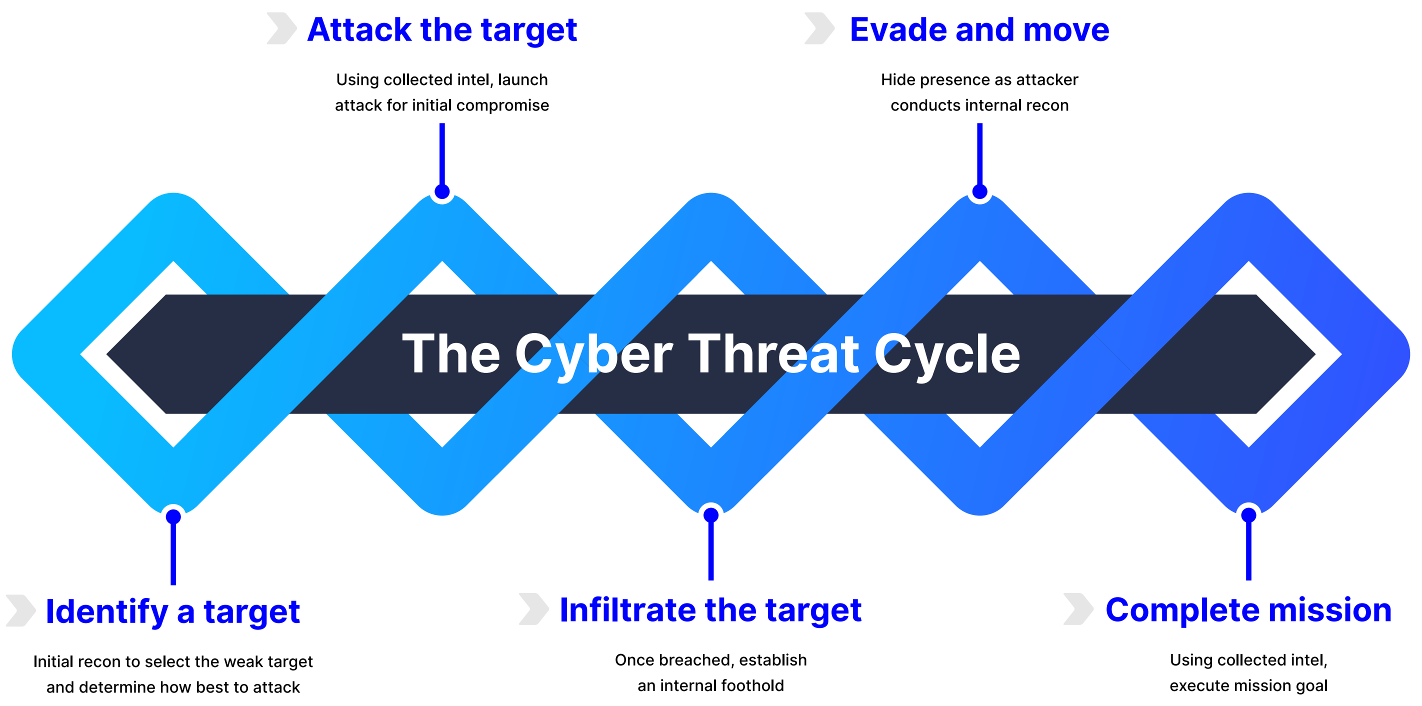
Threat Actors & Your Security Strategy

Cyberattacks making headlines like SolarWinds and Hafnium call into question the scale and sophistication of attacks infiltrating the mailbox. While the headlines may come and go, long term effects of these attacks will be felt across organizations. SolarWinds sites they anticipate 18 months of impact from the attack that all began in an M365 mailbox while the Hafnium attack across on-premise exchange servers enabled access to victim email accounts allowing the installation of added malware that paves the way for long-term access.

While some may think patching is enough ain today's cyber age, addressing the threat lifecycle of bad actors with a simple and proactive security strategy will close 95% of your attack prevention gap.

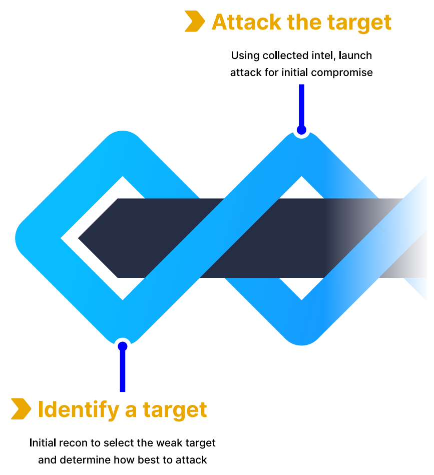
> *"We are sharing this information with our customers and the security community to emphasize the critical nature of these vulnerabilities and the importance of patching all affected systems immediately to protect against these exploits and prevent future abuse across the ecosystem."*
>
> — Microsoft Threat Intelligence Center

LET'S BREAKDOWN THE CYCLE



Attack the target
Using collected intel, launch attack for initial compromise
Evade and move
Hide presence as attacker conducts internal recon
The Cyber Threat Cycle
Identify a target
Initial recon to select the weak target and determine how best to attack
Infiltrate the target
Once breached, establish an internal foothold
Complete mission
Using collected intel, execute mission goal

APPRIVER SECURITY RESPONSE



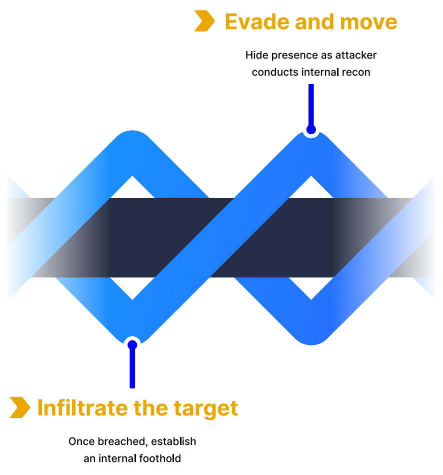
Attack the target
Using collected intel, launch attack for initial compromise
Identify a target
Initial recon to select the weak target and determine how best to attack

1. Multi-layered Email Defense

Present the initial reconnaissance and attack with a multi-layered email defense.

Why focus email defense? Solarwinds is just another reminder that email continues to be core to the threat lifecycle. It is the most difficult to secure and the easiest to exploit. There is a never-ending list of evidence that:

- *Email is wrought with a treasure trove of reconnaissance of information.*
- *Email attacks are very cheap for the threat actor.*
- *Employees are no more effective at detecting a phishing attack today than they were years ago.*



Evade and move
Hide presence as attacker conducts internal recon
Infiltrate the target
Once breached, establish an internal foothold

2. Security Audit Monitoring

Detect the Presence of a Threat Actor with a security audit monitoring motion.

A multi-layered email defense will close 95% of your prevention gap. Threat actors will figure out other ways to get into your network and ultimately protecting other vectors will be necessary, but you can quickly close this gap while evaluating other tools by leveraging security monitoring service. Particularly a solution that focus on:

- *Identifying weaknesses in user login and authentication.*
- *Identifying suspicious behavior related to mailbox rules and email communication.*

3. Act Through Containment & Remediation

Act on any suspicious behavior through containment and remediation to prevent attacker success.

The response to the potential breach must be immediate. The goal should be to maintain business productivity even in the face of an attack. Most growing businesses may not have the time or expertise to immediately triage the incident but they can begin their response and remediation process at no risk. Those tasks at minimum should be:

- *Immediately remove any malicious email that may have landed within the targeted employee's inbox.*
- *Scan the targeted employees log in activity and require any vulnerable passwords to be changed immediately (enforce MFA if disabled).*
- *Immediately clear their file system and provide the targeted employee with a clean working copy of their data.*

STRAIGHTFORWARD SECURITY STRATEGY

Turn a complex plan into a Simple operational Model

Protect

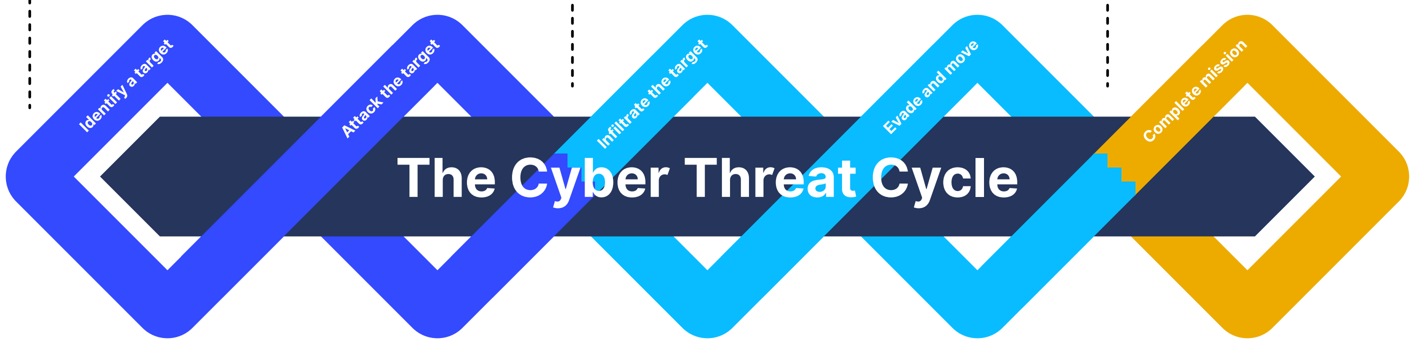
Advanced email threat protection
Azure AD multi-factor authentication
Advanced email encryption

Detect

Security audit (detect and alert)
AETP 24/7 threat protection

Respond

Security audit (remediate)
AETP (message retraction)
Backup and Recovery
Advanced email encryption (DLP)



Powered by appriver a zix company