Threat of the Month: IcedID Malware

ceriumnetworks.com/threat-of-the-month-icedid-malware/

July 29, 2021

About Threat of the Month Series

With the rise of cyberattacks, it's impossible for security and IT teams to keep track of every one. We'll identify an emerging cybersecurity threat and give information on what it is, why it's becoming more prevalent, and how you can prevent it.

The Threat of the Month blog series is a collaboration between Cerium Networks and Blumira.

This month's threat is IcedID (aka BokBot) a strain of malware that initially operated as a banking trojan but has now evolved into something far more dangerous: an initial access broker for ransomware threat actors.

The first half of 2021 alone has been a record-breaking time period for ransomware, during which six ransomware groups have compromised 292 organizations, according to an eSentire report. The report estimates that these attacks generated at least $45 million for the groups.

So, what does IcedID have to do with ransomware? The threat actors that are deploying ransomware aren't usually the ones deploying IcedID in the wild.

The threat actors behind IcedID typically launch a mass email campaign. Once IcedID has gained a foothold into an environment, the malware threat actors sell that initial access — which often includes reconnaissance intel such as the number of endpoints in the targeted organization, network range, and potential access points — in a cybercriminal marketplace. Ransomware-as-a-service affiliates will purchase the initial access which they use to launch the ransomware attack.

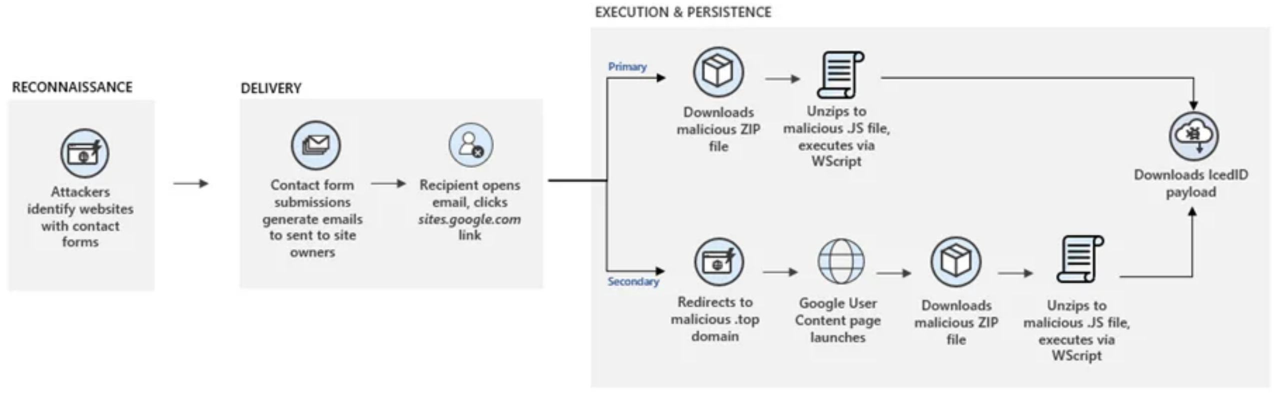
Learn more about the differences between malware and ransomware >

The evolution of IcedID from a banking trojan to an initial access broker means that financial institutions are no longer the only target. Any organization that doesn't have malware prevention in place can be a potential victim.

How Does IcedID Work?

Threat actors have used a few different methods to deploy an IcedID campaign, and as with most cyberattacks, these methods are always evolving — making IcedID more difficult to detect.

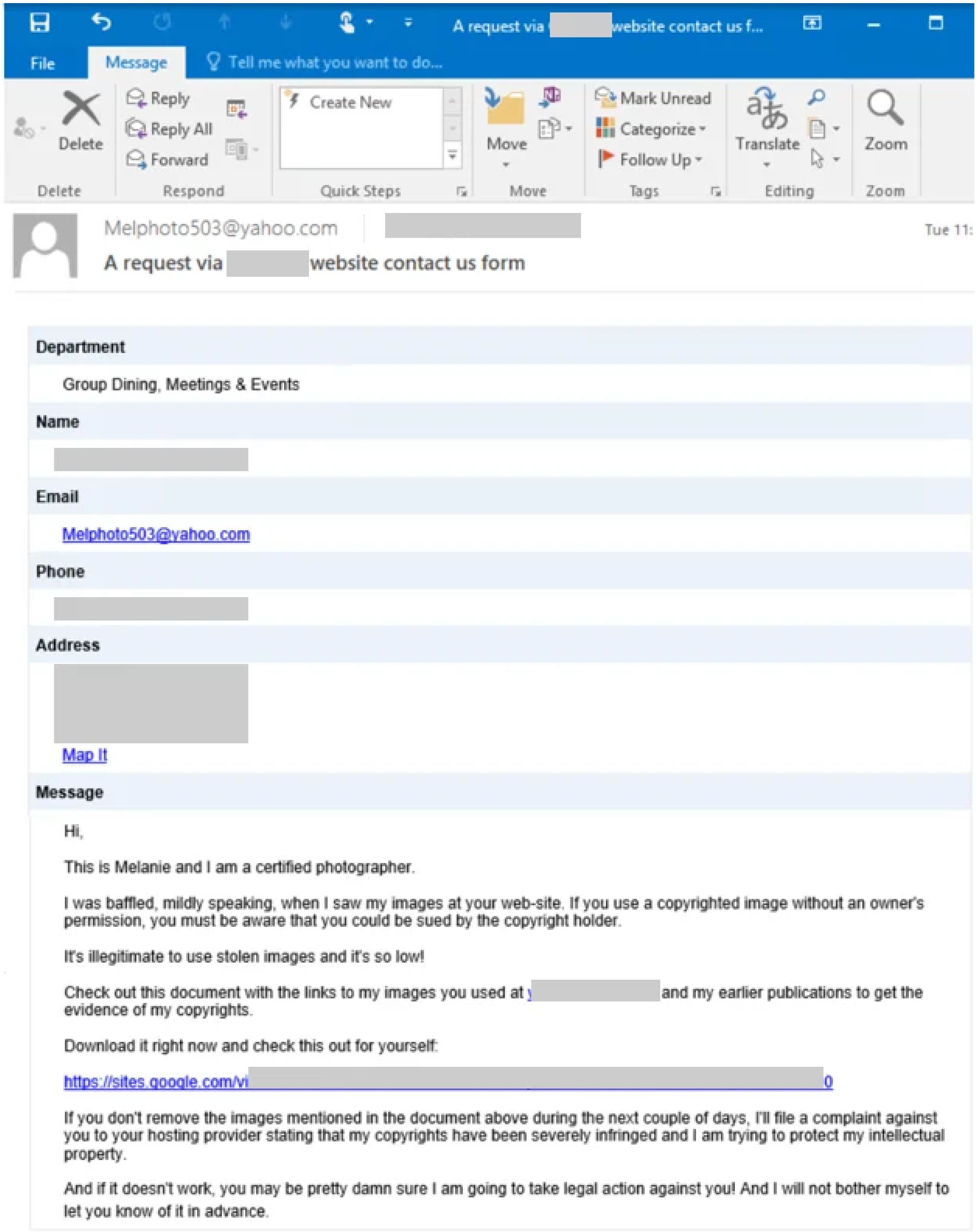
In some campaigns, threat actors use rigged Excel spreadsheets as a delivery mechanism. Threat actors typically use a naming convention that prompts victims to open it, using language such as “refusal,” “claim,” and “overdue.” Users that open the file will see a screen instructing them to enable macros to see the full version.


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
Secondary
Redirects to malicious .top domain
Google User Content page launches
Downloads malicious ZIP file
Unzips to malicious JS file, executes via WScript
Downloads IcedID payload

Once macros are enabled, the malicious formula embedded in the Excel sheet will execute. Malware developers often use white font on a white background to make the formula invisible to victims. Macros on the sheet then download three DLL files with the .dat extension from the command and control servers.

More recent IcedID campaigns involve threat actors using contact forms on legitimate company websites to send emails with malicious links. With this method, the emails that arrive in a victim's inbox look trustworthy because they are sent using email marketing systems. It's possible that threat actors have used tools to automate the process and evade CAPTCHA measures, according to Microsoft.

In one particular campaign, the email contained strong language and legal threats about stolen photography, with links to site.google.com for the recipient to view the stolen photos. Once a victim follows the link, which asks them to sign in with Google credentials, the site will automatically download a zip file. This contains a malicious .js file that launches the IcedID attack.



Melphoto503@yahoo.com [redacted] Tue 11:

A request via [redacted] website contact us form

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 y[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.

Why Now?

In January 2021, a coalition of eight international law enforcement officials brought down one of the most widespread malware variants, Emotet. On April 25, 2021, government officials uninstalled Emotet from all infected systems. Like IcedID, Emotet originated as a banking trojan designed to steal sensitive information. Over the years, however, it morphed into a more sophisticated strain of malware that evaded detection techniques and used command and control servers to receive updates. It eventually became capable of downloading secondary malware payloads, such as “Ryuk” ransomware.

The takedown of arguably one of the biggest players in malware created an opening in the marketplace for cybercriminals to fill — and IcedID is primed to take its place.

IcedID isn’t the only initial access broker for ransomware gangs; other malware families such as TrickBot and Qbot also deliver payloads for ransomware attacks. However, IcedID threat actors have managed to fly under the radar, while strains like TrickBot are heavily monitored by law enforcement.

A few signs have pointed to the rise of IcedID and its use within ransomware attacks. Threat researchers reported a spike in IcedID activity in March 2021. IcedID was also used to deliver Sodinokibi, MAZE and Egregor ransomware attacks.

How To Prevent IcedID

Organizations can do a few things to prevent IcedID. Deploying antivirus (AV) software may seem like an obvious first step. Although more advanced solutions can be helpful, IcedID uses sophisticated techniques like using a company’s contact forms to evade detection from many traditional antivirus tools.

Deploy detection and response. A detection and response solution that alerts security and IT teams about suspicious behaviors is typically more effective in preventing sophisticated malware strains like IcedID than an antivirus software. Blumira, for example, comes with prebuilt detections designed to detect behaviors that are associated with IcedID’s initial access attack path — like running built-in Windows utilities or enabling macros.

Train employees to detect phishing. Nearly every IcedID campaign starts with a phishing email, so employees that are able to detect these emails can prevent an IcedID attack altogether. Security teams can educate employees about phishing in a few ways depending on company culture, such as interactive quizzes, team meetings and casual discussions.

Disable macros. IcedID uses macros to download and execute its payload, so one step that IT and security admins can take is to disable macros for Microsoft Word through GPO, as this will have little to no business impact for most organizations. Enforcing any kind of macro policy for Excel, while recommended, will require more aggressive planning.

Try Blumira For Free

Not only does Blumira’s threat detection and response solution come with prebuilt detections designed to detect and alert you on suspicious behaviors, but it also comes with a team of real security advisors to help you remediate an issue and take next steps.

Deploying Blumira takes a matter of hours, not months or weeks. Try our free trial and start seeing the immediate value that Blumira can offer.

You can also contact Cerium to learn more about how Blumira can help.