REN-ISAC Daily Watch Report
2022-05-18
SHARING GUIDELINES: This report can be shared within -closed- communities of cyber security practitioners. It must NOT be shared publicly.

Handlers: Sheryl Swinson (REN-ISAC), Jennifer Pacenza (REN-ISAC), Ivan Valencia (REN-ISAC), and other credits [A].

CRITICAL NOTICES
================
Nothing to report.

VULNERABILITIES and EXPLOITS (only items of particular note)
==

Microsoft Warns of Brute-Force Attacks Targeting MSSQL Servers
https://www.bleepingcomputer.com/news/security/microsoft-warns-of-brute-force-attacks-targeting-mssql-servers/

Microsoft warned of brute-forcing attacks targeting Internet-exposed and poorly secured Microsoft SQL Server (MSSQL) database servers using weak passwords.

While this isn't necessarily the first time MSSQL servers have been targeted in such attacks, Redmond says that the threat actors behind this recently observed campaign are using the legitimate sqlps.exe tool as a LOLBin (short for living-off-the-land binary).

"The attackers achieve fileless persistence by spawning the sqlps.exe utility, a PowerShell wrapper for running SQL-built cmdlets, to run recon commands and change the start mode of the SQL service to LocalSystem," the Microsoft Security Intelligence team revealed.

Large-Scale Attack Targeting Tatsu Builder WordPress Plugin
https://www.securityweek.com/large-scale-attack-targeting-tatsu-builder-wordpress-plugin

Tens of thousands of WordPress websites are potentially at risk of compromise as part of an ongoing large-scale attack targeting a remote code execution vulnerability in the Tatsu Builder plugin.

Tracked as CVE-2021-25094 (CVSS score of 8.1), the vulnerability exists because one of the supported actions does not require authentication when uploading a zip file that is extracted under the WordPress upload directory.

While the plugin includes an extension control, this can be bypassed by adding a PHP shell with a filename that begins with a dot ("."). Furthermore, a race condition in the extraction process allows for an attacker to call the shell file.

National Cybersecurity Agencies Describe Commonly Used Initial Access Techniques
https://www.securityweek.com/national-cybersecurity-agencies-describe-commonly-used-initial-access-techniques

Cybersecurity agencies in the United States, the United Kingdom, Canada, the Netherlands, and New Zealand warn that threat actors exploit poor security practices for initial access to victim environments.

Common techniques employed by adversaries looking to compromise a target system include exploitation of public-facing applications or external remote services, phishing, the use of valid credentials, and exploitation of trusted relationships.

Authorities in the five concerned countries have identified a series of weaknesses that malicious actors typically look to exploit in their attacks, which include improper security controls, weak configurations, and overall poor cybersecurity practices.

CISA Advisory:
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-137A-Weak_Security_Controls_and_Practices_Routinely_Exploited_for_Initial_Access.pdf

-----

NVIDIA Patches Code Execution Vulnerabilities in Graphics Driver
https://www.securityweek.com/nvidia-patches-code-execution-vulnerabilities-graphics-driver

NVIDIA has announced the roll-out of updates for its graphics drivers to address multiple vulnerabilities, including four CVEs rated “high severity.”

The most severe of these issues are CVE-2022-28181 and CVE-2022-28182 (CVSS score of 8.5), which could lead to “code execution, denial of service, escalation of privileges, information disclosure, and data tampering,” NVIDIA says.

Both security holes could be exploited by an “unauthorized attacker on the network” to cause “an out-of-bounds write through a specially crafted shader.”

US-CERT:

Threat Actors Exploiting F5 BIG-IP CVE-2022-1388 (AA22-138A)
https://www.cisa.gov/uscert/ncas/alerts/aa22-138a

MALWARE and RANSOMWARE (only items of particular note)
==

Microsoft Warns of "Cryware" Info-Stealing Malware Targeting Crypto Wallets
https://thehackernews.com/2022/05/microsoft-warns-of-cryware-info.html

Microsoft is warning of an emerging threat targeting internet-connected cryptocurrency wallets, signaling a departure in the use of digital coins in cyberattacks.

The tech giant dubbed the new threat "cryware," with the attacks resulting in the irreversible theft of virtual currencies by means of fraudulent transfers to an adversary-controlled wallet.

"Cryware are information stealers that collect and exfiltrate data directly from non-custodial cryptocurrency wallets, also known as hot wallets," Berman Enconado and Laurie Kirk of the Microsoft 365 Defender Research Team said in a new report.

When Your Smart ID Card Reader Comes with Malware
https://krebsonsecurity.com/2022/05/when-your-smart-id-card-reader-comes-with-malware/

The Common Access Card (CAC) is the standard identification for active-duty uniformed service personnel, selected reserve, DoD civilian employees, and eligible contractor personnel. It is the principal card used to enable physical access to buildings and controlled spaces and provides access to DoD computer networks and systems.

Mark said when he received the reader and plugged it into his Windows 10 PC, the operating system complained that the device’s hardware drivers weren’t functioning properly. Windows suggested consulting the vendor’s website for newer drivers.

Out of an abundance of caution, Mark submitted Saicoo’s drivers file to Virustotal.com, which simultaneously scans any shared files with more than five dozen antivirus and security products. Virustotal reported that some 43 different security tools detected the Saicoo drivers as malicious. The consensus seems to be that the ZIP file currently harbors a malware threat known as Ramnit, a common but dangerous trojan horse that spreads by appending itself to other files.

HACKS, ATTACKS, and DATA THEFT/LOSS
===================================

Over 380,000 Kubernetes API Servers Exposed to Internet: Shadowserver
https://www.securityweek.com/over-380000-kubernetes-api-servers-exposed-internet-shadowserver

ShadowServer is conducting daily scans of the IPv4 space on ports 443 and 6443, looking for IP addresses that respond with an HTTP 200 OK status, which indicates that the request has succeeded.

Of the more than 450,000 Kubernetes API instances identified by Shadowserver, 381,645 responded with “200 OK”. This does not mean these servers are fully open or vulnerable to attacks, but Shadowserver believes they represent an “unnecessarily exposed attack surface” and this level of access was likely not intended.

More than half of the exposed instances are located in the United States, with many also seen in Western Europe, Southeast Asia, and Australia.

Hackers Compromise a String of NFT Discord Channels
https://www.vice.com/en/article/k7wmpy/hackers-compromise-a-string-of-nft-discord-channels

Hackers compromised several Discord servers of popular NFT projects on Tuesday in an attempt to trick users into giving up cryptocurrency or buying fake NFTs.

Late on Tuesday night, the blockchain cybersecurity firm PeckShield published an alert on Twitter warning that the Discord servers of the NFT projects Memeland, PROOF/Moonbirds, RTFKT, as well as the web3 infrastructure company CyberConnect, were compromised, the latest in a string of hacks against NFT projects through their Discord servers.

CyberConnect confirmed the hack on Twitter, asking users not to click on any link on Discord, and reminding them that the project will never ask for their private keys.

REPORTS, PAPERS, and PRESENTATIONS
==================================

Researchers Expose Inner Workings of Billion-Dollar Wizard Spider Cybercrime Gang
https://thehackernews.com/2022/05/researchers-expose-inner-working-of.html

The inner workings of a cybercriminal group known as the Wizard Spider have been exposed, shedding light on its organizational structure and motivations.

"Most of Wizard Spider's efforts go into hacking European and U.S. businesses, with a special cracking tool used by some of their attackers to breach high-value targets," Swiss cybersecurity company PRODAFT said in a new report shared with The Hacker News. "Some of the money they get is put back into the project to develop new tools and talent."

Wizard Spider, also known as Gold Blackburn, is believed to operate out of Russia and refers to a financially motivated threat actor that's been linked to the TrickBot botnet, a modular malware that was officially discontinued earlier this year in favor of improved malware such as BazarBackdoor.

APTs Overwhelmingly Share Known Vulnerabilities Rather Than Attack O-Days
https://threatpost.com/apts-overwhelmingly-share-known-vulnerabilities-rather-than-attack-o-days/179657/

Most advanced persistent threat groups (APTs) use known vulnerabilities in their attacks against organizations, suggesting the need to prioritize faster patching rather than chasing zero-day flaws as a more effective security strategy, new research has found.

Security researchers at the University of Trento in Italy did an assessment of how organizations can best defend themselves against APTs in a recent report published online. What they found goes against some common security beliefs many security professionals and organizations have, they said.

The team manually curated a dataset of APT attacks that covers 86 APTs and 350 campaigns that occurred between 2008 to 2020. Researchers studied attack vectors, exploited vulnerabilities–e.g., zero-days vs public vulnerabilities–and affected software and versions.

Arxiv Report:
https://arxiv.org/pdf/2205.07759.pdf

TOOLS and TIPS
==============

How to Protect Your Data When Ransomware Strikes
https://thehackernews.com/2022/05/how-to-protect-your-data-when.html

Initiating a ransomware attack is all about discretely gaining access. And as employees can now access your data from anywhere, you have lost visibility into how they do so. To safeguard against these attacks, you're not just looking for malware, you need continuous insights into your users, the endpoints they use and the applications and data they access.

Lookout, a leader in endpoint-to-cloud security, has published an interactive infographic to help you visualize how a ransomware attack happens and understand how to protect your data. Lookout will use this blog to set up 1) the climate that resulted in $20-billion dollars in ransom payments in 2021, and 2) how you can protect your organization from these ongoing threats.

Lookout Report:
https://www.lookout.com/infographic/ransomware

ARTICLES and OTHER
==================

Apple Unveils Online Training to Close IT Skills Gap Around Managing Apple Devices
https://techcrunch.com/2022/05/18/apple-unveils-online-training-to-close-it-skills-gap-around-managing-apple-devices/

As with many skilled professions these days, there is a gap between demand and supply when it comes to IT pros. As more people turn to Apple devices at work, whether computers, phones or tablets, the need for people who can service and manage these devices has increased.

While we may find ourselves in an economic downturn at the moment, it doesn’t really change the math when it comes to the IT skills gap, we are seeing, one that is expected to linger until the end of the decade.

To address this issue, Apple announced it has updated its certification and training for IT pros and management who are working with Apple products. That includes two specific courses being added online: Apple Device Support and Apple Deployment and Management.

NEWS
=======

CISA: Majority of US Government Will Get EDR Later in 2022
https://www.govinfosecurity.com/cisa-majority-us-government-will-get-edr-later-in-2022-a-19095

Endpoint detection and response deployments will be underway at more than half of federal civilian agencies by the end of September, according to federal officials.

The Cybersecurity and Infrastructure Security Agency is currently in the process of deploying EDR across 26 federal civilian agencies and expects to have work underway at 53 agencies by Sept. 30, says Eric Goldstein, CISA's executive assistant director for cybersecurity. Goldstein was one of four witnesses at a congressional hearing Tuesday focused on strengthening federal network cybersecurity.

"One of the lessons learned from the SolarWinds intrusion is that we need to correlate threat activity that we might see at the perimeter of a federal agency to something happening at a workstation to something happening in the cloud," Goldstein said at the hearing. "This EDR visibility is really foundational in giving us the ability to connect the dots on intrusions far more quickly."

PATCHES
========

Cisco Security Advisories and Alerts
https://tools.cisco.com/security/center/publicationListing.x

[HIGH]

Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Interface Privilege Escalation Vulnerability

-----

Debian:

[SECURITY] [DSA 5137-1] needrestart security update
https://lists.debian.org/debian-security-announce/2022/msg00105.html

[SECURITY] [DSA 5138-1] waitress security update
https://lists.debian.org/debian-security-announce/2022/msg00106.html

[SECURITY] [DSA 5139-1] openssl security update
https://lists.debian.org/debian-security-announce/2022/msg00107.html

-----

Debian LTS:

[SECURITY] [DLA 3013-1] needrestart security update
https://lists.debian.org/debian-lts-announce/2022/05/msg00024.html

[SECURITY] [DLA 3014-1] elog security update
https://lists.debian.org/debian-lts-announce/2022/05/msg00025.html

-----

SUSE:

SUSE-CU-2022:1062-1: Security update of bci/dotnet-aspnet
https://lists.suse.com/pipermail/sle-security-updates/2022-May/011066.html

SUSE-CU-2022:1064-1: Security update of bci/dotnet-sdk
https://lists.suse.com/pipermail/sle-security-updates/2022-May/011067.html

SUSE-CU-2022:1066-1: Security update of bci/dotnet-sdk
https://lists.suse.com/pipermail/sle-security-updates/2022-May/011068.html

SUSE-CU-2022:1068-1: Security update of bci/dotnet-sdk
https://lists.suse.com/pipermail/sle-security-updates/2022-May/011069.html

SUSE-CU-2022:1070-1: Security update of bci/dotnet-runtime
https://lists.suse.com/pipermail/sle-security-updates/2022-May/011070.html

SUSE-CU-2022:1072-1: Security update of bci/dotnet-runtime
https://lists.suse.com/pipermail/sle-security-updates/2022-May/011071.html

SUSE-CU-2022:1074-1: Security update of bci/dotnet-runtime
https://lists.suse.com/pipermail/sle-security-updates/2022-May/011072.html

SUSE-CU-2022:1076-1: Security update of bci/golang
https://lists.suse.com/pipermail/sle-security-updates/2022-May/011073.html

-----

Ubuntu:

[USN-5425-1] PCRE vulnerabilities
https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006567.html

[USN-5426-1] needrestart vulnerability
https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006569.html

[USN-5427-1] Apport vulnerabilities
https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006568.html

[USN-5423-2] ClamAV vulnerabilities
https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006570.html

[USN-5428-1] libXrandr vulnerabilities
https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006571.html

-----

UPCOMING CONFERENCES, WORKSHOPS, TRAINING, ETC.
==

<<< conferences >>>

REFERENCES
==========

[A] CREDITS

Thanks to the following individuals for contribution to the Daily Report:

Sheryl Swinson (REN-ISAC), co-editor
Jennifer Pacenza (REN-ISAC), co-editor
Ivan Valencia (REN-ISAC), writer