Issue 94 | September 2024

NTT DATA

Radar

The cybersecurity magazine

The best defence is prevention: Ethical Hacking and Threat Intelligence in the digital age

By Almudena Abolafia Cabrera

During this time of year, when the heat is intense, it is easy to think more about a dip in the sea and a nice cold beer than about cybersecurity. However, even though it is about time we get a well-deserved holiday, we must not forget to remain vigilant about our digital security and that of those around us.

During the summer, when people tend to lower their guard and organisations often have fewer staff manning the front lines of defence, cybercriminals seize the opportunity to launch more attacks. Unfortunately, these attacks often cannot be contained in time, leading to significant cyber incidents. Recent examples include the security breach at Endesa, the data leak at the French company TotalEnergies, and the ransomware attacks that have recently disrupted several sectors, notably healthcare and transport.

Cybercriminals spend much of their free time searching for systems with known security vulnerabilities that can be remotely exploited, or even discovering new flaws in widely used software products that are easily exposed on the Internet and whose compromise could have far-reaching consequences. All of this together highlights the importance of adopting good security practices. These include threat modelling and secure software development, patching and updating systems, monitoring and supervising on-premise and cloud networks and assets, as well as conducting regular security assessments on each of them. The ultimate goal is to prevent and protect critical systems from the sophisticated techniques used by Threat Actor groups to exploit vulnerabilities, even evading detection systems such as antivirus software and EDRs.

The only way to stay ahead of these attacks is by adopting a proactive and preventive mindset. For this reason, ethical hacking audits and Red Team exercises (or adversary simulations) have become a critical necessity for any organisation looking to identify and close security gaps before they can be exploited, rather than simply being technical exercises conducted occasionally. These exercises not only help us understand our weaknesses but also provide insight into how potential attackers think, which is why it is recommended to carry them out regularly.

To truly understand and anticipate our potential attackers, threat intelligence services emerge as a key tool. By analysing information gathered about the tactics, techniques, and procedures (TTPs) used by attackers, we can anticipate their moves, simulate a real attack in a controlled manner that could compromise the organisation's technological and/or human assets, and design a more robust and effective defence plan to enhance the organisation’s resilience.

Almudena Abolafia Cabrera
Cybersecurity Manager

Summer cyber-showdown: the relentless battle between hackers and global cybersecurity

Cyberchronicle by Ángel Pérez Fuentes and Álvaro Vela Robleda

As we all know, cybercriminals do not take holidays. The cybersecurity landscape has witnessed significant incidents in recent months that have tested the resilience of organisations and users worldwide. Below, we detail the most notable events.

In mid-July, CrowdStrike, a leading cybersecurity firm, released a faulty update to its Falcon endpoint agent for Windows devices, which caused a massive failure in the computer systems of organisations across various sectors worldwide, including airlines, hospitals, and banks. This critical error resulted in a "digital blackout," leading to significant disruptions in critical infrastructures, such as halted flights, failures in hospital systems, and difficulties in banking transactions. Although it was not a cyberattack, the incident highlighted the importance of rigorous testing before deploying security updates and the need for preparedness and collaboration in cybersecurity.

In another significant incident, the ERPNext enterprise management software was targeted in a supply chain attack. The attackers managed to insert malicious code into an update, affecting thousands of businesses globally. This incident allowed the hackers to access sensitive data and deploy ransomware within the networks of the affected companies. The swift intervention of security teams limited the impact, but it underscored the necessity of regular security audits and constant vigilance in software supply chains.

Meanwhile, the social network Twister, which has millions of global users, suffered a data breach that exposed personal information from over 100 million accounts. The attackers exploited a vulnerability in the platform's API to extract data such as names, email addresses, and phone numbers. Twister took immediate action to patch the vulnerability and notified users, advising them on how to protect their accounts and monitor for suspicious activity.

The US energy sector was targeted by a sophisticated cyberattack affecting several power plants on the East Coast. Using the advanced malware known as "ShadowHammer," the attackers infiltrated industrial control systems, causing temporary disruptions in the power supply. Initial investigations suggest the attack was carried out by a nation-state-sponsored group, raising concerns about the security of critical infrastructures and the need to enhance cyberdefences.

In the last weeks of June and July, there has been a significant increase in phishing attacks aimed at healthcare organisations in Europe and North America. Cybercriminals are using fake emails that mimic official communications to deceive employees and steal login credentials. Institutions such as Massachusetts General Hospital and the Mayo Clinic have reported security breaches resulting in the exposure of sensitive medical records. Authorities are working with healthcare providers to strengthen defences against these attacks and raise employee awareness about phishing risks.

Simultaneously, a team of security researchers from Kaspersky discovered multiple critical vulnerabilities in Internet of Things (IoT) devices used in smart homes and industrial environments. The vulnerabilities, found in devices such as security cameras and smart thermostats from brands like Xiaomi and TP-Link, allow attackers to remotely take control of the devices, potentially causing physical damage or stealing data. The affected device manufacturers have released firmware updates to mitigate the risks, and security experts advise users to update their devices immediately and follow best practices for IoT security.

According to the Cybersecurity Centre of Gipuzkoa (ZIUR), Spain has been ranked in the top 4 countries most affected by "hacktivism" since mid-2023. Specifically, the most targeted attacks have been related to DoS (Denial of Service) and information leaks from companies affected by other directed attacks. According to ZIUR, the most impacted sectors have been government and transport.

Among these hacktivist groups, the ransomware group Lockbit3 remains a global threat to the industry, with approximately 31% of attacks being denial of service.

Meanwhile, a team of researchers from Oligo Security has discovered a vulnerability termed "0.0.0.0 Day" that affects Chrome, Safari, and Firefox browsers on MacOS and Linux devices. This security flaw allows adversaries to exploit the IP 0.0.0.0 to access and execute malicious code on local services through the local network. Although the issue was first reported in 2006, no definitive solutions have been implemented until now.

The affected browsers have begun taking steps to mitigate this threat. Apple is implementing changes in the beta version of macOS Sequoia, and Chrome has started blocking direct access to certain private network endpoints from public websites. However, Firefox has not yet released a complete solution, though it is in the process of developing one.

With all this in mind, it is clear that both Black-Hat and White-Hat Hackers have not had a moment's rest during these summer months, metaphorically resembling the famous game of "tug of war," where sometimes attackers and defenders swap roles.

Ángel Pérez Fuentes
Cybersecurity Expert Analyst

Álvaro Vela Robleda
Cybersecurity Expert Analyst

Threat modelling: from theory to practice in risk assessment

Article by Yeiber Basilio Caso Ramirez and Rodrigo Rey Duarte

Threat modelling is a crucial technique in information security that helps identify, understand, and mitigate potential risks in systems and applications. This process has become a standard practice to ensure security in software development and technology infrastructure management. In this article, we will explore the theory behind threat modelling and reflect on the challenges and changes necessary to effectively implement this technique in practice.

Threat modelling theory

Threat modelling is a structured methodology that enables the identification of the most relevant threats to a specific system and the determination of vulnerabilities that could be exploited by attackers. Below are the most common theoretical steps in threat modelling:

1. **Asset Identification:** It involves determining which elements of the system are valuable and need protection. These may include sensitive data, critical services, hardware, and software.

2. **Creation of an Architecture Diagram:** A visual mapping of the system is created, showing components, connections, and data flows. This helps to understand how the parts of the system interact and where vulnerabilities may exist. This step, along with the previous one, forms the foundation of all threat modelling, as it defines the attack surface and the data flows of the entire system to be modelled.

3. **Identification of Threats:** Potential threats to each component of the system are identified.
4. **Risk Assessment:** Each threat is assessed in terms of likelihood and impact, thereby determining its risk level. This helps to prioritise the most critical threats.
5. **Development of Countermeasures:** Solutions and security controls are proposed to mitigate the identified risks, whether through changes to the architecture, implementation of new technologies, or adjustments to security procedures.

Several methodologies exist for threat modelling and identification, each with its own approach and specific characteristics. These methodologies provide a theoretical foundation for threat modelling, allowing for the structuring of information.

Below, we introduce three of the most popular ones:

STRIDE

Developed by Microsoft, STRIDE is one of the most well-known approaches to threat modelling. STRIDE is an acronym representing six types of threats:

- **Spoofing**: making something or someone appear as something they are not.
- **Tampering**: unauthorised modification of data.
- **Repudiation**: denial of previous actions.
- **Information Disclosure**: exposure of information to unauthorised entities.
- **Denial of Service**: disruption of service availability.
- **Elevation of Privilege**: gaining unauthorised access to resources.

STRIDE is useful for identifying specific threats and categorising the types of attacks that might occur.

DREAD

DREAD is another methodology that complements STRIDE. It allows for the assessment of threats in terms of:

- Damage Potential
- Reproducibility
- Exploitability
- Affected Users
- Discoverability

The combination of STRIDE and DREAD provides a comprehensive view of both the types of threats and their impact and likelihood.

PASTA

PASTA (Process for Attack Simulation and Threat Analysis) is a methodology focused on attack simulation and threat analysis. It consists of seven stages:

1. Definition of objectives.
2. Technical description of the system.
3. Identification of critical assets.
4. Threat analysis.
5. Attack modelling.
6. Risk and impact analysis.
7. Mitigation recommendations.

PASTA is suitable for organisations seeking detailed threat analysis and simulation of potential attacks.

These methodologies are very useful for approaching threat modelling; however, another key aspect is the use of tools that support the process and enable continuous improvement. One example of such a tool is:

Microsoft Threat Modeling Tool

The Microsoft Threat Modeling Tool is widely used due to its integration with the STRIDE approach. It allows users to create data flow diagrams, automatically identify threats, and generate detailed reports.

OWASP Threat Dragon

OWASP Threat Dragon is an open-source threat modelling tool. It offers an intuitive interface for creating threat diagrams and allows for team collaboration. It supports various threat modelling approaches and is ideal for agile projects.

Using these tools will help ensure adherence to a proper methodology and apply appropriate reporting approaches, which will undoubtedly be a key aspect in adding specific value to each project.

From Theory to Practice

Although the theoretical process of threat modelling seems clear and structured, implementing it in practice presents various challenges due to differences that may exist across projects, environments, and teams. The following discusses some common difficulties and necessary changes for effective implementation:

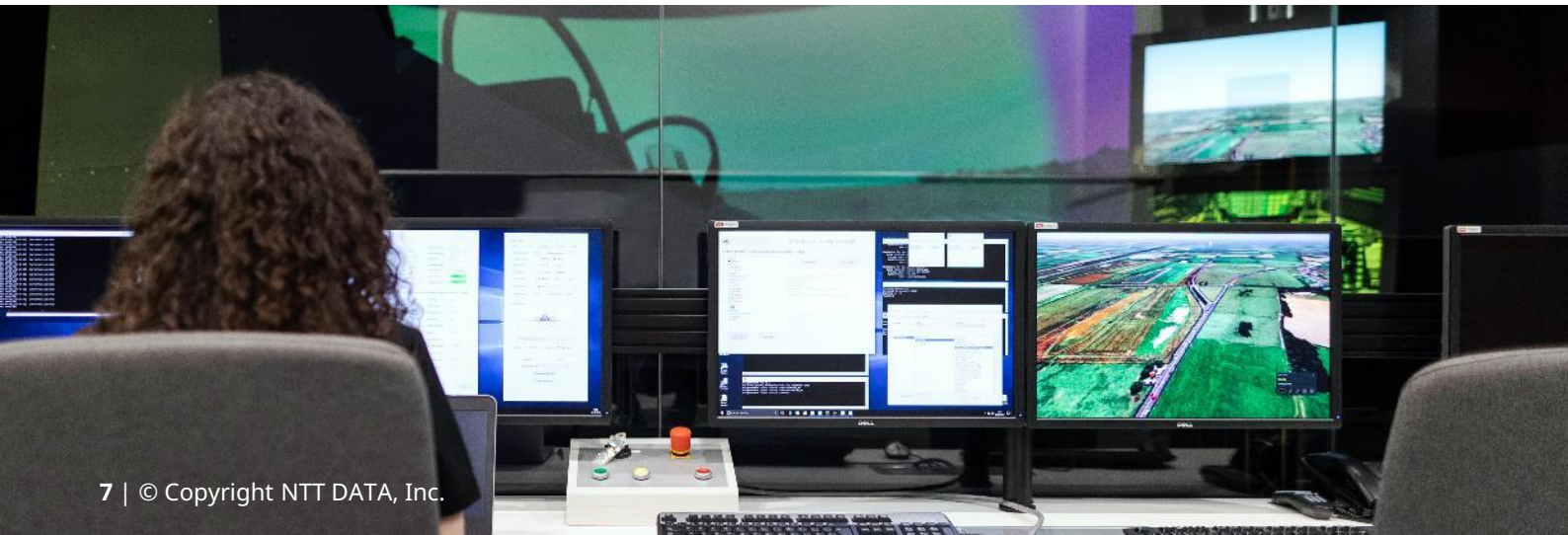
Difficulties in Identifying Assets

Identifying assets appears as a simple step where valuable elements of the system are listed.

In reality, it can be challenging to identify all relevant assets. Large and complex systems may have interdependent components and dispersed data, making comprehensive asset identification difficult. Additionally, the valuation of each asset can be subjective and may vary among different participants in threat modelling.

Complexity in Creating Architecture Diagrams

Architecture diagrams are clear visual tools that facilitate understanding of the system. However, this task is often simplified through the use of specific tools.



In real systems, especially in agile and constantly evolving environments, keeping these diagrams up-to-date can be a challenging task. A lack of documentation or rapid changes in infrastructure can result in outdated or incomplete diagrams, which compromises threat analysis.

Identification of Threats and Risk Assessment

Established models are used to identify threats and assess risks objectively (using methodologies).

In practice, models may not capture all threats specific to a particular environment. Additionally, risk assessment may be biased by personal perceptions or a lack of historical data on incidents. Subjectivity in estimating probability and impact can lead to incorrect prioritisation.

Development and Implementation of Countermeasures

Once risks are identified, appropriate countermeasures are implemented to mitigate them. Implementing countermeasures can face obstacles such as budget constraints, resistance to change from staff, or the need to maintain compatibility with legacy systems.

Theoretical solutions may not be feasible in the real operational environment, requiring adaptations and compromises.

Final Reflection

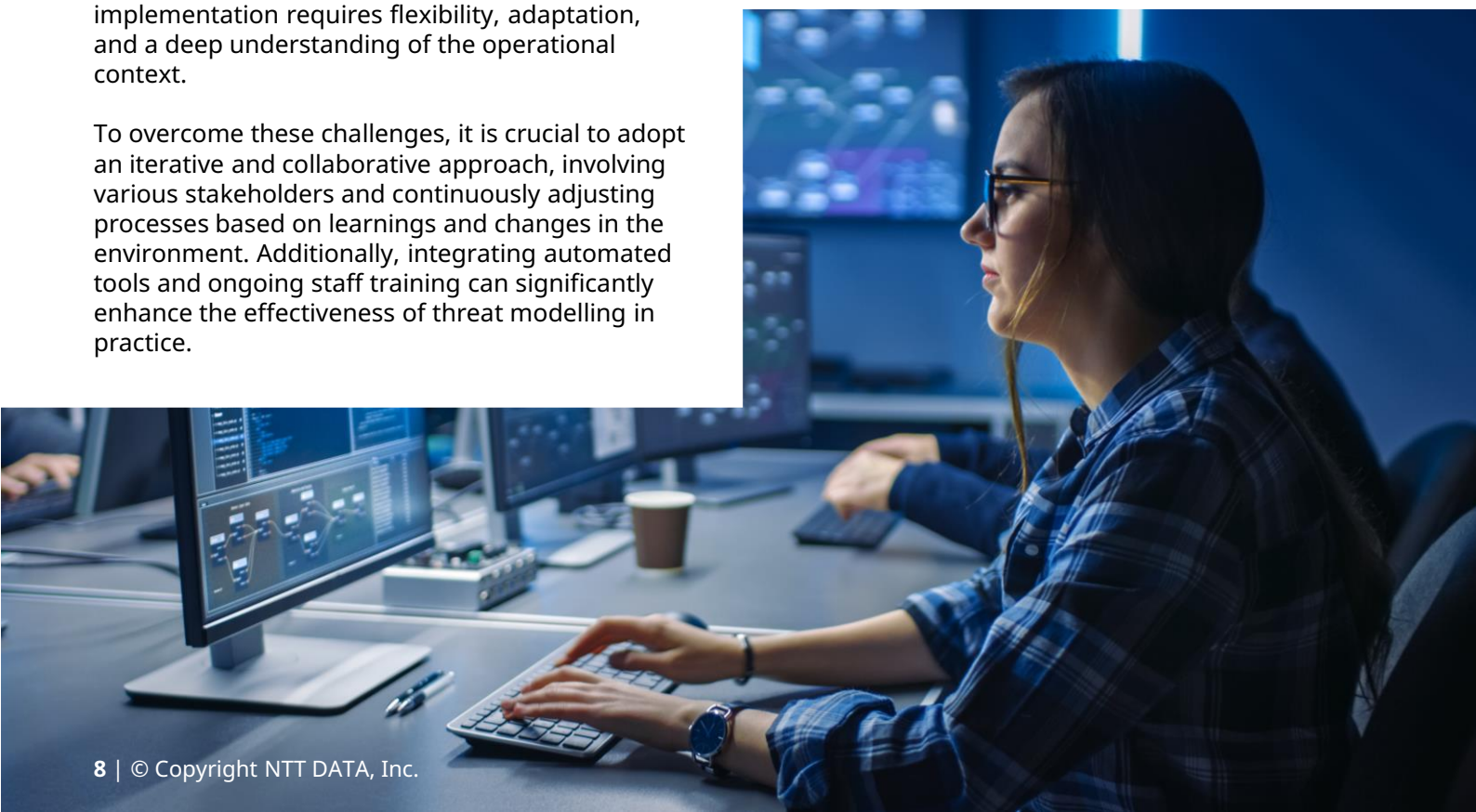
Threat modelling is a powerful tool in security risk management, but its effectiveness depends on how it is put into practice. Theory provides a solid and structured foundation, but practical implementation requires flexibility, adaptation, and a deep understanding of the operational context.

To overcome these challenges, it is crucial to adopt an iterative and collaborative approach, involving various stakeholders and continuously adjusting processes based on learnings and changes in the environment. Additionally, integrating automated tools and ongoing staff training can significantly enhance the effectiveness of threat modelling in practice.

Although threat modelling is rooted in well-defined theoretical principles, its success in practice depends on the ability to adapt to the complexities and realities of the environment in which it is applied. Only by doing so can effective risk management and continuous improvement in the security of systems and applications be ensured.

Yeiber Basilio Caso Ramírez
Cybersecurity Project Manager

Rodrigo Rey Duarte
Cybersecurity Analyst



RegreSSHion (CVE-2024-6387), old foes and new threats

Article by Antonio Pérez Sánchez

In June of this year, a critical security flaw affecting the "SSH" service was published, known as "CVE-2024-6387" and dubbed "regreSSHion." This name reflects its connection to previous security issues, and it is a clear example of how previously resolved security problems can resurface and create new challenges. In this case, the affected systems are those based on Unix that use "OpenSSH," specifically concerning an issue located in "glibc."

This finding was uncovered by security researchers from Qualys, who revealed that the sshd server is vulnerable to a race condition that could allow an unauthenticated adversary to achieve Remote Code Execution (RCE). If successfully exploited, adversaries could gain access to the system with root privileges, enabling them to perform almost any action on the compromised system.

The researchers discovered that if a client fails to authenticate within the maximum time allowed for completing an authentication attempt, defined by the LoginGraceTime parameter (defaulting to 120 seconds), the server's SIGALRM signal handler is invoked asynchronously. This can subsequently utilise functions that are unsafe for asynchronous signals, such as syslog(), potentially allowing arbitrary code execution.

Exploitation requires patience, as in laboratory conditions, according to OpenSSH researchers, it took between six and eight hours to bypass the race condition. Qualys researchers found that their tests were somewhat faster, requiring between three and four hours and approximately 10,000 attempts to exploit the race condition.

However, due to Address Space Layout Randomisation (ASLR), the researchers could only predict the location of glibc half of the time, requiring an additional six to eight hours to obtain a command shell with administrative privileges. In the proof-of-concept released, success depends on precise timing and thousands of attempts, with time and duration being the critical factors.

Below is the function prepare_heap(), which sets up memory in a specific manner to ensure the code's success:

```
prepare_heap (int sock)
{
  // Packet a: Allocate and free tcache chunks
  for (int i = 0; i < 10; i++)
    {
      unsigned char tcache_chunk[64];
      memset (tcache_chunk, 'A', sizeof (tcache_chunk));
      send_packet (sock, 5, tcache_chunk, sizeof (tcache_chunk));
      // These will be freed by the server, populating tcache
    }

  // Packet b: Create 27 pairs of large (~8KB) and small (320B) holes
  for (int i = 0; i < 27; i++)
    {
      // Allocate large chunk (~8KB)
      unsigned char large_hole[8192];
      memset (large_hole, 'B', sizeof (large_hole));
      send_packet (sock, 5, large_hole, sizeof (large_hole));

      // Allocate small chunk (320B)
      unsigned char small_hole[320];
      memset (small_hole, 'C', sizeof (small_hole));
      send_packet (sock, 5, small_hole, sizeof (small_hole));
    }
```

This proof of concept, as previously mentioned, is focused on 32-bit systems (x86), although a 64-bit (amd64) version is currently in development. Below is the function attempt_race_condition(), which attempts to exploit the security flaw by sending data at the precise moment to manipulate the server's memory and gain a command shell with administrative (root) privileges.

```
attempt_race_condition (int sock, double parsing_time, uint64_t glibc_base)
{
  unsigned char final_packet[MAX_PACKET_SIZE];
  create_public_key_packet (final_packet, sizeof (final_packet), glibc_base);

  // Send all but the last byte
  if (send (sock, final_packet, sizeof (final_packet) - 1, 0) < 0)
    {
      perror ("send final packet");
      return 0;
    }

  // Precise timing for last byte
  struct timespec start, current;
  clock_gettime (CLOCK_MONOTONIC, &start);

  while (1)
    {
      clock_gettime (CLOCK_MONOTONIC, &current);
      double elapsed = (current.tv_sec - start.tv_sec)
                     + (current.tv_nsec - start.tv_nsec) / 1e9;
      if (elapsed >= (LOGIN_GRACE_TIME - parsing_time - 0.001))
        { // 1ms before SIGALRM
          if (send (sock, &final_packet[sizeof (final_packet) - 1], 1, 0) < 0)
            {
              perror ("send last byte");
              return 0;
            }
          break;
        }
    }
```

Various well-known surface analysis tools have detected over 14 million potentially affected instances that could, therefore, be exploited. It is estimated that approximately 700,000 of these instances exposed to the internet could become targets for adversarial groups using "regreSSHion“.

This analysis has revealed that the security flaw is a "regression" of the previously patched CVE-2006-5051, reported in 2006. In this context, a regression means that a flaw previously resolved has reappeared in later versions of the software, typically due to changes or updates that reintroduce the problem.

This incident highlights the critical importance of conducting thorough testing before releasing a new version of a product, to prevent the reintroduction of previously resolved security flaws. This problem was reintroduced in October 2020 with OpenSSH 8.5p1.

Known threat groups have exploited vulnerabilities similar to CVE-2006-5051 in the past. For example, cyber-espionage groups such as APT28 (Fancy Bear) and APT29 (Cozy Bear) have used similar security flaws to compromise critical systems worldwide. This demonstrates their ability to exploit vulnerabilities in critical infrastructure, using initial access to deploy espionage and persistence tools, which underscores the importance of addressing regressions in software security.

Damien Miller, the founder of the OpenSSH project in 1999, has pointed out that any system running glibc may potentially be susceptible to this security flaw. To date, it has been shown that 32-bit systems are affected, although it is likely that 64-bit systems could also be vulnerable.

All versions of OpenSSH prior to 4.4p1 are affected, unless patches for both CVE-2006-5051 and CVE-2008-4109 have been applied. Versions from 8.5p1 to, but not including, 9.8p1 are also affected. However, versions from 4.4p1 to, but not including, 8.5p1 are not affected, as CVE-2006-5051 was patched as standard.

In addition to applying the necessary patches, it is advisable for organisations to limit access to the SSH service, avoiding exposure to the internet and implementing network-based controls, as well as proper network segmentation within the organisation. Furthermore, monitoring systems should be implemented to alert administrators about attempted exploits.

Despite the discovered security flaw and its criticality, researchers have praised the OpenSSH project, commenting that the discovery is "a slip in an otherwise nearly flawless implementation." They highlight that the defence-in-depth design and its code are exemplary models and express gratitude to the OpenSSH developers for their outstanding daily work.

In conclusion, the security flaw CVE-2024-6387 underscores the importance of conducting security analyses on software, especially on critical components like OpenSSH. The resurgence of previously patched security flaws, such as CVE-2006-5051, emphasises the need for secure development practices and cycles. Organisations must be proactive in implementing patches and mitigation measures, as well as in monitoring their systems to detect and respond to potential threats.

Additionally, collaboration between various cybersecurity entities and developers is crucial, enabling improvements in software security and protecting critical systems from sophisticated techniques. This case also serves as a reminder that even in well-known projects with ongoing maintenance like OpenSSH, errors can still emerge; therefore, security must remain a priority.

Antonio Pérez Sánchez
Cybersecurity Expert Analyst

Advanced phishing scams: lessons from the CrowdStrike incident

Trends by Alexis Martín García and Carlos Barrios Bastidas

Phishing disguised as a "service" is one of the new trends that security teams must contend with, as malicious actors employ advanced social engineering tactics to compromise organisational networks.

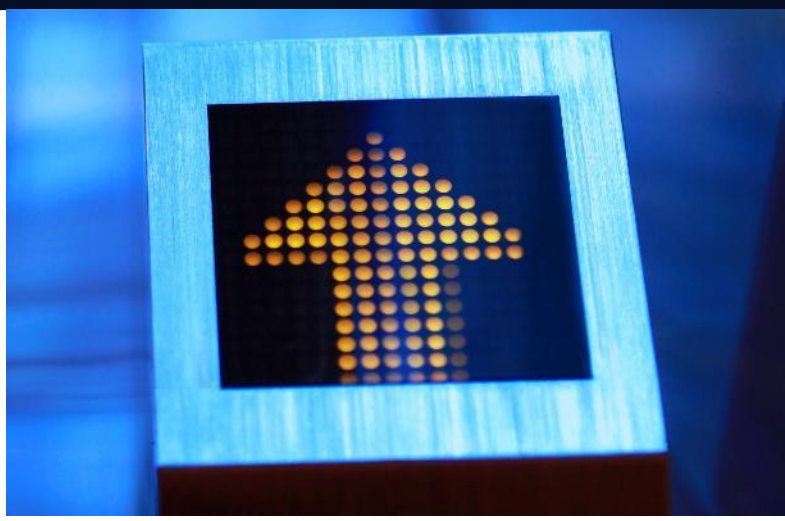
The number of spear-phishing attacks continues to rise, and the tactics employed by cybercriminals are evolving to become increasingly precise and capable of evading even the most advanced defences. Nevertheless, there is a worrying lack of awareness regarding the threat that spear-phishing poses to organisations. Many people still associate this danger with the typical fraudulent emails that traditional security barriers, such as spam filters or anti-malware sandboxes, usually detect.

However, the reality is quite different. A recent study by Barracuda, which examined more than 2.3 million phishing attacks targeting 80,000 global organisations over three months in 2023, reveals that spear-phishing attacks are increasing both in volume and complexity, as well as in their impact on businesses. Notably, there is a growth in the use of more sophisticated and targeted tactics, such as brand impersonation, conversation hijacking, and Business Email Compromise (BEC).

The increasing sophistication of these techniques is testing even the most prepared companies. The recent incident on 19th July 2024 involving CrowdStrike, one of the leading cybersecurity firms, underscores the growing threat that these tactics represent.

A routine software update from CrowdStrike caused a critical disruption in various infrastructures and organisations worldwide. The update triggered the infamous Blue Screen of Death (BSOD), rendering numerous systems inoperative. Although it was not initially classified as a cybersecurity incident, the situation highlights the fragility of digital security and the potential for such disruptions to become serious security threats.

The problems following this incident began to emerge shortly after users installed the latest CrowdStrike update. System crashes were widespread, causing significant operational disruptions at airports, banks, train stations, and other critical infrastructures.



The disruption caused by CrowdStrike has opened the door for threat actors. Cybercriminals have been quick to exploit the situation with social engineering attacks by creating fraudulent domains and phishing pages, posing as solutions to the BSOD problem.

For instance, the domain crowdstrike-office365[.]com hosted malicious compressed files containing a Microsoft Installer (MSI) loader that ultimately executed an information stealer known as Lumma.

Similarly, multiple domains redirected users to payment pages that requested cryptocurrencies like Bitcoin and Ethereum under the guise of offering a solution. Additionally, several pages claimed to offer support services to companies affected by the problem, with multiple researchers recommending caution, as these claims are potentially deceptive and could pose additional security risks.

The web infrastructure and security company Akamai reported that it discovered no fewer than 180 newly created typosquatting domains, falsely claiming to help resolve the incident by offering technical support, quick fixes, or legal assistance, in an attempt to introduce malware or steal sensitive information.

A key concern is the increased likelihood of phishing attacks designed to obtain credentials from CrowdStrike users. Malicious actors, such as the threat group Scattered Spider, could exploit phishing tactics to acquire CrowdStrike Falcon credentials. These attackers might employ sophisticated techniques, including email and SMS phishing campaigns, to deceive users into providing their login details. A common method used by these groups involves deploying an Adversary-in-the-Middle (AitM) proxy kit to intercept and steal credentials in real-time.

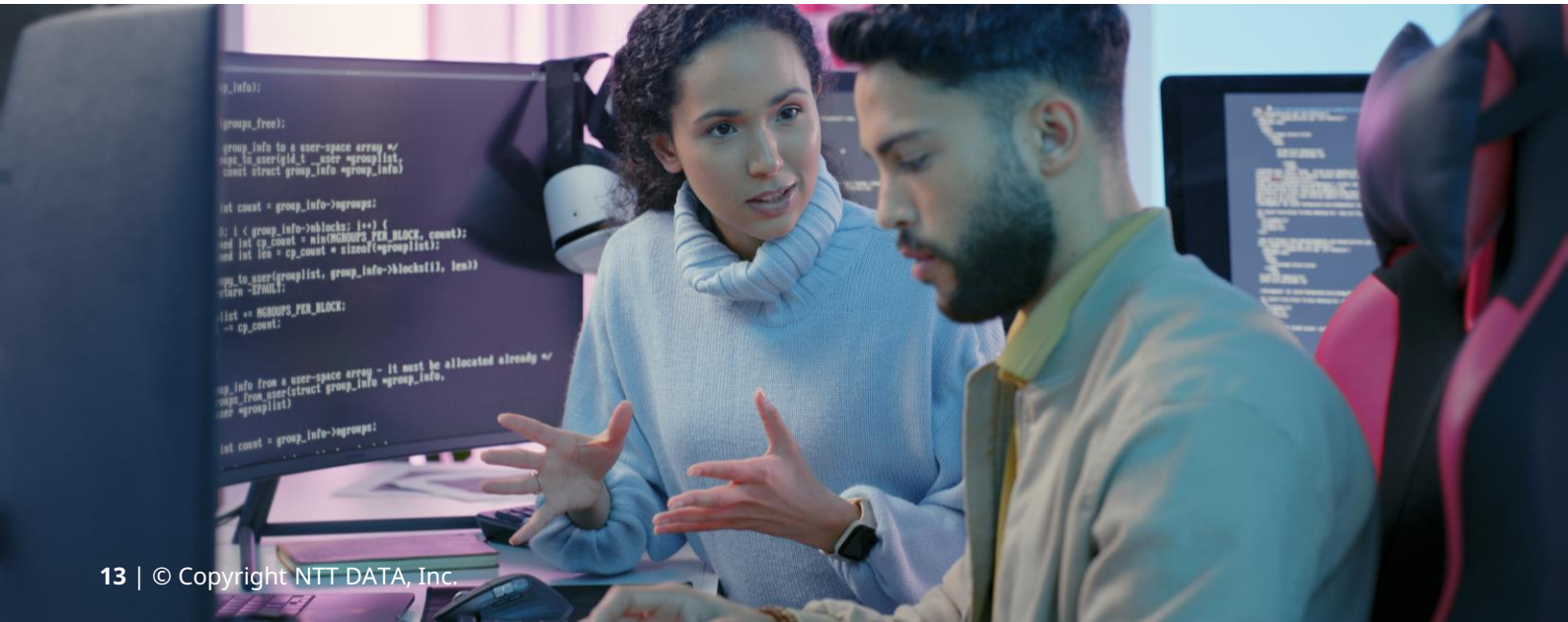
Once attackers gain access to CrowdStrike Falcon credentials, they could exploit the Real Time Response (RTR) module (if enabled). This module allows the execution of custom scripts and commands on endpoints. If custom scripts are enabled within RTR policies, threat actors could remotely execute code on the victim's host and leverage PowerShell. This could escalate into a situation potentially leading to a complete system takeover.

This incident underscores the critical importance of carefully managing software updates and maintaining constant cybersecurity vigilance. It is essential to confirm that any communication comes from official sources, and to use reliable services to verify the safety of websites and URLs, especially those promising assistance or solutions related to recent issues.

Finally, it is crucial to train employees on the risks of phishing and the importance of verifying the authenticity of information or access requests, thereby strengthening the organisation's first line of defence.

Alexis Martín García
Cybersecurity Project Manager

Carlos Barrios Bastidas
Cybersecurity Lead Analyst



The rise of attacks in cloud environments

Trends by Nicolás Fernández Martínez

Digital transformation has led many companies to move their operations and data to the cloud in pursuit of greater flexibility and efficiency. This trend has caught the attention of cybercriminals, who see the cloud as a desirable target, resulting in a significant increase in attacks directed at these environments, creating unusual challenges for cybersecurity experts.

Digital transformation has led many companies to move their operations and data to the cloud in pursuit of greater flexibility and efficiency. This trend has caught the attention of cybercriminals, who see the cloud as a desirable target, resulting in a significant increase in attacks on these environments, posing unusual challenges for cybersecurity experts.

Current trend

Attacks on cloud environments increased by 48% in 2022, according to a report by Continuity Central. Although the rise was somewhat more moderate in 2023, at 35%, according to Darktrace, this trend remains highly alarming. While this increase may be due to the fact that cloud environments represent a larger attack surface (as more and more companies operate in cloud environments), it could also be explained by the often inadequate security measures within these ecosystems. As a result, any error, such as incorrect permission settings or exposed cloud assets, allows attackers to access and extract sensitive information with relative ease.

Alternative initial access techniques

Cybercriminals have been using alternative methods to achieve initial infiltration, beyond exploiting environments suffering from misconfigurations. One of the most common forms of credential theft remains phishing. Once credentials are obtained, attackers can move laterally within the cloud environment, allowing them to increase their access and, consequently, the potential damage. Another widely used practice is the use of compromised credentials purchased from dark web marketplaces, which greatly simplifies the attackers' work and avoids early detection.

Common attack techniques in cloud environments

- **Misconfiguration**: attackers exploit misconfigurations in cloud environments to gain unauthorised access, such as excessive permissions and publicly accessible storage of sensitive data.
- **Denial of service (DoS)**: these attacks aim to prevent legitimate users from accessing cloud services. Attackers generate a large volume of traffic to destabilise critical services, cause significant disruptions, and overwhelm server resources.
- **Data interception**: attackers intercept and manipulate communication between two parties using techniques like "Man-in-the-Middle" (MitM), compromising the integrity and confidentiality of information.
- **Virtual infrastructure**: these attacks target the foundational cloud infrastructure, including virtualisation and hypervisors, impacting all virtual machines hosted on the same physical server.
- **Code injection**: attackers can inject malicious code into cloud applications to take control of the system and execute arbitrary commands.
- **Privilege escalation**: attackers seek to elevate their privileges within the cloud system by exploiting misconfigurations or software vulnerabilities, allowing them to control essential cloud resources.

Conclusions for Cybersecurity

It is crucial to conduct thorough and frequent security audits and assessments in cloud environments. Furthermore, each organisation should implement a set of best practices, such as reviewing and improving security configurations, managing identities and access (IAM), providing employee training and awareness, continuous monitoring, and rapid incident response.

Ultimately, the key is to adapt and evolve alongside the threats, using lessons learned from previous incidents to strengthen cybersecurity strategies and build a safer and more resilient future.

Nicolás Fernández Martínez
Cybersecurity Analyst

Vulnerabilities

Critical vulnerability in the AuthZ plugin in Docker Engine

Date: July 23, 2024
CVE: CVE-2024-41110

CVSS: 9.9

CRITICAL

Description

The critical vulnerability identified has been observed in Moby, an open-source project created by Docker and used for software containerisation.

The vulnerability has been detected in certain versions of Docker Engine. The identified flaw could allow an attacker to bypass the authorisation plugins (AuthZ) associated with Docker Engine. Under specific circumstances, by using a particular API request, a Docker Engine API client could cause a request or response from an authorisation plugin to be forwarded, leading to unauthorised actions, including privilege escalation.

Solution

The manufacturer recommends the following solutions to address the vulnerability:

- Update Docker Engine to apply the patches implemented by the manufacturer.
- Avoid using authorisation plugins (AuthZ) and restrict access to Docker APIs until updated to the latest version.
- Update to the most recent version of Docker Desktop:

Affected products

The vulnerability affects the following versions:

- Docker Engine v19.03.x and later versions that use authorisation plugins.
- Docker Desktop v4.32.0 versions and above.

References

- docker.com
- nvd.nist.gov

TLP:WHITE

Vulnerabilities

Critical vulnerability in Spring Cloud Data Flow

Date: July 25, 2024
CVE: CVE-2024-37084

CVSS: 9.8

CRITICAL

Description

A critical vulnerability (CVE-2024-37084) has been discovered in the Spring Cloud Data Flow platform.

The detected vulnerability is related to the lack of sanitisation in the file upload path of Spring Cloud Data Flow, which is a platform for streaming and batch data processing. An adversary with access to the Skipper server API could potentially use a manipulated upload request to write an arbitrary file to any location on the file system, which could compromise the server. The Skipper server API is not exposed to external users, and the likelihood of exploitation of this vulnerability is low.

Solution

Affected users are advised to update to version 2.11.4 of Spring Cloud Skipper, as it contains the necessary patch to address the identified critical vulnerability.

- Spring Cloud Skipper: Update to version 2.11.4.

Affected products

The vulnerability affects the following product versions:

- Spring Cloud Skipper: Versions 2.11.0 to 2.11.3.

References

- spring.io
- nvd.nist.gov

TLP:WHITE

Multiple security updates for Apple products

Date: July 29, 2024
CVE: CVE-2024-23296 and 280 more

Critical

Description

Apple has released a series of security updates for the operating systems of its major products, including iOS, iPadOS, and macOS.

Among the vulnerabilities addressed is a zero-day vulnerability, CVE-2024-23296, which affects the macOS Monterey operating system. Exploitation of this vulnerability could allow an attacker with read and write permissions to bypass kernel memory protections.

Additionally, other vulnerabilities have been fixed, which could potentially lead to unexpected system shutdowns, process crashes, or cross-site scripting (XSS) attacks, among other issues.

Affected products

Security updates include patches for the following Apple products:

- iOS 17.6 and 16.7.9;
- iPadOS 17.6 and 16.7.9;
- macOS Monterey 12.7.6, Sonoma 14.6, and Ventura 13.6.8;
- Safari 17.6;
- tvOS 17.6;
- visionOS 1.3;
- watchOS 10.6.

Solution

It is recommended to apply the updates published by the manufacturer.

References

- incibe.es
- cisa.gov
- support.apple.com

Android August security patch

Date: August 5, 2024
CVE: CVE-2024-23350 and 47 more

Critical

Description

The August Android security bulletin addresses a total of 48 vulnerabilities, including one of critical severity. Exploitation of these vulnerabilities could lead to privilege escalation, remote code execution, or the disclosure of sensitive information.

The critical vulnerability, identified as CVE-2024-23350, could result in a permanent denial-of-service attack due to an integrity check failure in DL NAS transport.

Additionally, the bulletin fixes a vulnerability in the Linux kernel identified as CVE-2024-36971, which had been actively exploited.

Affected products

The products affected by the update are as follows:

- Android Open Source Project (AOSP): versions 12, 12L, 13, and 14.
- Arm, MediaTek, Imagination Technologies, and Qualcomm components.

Solution

It is recommended to apply the security patches published by the manufacturer.

References

- bleepingcomputer.com
- source.android.com

Events

Cyber Security Summit 2024
September 6

The Security Summit 2024 brings together industry leaders and cybersecurity experts to discuss emerging threats and best practices for defending against them. The event will feature keynote speeches, workshops, and interactive sessions on topics such as cyber intelligence, incident response, and advanced defence technologies.

Link

Leveraging AI in Cybersecurity
September 8-9

This event focuses on the intersection between cybersecurity and artificial intelligence. Experts from both fields will come together to discuss how AI can enhance cybersecurity strategies and how to protect AI systems from cyber threats. It will include presentations, live demonstrations, and panel discussions.

Link

Cybersecurity for Critical Industries
September 10-11

This event focuses on the current cybersecurity challenges facing critical industries and how they can be mitigated through the development of resilient and responsive systems. Attendees will gain exclusive insights into new techniques and technologies and will have the opportunity to interact with cybersecurity experts from the United Kingdom.

Link

RSTCON 2024 (Reset)
September 13-15

RSTCON is a technical security conference that focuses on advanced research, exploitation, and tactics targeting the sensors, systems, and architectures used by critical industries.

Link

Eventos

Cybersecurity in Financial Services Summit
September 16

This annual event will address the cyber risks threatening London's financial services community. Discussions will cover government strategies, priorities of the National Cyber Security Centre, and the Bank of England's stance on cybersecurity resilience in the financial sector.

Link

Cybersecurity Defense Ecosystem Summit
September 19

This event will focus on building a robust cybersecurity defence ecosystem. It will feature cybersecurity experts who will discuss best practices and technologies for protecting critical infrastructure and sensitive information.

Link

Security & Risk Management Summit
September 24

This Gartner event will bring together experts and leaders in cybersecurity to explore the evolution of digital risks and strategies for resilience. Topics will include generative artificial intelligence, risk management and compliance, cloud security, and more.

Link

International Cyber Expo 2024
September 24-25

The International Cyber Expo is a global event focused on cybersecurity, data protection, and cyber resilience. Attendees will have the opportunity to explore the latest innovations and solutions in cybersecurity, as well as participate in discussions on security policies and risk management.

Link

SecureWorld 2024
September 26

SecureWorld is a series of cybersecurity conferences held in various cities. The event in Boston will offer two days of intensive learning and networking, featuring panel discussions, training sessions, and an exhibition showcasing the latest products and services in cybersecurity.

Link

Resources

Govolution/avet: Antivirus Evasion Tool

AVET is an innovative public tool developed by Govolution designed to assist security auditors and promote experimentation with advanced antivirus evasion techniques. It can combine various evasion strategies and generate payloads that bypass traditional defenses. Its focus on enhancing both effectiveness and efficiency in penetration testing of technological assets makes it an essential tool for those looking to stay ahead in the dynamic field of cybersecurity.

Link

Styx Crypter

Styx Crypter is an encryption tool used to conceal malicious software and evade antivirus detection. By encrypting the malicious code, it transforms a threat that is easily detectable into one that is nearly impossible for most antivirus engines to decipher. This tool not only encrypts the code but also employs advanced obfuscation techniques, making it highly effective for any attacker seeking to avoid detection.

Link

matro7sh/BypassAV

The matro7sh repository, BypassAV, offers a collection of techniques and tools dedicated to evading antivirus and EDR (Endpoint Detection and Response) systems. This resource is particularly valuable due to its focus on tools that are less likely to be detected. With a wide range of documented techniques and available tools, BypassAV enables users to explore innovative methods for bypassing advanced security solutions.

Link

EDRSandBlast

EDRSandBlast is a tool developed in C that exploits a vulnerable signed driver to evade EDR (Endpoint Detection and Response) detections. It is notable for its ability to manipulate notification routines and object callbacks, rendering traditional EDR detections ineffective. EDRSandBlast not only highlights the inherent vulnerabilities in some signed drivers but also provides a solid foundation for developing more advanced evasion techniques.

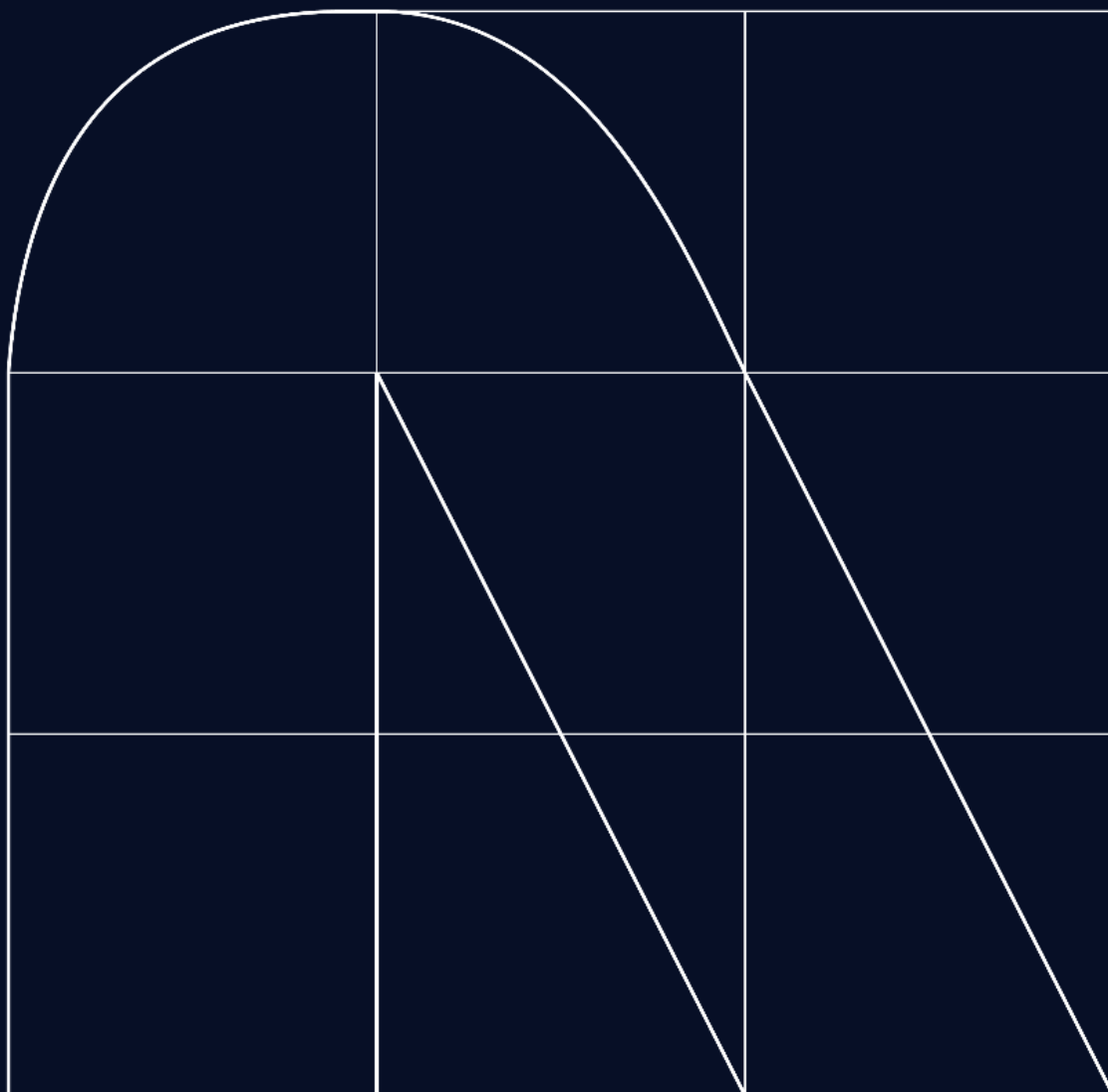
Link

Xencrypt

Xencrypt is a clever tool that uses PowerShell to evade antivirus detection by compressing and encrypting scripts, as well as randomising variable names to enhance evasion. This PowerShell script not only makes it harder to detect the code but also introduces an additional level of complexity that challenges the detection capabilities of antivirus engines. Xencrypt exemplifies the power of obfuscation and encryption in avoiding antivirus detection.

Link

Subscribe to RADAR



Powered by the cybersecurity NTT DATA team

es.nttdata.com