In an unreported first - GootLoader, a popular malware-as-a-service (MaaS) offering which leverages Search Engine Optimization (SEO) poisoning to distribute malicious payloads, has dropped IcedID as a payload while simultaneously shifting to a stealthier payload delivery procedure. IcedID is a former banking-trojan, turned malware loader. On May 30th, eSentire's research team, the Threat Response Unit (TRU), discovered that threat actors were trying to deploy IcedID onto a law firm's IT network via an employee's computer. eSentire's Security Operations Centre (SOC) immediately isolated the infected endpoint, and worked with TRU to diagnose the malware as IcedID, after cleaning the endpoint and ensuring that the legal firm's IT environment was clean and safe.

TRU has disrupted 16 distinct GootLoader incidents since January 2022, involving the Software, Legal, and Customer Service industries. However, most of these GootLoader campaigns have come and gone with little change (Figure 1), often deploying a generic Cobalt Strike beacon in default configuration. This method leverages noisy Windows registry keys, making detection difficult. The Windows operating system uses the registry to store configuration data for applications and Windows itself.

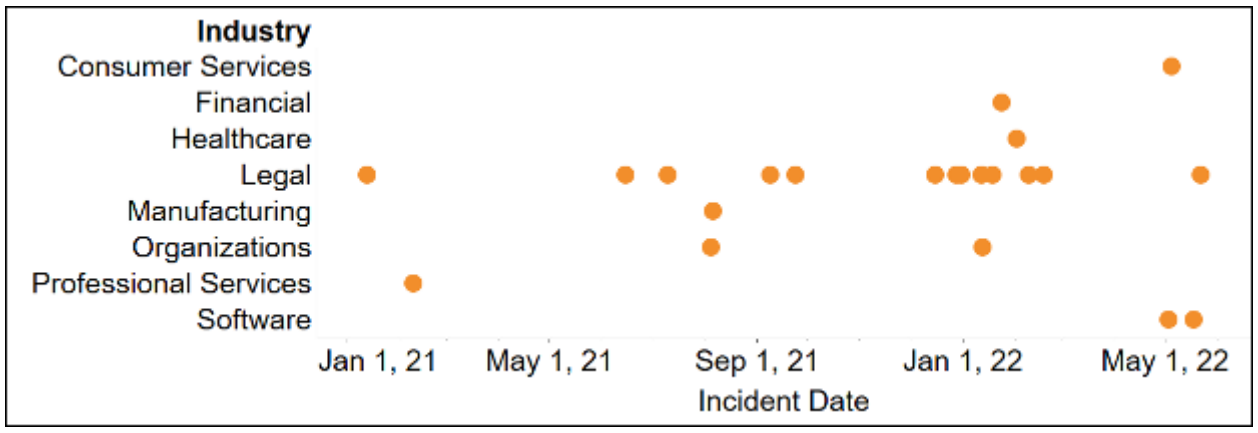

Figure 1 - Industries impacted by GootLoader's SEO poisoning procedure.

GootLoader dropping IcedID as a payload is significant because TRU recently observed IcedID deploying customized configurations of Cobalt Strike, the primary hands-on intrusion tool leveraged by some of the most lethal ransomware groups such as Conti, REvil, FiveHands and BlackCat. In particular, TRU has seen IcedID deliver Cobalt Strike in under 20 minutes from the time of the IcedID infection, giving organizations little time to respond before the threat actors compromise their network. The introduction of an additional step in the attack chain could serve several purposes, from obscuring the final payload to utilizing more sophisticated Cobalt Strike builds that are associated with IcedID.

TRU has disrupted 16 distinct GootLoader incidents since January 2022, involving the Software, Legal, and Customer Service industries.

GootLoader's Modus Operandi

GootLoader operators use SEO poisoning to ensnare their victims, baiting them with fake templates of business agreements pertaining to topics such as employee confidentiality, plea agreements, aviation safety and postnuptial agreements. When victims search for these documents online, GootLoader leverages infected WordPress sites to deliver a malicious javascript file, disguised as an agreement example.

A GootLoader Infection-- Step by Step

A business professional visits an infected website looking for a sample of an employee confidentiality agreement. Here they are presented with a forum overlay (Figure 2) and provided a link to download a zip archive, containing the malicious .js file. Once the employee executes the javascript file, they have initiated GootLoader which downloads and executes Cobalt Strike or IcedID.

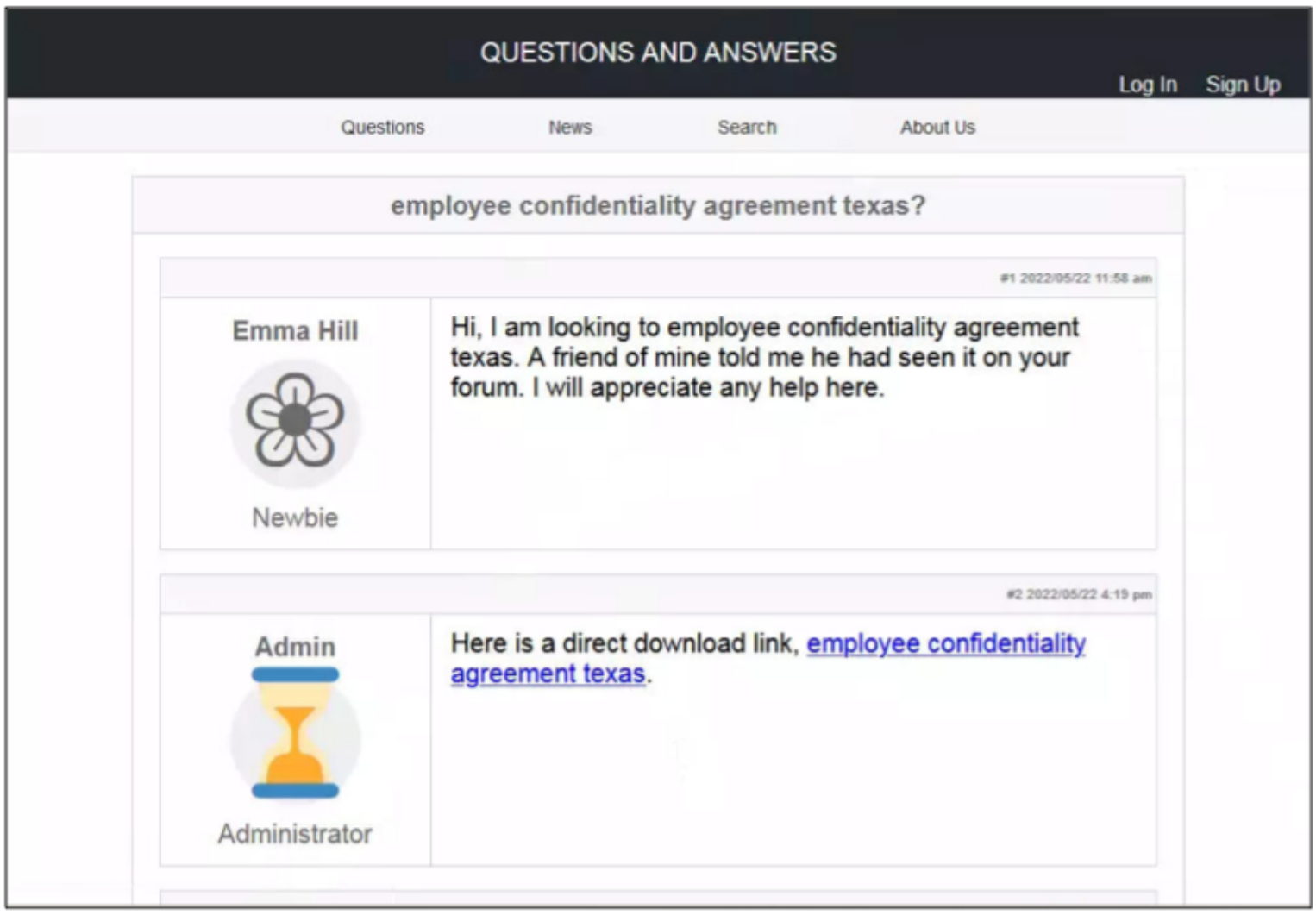

Figure 2 - An employee is tricked into downloading what they believe is a sample agreement.

In 2021, the security community saw the hackers behind GootLoader abandon an exclusive delivery model, in which it only dropped the GootKit Remote Access Trojan (RAT), and began focusing on adapting their loader to other payloads. In 2021, GootLoader was reported dropping an array of payloads, including the REvil ransomware (aka Sodinokibi), Cobalt Strike and the Gootkit banking trojan.

Stealthier Registry Keys for New Payload

In recent incidents involving GootLoader, the malware would write the Cobalt Strike payload to the Phone registry keys, a relatively easy detection. However, in the May 30th incident, GootLoader is using a more common registry key. As a result, the activity is more prone to false positives and some security teams might be hesitant to implement detections for it.

It‘s unclear whether customers of the GootLoader MaaS get to choose the registry targets, in addition to choosing their payload. However, this update reflects a small evolutionary step in GootLoader‘s malware delivery offering.

Two payloads were written to the victim’s User Registry Keys under:

1. HKEY_CURRENT_USER\SOFTWARE\Microsoft\<username>\
    1. contains the encrypted/obfuscated IcedID payload
2. HKEY_CURRENT_USER\SOFTWARE\Microsoft\<username>\
    1. contains the C# payload to decrypt the registry values under 1. above

After extracting and decrypting the payload from the registry keys, TRU identified the payload as IcedID.

From Generic Cobalt Strike to Customized Cobalt Strike

As previously stated, TRU has seen GootLoader exclusively using Cobalt Strike payloads in 2022. However, the Cobalt Strike beacon profiles for these samples demonstrated default settings, making them easy to find in the wild. This could be a sign that the actors managing the Cobalt Strike payload do not have the capabilities to configure stealthy Beacons — or that they really want to blend in so as to reduce the chance that their uniquely identifiable Tactics, Techniques, and Procedures (TTPs) will be detected. Despite these easily discoverable Cobalt Strike servers, GootLoader campaigns have recently resulted in successful hands-on intrusions.

In contrast, Cobalt Strike configurations associated with IcedID, particularly in connection to Conti and FiveHands ransomware infrastructure, were more sophisticated. Incidents utilizing this Cobalt Strike infrastructure leveraged malleable Command & Control (C2) profiles and custom injection targets which allowed intruders to hide their C2 and subsequent intrusion activities.

In GootLoader -> IcedID incident observed by TRU, IcedID's payload was not observed, but TRU acknowledges that future GootLoader infections could lead to more sophisticated Cobalt Strike infections.

If you're not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services to disrupt threats before they impact your business. Want to learn more about how we protect organizations globally? Connect with an eSentire Security Specialist.

Indicators:

IcedID sha256: a9fc2b58e0e714a5135bff2d7c5c3a1d46359363696bdfa3feaabeb6f6bdc3af

IcedID C2: 64.227.182.2 ilekvoyn[.]com

GootLoader C2 exracted from .js file: www[dot]liveshopping-aktuell[dot]de www[dot]lightnessofbeing[dot]net www[dot]lintelconsulting[dot]co[dot]uk

GootLoader filenames employee confidentiality agreement texas(9898).zip employee_confidentiality_agreement_texas 19855.js

Appendix

GootLoader SEO Poisoning without forum overlay: