SIM2K
Adapting Technology to Your Business Needs

10•20
Information you can use

SIMformation

Malware Targets Healthcare System

A major hospital chain has been hit by what appears to be one of the largest medical cyberattacks in United States history.

Computer systems for Universal Health Services, which has more than 400 locations throughout the US, began failing over the last weekend of September, causing some hospitals to resort to filing patient information with pen and paper.

UHS operates 328 inpatient behavioral healthcare facilities, one surgical hospital, six "ambulatory" surgery centers, and 14 "freestanding emergency departments."

Universal Health Services posted a statement on its website that the company-wide network was "currently offline, due to an IT security issue." The company did note, however, that no patient or employee data "appears to have been accessed, copied or misused." A person familiar with the company's response effort said the attack "looks and smells like ransomware." Hackers seeking to deploy ransomware often wait until the weekend, when a company is likely to not have as many technical staff members present.

As we have discussed many times in SIMformation, Ransomware is a type of malicious software that spreads across computer networks, encrypting files and demanding payment for a key to decrypt them. It's become a common tactic for hackers, though attacks of this scale against medical facilities aren't common. A patient died after a ransomware attack against a German hospital in early September required her to be moved to a different hospital, probably the first known death as a consequence of a ransomware attack.

Two Universal Health Services nurses, who requested to not be named because they weren't authorized by the company to speak with the media, said that the attack began over the weekend and had left medical staff to work with pen and paper.

One of the nurses, who works in a facility in North Dakota, said that computers slowed and then eventually simply would not turn on in the early hours of Sunday morning. "As of this a.m., all the computers are down completely," the nurse said.

Another registered nurse at a facility in Arizona who worked this weekend said "the computer just started shutting down on its own. Our medication system is all online, so that's been difficult." While many patient charts at that facility are on paper, medication information is maintained online, though it's backed up at the end of each day, the nurse said.

"We had those up to date as of the 26th," the person said. "Now we had to hand-label every medication," the nurse said. "It's all improv."

While UHS didn't mention what kind of attack it suffered, other information coming from workers seems to point to the Ryuk ransomware as the culprit. An employee said that encrypted files were being appended with the ".ryk" extension, and a ransom note that showed up on all affected computers referenced the phrase "Shadow of the Universe" which is known to be part of Ryuk ransom notes.

Some on-line forums floated the specter of patients dying because of a lack of care. "One of the busiest hospitals in the region is currently sending away all ambulances to different smaller hospitals because of this, and they themselves are losing patients while they are waiting for lab results to be delivered by courier….four people died tonight alone due to the waiting on results from the lab to see what was going on," the post reads. However, this was not confirmed, but added to the confusion involving this attack.

Ransomware can devastate hospitals. In 2017, a ransomware strain called WannaCry, created by hackers working for the North Korean government, spread across the world and infected the U.K.'s National Health System even though it wasn't a direct target. The attack disrupted at least 80 medical facilities, though there were no deaths reported from this incident.

A computer security engineer with experience working with hospital networks said that the delays caused by ransomware attacks can have dire consequences for patients. "When nurses and physicians can't access labs, radiology or cardiology reports, that can dramatically slow down treatment, and in extreme cases, force re-routing for critical care to other treatment centers," he said. "When these systems go down, there is the very real possibility that people can die."

While your business may not involve healthcare, this incident shows that Ransomware is never to be taken lightly. Last month, SIMformation discussed Vulnerability Management tools that SIM2K can use to help identify weak points in your company's security, and training for staff to identify possible malware attacks and how to handle these without infecting your network. We take security seriously and hope you will contact us if you have concerns.

Microsoft Azure Security Flaws

Researchers have disclosed two flaws in Microsoft's Azure web hosting application service, App Services, which if exploited could enable an attacker to take over administrative servers. Azure App Services is an HTTP-based service for hosting web applications, and is available in both Microsoft Azure Cloud and on-premise installations. Researchers found two vulnerabilities in the cloud service that specifically affect Linux servers.

"The two vulnerabilities we found allow us to combine them and enable any attacker with the ability to forge post requests (SSRF) or [remote] code execution on an Azure App Service to take over the Azure App Service administration server," said a researcher with Intezer. Both flaws were discovered three months ago and reported to Microsoft. Microsoft has since issued a fix.

The first flaw stems from an open-source project called KuduLite within Azure App Services. This Linux project manages the administration page that is used to register administrators into the App Service Plan. After discovering that the KuduLite instance's SSH service uses hardcoded credentials "root:Docker!" to access the application node, researchers were able to log in as root.

After taking control of the KuduLite instance, researchers could then gain control over the Software Configuration Management (SCM) web server, which systematically manages and controls changes in the documents and codes during the Software Development Life Cycle. This allowed them to then listen to a user's HTTP requests to the SCM web page, add their own pages and inject malicious Javascript into the user's web page. The attacker could then add malicious code to the software and extend this into other applications on the server.

The second flaw exists in the KuduLite API. The issue here stems from the application node being able to send requests to the KuduLite API without access validation. An attacker who manages to forge a GET request may access the application node's file system which would enable an attacker to easily steal source code and other assets.

These two vulnerabilities can be chained together, since once an attacker achieves code execution with the second vulnerability, they can then exploit the first one. One potential attack vector here is for an attacker to use this flaw to implant a phishing page.

Researchers stressed that cloud security is still relatively new, making is critical to implement some form of runtime security to catch malicious actions in the formative stage as it can detect malicious code injections and other in-memory threats that take place after a vulnerability has been exploited by an attacker.

If you are a Microsoft Azure Cloud user, be aware of this potential security hazard and be sure your underlying plaform has been updated and secure. Contact SIM2K for more information or assistance in establishing Cloud security.

Chrome Browser Improvements

Google released Chrome 85 in early September, making several enhancements to the browser's tab-based user interface and a 10% reduction in page load times. Chrome updates in the background, so most users can finish the refresh by relaunching the browser. To manually update, select "About Google Chrome" from the Help menu under the vertical ellipsis at the upper right; the resulting tab shows that the browser has been updated or displays the download process before presenting a "Relaunch" button.

What's New – Google bundled several new tab features into Chrome 85; one added functionality to the tab grouping that debuted earlier this year. With tab grouping, users can organize tabs in the tab bar by lumping together several tabs, each lump designated by color and name. New tabs can be added to the group by dragging and dropping or from a right-click menu; existing tabs can be dumped from a group as well.

Chrome 85 lets users collapse and expand those tab groups. A click on the group's label collapses all associated tabs into the label, removing them from the bar. A second click restores them to the bar. This feature is being gradually rolled out, meaning that it won't be available to everyone at once. To turn on the new feature manually, enter chrome://flags in the address bar and press Return or Enter. Search for the Tab Groups Collapse item and select Enabled from the menu list at the right. Finally, restart Chrome.

Google also introduced tab previews in Chrome 85, the Beta build. When the user pauses the mouse pointer atop a tab, a thumbnail of the page appears in a small pop-up, portraying what the tab leads to.

The other improvement is in page load time. Google claimes that pages will load up to 10% faster in Chrome 85 after "Profile Guided Optimization" (PGO) was switched on. Chrome 85 also suspends page painting in browser windows covered by other windows, a way to save on CPU processing and thus save on power consumption. Only some users will see this in the latest Chrome, however. Google promised a "full rollout" for Chrome 86, the next upgrade.

And, Google will enable a new PDF-related feature in Chrome 85 "over the next few weeks." Users will be able to fill out PDF-based forms – account applications, for instance – from within the browser, then save the results. If the same PDF document is later opened, the already-entered information is retained, and the user can pick up where they left off.

Chrome 85 also continues the implementation of a blockade imposed on downloads from insecure sources. The first download category – executable files in .exe format – was barred here with more categories to follow in subsequent releases.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Teams Updated for Better Collaboration

Microsoft Teams has unveiled new updates to its video conferencing software including a "Together Mode" that puts participants into a virtual meeting hall. The goal is to make video conferences more informal and bring participants together. Instead of, say, 49 individual participant rectangles as in Gallery mode, Together mode removes the "squares" and uses what Microsoft calls "AI segmentation technology" to place the head and shoulders of participants side-by-side in a virtual auditorium. Microsoft is currently working on other views that will available in this mode, including a virtual coffee shop.

Microsoft says the new viewing mode is a direct consequence of the pandemic and the significant increase in the number of video calls people make. With many employees now in the midst of their fourth month working from home because of the COVID-19 outbreak, daily video calls with colleagues have become the new normal as teams try to continue working collaboratively across different environments. During pandemic, Teams has seen its daily active user count race past 75 million users.

While Together mode might seem a like a gimmick, the underlying technology is fundamental to improving the video conferencing experience. On most video calls, eye contact – or the lack of – is an ongoing problem, with people often appearing to look in the wrong direction. Together mode mimics the geometry of reflection, meaning that every participant is looking at the whole group through a big virtual mirror. "Once direct eye contact errors become hard to detect, people intuitively position themselves to look as if they are reacting to one another appropriately," Microsoft explains, as research has shown that people tend to feel happier and more engaged in meetings.

Additionally, everyone in Together mode is in a fixed position. If one person happens to appear in the fourth seat of the bottom row on their own screen, that person would appear in the fourth seat of the bottom row on everyone else's screen.

While Together mode is the main new Microsoft Teams feature, it's not the only update rolling out in this month. Dynamic view will make it easier for participants to share content on-screen alongside the view of your participants – a direct contrast to Together mode which currently does not offer users the ability share content or present. Dynamic view also includes virtual breakout rooms, where participants can be split into smaller groups for more focused discussions or brainstorming sessions.

In a further effort to make meetings more inclusive, Teams is also rolling out live reactions and emojis, providing participants with the ability to react instantly to each other in a non-verbal way. In-meeting chats sent during a Teams session will appear as on-screen chat bubbles, eliminating the need for users to open a separate chat window and distracting them from the video call. Microsoft is also adding live transcripts to Teams later this year along with the ability to translate live captions into subtitles so anyone can follow a meeting conducted in another language.

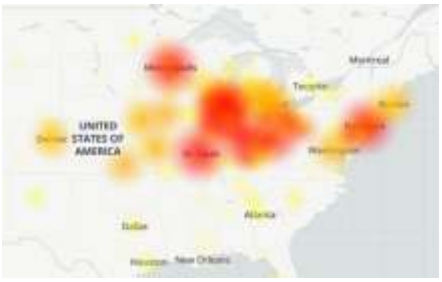
Finally, Teams users will be given access to video filters, allowing them to subtly adjust lighting levels and soften the focus of the camera to customize their appearance.

The pandemic is changing how businesses conduct meetings and we are seeing the IT industry race to adapt to these changing times. If you are interested in Teams, Zoom and other video tools please call SIM2K for information.

"Random Tid-Bytes"

Microsoft Outages Affecting Exchange, Teams

On September 28 and again on October 1 and 7, Microsoft users suffered a massive outage impacting Teams, Office 365 and Outlook. The September outage affected users worldwide. A Microsoft spokesperson said the downtime was a service interruption while performing authentication operations and no indication of malicious activity being the cause. Shortly thereafter, the Microsoft 365 Status account has tweeted that it is "reviewing recent changes to our service" in order to determine the cause of the service disruption, which appears to center on those accessing Exchange Online accounts Then, Microsoft said it was caused by a "recent change" as well, before relatively quickly confirming that rolling back to before that change was made had no effect. Microsoft ended up rerouting traffic to alternative infrastructure, which appeared to resolve the situation. The latest, on October 7, impacted North America and seemed to target the Midwest. Again, Microsoft blamed it on "infrastructure changes" and indicated services would be restored later that day. The question is, why did Microsoft apparently release an update that trashed their services without any prior testing in a non-production environment on multiple occasions? If the first outage wasn't a wake-up, why did they repeat this "infrastructure change" again a week later with the same impact? If you were affected, your services should be back up and functioning now.



October 7 outage map

Chrome Slipping?

Google's Chrome fell a full percentage point in browser share last month, while Microsoft's Edge added a third as much. Meanwhile, Mozilla's Firefox effectively held steady. According to data by Net Applications, Chrome's September share declined to 69.9%, falling back under the important psychological bar of 70% for the first time since May. The one-point decline was the largest since October 2019, when Chrome dumped 1.1%. September's decline meant that Chrome has fallen for two straight months, very uncharacteristic of the browser leader. Chrome last had a two-month downturn in November-December 2019. After that earlier loss, Chrome rebounded by adding four full percentage points over the following three quarters. In other words, while it may be tempting to see any sustained slide as evidence that Chrome has peaked, previous predictions along those lines have been proven wrong. Edge, on the other hand, closed September at 8.8%, a record for the browser. Since January, when Microsoft released a revamped Edge based on Google's Chromium project code, Edge has added more than 1.8% to its share. Over the past 12 months, Edge gained nearly 3 points. At that pace (about a quarter of a point per month), Edge should sit at 9.6% at year's end, at 12.8% by this time in 2021, at 14%, give or take, at the end of next year. Firefox earned a very small increase – less than one-tenth of a percentage point – to finish September at 7.2%, the second-lowest share since it first pushed towards double digits 15 years ago. Apple's Safari stuck with 3.6%, slight movement upwards caused by rounding. Opera software's Opera did the same, staying at 1% in September.

Long Live "Big Iron" Computing

The mainframe computer has been declared "dead", "morphed" and "transformed" so many times over the years sometimes it's sometimes hard to believe the Big Iron still has an identity in the enterprise world. But clearly it does and in a major way, too. As an example: According to IBM, 75% of the top 20 global banks are running the newest z15 mainframe, and the IBM Systems Group reported a 68% gain in Q2 IBM Z revenue year-over-year.

At the heart of its current vitality is Linux – primarily in the form of Big Iron-based Red Hat OpenShift – and a variety of software and open source applications. Applying Linux on mainframes has been a boon for this sector. "For the first five or so years we really were just experimenting with what we could do with Linux and the mainframe but then the server-consolidation movement hit, and we knew we had something big," said an IBM manger. "What really got us going was the big Wall Street financial companies who all had these Sun Solaris servers with big databases, and many decided to consolidate on the Z mainframe running Linux, and we were off and running," he said. Another contributing factor was Big Blue's 2002 $1B investment in Linux software development plus all of the open-source mainframe software work going on in the Linux Foundation's Open Mainframe Project. Now customers have a myriad of options for private or public Cloud-based workloads. Gartner recently wrote of that trend: "Now developers, testers, and infrastructure and operations staff have the capability to utilize the same tools which exist in the distributed world."

Another key development is an overarching security model called Confidential Computing which IBM broadly describes as a way to protect data, applications and processes at scale. It has rolled out a number products that adhere to the Confidential Computing mantra such as IBM's Secure Execution for Linux software lets customers isolate and protect large numbers of workloads from internal and external threats across a hybrid-cloud environment.

IBM is on its fourth generation of Confidential Computing technology which will keep it out in front of other industry cloud players and give the company a strong security weapon for the foreseeable future. Deloitte recently conducted a survey of business and IT decision makers with Forrester Consulting and found 80% of respondents are focused on modernizing mainframe toolsets in an effort to identify and prevent data breaches, and 73% are increasing their security footprint. Data protection and security are so critical, and mainframes remain one of the most secure and powerful platforms available when the right controls are in place," Gartner said.

Another direction IBM and the mainframe is moving is toward a more cloud-agile, consumption-based licensing model that lets customers pay only for what they consume. IBM rolled out its Tailored Fit Pricing model in 2019 and has upwards of 80 customers onboard so far. It offers two consumption-based pricing models that can help customers cope with ever-changing workload and hence software costs.

Others say technologies such as machine learning and artificial intelligence will also drive future mainframe development. "Data insights help drive actionable and profitable results—-but the pool of data is growing at astronomical rates. That's where AI can make a difference, especially when it's on a mainframe. Consider the amount of data that resides on a mainframe for an organization in the banking, manufacturing, healthcare, or insurance sectors. You'd never be able to make sense of it all without AI," said Deloitte.

As an example, core banking operations can do more than simply execute large volumes of transactions. "Banks need deep insights about customer needs, preferences, and intentions to compete effectively, along with speed and agility in sharing and acting on those insights. That's easier said than done when data is constantly changing. Now if you can analyze data directly on the mainframe, you can get near real-time insights and action. That makes the mainframe an important participant in the AI/ML revolution," the Deloitte spokesman said.

Another challenge is finding and developing the right people to cultivate the mainframe environment. It was predicted mainframes would eventually cease to exist so colleges stopped offering courses focused on COBOL and other critical mainframe skills. As Baby Boomers retire, mainframe talent concerns are becoming a reality. Deloitte's survey found that 71% of respondents said their teams are understaffed, and 93% said its "moderately" to "extremely challenging" to acquire the right mainframe resources and skills. Many large companies are addressing this issue by hiring and developing college recruits, developing a mentoring program, creating an internship, or turning to third parties for support. Mainframes aren't going anywhere—the talent pool needs to match the demand, according to industry watchers.

While there are challenges in the future, Deloitte says the consultancy's survey showed customers are looking to increase their investment in the mainframe with 91% of respondents identified as expanding their mainframe footprints as a moderate or critical priority in the next 12 months. So anyone thinking "big iron" is obsolete needs to change their views on the viability of mainframes.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com