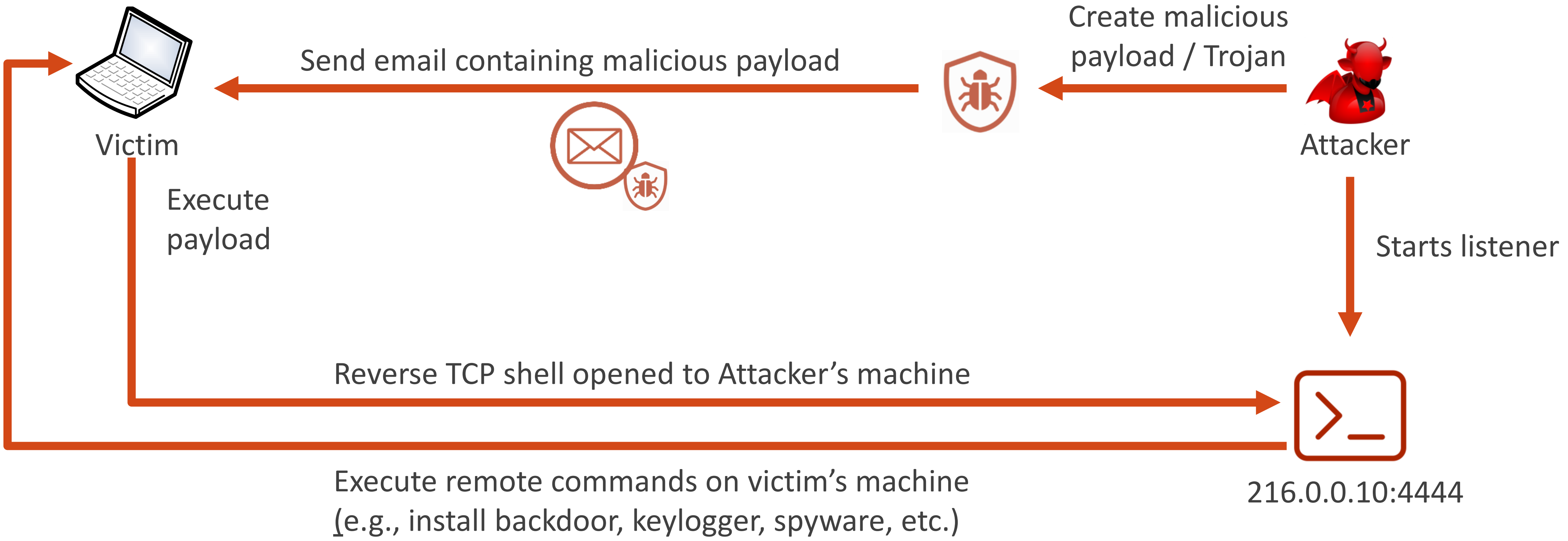
Reverse Shell

- Attacker establishes a connection from the victim to their own system
- Gain full shell access to the victim's machine


Create malicious payload / Trojan
Send email containing malicious payload
Victim
Attacker
Execute payload
Starts listener
Reverse TCP shell opened to Attacker's machine
216.0.0.10:4444

Reverse Shell

- Attacker establishes a connection from the victim to their own system
- Gain full shell access to the victim's machine


Create malicious
payload / Trojan
Send email containing malicious payload
Victim
Attacker
Execute
payload
Starts listener
Reverse TCP shell opened to Attacker's machine
Execute remote commands on victim's machine
(e.g., install backdoor, keylogger, spyware, etc.)
216.0.0.10:4444