EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

CELEBRATING OVER 30 YEARS

October 15, 2021 - Volume 13, Issue 19

Criminals Increasingly Targeting PC Gamers During The Pandemic

Who doesn't enjoy some late-night gaming to blow off some steam and earn bragging rights? Especially during a pandemic when folks are largely trapped in their homes and looking for ways to entertain themselves. Criminals are the perfect opportunists and also observed that online gaming has surged during COVID-19 lockdowns and have shifted their sight pattern to attack gamers. How bad has the problem escalated? The number of attacks reported from ONE security vendor showed a 66% increase between Q1 (1.48 million detections) and Q2 (2.48 million detections) of 2020 – and mobile (versus desktop computer) gamers were also increasingly targeted. The article provides a link to the researcher's findings.

NEWSLETTER NOTES

* Criminals …

* DRONE REMOTE ID RULE

* CFIUS, …

* TrickBot gang developer arrested …

* State Department Plans 'China …

* American Big Tech Firms Help China …

* China Wields New Legal Weapon to Fight …

* Today's Cyber Word …

* Why 2-Factor …

* New Report Reveals Traditional …

* Biden Administration Releases …

* Rethinking …

* FBI Official: Russia Hasn't Cracked …

* Cyber Criminals …

* SECURING …

* Online Gamers…

DRONE REMOTE ID RULE

https://www.faa.gov/uas/getting_started/remote_id/

UAS Remote Identification Overview

UAS Remote Identification

Drones or unmanned aircraft systems (UAS) are fundamentally changing aviation, and the FAA is committed to working to fully integrate drones into the National Airspace System (NAS). Safety and security are top priorities for the FAA and remote identification (remote ID) of drones is crucial to our integration efforts.

What is Remote ID?

Remote ID is the ability of a drone in flight to provide identification and location information that can be received by other parties.

Why Do We Need Remote ID?

Remote ID helps the FAA, law enforcement, and other federal agencies find the control station when a drone appears to be flying in an unsafe manner or where it is not allowed to fly. Remote ID also lays the foundation of the safety and security groundwork needed for more complex drone operations.
Final Rule on Remote ID

The final rule on remote ID will require most drones operating in US airspace to have remote ID capability. Remote ID will provide information about drones in flight, such as the identity, location, and altitude of the drone and its control station or take-off location. Authorized individuals from public safety organizations may request identity of the drone's owner from the FAA.

The FAA's Notice of Proposed Rulemaking (NPRM) on Remote Identification of Unmanned Aircraft Systems was published on December 31, 2019. The FAA received over 53,000 comments on the NPRM during the 60-day comment period following publication. The FAA reviewed all of the comments and considered them when writing the final rule. The final rule (PDF) was published in the Federal Register on January 15, 2021 with an original effective date of March 16, 2021. Corrections made to the rule and published in the Federal Register on March 10, 2021 delayed the effective date to April 21, 2021.

*(*Continued On The Following Column)*

There are three ways drone pilots will be able to meet the identification requirements of the remote ID rule:

- Operate a Standard Remote ID Drone (PDF) that broadcasts identification and location information about the drone and its control station. A Standard Remote ID Drone is one that is produced with built-in remote ID broadcast capability in accordance with the remote ID rule's requirements.
- Operate a drone with a remote ID broadcast module (PDF). A broadcast module is a device that broadcasts identification and location information about the drone and its take-off location in accordance with the remote ID rule's requirements. The broadcast module can be added to a drone to retrofit it with remote ID capability. Persons operating a drone with a remote ID broadcast module must be able to see their drone at all times during flight.
- Operate (without remote ID equipment) (PDF) at FAA-recognized identification areas (FRIAs) sponsored by community-based organizations or educational institutions. FRIAs are the only locations unmanned aircraft (drones and radio-controlled airplanes) may operate without broadcasting remote ID message elements.

CFIUS, Team Telecom, and China

In the past few years, two federal government interagency committees—the Committee on Foreign Investment in the United States (CFIUS) and Team Telecom—have begun to play an important role in the government’s effort to counter potential threats from Chinese companies’ involvement in the United States. Both committees review certain foreign companies’ American investments. CFIUS has jurisdiction over a broad swathe of foreign investment in the U.S., and Team Telecom’s jurisdiction covers certain licenses for foreign telecommunications companies to operate. Both committees have become more assertive—often retroactively ordering divestiture or revocation against Chinese companies, sometimes years after an investment was completed or a license granted. And notably, both committees seem to be broadly maintaining a similar posture under President Biden as under President Trump.

TrickBot gang developer arrested when trying to leave Korea

An alleged Russian developer for the notorious TrickBot malware gang was arrested in South Korea after attempting to leave the country.

The TrickBot cybercrime group is responsible for a variety of sophisticated malware targeting Windows and Linux devices to gain access to victim's networks, steal data, and deploy other malware, such as ransomware.

An alleged Russian developer for the notorious TrickBot malware gang was arrested in South Korea after attempting to leave the country.

The TrickBot cybercrime group is responsible for a variety of sophisticated malware targeting Windows and Linux devices to gain access to victim's networks, steal data, and deploy other malware, such as ransomware.

After waiting for over a year for his passport to be renewed, the individual attempted to depart South Korea again but was arrested at the airport due to an extradition request by the USA. It is alleged that the man worked as a web browser developer for the TrickBot operation while he lived in Russia in 2016. However, the Russian man claims that he did not know he worked for a cybercrime gang after getting hired from an employment site.

"When developing the software, the operation manual did not fall under malicious software," the man told the Seoul High Court.

The Russian individual's attorney is currently fighting the USA extradition attempt, claiming that the USA will prosecute the individual unfairly.

"If you send him to the United States, it will be very difficult to exercise your right of defense and there is a high possibility that you will be subjected to excessive punishment," argued the alleged TrickBot developer's attorney.

Law enforcement's siege on TrickBot

The TrickBot gang is responsible for numerous malware, including TrickBot, BazaLoader, BazaBackdoor, PowerTrick, and Anchor. All of these (malicious tools) are used to gain access to corporate networks, steal files and network credentials, and ultimately deploy ransomware on the network.

Both the Ryuk and Conti ransomware operations are believed to be operated by the TrickBot gang and are known to be deployed through their malware.

State Department Plans 'China House' to Counter Beijing

Some fear larger State Department China desk could be a "massive bureaucratic blob."

By Jack Detsch, Foreign Policy's Pentagon and national security reporter, and Robbie Gramer, a diplomacy and national security reporter at Foreign Policy.

September 21, 2021, 4:56 PM

The U.S. State Department is planning to expand the number of officials dedicated to monitoring China, a bid to track Beijing's growing footprint in key countries around the world. The changes, which could include adding between 20 to 30 staff members, would include a boost for regional China "watch" officers: a category of officials first created during the Trump administration to track Beijing's activities around the world under the State Department's regional bureaus.

The effort to carve out a more central China desk at State, termed "China House" by some in Washington, follows a move at the U.S. Defense Department to create a central hub to handle Washington and Beijing's military relationship. The State Department initiative would add officers in both Washington as well as to embassies around the world to monitor China's activities in specific countries, according to current and former officials familiar with the matter.

One official said the State Department is also looking at adding more staff to track China's procurement of emerging technologies and efforts to tackle climate change. A State Department spokesperson declined to comment.

Changes at Foggy Bottom come as U.S. President Joe Biden's administration seeks to pivot away from two decades of costly Middle East wars to long-term global competition with China. In his debut presidential address at the United Nations General Assembly on Tuesday, Biden vowed to "compete vigorously" with other major powers but said Washington was "not seeking a new Cold War or a world divided into rigid blocs." He did not mention China by name.

The first cadre of China officers at the State Department was deployed in 2019. But the advent of the program caused infighting during the early years of the Trump administration, one former senior Trump administration official told Foreign Policy. Some senior diplomats who opposed a more confrontational approach to China pushed back on the idea of designating "China watch officers." Susan Thornton, the former top acting State Department envoy for East Asia from 2017 to 2018, called the program a "bad idea."

*(*Continued On The Following Page)*

This isn't the only or even the main impetus for current distortion, but it's a contributor," she added.

After Thornton's departure, the program advanced as the State Department tried to catch up with the Justice Department and the Treasury Department, which were ramping up efforts to target sanctions more effectively against China and blunt Chinese espionage operations. The CIA has also weighed plans to establish its own special unit to address Chinese espionage, *Bloomberg* reported in August, shedding light on how U.S. national security bureaucracies are adapting to a new era of U.S. geopolitical competition with Beijing.

"If you're building sanctions packages against Chinese targets, you need to be able to do it. If you're trying to sort through intel to tell you whether a United Front organization is structured this way or that way, you need people who have the proper expertise, and they need the proper tools," the former senior Trump administration official said. "The State Department's China desk has never been structured for any of that."

"This was just a whole posture that didn't exist on China because effectively, in historical terms, until yesterday, we were still thinking that China wants to be our friend," the former official added.

The new State Department program is aimed at herding officials who work on China across various federal government agencies, patterned after interagency programs to coordinate counterterrorism efforts. Some critics of the program worry it could give the State Department a myopic view of China that could inflate China's influence and unnecessarily hype U.S.-China tensions. They also worry it could add a new layer of bureaucracy to an already cumbersome system.

Other former officials and experts disagree, viewing this program as a way to diversify the State Department's toolkit away from strictly an embassy-centric approach to confronting China's influence operations abroad. They point to China's United Front networks that have cropped up in places like Australia in efforts to infiltrate foreign political parties and disrupt U.S. interests in the Asia-Pacific. Chinese intelligence operatives have even extended their tendrils into the United States.

"There's clearly a small cadre of these folks that are around. And I think it would be best for [the] State Department to try to find ways to leverage the intelligence community more broadly," said Brent Sadler, a senior fellow at the conservative Heritage Foundation.

*(*Continued On The Following Column)*

The State Department's reshuffling appears to be patterned after the Defense Department's efforts, which included adding more intelligence analysts in the region and shuffling Pentagon staff to focus more acutely on Beijing. U.S. Indo-Pacific Command's joint intelligence center has doubled down on efforts to produce open-source products calling out China's military expansion in the South China Sea and Cambodia.

It's been rocky. The June 2019 appointment of Chad Sbragia as the Pentagon's top China policy official led to turf battles between Asia policy offices in the building, two former officials said, as the office tried to take control of most issues that touched on the military-to-military relationship with China, even if they fell into other portfolios.

It could turn into "this massive bureaucratic blob, which is going to want to chop on everything," a former Trump administration defense official said.

American Big Tech Firms Help China SURPASS U.S. in STEM Research Through Talent Poaching and Acquisition

By Price Sukhia

For decades, the Chinese Communist Party (CCP) has viewed advanced technology as a way to "leap frog" American leadership in the STEM fields (Science, Technology, Engineering, and Mathematics) and eventually overtake the U.S. as the world's foremost super power. Increasingly, American universities and Big Tech corporations are helping the Chinese acquire top-tier talent in scientific and technological research.

This development has come into focus after a recent report from the Center for Security and Emerging Technology found that a stunning 10 percent of the collective Artificial Intelligence (AI) labs of Big Tech firms – IBM, Microsoft, Google, and Facebook – are operated in China. According to the report, U.S. tech corporations carry out research in foreign countries like China primarily to access local talent and save on costs.

But by housing research facilities in China and recruiting Chinese STEM researchers, companies like IBM and Google are directly helping Xi Jinping achieve his goal of technological dominance by strengthening and advancing China's local talent pool. This trend seems to be the latest example of how Silicon Valley's near-term financial interests are undermining the long-term economic vitality and national security of the United States.

*(*Continued On The Following Page)*

Over the past 20 years, the Chinese have placed an emphasis on securing top-level talent in the fields of scientific research, with President Xi describing talent as the primary means for China to gain the high ground in scientific research and innovation. In May of 2015, the CCP announced new initiatives to recruit overseas experts in strategic sectors as part of a larger effort to wean China's research capabilities off its dependence on American innovation. In order to achieve that goal however, Beijing must first bridge the technological divide that exists between China and America. Although the U.S. still maintains its lead in advanced technology, the Chinese have significantly narrowed the gap by acquiring technology from U.S. corporations and educational institutions seeking to grow their top lines in the Chinese market.

But formal tech transfers from American organizations are just the tip of the iceberg. So called "recruitment programs" give the CCP a back door entry into U.S. research labs allowing agents to gather sensitive equipment and the "know-how" used to advance Chinese infrastructure and bolster the capabilities of China's military. By taking advantage of open-source data, encouraging academic exchanges, and recruiting top talent in high-tech fields, China has been able to effectively leverage America's experience, facilities, and resources in key technological industries.

Programs like the Thousand Talents Plan (TTP) have become a crucial aspect of China's move to surpass the U.S. in manufacturing and technological development by 2025. The TTP is a People's Republic of China (PRC) initiative to poach leading foreign experts in the STEM fields. According to the U.S. National Intelligence Council, the underlying mission of the program is "to facilitate the illegal and illicit transfer of US technology, IP and know-how to China." From the time the program was launched in 2008 to the summer of 2014, the TTP had successfully recruited more than 4,000 scientists and researchers to China. Another PRC recruitment program called Project 111 was able to entice thirty-nine Nobel Prize winners and nearly 600 university scholars to high-ranking positions in various labs, companies and research centers in China. While these programs are advertised as benevolent initiatives designed to bring countries together through friendly collaboration in the name of science and human progress, it's become clear that they actually serve as a front for Chinese intelligence operations.

In 2018, the Department of Justice's National Security Division launched an initiative to identify and prosecute individuals engaged in trade secret theft, hacking, and economic espionage. Since then, the DOJ has tried more than eighty cases of Chinese intelligence operations within university and corporate research centers. Last year, several prominent American researchers receiving grant funding from the National Institutes of Health (NIH) were indicted by the DOJ for hiding financial ties with China's TTP.

(*Continued On The Following Column)

China Wields New Legal Weapon to Fight Claims of Intellectual Property Theft

Chinese technology giants have seized on a new legal tactic to fight claims of intellectual property theft, raising concerns in the U.S. that Beijing's promises to strictly enforce patent and copyright laws will be undermined by Chinese courts. In four major cases since 2020, Chinese courts granted so-called anti-suit injunctions blocking foreign companies from taking legal action anywhere in the world to protect their trade secrets. Three of the rulings were in favor of Chinese telecom companies—Huawei Technologies Co., Xiaomi Inc., and BBK Electronics. The fourth supported South Korea's Samsung Electronics Corp. in a dispute with Swedish telecom giant Ericsson AB. In the Xiaomi case, the Beijing-based company was granted an anti-suit injunction against InterDigital Inc., a Delaware firm that holds patents on wireless and digital technology used in smartphones. Xiaomi, the world's biggest smartphone maker, has sold millions of handsets using InterDigital patents since 2013, under industry practice that allows companies to do so while licensing fees are being negotiated.

Today's Cyber Word Of The Day: "Stalkerware"

"Stalkerware" is a term used for software that is used to surreptitiously monitor communications that traverse a telecommunications system (i.e. a PC or a cell phone). There are some valid reasons to use stalkerware – for example, parents wanting to monitor their children's communications. However, too many nefarious stalkerware apps are on the market, and now the FTC has taken action against one stalkerware app company who exploited their access to cell phone data.

(*Continued On The Following Page)

Why 2-Factor Authentication Is More Important Than Ever

Everyone knows that passwords are required to protect valuable information from falling into the wrong hands. However, hackers have advanced the art of breaking passwords using advanced techniques that can largely render passwords as useless. For example, hackers can typically break passwords that are up to 10 characters in length nearly instantly; hacked passwords are shopped around on the Dark Web, and many individuals reuse the same password across all web site accounts. The only way to defeat the hackers is via 2-Factor authentication – because they typically DON'T have access to your email or phone.

New Report Reveals Traditional Anti-Malware Solutions Miss 74% of Threats

By Corey Nachreiner, Chief Security Officer, WatchGuard Technologies

The threat landscape is an erratic and ever-evolving beast. While it knows no master, its behavior is broadly directed by the host of threat actors that pull on its reins from all corners of the world, constantly adapting their tactics and techniques to better sniff out points of weakness and infiltrate organizations. Businesses must stay up to date on the latest threat intelligence to understand their adversaries, bolster defenses and avoid falling prey. For this reason, the WatchGuard Threat Lab research team produces a quarterly security report detailing the latest malware and network attack trends based on anonymized data from tens of thousands of WatchGuard appliances deployed across the globe.

The Threat Lab's latest Internet Security Report reveals the highest level of zero-day malware detections we've ever recorded. In fact, evasive malware rates have actually eclipsed those of traditional threats, which is yet another sign that organizations must continue to evolve their defenses in order to stay ahead of increasingly sophisticated threat actors. The research also covers new threat intelligence around rising network attack rates, how malicious actors are trying to disguise and repurpose old exploits, and the quarter's top malware attacks.

*(*Continued On The Following Column)*

Hungry for more? Here are some additional key findings to feast on:

- **Network attacks are on the rise –** WatchGuard appliances detected more than 4 million network attacks, a 21% increase compared to the previous quarter and the highest volume since early 2018. Corporate servers and assets on site are still high-value targets for attackers despite the shift to remote and hybrid work, so organizations must maintain perimeter security alongside user-focused protections.
- **Fileless malware variant surges in popularity–**JSLoader is a malicious payload that appeared for the first time in both WatchGuard's top malware by volume and most widespread malware detections lists. It was also the variant WatchGuard detected most often via HTTPS inspection in Q1'21. The sample WatchGuard identified uses an XML external entity (XXE) attack to open a shell to run command to bypass the local PowerShell execution policy and runs in a non-interactive way, hidden from the actual user or victim. This is another example of the rising prevalence of fileless malware and the need for advanced endpoint detection and response capabilities.
- **Attackers disguise ransomware loader as legitimate PDF attachments with the help of a simple file name trick–** Ransomware loader Zmutzy surfaced as a top-two encrypted malware variant by volume in Q1'21. Associated with Nibiru ransomware specifically, victims encounter this threat as a zipped file attachment to an email or a download from a malicious website. Running the zip file downloads an executable, which to the victim appears to be a legitimate PDF. Attackers used a comma instead of a period in the file name and a manually adjusted icon to pass the malicious zip file off as a PDF. This type of attack highlights the importance of phishing education and training, as well as implementing back-up solutions in the event that a variant like this unleashes a ransomware infection.
- **Hackers co-opt reputable domains to mine cryptocurrency–** In Q1'21, WatchGuard's DNSWatch service blocked several compromised and outright malicious domains associated with cryptomining threats. Cryptominer malware has become increasingly popular due to recent price spikes in the cryptocurrency market and the ease with which threat actors can siphon resources from unsuspecting victims.

*(*Continued On The Following Page)*

- **An old directory traversal attack technique comes back with a vengeance–** WatchGuard detected a new threat signature in Q1’21 that involves a directory traversal attack via cabinet (CAB) files, a Microsoft-designed archival format intended for lossless data compression and embedded digital certificates. A new addition to WatchGuard’s top 10 network attacks list, this exploit either tricks users into opening a malicious CAB file using conventional techniques, or by spoofing a network-connected printer to fool users into installing a printer driver via a compromised CAB file.
- **IoT devices continue to present an attractive attack surface for malicious actors –** While it didn’t make WatchGuard’s top 10 malware list for Q1’21, the Linux.Ngioweb.B variant has been used by adversaries recently to target IoT devices. The first version of this sample targeted Linux servers running WordPress, arriving initially as an extended format language (EFL) file. Another version of this malware turns the IoT devices into a botnet with rotating command and control servers.
- **Lessons learned from HAFNIUM zero days –** Last quarter, Microsoft reported that adversaries used the four HAFNIUM vulnerabilities in various Exchange Server versions to gain full, unauthenticated system remote code execution and arbitrary file-write access to any unpatched server exposed to the Internet, as most email servers are. WatchGuard incident analysis dives into the vulnerabilities and highlights the importance of HTTPS inspection, timely patching and replacing legacy systems. You can read more here.

If there’s one key takeaway from our latest threat analysis, it’s this: Traditional anti-malware solutions alone simply aren’t sufficient for today’s threat environment. Every organization needs to have a layered, proactive security strategy that involves machine learning and behavioral analysis to detect and block new and advanced threats. Remember, to the beast that is the threat landscape, every business is fair game – and the hunt never ends.

Biden Administration Releases Draft Zero-Trust Guidance

The documents form a roadmap for agencies to deploy the cybersecurity architectures by the end of fiscal 2024.

The federal government is pushing hard for agencies to adopt zero-trust cybersecurity architectures, with new guidance released Tuesday from the administration’s policy arm—the Office of Management and Budget—and lead cybersecurity agency—the Cybersecurity and Infrastructure Security Agency.

The administration released several documents Tuesday for public comment, seeking feedback on the overarching federal policy from OMB and draft technical reference architecture and maturity model from CISA. The guidance follows a May executive order on bolstering cybersecurity across the federal government, which cited specific security methods and tools such as multifactor authentication, encryption and zero trust.

Zero-trust models continuously check on a user’s credentials as they move throughout a network, verifying not only that they are who they claim to be but also that the user has appropriate privileges to access secure apps and data. In a mature zero-trust architecture, these checks are performed routinely, including whenever a user attempts to access different segments of the network.

“Never trust, always verify,” Federal Chief Information Officer Clare Martorana said Tuesday in a statement, echoing the zero-trust architecture refrain. “With today’s zero trust announcement, we are clearly driving home the message to federal agencies that they should not automatically trust anything inside or outside of their perimeters.”

Agencies were already under mandate to develop plans to implement zero trust to meet the executive order. Now, with the new guidance and reference architectures, OMB is requiring agencies to fold new deliverables into those plans.

The memo from OMB gives agencies until the end of September 2024 to meet five “specific zero trust security goals,” all of which should be added to agency implementation plans:

- Identity: Agency staff use an enterprisewide identity to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.
- Devices: The federal government has a complete inventory of every device it operates and authorizes for government use and can detect and respond to incidents on those devices.

*(*Continued On The Following Page)*

- **Networks:** Agencies encrypt all DNS requests and HTTP traffic within their environment and begin segmenting networks around their applications. The federal government identifies a workable path to encrypting email in transit.
- **Applications:** Agencies treat all applications as internet-connected, routinely subject their applications to rigorous testing and welcome external vulnerability reports.
- **Data:** Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data and have implemented enterprise-wide logging and information sharing.

The guidance documents give additional details on what is expected for each of the five goals. Agencies will also be given one month to name an implementation lead to engage with and report to OMB.

Also on Tuesday, CISA released publicly the Zero Trust Maturity Model, or ZTMM, which was developed in June and passed around federal agencies for consideration and feedback. The maturity model was not specifically required by the executive order, but officials developed the additional guidance to help agencies move to zero trust more quickly.

The maturity model aligns with the same five goals enumerated in the OMB memo, with additional context on the tools and procedures used by organizations with a well-developed zero-trust architecture. The model also includes a breakdown of how each focus area operates in a "traditional," "advanced" and "optimal zero trust environment.

Fully adopting zero trust security across a network will require agencies to configure systems in a coordinated fashion to enable the same security tools to work across a network.

To that end, "This modernization of the federal government's cybersecurity will require agencies to transition stove-piped and siloed IT services and staff to coordinated and collaborative components of a zero trust strategy," the maturity model states.

CISA Director Jen Easterly noted the maturity model is only one of the tools the agency has developed to help the government improve its cybersecurity posture.

"Additionally, CISA teamed up with the United States Digital Service and the Federal Risk and Authorization Management Program to co-author the Cloud Security Technical Reference Architecture, which will guide agencies' secure cloud migration efforts," she said. "Through our strong partnerships and ongoing collaborative efforts, CISA will develop new and innovative ways to secure constantly changing network perimeters to enable critical federal IT modernization."

*(*Continued On The Following Column)*

The documents released Tuesday by CISA include the agency's current offerings and plans for future tools and services as the Quality Service Management Office, or QSMO, for cybersecurity.

The strategy and guidance documents provide a "common roadmap" for agencies to follow, though they are not meant to be a proscriptive guide.

"This recognizes that each agency is currently at a different state of maturity, and ensures flexibility and agility for implementing required actions over a defined time horizon," the OMB guidance states.

The guidance documents are out for public comment through Oct. 1.

"The federal government's approach to cybersecurity must rapidly evolve to keep pace with our adversaries and moving toward zero trust principles is the road we need to travel to get there," Chris DeRusha, federal chief information security officer, said in a statement. "While we feel the urgency to begin implementing this plan, we know that input from the broader community of experts will help ensure it is the right plan. We welcome feedback on how we can refine this strategy to best advance federal cybersecurity."

Rethinking backups to combat ransomware

One of the reasons ransomware attacks are successful is that victims cannot afford to be offline. Even if organizations have backups, the associated data loss and disruption caused by long restore times is often more costly than just paying off the criminals and being done with it.

Sometimes it's even worse: Cybercriminals have been known not only to encrypt an organization's data but also to target the backups themselves. In fact, on average, only 69% of health care data could be restored even after the organizations paid and got the decryption key.

This situation could be avoided if there were a way to reliably restore data from trusted and secure backups in minutes, not days or weeks.

There is, but it requires thinking about backups and data differently.

*(*Continued On The Following Page)*

Backups’ soft underbelly

Cybercriminals leverage one of the most obvious and fundamental facts about backups: backups files are written and read by the same networked operating system that are used for day-to-day business. Of course, backup files are special: They require a high level of permission to be accessed, they are compressed, redundant copies may be kept in other locations, they are kept up-to-date with a frequency that depends on how long it takes to update them and the like. But ultimately, they are just files on the system.

The integrity of those systems, therefore, depends on how secure the organization’s system is. Clearly, if criminals can encrypt an agency’s production data, then that system can be compromised, and its backups are also at risk.

Even if the hackers can’t get to the backups, the recency of those backups is a critical factor. Once-a-day backups leave an incredible amount of data unprotected, and the loss of one day’s worth of data is more than a bother, it’s often catastrophic. Imagine the financial or health-care sectors, where the loss of an hour’s worth of data can open the organization up to serious liabilities. For modern businesses, the speed and reliability of backups matter.

In addition to the loss of data, time to restore the data is another critical factor. Depending on the size of the data stores, the restoration from backups can take several hours to days resulting in unacceptable business disruption.

Rethinking backups with “air gaps”

If paying the ransom is Door #1, and successfully restoring from a backup is Door #2, agencies can make a two-part change that would let them walk through that second door. The first part of the change is to isolate the backup network and remove system-level access to backups, creating a type of logical “air gap” between the two systems. Of course, the backup system remains connected to the rest of system -- otherwise, agencies wouldn’t be able to do backups or restore -- but even a hacker who has access to production data will be locked out of the backup files.

Think of this “air-gapped” backup system as a separate data appliance: It looks to the operating system like a physical device that runs by its own rules, but it is in fact a virtual device that can read and write to the system when given the proper login credentials. It’s important that these credentials are 100% independent of the credentials expected by the main system. The original backups must be kept as read-only data behind the appliance’s sturdy door.

(*Continued On The Following Column)

Such an appliance creates the second change necessary to make Door #2 a viable alternative to paying the ransom: It creates a virtual data space. It not only manages the storing of the agency’s data on physical media, with as many off-site copies as needed, it also creates a virtualized copy of that data for production. This means that the backups can be restored in minutes, avoiding multiple days of downtime and disruption. Moreover, the frequency of backups can be increased to minutes or even to real-time, minimizing the data loss during the restore process.

Adopting such an approach affects more than how backups are made. It means that data requests can be accommodated in seconds or minutes, a huge benefit for agencies that rely on real-time transactions, and for research and development departments doing innovative work that depends on rapid iteration.

The ability of ransomware to reduce an organization’s choices to two -- pay up or lose days hoping restoring from a backup will work -- depends on a system architecture for data that needs to be urgently updated. It’s imperative agencies explore a new data architecture and rethink how they protect their backups against the scourge of ransomware.

FBI Official: Russia Hasn’t Cracked Down On Their Ransomware Gangs

Many ransomware gangs reside in Russia, with dotted lines connecting their malicious activity to Russian government officials. The U.S. has directly linked Russia to several high profile ransomware attacks launched against U.S. critical infrastructure facilities. During a recent cybersecurity summit, the FBI’s #2 stated that his agency has observed zero indicators that the Russian government has dissuaded ransomware actors operating from within Russia’s borders from attacking U.S. networks. During the first Presidential summit between the U.S. and Russian Presidents held on 16 Jun 2021, the U.S. discussed Russian ransomware attacks at length –with the U.S. sternly warning that Russian cyberattacks against U.S. critical infrastructure would not be tolerated and Russian government “help and cooperation” on this topic was expected.

Cyber Criminals Turning To Instant Messaging Apps

The Dark Web has traditionally been the “cyber swap meet” for criminals to seek out hacking tools and peddle stolen information. Apparently a new dawn is before us, as criminals are increasingly turning to a popular instant messaging (IM) software app to purchase/sell/share stolen information and software hacking tools to like-minded peers. The IM approach has the benefits of (a) not being blocked by many corporate network servers and (b) circumvents antivirus software applications.

SECURING IOT Products better

To help you properly secure your IoT devices, NordPass offers the following tips:

- **Change your default password immediately**. Create and apply a strong and secure password on your device using a password generator or a password manager.
- **Update your IoT devices**. Check your devices to see if they automatically receive security updates. If not, make sure they're running the latest firmware. Remember that software updates are vital as they fix security flaws and patch bugs.

Install a VPN on your router. A VPN can thwart man-in-the-middle attacks by encrypting your traffic, thereby compensating for the poor encryption built into many IoT devices.

“Every accomplishment starts with the decision to try.”

Online Gamers Beware - New Russian Malware On The Loose!

Russian cybersecurity company “Kaspersky” revealed they had discovered a new malware strain (coined “BloodyStealer”) that appears to primarily target highly popular gaming platforms that possess millions of user accounts. Those online gaming platforms are typically subscription-based: which means they also store credit card information that can be used for financial fraud. The malware also targets Internet browser cookie files and other software application configuration files. The “BloodyStealer” malware is being offered up to criminals for $10 a month; a one-time payment of $40 provides lifetime access.

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)

NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.

Reproduction for private use or gain is subject to original copyright restrictions.