# Picus Cyber Threat Intelligence Report May 2023: Top 10 MITRE ATT&CK Techniques

picussecurity.com/resource/blog/cyber-threat-intelligence-report-may-2023

Sıla Özeren

By Sıla Özeren • June 14, 2023

Related Content

May 8, 2023 • MITRE

T1550.002 Pass the Hash: Adversary Use of Alternate Authentication

READ MORE

**The Red Report 2023**

The Top 10 MITRE ATT&CK Techniques Used by Adversaries

DOWNLOAD

Welcome to Picus Security's monthly cyber threat intelligence blog, where we list and examine the most frequently employed MITRE ATT&CK techniques observed in the wild.

Each month, we gather data from a diverse range of including *threat intelligence*and *malware dump platforms*, *CTI blogs*, *exploit databases*, ***s**andboxes*, and *network data query* results. This data is used for an in-depth analysis of malware samples, as well as threat actor and Advanced Persistent Threat (APT) campaigns.

Our main goal is to identify the tactics, techniques, and procedures (TTPs) used by cybercriminals and map these onto the MITRE ATT&CK framework. This focus facilitates a comprehensive understanding of the prevalent attack paths, helping to shape more effective mitigation strategies.

In this blog, you'll come across a thorough list of ATT&CK techniques adopted by threat actors, APT groups, and malware campaigns. As you progress further into the blog, you'll find detailed explanations of these techniques, coupled with relevant procedures for a better understanding of these ATT&CK techniques.

Simulate Emerging Cyber Threats with 14-Day Free Trial of the Picus Platform

| ATT&CK Technique | Threat Groups | Malware and Tools |
|---|---|---|

| | | | |
|---|---|---|---|
| 1 | Phishing (ATT&CK T1566) | SideWinder, APT 28, BianLian Ransomware Gang, IceID, Water Orthrus [1] | Greatness “Phishing-as-a-Service” tool, CopperStealer |
| 2 | Command and Scripting Interpreter (ATT&CK T1059) | Volt Typhoon APT, Cactus Ransomware Gang, BlackByte Ransomware Gang, Rancoz Ransomware Gang, BlackSuite Ransomware Gang, 8220 Gang [2] | COSMICENERGY OT malware, Cobalt Strike, BlackByte NT, CloudWizard APT framework, IceID banking trojan |
| 3 | System Information Discovery (ATT&CK T1082) | SharpPanda APT, Volt Typhoon APT, GoldenJackal APT, BlackByte Ransomware Gang, Rancoz Ransomware Gang, BlackSuite Ransomware Gang | DarkWatchman RAT,<br><br>SeroXen RAT, Mélofée and<br><br>AlienReverse implants [3] |
| 4 | Obfuscated Files or Information (ATT&CK T1027) | SideWinder APT, Void Rabisu APT, SharpPanda APT, LancefLy APT, ALPHV Ransomware Gang | COSMICENERGY OT malware, VMProtect tool [4], RomCom RAT, HackTool webshell encoder (tool.exe) [5], Safengine Protector v2.4.0.0 |
| 5 | Process Injection (ATT&CK T1055) | RedStinger APT, MEME#4CHAN Campaign Actors, Minas cryptocurrency miner [6] | Genesis Market malware, XWorm |
| 6 | Ingress Tool Transfer (ATT&CK T1105) | BlackCat Ransomware Gang, BianLian Ransomware Gang, Royal Ransomware Gang | Cobalt Strike, Chisel hacking tool, Ursnif/Gozi, PowerShell toolkit downloader, Advanced Port Scanner, SoftPerfect Network Scanner (netscan.exe), SharpShares, PingCastle, Rclone, Mega, Safengine Protector v2.4.0.0 |
| 7 | Scheduled Task/Job (ATT&CK T1053) | GoldenJackal APT, Earth Longzhi APT | IceID banking trojan |

| | | | |
|---|---|---|---|
| 8 | Application Layer Protocols (ATT&CK T1071) | Void Rabisu APT, 8220 Gang | |
| 9 | Impair Defenses (ATT&CK T1562) | Earth Longzhi APT, Volt Typhoon APT | AuKill EDR bypass tool, SPHijacker [7] |
| 10 | OS Credential Dumping (ATT&CK T1003) | Volt Typhoon APT, Unidentified China State-Sponsored Threat Actors [8], Cactus Ransomware Gang | LaZagne tool, HackBrowserData tool, IceID banking trojan |

## Phishing (ATT&CK T1566)

Throughout May 2023, a wide range of threat actors ramped up their use of phishing and spear-phishing techniques in their attack campaigns.

Threat actors such as SideWinder APT [9], APT28 [10], and the **BianLian Ransomware Gang** [11] used these techniques, targeting various sectors with mimicked domains and decoy emails. The APT28 group, associated with Russian GRU, notably employed diverse phishing methods against Ukrainian society. Meanwhile, the threat actors infected the target with the **IceID banking trojan** using macro-embedded Office documents, underscoring the continued effectiveness of the phishing ATT&CK technique.

Additionally, a new “Phishing-as-a-Service**”** (PaaS) tool, "Greatness" [12], targeted Microsoft 365 users, and Water Orthrusunveiled its CopperPhish [13] campaign, leveraging phishing to distribute malware and steal credit card information.

These cases emphasize the adaptability of threat actors and the importance of proactive defense strategies against evolving phishing techniques.

## Command and Scripting Interpreter (ATT&CK T1059)

Command and scripting tools were extensively used in May, enabling attackers to carry out their malicious activities swiftly.

For instance,**Volt Typhoon APT**, [14] used various tools and commands in their attack campaign, such as WMI/WMIC for gathering local drive info, PowerShell for identifying logons, portproxy commands for port forwarding, and ntdsutil.exe for copying ntds.dit files

and SYSTEM registry hives.

In addition, it is observed that COSMICENERGY, a novel OT malware, is using a command-line interface and Python scripting to interact with IEC 60870-5-104 devices, causing electric power disruption in electric transmission and distribution operations in Europe, the Middle East, and Asia [15].

BlackByte Ransomware Gang have launched a new version of their ransomware, BlackByte NT [16], and used Windows commands to perform anti-debugging measures that deletes its executable and to encrypt files, posing a significant threat to organizations' systems and data.

**IcedID** operators used tools like Cobalt Strike for privilege escalation, AdFind and adget.exefor domain discovery, and utilities like rundll32.exe and PSExec for remote execution and lateral movement [17]. These tools, while legitimate, can be exploited by threat actors like those using IcedID for nefarious activities, presenting a significant risk to network security.

Lastly and not surprisingly, ransomware actors such as BianLian[11], Rancoz[18] and BlackSuite Ransomware Gangs[19] also leveraged command and scripting tools. For instance, the new Cactus ransomware [20] variant notably demonstrates an advanced use of command and scripting techniques, particularly through PowerShell and batch scripting, to execute multi-stage encryption and obfuscation processes, raising serious concerns regarding the potential for this ransomware to evade traditional detection mechanisms and escalate its impact on unprepared systems.

## System Information Discovery (ATT&CK T1082)

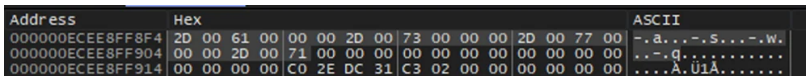
Threat actors showed a consistent trend in May: they harness the power of system information discovery to elevate the efficacy and stealthiness of their malicious campaigns.

The SharpPanda APT, known for its emphasis on system information discovery, performs comprehensive network reconnaissance prior to launching targeted attacks. The Volt Typhoon APT, another adept at system information discovery, leverages this intelligence to mount customized attacks on its targets. GoldenJackal APT, on the other hand, exploits this technique not only for system profiling but also to prepare for their intricate cyber-espionage operations.

In the ransomware realm, the BlackByte NT ransomware employs techniques such as dynamic API import, PEB structure examination, execution argument checks, and DLL retrieval for enabling the ransomware to access system functionality, showcasing its active system information discovery capabilities.

Similarly, Rancoz ransomware employs drive enumeration to identify and traverse through available local and remote drives, including network shares, in order to locate and target files for encryption [16]. DarkWatchman RAT operators, another significant threat, rely on system information discovery to maintain persistence and avoid detection, showing a trend in cyber threats exploiting this attack technique for a variety of malicious objectives.

| Threat Actors and Malware | Commands, Tools and Files Used for Information Discovery |
|---|---|
| SharpPanda APT | DLL Downloader (“c6gt.b”) - When the loader is executed through rundll32.exe, it collects various data from the target’s system. [21] |
| Volt Typhoon APT | netstat -ano,<br>reg query hklm\software\,<br>systeminfo,<br>tasklist /v,<br>whoami,<br>net group "Domain Admins" /dom,<br>netsh interface firewall show all,<br>netsh interface portproxy show all [14] |
| GoldenJackal APT | netstat -aon,<br>ipconfig /displaydns,<br>reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings" /v,<br>tasklist,<br>netsh winhttp show proxy [22] |

| | |
|---|---|
| BlackByte Ransomware Gang | anti-debug check by examining the "BeingDebugged" flag within the PEB structure,<br><br>checking the arguments passed during the execution of needed APIs for the following flags: -a, -s, -w, -q,<br><br>  <br><br><br>retrieving functions from various DLLs, such as kernel32.dll, ntdll.dll, advapi32.dll [16] |
| Rancoz Ransomware Gang | The main thread of the ransomware evaluates the drive types, which can be categorized as DRIVE_UNKNOWN, DRIVE_NO_ROOT_DIR, DRIVE_REMOVABLE, DRIVE_FIXED, and DRIVE_REMOTE [16]. |
| BlackSuite Ransomware Gang | NetShareEnum() APIto obtain information about the available network shares, such as (ADMIN$) and interprocess communication (IPC$) shares, on the local system [17]. |
| DarkWatchman RAT Operators | start_instance() function within the DarkWatchMan RAT collects the victim's system information, including the operating system version, domain role, and antivirus software. |

## Obfuscated Files or Information (ATT&CK T1027)

May was another month that demonstrates the malicious use of advanced obfuscation techniques to evade detection by security software.

For instance, SideWinder APTuses obfuscation and decoding techniques in their recent campaign, which targets Pakistan government organizations and now Turkey by delivering the next stage payload through server-based polymorphism to evade detection by signature-based antivirus [23].

In another case, Void Rabisu APT has employed binary padding as a technique for obfuscation in their attacks [7]. Binary padding involves adding a significant amount of overlay bytes to the payload files, thereby increasing the size of the malicious payload. This method aims to evade detection by security scanners and make analysis more challenging.

The COSMICENERGY, assumed to be related to the Russian Emergency Response Exercises, is using the certutil utility to handle the Base64-encoded malicious executables. This shows us a sign that classical obfuscation techniques like file encoding are still used by adversaries as they can bypass security controls that rely on detecting specific file formats or signatures.

| Threat Actors and Malware | Commands, Tools and Files used |
|---|---|
| SideWinder APT | In their attack campaign, the "**1.a**" object extracted from the RTF file is a highly obfuscated JavaScript that is decoded to reveal a base64 encoded data blob, two communication URLs, and other important information used to communicate with the command and control server [23]. |
| Lancefly APT | In their attack campaign, Lancefly encoded the MerDoor backdoormalware for obfuscation [5]. |
| Earth Longzhi APT | In the course of their attack campaigns, Earth Longzhi APTconceals their malicious payloads through encryption. Disguised under the name "MPClient.dll," the newly introduced Croxloadervariant accesses the encrypted payload "MpClient.bin," and proceeds to decrypt its hidden content [7]. |

## Process Injection (ATT&CK T1055)

In May, we witnessed a surge in sophisticated process injection methods designed to impair defense controls.

The RedStinger APT utilized a DLL with Process Doppelganging (ATT&CK T1055.013) capabilities for stealthy operations and bypassing security protocols like whitelisting [24].

The MEME#4CHAN campaign employed the Proc Memory (ATT&CK T1055.009) technique, using .NET reflection for in-memory execution of malicious code and making it challenging for security professionals to predict and counter the attack's behavior [25].

Genesis Market's tactics involved Process Hollowing (ATT&CK T1055.012) by replacing the Portable Executable (PE) of its host process with a new PE, bypassing routine security measures [26].

The level of sophistication in these process techniques highlight the need for enhanced detection and response strategies, as it becomes more and more difficult for security professionals to detect the existence of an adversary.

| Threat Actors and Malware | Commands, Tools and Files used |
|---|---|

| | |
|---|---|
| RedStinger APT | In the case of RedStinger, the DLL file named InjectorTransactedHollow.dllis used to perform the injection technique. The injected code runs in the memory space of a legitimate process, mobisync.exe, which makes it difficult for security software to detect. |
| MEME#4CHAN | The MEME#4CHAN Attack Campaign leverages process memory injection by embedding binary data within a **PowerShell** script which is then loaded into the memory of system processes like RegSvcs.exe or Msbuild.exe, using .NET assemblies via reflection. |
| Genesis Market | The malware decrypts nested encrypted shellcode stages via a legitimate **svchost.exe** process, ultimately using process hollowing to replace the svchost.exe's own Portable Executable(PE) with the final decrypted shellcode stage's PE. |

## Ingress Tool Transfer (ATT&CK T1105)

In May 2021, there was an alarming increase in the use of third-party and ingress tools by cyber adversaries.

The BianLian Ransomware Gang, in particular, has made use of advanced port scanners and SoftPerfect network scanners for reconnaissance, while relying on PingCastle for AD enumeration. Additionally, Rclone and Mega have been used for data exfiltration purposes.

In their attack campaign, the Royal Ransomware Gang has also been observed using a wide array of tools, including Chisel and Cobalt Strike for covert communication and lateral movement within targeted systems. Legitimate remote access tools like AnyDesk and LogMeIn have also been repurposed by attackers for long-term persistence.

Finally, BlackCat Ransomware Ganghave used a custom kernel driver for evasion, while using the Safengine Protector tool for obfuscation purposes [27].

This increased use of third-party tools highlights the growing sophistication of ransomware attacks and the need for organizations to prioritize proactive defense strategies.

| Threat Actors and Malware | Tools and Software Used |
|---|---|
| BlackCat Ransomware Gang | Safengine Protector v2.4.0.0 |

| | |
|---|---|
| BianLian Ransomware Gang | Advanced Port Scanner,<br>SoftPerfect Network Scanner (netscan.exe),<br>SharpShares,<br>PingCastle,<br>Rclone,<br>Mega |
| Royal Ransomware Gang | Chisel (TCP/UDP tunnel over HTTP)<br>Cobalt Strike<br>AnyDesk<br>LogMeIn<br>Atera<br>Exfil<br>Ursnif/Gozi<br>PowerShell Toolkit Downloader |

## Scheduled Task/Job (ATT&CK T1053)

May spotlighted advanced task scheduling tactics by cyber threat groups.

GoldenJackal APT utilized 'schtasks.exe', ensuring malware persistence post-infiltration [20].

Earth Longzhi APT exploited Windows COM objects for privilege escalation, bypassing the Windows User Account Control (UAC), and hiding payloads effectively [1].

IcedID banking trojan harnessed task scheduling to maintain a malicious DLL active on the system [28]. This intricate layering of techniques signifies an alarming evolution in threat actor capabilities.

For IT security, it underscores the necessity of continuous system monitoring, cutting-edge detection systems, and thorough audits to safeguard against these progressively sophisticated attacks.

| Threat Actors and Malware | Tools and Commands Used |
|---|---|

| | |
|---|---|
| GoldenJackal APT | GoldenJackal APT uses its JackalWorm malware to create a Windows Task Scheduler job, typically by calling the 'schtasks.exe' utility with parameters like '/create /tn "taskname" /tr "tasklocation\malware.exe" /sc minute /mo 1'. |
| Earth Longzhi (a subgroup of the APT41) | The Earth Longzhi employs a tool called dwm.exe, which modifies image paths and command-line information for obfuscation, leverages the COM object 'IElevatedFactoryServer' to bypass the Windows UAC, and establishes the high-privilege scheduled task disguised as legitimate Google Update, which also deploys a payload downloader named '**dllhost.exe**'. |
| IceID | After the initial execution of the IcedID malware, it creates a DLL file named Utucka.dll. Following this, a new scheduled task was created to execute this DLL file at specific intervals. This task is executed in the background by the Task Scheduler service (svchost.exe -k netsvcs -p -s Schedule). |

## Application Layer Protocols (ATT&CK T1071)

In May, our observations pointed to the "Web Protocols" sub-technique as the predominant method used in Application Layer Protocols attacks. Attackers exploit this technique to establish and maintain an encrypted command and control (C2) channel over HTTPS. This channel serves a dual purpose: facilitating communication with the target system and enabling the extraction of sensitive data to a server under the control of the attacker.

For instance, the Russian-originated Void Rabisu APTgroup is using a remote access trojan called RomCom that uses HTTPS for C&C communications [29].

In addition, the 8220 Gang has been found to cunningly use HTTP requests for malicious purposes, most notably exploiting the Oracle WebLogic vulnerability CVE-2017-3506 [2]. By executing arbitrary commands via a specifically crafted XML document embedded in an HTTP request, they're able to gain unauthorized access to sensitive data and even compromise entire systems.

## Impair Defenses (ATT&CK T1562)

Upon gaining access to a target system, adversaries consistently aim to employ the stealthiest attack techniques to evade detection by defense controls. This is precisely why the “Impair Defenses” has positioned itself among the top ten techniques.

Earth Longzhi APTperformed a sophisticated defense evasion attack called “Stack Rumbling” to disable security defenses [30], impairing running security products via a vulnerable driver in a “Bring Your Own Vulnerable Driver” attack [7].  On the other hand, Volt

Typhoon APT selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity [31].

On the other hand, an emerging defense evasion tool called AuKilluses an old Windows driver tobypass EDR software and prepare for malware installation, leveraging a BYOVD attack like Earth Longzhi [32]. This technique, bypassing critical security measures using an authorized yet outdated driver, presents significant concern for potential widespread cyberattacks across crucial sectors.

## OS Credential Dumping (ATT&CK T1003)

Credential dumping remains a persistent and powerful tool in the top ten most deployed tactics, techniques, and procedures (TTPs), as demonstrated by Chinese threat actors in their sophisticated cyber attack on Taiwan's critical infrastructure. Using advanced tools like LaZagne and HackBrowserData, they extracted NTLM hash passwords, enabling an alarming level of privilege escalation and underscoring the pressing need for robust cybersecurity measures [8]. This tactic was also seen in the deployment of Cactus ransomware, which dumped browser credentials and manually scanned for password files [20].

The Volt Typhoon APTfurther escalated this approach, specifically targeting the Local Security Authority Subsystem Service (LSASS) to acquire OS credential hashes and increase their privileges. They also used the command-line tool, Ntdsutil.exe, to create installation media containing usernames and password hashes from domain controllers, which could be cracked offline, ensuring persistent system access. Similarly, **IceID** conducted credential dumping [33] and ran Windows discovery commands to survey RDP access across the environment, further showcasing the evolving complexity of these threat strategies.

## References


[1] “Water Orthrus New Campaigns Deliver Rootkit and Phishing Modules,” *Trend Micro*, May 15, 2023. [Online]. Available: https://www.trendmicro.com/en_us/research/23/e/water-orthrus-new-campaigns-deliver-rootkit-and-phishing-modules.html. [Accessed: Jun. 09, 2023]

[2] “8220 Gang Evolves With New Strategies,” *Trend Micro*, May 16, 2023. [Online]. Available: https://www.trendmicro.com/en_us/research/23/e/8220-gang-evolution-new-strategies-adapted.html. [Accessed: Jun. 09, 2023]

[3] “Mélofée: a new alien malware in the Panda’s toolset targeting Linux hosts.” [Online]. Available: https://blog.exatrack.com/melofee/. [Accessed: Jun. 09, 2023]

[4] “Void Rabisu’s Use of RomCom Backdoor Shows a Growing Shift in Threat Actors’ Goals,” *Trend Micro*, May 30, 2023. [Online]. Available: https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html. [Accessed: Jun. 09, 2023]

[5] “Lancefly: Group Uses Custom Backdoor to Target Orgs in Government, Aviation, Other Sectors.” [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor. [Accessed: Jun. 09, 2023]

[6] I. Borisov, “Minas – on the way to complexity,” *Kaspersky*, May 17, 2023. [Online]. Available: https://securelist.com/minas-miner-on-the-way-to-complexity/109692/. [Accessed: Jun. 09, 2023]

[7] “Attack on Security Titans: Earth Longzhi Returns With New Tricks,” *Trend Micro*, May 02, 2023. [Online]. Available: https://www.trendmicro.com/en_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks.html. [Accessed: Jun. 02, 2023]

[8] “Chinese Threat Actor Used Modified Cobalt Strike Variant to Attack Taiwanese Critical Infrastructure.” [Online]. Available: https://blog.eclecticiq.com/chinese-threat-actor-used-modified-cobalt-strike-variant-to-attack-taiwanese-critical-infrastructure. [Accessed: Jun. 09, 2023]

[9] “The distinctive rattle of APT SideWinder” [Online]. Available: https://www.group-ib.com/blog/hunting-sidewinder/

[10] F. Aimé, “APT28 leverages multiple phishing techniques to target Ukrainian civil society,” *Sekoia.io Blog*, May 17, 2023. [Online]. Available: https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/. [Accessed: Jun. 02, 2023]

[11] “#StopRansomware: BianLian Ransomware Group,” *Cybersecurity and Infrastructure Security Agency CISA*. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a. [Accessed: Jun. 02, 2023]

[12] T. Pereira, “New phishing-as-a-service tool ‘Greatness’ already seen in the wild,” *Cisco Talos Blog*, May 10, 2023. [Online]. Available: https://blog.talosintelligence.com/new-phishing-as-a-service-tool-greatness-already-seen-in-the-wild/. [Accessed: Jun. 06, 2023]

[13] “Water Orthrus New Campaigns Deliver Rootkit and Phishing Modules,” *Trend Micro*, May 15, 2023. [Online]. Available: https://www.trendmicro.com/en_us/research/23/e/water-orthrus-new-campaigns-deliver-rootkit-and-phishing-modules.html. [Accessed: Jun. 06, 2023]

[14] M. T. Intelligence, “Volt Typhoon targets US critical infrastructure with living-off-the-land techniques,” *Microsoft Security Blog*, May 24, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-

infrastructure-with-living-off-the-land-techniques/. [Accessed: Jun. 02, 2023]

[15] “New COSMICENERGY Malware Exploits ICS Protocol to Sabotage Power Grids,” *The Hacker News*, May 26, 2023. [Online]. Available: https://thehackernews.com/2023/05/new-cosmicenergy-malware-exploits-ics.html. [Accessed: Jun. 06, 2023]

[16] “Back in Black: BlackByte Ransomware returns with its New Technology (NT) version,” May 22, 2023. [Online]. Available: https://blog.cluster25.duskrise.com/2023/05/22/back-in-black-blackbyte-nt. [Accessed: Jun. 06, 2023]

[17] “IcedID Macro Ends in Nokoyawa Ransomware,” *The DFIR Report*, May 22, 2023. [Online]. Available: https://thedfirreport.com/2023/05/22/icedid-macro-ends-in-nokoyawa-ransomware/. [Accessed: Jun. 06, 2023]

[18] “Dissecting Rancoz Ransomware,” *Cyble*, May 11, 2023. [Online]. Available: https://blog.cyble.com/2023/05/11/dissecting-rancoz-ransomware/. [Accessed: Jun. 06, 2023]

[19] “BlackSuit Ransomware Strikes Windows and Linux Users,” *Cyble*, May 12, 2023. [Online]. Available: https://blog.cyble.com/2023/05/12/blacksuit-ransomware-strikes-windows-and-linux-users/. [Accessed: Jun. 06, 2023]

[20] L. Iacono, S. Green, and D. Truman, “CACTUS Ransomware: Prickly New Variant Evades Detection,” *Kroll*, May 10, 2023. [Online]. Available: https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection. [Accessed: Jun. 06, 2023]

[21] “SharpPanda APT Campaign Expands its Arsenal Targeting G20 Nations,” *Cyble*, Jun. 01, 2023. [Online]. Available: https://blog.cyble.com/2023/06/01/sharppanda-apt-campaign-expands-its-arsenal-targeting-g20-nations/. [Accessed: Jun. 06, 2023]

[22] G. Dedola, “Meet the GoldenJackal APT group. Don’t expect any howls,” *Kaspersky*, May 23, 2023. [Online]. Available: https://securelist.com/goldenjackal-apt-group/109677/. [Accessed: Jun. 06, 2023]

[23] “SideWinder Uses Server-side Polymorphism to Attack Pakistan Government Officials — and Is Now Targeting Turkey,” *BlackBerry*, May 08, 2023. [Online]. Available: https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan. [Accessed: Jun. 06, 2023]

[24] “Uncovering RedStinger - Undetected APT cyber operations in Eastern Europe since 2020,” *Malwarebytes*, May 10, 2023. [Online]. Available: https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger. [Accessed: Jun. 06, 2023]

[25] “Securonix Threat Labs Security Advisory: Latest Update: Ongoing MEME#4CHAN Attack/Phishing Campaign uses Meme-Filled Code to Drop XWorm Payloads,” *Securonix*, May 12, 2023. [Online]. Available: https://www.securonix.com/blog/securonix-threat-labs-security-meme4chan-advisory/. [Accessed: Jun. 07, 2023]

[26] “Technical analysis of the Genesis Market,” Apr. 05, 2023. [Online]. Available: https://sector7.computest.nl/post/2023-04-technical-analysis-genesis-market/.[Accessed: Jun. 07, 2023]

[27] “BlackCat Ransomware Deploys New Signed Kernel Driver,” *Trend Micro*, May 22, 2023. [Online]. Available: https://www.trendmicro.com/en_us/research/23/e/blackcat-ransomware-deploys-new-signed-kernel-driver.html. [Accessed: Jun. 07, 2023]

[28] “Malicious ISO File Leads to Domain Wide Ransomware,” *The DFIR Report*, Apr. 03, 2023. [Online]. Available: https://thedfirreport.com/2023/04/03/malicious-iso-file-leads-to-domain-wide-ransomware/. [Accessed: Jun. 07, 2023]

[29] “Void Rabisu’s Use of RomCom Backdoor Shows a Growing Shift in Threat Actors’ Goals,” *Trend Micro*, May 30, 2023. [Online]. Available: https://www.trendmicro.com/en_id/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html. [Accessed: Jun. 09, 2023]

[30] A. Mascellino, “Earth Longzhi Uses ‘Stack Rumbling’ to Disable Security Software,” *Infosecurity Magazine*, May 03, 2023. [Online]. Available: https://www.infosecurity-magazine.com/news/earth-longzhi-disable-security/. [Accessed: Jun. 02, 2023]

[31] “People’s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection,” *Cybersecurity and Infrastructure Security Agency CISA*. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a. [Accessed: Jun. 09, 2023]

[32] “AuKill: A ‘defense evasion tool’ disables EDR software via BYOVD attack,” *SISA*, May 19, 2023. [Online]. Available: https://www.sisainfosec.com/threat-a-licious/aukill-defense-evasion-tool-disables-edr-software-via-byovd-attack/. [Accessed: Jun. 09, 2023]

[33] Y. Ernalbant, “IcedID Macro Attacks Deploy Nokoyawa Ransomware,” *SOCRadar® Cyber Intelligence Inc.*, May 22, 2023. [Online]. Available: https://socradar.io/icedid-macro-attacks-deploy-nokoyawa-ransomware/. [Accessed: Jun. 09, 2023]

#Article #Cyber Threat Intelligence

Related Content

May 8, 2023 • MITRE

T1550.002 Pass the Hash: Adversary Use of Alternate Authentication

READ MORE

**The Red Report 2023**

---

The Top 10 MITRE ATT&CK Techniques Used by Adversaries

DOWNLOAD