infinitum IT
Power of integrated Security

Zero Day MoTW Bypass Attack

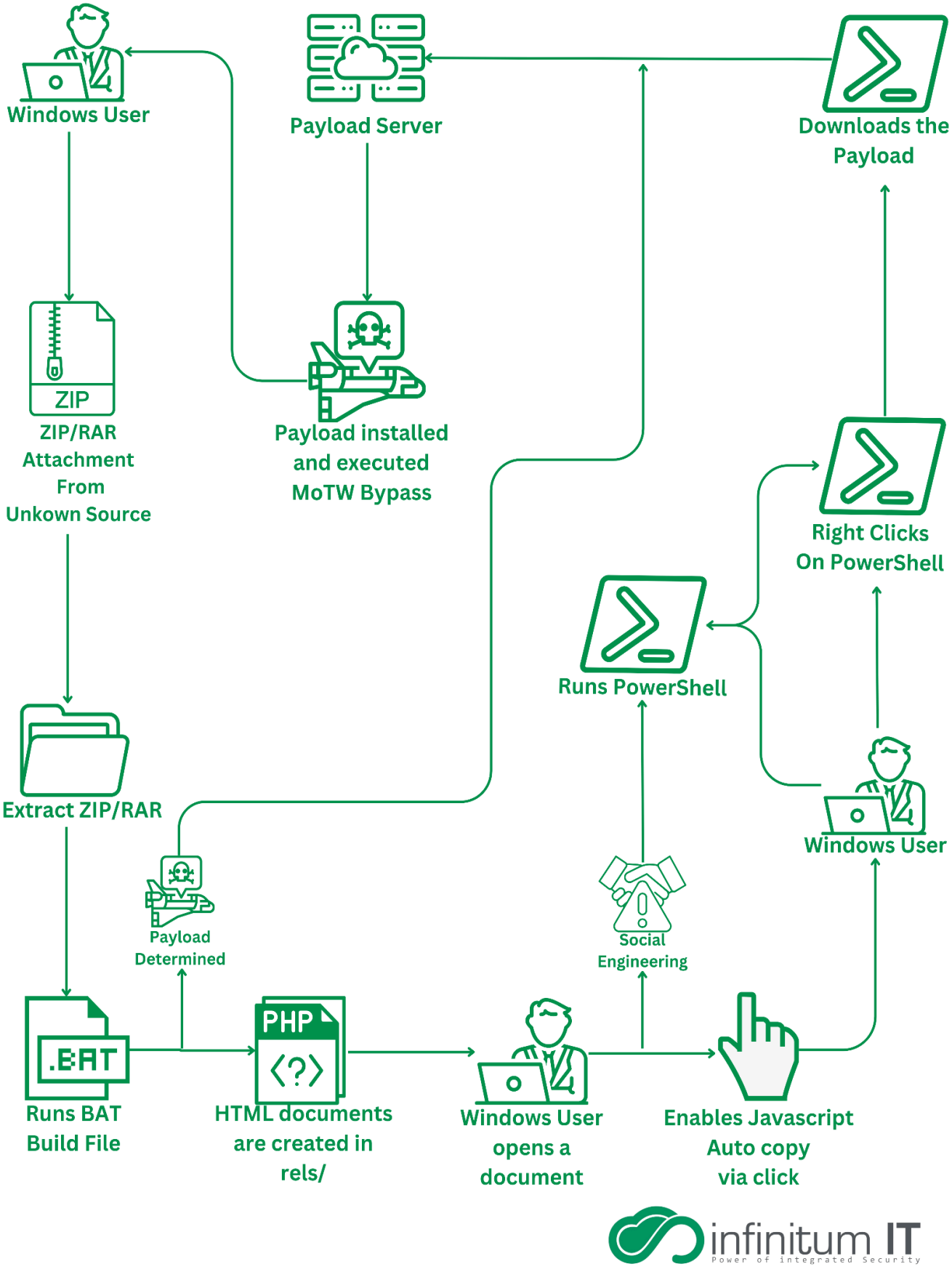
CTI Report

infinitumitlabs

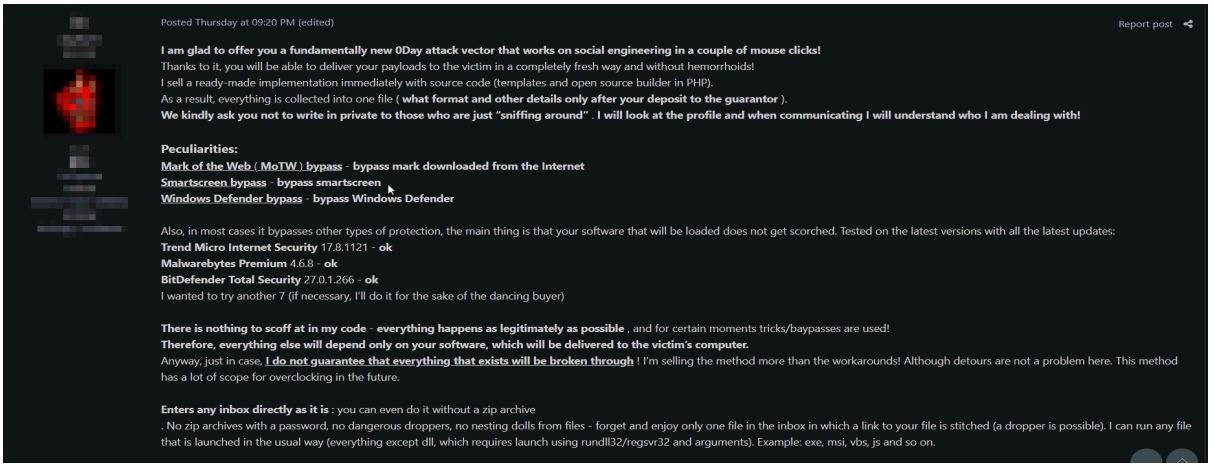
www.infinitumit.com.tr

Contents

Attack Chain



About the New Zero Day Attack



"A zero-day attack" is a situation when a security vulnerability in a software or in a system has been discovered, but the developer has not yet released a fix or update. During this period, malicious individuals or groups may exploit the vulnerability to gain unauthorized access to systems or engage in harmful activities. A new zero-day attack was first identified on the dark web. The individual who discovered the vulnerability is selling it for a specific price on the dark web. The security vulnerability occurs through social engineering. According to the hacker's disclosure, the targeted user is directed through a few clicks via social engineering to execute the payload owned by the hacker within the system.

Features of the New Zero Day Attack

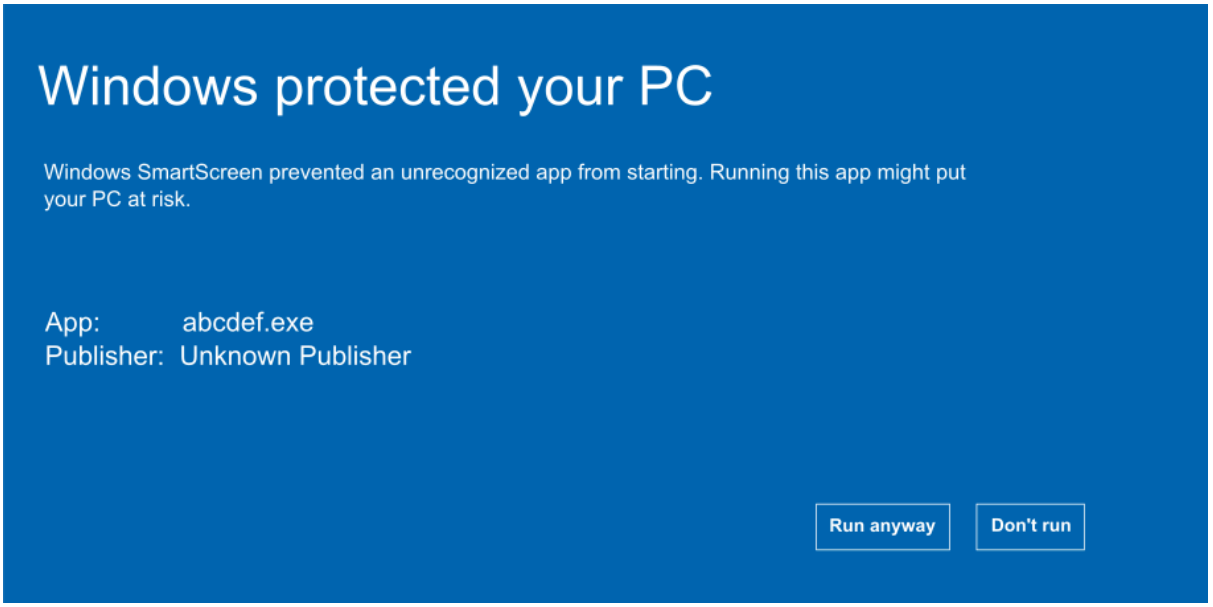
Among the features of the newly emerged zero-day attack are the capability to bypass security elements such as MoTW (Mark of The Web), Smartscreen, Windows Defender, Trend Micro Internet Security, MalwareBytes Premium, Bitdefender Total Security.

MoTW, short for Mark of The Web, is actually a security feature used in Windows operating systems. It checks the reliability of downloaded files and applications, and if they don't come from a trustworthy source, it warns the user and prevents the download. For the user to proceed with the download, additional permissions need to be granted through browser settings. However, this poses a challenge for malicious users because many users may choose not to run the downloaded file due to this warning. Bypassing this feature makes it much easier for attackers to introduce viruses into the targeted system

The Importance of MoTW Bypass

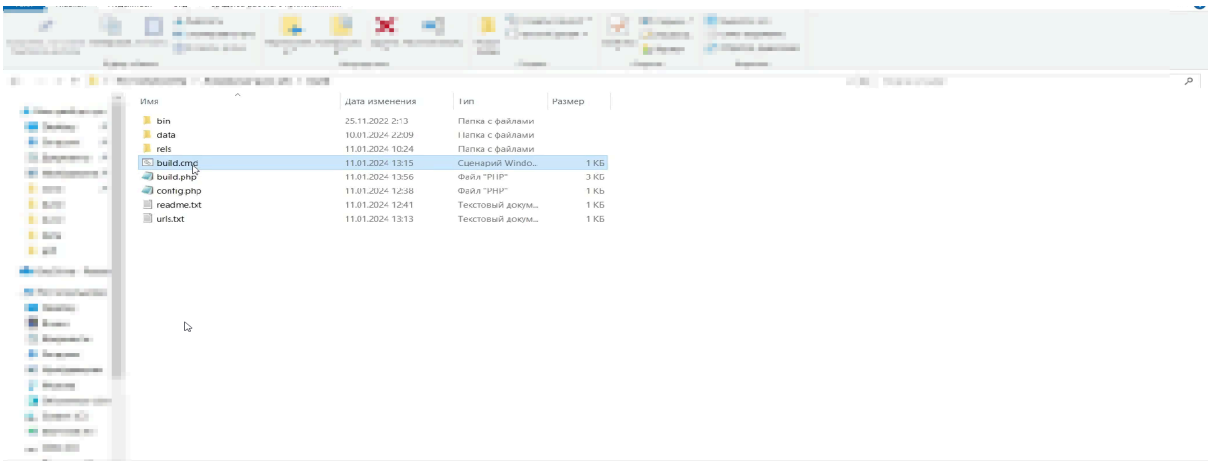
MoTW is used to indicate that a file comes from the internet. This allows additional inspection on Smartscreen on Windows systems.

By successfully bypassing the Mark of the Web (MoTW) feature, which is designed to indicate the origin of files from the internet, attackers can exploit a vulnerability in Windows systems. This circumvention enables them to clandestinely download and execute potentially malicious files without triggering the additional scrutiny and warnings provided by Smartscreen. The absence of MoTW safeguards poses a significant risk, as users may inadvertently engage with harmful content, mistakenly assuming the files are safe. This evasion tactic not only undermines the protective mechanisms in place but also highlights the importance of robust security measures to prevent unauthorized access and potential exploitation of user trust in online file downloads.

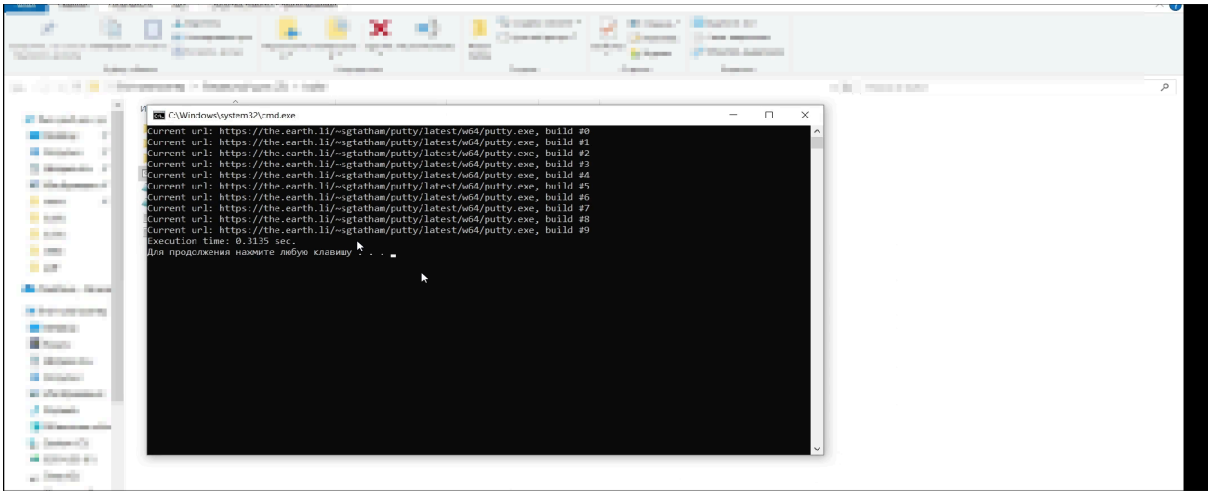


In systems where the Mark of the Web (MoTW) feature is active, users are notified after opening files from external sources, triggering Smartscreen to intervene. However, in cases where this feature is bypassed, additional warnings screen does not appear before the user

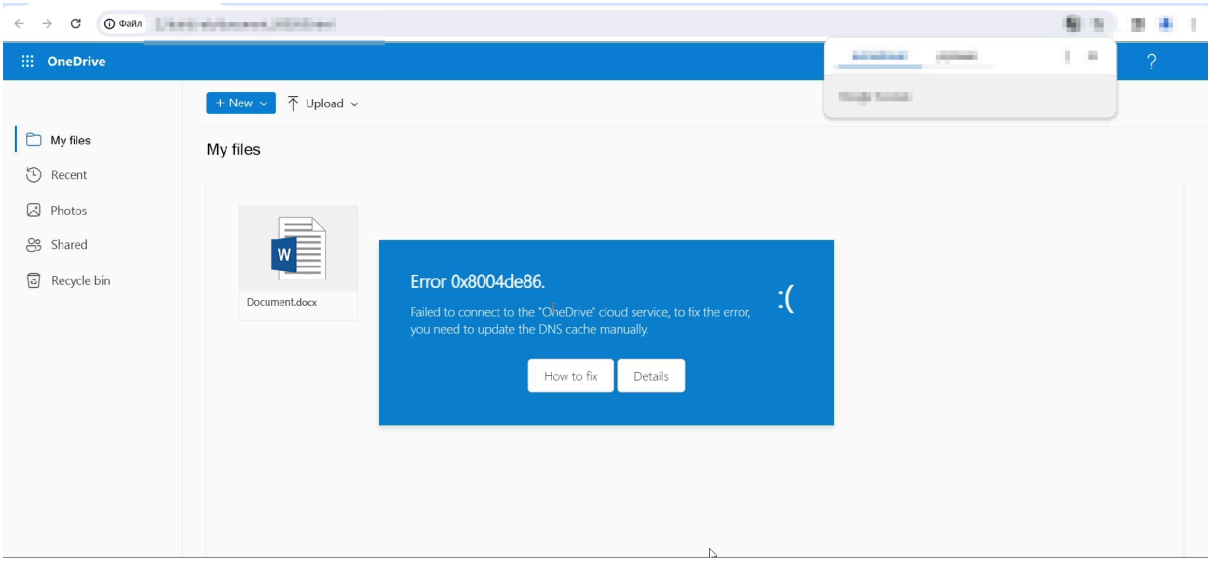
A Glimpse into the New Zero-Day Attack



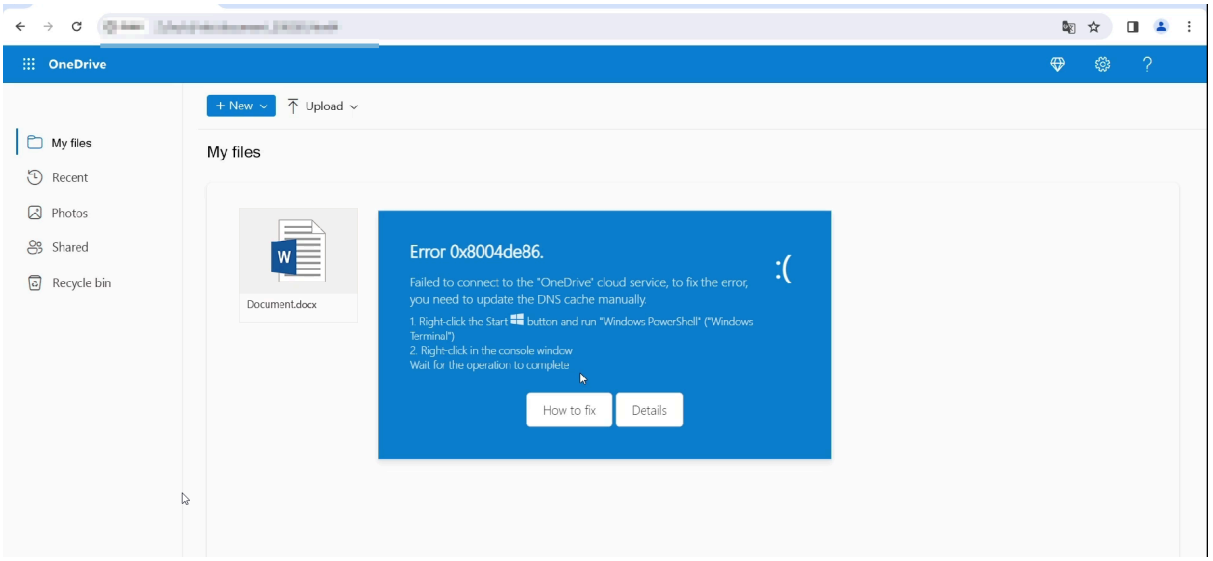
There are several different scenarios in which this attack can occur. One involves hosting a website and installing the necessary tools on the server (From the attacker's side). In this type of attack, the user triggers the payload by clicking on a website using social engineering tactics. Another scenario is a Man-in-the-Middle attack. In this attack, a DNS spoofing attack is carried out, redirecting the user to the attacker-hosted website, where the payload is executed using social engineering tactics. The third and final scenario involves sending files to the user in the form of software, specifically as ZIP/RAR archives. In this context, the user is asked to run a build file.



Once the Build file is started, HTML files are created in the Rels/ directory. These files contain PHP and JS code. Subsequently, the user is expected to open one of these HTML files. Putty is used here for illustrative purposes, but malicious payloads can also be injected based on malicious activities.

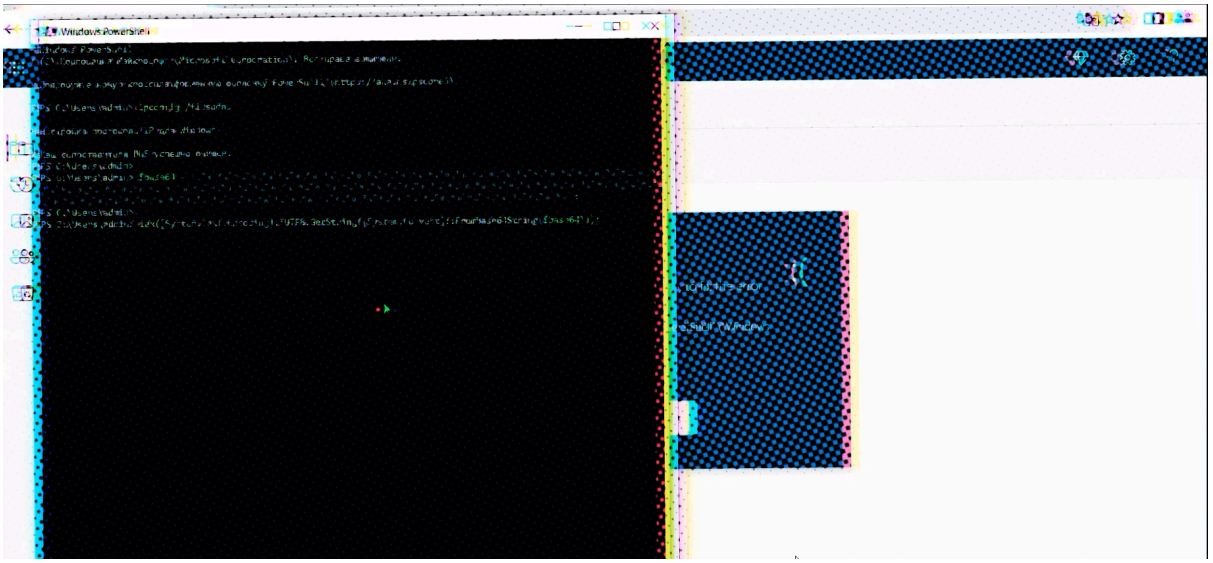


After the user opens one of the HTML files or connects to the attacker's website, the user encounters with an error. Social engineering comes into play here, and the attacker presents a seemingly legitimate error on Onedrive.

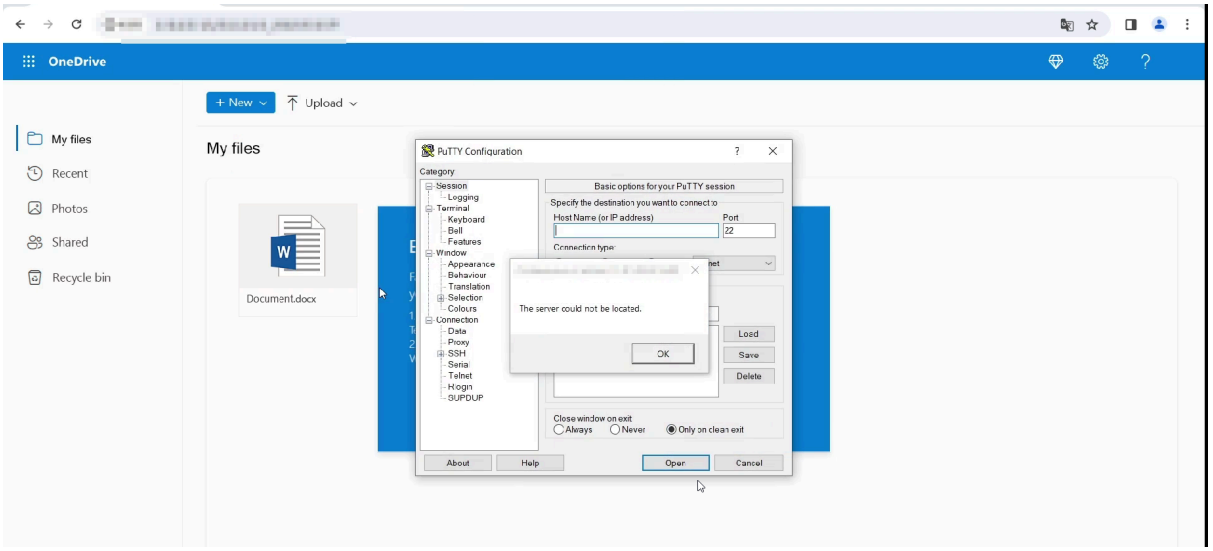


After clicking the 'How to Fix' button , the user is directed to open PowerShell. When this button is clicked, malicious commands that the user needs to execute on the JavaScript side are automatically copied.

When the targeted Windows user clicks the button, it copies the commands intended for execution in PowerShell via JavaScript. Due to PHP not directly issuing a command like ***'echo shell_exec('powershell <command>');'***, security measures on the system do not identify this activity as malicious.



After the user launches PowerShell, they are prompted to manually paste the commands automatically copied on the JavaScript side through social engineering. In reality, the attacker doesn't directly instruct to paste all commands; the website simply asks to right-click on the opened PowerShell prompt. However, all commands are processed in memory during this action. Following this process, the payload is downloaded and executed, bypassing MoTW, Smartscreen, and Microsoft Defender.



Finally, all the necessary commands are executed, and the targeted file/payload is run by bypassing security elements such as MoTW, SmartScreen, Windows Defender.

Here, Putty was preferred, so Putty was executed, but if a malicious payload had been chosen, that payload would have been executed.

Difference from Other MoTW Vulnerabilities

There are security vulnerabilities associated with MoTW bypass, identified as CVE-2022-41091 and CVE-2019-1054.

CVE-2022-41091 is a Windows Mark of the Web Security Feature Bypass Vulnerability, operating by altering the ZoneID during the ZoneTransfer process.

CVE-2019-1054 is a Windows Mark of the Web Security Feature Bypass Vulnerability, exploiting this through vulnerabilities present in older versions of Microsoft Edge.

This security weakness mostly comes from users. What makes this attack different is the use of social engineering. It's not the kind of attack that happens if the user doesn't click on things via social engineering. Unlike other attacks, this one uses BATCH, PHP, and JAVASCRIPT codes and tricks the user into clicking on things.

Summary of The New Zero-Day Attack

- The vulnerability exists in Windows systems
- The goal is to bypass MoTW, Smartscreen, and Microsoft Defender security measures in order to execute a malicious payload.
- In this type of attack, social engineering and phishing tactics are commonly employed. The attacker hosts a website or sends the user an archive in ZIP/RAR format. Ultimately, the targeted user is redirected to a website. This website displays real errors to the user, and to resolve this error, it contains a 'How to Fix' button on the site. After the targeted Windows user clicks on this button, they are instructed to launch a PowerShell prompt and right-click on the prompt. While the attacker may not explicitly mention pasting commands, when the Windows user right-clicks on the opened PowerShell prompt, all commands are processed in memory. With this action, the payload is being installed and executed. Throughout this attack, the attacker avoids detection by security elements such as MoTW, SmartScreen, and Microsoft Defender.

How Could an Attacker Perform the New Zero-Day

- In a man in the middle attack scenario, the attacker could use arp + dns spoofing for directing the user to the attacker's website to exploit the security feature bypass.
- In a phishing scenario, the attacker could send the local attachments as ZIP/RAR compressed via email in order to exploit the security feature bypass.
- In another phishing scenario, the attacker could host a malicious website. In this type of attack a ZIP/RAR archive is not being sent. The attacker only makes the user connect to the hosted website and uses social engineering tactics via the website in order to exploit the security feature bypass.

Mitigations

- Regularly update and patch all software, including operating systems, applications, and third-party software.
- Use application whitelisting to allow only approved and necessary applications to run on systems.
- Educate users about security best practices, including not clicking on suspicious links, avoiding downloads from untrusted sources, and being cautious with email attachments.
- Stay informed about the latest threats and vulnerabilities by leveraging threat intelligence feeds.
- Employ EDR solutions to monitor and respond to advanced threats and suspicious activities on endpoints.
- Employ FIM solutions to monitor critical system files for unauthorized changes, helping to detect potential compromise
- Implement a SIEM solution to collect and analyze logs from various sources, aiding in the detection of anomalous activities.
- Implement application control solutions to allow only trusted applications to run on endpoints, preventing the execution of unauthorized or unknown binaries.
- Provide regular security awareness training to educate users about potential threats, social engineering tactics, and safe online practices.
- Enforce the principle of least privilege by restricting user permissions to only what is necessary for their job functions, limiting the impact of potential compromises.

All the **services** you need to keep your **business** secure

Secure your business effectively against cyber threats and attacks

In **InfinitumIT** we provide

Risk and Threat Analysis
Penetration Testing
Managed Security
Digital Forensics
Consultancy

Services at a glance

consultancy

- Continuous Cyber Security Consultancy
- Continuous Vulnerability Analysis Service
- Managed Detection and Response (MDR) Service
- SOC (Security Operations Center) Service

Managed Security

- Managed Detection and Response (MDR) Service
- SOC (Security Operations Center) Service
- Cyber Incident Response (SOME) Service
- SIEM / LOG Correlation Services

Risk & Threat Analysis

- Cyber Risk and Threat Analysis Service
- Ransomware Risk Analysis Service
- APT Detection & Cyber Hygiene Analysis Service
- Purple Teaming Service

Penetration Testing

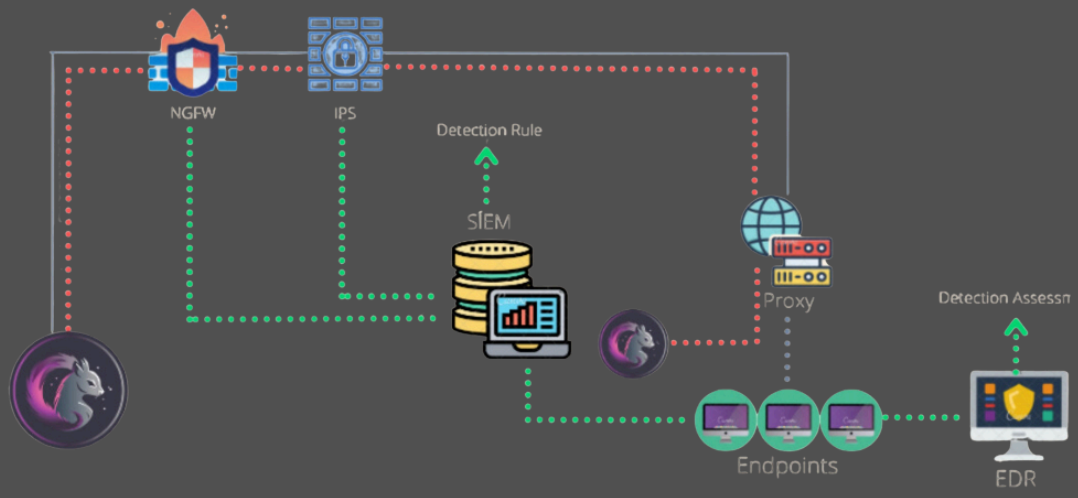
- Penetration Testing
- Red Teaming Service
- Source Code Analysis Service

Forensics

- Network Forensic Service
- Digital Forensic Service
- Mobile Forensic Service

Threatblade

Attack Simulation platform ThreatBlade simulates cyber attacks against your organization's network and systems.



Endpoint Risk Assessment

- Evaluate the security posture of individual endpoints, identify vulnerabilities, and mitigate risks by conducting endpoint-specific scenarios.

Network Risk Assessment

- Continuously monitor the network security posture using network specific attack scenarios, produce trend reports, and improve network security posture.

Identify Weaknesses

- Identify potential weaknesses in an organization's cybersecurity infrastructure and provide actionable insights for improvement purposes.

infinitum IT

"Power of Integrated Security"

Your Business's Weaknesses Do you know?

Contact us now to find out

Check Your MDR Healthcheck For Free

@infinitumitlabs @infinitumitlabs @infinitumitlab1