SEPTEMBER 2023

# MONTHLY MALWARE DIGEST

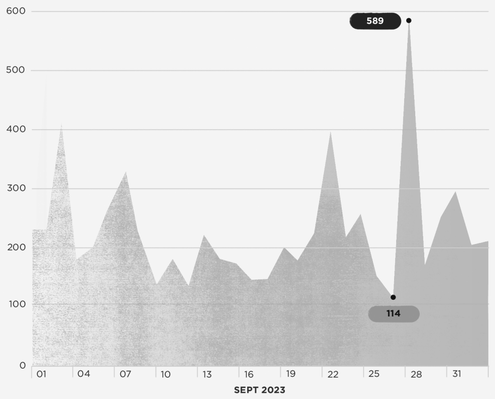
In this report, we highlight malware trends utilizing data from abuse.ch's open platforms. These collect, track and share resources relating to malware campaigns, including the URLs of malware distribution sites, malware samples, and indicators of compromise.

Each section will provide you with a detailed look at who and what data has been shared in the past month showing possible trends in malware operations.




## NUMBER OF SUBMISSIONS

The chart below documents the number of submissions (unique malware URLs) reported to URLhaus per day this month.




## TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

Community is at the heart of abuse.ch, so a special thanks to all those who report malware URLs. Those listed below have submitted the largest number of reports to URLhaus over this month.

| RANK | # OF REPORTS | % CHANGE | CONTRIBUTOR |
|---|---|---|---|
| 01 | 1,182 | — New entry | tolisec |
| 02 | 874 | -81.41 | geenensp |
| 03 | 470 | -89.34 | lrz_urlhaus |
| 04 | 412 | +285.05 | Cryptolaemus1 |
| 05 | 241 | New entry | onecert_ir |
| 06 | 235 | — New entry | abus3reports |
| 07 | 212 | +127.96 | JAMESWT_MHT |
| 08 | 207 | +38 | andretavare5 |
| 09 | 109 | +23.86 | Casperinous |
| 10 | 98 | — New entry | bryancampbell |
| 11 | 43 | -84.64 | Gootloader2 |
| 12 | 35 | — New entry | aubrey_eats_pie |
| 13 | 33 | — New entry | johnk3r |
| 14 | 32 | — New entry | cre4milk |

# ABOUT THE DATA

All the data in this report is provided by **abuse.ch**, a project committed to fighting abuse on the internet.

abuse.ch operates multiple community driven platforms which are open to everyone to both contribute and consume cyber threat intelligence data.

Security researchers, internet service providers and network operators trust in data provided by abuse.ch to protect their infrastructure from malware and botnet threats.

## HOW TO BECOME A CONTRIBUTOR

If you would like to contribute URLs of sites distributing malware, malware samples, IOCs or YARA files, then please go to the relevant platform and register by validating with a Twitter account.

Once you have proved to be a trustworthy contributor, you will then be invited to become a trusted member of the abuse.ch community.

| | |
|---|---|
| **URLhaus** | **MalwareBazaar** |
| https://urlhaus.abuse.ch | https://bazaar.abuse.ch |
| **ThreatFox** | **YARAify** |
| https://threatfox.abuse.ch | https://yaraify.abuse.ch |

## HOW TO CONSUME THE DATA

Currently, all data available via abuse.ch's platforms is free. Below are the links to the relevant APIs:

| | |
|---|---|
| **URLhaus** | **MalwareBazaar** |
| https://urlhaus.abuse.ch/api/ | https://bazaar.abuse.ch/api/ |
| **ThreatFox** | **YARAify** |
| https://threatfox.abuse.ch/api/ | https://yaraify.abuse.ch/api/ |

# URLHAUS

This platform focuses on collecting, tracking and sharing actionable threat intelligence on active malware distribution sites.

Trusted third parties, including security researchers, are continually reporting sites hosting malware to URLhaus. This community-led approach enables hosting companies and network owners to take rapid action on harmful content. Additionally, it provides organizations with actionable threat intelligence data to protect against malware threats.

Explore URLhaus

## ACTIVE MALWARE DISTRIBUTION SITES

**6,649**

**Malware sites** shared by security researchers on URLhaus

**-54%**

**decrease on** the previous month

**9,605**

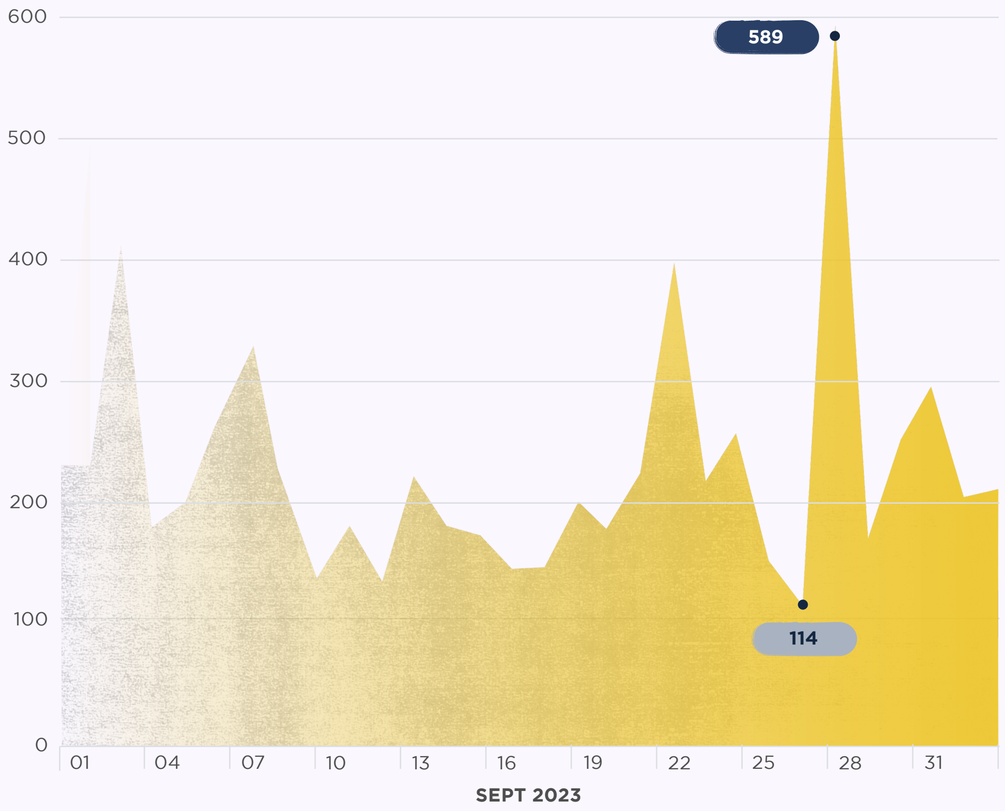
**Abuse reports** sent out to hosting providers and network owners

**86.1%**

of abuse reports **have been acted upon**

## NUMBER OF SUBMISSIONS

The chart below documents the number of submissions (unique malware URLs) reported to URLhaus per day this month.

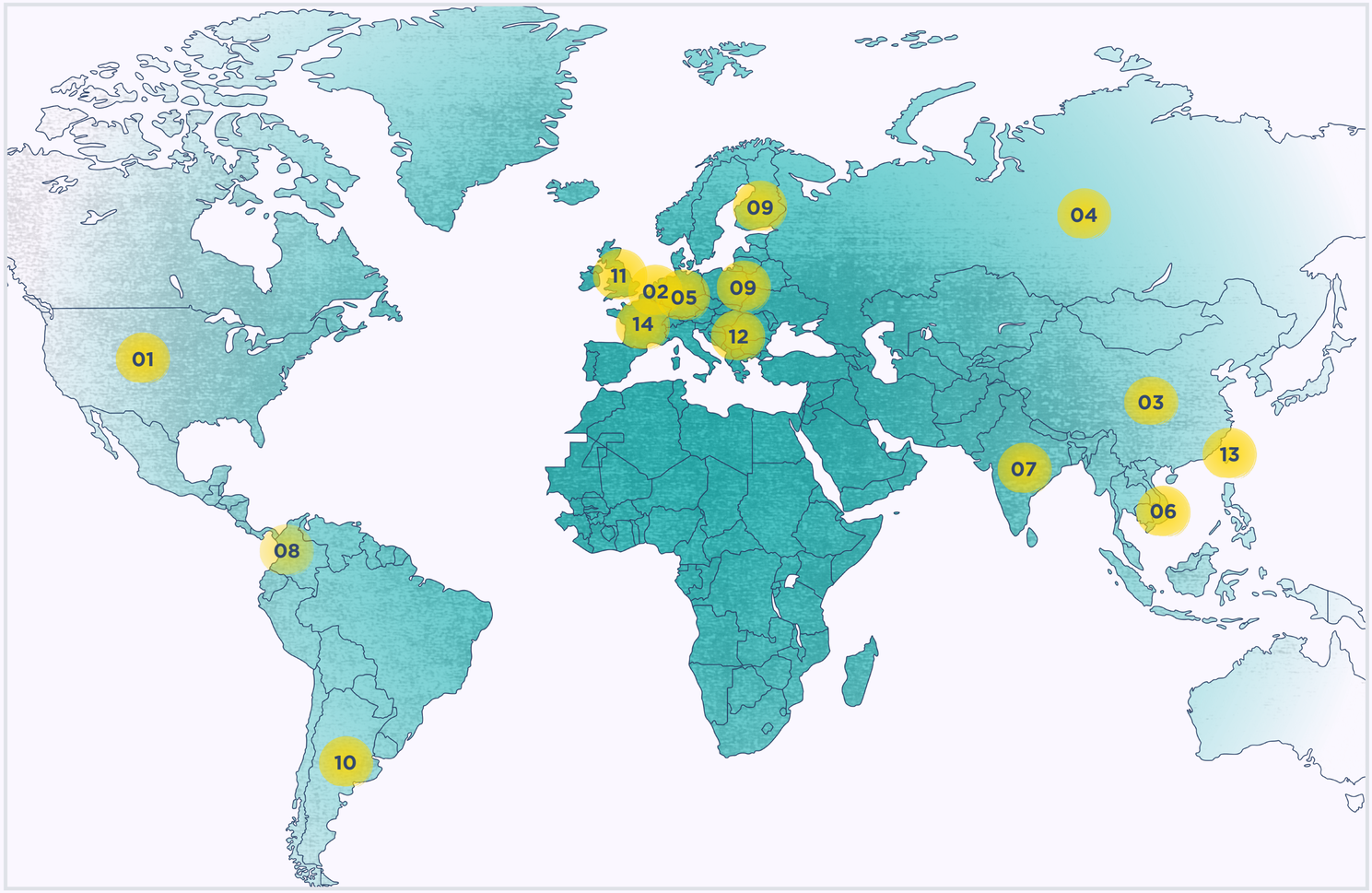



## TOP MALWARE DISTRIBUTION SITE CONTRIBUTORS

Community is at the heart of abuse.ch, so a special thanks to all those who report malware URLs. Those listed below have submitted the largest number of reports to URLhaus over this month.

| RANK | # OF REPORTS | % CHANGE | CONTRIBUTOR |
|---|---|---|---|
| 01 | 1,182 | — New entry | tolisec |
| 02 | 874 | -81.41 | geenensp |
| 03 | 470 | -89.34 | lrz_urlhaus |
| 04 | 412 | +285.05 | Cryptolaemus1 |
| 05 | 241 | — New entry | onecert_ir |
| 06 | 235 | — New entry | abus3reports |
| 07 | 212 | +127.96 | JAMESWT_MHT |
| 08 | 207 | +38.00 | andretavare5 |
| 09 | 109 | +23.86 | Casperinous |
| 10 | 98 | — New entry | bryancampbell |
| 11 | 43 | -84.64 | Gootloader2 |
| 12 | 35 | — New entry | aubrey_eats_pie |
| 13 | 33 | — New entry | johnk3r |
| 14 | 32 | — New entry | cre4milk |
| 14 | 32 | — New entry | vovaan |

## GEOLOCATION OF ACTIVE MALWARE DISTRIBUTION SITES




| RANK | # OF SITES | % CHANGE | COUNTRY |
|---|---|---|---|
| 01 | 1,975 | +47.50 | United States |
| 02 | 972 | +25.91 | Netherlands |
| 03 | 516 | -90.66 | China |
| 04 | 422 | -6.22 | Russia |
| 05 | 378 | -31.27 | Germany |
| 06 | 226 | +30.64 | Vietnam |
| 07 | 187 | -93.07 | India |
| 08 | 146 | New entry | Colombia |
| 09 | 135 | New entry | Finland |
| 09 | 135 | New entry | Lithuania |
| 10 | 133 | -68.71 | Argentina |
| 11 | 130 | New entry | United Kingdom |
| 12 | 100 | New entry | Hungary |
| 13 | 93 | -7.92 | Taiwan (PoC) |
| 14 | 84 | -56.25 | France |

## TOP NETWORKS HOSTING MALWARE DISTRIBUTION SITES

The following table shows the networks hosting the largest number of malware distribution sites this month.

| RANK | # OF URLs | AS NUMBER | ORGANIZATION NAME | COUNTRY |
|---|---|---|---|---|
| 01 | 760 | AS211252 | AS_DELIS | Netherlands |
| 02 | 397 | AS13335 | CLOUDFLARENET | United States |
| 03 | 309 | AS4837 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone | China |
| 04 | 181 | AS22612 | NAMECHEAP-NET | United States |
| 05 | 176 | AS36352 | AS-COLOCROSSING | United States |
| 06 | 173 | AS19557 | CHANGEIP-01 | United States |
| 07 | 166 | AS4134 | CHINANET-BACKBONE No.31,Jin-rong Street | China |
| 08 | 159 | AS47541 | VKONTAKTE-SPB-AS vk.com | Russia |
| 09 | 158 | AS9829 | BSNL-NIB National Internet Backbone | India |
| 10 | 154 | AS14061 | DIGITALOCEAN-ASN | United States |
| 11 | 128 | AS203727 | ALTAWK | Ukraine |
| 12 | 126 | AS10617 | SION S.A | Argentina |
| 13 | 125 | AS8075 | MICROSOFT-CORP-MSN-AS-BLOCK | United States |
| 14 | 122 | AS46606 | UNIFIEDLAYER-AS-1 | United States |
| 15 | 108 | AS209605 | HOSTBALTIC | Lithuania |

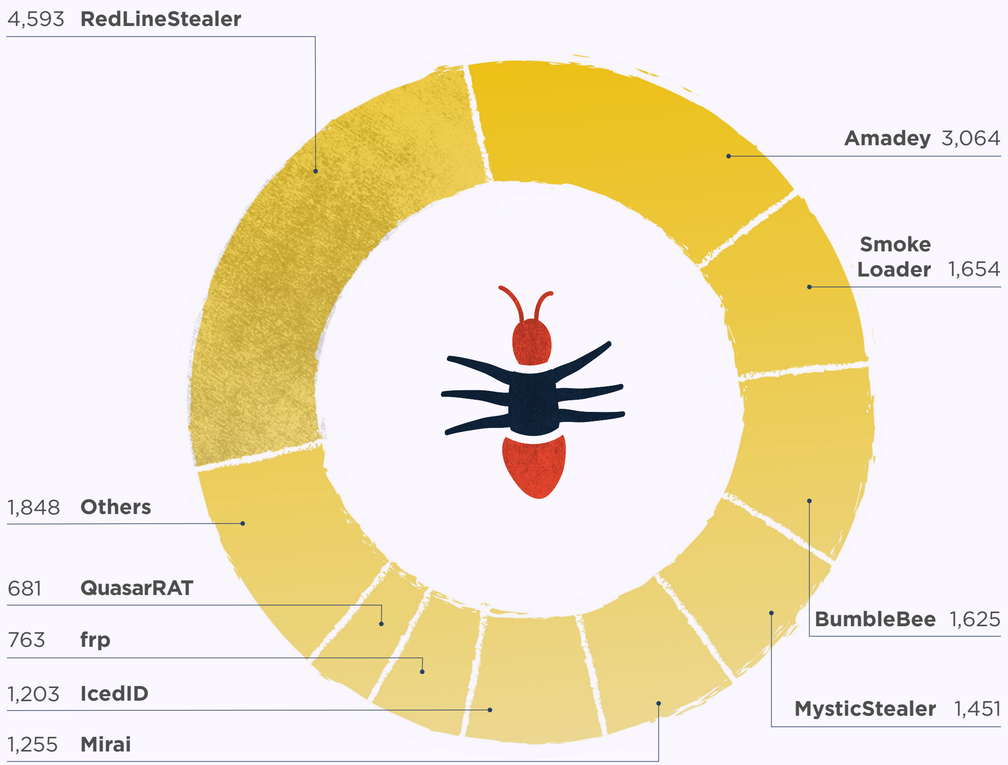
## TOP MALWARE HOSTS

The following table shows the details of the top malware hosts and their associated providers this month.

| RANK | # OF MALWARE SITES | HOST | PROVIDER | COUNTRY |
|---|---|---|---|---|
| 01 | 161 | vk.com | VK | Russia |
| 02 | 67 | wtools.io | n/a | null |
| 03 | 56 | cdn.discordapp.com | Discord | United States |
| 04 | 44 | pasteio.com | n/a | null |
| 05 | 23 | transfer.sh | n/a | null |
| 06 | 17 | filebin.net | n/a | null |

## TOP MALWARE FAMILIES ASSOCIATED WITH MALWARE SITES

This chart shows the malware families associated with the largest number of reported sites.




## TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

The following table shows the malware families that experienced the greatest percentage increases this month, compared to the previous one.

| RANK | MALWARE FAMILY | % CHANGE | LAST 3 MONTHS | # OF SAMPLES |
|---|---|---|---|---|
| 01 | Smoke Loader | +334.12 | | 1,654 |
| 02 | BumbleBee | +62.34 | | 1,625 |
| 03 | Fabookie | +41.67 | | 136 |
| 04 | RedLineStealer | +41.28 | | 4,593 |
| 05 | QuasarRAT | +40.99 | | 681 |
| 06 | Ransomware.Stop | +10.46 | | 602 |
| 07 | Amadey | -4.73 | | 3,064 |
| 08 | CoinMiner | -5.28 | | 233 |
| 09 | UACModuleSmokeLoader | -16.92 | | 216 |
| 10 | Mirai | -20.57 | | 1,255 |
| 11 | IcedID | -35.18 | | 1,203 |
| 12 | MysticStealer | New entry | | 1,451 |
| 12 | frp | New entry | | 763 |
| 12 | Backdoor.TeamViewer | New entry | | 360 |
| 12 | Stealc | New entry | | 301 |

# MALWARE BAZAAR

Through this platform security researchers and the wider industry can share, classify and hunt for confirmed malware samples.

The platform allows security researchers to hunt for malware samples by deploying custom hunting rules, e.g., using the power of vendor-based threat detections.

Explore MalwareBazaar

## MALWARE SAMPLES

**9,755**

**Malware samples** shared by security researchers on MalwareBazaar

**+1.8%**

**increase on** the previous month

**1,318**

**Active hunting rules**

**+0.3%**

**increase on** the previous month

**11.64MB**

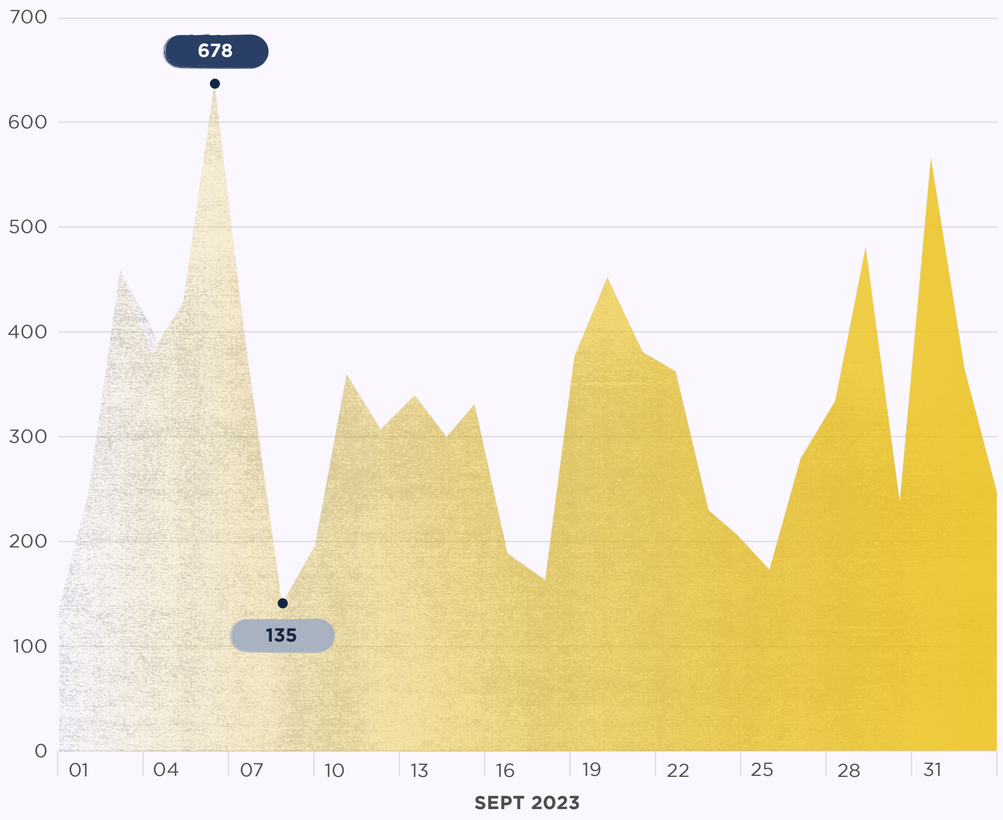
**Average size** of a malware sample

**EXE FILES**

Windows executables (exe) are the **top reported file types**

## MALWARE SAMPLES

The chart below shows the number of unique malware samples shared on MalwareBazaar per day this month.



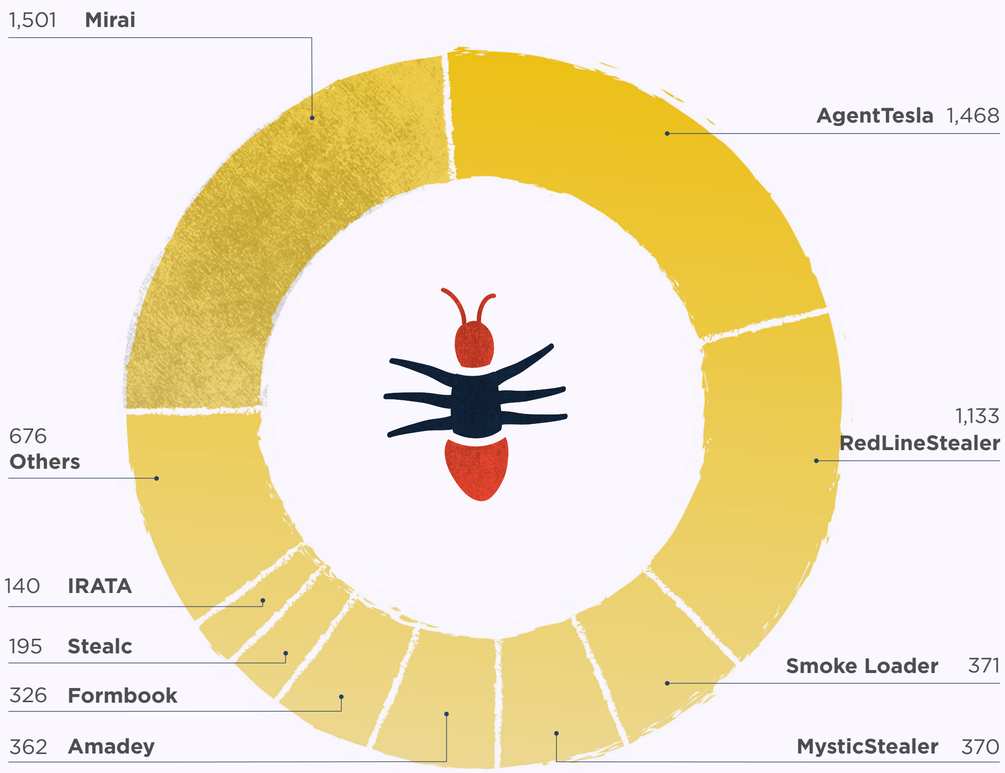

## TOP SAMPLE CONTRIBUTORS

Community is at the heart of abuse.ch, so a special thanks to all those who provide malware samples. Those listed below have submitted the largest number of samples to MalwareBazaar over this month.

| RANK | # OF MALWARE SAMPLES | % CHANGE | CONTRIBUTOR |
|---|---|---|---|
| 01 | 1,287 | +337.76 | @andretavare5 |
| 02 | 475 | New entry | @elfdigest |
| 03 | 466 | +146.56 | @JAMESWT_MHT |
| 04 | 428 | -16.89 | @cocaman |
| 05 | 398 | +36.30 | @lowmal3 |
| 06 | 213 | -14.11 | @adrian__luca |
| 07 | 204 | New entry | @r3dbU7z |
| 08 | 164 | New entry | @Turkeytmfounder |
| 09 | 136 | New entry | @onecert_ir |
| 10 | 131 | +43.96 | @TeamDreier |
| 11 | 101 | -25.19 | @smica83 |
| 12 | 91 | -18.02 | @malwarelabnet |
| 13 | 85 | +37.10 | @jstrosch |
| 14 | 84 | +18.31 | @Porcupine |
| 15 | 78 | New entry | @monitorsg |

## TOP MALWARE FAMILIES ASSOCIATED WITH SAMPLES SHARED

This chart shows the malware families that were associated with the largest number of samples.



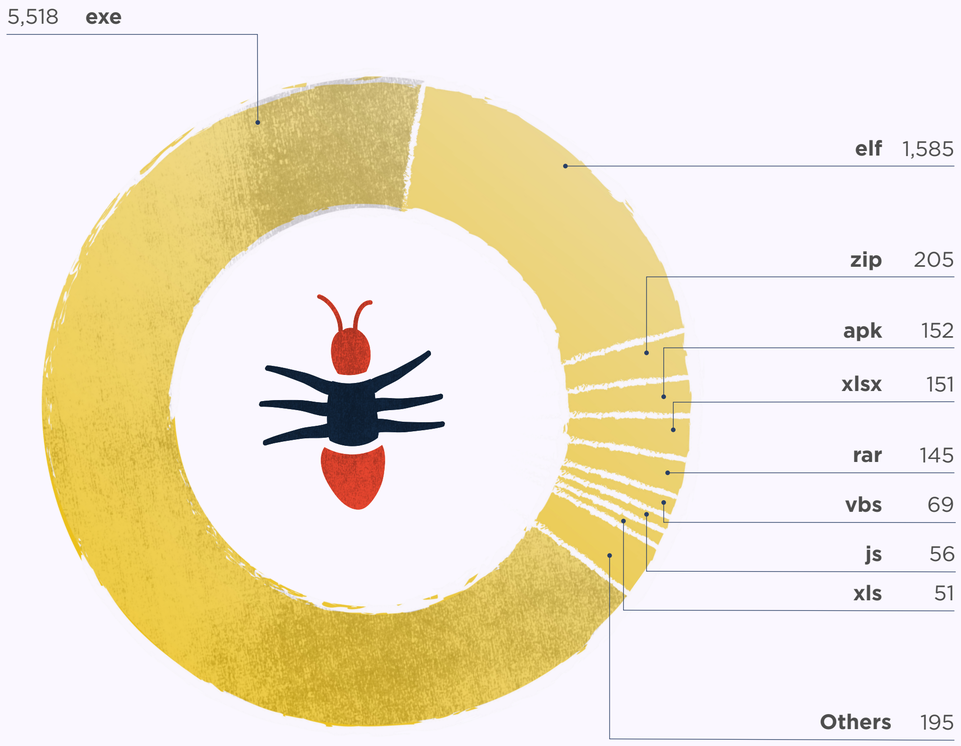

## TOP MALWARE FAMILIES - % CHANGE MONTH ON MONTH

The following table shows the malware families that experienced the greatest percentage increases this month, compared to the previous one.

| RANK | MALWARE FAMILY | % CHANGE | LAST 3 MONTHS | # OF SAMPLES |
|---|---|---|---|---|
| 01 | AsyncRAT | ^ +15.66 | | 96 |
| 02 | SnakeKeylogger | ^ +14.41 | | 135 |
| 03 | RedLineStealer | ^ +6.38 | | 1,133 |
| 04 | AgentTesla | v -3.36 | | 1,468 |
| 05 | RemcosRAT | v -7.14 | | 130 |
| 06 | Mirai | v -10.65 | | 1,501 |
| 07 | Formbook | v -30.49 | | 326 |
| 08 | Loki | vv -43.94 | | 111 |
| 09 | Amadey | vv -46.29 | | 362 |
| 10 | Smoke Loader | — New entry | | 371 |
| 10 | MysticStealer | — New entry | | 370 |
| 10 | Stealc | — New entry | | 195 |
| 10 | IRATA | — New entry | | 140 |
| 10 | DarkGate | — New entry | | 106 |
| 10 | Backdoor.TeamViewer | — New entry | | 98 |

## TOP FILE TYPES

This chart shows the most popular tags related to the reported IOCs.




## TOP MATCHING YARA RULES

Community is at the heart of abuse.ch, so a special thanks to all those who contribute. The following table lists the YARA rules and their authors associated with the largest number of samples submitted.

| RANK | # MALWARE SAMPLES | YARA RULE | AUTHOR |
|---|---|---|---|
| 01 | 2,799 | NET | malware-lu |
| 02 | 2,566 | DebuggerCheck__API | n/a |
| 03 | 1,780 | maldoc_find_kernel32_base_method_1 | Didier Stevens |
| 04 | 1,335 | NETexecutableMicrosoft | malware-lu |
| 05 | 782 | cobalt_strike_tmp01925d3f | The DFIR Report |
| 06 | 762 | linux_generic_ipv6_catcher | @_lubiedo |
| 07 | 730 | myMirai | n/a |
| 08 | 723 | MALWARE_Win_RedLine | ditekSHen |
| 09 | 652 | INDICATOR_EXE_Packed_ConfuserEx | ditekSHen |
| 10 | 620 | unixredflags3 | Tim Brown @ timb_machine |
| 11 | 524 | PE_Digital_Certificate | albertzsigovits |
| 12 | 508 | redline_stealer_1 | Nikolaos 'n0t' Totosis |
| 13 | 495 | detect_Redline_Stealer | Varp0s |
| 14 | 482 | win_smokeloader_a2 | pnx |
| 15 | 474 | ThreadControl__Context | n/a |

# THREATFOX

This platform enables organizations and security researchers to consume and contribute technical indicators connected to cyber attacks in a structured way. The shared indicators of compromise (IOCs) help others to detect potential cyber attacks within their environment.

Explore ThreatFox

## INDICATORS OF COMPROMISE (IOCs)

**27,379**

**Indicators of compromise (IOCS)** shared on ThreatFox

**+206.1%**

**increase on** the previous month

**5,129**

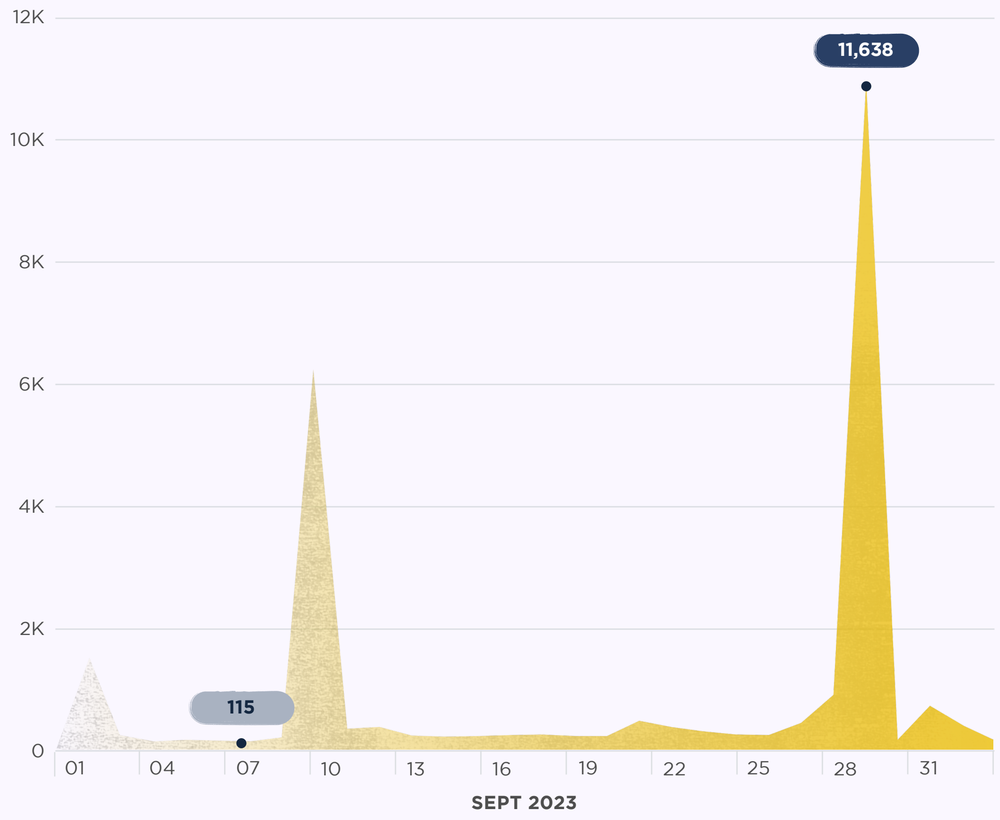
**IOCs relating** to NJRAT

**+2,149.56%**

**increase on** the previous month

## NUMBER OF IOCs SHARED PER DAY

The chart below shows the number of indicators of comprimise (IOCs) shared on ThreatFox per day this month.



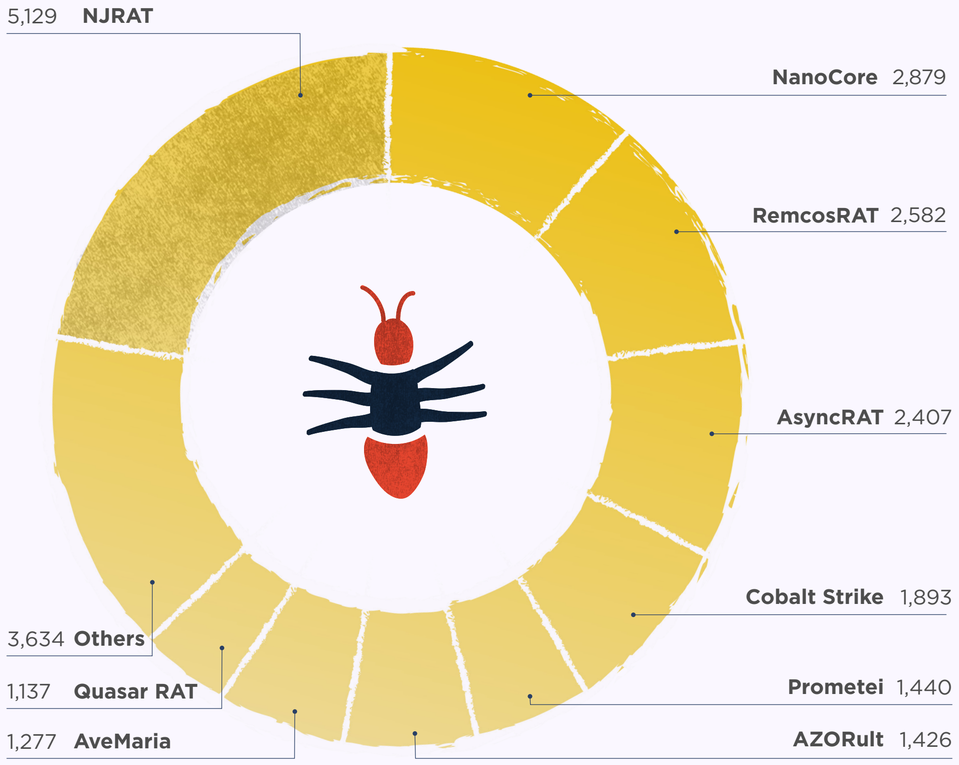

## IOC TYPE

An IOC can be a domain name, IP address, or file hash. The following table identifies and explains the most common IOC types reported this month.

| RANK | # OF IOCS | IOC TYPE | THREAT TYPE | EXPLANATION |
|---|---|---|---|---|
| 01 | 15,819 | domain | botnet_cc | Domain that is used for botnet Command&control (C&C) |
| 02 | 6,914 | ip:port | botnet_cc | ip:port combination that is used for botnet Command&control (C&C) |
| 03 | 3,319 | url | botnet_cc | URL that is used for botnet Command&control (C&C) |
| 04 | 546 | url | payload_ delivery | URL that delivers a malware payload |
| 05 | 473 | domain | payload_ delivery | Domain name that delivers a malware payload |
| 06 | 177 | md5_hash | payload | MD5 hash of a malware sample (payload) |
| 07 | 153 | sha256_ hash | payload | SHA256 hash of a malware sample (payload) |
| 08 | 22 | ip:port | payload_ delivery | ip:port combination that delivers a malware payload |

## TOP MALWARE FAMILIES

This chart shows the malware families that were associated with the largest number of IOCs this month.



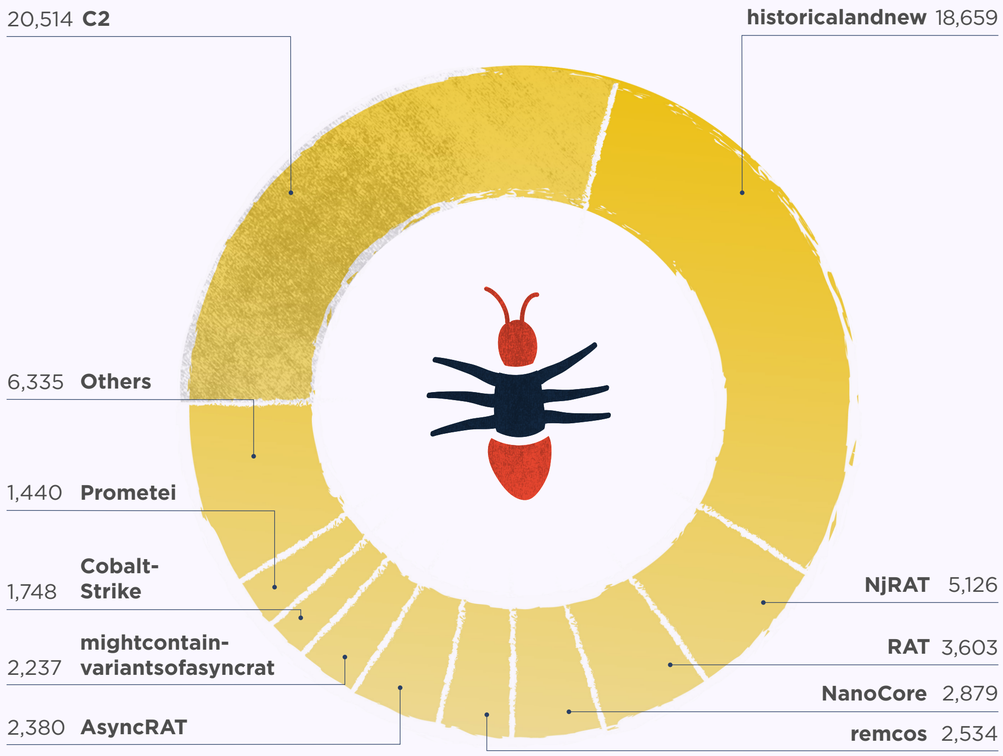

## TOP MALWARE FAMILIES - % CHANGES MONTH ON MONTH

The following table shows the malware families that experienced the greatest percentage increases this month, compared to the previous one.

| RANK | MALWARE FAMILY | % CHANGE | LAST 3 MONTHS | # OF IOCS |
|---|---|---|---|---|
| 01 | NJRAT | **+2,149.56** | | 5,129 |
| 02 | RemcosRAT | **+1,392.49** | | 2,582 |
| 03 | CryptBot | **+733.66** | | 842 |
| 04 | IRATA | **+574.07** | | 1,092 |
| 05 | IcedID | **+200.00** | | 501 |
| 06 | Cobalt Strike | **+3.33** | | 1,893 |
| 07 | Prometei | **-0.07** | | 1,440 |
| 08 | NanoCore | **New entry** | | 2,879 |
| 08 | AsyncRAT | **New entry** | | 2,407 |
| 08 | AZORult | **New entry** | | 1,426 |
| 08 | AveMaria | **New entry** | | 1,277 |
| 08 | Quasar RAT | **New entry** | | 1,137 |
| 08 | Gozi | **New entry** | | 533 |
| 08 | BitRAT | **New entry** | | 359 |
| 08 | Xworm | **New entry** | | 307 |

## TOP TAGS

Tags allow the contributer of an IOC to provide additional context about a threat. This chart shows the most popular tags used this month.




## TOP TAGS - % CHANGES MONTH ON MONTH

The following table shows the malware families that experienced the greatest percentage increases this month, compared to the previous one.

| RANK | MALWARE FAMILY | % CHANGE | # OF IOCS |
|---|---|---|---|
| 01 | RAT | **+1,280.46** | 3,603 |
| 02 | C2 | **+844.91** | 20,514 |
| 03 | DGA | **0.00** | 1,440 |
| 03 | Prometei | **-0.07** | 1,440 |
| 04 | CobaltStrike | **-4.17** | 1,748 |
| 05 | historicalandnew | **New entry** | 18,659 |
| 05 | NjRAT | **New entry** | 5,126 |
| 05 | NanoCore | **New entry** | 2,879 |
| 05 | remcos | **New entry** | 2,534 |
| 05 | AsyncRAT | **New entry** | 2,380 |
| 05 | mightcontainvariantsofasyncrat | **New entry** | 2,237 |
| 05 | AZORult | **New entry** | 1,426 |
| 05 | warzonerat | **New entry** | 1,260 |
| 05 | QuasarRAT | **New entry** | 1,123 |
| 05 | IRATA | **New entry** | 1,086 |

# YARAIFY

A platform for threat hunters and security researchers to be able to hunt for suspicious files using YARA. Additionally, this community-based platform allows users to share their own YARA rules in structured way.

[**YARA rules** are used to identify malware based on certain characteristics]

**Explore YARAify**

## YARAIFY STATISTICS

**3,008,981**

**File scans conducted** on YARAify

**2,530,996**

**Distinct files** that had scans performed on them

**+25.2%**

**increase in** file scans on the previous month

**+28.5%**

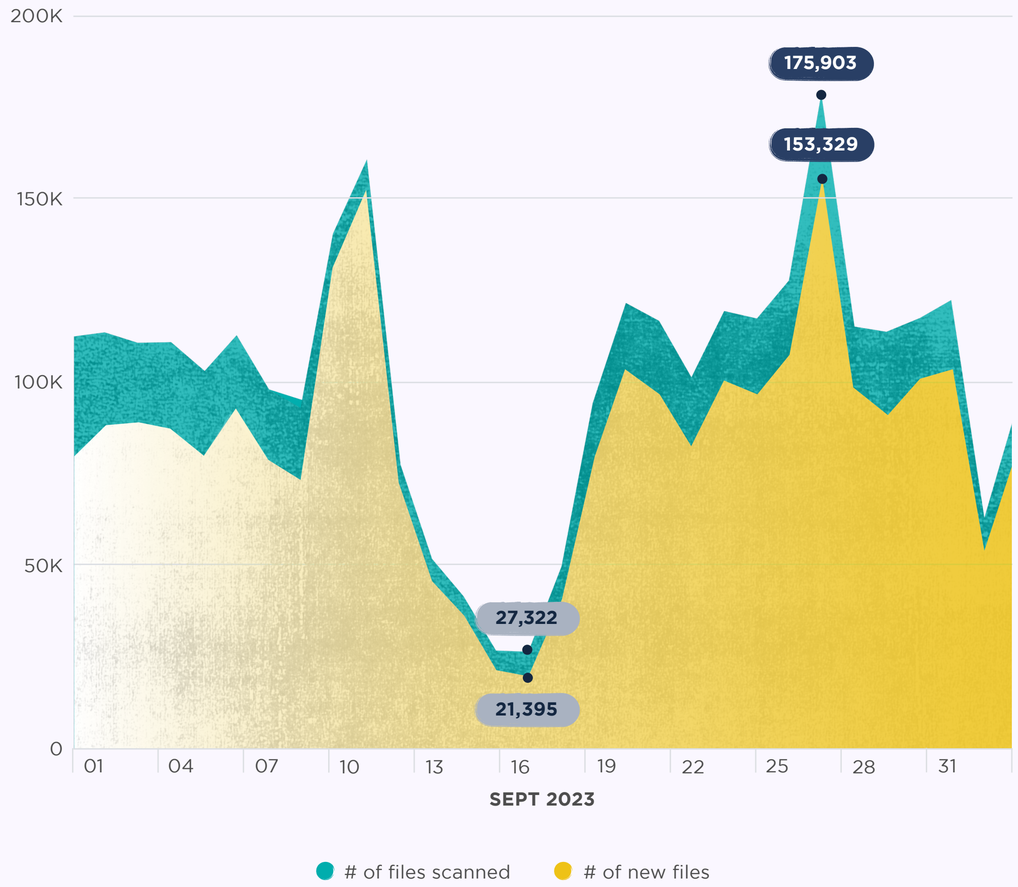
**increase in distinct** files on the previous month

**17,874**

**YARA rules deployed** on YARAify and available for hunting

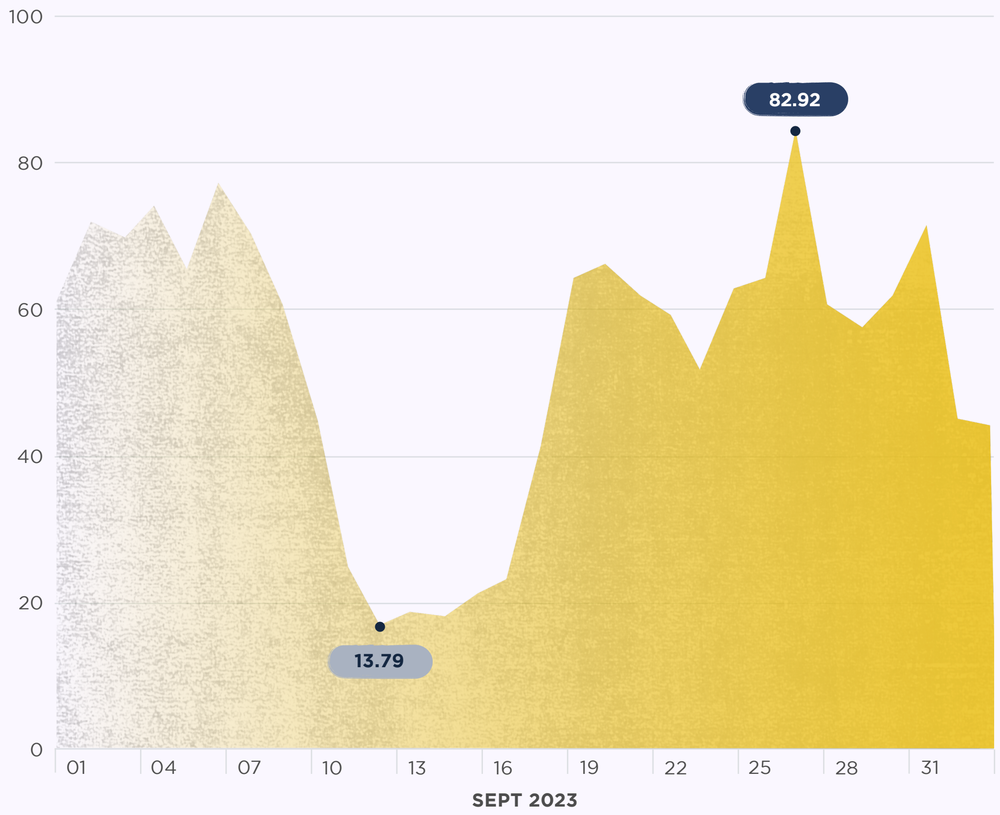
## FILES SCANNED PER DAY

The chart below shows the number of file scans conducted by YARAify this month.




## DATA SCANNED PER DAY

The chart below shows the amount of data scanned in gigabytes (GB) this month.



## TOP MATCHING YARA RULES

The following table lists the YARA rules and their authors associated with the largest number of files matched.

| RANK | # OF FILES MATCHED | % CHANGE | YARA RULE | AUTHOR |
|---|---|---|---|---|
| 01 | 1,208,227 | **+87.73** | maldoc_getEIP_method_1 | Didier Stevens |
| 02 | 310,315 | **-18.30** | DebuggerCheck__API | n/a |
| 03 | 227,157 | **New entry** | mal_rndwormie | Nikolaos 'n0t' Totosis |
| 04 | 212,840 | **+23.31** | NET | malware-lu |
| 05 | 184,839 | **-19.53** | UPXV200V290MarkusO-berhumerLaszloMolnar-JohnReiser | malware-lu |
| 06 | 179,579 | **-9.24** | maldoc_find_kernel32_base_method_1 | Didier Stevens |
| 07 | 168,287 | **-15.31** | UPXv20MarkusLaszloReiser | malware-lu |
| 08 | 111,335 | **-12.09** | RIPEMD160_Constants | phoul (@phoul) |
| 08 | 111,335 | **-12.09** | SHA1_Constants | phoul (@phoul) |
| 09 | 74,375 | **-32.60** | DebuggerException__SetConsoleCtrl | n/a |
| 10 | 74,183 | **-31.70** | MD5_Constants | phoul (@phoul) |
| 11 | 62,049 | **New entry** | SEH__vba | n/a |
| 12 | 56,356 | **-28.34** | Borland | malware-lu |
| 13 | 51,476 | **-30.41** | ThreadControl__Context | n/a |
| 14 | 49,916 | **-35.42** | Check_OutputDebugStringA_iat | n/a |

## TOP MATCHING CLAMAV SIGNATURES

The following table lists the Clam AntiVirus signatures that were used in the most tasks.

| RANK | TASK COUNT | % CHANGE | CLAMAV SIGNATURE |
|---|---|---|---|
| 01 | 959,186 | **+167.41** | PUA.Win.Packer.Lccwin-2 |
| 02 | 650,724 | **+169.44** | Win.Trojan.Obfus-38 |
| 03 | 482,142 | **+211.71** | Win.Trojan.Qukart-6874817-0 |
| 04 | 275,765 | **+165.84** | Win.Trojan.Padodor-9877164-0 |
| 05 | 231,977 | **+189.71** | Win.Malware.Qukart-6838239-0 |
| 06 | 212,608 | **+76.51** | Win.Trojan.Crypted-30 |
| 07 | 211,909 | **+75.92** | Win.Trojan.Crypted-29 |
| 08 | 102,259 | **+91.90** | Win.Trojan.Crypted-28 |
| 09 | 93,499 | **-24.19** | Win.Malware.Dqqw-9951425-0 |
| 10 | 93,381 | **-23.82** | Win.Trojan.QQPass-5710308-0 |
| 10 | 93,381 | **-23.82** | Win.Malware.Zusy-6804618-0 |
| 11 | 76,660 | **+55.78** | Win.Trojan.Crypted-31 |
| 12 | 55,469 | **+33.31** | Win.Packed.Lazy-10005437-0 |
| 13 | 55,273 | **+35.37** | Win.Trojan.Berbew-9845290-1 |
| 14 | 41,527 | **+63.26** | Win.Trojan.Qbot-10002723-0 |

SPAMHAUS ABUSE|ch

# LOOK OUT FOR THE NEXT MALWARE DIGEST EARLY IN NOVEMBER

Remember, sharing is caring.