News from Monday, June 19, 2023. Reported on Tuesday, June 20, 2023.

Live links are embedded throughout today's briefing. To see the actual URL, hover your mouse over the link for a moment before clicking. These links were copied directly from the web site of the source article. Tyler Cybersecurity has not performed any testing on the sites / links for security.

Sources	Articles
Information Security Media Group	**SeroXen Malware Latest to Deploy BatCloak Evasion Tool** A batch file obfuscation engine known as BatCloak requires minimal programming skills to use. Among its recent successes is a recent remote access Trojan dubbed SeroXen that researchers from multiple firms said resists detection by antivirus and endpoint detection and response tools. A SeroXen sample analyzed by AT&T in May provoked zero detections on VirusTotal. Analysis published by Trend Micro earlier this month, of hundreds of infected batch file samples taken from a public repository, concluded that BatCloak shielded 80% of the files from detection by security software. Batch files, often designated with a .bat extension, are plain text files with scripts for a command-line interpreter. SeroXen showed up in late 2022 and retailed for $30 a month or $60 outright. It is a variation of the well-established Quasar RAT, AT&T reported. The hacker apparently behind SeroXen used a still-active website, seroxen.net, to distribute the Trojan, although the site currently says sales are suspended "as of now." The site marketed the malware as "fully undetectable," or "FUD." TrendMicro on Thursday released analysis that says one of the techniques BatCloak uses to hide SeroXen from detection is sophisticated string manipulation, which obfuscates the malware's use of a Windows command prompt interface to designate environment variables through the set command.
Bleeping Computer	**Android spyware camouflaged as VPN, chat apps on Google Play** Three Android apps on Google Play were used by state-sponsored threat actors to collect intelligence from targeted devices, such as location data and contact lists. The malicious Android apps were discovered by Cyfirma, who attributed the operation with medium confidence to the Indian hacking group "DoNot," also tracked as APT-C-35, which has targeted high-profile organizations in Southeast Asia since at least 2018. In 2021, an Amnesty International report linked the threat group to an Indian cybersecurity firm and highlighted a spyware distribution campaign that also relied on a fake chat app. The apps used in DoNot's latest campaign perform basic information gathering to prepare the ground for more dangerous malware infections, representing what appears to be the first stage of the threat group's attacks. The suspicious applications found by Cyfirma on Google Play are nSure Chat and iKHfaa VPN, both uploaded from 'SecurITY Industry.' Both apps and a third from the same publisher, which does not appear malicious according to Cyfirma, remain available on Google Play. The download count is low for all SecurITY Industry's apps, indicating they are used selectively against specific targets. The two apps request risky permissions during installation, such as access to the user's contact list (READ_CONTACTS) and precise location data (ACCESS_FINE_LOCATION), to exfiltrate this information to the threat actor.

Sources	Articles
Bleeping Computer	**ASUS urges customers to patch critical router vulnerabilities** ASUS has released new firmware with cumulative security updates that address vulnerabilities in multiple router models, warning customers to immediately update their devices or restrict WAN access until they're secured. As the company explains, the newly released firmware contains fixes for nine security flaws, including high and critical ones. The most severe of them are tracked as CVE-2022-26376 and CVE-2018-1160. The first is a critical memory corruption weakness in the Asuswrt firmware for Asus routers that could let attackers trigger denial-of-services states or gain code execution. The other critical patch is for an almost five-year-old CVE-2018-1160 bug caused by an out-of-bounds write Netatalk weakness that can also be exploited to gain arbitrary code execution on unpatched devices. "Please note, if you choose not to install this new firmware version, we strongly recommend disabling services accessible from the WAN side to avoid potential unwanted intrusions. These services include remote access from WAN, port forwarding, DDNS, VPN server, DMZ, port trigger," ASUS warned in a security advisory published today. "We strongly encourage you to periodically audit both your equipment and your security procedures, as this will ensure that you will be better protected." The list of impacted devices includes the following models: GT6, GT-AXE16000, GT-AX11000 PRO, GT-AX6000, GT-AX11000, GS-AX5400, GS-AX3000, XT9, XT8, XT8 V2, RT-AX86U PRO, RT-AX86U, RT-AX86S, RT-AX82U, RT-AX58U, RT-AX3000, TUF-AX6000, and TUF-AX5400. **Malwarebytes issues fix for Chrome broken by Windows 11 KB5027231** Malwarebytes released a fix for a known issue breaking Google Chrome on its customers' systems after installing the Windows 11 22H2 KB5027231 cumulative update released last week. On Wednesday, the company confirmed user reports that the Google Chrome user interface would no longer show up after deploying this month's Patch Tuesday cumulative updates. The conflict with Google Chrome is caused by Malwarebytes' anti-exploit module blocking the web browser from loading or crashing after installing the KB5027231 update. Customers affected by this known issue were advised to toggle off Chrome's entry from the list of protected applications in their Malwarebytes product as a temporary workaround. Malwarebytes has now fixed the conflict with the Chrome web browser on up-to-date Windows 11 systems. "This fix enables Chrome as a protected application for all Windows 11 devices but does not apply our Anti-exploit code to all Chrome processes," the company says. "Update to Component version: 1.0.2047 and Malwarebytes version: 4.5.31.270 to receive this fix. This update is automatic over time. To manually update, open Malwarebytes, click Settings > About > Check for updates." Malwarebytes says the update will be automatically applied to new installations and advises customers who used the workaround to re-enable the anti-exploit protection for Chrome after the fix is installed.

Sources	Articles
HIPAA Journal	**TimisoaraHackerTeam Ransomware Group Linked to Recent Attack on U.S. Cancer Center** An alarm has been sounded about a relatively unknown threat group called TimisoaraHackerTeam following a recent attack on a U.S. medical facility. TimisoaraHackerTeam is believed to be a financially motivated threat group, which in contrast to many cybercriminal and ransomware groups, has no qualms about attacking the healthcare and public health (HPH) sector and appears to actively target HPH sector organizations, mainly conducting attacks on large organizations. The group was first identified in July 2018 but has largely stayed under the radar. According to the Healthcare Sector Cybersecurity Coordination Center (HC3), which issued the alert on June 16, the group has resurfaced and conducted a June 2023 ransomware attack on a U.S. cancer center which rendered its digital services unavailable, put the protected health information of patients at risk, and significantly reduced the ability of the medical center to provide treatment for patients. The group has exploited known vulnerabilities to gain initial access to HPH sector networks, then escalates privileges, moves laterally, and encrypts files. The group uses Microsoft's native disk encryption tool, BitLocker, along with Jetico's BestCrypt, rather than custom ransomware. This allows the group to encrypt files without being detected by security solutions. Previous attacks that have been loosely attributed to TimisoaraHackerTeam include an attack on a French hospital in April 2021 which involved similar living-off-the-land tactics, and an attack on Hillel Yaffe Medical Center in Israel, which resulted in the cancellation of non-elective procedures and forced the medical center to switch to alternative systems to continue to provide patient care.
The Hacker News	**Researchers Discover New Sophisticated Toolkit Targeting Apple macOS Systems** Cybersecurity researchers have uncovered a set of malicious artifacts that they say is part of a sophisticated toolkit targeting Apple macOS systems. "As of now, these samples are still largely undetected and very little information is available about any of them," Bitdefender researchers Andrei Lapusneanu and Bogdan Botezatu said in a preliminary report published on Friday. The Romanian firm's analysis is based on an examination of four samples that were uploaded to VirusTotal by an unnamed victim. The earliest sample dates back to April 18, 2023. Two of the three malicious programs are said to be generic Python-based backdoors that are designed to target Windows, Linux, and macOS systems. The payloads have been collectively dubbed **JokerSpy**. The first constituent is shared.dat, which, once launched, runs an operating system check (0 for Windows, 1 for macOS, and 2 for Linux) and establishes contact with a remote server to fetch additional instructions for execution. This includes gathering system information, running commands, downloading and executing files on the victim machine, and terminating itself. On devices running macOS, Base64-encoded content retrieved from the server is written to a file named "/Users/Shared/AppleAccount.tgz" that's subsequently unpacked and launched as the "/Users/Shared/TempUser/AppleAccountAssistant.app" application. The same routine, on Linux hosts, validates the operating system distribution by checking the "/etc/os-release" file. It then proceeds to write C code to a temporary file "tmp.c," which is compiled to a file called "/tmp/.ICE-unix/git" using the cc command on Fedora and gcc on Debian. Bitdefender said it also found a "more potent backdoor" among the samples, a file labeled "sh.py" that comes with an extensive set of capabilities to gather system metadata, enumerate files, delete files, execute commands and files, and exfiltrate encoded data in batches.

Sources	Articles
The Record Media	**Microsoft resolves 'dangerous' new Azure vulnerabilities** Microsoft recently fixed two vulnerabilities affecting two Azure-related tools that would have allowed hackers to access a victim's data and make changes to their virtual environment. Researchers with Orca Security said they discovered two "dangerous" vulnerabilities with Azure Bastion and Azure Container Registry that could allow attackers to achieve cross-site scripting (XSS) – a process involving hackers injecting malicious scripts into trusted websites. These kinds of vulnerabilities can lead to unauthorized access, data theft, and even the complete compromise of the affected system. Orca Security's Lidor Ben Shitrit said the vulnerabilities they discovered "acted as the entry point for attackers to exploit XSS flaws" and could "lead to severe consequences, including unauthorized data access, unauthorized modifications, and disruption of the Azure services iframes." Azure Bastion allows users to access virtual machines within an Azure cloud environment, while Azure Container Registry provides users with a centralized location to store container images – foundational files containing code that runs on IT infrastructure. Microsoft told Recorded Future News that it is not aware of any exploitation of the vulnerabilities beyond the proof-of-concept provided by Orca researchers. Both Microsoft and Orca Security said the Azure Bastion issue was reported to the Microsoft Security Response Center on April 1 and the Azure Container Registry problem was reported on May 3. Microsoft confirmed in a statement that exploitation of the vulnerabilities could have potentially allowed hackers to gain access to a target's session within the compromised Azure service, leading to "data tampering or resource modification." "A series of fixes were developed and deployed according to our Safe Deployment Practices and completed on 24 May 2023, after which the issue is considered mitigated for both services. No further action is required from customers to remain secure."
SANS	**CISA: Government Agencies' Systems Suffered Cyberattack** The MOVEit vulnerability was exploited against systems at some US federal agencies, according to Cybersecurity and Infrastructure Security Agency (CISA) executive assistant director for cybersecurity Eric Goldstein. CISA "is providing support to several federal agencies that have experienced intrusions affecting their MOVEit applications." A Department of Energy spokesperson confirmed that they are among the affected agencies. **Ransomware Attack Contributed to Hospital's Decision to Shut Down Permanently** St. Margaret's Health (SMH) will shut down multiple facilities in Spring Valley and Peru, Illinois, on Friday, June 16 due to several factors, including a ransomware attack that began in February 2021. SMH has been serving the community since 1903. The ransomware attack impacted SMH systems for four months, impeding their ability to collect payments from insurers. Other factors cited in the decision to close the facilities were COVID-19 expenses and staff shortages. **FCC Will Establish Privacy and Data Protection Task Force** The US Federal Communications Commission (FCC) has announced that it will establish a Privacy and Data Protection task force. Among the task force's responsibilities are updating the agency's data breach rules, overseeing investigations and enforcement actions, and helping to create rules to protect consumers from SIM-swapping.

Source	Long Form Article
Dark Reading by Stephen Lawton (6-8 Minute Read)	**Generative AI Has Its Risks, But the Sky Isn't Falling** Generative artificial intelligence (GenAI) and large language models (LLMs) are the disruptive technologies *du jour*, redefining how enterprises do business and spurring the debate on just how much AI will change the way the civilization interacts with computers in the future. The hyperbole is reaching epic proportions as social scientists and pundits debate the End Times facing civilization due to smarter and potentially proactive computing. Perhaps some perspective is in order. A recent report from the Israeli venture firm Team8, "Generative AI and ChatGPT Enterprise Risk," addresses some of the realistic technical, compliance, and legal risks GenAI and LLMs place on corporate boards, C-suites, and cybersecurity personnel. The Team8 report underscored the potential operational and regulatory vulnerabilities of GenAI, but cautioned that some concerns might be premature. One concern — that exposing private data submitted to a GenAI application such as ChatGPT might make that data available to others in near real time — is discredited in the report. "As of this writing, Large Language Models (LLMs) cannot update themselves in real-time and therefore cannot return one's inputs to another's response, effectively debunking this concern," the report states. "However, this is not necessarily true for the training of future versions of these models." "The CISO is in a position to have the technical knowledge to support processes not necessarily under their umbrella which might affect their role," says Gadi Evron, CISO-in-residence at Team8 and one of the report's authors. "Some interpretations of upcoming European Union regulation may push the CISO into a position of responsibility when it comes to AI. This may elevate the CISO to a position of responsibility where they are 'Ambassadors of Trust,' and this is a positive thing for the CISO role." Chris Hetner, cybersecurity advisor at Nasdaq and chair of Panzura's Customer Security Advisory Council, says an initial risk assessment would identify potential issues with who has access, what can be done, and how the technology will interact with existing applications and data stores. "You need to determine who has access to the platform, what level of data and code are they going to introduce, [and does] that data and code introduce any proprietary exposure to the enterprise. Once those decisions are made, there's a process to proceed forward," he notes. The threat organizations face with GenAI is not new, but it could speed how quickly private data reaches a wider audience. "When it comes to security, it is clear that most companies are in much worse condition to mitigate the risks of their corporate and customer being stolen or leaked than they were just six months ago," opines Richard Bird, chief security officer at Traceable AI. "If we're being intellectually and historically honest with ourselves, the vast majority of companies were already struggling to keep that same data safe before the rise of generative AI. "The ease of use and access that employees are already taking advantage of with AI technologies with little to no security controls is already showing the increased risk to companies," he continues. Bird takes a pragmatic approach to GenAI, adding that companies are going to move fast and not wait on compliance demands to protect their data, customers, supply chains, and technologies. Users have shown "a complete lack of restraint combined with no awareness of the unintended security consequences of using AI," he notes. "This toxic combination is what companies must work quickly to address," Bird says. "AI isn't the key threat here, human behavior is." One issue that has yet to be fully analyzed is how users interact with GenAI based on their existing habits and experience. Andrew Obadiaru, CISO for Cobalt Labs, notes that iPhone users, for example, already have native experience with AI through Siri, and thus will adapt quicker than users who do not have that experience. Like Bird, Obadiaru thinks those habits might make those users more susceptible to misusing the applications by inputting data that should not get out of an organization's direct control. "The concerns are, 'What are the additional risks?' Everyone has the ability to tap into (GenAI technology) without necessarily going through a security review. And you can just do that on their personal device," he says.

Source	Long Form Article
	If employees use personal devices outside of the IT department's control to conduct business, or if employees use GenAI as they use Siri or similar applications, this could pose a security risk, Obadiaru says. Using GenAI like a personal digital assistant potentially could put confidential data at risk. Sagar Samtani, assistant professor in the Data Science and Artificial Intelligence Lab at the Indiana University Kelley School of Business, cautions that AI models are extensively shared via the open source software landscape. These models contain significant quantities of vulnerabilities within them, some of which CISOs need to be aware of. "These vulnerabilities place an impetus on organizations to understand what models they are using that is open source, what vulnerabilities they contain, and how their software development workflows should be updated to reflect these vulnerabilities," Samtani says. He adds that asset management is a critical aspect to any strong cybersecurity program. It's "not the exciting answer, but an essential ingredient. Automated tools for detecting and categorizing data and assets can play a pivotal role in mapping out corporate networks. ... Generative AI could help provide layouts of corporate networks for possible asset management and vulnerability management tasks. Creating inventory lists, priority lists, vulnerability management strategies, [and] incident response plans can all be more [easily] done with LLMs in particular."