September 2, 2021

The Security Brief

CyberSecurity Updates from Computer Orange

Top Threats This Week

computerorange
fresh technology solutions

THE HIVE

FBI Identifies Ransomware Group

The Federal Bureau of Investigation released a flash report detailing an organization containing a group of malicious actors and their practices known as "The Hive".

The group is responsible for deploying multiple ransomeware mechanisms to infiltrate business networks and exfiltrate data. The Hive takes advantage of the biggest security risk in any organization - the employee. The organization will send out phishing emails in attempt to lure the employee into giving the group remote access to the machine. Once inside the network, the group can move from machine to machine using remote desktop services. Their main objective is to encrypt files on machines while leaving a ransomware note.

The report notes a few key points:

1) Hive ransomware focuses on backups and antivirus by interrupting and taking over process to manipulate files
2) The group will encrypt the stolen files but not remove them so they are unreadable
3) A trail will be left

To better protect your organization, please ensure your employees know and understand best security practices such as blocking phishing emails and avoiding downloadable links from untrusted sources.

If you would like additional training for your employees to avoid phishing emails, please contact us.

For more info, please visit: https://www.ic3.gov/media/news/2021/210825.pdf

HOME WIFI VUNERABILITY

As many employees are still working remotely, vulnerabilities in their home network is of increasing concern. Please share the following with your staff, particularly if they conduct work on their home WiFi.

If your WiFi router was manufactured prior to 2015, it may be time to consider upgrading. Many devices prior to 2015 had chipset flaws allowing remote hackers to control connected devices. This flaw was found in at least 65 different companies and hackers are already exploiting the vulnerability according to the IoT (internet of things) inspectors report.

A group known for using Mirai malware has already begun launching attacks on specific models prior to 2015. All the vulnerable devices were made by a Taiwanese company called Realtek.

In response to the flaw, the company has made patches for its models that were made in 2015 and newer leaving anything made prior to 2015 exposed.

What you need to do:

- If your model is from 2015 or newer, please ensure your firmware is up to date on the devices.

- If your model was manufactured before 2015, please check the full list of venerable devices at: https://www.tomsguide.com/news/router-attack-botnet-realtek

- If you are not sure if your WiFi is safe or not, feel free to contact us for assistance!

AVOIDING SCAMS & HACKERS

As a penetration tester, I found it necessary to showcase the importance of teaching your employees the basics of Information Security.

For a hacker to gain access to a system, it only takes one wrong click from an employee. As your company grows and you onboard new employees, the number of opportunities for accidents happen grows proportionately. In most cases, a hacker or scam artist's success relies on well-intentioned employees accidentally creating an opportunity for exploitation.

For example, CISA released an article on hurricane phishing email scams, which can be found at : https://us-cert.cisa.gov/ncas/current-activity/2021/08/21/hurricane-related-scams

The senders of these emails are well aware that hurricanes are ravaging our country right now, and are using that to prey on those impacted.

Always ensure your employees do not give away personal information or click on untrusted/unfamiliar links.

For any questions or concerns , please contact us.

WELCOME TO
computerorange
fresh technology solutions
"We got where we are because our choices mapped the route and paved the road."
— Tim Cook