Exchange Online Advanced Threat Protection

Sławomir Sip
Evolving threat space

Any new outbreak consists of two parts
A. Zero hour attack
B. Elongated period of attack

Traditional AV/AS cannot protect against zero day attack comprehensively

Attackers can go completely unnoticed during zero day attack
Evolving threat space

Short-span attacks can be just minutes to hours

Serial variant attacks generally repeat pattern every few hours

Attacker can easily change the links in the message after mail is delivered
Exchange Online advanced threat protection

Protection against unknown malware/virus
- Behavioral analysis with machine learning
- Admin alerts

Time of click protection
- Real time protection against Malicious URLs
- Growing URL coverage

Rich reporting and tracing
- Built-in URL trace
- Reports for advanced threats
Service architecture

Sender

Detonation chamber (sandbox)
Executable?
Registry call?
Elevation?
.......?

Unsafe
Safe

Suspicious attachment

Multiple filters + 3 antivirus engines with Exchange Online protection

Malicious links

Recipient

Safe links rewrite

Recipient
Safe attachments

- Protect against zero day exploits in email attachments by blocking messages
- Provides admins visibility into compromised users
- Leverages sandboxing technology
Safe attachment experience

Admin sets policy

Admin gets notification if message is blocked
Safe links

- Protect against sites with malicious content, phishing sites
- Provides admins visibility into compromised users
- Rewriting the URLs to proxy them through another server
Safe links—experience

Admin sets policy

Users notified if a malicious link is clicked in email
Rich reporting and click trace

Admins have complete visibility into who clicked on what links

Reporting by file types and disposition

[Image of a graph showing data analysis]