Inside Intelligence Center: LUNAR SPIDER Enabling Ransomware Attacks on Financial Sector with Brute Ratel C4 and Latrodectus

Archived: 2026-04-05 16:53:59 UTC

Executive Summary

In October 2024, EclecticIQ analysts observed a malvertising campaign employing an obfuscated JavaScript downloader known as Latrodectus [1] to deliver a malicious payload associated with Brute Ratel C4 (BRc4) [2]. Analysts assess with high confidence that this campaign is very likely linked to LUNAR SPIDER [3], a Russian-speaking, financially motivated threat actor group active since at least 2009. LUNAR SPIDER is responsible for developing several high-profile malware families, including IcedID [4] and Latrodectus. IcedID malware is often distributed via malware-as-a-service (MaaS) offerings, enabling affiliates, such as the ALPHA SPIDER/BlackCat ransomware group [5], to leverage these services for initial compromise.

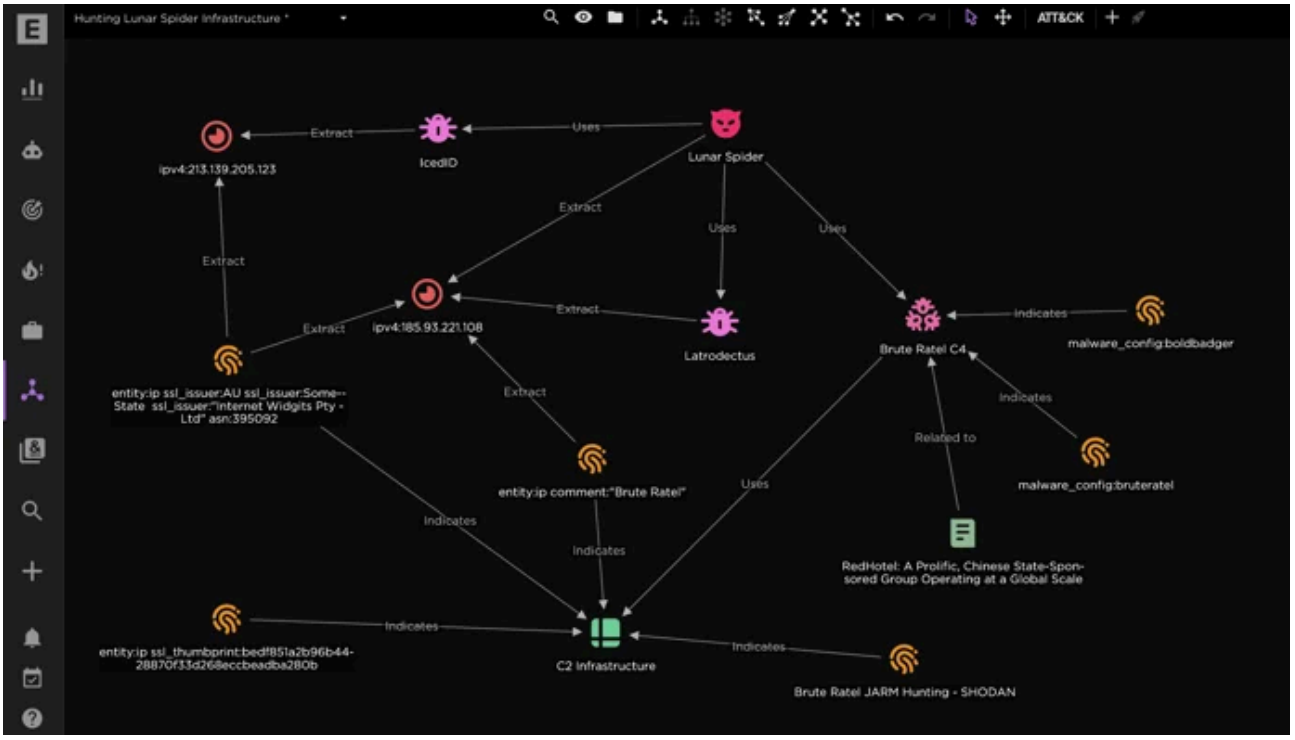

Figure 1 - Graph view of LUNAR SPIDER malvertising campaign
as seen in EclecticIQ Intelligence Center *(click on image to enlarge)*.

On May 30, 2024, the FBI and international partners executed Operation Endgame [6], dismantling the command-and-control infrastructures of at least four malware variants, including IcedID (BokBot), Smokeloader [7] , Pikabot [8], and Bumblebee [9]. EclecticIQ analysts assess with high confidence that LUNAR SPIDER resumed operations following law enforcement actions that disrupted their infrastructure. In their latest campaigns, the

actor leveraged Brute Ratel C4, demonstrating notable adaptability and determination to continue their activities despite heightened law enforcement pressure.

Conti Leak Revealed the Connection Between LUNAR SPIDER and WIZARD SPIDER members

EclecticIQ analysts assess with high confidence that, based on leaked Conti ransomware group communications that was published in 2022, LUNAR SPIDER has established significant connections within the cybercrime ecosystem [10]. They have very likely provided initial access to ransomware operators such as WIZARD SPIDER [11], the Russia-based group behind the TrickBot [12] malware and the Conti Ransomware-as-a-Service (RaaS) [13]. This collaboration between LUNAR SPIDER and WIZARD SPIDER has facilitated ransomware campaigns by sharing tools and infrastructures like IcedID and other services for evading EDR/AV detection.

The LUNAR SPIDER group was previously led by Vyacheslav Igorevich Penchukov [14], also known by several aliases including Tank, Zeus, Zevs, Father, and TopBro. Penchukov was a key figure in LUNAR SPIDER's operations before his arrest in Switzerland in September 2022. Figure 2 shows the leaked conversation between Russian speaking threat actors angelo and manuel, very likely the developers inside the Conti Ransomware as a service (RaaS). Translated conversation revealed that LUNAR SPIDER leader Zeus (Penchukov) was their partner.

Despite his extradition to the United States and sentencing to 18 years in prison in 2024, LUNAR SPIDER continues to operate, adapting to leadership changes and law enforcement actions with resilience.

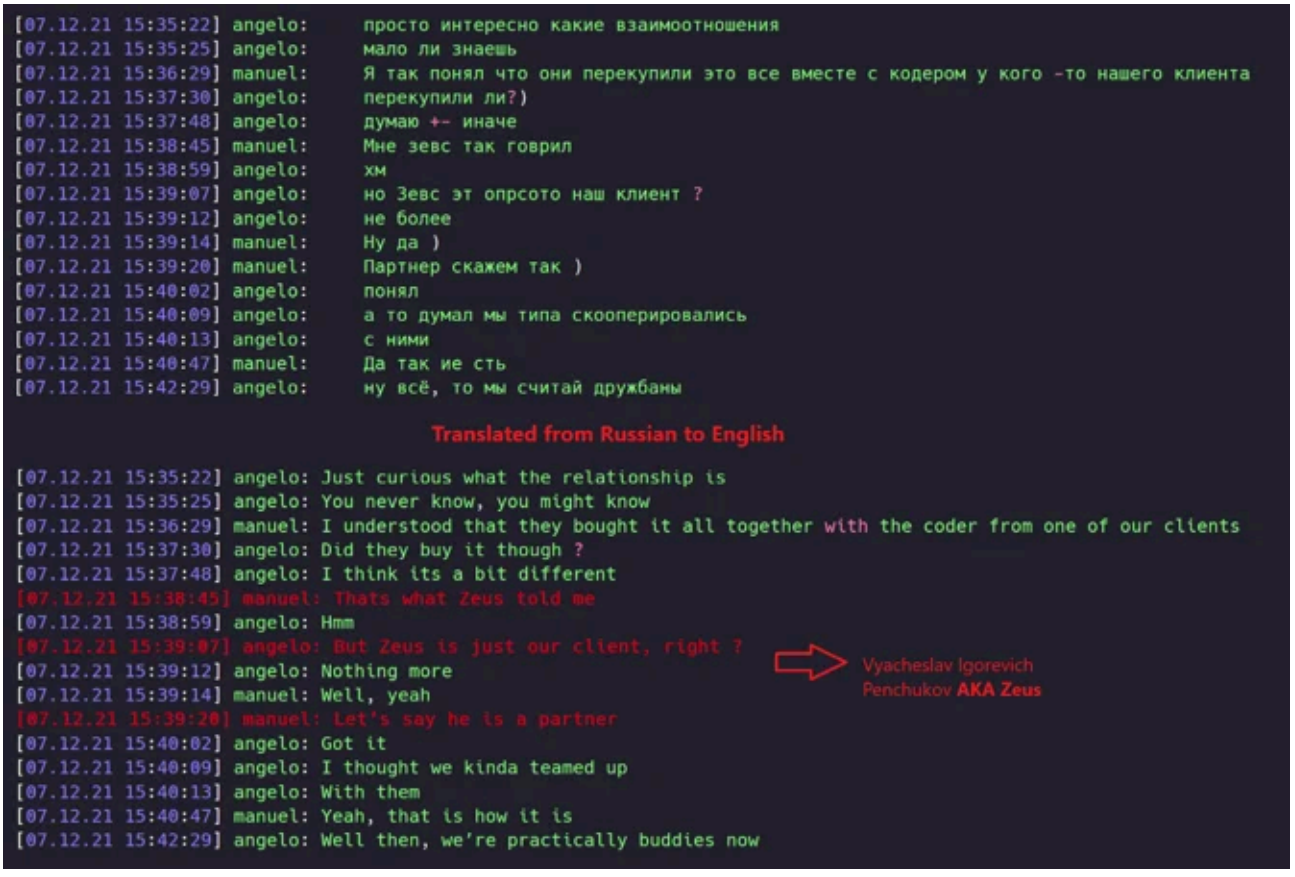

Figure 2 – Conversation between Conti Ransomware (WIZARD SPIDER) developers.

Analysts assess with high confidence that LUNAR SPIDER maintains affiliations with other ransomware groups, including Nemty [15] (aka: TRAVELING SPIDER) and TA2101 (aka: TWISTED SPIDER) [16], which have leveraged LUNAR SPIDER's malware IcedID to gain initial access to victim environments. These collaborations further emphasize LUNAR SPIDER's central role as an initial access broker in the cybercrime ecosystem.

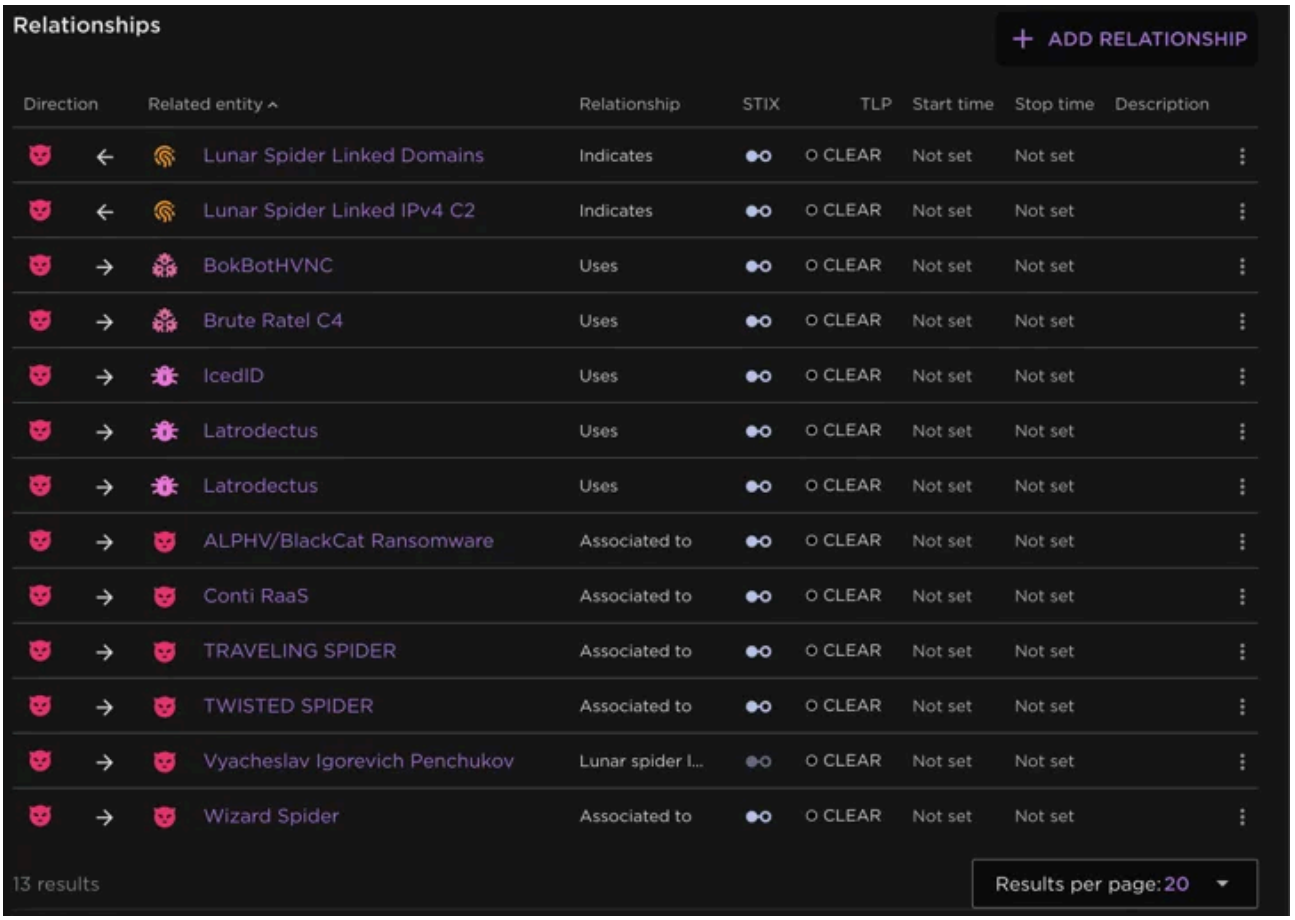

Figure 3 – Relationships of LUNAR SPIDER.

LUNAR SPIDER Threat Actor Switched from IcedID to Brute Ratel C4 Malware

EclecticIQ analysts assess with high confidence that LUNAR SPIDER has shifted tactics, moving away from their previous use of IcedID (BokBot) to now leveraging Latrodectus and Brute Ratel C4 malware.

Analysts have uncovered that the threat actor group LUNAR SPIDER is behind over 200 malicious infrastructures (figure 4) associated with both the IcedID and Latrodectus malware families. While these malware operations were previously considered separate, they share significant overlaps in their underlying infrastructure. For instance, both use SSL certificates with nearly identical issuer details like "AU," "Some-State," and "Internet Widgits Pty Ltd." Additionally, LUNAR SPIDER consistently employs the same service providers, such as SHOCK-1 (ASN 395092), across both campaigns. This consistent use of shared providers and similar infrastructure highlights how LUNAR SPIDER is efficiently coordinating its malicious activities across different malware families.

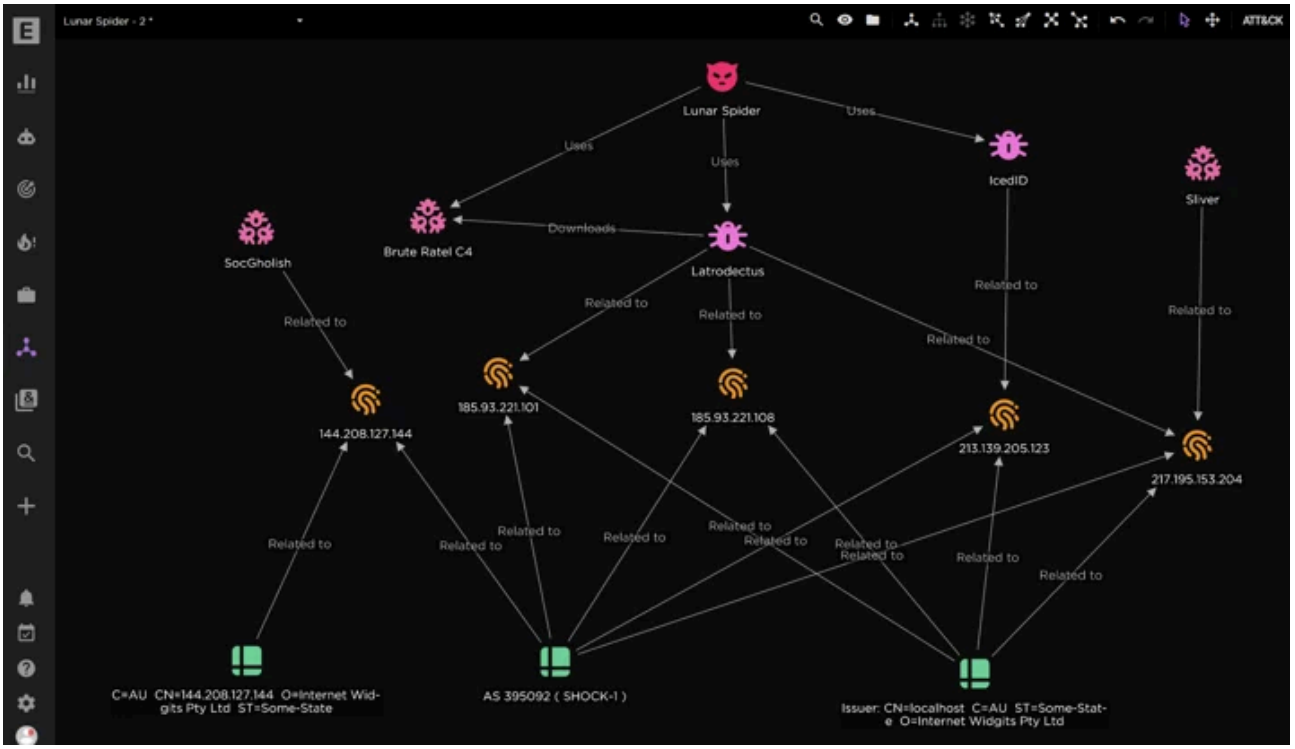

Figure 4 – Overlaps of infrastructures between different malware variants.

The LUNAR SPIDER-associated downloader, Latrodectus, was observed targeting financial services to deploy Brute Ratel, signalling a strategic change in their malware deployment approach. This switch highlights the group's continued evolution and adaptation in their cyber operations, as they adopt stealthier attacks.

Tracking Latrodectus Infrastructures

Analysts utilized the EclecticIQ Threat Intelligence Platform (TIP), Intelligence Center, to extract malicious infrastructures that were linked to Latrodectus. According to Open-Source Intelligence, analysts observed more than 200 Latrodectus servers that are very likely managed by members of the LUNAR SPIDER threat actor.

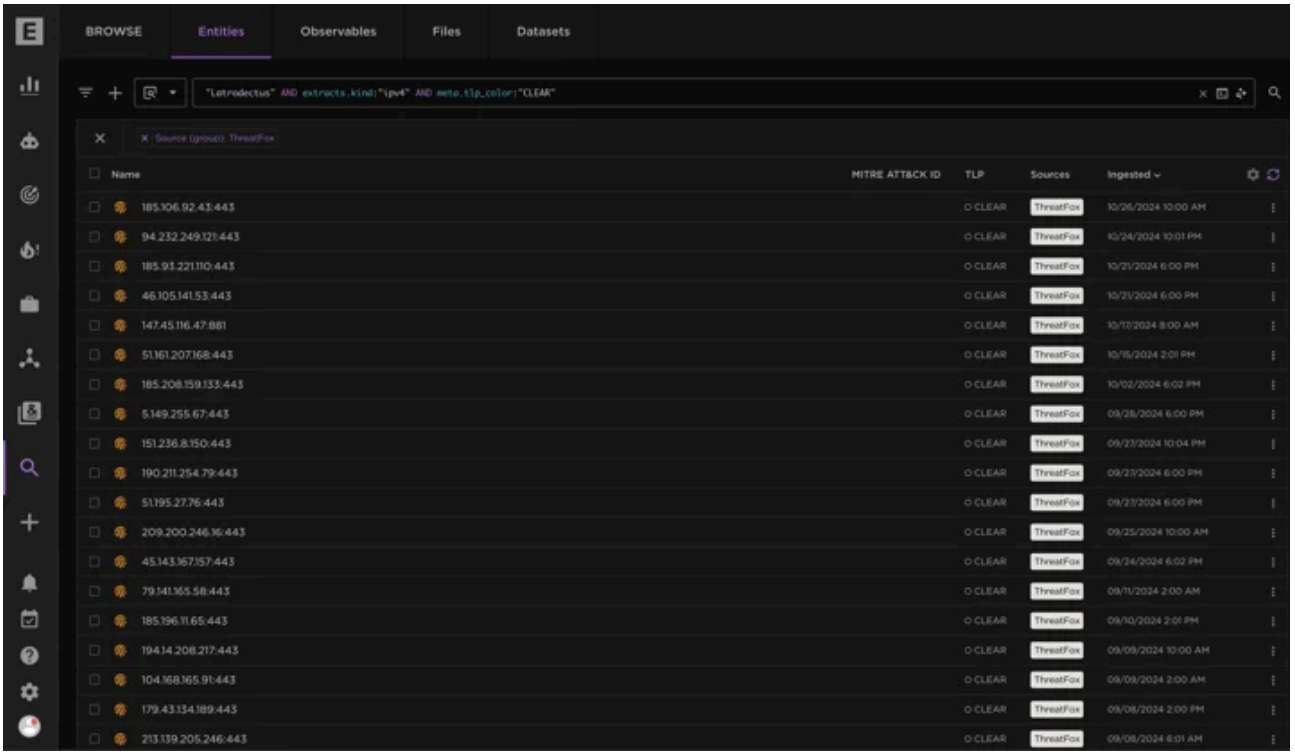

Figure 5 – Tracking Latrodectus infrastructures
in Intelligence Center.

Figure 6 highlights the top Autonomous System Numbers (ASNs) linked with previously detected Latrodectus infrastructure. ASNs are critical for identifying key service providers that may facilitate cyber threat activity. Leading the list is BlueVPS OU (AS 62005) with 33 instances, followed by OVH SAS (AS 16276) and The Infrastructure Group B.V. (AS 60404). Tracking these ASNs provides valuable insight into malicious infrastructure, as attackers often rely on specific hosting services to operate attacks or host command and control (C2) servers.

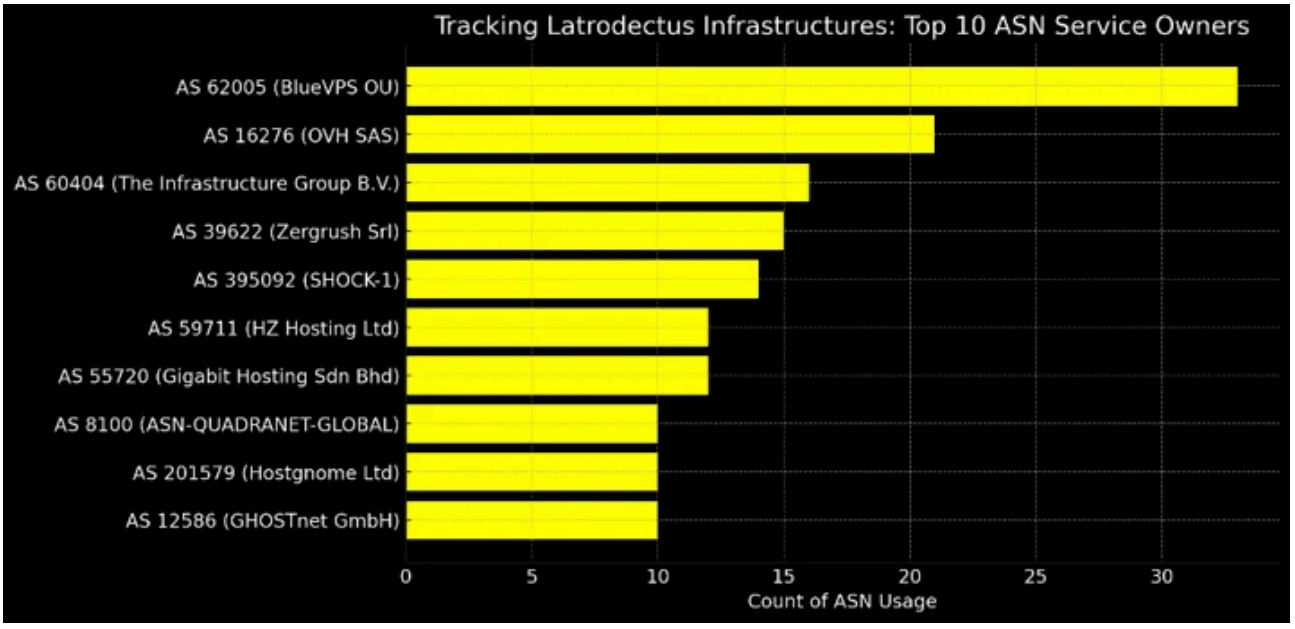

Figure 6 – Top 10 ASN service owners used by Latrodectus malware.

IcedID Malware Enables ALPHV Ransomware Attack, Revealing Shared Infrastructure with LUNAR SPIDER

In a campaign observed in October 2023, threat actors linked to ALPHV (also known as BlackCat) executed a Ransomware attack by using IcedID malware as the initial compromise vector. [17] The operation began with a spam campaign delivering a version of IcedID through a malicious ZIP file containing a Visual Basic Script (VBS). Upon execution, the IcedID loader installed itself, and the attackers used Impacket's wmiexec [18] and RDP for lateral movement, deploying ScreenConnect across systems. The campaign further escalated with the deployment of Cobalt Strike beacons for command-and-control (C2) purposes and the use of the CSharp Streamer RAT [19] to exfiltrate credentials and sensitive data via tools like Rclone [20]. Eight days after the initial breach, ALPHV ransomware was deployed across all domain-joined Windows systems, leading to successful data encryption and a ransom note being left behind.

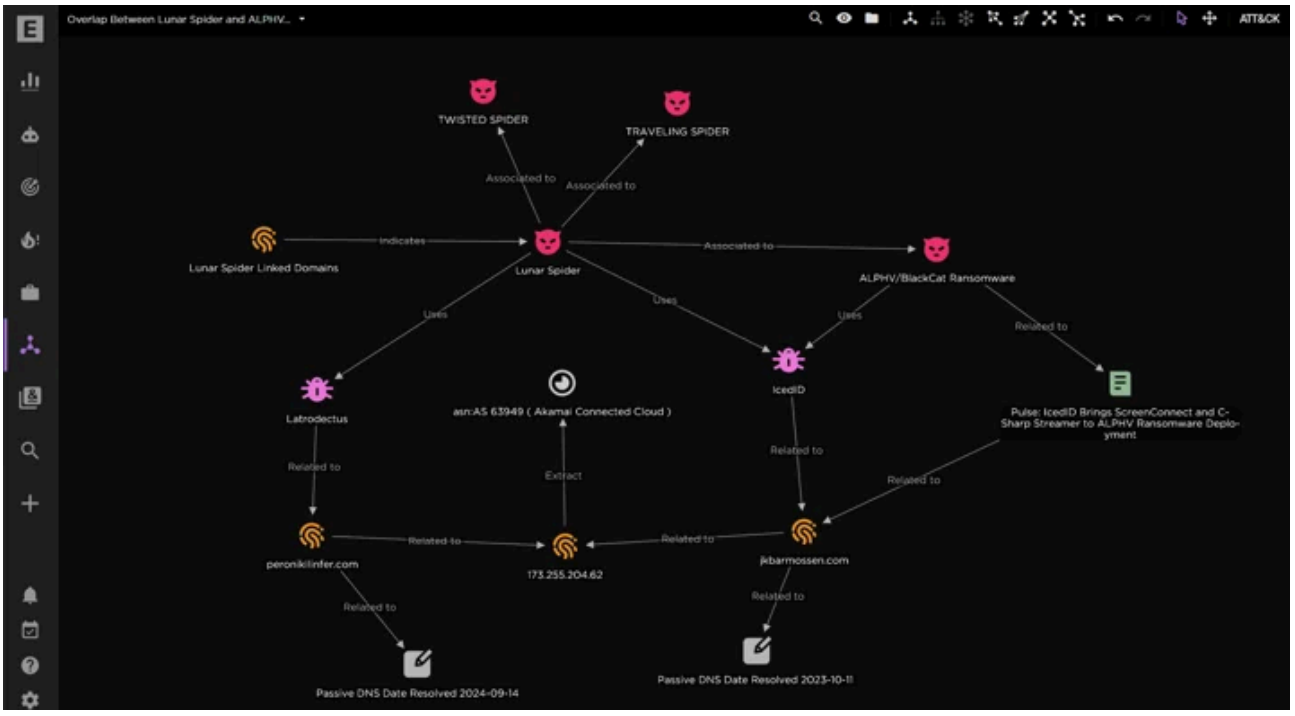

Figure 7 – Possible infrastructure sharing between LUNAR SPIDER and ALPHV/BlackCat Ransomware.

EclecticIQ analysts have uncovered evidence suggesting a very likely connection between LUNAR SPIDER and ALPHV/BlackCat ransomware affiliates. The domain peronikilinfer[.]com, which serves as a command-and-control (C2) server for Latrodectus malware in September 2024 - developed and managed by LUNAR SPIDER - was hosted on the IP address 173[.]255[.]204.[]62. In October 2023, ALPHV/BlackCat used another domain, jkbarmossen[.]com, also hosted on the same IP address and functioning as a C2 server for IcedID, another malware family developed and managed by LUNAR SPIDER. This overlapping use of the same infrastructures and malware usage emphasizes that both IcedID and Latrodectus are central to LUNAR SPIDER's operations. The shared infrastructure indicates that LUNAR SPIDER's malware is enabling ALPHV/BlackCat's ransomware activities, highlighting a collaborative relationship between these groups.

The reuse of infrastructure and overlapping command-and-control assets, evidenced by passive DNS records, reinforces the theory of coordination between LUNAR SPIDER and ALPHV/BlackCat. LUNAR SPIDER likely facilitated initial access through IcedID, which was then leveraged by ALPHV/BlackCat operators to deploy ransomware and exfiltrate sensitive data. These connections, supported by passive DNS evidence, highlight the operational synergy between the two groups, further bolstering the assessment of shared tactics, techniques, and infrastructure.

Latrodectus Malware Targets Financial Services via SEO Poisoning to Deliver Brute Ratel C4

EclecticIQ analysts observed a Latrodectus downloader variant in a SEO poisoning malvertising campaign against financial services to download and execute the Brute Ratel C4 malware. After execution of Brute Ratel C4, the malware communicates through the command-and-control server very likely owned by LUNAR SPIDER members and give them remote access to victim devices.

Figure 8 illustrates the attack flow of the malvertising campaign, which leveraged an SEO poisoning technique to deliver its payload. SEO poisoning involves manipulating search engine rankings to display malicious links prominently, tricking users into clicking them. In this case, victims searching for tax-related content on the Bing browser were redirected to download a malicious, obfuscated JavaScript file named Document-16-32-50.js.

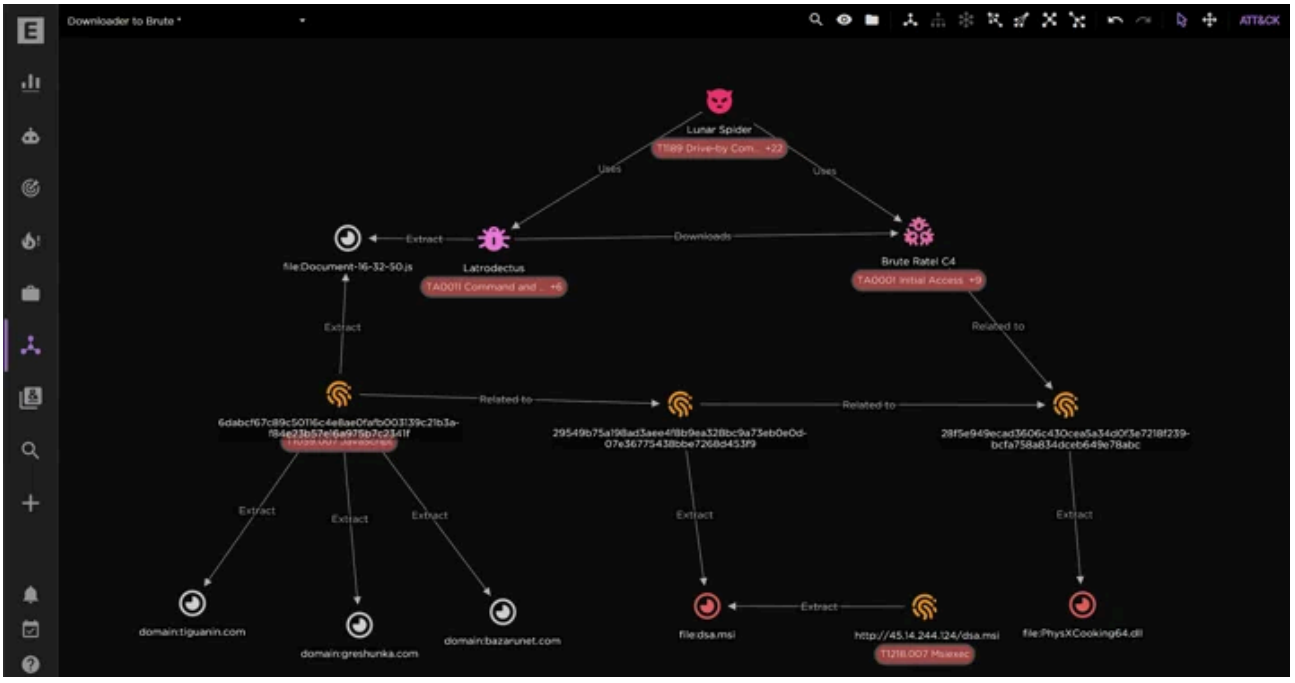

Figure 8 – Execution flow of the Latrodectus Malware.

Upon execution, the JavaScript file retrieved a Windows Installer (MSI) from a remote server, which installed the Brute Ratel malware. The MSI file, downloaded from 45[.]14[.]244[.]124/dsa.msi, executed via the rundll32.exe process, disguising the malicious DLL (vierm_soft_x64.dll) as a legitimate NVIDIA file.

Persistence Mechanism and Command & Control (C2):
To establish persistence, the malware created a registry key entry under:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

This enabled it to remain active even after system reboots. After installation, Brute Ratel made multiple connections to command and control (C2) servers controlled by the attackers, including bazarunet[.]com, greshunka[.]com, and tiguanin[.]com. These C2 servers facilitated communication between the compromised device and the attackers, allowing them to issue commands and control the infected system.

De-obfuscating the JavaScript File:
The malicious JavaScript file Document-16-32-50.js was obfuscated as part of the Latrodectus malware family. Analysts de-obfuscated the script and revealed its functionality (Figure 7). It was designed to download the MSI payload from the server, leading to the final stage of the infection.

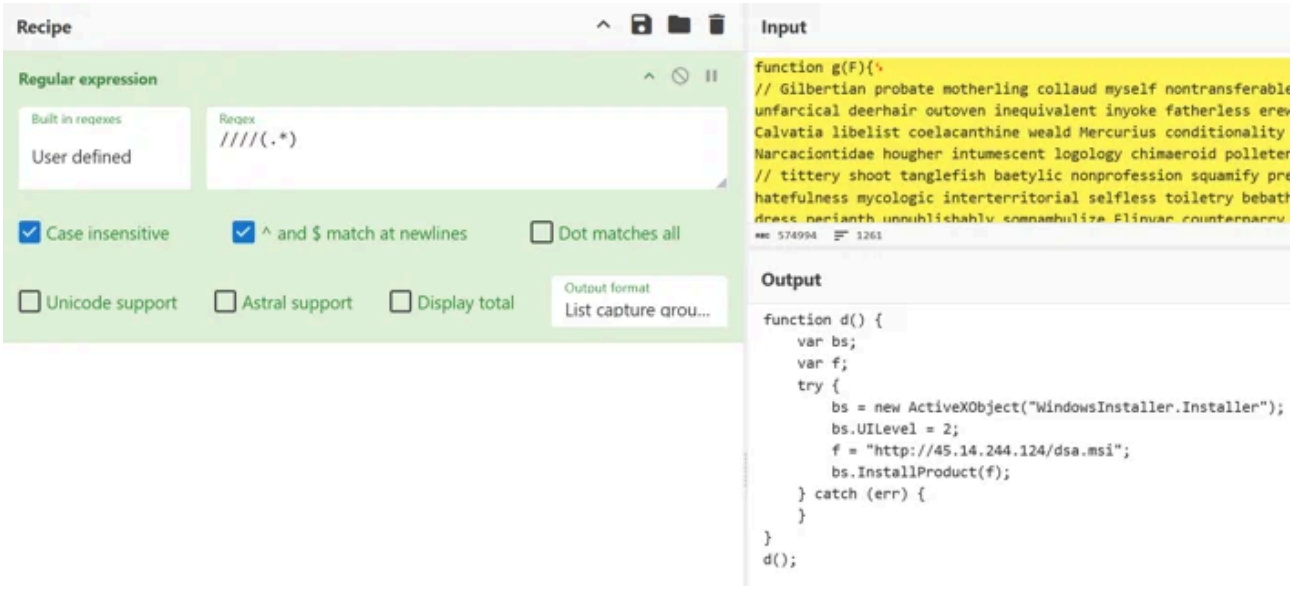

Figure 9 – De-obfuscated JavaScript file.

Once the MSI file was downloaded, it dropped Brute Ratel C4 in DLL format at the following location: C:\Users\<user-name>\AppData\Roaming\vierm_soft_x64.dll. The malware then executed via rundll32.exe, establishing communication with the attacker-controlled C2 servers to maintain control over the victim's device. These C2 servers are central to the attack, enabling further malicious activity or data exfiltration.

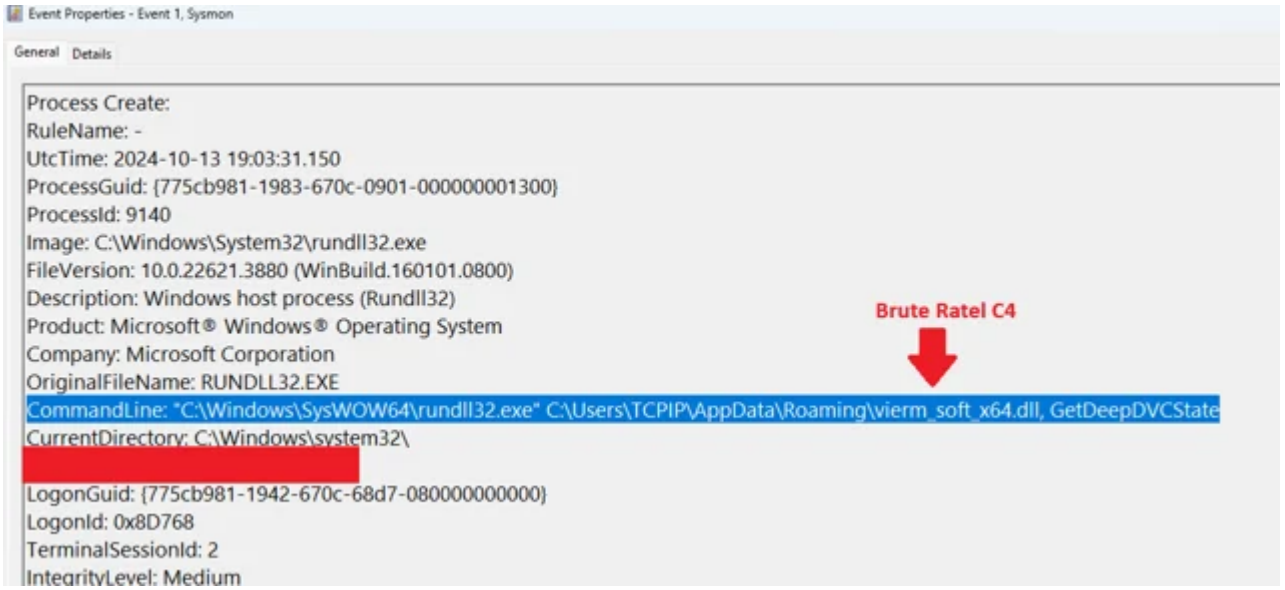

Figure 10 – Execution of the Brute Ratel C4 DLL in Sysmon Event Logs.

Analysts leveraged the MITRE ATT&CK Analysis Tool within the EclecticIQ Intelligence Center to map Lunar Spider's tactics, techniques, and procedures (TTPs). This mapping is crucial for defenders, as it helps identify the threat actor’s operational patterns. By understanding these techniques, security teams can build more effective detection and response strategies, enhancing their ability to prevent similar attacks.

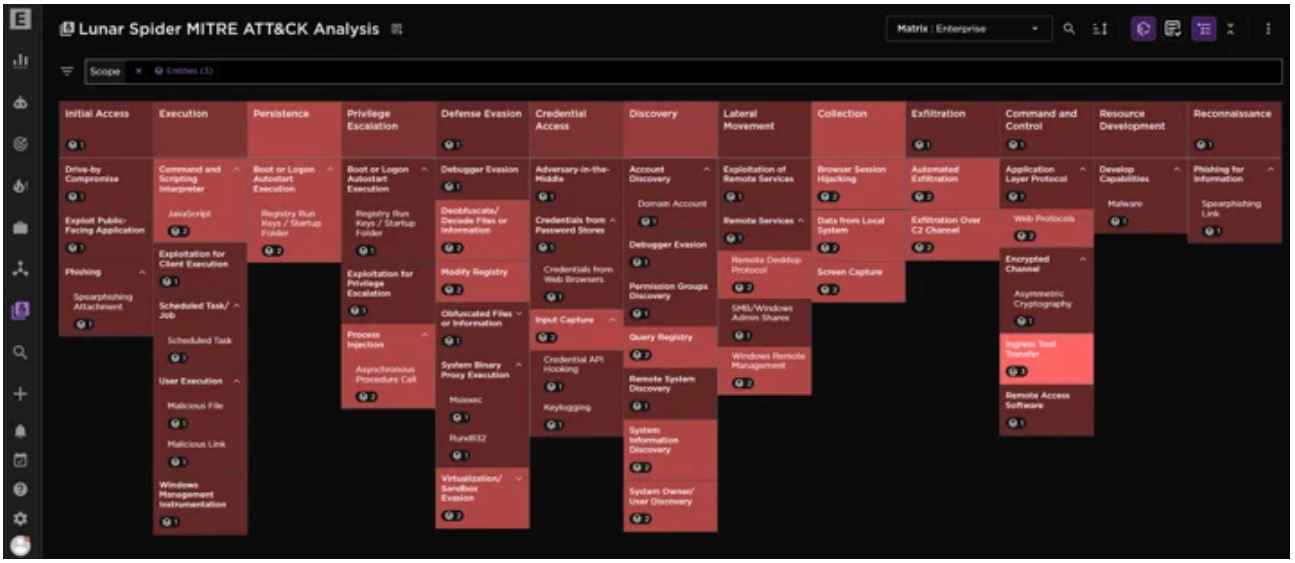

Figure 11 – Lunar Spider activates automaticity mapped to
EclecticIQ MITRE ATT&CK Analysis Tool.

In Figure 11, Intelligence Center's automatic mapping of Lunar Spider's TTPs to the EclecticIQ MITRE ATT&CK Analysis Tool showcases the power of intelligence-driven defense. This approach empowers defenders by providing clear insights into the adversary's behavior, enabling proactive threat hunting and mitigation efforts against the evolving threat landscape.

The Power of EclecticIQ Intelligence Center

- **Uncovering Hidden Connections:** Detecting previously unknown infrastructure and malware links between threat actors like LUNAR SPIDER and ALPHV/BlackCat using EclecticIQ threat graph views. This enables security teams to proactively disrupt coordinated cyber threats before they escalate.
- **Rapid Intelligence Gathering:** Aggregating intelligence and IOCs from diverse OSINT sources on LUNAR SPIDER's tools like IcedID and Latrodectus to deepen insights into their TTPs and infrastructure. This accelerates response times and enhances threat mitigation strategies, keeping organizations always one step ahead of attackers.
- **Strategic TTP Mapping:** Utilizing EclecticIQ's MITRE ATT&CK analysis tool to directly map LUNAR SPIDER's activities to the MITRE framework. This provides a clear understanding of their attack patterns, allowing organizations to develop better defenses against specific tactics used by the threat actor.
- **Automated Data Enrichment:** Leveraging automated enrichment features to pivot from known C2 servers and swiftly identify new attacker-controlled infrastructures. This reduces the window of exposure,

improves threat detection accuracy, and strengthens the overall security posture.

YARA Rules

```
rule CRIME_LOADER_Latrodectus_JS_LunarSpider_Oct2024_01
{
   meta:
      author = "Arda Buyukkaya, EclecticIQ"
      description = "Detects JavaScript files associated with the Latrodectus loader, also known as Lotus Loader, used to download MSI payloads. This activity is linked to the Lunar Spider crime group. The rule identifies specific patterns within JavaScript code indicative of malicious loader behavior."
      malware_family = "Latrodectus (Lotus Loader)"
      last_modified = "2024-10-15"
      tags = "loader, lotus, JavaScript, MSI, LunarSpider, Oct2024"

   strings:
      $x_installer_reference = "WindowsInstaller.Installer"
      $x_encoded_signature = "/ EGqk1paQjoH4fKsvtaNXM9JYe5QObQ+lkSYqs4NPcrGK\r\n// SIG // e2SS0PC0VV+WCxHl"

            // Grouped strings for drive checking and script execution flow
      $s_drive_check = "i < drives.length"
      $s_script_path = "filePath = WScript.ScriptFullName,"
      $s_script_buffer = "scriptBuffer = \""

      // Fallback patterns for JavaScript MSI execution
      $a_msiexec_keyword = {2F 2F 2F 2F 20 20 20 20 76 61 72 20 69 6E 73 74 61 6C 6C 43 6F 6D 6D 61 6E 64 20 3D 20 27 6D 73 69 65 78 65 63 2E 65 78 65}
      $a_comment_block = {2F 2F 2F 2F 20 20 20 20}

   condition:
      // The file must be larger than 256KB, and the following must hold:
      // 1. Either all primary detection strings are present.
      // 2. If no primary strings are found, fallback strings for JavaScript MSI must be present.
      filesize > 256000 and (
         (all of ($x_installer_reference, $x_encoded_signature) or all of ($s_drive_check, $s_script_path, $s_script_buffer)) or
         ($a_msiexec_keyword and $a_comment_block)
      )
}

rule MAL_LOADER_LunarSpider_Lotus_Aug2024_01
{
   meta:
```

```
        author = "Arda Buyukkaya - EclecticIQ"
        description = "Detects Lotus loader linked to Lunar Spider threat actor, observed in August 2024."
        last_modified = "2024-08-16"
        threat_actor = "Lunar Spider"
        malware_family = "Lotus Loader"
        tags = "loader, lotus, LunarSpider, August2024"

    strings:
        $x_debug_function = {e8 [4] 0f b6 40 02 48 83 c4 28}
        $x_process_environment_block = {65 48 8b 04 25 60 00 00 00 c3}
        $x_sleep_interval = {b9 58 02 00 00 f7 f1 8b c2 05 dc 05 00 00 69 c0 e8 03 00 00}

    condition:

        // Ensures the PE import hash matches and all specific detection patterns are present
        pe.imphash() == "db7aeb75528663639689f852fd366243"
        and all of ($x_debug_function, $x_process_environment_block, $x_sleep_interval)
}
```

Indicators of Compromise (IOCs)

Description	**Indicator**
Malvertising URL	https[://]qasertol[.]club/forms-pubs/about-form-w-2/?msclkid=58393294f21c1006efe854eff1b652d5 https[://]grupotefex[.]com/forms-pubs/about-form-w-4/?msclkid=275de1ee6e9c11cb920c879bf6a21339
Latrodectus JS file SH256	937d07239cbfee2d34b7f1fae762ac72b52fb2b710e87e02fa758f452aa62913 6dabcf67c89c50116c4e8ae0fafb003139c21b3af84e23b57e16a975b7c2341f fb242f64edbf8ae36a4cf5a80ba8f21956409b448eb0380949bb9152373db981
MSI Downloading URL	http[://]45[.]14[.]244[.]124/dsa[.]msi https[://]188[.]119[.]112[.]115/DLPAgent[.]msi http[://]188[.]119[.]113[.]152/CITROEN[.]msi http[://]193[.]32[.]177[.]192/vpn[.]msi http[://]188[.]119[.]112[.]7/das[.]msi http[://]95[.]164[.]17[.]212/BEST[.]msi
MSI files SHA256	1b9e17bfbd292075956cc2006983f91e17aed94ebbb0fb370bf83d23b14289fa ea1792f689bfe5ad3597c7f877b66f9fcf80d732e5233293d52d374d50cab991

	29549b75a198ad3aee4f8b9ea328bc9a73eb0e0d07e36775438bbe7268d453f9 c3f8ebc9cfb7ebe1ebbe3a4210753b271fecf73392fef98519b823a3e7c056c7
Latrodectus Malware C2	peronikilinfer[.]com opewolumeras[.]com eniloramesta[.]com restoreviner[.]com rilomenifis[.]com isomicrotich[.]com
Brute Ratel C4 SHA256	28f5e949ecad3606c430cea5a34d0f3e7218f239bcfa758a834dceb649e78abc 29549b75a198ad3aee4f8b9ea328bc9a73eb0e0d07e36775438bbe7268d453f9 c3f8ebc9cfb7ebe1ebbe3a4210753b271fecf73392fef98519b823a3e7c056c7 1b9e17bfbd292075956cc2006983f91e17aed94ebbb0fb370bf83d23b14289fa
Brute Ratel C4 C2 domains	tiguanin[.]com greshunka[.]com bazarunet[.]com obobobo[.]com sosachwaffen[.]com

---

Structured Data

Explore our TAXII collection to integrate valuable research into your security stack. Please note that access requires an API key or token. For guidance on how to obtain access and set up the feeds, visit our **support page.**

About EclecticIQ Intelligence & Research Team

EclecticIQ is a global provider of threat intelligence technology and services. Headquartered in Amsterdam, the EclecticIQ Intelligence & Research Team is made up of experts with decades of experience in cyber security and intelligence in industry and government.

We would love to hear from you. Please send us your feedback by emailing us at research@eclecticiq.com.

You might also be interested in

Ransomware in the Cloud: Scattered Spider Targeting Insurance and Financial Industries

EclecticIQ Intelligence Center 3.4 is here

ONNX Store: Phishing-as-a-Service Platform Targeting Financial Institution

References

[1] "Latrodectus: This Spider Bytes Like Ice | Proofpoint US," Proofpoint. Accessed: Oct. 15, 2024. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice

[2] "Brute Ratel C4 (Malware Family)." Accessed: Oct. 15, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.brute_ratel_c4

[3] "LUNAR SPIDER (Threat Actor)." Accessed: Oct. 15, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/actor/lunar_spider

[4] "IcedID (Malware Family)." Accessed: Jan. 29, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid

[5] "Alpha Spider (Threat Actor)." Accessed: Oct. 15, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/actor/alpha_spider

[6] "Operation Endgame." Accessed: Oct. 15, 2024. [Online]. Available: https://www.operation-endgame.com/

[7] "SmokeLoader (Malware Family)." Accessed: Oct. 15, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.smokeloader

[8] "Pikabot (Malware Family)." Accessed: Oct. 15, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.pikabot

[9] "BumbleBee (Malware Family)." Accessed: Oct. 15, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.bumblebee

[10] "Conti Ransomware Group Internal Chats Leaked | Rapid7 Blog," Rapid7. Accessed: Oct. 15, 2024. [Online]. Available: https://www.rapid7.com/blog/post/2022/03/01/conti-ransomware-group-internal-chats-leaked-over-russia-ukraine-conflict/

[11] "WIZARD SPIDER (Threat Actor)." Accessed: Oct. 15, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/actor/wizard_spider

[12] "TrickBot Malware | CISA." Accessed: Oct. 15, 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-076a

[13] "Conti Ransomware | CISA." Accessed: Oct. 15, 2024. [Online]. Available: https://www.cisa.gov/news-events/alerts/2021/09/22/conti-ransomware

[14] "Office of Public Affairs | Foreign National Pleads Guilty to Role in Cybercrime Schemes Involving Tens of Millions of Dollars in Losses | United States Department of Justice." Accessed: Oct. 15, 2024. [Online]. Available:

https://www.justice.gov/opa/pr/foreign-national-pleads-guilty-role-cybercrime-schemes-involving-tens-millions-dollars

[15] “Nemty (Malware Family).” Accessed: Oct. 15, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.nemty

[16] “TA2101 Plays Government Imposter to Distribute Malware | Proofpoint US,” Proofpoint. Accessed: Oct. 15, 2024. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us

[17] “IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment,” The DFIR Report. Accessed: Oct. 15, 2024. [Online]. Available: https://thedfirreport.com/2024/06/10/icedid-brings-screenconnect-and-csharp-streamer-to-alphv-ransomware-deployment/

[18] “Impacket - Red Canary Threat Detection Report,” Red Canary. Accessed: Oct. 15, 2024. [Online]. Available: https://redcanary.com/threat-detection-report/threats/impacket/

[19] “csharp-streamer RAT (Malware Family).” Accessed: Oct. 15, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.csharpstreamer

[20] M. T. Intelligence, “The many lives of BlackCat ransomware,” Microsoft Security Blog. Accessed: Oct. 15, 2024. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/
