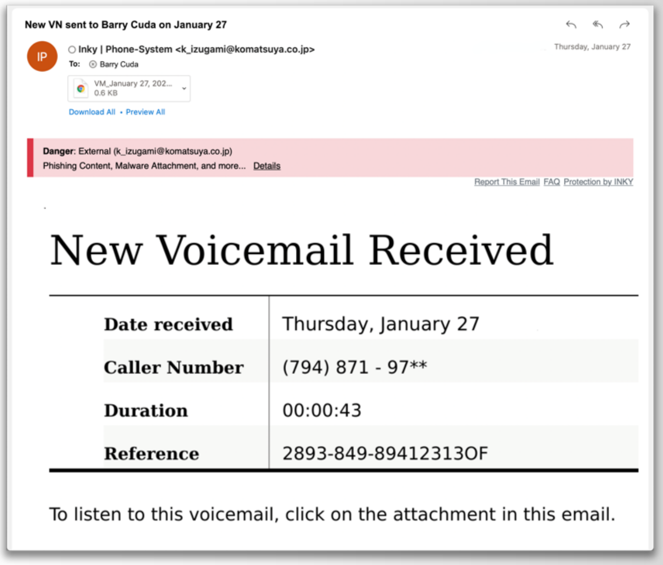
SOLUTION BRIEF

Advanced Attachment Analysis

Detect malware cleverly concealed in email attachments.



New VN sent to Barry Cuda on January 27

○ Inky | Phone-System <k_izugami@komatsuya.co.jp>

To: Barry Cuda

Thursday, January 27

VM_January 27, 202...
0.6 KB

Download All • Preview All

Danger: External (k_izugami@komatsuya.co.jp)
Phishing Content, Malware Attachment, and more... Details

Report This Email FAQ Protection by INKY

New Voicemail Received

Date received	Thursday, January 27
Caller Number	(794) 871 - 97**
Duration	00:00:43
Reference	2893-849-894123130F

To listen to this voicemail, click on the attachment in this email.

What is INKY Advanced Attachment Analysis?

Bad actors sometimes hide a malware payload in an attachment. Sometimes, this payload is particularly well hidden. In one ruse, for example, the black hats hide malware in an encrypted PDF file, which they attach to an email. In the body of the email, they enclose the key. The recipient might ask, why did they encrypt a file only to give me the key in the open? The answer is: because that way, the file itself won't be inspected by the email security system.

Advanced Attachment Analysis finds and stops these sorts of attacks, using a combination of fast — but thorough — techniques. Created by cybersecurity experts, Advanced Attachment Analysis breaks attachments down into separate parts, analyzes each separately, sees how they are connected, and makes an assessment. By looking at what the component parts do in addition to matching them against known threats, Advanced Attachment Analysis can detect both known threats and malware that has never been seen before.

How is INKY's Approach to INKY Advanced Attachment Analysis Different?

Attachment analysis is in its infancy. It's only been a few years since black hats started using attachments to hide malware. Thus, most capabilities on the market today are only rudimentary. Other techniques involve signature matching, which has the singular weakness that it cannot catch new threats. To evade legacy file scanning detection tools, all the bad guys have to do is change one bit in a poisoned file.

By using a method that relies on understanding tactics, techniques, and procedures rather than known pattern-matching, INKY Advanced Attachment Analysis can identify the trickiest exploits that threat actors dish out.

Another key difference relates to sandboxing (isolating a suspect file, limiting its access to system resources, and executing it in this safe environment to prevent harm to the rest of the system). Legacy solutions available today utilize sandboxing to protect against threats embedded in files. Sandboxing is expensive, resource-intensive, and delays delivery, sometimes causing missing attachments to show up after original message delivery.

Advanced Attachment Analysis aligns well with INKY's general approach to email security, which involves behavioral analysis (e.g., detecting impersonation) and modification (e.g., assisting employees in making better decisions) in place of pattern matching.

Why is INKY Advanced Attachment Analysis Needed?

Standard INKY comes with a basic level of attachment analysis. INKY's standard analysis involves file-level checking for known virus signatures, URL analysis of any links found in the attachment, and deeper analysis of linked websites' rendered content. In many cases, this basic level is enough. But for those organizations that pass highly sensitive material through email, a higher level of security is warranted.

How does INKY Advanced Attachment Analysis Protect Mail?

INKY Advanced Attachment Analysis uses a file parser to break apart files, allowing it to get at the bad thing hidden inside. Running in line, INKY Advanced Attachment Analysis check runs its checks in less than a second, and yet rarely flags an attachment that's not actually bad. By looking at the behavior of software components rather than their signatures, INKY Advanced Attachment Analysis protects against exploits — including new ones — rather than known payloads. INKY Advanced Attachment Analysis runs on a private network, can scale to handle a huge volume, and doesn't disrupt mail flow.

About INKY

INKY is a behavioral email security platform that blocks threats, prevents data leaks, and coaches users to make smart decisions. The platform intelligently eliminates security threats by blocking malicious emails while assisting employees in real time to handle suspicious emails. INKY's patented technology sanitizes and rewrites all emails, detects, and blocks brand forgery attempts using computer vision and machine learning models, and mitigates sender impersonation attacks using social profiling and stylometry algorithms. The INKY platform was designed for mobile-first IT organizations and works seamlessly on any device, operating system, and mail client.

INKY™