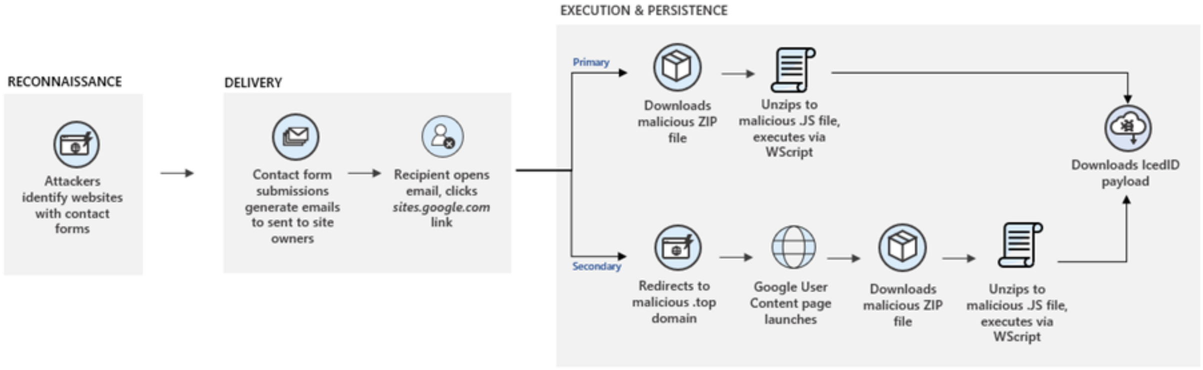
Investigating a unique “form” of email delivery for IcedID malware

microsoft.com/security/blog/2021/04/09/investigating-a-unique-form-of-email-delivery-for-icedid-malware/

April 9, 2021


RECONNAISSANCE
Attackers identify websites with contact forms
DELIVERY
Contact form submissions generate emails to sent to site owners
Recipient opens email, clicks *sites.google.com* link
EXECUTION & PERSISTENCE
Primary
Downloads malicious ZIP file
Unzips to malicious JS file, executes via WScript
Downloads IcedID payload
Secondary
Redirects to malicious .top domain
Google User Content page launches
Downloads malicious ZIP file
Unzips to malicious JS file, executes via WScript

Microsoft threat analysts have been tracking activity where contact forms published on websites are abused to deliver malicious links to enterprises using emails with fake legal threats. The emails instruct recipients to click a link to review supposed evidence behind their allegations, but are instead led to the download of IcedID, an info-stealing malware. Microsoft Defender for Office 365 detects and blocks these emails and protects organizations from this threat.

In this blog, we showcase our analysis on this unique attack and how the techniques behind it help attackers with their malicious goals of finding new ways to infect systems. This threat is notable because:

1. Attackers are abusing legitimate infrastructure, such as websites’ contact forms, to bypass protections, making this threat highly evasive. In addition, attackers use legitimate URLs, in this case Google URLs that require targets to sign in with their Google credentials.
2. The emails are being used to deliver the IcedID malware, which can be used for reconnaissance and data exfiltration, and can lead to additional malware payloads, including ransomware.
3. This threat shows attackers are always on the hunt for attack paths for infiltrating networks, and they often target services exposed to the internet. Organizations must ensure they have protections against such threats.

While this specific campaign delivers the IcedID malware, the delivery method can be used to distribute a wide range of other malware, which can in turn introduce other threats to the enterprise. IcedID itself is a banking trojan that has evolved to become an entry point for more sophisticated threats, including human-operated ransomware. It connects to a command-and-control server and downloads additional implants and tools that allow attackers to perform hands-on-keyboard attacks, steal credentials, and move laterally across affected networks to delivering additional payloads.

We continue to actively investigate this threat and work with partners to ensure that customers are protected. We have already alerted security groups at Google to bring attention to this threat as it takes advantage of Google URLs.

Microsoft 365 Defender defends organizations by using advanced technologies informed by Microsoft Defender for Office 365 and backed by security experts. Microsoft 365 Defender correlates signals on malicious emails, URLs, and files to deliver coordinated defense against evasive threats, their payloads, and their spread across networks.

Microsoft Defender for Office 365 supports organizations throughout an attack’s lifecycle, from prevention and detection to investigation, hunting, and remediation–effectively protecting users through a coordinated defense framework.

Tracking malicious content in contact forms

Websites typically contain contact form pages as a way to allow site visitors to communicate with site owners, removing the necessity to reveal their email address to potential spammers.

However, in this campaign, we observed an influx of contact form emails targeted at enterprises by means of abusing companies’ contact forms. This indicates that attackers may have used a tool that automates this process while circumventing CAPTCHA protections.

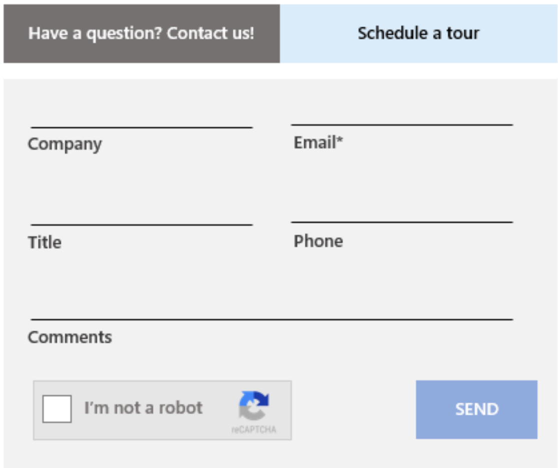
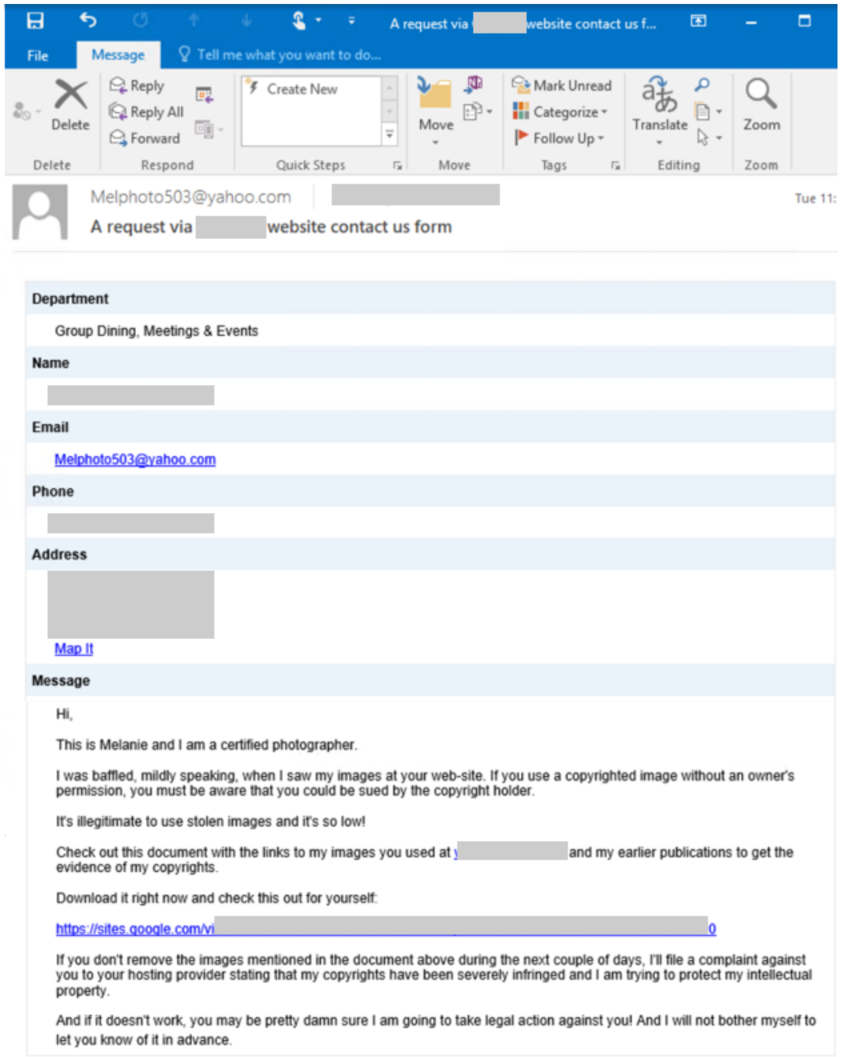


Figure 1. Sample contact form that attackers take advantage of by filling in malicious content, which gets delivered to the target enterprises

In this campaign, we tracked that the malicious email that arrives in the recipient's inbox from the contact form query appears trustworthy as it was sent from trusted email marketing systems, further confirming its legitimacy while evading detection. As the emails are originating from the recipient's own contact form on their website, the email templates match what they would expect from an actual customer interaction or inquiry.

As attackers fill out and submit the web-based form, an email message is generated to the associated contact form recipient or targeted enterprise, containing the attacker-generated message. The message uses strong and urgent language ("Download it right now and check this out for yourself"), and pressures the recipient to act immediately, ultimately compelling recipients to click the links to avoid supposed legal action.



Melphoto503@yahoo.com [redacted]

A request via [redacted] website contact us form

Tue 11:

Department

Group Dining, Meetings & Events

Name

[redacted]

Email

Melphoto503@yahoo.com

Phone

[redacted]

Address

[redacted]

Map It

Message

Hi,

This is Melanie and I am a certified photographer.

I was baffled, mildly speaking, when I saw my images at your web-site. If you use a copyrighted image without an owner's permission, you must be aware that you could be sued by the copyright holder.

It's illegitimate to use stolen images and it's so low!

Check out this document with the links to my images you used at [redacted] and my earlier publications to get the evidence of my copyrights.

Download it right now and check this out for yourself:

https://sites.google.com/vi[redacted]0

If you don't remove the images mentioned in the document above during the next couple of days, I'll file a complaint against you to your hosting provider stating that my copyrights have been severely infringed and I am trying to protect my intellectual property.

And if it doesn't work, you may be pretty damn sure I am going to take legal action against you! And I will not bother myself to let you know of it in advance.

Figure 2. A sample email delivered via contact forms that contain malicious content added by attackers

Along with the fake legal threats written in the comments, the message content also includes a link to a *sites.google.com* page to view the alleged stolen photos for the recipient to view.

Clicking the link brings the recipient to a Google page that requires them to sign in with their Google credentials. Because of this added authentication layer, detection technologies may fail in identifying the email as malicious altogether.

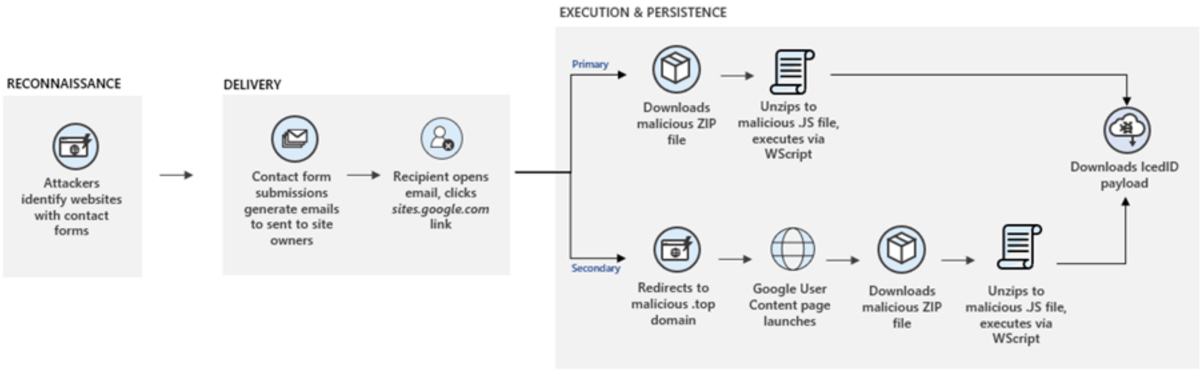
After the email recipient signs in, the *sites.google.com* page automatically downloads a malicious ZIP file, which contains a heavily obfuscated .js file. The malicious .js file is executed via WScript to create a shell object for launching PowerShell to download the IcedID payload (a .dat file), which is decrypted by a dropped DLL loader, as well as a Cobalt Strike beacon in the form of a stageless DLL, allowing attackers to remotely control the compromised device.

The downloaded .dat file loads via the rundll32 executable. The rundll32 executable then launches numerous commands related to the following info-stealing capabilities:

- Machine discovery
- Obtaining machine AV info
- Getting IP and system information
- Domain information
- Dropping SQLite for accessing credentials stored in browser databases

Contact form email campaign attack chains lead to IcedID malware

The diagram in Figure 3 provides a broad illustration of how attackers carry out these malicious email campaigns, starting from identifying their targets' contact forms and ending with the IcedID malware payload.



RECONNAISSANCE
Attackers identify websites with contact forms
DELIVERY
Contact form submissions generate emails to sent to site owners
Recipient opens email, clicks *sites.google.com* link
EXECUTION & PERSISTENCE
Primary
Downloads malicious ZIP file
Unzips to malicious JS file, executes via WScript
Downloads IcedID payload
Secondary
Redirects to malicious .top domain
Google User Content page launches
Downloads malicious ZIP file
Unzips to malicious JS file, executes via WScript

Figure 3. Contact form attack chain results in the IcedID payload

We noted a primary and secondary attack chain under the execution and persistence stages. The primary attack chain follows an attack flow from downloading malicious .zip file from the *sites.google.com* link, all the way to the IcedID payload. The secondary attack chain, on the other hand, appears to be a backup attack flow for when the *sites.google.com* page in the primary attack chain has already been taken down.

In the secondary chain, users are redirected to a .top domain, while inadvertently accessing a Google User Content page, which downloads the malicious .ZIP file. Further analysis reveals that the forms contain malicious *sites.google.com* links that download the IcedID malware.

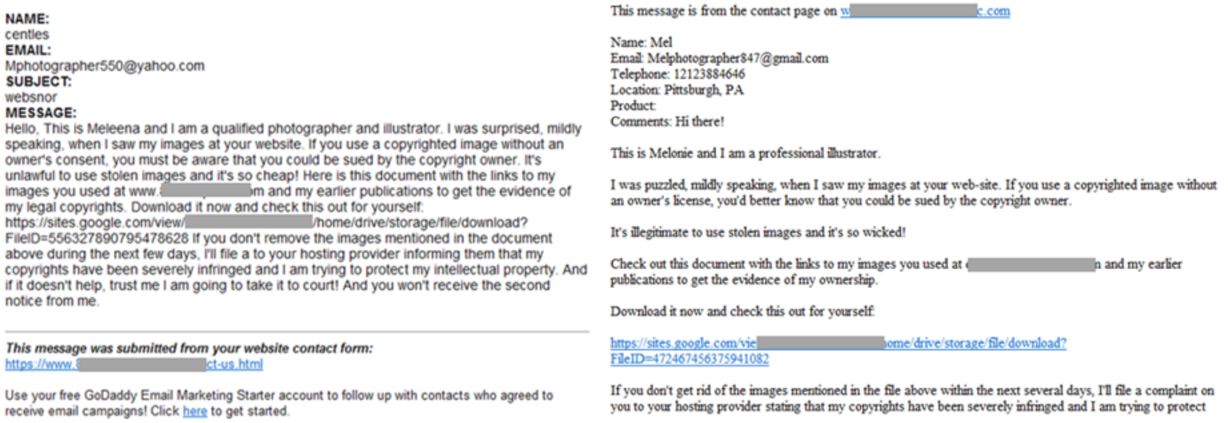
When run, IcedID connects to a command-and-control server to download modules that run its primary function of capturing and exfiltrating banking credentials and other information. It achieves persistence via schedule tasks. It also downloads implants like Cobalt Strike and other tools, which allow remote attackers to run malicious activities on the compromised system, including collecting additional credentials, moving laterally, and delivering secondary payloads.

Using legal threats as a social engineering tactic

This campaign is not only successful because it takes advantage of legitimate contact form emails, but the message content also passes as something that recipients would expect to receive. This creates a high risk of attackers successfully delivering email to inboxes, thereby allowing for "safe" emails that would otherwise be filtered out into spam folders.

In the samples we found, attackers used legal threats as a scare tactic while claiming that the recipients allegedly used their images or illustrations without their consent, and that legal action will be taken against them. There is also a heightened sense of urgency in the email wording, with phrases such as "you could be sued," and "it's not legal." It's a sly and devious approach since everything else about this email is authentic and legitimate.

We observed more emails sent by attackers on other contact forms that contain similar wording around legal threats. The messages consistently mention a copyright claim lure by a photographer, illustrator, or designer with the same urgency to click the *sites.google.com* link.



NAME:
centles
EMAIL:
Mphotographer550@yahoo.com
SUBJECT:
websnor
MESSAGE:
Hello, This is Meleena and I am a qualified photographer and illustrator. I was surprised, mildly speaking, when I saw my images at your website. If you use a copyrighted image without an owner's consent, you must be aware that you could be sued by the copyright owner. It's unlawful to use stolen images and it's so cheap! Here is this document with the links to my images you used at www.[redacted]m and my earlier publications to get the evidence of my legal copyrights. Download it now and check this out for yourself: https://sites.google.com/view/[redacted]/home/drive/storage/file/download?FileID=556327890795478628 If you don't remove the images mentioned in the document above during the next few days, I'll file a to your hosting provider informing them that my copyrights have been severely infringed and I am trying to protect my intellectual property. And if it doesn't help, trust me I am going to take it to court! And you won't receive the second notice from me.

This message was submitted from your website contact form:
https://www.[redacted]ct-us.html

Use your free GoDaddy Email Marketing Starter account to follow up with contacts who agreed to receive email campaigns! Click here to get started.

This message is from the contact page on w[redacted]c.com

Name: Mel
Email: Melphotographer847@gmail.com
Telephone: 12123884646
Location: Pittsburgh, PA
Product:
Comments: Hi there!

This is Melonie and I am a professional illustrator.

I was puzzled, mildly speaking, when I saw my images at your web-site. If you use a copyrighted image without an owner's license, you'd better know that you could be sued by the copyright owner.

It's illegitimate to use stolen images and it's so wicked!

Check out this document with the links to my images you used at [redacted]n and my earlier publications to get the evidence of my ownership.

Download it now and check this out for yourself:

https://sites.google.com/vie[redacted]ome/drive/storage/file/download?FileID=472467456375941082

If you don't get rid of the images mentioned in the file above within the next several days, I'll file a complaint on you to your hosting provider stating that my copyrights have been severely infringed and I am trying to protect

Figure 4. Samples of contact form emails that use the photographer copyright lure with a sites.gooogle.com link

In a typical contact form, users are required to input their name, email address, and a message or comment. In the samples we obtained, attackers used fake names that start with “Mel,” such as “Melanie” or “Meleena,” and used a standard format for their fake email addresses that include a portion of their fake name + words associated photography + three numbers. Some examples include:

- mphotographer550@yahoo.com
- mephotographer890@hotmail.com
- mgallery487@yahoo.com
- mephoto224@hotmail.com
- megallery736@aol.com
- mshot373@yahoo.com

Defending against sophisticated attacks through coordinated defense

As this research shows, adversaries remain motivated to find new ways to deliver malicious email to enterprises with the clear intent to evade detection. The scenarios we observed offer a serious glimpse into how sophisticated attackers’ techniques have grown, while maintaining the goal of delivering dangerous malware payloads such as IcedID. Their use of submission forms is notable because the emails don’t have the typical marks of malicious messages and are seemingly legitimate.

To protect customers from this highly evasive campaign, Microsoft Defender for Office 365 inspects the email body and URL for known patterns. Defender for Office 365 enables this by leveraging its deep visibility into email threats and advanced detection technologies powered by AI and machine learning, backed by Microsoft experts who constantly monitor the threat landscape for new attacker tools and techniques. Expert monitoring is especially critical in detecting this campaign given the delivery method and the nature of the malicious emails.

In addition, the protection delivered by Microsoft Defender for Office 365 is enriched by signals from other Microsoft 365 Defender services, which detect other components of this attack. For example, Microsoft Defender for Endpoint detects the IcedID payload and surfaces this intelligence across Microsoft 365 Defender. With its cross-domain optics, Microsoft 365 Defender correlates threat data on files, URLs, and emails to provide end-to-end visibility into attack chains. This allows us to trace detections of malware and malicious behavior to the delivery method, in this case, legitimate-looking emails, enabling us to build comprehensive and durable protections, even as attackers continue to tweak their campaigns to further evade detection.

By running custom queries using advanced hunting in Microsoft 365 Defender, customers can proactively locate threats related to this attack.

To locate emails that may be related to this activity, run the following query:

```
EmailUrlInfo
| where Url matches regex @"\bsites\.google\.com\/view\/(?:id)?\d{9,}\b"
| join EmailEvents on NetworkMessageId
// Note: Replace the following subject lines with the one generated by your website's Contact submission form if no
results return initially
| where Subject has_any('Contact Us', 'New Submission', 'Contact Form', 'Form submission')
```

To find malicious downloads associated with this threat, run the following query:

```
DeviceFileEvents
| where InitiatingProcessFileName in~
("msedge.exe", "chrome.exe", "explorer.exe", "7zFM.exe", "firefox.exe", "browser_broker.exe")
| where FileOriginReferrerUrl has ".php" and FileOriginReferrerUrl has ".top" and FileOriginUrl  has_any("googleusercont
```

As this attack abuses legitimate services, it’s also important for customers to review mail flow rules to check for broad exceptions, such those related to IP ranges and domain-level allow lists, that may be letting these emails through.

We also encourage customers to continuously build organizational resilience against email threats by educating users about identifying social engineering attacks and preventing malware infection. Use Attack simulation training in Microsoft Defender for Office 365 to run attack scenarios, increase user awareness, and empower employees to recognize and report these attacks.

Emily Hacker with Justin Carroll
Microsoft 365 Defender Threat Intelligence Team

Additional resources

Listen to Episode 28 of the Security Unlocked podcast, Contact Us; Phish You!, where threat analyst Emily Hacker speaks about this new form of phishing email delivery