CYBERWEEK OF

SORINTSEC

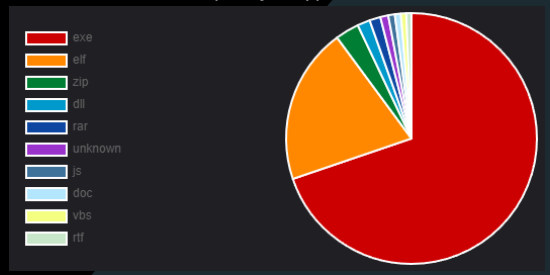
INDEX

GLOBAL WEEKLY THREAT OVERVIEW

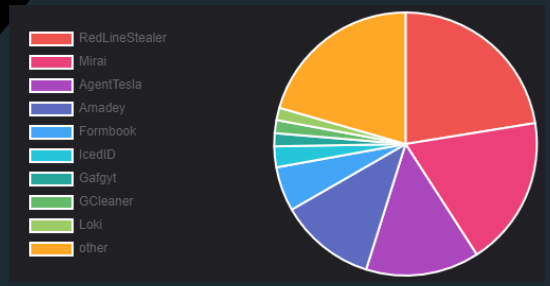
Microsoft is again pushing a Defender Antivirus update (first issued in April and pulled in May) that fixes a known issue triggering Windows Security warnings that Local Security Authority (LSA) Protection is off. Microsoft acknowledged this issue impacts Windows 11 21H2 and 22H2 systems after numerous user reports about "Local Security Authority protection is off. Your device may be vulnerable." warnings, although LSA Protection was already enabled. LSA Protection safeguards Windows users from credential theft by blocking the injection of untrusted code into the LSASS.exe process, which could help attackers extract sensitive information.

Security researchers have dissected a recently emerged ransomware strain named ‘Big Head’ that may be spreading through malvertising that promotes fake Windows updates and Microsoft Word installers. ‘Big Head’ ransomware is a .NET binary that installs three AES-encrypted files on the target system: one is used to propagate the malware, another is for Telegram bot communication, and the third encrypts files and can also show the user a fake Windows update. On execution, the ransomware also performs actions such as creating a registry autorun key, overwriting existing files if needed, setting system file attributes, and disabling the Task Manager.

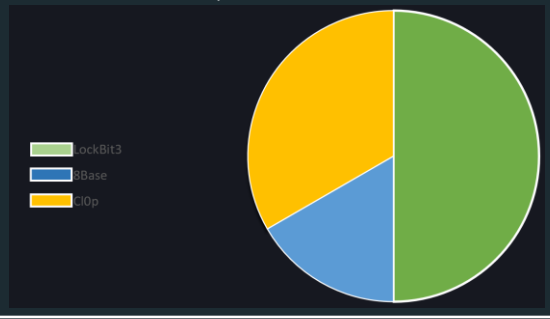
Top 10 file types



Top 10 Malware family



Top 3 Ransomware



WEEK FROM 03/07/2023 TO 07/07/2023

GLOBAL WEEKLY NOTABLE ONE

ADExplorer Sysinternal Tool – Discovery

One of the most common techniques used by malicious threat actors is to execute signed and trusted tools for malicious purposes. Mark Russinovich's Sysinternal tool suite offers powerful tools, such as ADExplorer: an advanced Active Directory (AD) viewer and editor.
A destructive cyber attack against the Albanian government by Iranian government-sponsored actors has been observed in the past. During the various phases of the attack, custom tools such as ransomware and wiper were used, but was also observed use of the ADExplorer tool in order to enumerate AD: The tool was used to easily navigate an AD database, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches.

THREAT HUNTING ACTIVITY

ADExplorer Sysinternal Tool – Discovery

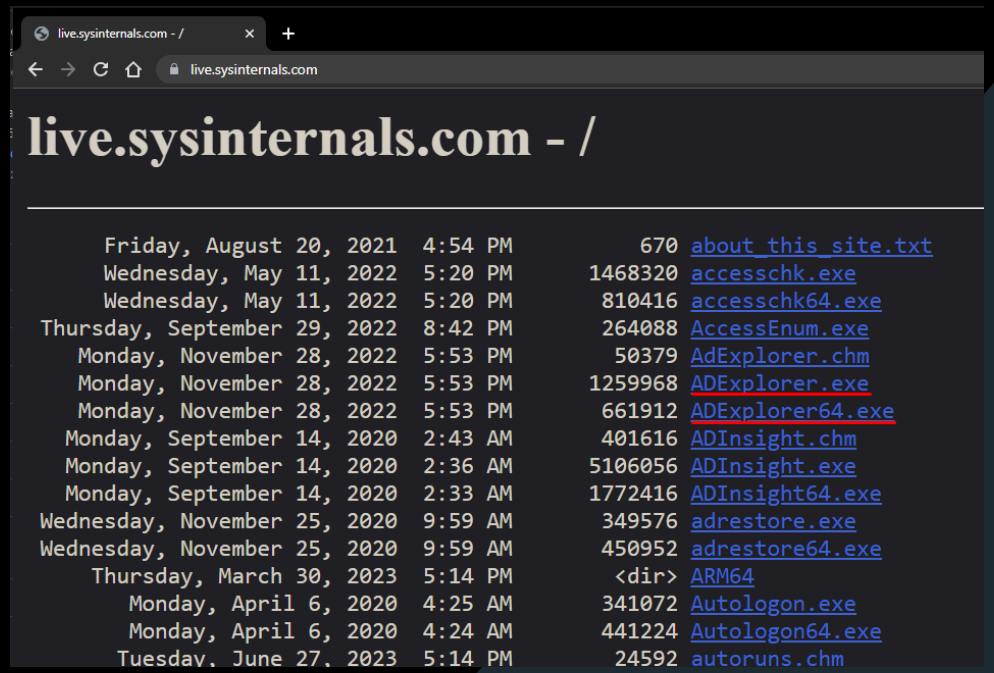
TYPE	Discovery
TACTICS & TECHNIQUES	T1087 – Account Discovery

The adversary is trying to figure out your environment. Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

THREAT HUNTING ACTIVITY

ADExplorer Sysinternal Tool – Discovery

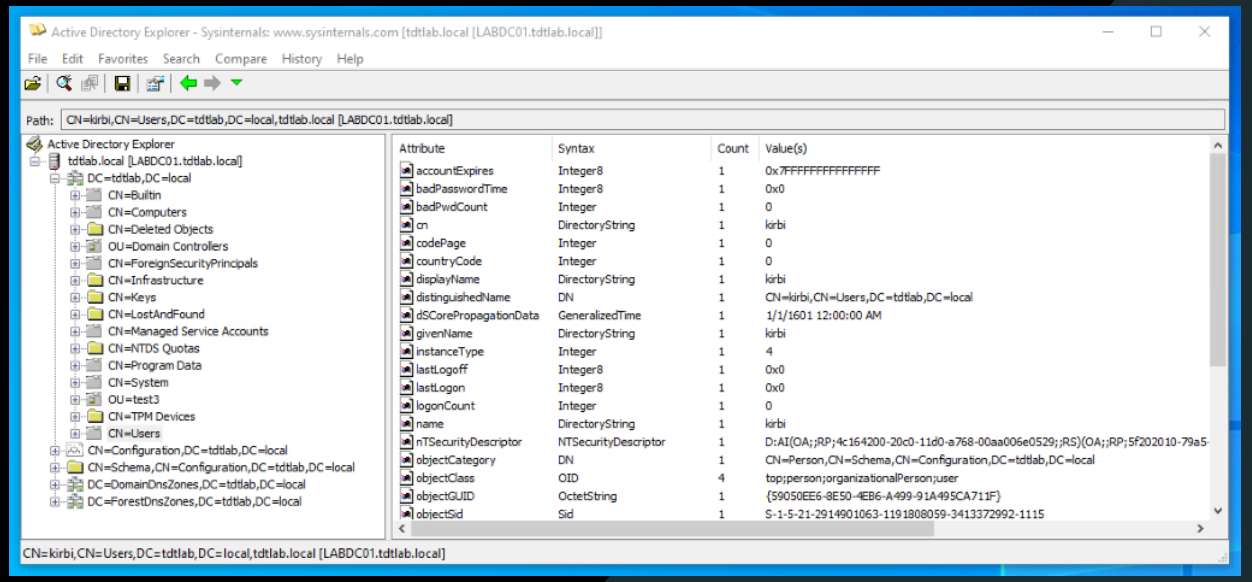
Being part of the Sysinternal tools suite, ADExplorer is a standalone executable and does not require installation. In addition to the official MS store, you can download the tool directly from live.sysinternals.com .



THREAT HUNTING ACTIVITY

ADExplorer Sysinternal Tool – Discovery

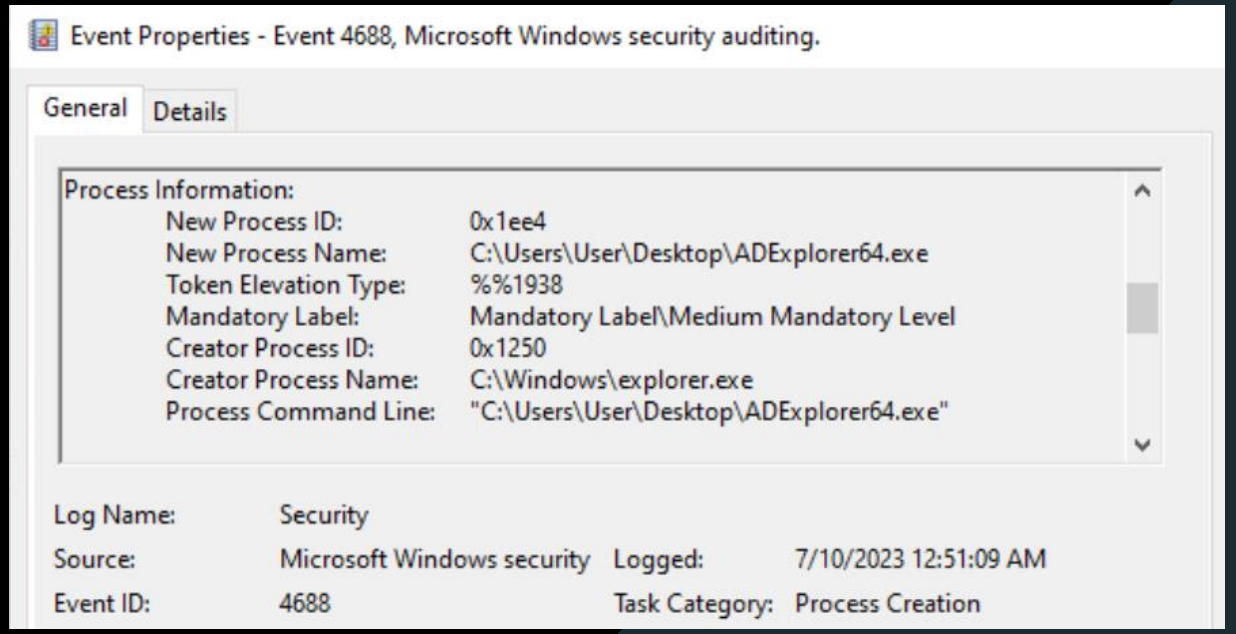
Threat Detection Team tests the execution of the tool. It's need to indicate which AD you want to connect to and a domain account. Once these values are set, It can be query entire AD through the tool, It will layout the OU structure, the user accounts and computer accounts. It may offer some help on finding juicy targets for bad actors like privileged users and database servers. Through the tool, it is also possible to create snapshots of the AD that can be verified offline, trying to discover vulnerabilities or configuration changes over time.



THREAT HUNTING ACTIVITY

ADExplorer Sysinternal Tool – Discovery

Detection can be made on evidences from EventID 4688 in order to detect the execution of the tool.



ABOUT SORINT.SEC

Sorint.SEC is the Network & Security Company of Sorint.LAB group focused on Cyber and Information Security.

Sorint.SEC services:

SOLUTION DESIGN & DELIVERY

Our D&D department can design and implements network and security solutions, evaluating the existing architecture, the
targets and helps in identifying the best solution for the customer.

MANAGED SECURITY SERVICES

24 hours per day, 7 days per week, 365 days per year, we care about Customer security.

CONSULTANCY

We offer consultancy services on all security aspects:
Vulnerability Assessments, Penetration Testing, Red Team, Incident Response and Forensic.

HTTPS://SEC.SORINT.IT
VIA VITTORIO VENETO, 25
BREMBATE (BG)