QOMPLX:CYBER

Attacker Scenario: How to Mitigate, Detect, and Respond

Rob Saland, Vertical Sales Director, Americas

January 2022

Attacker Scenario

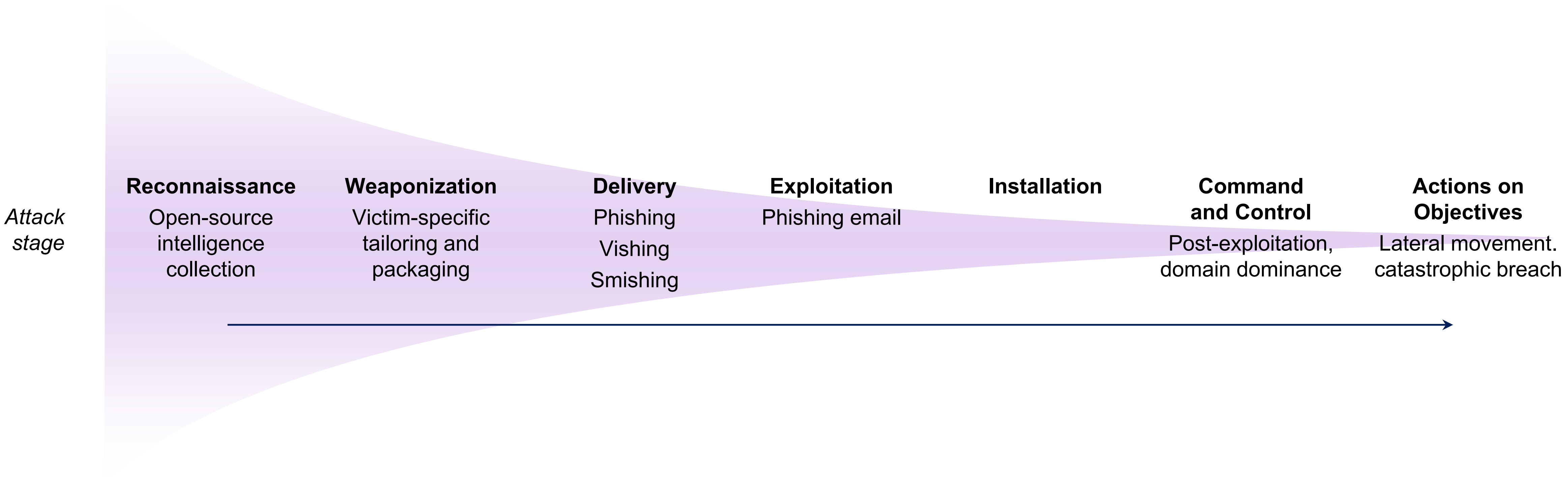
- A litigator is concluding a case and making arrangements to bring into his trust account by wire transfer settlement funds from an international entity with a bank account in Europe.
- Wire data is shared. Funds eventually are received and await distribution.
- In preparing for distribution, the lawyer realizes he has not received emails about the matter from persons he had been dealing with.
- Thinking there is something wrong with his Microsoft 365 account, he asks his IT contractor to see what's going on.
- His IT contractor determines that, at the time he was arranging for the wire transfer, a bad actor invaded his system and, in Outlook, set up a folder along with a rule to divert all emails that contained the term settlement, funds, distribution, interest, resolve and other items tied to the specific representation such as party names. The missing emails had been diverted to this folder setup by the bad actor.

Let’s Break It Down

- An attacker does not intervene at the precise time of a wire transfer; they dwell and wait for the opportune time to strike
- This attack is right in line with the typical playbook: they get in, elevate privilege, move laterally, forge credentials, and persist as a legitimate user; they are “trusted” on the network layer
- This “legitimate user” has the credentials, and thus privileges, to view/access whatever they want -- i.e. an O365 account -- without raising any red flags
- Network persistence allows attackers to live off the land for extended periods of time remaining undetected
- During this dwell time, attackers lay their ground work -- i.e. in this case setting up email parameters for diversion -- without making any noise
- Now, the trap is set and the attacker is gone without a trace before the nefarious event actually takes place

What attackers do

Defenders must think like attackers do: know what weaknesses they will exploit. Stop them before they achieve their most important intermediate objective: *elevating access* , so they can do anything they want.



Attack stage

Reconnaissance
Open-source intelligence collection

Weaponization
Victim-specific tailoring and packaging

Delivery
Phishing
Vishing
Smishing

Exploitation
Phishing email

Installation

Command and Control
Post-exploitation, domain dominance

Actions on Objectives
Lateral movement. catastrophic breach

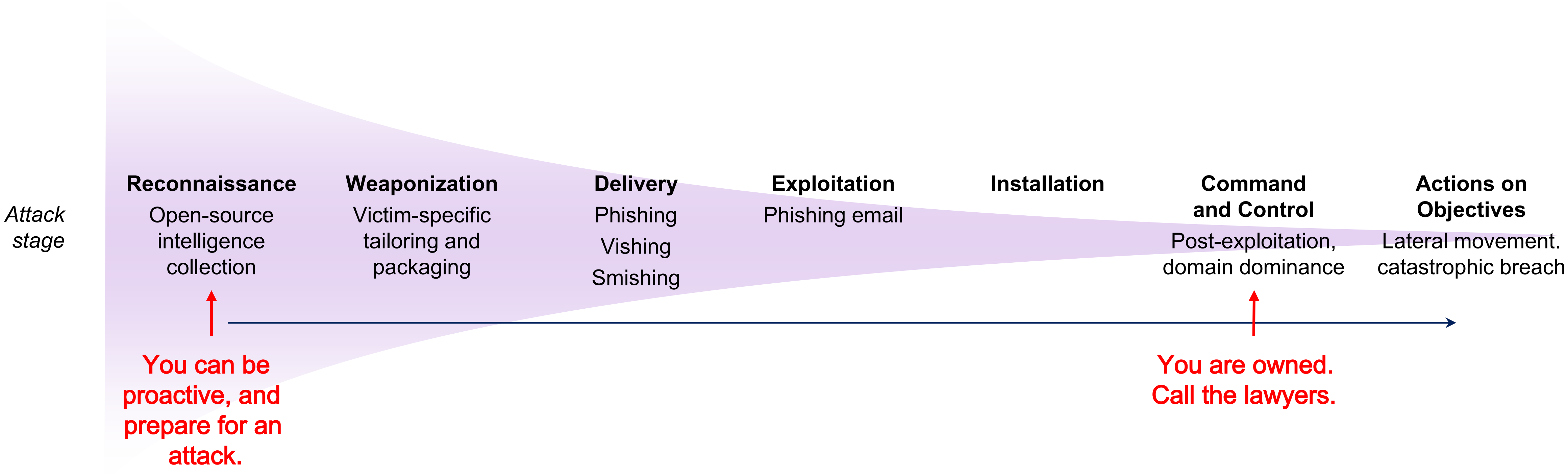
Long time horizon, many options

The Cyber Kill Chain

No time, few options

What attackers do

Defenders must think like attackers do: know what weaknesses they will exploit. Stop them before they achieve their most important intermediate objective: *elevating access* , so they can do anything they want.



Attack stage

Reconnaissance
Open-source intelligence collection

Weaponization
Victim-specific tailoring and packaging

Delivery
Phishing
Vishing
Smishing

Exploitation
Phishing email

Installation

Command and Control
Post-exploitation, domain dominance

Actions on Objectives
Lateral movement. catastrophic breach

You can be proactive, and prepare for an attack.

You are owned. Call the lawyers.

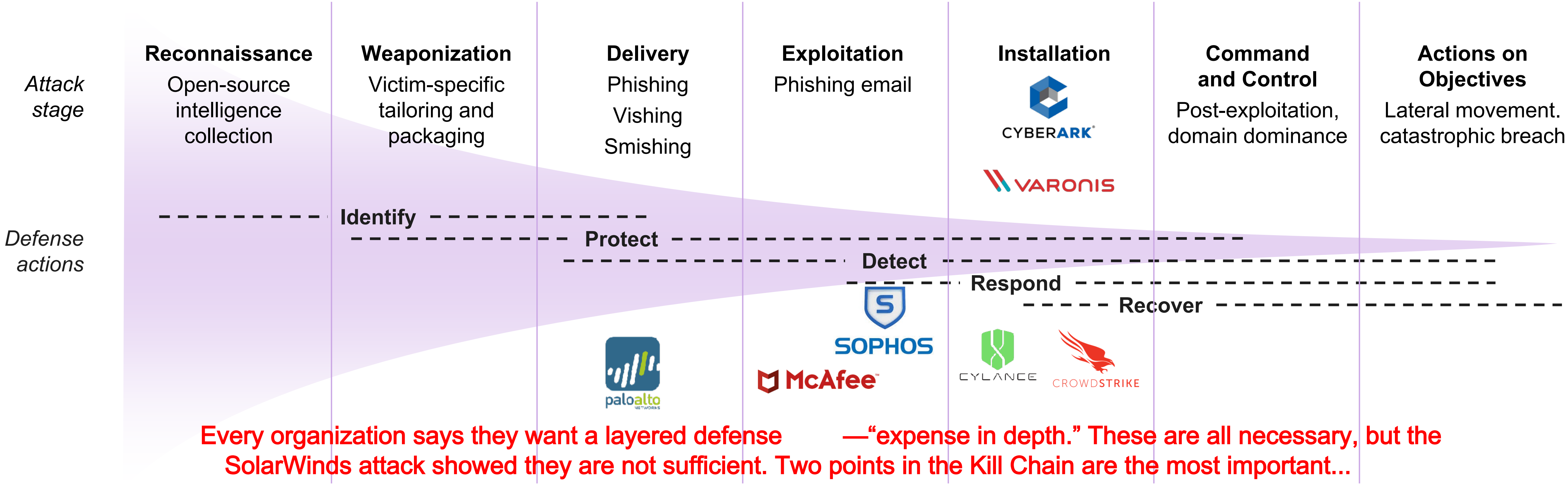
Long time horizon, many options

The Cyber Kill Chain

No time, few options

What defenders *try* to do

Defenders must think like attackers do: know what weaknesses they will exploit. Stop them before they achieve their most important intermediate objective: *elevating access* , so they can do anything they want.



	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Actions on Objectives
Attack stage	Open-source intelligence collection	Victim-specific tailoring and packaging	Phishing Vishing Smishing	Phishing email		Post-exploitation, domain dominance	Lateral movement. catastrophic breach

Defense actions

Identify

Protect

Detect

Respond

Recover

Every organization says they want a layered defense —"expense in depth." These are all necessary, but the SolarWinds attack showed they are not sufficient. Two points in the Kill Chain are the most important...

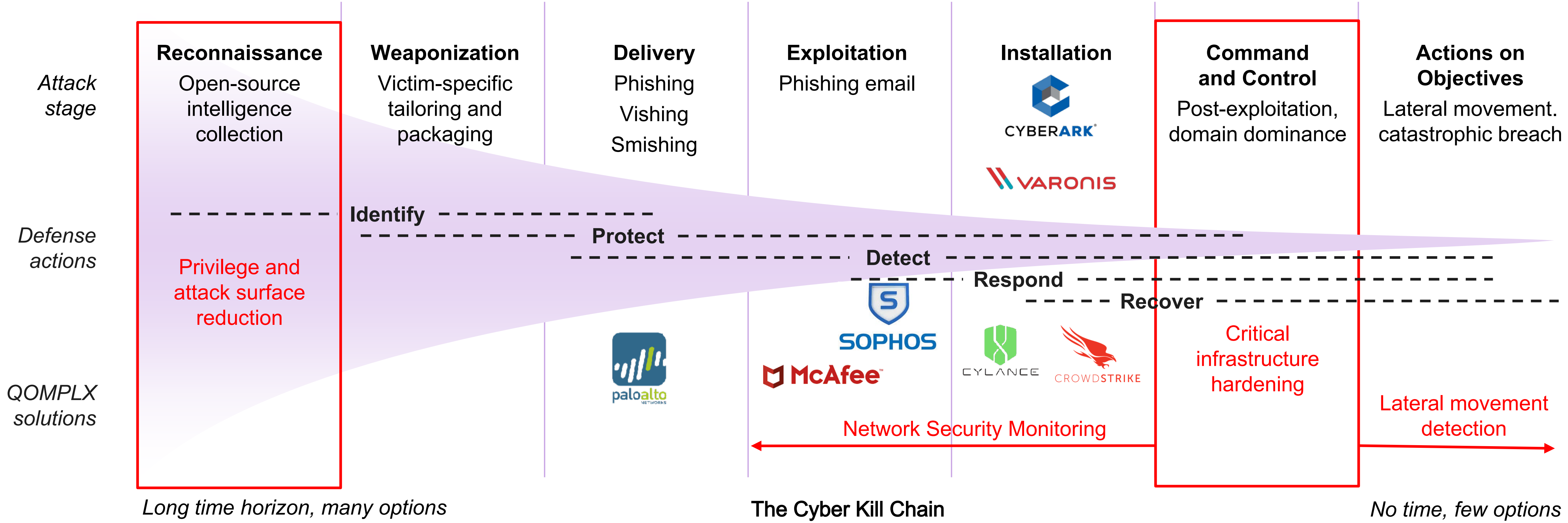
Long time horizon, many options

The Cyber Kill Chain

No time, few options

Disrupt the attacker playbook

Identify and reduce attack surfaces well before a breach. Validate that every log -in is what it claims to be, thus avoiding abuse of command and control.



	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Actions on Objectives
Attack stage	Open-source intelligence collection	Victim-specific tailoring and packaging	Phishing Vishing Smishing	Phishing email		Post-exploitation, domain dominance	Lateral movement. catastrophic breach

Defense actions

Identify

Protect

Detect

Respond

Recover

QOMPLX solutions

Privilege and attack surface reduction

Network Security Monitoring

Critical infrastructure hardening

Lateral movement detection

Long time horizon, many options

The Cyber Kill Chain

No time, few options

Step 1: Harden Your External Network

- Follow proper hygiene and best practices (NIST, ISO, etc.) to make your firm a hard and unattractive target
- Password best practices (NIST framework): 16 characters+, more complex = better, no reuse of passwords

  **Password managers make adherence easy and there are both commercial (1Password, LastPass, etc.) and free (Keepass, Lastpass, etc) available*

- Enable MFA on every account that supports it: security keys which requires physical possession of the key for user log-in; security tokens like Google authenticator or duo which requires a time-boxed one time password as a 2nd form of authentication

  **Do not store sensitive information where MFA is not enabled*

- Monitor external network posture: Native, open-source and commercial tools exist to monitor the most common external exploitation vectors: domains, subdomains, DNS records, DMARC, SPF, zone transfers, open ports, exposed services, TLS certificate health, malware indicators, etc.

  **Zero tolerance for highly-targeted services on Internet-facing Windows servers, such as RDP*

  **Kill any out-of-support, non-patchable Windows OS's (Windows <= 7, Windows Server <= 2008)*

- Encrypt data in transit: Use VPN solutions for End-to-end encryption to make it difficult for a threat actor to eavesdrop on network traffic

  **Both the Freedom Press Foundation and Electronic Frontier Foundation have extensive guides for choosing the right VPN*

- Threat actors will commonly reuse credentials in an attempt to gain access without detection: scan the open web for leaked credentials (i.e. passwords, etc.) tied to firm employees. Again, both open source and commercially available tools for this exist
- Perform regular software and hardware updates, as well as penetration testing exercises

Step 2: Implement Detection Methods

- Phishing is amongst the most common vectors to gain a foothold in a network of any size; counter phishing measures include:

  *It’s possible for advanced attackers to spoof emails from legitimate sources or even compromise one of your associate’s accounts to launch an attack on you; be paranoid of every email you receive, especially if you are known to be a target

  *Advanced phishing attacks will be tailored to the target and may look indistinguishable from legitimate emails; never click on links contained in emails. Instead, manually type in the address

  *Trust your instinct. Even if an email appears to be from a trusted source, if it seems “off” then contact that source through some other means to verify it. It doesn’t hurt to pick up the phone and ask for clarification on any odd email.

- Routinely (e.g., weekly) review access logs for anomalies related to date, time, login attempts, and public IP addresses
- For example, some anomalies may include login outside of normal activity hours, failed password attempts, or unusual countries of origin. If an anomaly cannot be explained, then a response plan should be followed
- Consolidate and analyze all network security logs such that any suspicious activity can be identified, investigated, and triaged before the attacker has a chance to strike
- Consider replicating the logs to a secure server or device for anomaly detection and help with future investigations if necessary

Step 3: Implement Response Plans

- Regularly backup any sensitive data that you want to keep including contacts, pictures, and documents. It is critical that back -ups are properly protected with encryption and stored in a location that is physically secure
- Backup data to a dedicated storage device (external hard drive) or consider backing sensitive data to ProtonDrive or Tresorit. Physical storage should be stored in a secure location
- If it’s suspected that unauthorized access to a resource or service has been obtained by a threat actor, then immediately change to a unique password and force log out all other sessions if the application supports it
- As a last resort, there may come a time when replacing all devices and abandoning accounts is recommended
- While the threshold for such an event varies, a security -aware professional should be ready to immediately power off, replace all devices, and transfer no files/information between devices
- Use of all previously used accounts (including usernames and passwords) should also cease
- Managed services such as MDR (managed detection and response) go beyond the traditional MSP or MSSP to support organization’s need to detect and respond to advanced threats

Content Resources

For extensive guides and details regarding any content please visit https://www.qomplx.com/resources/ or contact Rob Saland at rob.saland@qomplx.com

Thank you

QOMPLX
1775 Tysons Boulevard, Suite 800
Tysons, Virginia   22102
703.995.4199
qomplx.com