



Inspired eLearning April Newsletter

PHISHING PREVENTION IN 2021

PHISHPROOF REPORT: PHISHING PREVENTION IN 2021

Learn phishing statistics from 2020 and prevention techniques to protect your organization in 2021.

[VIEW REPORT](#)

WEBINAR

Security Awareness In 2021:
What You Don't Know *Can* Hurt You

WEBINAR: SECURITY AWARENESS IN 2021

Watch our webinar for a discussion that considers how and what to train for in Security Awareness in 2021.

[WATCH WEBINAR](#)

Hackers Using Website's Contact Forms to Deliver IcedID Malware

Microsoft has warned organizations of a "unique" attack campaign that abuses contact forms published on websites to deliver malicious links to businesses via emails containing fake legal threats, in what's yet another instance of adversaries abusing legitimate infrastructure to mount evasive campaigns that bypass security protections.

"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," the company's threat intelligence team said in a write-up published last Friday.



IcedID is a Windows-based banking trojan that's used for reconnaissance and exfiltration of banking credentials, alongside features that allow it to connect to a remote command-and-control (C2) server to deploy additional payloads such as ransomware and malware capable of performing hands-on-keyboard attacks, stealing credentials, and moving laterally across affected networks.

Microsoft researchers said the attackers might have used an automated tool to deliver the emails by abusing the enterprises' contact forms while circumventing CAPTCHA protections. The emails themselves employ legal threats to intimidate victims, claiming that the recipients "allegedly used their images or illustrations without their consent and that legal action will be taken against them." By invoking a sense of urgency, the idea is to lead the victim into revealing sensitive information, click a sketchy link, or open a malicious file. This infection chain links to a sites.google.com page, which requires users to sign in with their Google credentials, following which a ZIP archive file is automatically downloaded.

The ZIP file contains a heavily obfuscated JavaScript file that downloads the IcedID malware. What's more, the malicious code has the capacity to download secondary implants like Cobalt Strike, potentially putting affected victims at further risk.

The novel intrusion route notwithstanding, the attacks are yet another sign of how threat actors constantly tweak their social engineering tactics to target companies with an intent to distribute malware while evading detection.

"The scenarios [...] offer a serious glimpse into how sophisticated attackers' techniques have grown while maintaining the goal of delivering dangerous malware payloads such as IcedID," the researchers said. "Their use of submission forms is notable because the emails don't have the typical marks of malicious messages and are seemingly legitimate."

This article was originally posted by The Hacker News. Read the full article [here](#).

CISA Releases Tool to Detect Microsoft 365 Compromise

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has released a new tool to help with the detection of potential compromise within Microsoft Azure and Microsoft 365 environments.

Dubbed Aviary, the new tool is a dashboard that makes it easy to visualize and analyze output from Sparrow, the compromise detection tool that was released in December 2020.



Built by CISA to help with the detection of malicious activity related to SolarWinds compromise,

Sparrow can be used by network defenders to hunt for potential malicious activity within Microsoft Azure Active Directory (AD), Microsoft 365 (M365), and Office 365 (O365) environments.

Sparrow was designed to help identify both accounts and applications that might have been compromised within an organization's Azure/M365 environment.

With Sparrow, defenders can look out for domain authentication or federation modifications, find new and modified credentials in logs, detect privilege escalation, detect OAuth consent and users' consent to applications, identify anomalous SAML token sign-ins, and check the Graph API application permissions for service principals and apps in the environment, among others.

A Splunk-based dashboard, the newly released Aviary is meant to facilitate the analysis of output data from Sparrow.

The tool is now available on GitHub, with additional information on how to install Aviary, after running Sparrow, included in CISA's January announcement for the detection tool, which has been updated this week with instructions on using Aviary.

For more details, read the full article [here](#).

New Malware Downloader Spotted in Targeted Campaigns

In recent weeks, a relatively sophisticated new malware downloader has emerged that, while not widely distributed yet, appears to be gaining momentum.

Malwarebytes researchers recently discovered the Saint Bot dropper, as they have termed it, being used as part of the infection chain in targeted campaigns against government institutions in Georgia.



Saint Bot was discovered by researchers while investigating a phishing email containing a zip file containing malware they had never seen before. The zip file included an obfuscated PowerShell script disguised as a link to a Bitcoin wallet. According to Malwarebytes, the script started a chain of infections that led to Saint Bot being dropped on the compromised system.

In each case, the attackers used Saint Bot to drop information stealers and other malware downloaders. According to the security vendor, the new loader is probably being used by a few different threat actors, implying that there are likely other victims.

One of the information stealers that Saint Bot has noticed dropping is Taurus, a malware tool designed to steal passwords, browser history, cookies, and data from auto-fill. The Taurus stealer can also steal FTP and email client credentials, as well as system information such as configuration

details and installed software. According to Malwarebytes, while Saint Bot mostly has been observed dropping stealers, the dropper is designed to deliver any malware on a compromised system.

Malware droppers are specialized tools designed to install various types of malware on victim systems. One of the most notable recent examples of such malware is Sunburst, the tool that was distributed via poisoned SolarWinds Orion software updates to some 18,000 organizations worldwide. In that case, the dropper was specifically designed to deliver targeted payloads on systems belonging to organizations of particular interest to the attackers.

Basically, the downloaders are first-stage malware tools designed to deliver a wide range of secondary and tertiary commodity payloads, such as ransomware, banking Trojans, cryptominers, and other malicious tools. Some of the most popular droppers in recent years, such as Emotet, Trickbot, and Dridex, began as banking Trojans before their operators switched tactics and used their Trojans as malware-delivery vehicles for other criminals.

Saint Bot, like many other droppers, has several unclear and anti-analysis features to help it avoid malware detection tools. It is designed to detect virtual machines and, in some cases, to detect but not execute on systems located in specific Commonwealth of Independent States countries, which include former Soviet bloc countries such as Russia, Azerbaijan, Armenia, Uzbekistan, Ukraine, and Moldova.

"As we were about to publish on this downloader, we identified a few new campaigns that appear to be politically motivated and where Saint Bot was being used as part of the infection chain. In particular, we observed malicious documents laced with exploits often accompanied by decoy files." a spokesman from Malwarebytes' threat intelligence team states. In all instances, Saint Bot was eventually used to drop stealers.

According to Malwarebytes, while Saint Bot is not yet a widespread threat, there are indications that the malware's creators are still actively working on it. According to the security vendor, its investigation of the Saint Bot reveals that a previous version of the tool existed not long ago. " Additionally, we are also seeing new campaigns that appear to be from different customers, which would indicate that the malware author is involved in further customizing the product," a Malwarebytes spokesman said.

This article was originally posted on E Hacking News. Read the full article [here](#).

Product Updates

We have exciting new updates to share! Click below to learn more about what Inspired eLearning is doing to better our product experience for our customers.

LEARN MORE

Connect with us:



© 2021 Inspired eLearning, LLC. All rights reserved.

info@inspiredelearning.com | 800.631.2078

4630 N Loop 1604 W, Suite 401

San Antonio, TX 78249 USA

[Privacy Notice](#)