FEB EDITION 2022

THE THINGS YOU SHOULD KNOW

Low-Detection Phishing Kits Increasingly Bypass MFA

As MFA continues to see widespread consumer and business adoption, a full 78 percent of respondents in a recent poll said they used it in 2021 – cybercriminals have devoted resources into keeping up. According to an analysis from Proofpoint, MFA-bypass phishing kits are proliferating rapidly, ''ranging from simple open-source kits with human-readable code and no- frills functionality to sophisticated kits utilizing numerous layers of obfuscation and built-in modules that allow for stealing usernames, passwords, MFA tokens, social security numbers and credit-card numbers.''

One of the phishing-kit approaches that are particularly gaining steam is the use of transparent reverse proxies (TRPs), which enable attackers to insert themselves into existing browser sessions. This MiTM approach lets adversaries hide and harvest information as it is entered or appears on the screen.

There are three TRP kits in particular that have seen upticks in use lately.

- **Muraena/Necro Browser**
- **Evilginx2**
- **Modlishka**

PowerPoint Files Abused to Take Over Computers

Attackers are using socially engineered emails with .ppam file attachments that hide malware which can rewrite Windows registry settings on targeted machines.

Researchers have found that attackers use an under-the-radar PowerPoint file to hide malicious executables that can rewrite Windows registry settings to take over an end user's computer.

It is one of the numerous stealthy ways used by threat actors recently to target desktop users through trusted applications they use daily, via emails designed to evade security detections and appear **legitimate.**

Mitigations and Prevention

One is to install email protection that downloads all files into a sandbox and to inspect them for
malicious content. Another is to take extra security steps, such as dynamically analyzing emails for indicators of compromise (IoCs), to ensure the safety of messages coming into the corporate network, he said.

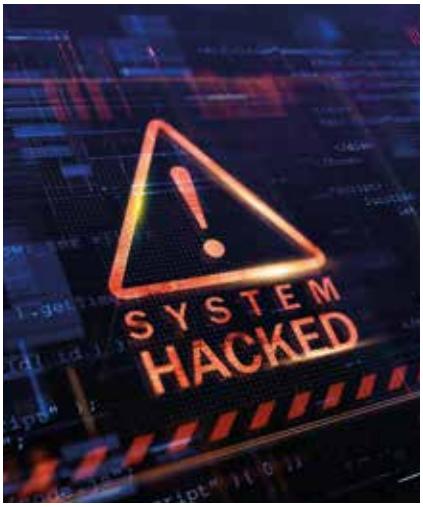
"This email failed an SPF check, and there was an insignificant historical reputation with the sender." SPF, Sender Policy Framework, is an email authentication technique used to prevent spammers and other bad actors from sending messages spoofed to come from another domain name.

Apple Pays $100.5K Bug Bounty for Mac Webcam Hack

A researcher who showed Apple how its webcams can be hijacked via a universal cross-site scripting bug (UXSS) - Safari bug, has been awarded what is reportedly a record $100,500 bug bounty. An adversary could use the bug as part of an attack to gain full access to every website ever visited by the victim.

The bug-finder is Ryan Pickren, founder of proof-of-concept sharing platform BugPoC and a former Amazon Web Services security engineer. This isn't the first time he has found bugs that let him hoodwink Apple's cameras. In 2020, he discovered vulnerabilities in the Safari browser that could be used to snoop on iPhones, iPads and Mac computers using their microphones and cameras just by convincing a target to click one malicious link.

DeadBolt – A Virus – A Ransomware



DeadBolt is Crypto-Virus able to make all your files inaccessible. DeadBolt does this in order to blackmail you for your access to the said files.

Once the malware infiltrates its victims' computers, it starts seeking all files in the system that belong to some predefined formats and types. Usually, the targets are text files, spreadsheets, presentations, and other document data, as well as images, videos, audio files, and so on. As soon as the malware finds all of the predetermined data types in the computer, it begins the process of locking them up. The lockdown procedure may take some time, especially if the computer is not very powerful and has a lot of data on it, which the virus has targeted. During this period of time, the user may be able to spot some of the potential infection symptoms – a slow-down of the system, spikes in the use of RAM and CPU, as well as occasional freezes of the whole system and maybe some unusual errors.

Upon the completion of the lockdown on the files, the virus spawns a banner message on the desktop, and within this message, hackers state their demands. The victim is told that their only hope for restoring the data is through the payment of a ransom. This is why this type of virus is known as Ransomware; their main goal is to extort money from you via blackmailing.

The DeadBolt virus is known for using data encryption. The encryption algorithm of the DeadBolt virus is what makes this Ransomware capable of sealing your files.

The .DeadBolt file encryption is a tricky obstacle to overcome. To unlock the .DeadBolt file encryption, you will need a key corresponding to the applied algorithm.

That key is, of course, held by the hackers – the payment they want you to make is in exchange for the said key. However, as we established, the payment isn't a very wise option, so what can one do then? Well, removing the virus is a good start – it won't automatically make your files free, but it will allow you to try some alternative recovery options.

What to do? Want to try a decrypting tool...instead of recovering!

Emsisoft Decryptor for DeadBolt

DeadBolt encrypts QNAP devices using AES-128 and appends the extension ".deadbolt".

This decryptor requires a key received after paying the criminals. More details in the following source:

https://www.emsisoft.com/ransomware-decryption-tools/how-tos/emsisoft_howto_deadbolt.pdf

Govt. Improves Cyber Fraud Redressal Mechanism on National Consumer Helpline

Amid the rising number of cyber fraud complaints on the National Consumer Helpline (NCH), the Consumer Affairs Ministry has tied up with its Home, Finance and IT/Telecom counterparts to improve cyber fraud redressal mechanism on the NCH. Currently, there is a national helpline 155260 under the home ministry, where people can report cyber fraud cases. It is valid in a few states, and time-bound restrictions are in place to call for the service.

Nation-State Cyber-Attack Tools Enter Black Market, With Rise In Ransomware As A Service

India has been ranked among the top-3 most frequently attacked countries for years, according to our own Cyber Readiness Report 2020/2021. With 1.15 billion phones and 700 million internet users, India exposes a vulnerable and large user base and plenty of surfaces for cyber-attacks to take off.

Ransomware as a Service (RaaS) groups coordinate supply chain attacks, with the operators of the Maze RaaS using data extortion as a tactic to pressure their victims into paying ransoms, netting an estimated $75 million from their victims.

Employees can be trained in basic cybersecurity measures to drastically reduce the instances of cyber-attacks and the amount of data compromised. Employee training involves teaching your employees to recognize phishing attacks,

creating strong passwords, and being cautious about what data they entrust whom with. Especially with the pandemic encouraging a large surge in remote work, cybersecurity training for employees is more critical than ever.

At TSAROLABS, Cybersecurity experts are available for hire to train employees, with annual refresher courses encouraged as the landscape of cyber-attacks is constantly changing. Conducting drills is another way to keep employees on their toes, with fake phishing attempts or fake social engineering attacks being a couple of examples.

Phishing Campaign by TSAROLABS

Cracking Human Mind is much easier than hacking a computer or business. Attackers prey on human weaknesses like fear, greed, trust, desire, ego, sympathy, ignorance, carelessness, and haste.

Phishing is the process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity using bulk emails, which try to evade spam filters. Emails claiming to be from popular social websites, banks, auction sites, or IT administrators are commonly used to lure the unsuspecting public. It is a form of criminally fraudulent social engineering.

Phishing was officially recognized in 2004 as a fully organized part of the black market. Specialized software emerged on a global scale that could handle phishing payments, which in turn outsourced a huge risk. The software was then implemented into phishing campaigns by organized crime gangs. In late 2006, a computer worm unleashed on MySpace altered links for direct users to fake websites made to steal login credentials. Experiments have shown a success rate of more than 70% for phishing attacks on social networks.

The availability of data on the dark web makes it easy for cybercriminals, even those with minimal technical skills, to launch phishing campaigns. Once the data from the dark web is purchased, all the attacker needs to do is send out emails, SMS, WhatsApp messages to potential victims. Phishtank and OpenPhish are a few sites where crowd-sourced lists of known are kept and are often referred to as phishing kit sites.

Interesting series to watch: Jamtara, a serial on Netflix, is a direct replica of how phishing is done at Jamtara, a city in Jarkhand State.

Types of Phishing attacks:

Spear phishing attacks target an individual or small group, typically with access to sensitive information or the ability to transfer funds. Cybercriminals gather information about the intended target in advance, leverage it to personalize the attack, create a sense of familiarity and make the malicious email seem trustworthy.

Whaling is a spear-phishing attack that specifically targets senior executives at a business.

Vishing, or voice phishing, uses a telephone message to get potential victims to call back with their personal information. Cybercriminals often use fake caller-ID details to make the calls appear from a legitimate organization or business.

Smishing, also known as SMS phishing, uses text messages to try to lure victims into revealing account information or installing malware.

Business Email Compromise is a form of phishing in which the attacker obtains access to the business email account of a high-ranking executive (like the CEO). With the compromised account at their disposal, they send emails to employees within the organization impersonating as the CEO with the goal of initiating a fraudulent wire transfer or obtaining money through fake invoices.

Evil twin phishing involves setting up what appears to be a legitimate Wi-Fi network that lures victims to a phishing site when they connect to it. Once they land on the site, they're typically prompted to enter their personal data, such as login credentials, which then goes straight to the hacker. Once the hacker has these details, they can log into the network, take control of it, monitor unencrypted traffic and find ways to steal sensitive information and data.

Tips to Spot and Prevent Phishing Attacks:

• An email asks you to confirm personal information: If you get an email that seems authentic but seems out of the blue, it's a strong sign that it's an untrustworthy source.

• Poor grammar: Misspelled words, poor grammar or a strange turn of phrase is an immediate red flag of a phishing attempt.

• Messages about a high-pressure situation: If a message seems like it was designed to make you panic and take action immediately, tread carefully—this is a common maneuver among cybercriminals.

• Suspicious links or attachments: If you received an unexpected message asking you to open an unknown attachment, never do so unless you're fully certain the sender is a legitimate contact.

• Too good to be true offers: If you're being contacted about what appears to be a once-in-a-lifetime deal, it's probably fake.