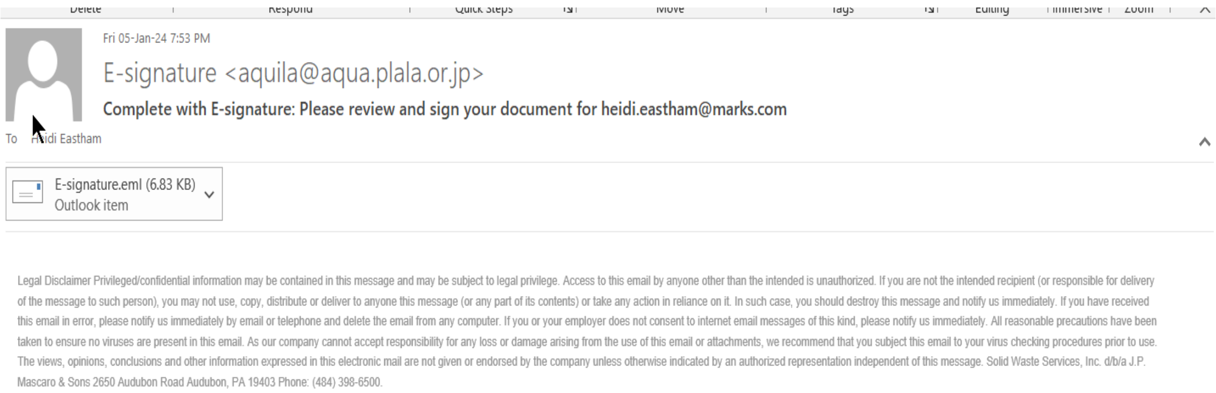
Email Analysis

In this example, a malicious email was analyzed. The sample was taken from any.run named ‘Complete.eml.zip’ file which consisted of an email file named ‘Complete.eml’. The email claimed to be from Solid Waste Services, Inc. d/b/a J.P. Mascaro & Sons 2650 Audubon Road Audubon and contains attachment which is another email or message file named ‘E-signature.eml (6.83 KB).msg’ attached to it. After investigation the following artefacts are retrieved:

- Sender: "E-signature" aquila[@]aqua.plala.or.jp
- Sender IP: 60[.]36[.]166[.]77
- Subject: Complete with E-signature: Please review and sign your document for heidi.eastham@marks.com
- Attached file: E-signature.eml (6.83 KB).msg
- File MD5 hash: 27b5d8d027f9b7b6d08d810160eb7977
- Authentication-Results: spf=pass (sender IP is 60.36.166.77); dkim=none (message not signed) header.d=none

Detailed Analysis Report

[1] The email formatting was suspicious and didn’t look like it came from any official person or workplace as it was containing an attachment which was another email which looked suspicious as no one will attach other email to an email.



Fri 05-Jan-24 7:53 PM

E-signature <aquila@aqua.plala.or.jp>

Complete with E-signature: Please review and sign your document for heidi.eastham@marks.com

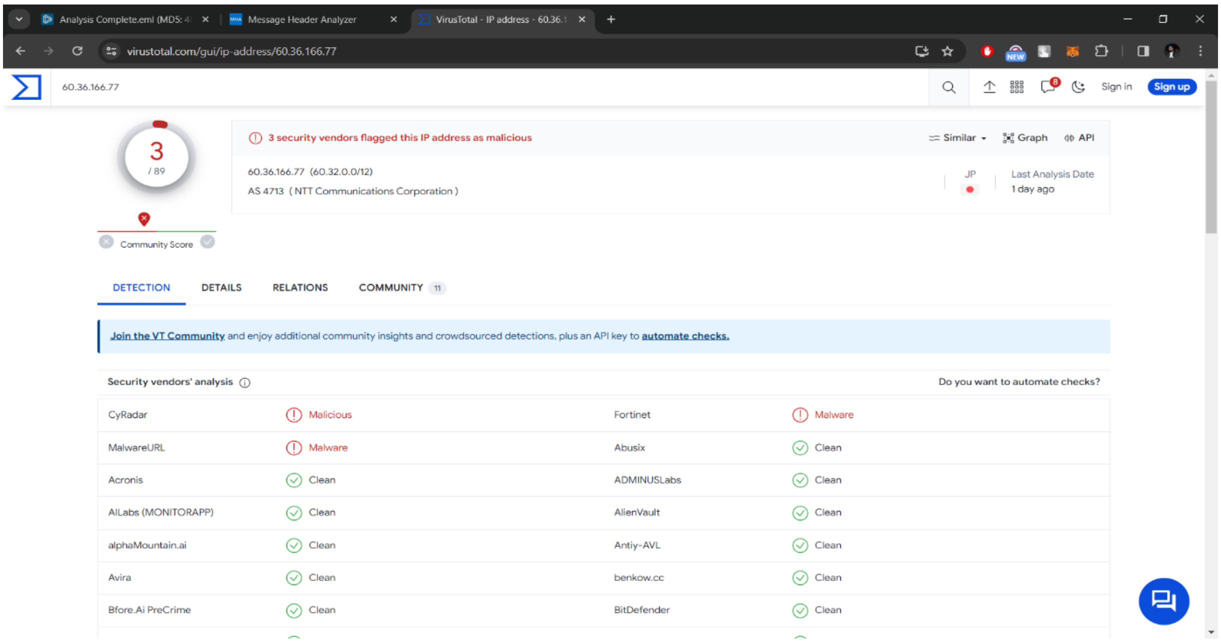
To Heidi Eastham

E-signature.eml (6.83 KB)
Outlook item

Legal Disclaimer Privileged/confidential information may be contained in this message and may be subject to legal privilege. Access to this email by anyone other than the intended is unauthorized. If you are not the intended recipient (or responsible for delivery of the message to such person), you may not use, copy, distribute or deliver to anyone this message (or any part of its contents) or take any action in reliance on it. In such case, you should destroy this message and notify us immediately. If you have received this email in error, please notify us immediately by email or telephone and delete the email from any computer. If you or your employer does not consent to internet email messages of this kind, please notify us immediately. All reasonable precautions have been taken to ensure no viruses are present in this email. As our company cannot accept responsibility for any loss or damage arising from the use of this email or attachments, we recommend that you subject this email to your virus checking procedures prior to use. The views, opinions, conclusions and other information expressed in this electronic mail are not given or endorsed by the company unless otherwise indicated by an authorized representation independent of this message. Solid Waste Services, Inc. d/b/a J.P. Mascaro & Sons 2650 Audubon Road Audubon, PA 19403 Phone: (484) 398-6500.

[2] The sender was spoofing Solid Waste Services, Inc. d/b/a J.P. Mascaro & Sons 2650 however, the sending IP revealed it belonged to aquila[@]aqua.plala.or.jp which doesn’t look like their official email address.

[3] Also, the ip address was reported malicious when searched on virustotal. The smtp.mailfrom[aqua.plala.or.jp] was also checked but it was found clean.



3
/ 89

3 security vendors flagged this IP address as malicious

60.36.166.77 (60.32.0.0/12)
AS 4713 (NTT Communications Corporation)

JP

Last Analysis Date
1 day ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

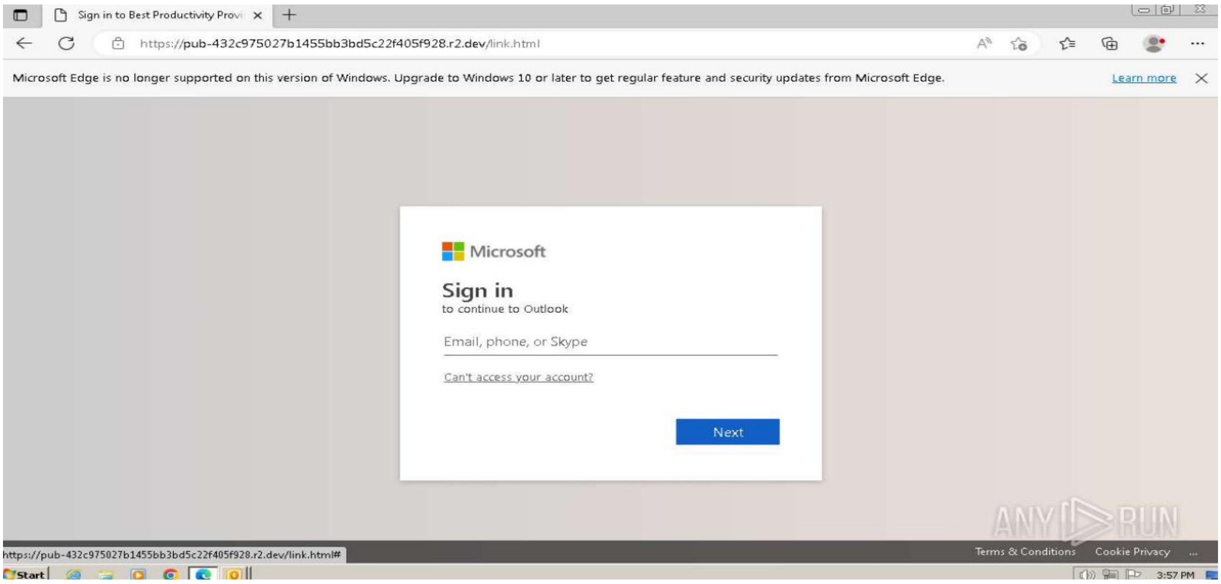
CyRadar	Malicious	Fortinet	Malware
MalwareURL	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Avira	Clean	benkow.cc	Clean
Bfore.Ai PreCrime	Clean	BitDefender	Clean

[4] The attached email when opened was asking us to review and sign the document that day only in order for the recipient to make an error in hurry.

[5] The verify button contained a link “https://assets-usa.mkt.dynamics.com/0431d997-23ab-ee11-be32-6045bd059008/digitalassets/standaloneforms/d993aea3-a5ab-ee11-be37-6045bd0062b9” which took us to a captcha page where we have to enter the alphanumeric values in order to go through that page.

[7] After entering the captcha correctly it took us to some other site which required the recipient’s Microsoft login in order to verify the recipient, but the designed login page is fake and can be figured out by looking closely.

[8] Also, the Microsoft login page was addressed at a different address than the Microsoft accounts webpage.



Sign in to Best Productivity Provi

https://pub-432c975027b1455bb3bd5c22f405f928.r2.dev/link.html

Microsoft Edge is no longer supported on this version of Windows. Upgrade to Windows 10 or later to get regular feature and security updates from Microsoft Edge. Learn more

Microsoft

Sign in

to continue to Outlook

Email, phone, or Skype

Can't access your account?

Next

https://pub-432c975027b1455bb3bd5c22f405f928.r2.dev/link.html#

[9] Also if you click on the “Can’t access your account” button it does nothing which was suspicious as the original Microsoft login page button must help the user in logging in if the user is facing difficulity.